Quantified propositional logic and the number of lines of tree-like proofs

A. CARBONE

June 26, 1999

Abstract

There is an exponential speed-up in the number of lines of the quantified propositional sequent calculus over Substitution Frege Systems, if one considers proofs as trees. Whether this is true also for the number of symbols, is still an open problem.

1 Some background

The existence of a propositional proof system which has polynomial size proofs for all tautologies is equivalent to say that $NP = co\text{-}NP$ [CR79]. This simple observation drew the attention in recent years on the formalisms of propositional logic for the study of questions of computational complexity (for a review see [Krajíček95] or [Pudlàk98]). A hierarchy of propositional proof systems has been defined and the relations between these systems are currently analyzed. New systems are discovered and as a consequence the computational power of old ones is better understood. In this note we show that the addition of quantifier rules to the propositional sequent calculus induces an exponential speed-up over Substitution Frege systems when proofs are considered as trees.

Let us denote PK the usual sequent calculus LK where the rules are restricted to propositional logic. The system PK *without* cut rule will be denoted PK^-. The quantifier system G is defined as the propositional sequent calculus PK, where a new set of rules for the quantifiers is added

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

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

where B is any quantified propositional formula. The application of the rules $\exists : left$ and $\forall : right$ is restricted to the following requirements: the eigenvariable b does not occur free in the lower sequent of the rule, and all occurrences of q in $A(q)$ are substituted by p. The rules $\exists : right$ and $\forall : left$ require B not to contain variables which are under the scope of some quantifier.

In the hierarchy of propositional proof systems, which do not include or depend on non-propositional concepts (see pp.590 of [Pudlàk98] for a presentation), the system G is the strongest that we know at the moment. Therefore, it is natural to ask whether the use of quantifiers enable us to prove ordinary propositions faster. This seems plausible, as polynomial sized quantified propositional formulas can define functions in $PSPACE$, and it is reasonable to expect them to have stronger expressive power than ordinary propositional formulas. On the other hand, it might be the case that for some tautologies, G would have only proofs with essentially the same size as proofs in PK, or that quantified propositional formulas of polynomial size would define the same functions as ordinary propositional formulas of polynomial size.

Clearly any proof in PK is also a proof in G but it is unknown [Pudlàk98] whether or not PK *polynomially simulates* G, i.e. whether or not there is a polynomial $p(x)$ and a polynomial time algorithm such that for all tautologies S, any proof $\Pi_1 : S$ in G can be transformed by the algorithm into a proof $\Pi_2 : S$ in PK and $|\Pi_2| \leq p(|\Pi_1|)$, where $|-|$ denotes the number of symbols in a proof. (The definition of 'polynomial simulation' was introduced in [CR79].)

Before describing what is happening when one looks at the *number of lines* in proofs instead of the *size* of a proof, we need to make two observations.

First, there are two ways one can measure the number of lines in a proof. Once a formula is derived, one might decide to use it as many times as needed without reproving it again. We talk in this case of *linear* proofs. If a formula can be used exactly once in a proof, then each use of it requires a new proof, and we will talk about proofs as *trees*. It turns out that speed-up results are sensitive to this distinction.

Second, the system G "resembles" the system SPK (Substitution Sequent Calculus) defined by adding to PK the following rule of substitution

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

where simultaneous substitution of the formula B is allowed for the variable p, and where p does not appear in Γ, Δ. Notice that given a linear proof in SPK one can always find a linear proof in G of the same tautology having the same number of lines. It is sufficient to notice that the sequent $(\forall p)A(p), \Gamma \to \Delta, A(B)$ is provable for all A, B. By combining it (through a cut) with the sequent $\Gamma \to \Delta, (\forall p)A(p)$ (which is derivable from $\Gamma \to \Delta, A(p)$ in one step) one derives $\Gamma \to \Delta, A(B)$. We will show here that the converse is not true if one considers *tree-like* proofs.

In this note we work with proof systems whose rules are formulated in the language of the sequent calculus. It should be noticed that the systems PK and SPK are natural examples of the Frege system F and the Substitution Frege system SF, whose definition we recall here. The *Frege system* F is defined, for a complete set of propositional connectives, to be a finite set of schematically defined rules of inference which admits modus ponens as a derived rule, and it is sound and complete, i.e., it must prove every tautology and no more than that. 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. Clearly, many choices of rules of inference and logical connectives which satisfy the definitions of F and SF are possible. These choices affect the length of proofs, but only by polynomial amounts. Therefore, our results extend to F and SF as well.

In the following we will also mention the *Extended Frege system* EF which is obtained by adding to F the extension rule

$$p \leftrightarrow A$$

where A is any formula and p is a variable which does not occur in A, it does not appear in any earlier extension rule used in the proof, and it does not occur in the final formula of the proof (the formula being proved). The idea of the extension rule is to allow the variable p to act as an abbreviation for the formula A. We refer the reader to [Krajíček95] and [Pudlàk98] for a survey of results on F, SF, EF and their simulations.

2 An exponential speed-up

In [Krajíček95] it is shown that there is a tautology of size $\mathcal{O}(2^n)$ such that there are *linear* proofs in the system SF of $\mathcal{O}(n)$ lines and all proofs in F have of at least 2^n lines. If one considers tree-like proofs this is no longer true. In fact for tree-like proofs it is easy to check that any proof in SPK can be transformed in a PK-proof with the same number of lines and symbols. For each occurrence of the substitution rule in the SPK-proof which transforms a sequent $\Gamma \rightarrow \Delta, A(p)$ into a sequent $\Gamma \rightarrow \Delta, A(B)$, it is enough to replace each occurrence of p in the proof with the formula B and eliminate the application of the rule of substitution.

Here we show that there is a tautology of size $\mathcal{O}(2^{2^n})$ such that there are *tree*-like proofs with $\mathcal{O}(n)$ lines in the system G and all tree-like proofs in SPK (and therefore PK) have of at least 2^n lines. (See Remark 4 for a tautology of size $\mathcal{O}(2^n)$ with the same properties.)

The result is interesting for two reasons. First it gives an exponential speed-up of G over SPK and second it points out how large tautologies of $\mathcal{O}(2^{2^n})$ symbols can be built in $\mathcal{O}(n)$ steps using formulas with one single quantifier.

Let the *nested* conjunction p^m be defined inductively as $p^1 \equiv p$ and $p^{i+1} \equiv (p^i \wedge p^i)$, for $i \geq 1$. It is easy to verify that the formula p^m has logical depth m, it contains roughly 2^m symbols and has m distinct subformulas.

Theorem 1 *Let n be sufficiently large and let S be the sequent $\rightarrow p \supset p^{2^n}$. The following holds:*

1. *there is a tree-like proof of S in G of $\mathcal{O}(n)$ lines;*
2. *any tree-like proof of S in SPK (and also SF) has $\Omega(2^n)$ lines;*
3. *any proof of S in PK (and also F and EF) has $\Omega(2^n)$ lines;*
4. *any tree-like proof of S in PK^- has $\Omega(2^{2^n})$ lines.*

Proof. We want to build a proof of $\rightarrow p \supset p^{2^n}$ in G with $\mathcal{O}(n)$ lines. To do this we consider the provable sequent

$$\forall q(q \supset q^k) \rightarrow \forall q(q \supset q^{2k})$$

where k is an arbitrary integer and $q^{2k} = (q^k)^k$. The proof of this sequent will not depend on k and can be obtained in a constant number of lines with the following argument

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p \rightarrow p \quad p^k \rightarrow p^k}{p \supset p^k, p \rightarrow p^k}}{\forall q(q \supset q^k), p \rightarrow p^k} \quad p^{2k} \rightarrow p^{2k}}{\forall q(q \supset q^k), p^k \supset p^{2k}, p \rightarrow p^{2k}}}{\forall q(q \supset q^k), p^k \supset p^{2k} \rightarrow p \supset p^{2k}}}{\forall q(q \supset q^k), \forall q(q \supset q^k) \rightarrow p \supset p^{2k}}}{\forall q(q \supset q^k) \rightarrow p \supset p^{2k}}}{\forall q(q \supset q^k) \rightarrow \forall q(q \supset q^{2k})}$$

By combining n times the above sequents, one obtains

$$\forall q(q \supset q^2) \rightarrow \forall q(q \supset q^{2^n})$$

and since $\forall q(q \supset q^2)$ is provable in a few lines one infers $\forall q(q \supset q^{2^n})$ and therefore $\rightarrow p \supset p^{2^n}$ in $\mathcal{O}(n)$ lines. This concludes the proof of the claim 1.

To show that in F and in EF the smallest proof of the sequent has $\Omega(2^n)$ lines we use Theorem 5 in [Buss95] which says that if A is a tautology which is not a substitution instance of a shorter tautology, then any Frege or Extended Frege proof of A requires $c \cdot ||A||$ lines, where c is a constant symbol which depends on the proof system and $||A||$ is the number of distinct subformulas of A. By a straighforward checking we observe that the tautology $\rightarrow p \supset p^{2^n}$ is not a substitution instance of a shorter tautology and that $||p \supset p^{2^n}||$ is roughly 2^n. We can therefore apply the result above and derive claim 3 for F and EF. Since PK is an instance of a Frege System, the argument holds for PK as well.

Since for any tree-like proof in SPK there is a proof in PK with the same number of lines (as observed above), claim 2 follows from claim 3.

To show claim 4 we basically apply the method of "active subformulas" used by Buss to show Theorem 5 in [Buss95]. Since our application is easy, we shall explain the proof directly, without defining the general machinery. We first notice that $\rightarrow p \supset p^{2^n}$ contains one *negative* occurrence of p (i.e. the antecedent of the implication) and roughly 2^{2^n} *positive* occurrences of p (in the conjunct p^{2^n}). In particular, each positive occurrence of p should be "active" in the sense that it should be introduced in the proof by some axiom of the form $p \rightarrow p$ and should be used in the proof as an auxiliary formula of some $\wedge : right$ rule. If this was not the case, then some non-atomic subformula B of p^{2^n} should be introduced by some axiom of the form $B \rightarrow B$. But this is not possible since we would end-up with more than one negative occurrence of p in the end-sequent (by the subformula property). This means that any tree-like cut-free proof of the statement has $\Omega(2^{2^n})$ lines.

□

The following corollaries are a direct consequence of Theorem 1.

Corollary 2 *There is no transformation between proofs in G and tree-like proofs in SF which is polynomial in the number of steps of the G-proofs.*

Corollary 3 *There is no transformation between proofs in G and proofs in F or in EF which is polynomial in the number of steps of the G-proofs.*

Theorem 1 shows how quantifiers can help to get shorter representations of very large tautologies displaying a lot of symmetry. On the other hand, if the tautology is not large, we still do not know whether quantifiers can help or not.

Remark 4 It is possible to obtain the lower bound claimed in 1 of Theorem 1 by using the formula r^{2^n} where $r^0 \equiv r$ and $r^{i+1} \equiv \perp \vee (r^i)$. The formula r^{2^n} is much smaller than p^{2^n}, it has 2^n symbols, but has the same depth and the same number of distinct subformulas of p^{2^n}. The proof of Theorem 1 still goes through except for claim 4, since there is a cut-free proof of $\rightarrow r \supset r^{2^n}$ of $\mathcal{O}(2^n)$ lines.

Remark 5 The systems SF and EF polynomially simulate each other. Nevertheless, when one looks at the number of lines of proofs, it turns out that SF speeds-up over EF. In [Buss95] it is proved that the tautologies $r \supset r^{2^n}$ defined in Remark 4, have SF-proofs of $\mathcal{O}(h)$ lines and $\mathcal{O}(k)$ symbols but that they require EF-proofs of $\Omega(2^h)$ lines and $\mathcal{O}(k^2)$ symbols. A related result is the super-logarithmic lower bound on the number of lines in SF proved in [Urquhart96]. More precisely, Urquhart considers the tautologies $\top_S$ associated to the binary string S, which are defined inductively as follows: if S is the empty string, then $\top_S$ is $\top$. If $0S$ and $1S$ are strings of length $k+1$, then $\top_{0S}$ is $(\bot \vee \top_S)$ and $\top_{1S}$ is $(\top \supset \top_S)$. The result says that for almost all binary strings S of length n, any proof of $\top_S$ in SF must have $\Omega(n/\log n)$ lines. The proof is non-constructive but based on a counting argument, and the technique does not provide a lower bound to the number of symbols in SF-proofs. Any improvement in this direction will be of interest.

Remark 6 The rule of substitution in the system SPK (or SF) could have been defined as follows

$$\frac{\Gamma \to \Delta, A(p_1, \ldots, p_n)}{\Gamma \to \Delta, A(B_1, \ldots, B_n)}$$

where simultaneous substitution of the formulas $B_1, \ldots, B_n$ is allowed for the variables $p_1, \ldots, p_n$, and where $p_1, \ldots, p_n$ do not appear in Γ, Δ. In the same spirit one could have defined G as having quantifier rules simultaneously introducing several quantifiers in ones. For instance the $\forall$:*right* rule could have been defined as

$$\frac{\Gamma \to \Delta, A(q_1, \ldots, q_n)}{\Gamma \to \Delta, \forall p_1 \ldots \forall p_n A(p_1, \ldots, p_n)}$$

and similarly for the other quantifier rules. The content of Theorem 1 holds also for this setting.

Acknowledgments

We wish to thank Pavel Pudlàk for some remarks and an anonymous referee for his/her helpful suggestions.

References

[Buss95] S. Buss. Some remarks on the length of propositional proofs. In *Archiv f. Mathematical Logic*, 34:377–394, 1995.

[CR79] S. Cook and R. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36–50, 1979.

[Krajíček95] J. Krajíček. *Bounded arithmetic, propositional logic, and complexity theory.* Encyclopedia of Mathematics and its Applications 60, Cambridge University Press, 1995.

[Pudlàk98] P. Pudlàk. The lengths of proofs. In S. Buss, editor, *Handbook of Proof Theory.* North Holland, 1998, pp. 547–637.

[Urquhart96] A. Urquhart. The number of lines in Frege proofs with substitution. In *Archiv f. Mathematical Logic*, 37:15–19, 1996.

A. Carbone
Mathématiques/Informatique
Université de Paris XII
61 Avenue du Général de Gaulle
94010 Créteil CEDEX
FRANCE