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

Հատոր Том Volume 122 2022 № 3

APPLIED MATHEMATICS

УДК 510.64
DOI: 10.54503/0321-1339-2022.122.3-182

A. A. Chubaryan

Relations between the Proof Complexities in Frege Systems, Deep-Inference Proof Systems KS and eKS

(Submitted by academician Yu. H. Shoukourian 4/VIII 2022)

Keywords: *deep-inference system, Frege system, determinative size of formula, exponential speed-up.*

Introduction. Traditionally, proof theory has been concerned with formal representations of the notion of proof as it occurs in mathematics or other intellectual activities, but the rapid development of computer science has brought about a dramatic change of attitude. Efficiency has become a primary concern and this fact has given rise to a whole new area of research in which the considerations of complexity playing a major role. Open questions of theoretical computer science like P =?NP and NP =?co-NP have tight connection with the proof complexities in the field of propositional logic [1].

Deep inference is a relatively new methodology in proof theory, consisting in dealing with proof systems whose inference rules are applicable at any depth inside formulae [2-4]. While the inference rules of well known sequent calculus or natural deductions decompose formulas along their main connectives, deep inference rules are allowed to do arbitrary rewriting inside formulas. The main interesting results about the proof complexity of deep inference are 1) some deep-inference proof systems (SKS) is as powerful as Frege ones; 2) there is deep-inference proof systems (KS) that exhibit an exponential speed-up over cut-free Gentzen proof systems; 3) Frege systems and some deep-inference system eKS polynomially simulate the system KS. The reverse relations are pointed in [2] as open problems. It is proved here that a Frege system and the system eKS have an exponential speed-up over the system KS.

2. Preliminaries. To prove our main result, we recall some notions and notations from [1-4]. We will use the current concepts of the unit Boolean cube (E^n), a propositional formula, a tautology, a proof system for propositional logic and proof complexities. The language of considered systems contains the propositional variables, logical connectives $\neg, \&, \vee$ and parentheses (,). Note that some parentheses can be omitted in generally accepted cases. For the sake of simplicity, we consider only formulas in negation normal form. More precisely, formulas are generated from a countable set of propositional variables and their negations via the binary connectives & and ∨.

2.1. Considered proof systems and proof complexities. The inference rules of system KS (original CoS – *calculus of structures*) are

$$\boldsymbol{ai}\downarrow\frac{\boldsymbol{F}\{\boldsymbol{B}\}}{\boldsymbol{F}\{\boldsymbol{B}\&[\neg\boldsymbol{a}\vee\boldsymbol{a}]\}}\quad \mathbf{s}\frac{\boldsymbol{F}\{\boldsymbol{A}\&[\boldsymbol{B}\vee\boldsymbol{C}]\}}{\boldsymbol{F}\{(\boldsymbol{A}\&\boldsymbol{B})\vee\boldsymbol{C}\}}\quad \mathbf{w}\downarrow\frac{\boldsymbol{F}\{\boldsymbol{B}\}}{\boldsymbol{F}\{\boldsymbol{B}\vee\boldsymbol{A}\}}\quad \boldsymbol{ac}\downarrow\frac{\boldsymbol{F}\{\boldsymbol{a}\vee\boldsymbol{a}\}}{\boldsymbol{F}\{\boldsymbol{a}\}}$$

$$\mathbf{m}\frac{\boldsymbol{F}\{(\boldsymbol{A}\&\boldsymbol{B})\vee(\boldsymbol{C}\&\boldsymbol{D})\}}{\boldsymbol{F}\{[\boldsymbol{A}\vee\boldsymbol{C}]\&[\boldsymbol{B}\vee\boldsymbol{D}]\}}, \tag{1}$$

where $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, and $\boldsymbol{D}$ must be seen as formula variables, and $\boldsymbol{a}$ is a propositional variable or its negation and $\boldsymbol{F}\{\mathbf{E}\}$ means that **E** is some subformula in $\boldsymbol{F}$. These rules are called *(atomic) identity*, *switch*, *weakening*, *(atomic) contraction*, and *medial*, respectively. The rules in (1) are written in the style of inference rule schemes in proof theory but they behave as rewrite rules in term rewriting, i.e., they can be applied *deep* inside any (positive) formula context.

In order to obtain proofs without hypotheses, we need an axiom, which is in our case just a variant of the rule ai↓:

$$\boldsymbol{ai}\downarrow\frac{}{\neg\boldsymbol{a}\vee\boldsymbol{a}}.$$

A proof in KS uses the axiom exactly once.

The system eKS (sKS) is obtained from the system KS by adding the specific *extension* (*substitution*) inference rule [3].

A **Frege system** $\mathcal{F}$ uses a denumerable set of propositional variables, a finite, complete set of propositional connectives; $\mathcal{F}$ has a finite set of inference rules defined by a figure of the form $\frac{A_1A_2\ldots A_m}{B}$ (the rules of inference with zero hypotheses are the axioms schemes); $\mathcal{F}$ must be sound and complete, i.e., for each rule of inference $\frac{A_1A_2\ldots A_m}{B}$ every truth-value assignment, satisfying $A_1A_2\ldots A_m$, also satisfies B, and $\mathcal{F}$ 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 $l^{\Phi}(\varphi)$ ($t^{\Phi}(\varphi)$).

Let Φ_1 and Φ_2 be two different proof systems.

Definition 2.1.1. The system Φ_1 *p-l-simulates (p-t-simulates)* the system Φ_2 if there exist the polynomial *p()* such, that for each formula φ provable both in the systems Φ_1 and Φ_2, we have

$l^{\Phi 1}(\varphi) \leq p(l^{\Phi 2}(\varphi))$ $(t^{\Phi 1}\, t(\varphi) \leq p(t^{\Phi 2}(\varphi)))$.

Definition 2.1.2. The systems Φ_1 and Φ_2 are *p-l-equivalent (p-t-equivalent),* if systems Φ_1 and Φ_2 *p-l-simulate (p-t-simulate)* each other.

It is well-known that any two Frege systems are *p-l*-equivalent (*p-t*-equivalent) [1].

It is proved in [3] that

- Frege systems *p-l-simulate (p-t-simulate)* the system KS,
- the system eKS *p-l-simulates (p-t-simulates)* both the systems KS and sKS.

Definition 2.1.3. If for some sequence of formulas φ_n in the two systems ϕ_1 and ϕ_2 for sufficiently large n is valid $t^{\phi_1}(\varphi_n) = \Omega(2^{t^{\phi_2}(\varphi_n)})$ $(l^{\phi_1}(\varphi_n) = \Omega(2^{l^{\phi_2}(\varphi_n)}))$, then we say that the system ϕ_2 has exponential sped-up by lines (by sizes) over the system ϕ_1.

2.2. Determinative size of formulas. 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 [5] the following notions were introduced.

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

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

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 $\boldsymbol{\varphi}$ be a propositional formula, let $P = \{p_1, p_2, \ldots, p_n\}$ be the set of the variables of $\boldsymbol{\varphi}$, and let $P' = \{p_{i_1}, p_{i_2}, \ldots, p_{i_m}\}$ $(1 \leqslant m \leqslant n)$ be some subset of P.

Definition 2.2.1. Given $\sigma = \{\sigma_1, \ldots, \sigma_m\} \in E^m$, the conjunct $K^\sigma = \{p_{i_1}^{\sigma_1}, p_{i_2}^{\sigma_2}, \ldots, p_{i_m}^{\sigma_m}\}$[1)] is called ***φ**-determinative* if assigning σ_j $(1 \leqslant j \leqslant m)$ to each p_{ij} and successively using replacement-rules we obtain the value of $\boldsymbol{\varphi}$ (0 or 1) independently of the values of the remaining variables.

Definition 2.2.2. We call the minimal possible number of variables in a $\boldsymbol{\varphi}$-1-determinative conjunct the *determinative size of* $\boldsymbol{\varphi}$ and denote it by $ds(\boldsymbol{\varphi})$.

A tautology is called *minimal* if it can not be obtained by some substitution in a shorter tautology.

It is proved in [5] that

1) if for some minimal tautology $\boldsymbol{\varphi}$ $ds(\boldsymbol{\varphi})$=m, then the number of $\boldsymbol{\varphi}$-1-determinative conjuncts is at least $\mathbf{2^m}$;

2) if for some minimal tautology $\boldsymbol{\varphi}$ there is such $\boldsymbol{m}$ that every conjunct with $\boldsymbol{m}$ literals is $\boldsymbol{\varphi}$-1-determinative, then the number of $\boldsymbol{\varphi}$-1-determinative conjuncts is no more than $\mathbf{2}^{\boldsymbol{m}}$.

Note that every subformula is formula ones, hence above definitions are applicable to subformulas as well.

By $|\boldsymbol{\varphi}|$ we denote the *size of a formula* $\boldsymbol{\varphi}$, defined as the number of all propositional variables entries in it. If formula is given in negative normal form, then it is obvious that the full size of a formula, which is understood to be the number of all symbols is bounded by some linear function in $|\boldsymbol{\varphi}|$.

3. Main formulas. Before we shall prove the main theorems, we must give some auxiliary results.

3.1. In some papers in area of propositional proof complexity for classical logic the following tautologies (Topsy-Turvy Matrix) play key role

$$TTM_{n,m} = \vee_{(\sigma_1,\ldots,\sigma_n)\in E^n} \&_{j=1}^{m} \vee_{i=1}^{n} p_{ij}^{\sigma_i} \quad (n \geq 1,\ 1 \leq m \leq 2^n\text{-}1).$$

For all fixed $\boldsymbol{n} \geq \mathbf{1}$ and $\boldsymbol{m}$ in above indicated intervals every formula of this kind expresses the following true statement: given a 0,1- matrix of order $\boldsymbol{n} \times \boldsymbol{m}$ 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.

For the below given Theorem 1. the main tautologies of our consideration are $\boldsymbol{\varphi_n}=TTM_{n,\,\mathbf{2}^{\boldsymbol{n}}-\mathbf{1}}$.

It is not difficult to see that $|\boldsymbol{\varphi_n}|=n(2^n\text{-}1)2^n$, $ds(\boldsymbol{\varphi_n})=2^n\text{-}1$ and number of different $\boldsymbol{\varphi_n} - \mathbf{1} - \mathbf{determinative}$ conjncts is $\mathbf{2}^{\mathbf{2}^{\boldsymbol{n}}\text{-}1}$.

3.2. **Balanced formulas.** A formula **A** is balanced if every propositional variable occurring in **A** occurs exactly twice, once positive and once negated. For the below given Theorem 2. the main tautologies of our consideration are the balanced tautologies $\mathbf{QHQ_n}= \vee_{0\leq i\leq n} \&_{1\leq j\leq n}[\vee_{\mathbf{1\leq k\leq i}} \overline{\mathbf{q}}_{\mathbf{i,j,k}} \vee \vee_{\mathbf{i<\boldsymbol{k}\leq \boldsymbol{n}}} \mathbf{q}_{\mathbf{k,j,i+1}}]$ $(n \geq \mathbf{1})$. Put $\boldsymbol{Q_{i,j}} = \vee_{\mathbf{1\leq k\leq i}} \overline{\mathbf{q}}_{\mathbf{i,j,k}} \vee \vee_{\mathbf{i<\boldsymbol{k}\leq \boldsymbol{n}}} \mathbf{q}_{\mathbf{k,j,i+1}}$ $(n \geq \mathbf{1},\ \mathbf{0 \leq i \leq n},\ \mathbf{1 \leq j \leq n})$, then $\mathbf{QHQ_n} = \vee_{\mathbf{0\leq i\leq n}} \left(\boldsymbol{Q_{i1}} \& \boldsymbol{Q_{i2}} \& \ldots \& \boldsymbol{Q_{ij}} \& \ldots \& \boldsymbol{Q_{i(n-1)}} \& \boldsymbol{Q_{in}}\right)$ and hence $ds(\mathrm{QHQ_n})=n$, therefore the number of $\mathbf{QHQ_n}$ -1-determinative conjuncts is at least $\mathbf{2}^{\boldsymbol{n}}$. It is also not difficult to see, that $|\,\mathbf{QHQ_n}\,|= \frac{\mathbf{3n^2(n+1)}}{\mathbf{2}} - \mathbf{1}$.

4.Main results.

Theorem 1. *Every Frege system has exponential speed-up over the system KS.*

Proof is founded on the two following propositions:

1) Frege-proofs of tautologies φ_n $(n \geq 1)$ are *t*-polynomially (*l*-polynomially) bounded (this statement is proved in [6]);
2) for sufficiently large n and sequence of formulas φ_n the following holds: $t^{KS}(\varphi_n) = \Omega(2^{2^n})$, therefore $l^{KS}(\varphi_n) = \Omega(2^{2^n})$ as well.

   The proof of second statement follows from the values of determinative sizes of φ_n and number of different $\varphi_n - 1 - \text{determinative}$ conjuncts, as well from possible changes of determinative sizes by applications of inference rules of KS:

$$\mathrm{ds}(\neg a \lor a)=1, \quad \mathrm{ds}(B\&[\neg a \lor a]) \le \mathrm{ds}(B)+1,$$
$$\mathrm{ds}([(A\&B) \lor \mathrm{C}]) \le \mathrm{ds}((\mathrm{A}\&[B \lor \mathrm{C}]), \quad \mathrm{ds}(B \lor A) \le \mathrm{ds}(B),$$
$$\mathrm{ds}(a) = \mathrm{ds}(a \lor a), \quad \mathrm{ds}([\mathrm{A}\lor \mathrm{C}] \&[B \lor \mathrm{D}]) \le \mathrm{ds}(A\&B \lor \mathrm{C}\&D),$$

and some important condition of rule **s**.

Theorem 2. *The system eKS has exponential speed-up over the system KS.*

Proof is founded on the following propositions:

1) sKS-proofs of of tautologies $\mathbf{QHQ_n}$ ($\mathrm{n} \ge \mathbf{1}$) are *t*-polynomially (*l*-polynomially) bounded (this statement is proved in [3]);
2) the system eKS *p-l-simulates (p-t-simulates)* the system sKS [3].
3) for sufficiently large n and sequence of formulas $\mathbf{QHQ_n}$ the following holds: $\boldsymbol{t^{KS}}(\mathbf{QHQ_n}) = \boldsymbol{\Omega}(\mathbf{2}^{\boldsymbol{n}})$, therefore $\boldsymbol{l^{KS}}(\mathbf{QHQ_n}) = \boldsymbol{\Omega}(\mathbf{2}^{\boldsymbol{n}})$ as well.

The proof of last statement follows from the values of determinative sizes of $\mathbf{QHQ_n}$ and number of different $\mathbf{QHQ_n}$ -1-determinative conjuncts.

Remark. Both theorems can proved only on the base of formulas $\mathbf{QHQ_n}$ because it is proved that they have *t*-polynomially (*l*-polynomially) bounded Frege-proofs (this statement is proved in one of my previous paper, which is now in the process of publication).

Conclusion. L. Strasburger's conjectures that KS does not p-simulate Frege systems and eKS system are proved.

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

A. A. Chubaryan

Relations between the Proof Complexities in Frege Systems, Deep-Inference Proof Systems KS and eKS

Using the determinative sizes for tautologies of some sequences, it is proved in this paper that a Frege system and deep-inference proof system eKS exhibit an exponential speed-up over the deep-inference proof systems KS both by lines and size of proofs.

Ա. Ա. Չուբարյան

Արտածումների բարդությունների հարաբերությունները Ֆրեգեի համակարգերի, խորքային արտածման կանոններով KS և eKS համակարգերի միջև

Օգտագործելով որոշակի հաջորդականությունների նույնաբանությունների որոշիչ երկարությունները՝ ապացուցվել է, որ Ֆրեգեի համակարգերը և խորքային արտածման կանոններով eKS համակարգը ցուցաբերում են էքսպոնենցիալ արագացում խորքային արտածման կանոններով KS համակարգի նկատմամբ՝ և՛ ըստ արտածումների քայլերի, և՛ ըստ դրանց երկարությունների:

А. А. Чубарян

Отношение между сложностями выводов в системах Фреге и системах глубинных правил выводов KS и eKS

Используя величины определяющих длин тавтологий некоторых последовательностей, доказано, что системы Фреге и система глубинных правил выводов eKS проявляют экспоненциальное ускорение относительно системы глубинных правил выводов KS как по шагам, так и по длинам выводов.

References

1. *Cook S., Reckhow A. R.* – Symbolic Logic. 1979. V. 44. P. 36-50.
2. *Guglielmi A., Straßburger L.* – Computer Science Logic, CSL. 2001. V. 2142 of LNCS. 2001. P. 54–68.
3. *Sraßburger L.* – Annals of Pure and Applied Logic. 2012. V. 163. P. 1995-2007.
4. *Bruscoli P., Guglielmi A.* – ACM Transactions on Computational Logic. 2009. V. 10 (2). P. 1–34, article 14.
5. *Чубарян Ан. А., Чубарян Арм. А.* – Отечественная наука в эпоху изменений: постулаты прошлого и теории нового времени, НАУ, часть 10, 2(7). 2015. С.11-14.
6. *Chubaryan An.* – Proceedings of NASA RA. 2002. V. 37. № 5 and Journal of CMA (AAS). 2002. V. 37. № 5. P. 71-84.