Comment.Math.Univ.Carolinae 30,1(1989)137–140 

# Speed-up for propositional Frege systems via generalizations of proofs

JAN KRAJÍČEK

*Abstract.* A Frege system with the substitution rule has a speed–up over a Frege system with respect to the number of proof–steps which is of the form: $\Omega(2^{n^{\varepsilon}})$

*Keywords:* Frege system, generalizations of proofs, the number of proof–steps

*Classification*: Prim.:03F20, Sec.:03F07

Let us denote by $F$ ($EF$, $SF$ respectively) some Frege system (Frege system with the extension rule, Frege system with the substitution rule respectively). Frege system is a usual propositional calculus based on a finite number of axiom schemes and rules. The extension rule allows to infer the formula $p \equiv A$, provided the atom $p$ does not occur in $A$, in any line preceeding $p \equiv A$ and in the last formula of the proof. The substitution rule allows to infer from formula $A(p_1, \ldots, p_k)$ any formula $A(B_1, \ldots, B_k)$ where formulas $B_i$ are simultaneously substituted for atoms $p_i$. These propositional calculi were defined in [2].

In this note we are interested in the number of steps (= proof lines) in proofs in these calculi. For these purposes the exact choice of the systems is not essential. In [2] it was shown that for any two Frege systems $F_1$, $F_2$ there is a polynomial–time computable function (=polynomial simulation) $f(x, y)$ such that if $d$ is an $F_1$–proof of the formula $A$ then $f(d, A)$ is an $F_2$–proof of $A$. The same holds for any two Frege systems with the extension rule and for any two Frege systems with the substitution rule. It is easily seen that these polynomial simulations increase the number of steps only linearly. Moreover, $EF$–proofs can be transformed into $F$–proofs increasing the number of steps only linearly too–*cf.*[2, Prop.4.3].

In [3], [7] it was shown that $EF$ polynomially simulates $SF$. The explicit simulation constructed in [7] increase sometimes the number of steps exponentially. It follows from the result of Cejtin and Čubarjan [1] that this must hold for any such a simulation. Namely they have proved that $SF$ has an exponential speed–up over $F$ w.r.t. the number of steps.

The aim of this note is to present a new proof of this result (with an improved bound) which is a simple application of the results about generalizations of proofs [4,5,6,8].

It should be stressed explicitely that this speed–up result does not solve the important open problem whether $F$ polynomially simulates $SF$ since the formulas on which the speed–up is realized are themselves of an exponential length.

Propositional formulas are built up from atoms $p_0, p_1, \ldots$ $q_0, q_1 \ldots$, constants 0,1 and connectives including $\neg$ and $\rightarrow$.

The depth $dp(A)$ of a formula is inductively defined by:

(i) $dp(A) = 0$ iff $A$ is an atom or a constant,
(ii) $dp(\neg A) = 1 + dp(A)$,
(iii) $dp(A \to B) = 1 + \max(dp(A), dp(B))$.

In the sequel $(\neg)^m(A)$ will abbreviate the formula:

$$\underbrace{\neg(\neg(\neg(\ldots(\neg}_{m\text{-times}} A)$$

**Theorem.** *There are constants $c, \varepsilon > 0$ such that for all $1 \leq k < \omega$ it holds.*

(i) *there is an $SF$-proof of $(\neg)^{2^k}(1)$ with $\leq c.k$ steps,*
(ii) *any $F$-proof of $(\neg)^{2^k}(1)$ must have $\geq \varepsilon \cdot 2^k$ steps.*

PROOF: Assume $k \geq 1$.

(i) Consider formulas

$$B_k := p \to (\neg)^{2^k}(p).$$

Obviously $SF \vdash B_0$. Also $B_{k+1}$ can be derived from $B_k$ in $SF$ within a constant number of steps: by substitution

$$p \mapsto (\neg)^{2^k}(p)$$

derive from $B_k$ the formula:

$$(\neg)^{2^k}(p) \to (\neg)^{2^{k+1}}(p),$$

and by cut–rule (which is a derived rule in $SF$) applied to this formula and $B_k$ derive $B_{k+1}$.

Hence $B_k$'s have $SF$–proofs with $O(k)$ steps. But $(\neg)^{2^k}(1)$ is inferred from $B_k$ by the substitution $p \mapsto 1$ and one more application of cut–rule. This proves the first part of the theorem.

(ii) We must show that any $F$–proof of $(\neg)^{2^k}(1)$ has at least $\varepsilon \cdot 2^k$ steps, for some constant $\varepsilon > 0$.

**Claim.** There is a constant $c_0 > 0$ such that for any $F$–proof $d = C_1, \ldots, C_l$ there is a sequence $d^* = C_1^*, \ldots, C_l^*$ of propositional formulas built–up from the atoms occurring in $d$ and new ones $\bar{q} = q_0, \ldots, q_s$ such that:

(i) $d^*$ is an $F$–proof,
(ii) $dp(C_i^*) \leq c_0 \cdot l$, for $i \leq l$,
(iii) there is a substitution $\alpha$ assigning to atoms $\bar{q}$ some propositional formulas such that $\alpha(d^*) = d$.

Proof of the claim: The claim is an immediate corollary to Theorem 2.1 of [5]. However, to make the exposition reasonably accessible we outline another argument based on the technique developed in [4,6,8]. For the details see there.

To any $F$–proof $d$ with $l$ steps is assigned a unification problem $\Omega_d$,

$$\Omega_d = \{(s_1, t_1), \ldots, (s_r, t_r)\}$$

such that

(a) $dp(s_j), dp(t_j) \leq c_1$, for all $j \leq r$,
(b) $r \leq c_2 \cdot l$,

where the constants $c_1$, $c_2$ depend only on the particular system $F$.

As proved in [4,6,8] any unifier $\delta$ of $\Omega_d$ determines an $F$–proof $d_\delta$ of depth

$$dp(d_\delta) \leq \max_{j \leq r}(dp(\delta(s_j)), dp(\delta(t_j))).$$

Let $\delta_0$ be a most general unifier of $\Omega_d$. By the results of [6,Lemmas 1.1 and 1.2] it holds:

$$dp(d_{\delta_0}) \leq 2 \cdot r \cdot \max_{j \leq r}(dp(s_j), dp(t_j)),$$

i.e. by (a) and (b) above:

$$dp(d_{\delta_0}) \leq 2 \cdot c_1 \cdot c_2 \cdot l.$$

Moreover, for any unifier $\delta$ of $\omega_d$, $d_\delta$ is a substitution instance of $d_{\delta_0}$. In particular, $d$ is a substitution instance of $d_{\delta_0}$. Put $d^* = d_{\delta_0}$ and $c_0 = 2 \cdot c_1 \cdot c_2$. This proves the claim.

Assume now that

$$d = C_1, \ldots, C_l$$

is an $F$–proof of the formula $(\neg)^{2^k}(1)$, i.e. $C_l = (\neg)^{2^k}(1)$.

By the claim there is an $F$–proof $d^* = C_1^*, \ldots, C_l^*$ such that in particular it holds:

(i) $dp(C_l^*) \leq c_0 \cdot l$, and
(ii) $C_l$ is a substitution instance of $C_l^*$.

Thus if $c_0 \cdot l < 2^k$, $C_l^*$ has necessarily the form:

$$\neg)^m(q_0),$$

for some atom $q_0$ and $m \leq c_0$

Define the substitution $\alpha$:

$$\alpha(q_0) = 0, \text{ if } m \text{ is even}$$
$$= 1, \text{ if } m \text{ is odd.}$$

It follows from the claim that $\alpha(d^*)$ is an $F$–proof of a false formula. Thus it must hold:

$$c_0 \quad \geq 2^k.$$

Put $\varepsilon := c_0^{-1}$. ■

This bound improves the bound obtained in [1] which was only of the form $2^{k^\varepsilon}$, $\varepsilon > 0$.

## References

[1] G.C.Cejtin, A.A.Čubarjan, *On some bounds to the lengths of logical proofs in classical propositional calculus (Russian)*, Trudy Vyčisl. Centra AN ArmSSR i Erevan.univ. **8** (1975), 57-64.

[2] S.A.Cook, R.A.Reckhow, *The relative efficiency of propositional proof systems*, J.Symb. Logic **44** (1979), 36-50.

[3] M.Dowd, *Model-theoretic aspects of* $P \neq NP$, preprint (1985).

[4] W.F.Farmer, "Length of proofs and unification theory, Ph.D. thesis," Univ. of Wisconsin-Madison, 1984.

[5] J.Krajíček, *On the number of steps in proofs*, to appear in Annals of Pure and Applied Logic.

[6] J.Krajíček, P.Pudlák, *The number of proof lines and the size of proofs in first order logic*, Archive for Mathematical Logic **27** (1988), 69-84.

[7] J.Krajíček, P.Pudlák, *Propositional proof systems, the consistency of first order theories and the complexity of computations*, to appear in J.Symbolic Logic.

[8] R.Parikh, *Some results on the length of proofs*, Trans.Amer.Math.Soc. **117** (1973), 29-36.

Mathematical Institute Czechoslovak Academy of Sciences, Žitná 25, Praha 1, 115 67 Czechoslovakia

(*Received* June 4,1988)