PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 81, Number 3, March 1981

SPEED-UP BY THEORIES WITH INFINITE MODELS

R. STATMAN

ABSTRACT. We prove that if S is a finite set of schemata and A is a sentence undecided by S such that $S \cup \{\neg A\}$ has an infinite model then $S \cup \{A\}$ is an unbounded speed-up of S for substitution instances of tautologies. As a corollary, we obtain a conjecture of Parikh's.

I. Let P be any of the usual (schematic) formulations of predicate logic with equality, relation and function symbols, and individual constants and let S be a finite set of schemata; by '$S \vdash^{n}_{P} A$' we mean that there is a P-derivation of A from (substitution instances of members of) S with $< n$ inferences (lines). We shall prove the following:

THEOREM. *Suppose that A is a sentence undecided by S and $S \cup \{\neg A\}$ has an infinite model, then there is a number n such that for each number m there is a substitution instance of a tautology B with $S \cup \{A\} \vdash^{n}_{P} B$ and $S \not\vdash^{m}_{P} B$.*

In short $S \cup \{A\}$ is an unbounded speed-up of S for substitution instances of tautologies.

II. Since for any such P_1 and P_2 it is easy to find a function f satisfying $S \vdash^{k}_{P_1} B \Rightarrow S \vdash^{f(k)}_{P_2} B$, it suffices to set $P = \mathrm{NE}_1$, for NE_1 the system of natural (deduction) rules for predicate logic with equality (see for example 3.1.6, p. 249 of [3], or the proof of Lemma 2 below). We consider the usual first-order language on $\rightarrow$, $\perp$ and $\forall$; for the proof it will be convenient to distinguish relation constants from relation parameters, the latter being the arguments of substitutions.

Let S and A be fixed as above; if C is a propositional formula, built up from propositional variables, $\rightarrow$ and $\perp$, a code F of C is any formula $\neg A \rightarrow B$ where B is obtained from C by a 1-1 substitution of equations $u_i = v_i$ for propositional variables p_i such that all the u_i and v_i are distinct. Note that if F is a code of C then; $S \vDash F. \Leftrightarrow .C$ is a tautology (this only requires that $S \cup \{\neg A\}$ has a ≥ 2 element model), and $S \cup \{A\} \vdash^{3}_{\mathrm{NE}_1} F$. Consequently, it suffices to prove the following:

There is no number m such that if $\neg A \rightarrow B$ is the code of a tautology then

$$S \cup \{\neg A\} \vdash^{m}_{\mathrm{NE}_1} B.$$

We shall prove the following bounded speed-up result:

There is a function f such that

$$S \cup \{\neg A\} \vdash^{n}_{\mathrm{NE}_1} B \Rightarrow \vdash^{f(n)}_{\mathrm{NE}_0} B$$

Received by the editors April 23, 1979 and, in revised form, February 8, 1980.
AMS (MOS) subject classifications (1970). Primary 02D99.

for codes of tautologies $\neg A \rightarrow B$, where NE_0 is the quantifier-free fragment of NE_1 (see 3.1.6, p. 249 of [3]).

Our result then follows from the routine:

PROPOSITION. *There is no number n s.t. for codes of tautologies* $\neg A \rightarrow B$, $\vdash^{n}_{NE_0} B$.

III. A quantifier-free formula is said to be 'simple' if each of its prime subformulae has the form

(a) $u = v$, or

(b) $Uu_1 \cdots u_n$ for U a relation parameter.

In particular, a simple formula contains no nonlogical constants. Let $\lg(B) =_{df}$ the number of occurrences of logical operations and prime subformulae in B:

LEMMA 1. *There is a function f s.t. for simple B if B is valid then* $\vdash^{f(\lg(B))}_{NE_0} B$.

PROOF. If Γ is a set of simple prime formulae let $\mathrm{pm}(\Gamma) =_{df}$ the number of individual parameters occurring in equations in Γ: so, in particular, $\mathrm{pm}(\Gamma) \leq \overline{\overline{\Gamma}} \cdot 2$. Observe that by the method of 1.5.2 on p. 237 of [3] if B is a simple prime formula and $\Gamma \vDash B$ then $\Gamma \vdash^{n}_{NE_0} B$ for $n = 2^{\mathrm{pm}(\Gamma \cup \{B\})}$. In addition if Δ is a set of simple prime formulae and $\Gamma \vDash \bigvee \Delta$ then for some $B \in \Delta$, $\Gamma \vDash B$.

Now suppose that Γ and Δ are collections of simple formulae and $A \rightarrow B$ is simple then

$$\Gamma \cup \neg\Delta \cup \{A_1\} \vdash^{n}_{NE_0} \bot \quad \text{and} \quad \{A_2\} \cup \Gamma \cup \neg\Delta \vdash^{m}_{NE_0} \bot \Rightarrow \qquad (1)$$
$$\{A_1 \rightarrow A_2\} \cup \Gamma \cup \neg\Delta \vdash^{n+m+4}_{NE_0} \bot,$$

and

$$\{A_1\} \cup \Gamma \cup \neg\Delta \cup \{\neg A_2\} \vdash^{n}_{NE_0} \bot \Rightarrow \Gamma \cup \neg\Delta \cup \{\neg(A_1 \rightarrow A_2)\} \vdash^{n+3}_{NE_0} \bot. \quad (2)$$

Let $\lg(\Gamma) = \Sigma_{A \in \Gamma} \lg(A)$; it follows easily from the above that

$$\Gamma \vDash \bigvee \Delta \Rightarrow \Gamma \cup \neg\Delta \vdash^{n}_{NE_0} \bot$$

for $n = 4^{\lg(\Gamma) + \lg(\Delta)}$ so we can set $f(x) =_{df} 4^x + 1$.

By a substitution we mean a substitution of relation terms $\lambda x_1 \cdots x_n A$ (with the restriction that each x_i occurs in A) for relation parameters under the definition:

$$\lambda x_1 \cdots x_n A(x_1 \cdots x_n) t_1 \cdots t_n =_{df} A(t_1 \cdots t_n).$$

For what follows we refer the reader to 4.1-2, pp. 251–255 of [3].

If θ and ϕ are substitutions, then $\theta\phi$ is their composition.

If F_i is a finite set of relation terms and $F = F_1 \cdots F_n$, then $\theta \restriction F$ is the substitution defined by

$$(\theta \restriction F)U = \theta U \quad \text{if } U \text{ occurs in a member of some } F_i,$$
$$= U \quad \text{otherwise.}$$

We say that θ unifies F if for each $1 \leq i \leq n$, $\mathrm{card}(\theta'' F_i) = 1$.

If F_i is a finite set of relation terms and $F = F_1 \cdots F_n$, then $\lg(F)$ is the maximum logical complexity of a relation term belonging to some F_i and $\mathrm{rel}(F)$ is the total number of relation symbols occurring in members of the F_i.

If θ is a substitution, then $\lg(\theta) =_{\mathrm{df}} \max\{\lg(\theta U);\ U \in \operatorname{dom}\theta\}$. Note that $\lg(\theta\phi) \leqslant \lg(\theta)\cdot\lg(\phi)$ and $\lg(\theta F) \leqslant \lg(\theta)\cdot\lg(F)$ where $\theta F =_{\mathrm{df}} \theta'' F_1 \cdots \theta'' F_n$.

In [3] we proved the following lemma (4.2.1).

Suppose that F_i is a finite set of formulae, $F = F_1 \cdots F_n$, and θ unifies F, then there are sustitutions ϕ_1, ϕ_2 such that

(1) ϕ_1 *unifies* F,

(2) $\theta \restriction F = (\phi_2\phi_1) \restriction F$, *and*

(3) $\lg(\phi_1) \leqslant \lg(F)^m$ *where* $m = 2^{\mathrm{rel}(F)}$.

Let S be a finite set of schemata.

LEMMA 2. *There is a function f s.t. for each* NE_1*-derivation D from S there is an* NE_1*-derivation D^* from S and a substitution θ s.t.*

(1) $D = \theta D^*$, *and*

(2) *if A occurs in D^* then* $\lg(A) \leqslant f(\mathrm{length}(D))$.

PROOF. Let w be an injective assignment of 0-ary relation parameters to the formula occurrences of D and let S^* be a finite set of schemata s.t.

(i) each member of S^* is a substitution instance in the unrestricted sense of a member of S,

(ii) each substitution instance in the unrestricted sense of a member of S is a substitution instance in the restricted sense of a member of S. By a copy of a schema we mean the schema up to a permutation of relation parameters. Let W assign to each occurrence of an instance of a member of S^* as an assumption in D a copy of the associated member of S^* so that different occurrences are assigned copies on disjoint sets of new relation parameters. To each formula occurrence in D we assign a sequence of finite sets of formulae as follows ($B \mapsto X$ means X is assigned to B).

(a) A formula occurrence which is the conclusion of an inference by a rule other than $=$ is assigned the sets assigned to the inference in 4.2.2 on p. 253 of [3]. Namely:

(i) If B is the conclusion of

$$\frac{\begin{array}{c}(A) \neq \varnothing\\ C\end{array}}{A \to C}$$

then

$$B \mapsto \{w(F) \to w(C):\ F \in (A)\} \cup \{w(B)\}.$$

(ii) If B is the conclusion of

$$\frac{C}{A \to C}$$

then

$$B \mapsto \{U \to w(C),\ w(B)\}$$

for U a new 0-ary relation parameter.

(iii) If B is the conclusion of

$$\frac{\begin{matrix}(\neg B)\\ \bot\end{matrix}}{B}$$

then

$$B \mapsto \{w(\bot), \bot\}\{w(C): C \in (\neg B)\} \cup \{w(B) \to \bot\}.$$

(iv) If B is the conclusion of

$$\frac{A \to B \quad A}{B}$$

then

$$B \mapsto \{w(A) \to w(B), w(A \to B)\}.$$

(v) If B is the conclusion of

$$\frac{A(u)}{\forall x A(x)}$$

then

$$B \mapsto \{w(A(u)), Uu\}\{w(\forall x A(x)), \forall x Ux\}$$

for U a new 1-ary relation parameter and u a proper parameter.

(vi) If B is the conclusion of

$$\frac{A}{\forall x A}$$

then

$$B \mapsto \{w(A), U\}\{w(\forall x A), \forall x U\}$$

for U a new 0-ary relation parameter.

(vii) If B is the conclusion of

$$\frac{\forall x A(x)}{A(t)}$$

then

$$B \mapsto \{w(A(t)), Ut\}\{w(\forall x A(x)), \forall x Ux\}$$

for U a new 1-ary relation parameter, and x actually occurring free in $A(x)$.

(viii) If B is the conclusion of

$$\frac{\forall x A}{A}$$

then

$$B \mapsto \{w(A), U\}\{w(\forall x A), \forall x U\}$$

for U a new 0-ary relation parameter.

(b) If B is the conclusion of

$$\frac{A(a) \quad a \ominus b}{A(b)}$$

then

$$B \mapsto \{w(A(a)), Ua\}\{w(A(b)), Ub\}\{w(a \ominus b), a \ominus b\}$$

for U a new 1-ary relation parameter.

(c) If B is the conclusion of

$$\frac{A \quad a \ominus b}{A}$$

then

$$B \mapsto \{w(a), U\}\{w(B), U\}\{w(a \ominus b), a \ominus b\}$$

for U a new 0-ary relation parameter.

(d) If B is an axiom occurrence then

$$B \mapsto \{w(B), \forall x(x = x)\}.$$

(e) If B is an occurrence of an instance of a member of S^* as an assumption then

$$B \mapsto \{w(B), \bigvee\!\!\bigvee(B)\}$$

(f) Otherwise, $B \mapsto \{w(B)\}$, where $a \ominus b$ means ambiguously $a = b$ and $b = a$. (Below, in order to apply Lemma 4.2.1 of [3] we shall allow relation constants to be the arguments of substitutions.)

Let F be the sequence of all such sets, then there is a substitution θ such that θ unifies F, $\theta R = R$ for each relation constant in F, and for each occurrence A in D we have $A = \theta w(A)$. By Lemma 4.2.1 of [3, p. 252] there are $\phi_1\phi_2$ satisfying the conditions (1), (2), and (3) stated there; let D^* result from D by replacing each formula occurrence A by $\phi_1 w(A)$ (and apply a permutation of relation symbols to replace $\phi_1 R$ by R).

We now compute an upper bound for $\lg(A)$ for A occurring in D^*. Let $m = \max\{\lg(B): B \in \Gamma^*\}$ and $k = \max\{\mathrm{rel}(B): B \in S^*\}$, then $\lg(F) < \max\{m, 3\}$ and $\mathrm{rel}(F) \leqslant (2 \cdot lh(D) + 1) \cdot \max\{k, 2\}$. Now $\lg(A) < \lg(\phi_1) \cdot \lg(F)$; thus there is a linear e s.t. $\lg(A) \leqslant 2_2^{e(\mathrm{lh}(D))}$, where $2_2^x = 2^{(2^x)}$.

Proposition. *Suppose S has an infinite model then there is a function f s.t. for simple B,*

$$S \mathrel{\vert\!\!\frac{n}{\mathrm{NE}_1}} B \Rightarrow \mathrel{\vert\!\!\frac{f(n)}{\mathrm{NE}_0}} B.$$

Proof. Note that if $\theta A = B$ and B is simple then A is simple. Also, if A is simple and $S \models A$ then A is valid. The proposition now follows from the lemmas.

III. One special case of the theorem is that Theorem 4 of [2] holds for any of the usual formulations of first-order arithmetic (the corresponding result for the ε-calculus can be found in [1, Theorem 2, p. 107]). More precisely, analysis is an unbounded speed-up of arithmetic for quantifier-free formulae.

References

1. G. Kreisel and H. Wang, *Some applications of formalized consistency proofs*, Fund. Math. **42** (1955), 101–110.

2. R. Parikh, *Some results on the length of proofs*, Trans. Amer. Math. Soc. **177** (1973), 29–36.

3. R. Statman, *Proof-search and speed-up in the predicate calculus*, Ann. Math. Logic **15** (1978), 225–287.

Department of Mathematics, Rutgers University, New Brunswick, New Jersey 08903