Mathematical Problems of Computer Science 59, 27–34, 2023.
doi: 10.51408/1963-0099

UDC 510.64

The Relationship Between the Proof Complexities of Linear Proofs in Quantified Sequent Calculus and Substitution Frege Systems

Hakob A. Tamazyan

Yerevan State University, Yerevan, Armenia
e-mail: hakob.tamazyan@ysu.am

Abstract

It has formerly been proved that there is an exponential speed-up in the number of lines of the quantified propositional sequent calculus over substitution Frege systems when considering proofs as trees. This paper shows that a linear proof of any quantifier-free tautology in quantified propositional sequent calculus can be transformed into a linear proof of the same tautology in a substitution Frege systems with no more than polynomially increasing proof lines and size.

Keywords: Sequent systems, Frege systems, Proof size, Number of proof lines, Exponential speed-up.

Article info: Received 23 March 2023; sent for review 2 April 2023; accepted 19 May 2023.

1. Introduction

The existence of a propositional proof system that has proofs of polynomial size for all tautologies is equivalent to the equation $NP = co\text{-}NP$ [1]. This observation has gained attention in recent years, leading to the examination of new proof systems. Through the discovery of new systems, the computational power of existing ones is gaining a greater understanding. A hierarchy of proof systems has been established based on two complexity measures (size and lines), and the relationships between these systems are being explored. Alessandra Carbone in [2] compared the number of derivation lines in the form of a tree in some propositional calculus systems and revealed a distinctive property of the quantified propositional sequent calculus (QPK system). Namely, for some sequences of formulas, the QPK system has an exponential speed-up by lines with respect to the substitution sequent calculus (SPK system) and substitution Frege systems (SF systems) when proofs are considered as trees. It was shown in [3] that the lines of linear proofs of the same formulae families in all three systems are the same by order. Later, in [4], the same result was achieved if one considers the sizes of linear proofs of the same formulae families for comparison.

In this paper, the relationship between the proof complexities of linear proofs in QPK and SF has been investigated for all quantifier-free tautologies: it turns out that QPK system has no significant advantage over SF when only linear proofs are considered. Specifically, after the transformation of linear QPK-proof of a quantifier-free tautology into a linear SF-proof of the same tautology by some algorithm, both complexities (the number of lines and sizes) of linear proofs in SF can increase polynomially at most.

2. Preliminaries

First and foremost, lets define several proof systems according to [1, 5, 6].

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

The Substitution Frege system SF is defined by adding to F the substitution rule

$$\frac{A(p)}{A(B)}$$

where simultaneous substitution of the formula B is allowed for the variable p.

The LK Sequent calculus was introduced by Gentzen [7] for first-order logic. Each line in LK-proof is a sequent: a sequent is written in the form:

$$A_1, \dots, A_n \to B_1, \dots, B_m$$

where $A_1, \dots, A_n$ and $B_1, \dots, B_m$ are formulas. We denote these sequences of formulas by capital Greek letters Γ, Δ, etc. As a quantifier symbol in LK, we will include only the universal quantification $\forall$. The existential quantification symbol $\exists$ will be added by the following definition:

$$(\exists x)A(x) \equiv \neg(\forall x)\neg A(x).$$

The inference rules of the sequent calculus LK are as follows:

- Initial sequents are sequents of the following form:

  $$A \to A$$

  where A is any formula.

- Structural rules:

$$Weakening : left \quad \frac{\Gamma \to \Delta}{A, \Gamma \to \Delta} \qquad Weakening : right \quad \frac{\Gamma \to \Delta}{\Gamma \to \Delta, A}$$

$$Exchange : left \quad \frac{\Gamma_1, A, B, \Gamma_2 \to \Delta}{\Gamma_1, B, A, \Gamma_2 \to \Delta} \qquad Exchange : right \quad \frac{\Gamma \to \Delta_1, A, B, \Delta_2}{\Gamma \to \Delta_1, B, A, \Delta_2}$$

$$Contraction : left \quad \frac{\Gamma_1, A, A, \Gamma_2 \to \Delta}{\Gamma_1, A, \Gamma_2 \to \Delta} \qquad Contraction : right \quad \frac{\Gamma \to \Delta_1, A, A, \Delta_2}{\Gamma \to \Delta_1, A, \Delta_2}$$

- Logical rules:

$$\neg : left \quad \frac{\Gamma \to \Delta, A}{\neg A, \Gamma \to \Delta} \qquad\qquad \neg : right \quad \frac{A, \Gamma \to \Delta}{\Gamma \to \Delta, \neg A}$$

$$\wedge : left \quad \frac{A, B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta} \qquad\qquad \wedge : right \quad \frac{\Gamma \to \Delta, A \quad \Gamma \to \Delta, B}{\Gamma \to \Delta, A \wedge B}$$

$$\vee : left \quad \frac{A, \Gamma \to \Delta \quad B, \Gamma \to \Delta}{A \vee B, \Gamma \to \Delta} \qquad\qquad \vee : right \quad \frac{\Gamma \to \Delta, A, B}{\Gamma \to \Delta, A \vee B}$$

$$\supset : left \quad \frac{\Gamma \to \Delta, A \quad B, \Gamma \to \Delta}{A \supset B, \Gamma \to \Delta} \qquad\qquad \supset : right \quad \frac{A, \Gamma \to \Delta, B}{\Gamma \to \Delta, A \supset B}$$

- The cut rule:

$$\frac{\Gamma \to \Delta, A \quad A, \Gamma \to \Delta}{\Gamma \to \Delta}$$

Let us denote by PK the sequent calculus LK, where the rules are restricted to propositional logic.

The substitution system SPK is defined as the propositional sequent calculus PK with an additional substitution rule:

$$S_p^B \quad \frac{\Gamma \to \Delta, A(p)}{\Gamma \to \Delta, A(B)},$$

where simultaneous substitution of the formula B is allowed for the variable p, and p does not appear in Γ, Δ.

The quantifier system QPK is defined as the propositional sequent calculus PK, where new quantification rules are added:

$$\forall : left \quad \frac{A(B), \Gamma \to \Delta}{(\forall q)A(q), \Gamma \to \Delta} \qquad\qquad \forall : right \quad \frac{\Gamma \to \Delta, A(p)}{\Gamma \to \Delta, (\forall q)A(q)}$$

where B is any formula such that no free variable occurrence in B becomes bounded in $A(B)$, and with the restriction that the atom p does not occur freely in the lower sequents of $\forall : right$.

Notice that the the following two inferences can be derived in QPK system using the definition of the quantifier $\exists$:

$$\exists : left \quad \frac{A(p), \Gamma \to \Delta}{(\exists q)A(q), \Gamma \to \Delta} \qquad\qquad \exists : right \quad \frac{\Gamma \to \Delta, A(B)}{\Gamma \to \Delta, (\exists q)A(q)}$$

$$\dfrac{\dfrac{\dfrac{A(p), \Gamma \to \Delta}{\Gamma \to \Delta, \neg A(p)}}{\Gamma \to \Delta, (\forall q)(q)}}{\neg(\forall q)\neg A(q), \Gamma \to \Delta} \qquad\qquad \dfrac{\dfrac{\dfrac{\Gamma \to \Delta, A(B)}{\neg A(B), \Gamma \to \Delta}}{(\forall q)(q), \Gamma \to \Delta}}{\Gamma \to \Delta, \neg(\forall q)\neg A(q)}$$

3. Main Results

For a given linear proof in QPK with n number of lines and proof size s, one can always find a linear proof in SPK of the same tautology having $O(n^2)$ lines and $O(s^5)$ proof size.

First of all, notice that for any linear proof in SPK, there exists a linear proof in QPK of the same tautology with the same number of lines. The sequent $(\forall p)A(p), \Gamma \to \Delta, A(B)$ is provable for all A, B, and the sequent $\Gamma \to \Delta, (\forall p)A(p)$ is derivable from $\Delta \to \Delta, A(p)$. Hence, after combining them through a cut rule, one derives $\Gamma \to \Delta, A(B)$. Here we examine the relationship between these systems in the opposite scenario.

Lemma. *For $n, m \geq 0$ and p not appeared in Γ, Δ, the following inference*

$$\frac{\Gamma, A_1(p), \dots, A_n(p) \to \Delta, A_{n+1}(p), \dots, A_{n+m}(p)}{\Gamma, A_1(B), \dots, A_n(B) \to \Delta, A_{n+1}(B), \dots, A_{n+m}(B)}$$

can be achieved in SPK system with $O(n+m)$ lines using the substitution rule only once.

Proof. First, let's prove these additional inferences:

1. $$\frac{\Gamma \to \Delta, \neg A}{A, \Gamma \to \Delta}$$

$$\begin{array}{c}
\Gamma \to \Delta, \neg A \quad A \to A \\ \hline
\Gamma \to \Delta, \neg A \quad \neg A, A \to \\ \hline
A, \Gamma \to \Delta
\end{array}$$

2. $$\frac{\Gamma \to \Delta, A \vee B}{\Gamma \to \Delta, A, B}$$

$$\begin{array}{c}
\Gamma \to \Delta, A \vee B \quad A \to A \quad B \to B \\ \hline
\Gamma \to \Delta, A \vee B \quad A \to A, B \quad B \to B \\ \hline
\Gamma \to \Delta, A \vee B \quad A \to A, B \quad B \to A, B \\ \hline
\Gamma \to \Delta, A \vee B \quad A \vee B \to A, B \\ \hline
\Gamma \to \Delta, A, B
\end{array}$$

3. $$\frac{\Gamma, A \wedge B \to \Delta}{\Gamma, A, B \to \Delta}$$

$$\begin{array}{c}
\Gamma, A \wedge B \to \Delta \quad A \to A \quad B \to B \\ \hline
\Gamma, A \wedge B \to \Delta \quad A, B \to A \quad B \to B \\ \hline
\Gamma, A \wedge B \to \Delta \quad A, B \to A \quad A, B \to B \\ \hline
\Gamma, A \wedge B \to \Delta \quad A, B \to A \wedge B \\ \hline
\Gamma, A, B \to \Delta
\end{array}$$

The final proof will look like this:

$$\begin{array}{c}
\Gamma, A_1(p), \ldots, A_n(p) \to \Delta, A_{n+1}(p), \ldots, A_{n+m}(p) \\ \hline
\Gamma, A_1(p) \wedge A_2(p), \ldots, A_n(p) \to \Delta, A_{n+1}(p), \ldots, A_{n+m}(p) \\
\vdots \\ \hline
\Gamma, A_1(p) \wedge \ldots \wedge A_n(p) \to \Delta, A_{n+1}(p), \ldots, A_{n+m}(p) \\
\vdots \\ \hline
\Gamma, A_1(p) \wedge \ldots \wedge A_n(p) \to \Delta, A_{n+1}(p) \vee \ldots \vee A_{n+m}(p) \\ \hline
\Gamma \to \Delta, A_{n+1}(p) \vee \ldots \vee A_{n+m}(p), \neg(A_1(p) \wedge \ldots \wedge A_n(p)) \\ \hline
\Gamma \to \Delta, A_{n+1}(p) \vee \ldots \vee A_{n+m}(p) \vee \neg(A_1(p) \wedge \ldots \wedge A_n(p)) \\ \hline
\Gamma \to \Delta, A_{n+1}(B) \vee \ldots \vee A_{n+m}(B) \vee \neg(A_1(B) \wedge \ldots \wedge A_n(B)) \\ \hline
\Gamma \to \Delta, A_{n+1}(B) \vee \ldots \vee A_{n+m}(B), \neg(A_1(B) \wedge \ldots \wedge A_nB) \\ \hline
\Gamma, A_1(B) \wedge \ldots \wedge A_n(B) \to \Delta, A_{n+1}(B) \vee \ldots \vee A_{n+m}(B) \\
\vdots \\ \hline
\Gamma, A_1(B), \ldots, A_n(B) \to \Delta, A_{n+1}(B), \ldots, A_{n+m}(B)
\end{array}$$

Note that in this proof the substitution rule is applied only once. ■

Theorem 1. *For a given linear proof in QPK of some quantifier-free tautology with n number of lines, there exists a linear proof in SPK of the same tautology having $O(n^2)$ number of lines.*

Proof. Suppose P is a given linear proof in QPK. Since P is the proof of a quantifier-free tautology, if a formula with a quantifier appears in the proof, then it must disappear at some point in the next lines. These formulas can appear either by quantification rules or by weakening rules, and the cut rule is the only inference rule capable of removing a formula from the sequent. Notice that if we apply the cut rule to two sequents and some formula A with a quantifier is removed, then it is impossible that both of these sequents got this quantifier by the $\forall : left$ rule.

First of all, we will remove all applications of the $\forall : left$ rule in the proof of P. Let $(\forall q)A(q)$ be some formula or subformula in the proof. Suppose it appeared by $\forall : right$ rule that infers $\Gamma \to \Delta, (\forall q)A(q)$ from $\Gamma \to \Delta, A(p)$. Since p does not occur free in sequent $\Gamma \to \Delta, (\forall q)A(q)$, instead of the $\forall : right$ rule, we can apply the substitution rule to $\Gamma \to \Delta, A(p)$ and substitute p with some new variable k that did not appear throughout the proof. If $(\forall q)A(q)$ appeared by weakening rules, we will replace it with the formula $A(k)$, where k is again some new variable that did not appear throughout the proof. According to the previously mentioned claim, the formula $(\forall q)A(q)$ should have been removed at some point via the cut rule. Therefore, just before the application of cut rule, we will substitute the variable k with the corresponding matching formula to be able to apply the cut rule successfully. This substitution is allowed since k does not appear in the remaining formulas of the sequent.

This removal of formulas with quantifiers from the proof can have the following effects.

Firstly, since these formulas have been replaced with different ones, the contraction rule can not be applied to these replacements anymore, as they can differ from each other. Therefore, instead of applying the contraction rule to them, in the next lines we will apply the same inference rules to both of them. As these formulas should disappear in one of the next lines by the cut rule, we will apply the cut-elimination rule twice so that both of them will be removed. There are $O(n)$ applications of the contraction rule, then after this change, the number of lines will become $O(n^2)$. However, according to the lemma, the number of applications of the substitution rule will not change and will remain $O(n)$.

Secondly, the $\forall : left$ rule that transformed some sequent $A(B), \Gamma \to \Delta$ into $(\forall q)A(q), \Gamma \to \Delta$, will not be applied to the proof, and the formula B will appear in the next lines. Hence, there might be an application of the substitution rule in these next lines that substitutes some variable x into some formula C so that x also appears in the formula B. This means that besides the formula C, there can also be other formulas with the variable x in the sequent. Therefore, to fix this, we will apply the substitution to these formulas too. Considering that the number of applications of the $\forall : left$ rule was $O(n)$ and removing each application of the contraction rule adds just one formula to the sequent, the number of such formulas in the sequent will be $O(n)$. Therefore, according to the lemma, each such substitution will require $O(n)$ additional lines. Since there are $O(n)$ applications of the substitution rule, this change will add $O(n^2)$ number of lines to our proof. This will conclude the transformation process, and the transformed SPK proof will have $O(n^2)$ lines. ■

Theorem 2. *For a given linear proof in QPK of some quantifier-free tautology with a proof size s, there exists a linear proof in SPK of the same tautology having $O(s^5)$ proof size.*

Proof. Suppose P is a given linear proof in QPK with n number of lines and proof size s. Let P' be the transformed SPK proof according to the process described above. To calculate its size, let's dive into the transformation process step by step.

We replaced each application of the $\forall : right$ rule with a substitution rule to substitute one variable with another. The formulas with quantifiers that appeared by weakening rules have been replaced by formulas with the same size. Afterwards, we added a substitution before the application of the cut rule to match the corresponding formula. All these steps change the number of proof lines and the proof size linearly. Let's denote them by n', s', respectively.

Moreover, we removed all applications of the $\forall : left$ rule. Therefore, if some application of the $\forall : left$ rule transformed the sequent $A(B), \Gamma \to \Delta$ into $(\forall q)A(q), \Gamma \to \Delta$, then after the removal, the formula B will appear in the next lines. This will increase the proof size by at most $n' \cdot |A(B)|$, where $|A(B)|$ is the size of the formula $A(B)$. Removing the i^th application of the $\forall : left$ rule increases the proof size by at most $n' \cdot |A_i(B_i)|$, then removing all of them will add no more than

$$\sum_i n' \cdot |A_i(B_i)| = n' \cdot \sum_i |A_i(B_i)| \leq n' \cdot s' \leq s'^2$$

to the proof size. As s' is $O(s)$, after this step, the proof size will be $O(s^2)$ and the number of lines will remain $O(n)$.

Removing applications of the contraction rule has the following two effects on the proof size.

First of all, it will keep the eliminated formula in a sequent, so it will appear in the next lines. The added proof size can be calculated completely like the previous method. Since the number of applications of the contraction rule is $O(n)$ and the proof size is $O(s^2)$, this change will make the proof size $O(s^3)$. The number of lines will remain $O(n)$.

The second effect of removing applications of the contraction rule will be applying the same inference rules to both formulas. Since the proof size is $O(s^3)$, then applying the same inference rule to the previously eliminated formula can increase the proof size by $O(s^3)$. The number of applications of the contraction rule is $O(n)$, and since $n \leq s$, the overall proof size will become $O(s^4)$.

Finally, the removal of the $\forall : left$ rule causes some substitution steps to also substitute the same variable in several other formulas of the same sequent. Notice that all these substitution steps were $\forall : right$ rule replacements that substitute one variable with another, as otherwise we won't face such a problem. Each such substitution that simultaneously substitutes the same variable in these sequent formulas required $O(n)$ lines. If the i^th such substitution is applied to the sequent S_i, then this change will overall add no more than

$$\sum_i c \cdot n \cdot |S_i| = c \cdot n \cdot \sum_i |S_i| \leq c \cdot s \cdot \sum_i |S_i|$$

to the proof size, where $|S_i|$ is the size of the sequent S_i and c is some constant. $\sum_i |S_i|$ is smaller than the current proof size, therefore the transformed SPK proof will have $O(s^5)$ size. ■

Corollary. *Since the system SPK is polynomially equivalent to the system SF, there is a transformation of a linear proof of any quantifier-free tautology in QPK into a linear proof in the system SF that increases the proof lines and size at most polynomially.*

4. Conclusion

This work described an algorithm according to which any QPK linear proof can be transformed into a SF linear proof by increasing its lines and size to at most a polynomial extent. The obtained results show that the QPK system does not have a substantial advantage over the system SF in terms of linear proofs.

References

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

[2] A. Carbone, "Quantified propositional logic and the number of lines of tree-like proofs", *Studia Logica*, vol. 64, pp. 315–321, 2000.

[3] H. A. Tamazyan and A. A. Chubaryan, "On proof complexities relations in some systems of propositional calculus, *Mathematical Problems of Computer Science*, vol. 54, pp. 138–146, 2020.

[4] L. A. Apinyan and A. A Chubaryan, "On sizes of linear and tree-like proofs for any formulae families in some systems of propositional calculus", *Mathematical Problems of Computer Science*, vol. 57, pp. 47–55, 2022.

[5] P. Pudlák, *The Lengths of Proofs*, in S. Buss (ed.), Handbook of Proof Theory, Elsevier, vol. 137, pp. 547-637, 1998.

[6] J. Krajíček, *Proof Complexity, Encyclopedia of Mathematics and Its Applications*, Cambridge University Press, vol. 170, 2019.

[7] G. Gentzen, "Die Widerspruchsfreiheit der reinen Zahlentheorie", *Mathematische Annalen*, vol. 112, pp. 493–565, 1936.

Գծային արտածումների բարդությունների կապը ծավալիչներով սեկվենցիալ համակարգում և տեղադրման կանոնով Ֆրեգեի համակարգերում

Հակոբ Ա. Թամազյան

Երևանի պետական համալսարան, Երևան, Հայաստան
e-mail: hakob.tamazyan@ysu.am

Ամփոփում

Նախկինում ապացուցվել է, որ ծավալիչներով սեկվենցիալ համակարգում առկա է քայլերի քանակի էքսպոնենցիալ արագացում տեղադրման կանոնով Ֆրեգեի համակարգերի նկատմամբ, երբ դիտարկում ենք ծառային արտածումները։ Այս հոդվածը ցույց է տալիս, որ առանց ծավալիչների, ցանկացած նույնաբանության գծային արտածումը ծավալիչներով սեկվենցիալ համակարգում հնարավոր է վերածել նույն նույնաբանության գծային արտածման տեղադրման կանոնով Ֆրեգեի համակարգերում՝ ունենալով արտածման քայլերի քանակի և երկարության առավելագույն բազմանդամային աճ։

Բանալի բառեր՝ սեկվենցիալ համակարգեր, Ֆրեգեի համակարգեր, արտածման երկարություն, արտածման քայլերի քանակ, էքսպոնենցիալ արագացում։

Связь между сложностями доказательств линейных выводов в системе секвенциального исчисления с кванторами и системах Фреге с правилом подстановки

Акоб А. Тамазян

Ереванский государственный университет, Ереван, Армения
e-mail: hakob.tamazyan@ysu.am

Аннотация

Ранее было доказано, что существует экспоненциальное ускорение количества шагов в системе секвенциального исчисления высказываний с кванторами по сравнению с системами Фреге с правилом подстановки, когда мы рассматриваем выводы в виде деревьев. Эта статья показывает, что линейный вывод любой бескванторной тавтологии в системе секвенциального исчисления высказываний с кванторами можно превратить в линейный вывод той же тавтологии в системах Фреге с правилом подстановки с не более чем полиномиально возрастающим количеством шагов и длиной вывода.

Ключевые слова: секвенциальные системы, системы Фреге, длина вывода, количество шагов вывода, экспоненциальное ускорение.