TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 177, March 1973

SOME RESULTS ON THE LENGTH OF PROOFS

BY

R. J. PARIKH

ABSTRACT. Given a theory T, let $\vdash_T^k A$ mean "A has a proof in T of at most k lines". We consider a formulation PA^* of Peano arithmetic with full induction but addition and multiplication being ternary relations. We show that $\vdash^k A$ is decidable for PA^* and hence PA^* is closed under a weak ω-rule. An analogue of Gödel's theorem on the length of proofs is an easy corollary.

1. **Introduction.** In this paper we shall consider questions regarding the length([1]) of proofs. Now the length of (the shortest) proof of a given formula in a formal system depends strongly on the way in which the system is presented. E.g. adjoining one of the theorems as an axiom reduces the length of some proofs. Thus in order to get significant results, we have either to confine ourselves to particular formalisations of particular theories or else to formulate a criterion which distinguishes "nice" and "not so nice" formalisations of the same theory. We shall take here the second approach. In particular we shall consider theories formalised in some language of the lower predicate calculus by means of a finite number of axioms, axiom schemata and schematic rules of inference. Formalisations of this kind will include Hilbert type and Gentzen type formalisations of classical and intuitionistic arithmetic.

2. **Schematic systems.** Since axiom schemata and rules of inference are generally explained in the literature with the help of formula variables, in order to define the notion of a schematic system we do the obvious, namely, we expand the notation of the predicate calculus to include metamathematical symbols and emphasize substitution as the central idea. Precise details follow:

(a) Notation of the predicate calculus:

(i) variables: $x, y, z, x_1, \cdots,$

Received by the editors December 2, 1970.

AMS (MOS) subject classifications (1969). Primary 1018, 0230.

Key words and phrases. Peano arithmetic, length of proofs, Presburger arithmetic.

([1]) Throughout this paper the length of a proof will mean the number of lines. See [Pa$_4$] for related results where the length is taken to be the number of symbols.

(ii) constants: $c, c_1, c_{11}, \cdots$,

(iii) n-ary predicate symbols for $n \geq 0$: $F, G(x), H(x, y), \cdots$,

(iv) function symbols: $f, g, h, f_1, \cdots$,

(v) logical symbols: $\neg$, &, $\vee$, $\rightarrow$, $\forall$, $\exists$ etc.,

(vi) brackets.

Remark. We do not assume that all the apparatus mentioned in (ii)$\rightarrow$(v) is present.

(b) Metanotation:

(i) metavariables: $u, v, w, u_1, \cdots$,

(ii) term variables: $r, s, t, r_1, \cdots$,

(iii) n-ary predicate (formula) variables for $n \geq 0$: $P, Q(x), R(x, y), \cdots$.

We can assume without loss of generality that the n in (iii) is bounded above, but we shall need infinitely many n-ary predicate variables for each permissible n.

Terms will be formed from variables, constants, metavariables and term variables, by means of the function symbols. Lower case Greek letters will denote terms. Terms which do not have metanotation will be called regular terms, and will be denoted by early Greek letters $\alpha, \beta, \cdots$.

Atomic formulae will be formed from the predicate variables and constants by adjoining terms. Formulae will be formed from these in the usual way with truth functional connectives and quantifiers $\forall x$, $\exists x$, $\forall u$, $\exists u, \cdots$. Formulae will be denoted by script letters, by roman if they are regular.

Substitution. A substitution δ will be an assignment of variables $x_1, \cdots, x_n$ to certain metavariables $u_1, \cdots, u_n$, of regular terms $\alpha_1, \cdots, \alpha_m$ to certain term variables $t_1, \cdots, t_m$, and of regular formulae $A, B, \cdots$ to certain predicate variables $P, Q(x), \cdots$. The substitutions will be informal objects used to study the formal system and the variables after the $P, Q, \cdots$ will always be such as to avoid conflict.

δ will induce a map, also called δ, from certain terms to regular terms, defined uniquely by

$$\delta(u_i) = x_i, \quad \delta(t_j) = \alpha_j, \qquad i = 1, \cdots, n, \ j = 1, \cdots, m,$$

and

$$\delta(f(\sigma_1, \cdots, \sigma_k)) = f(\delta(\sigma_1), \cdots, \delta(\sigma_k))$$

provided that right-hand side is defined, and f is a k-ary function symbol. We can define $\delta(\mathcal{F})$ for certain formulae $\mathcal{F}$ by

Definition. (i) $\mathfrak{F}$ atomic with regular predicate symbol: $\mathfrak{F} = F(\sigma_1, \cdots, \sigma_k)$. Then $\mathfrak{S}(\mathfrak{F}) = F(\mathfrak{S}(\sigma_1), \cdots, \mathfrak{S}(\sigma_k))$ provided that the right-hand side is defined.

(ii) $\mathfrak{F}$ atomic with a predicate variable $P(x_1, \cdots, x_k)$ for the predicate symbol: $\mathfrak{F} = P(\sigma_1, \cdots, \sigma_k)$, $\mathfrak{S}(P(x_1, \cdots, x_k)) = A$. Then $\mathfrak{S}(\mathfrak{F}) = S(x_1, \cdots, x_k; \mathfrak{S}(\sigma_1), \cdots, \mathfrak{S}(\sigma_k))A$ (if defined) where S is the usual substitution and only free occurrences of the x_i are substituted for.

(iii) $\mathfrak{S}(\mathfrak{F} \,\&\, \mathfrak{G}) = \mathfrak{S}(\mathfrak{F}) \,\&\, \mathfrak{S}(\mathfrak{G})$, etc.,

(iv) $\mathfrak{S}((\forall x)\mathfrak{F}) = (\forall x)\mathfrak{S}(\mathfrak{F})$,

(v) $\mathfrak{S}((\forall u)\mathfrak{F}) = (\forall \mathfrak{S}(u))\mathfrak{S}(\mathfrak{F})$, etc.

Admissible restrictions. A restriction is called admissible if it is of the form "provided σ is free for u (for x) in P" or "provided $u(x)$ is not free in P" or "provided $u(x)$ does not occur in $P(\sigma)$" where u is a metavariable, x is a variable, σ is a term and P is a predicate variable.

It is clear what is meant by a substitution $\mathfrak{S}$ obeying a restriction R. E.g. $\mathfrak{S}$ obeys "provided σ is free for u in P" iff $\mathfrak{S}(\sigma)$ is free for $\mathfrak{S}(u)$ in $\mathfrak{S}(P)$. A substitution obeys a finite set of restrictions iff it obeys all of them. Henceforth we shall use the expression "restriction", meaning admissible restriction.

Thus an axiom schema will be simply an ordered pair $(\mathfrak{F}, R)$ where $\mathfrak{F}$ is a formula and R is a finite set of restrictions. Axioms falling under the schema will be formulae $\mathfrak{S}(\mathfrak{F})$ where $\mathfrak{S}$ obeys R. Similarly a k-ary rule of inference will be a sequence $(\mathfrak{F}_1, \cdots, \mathfrak{F}_k, \mathfrak{G}, R)$ where $\mathfrak{F}_1, \cdots, \mathfrak{F}_k, \mathfrak{G}$ are formulae and R is a finite set of restrictions, and will be applied as follows: "If $A_1, \cdots, A_k, B$ are $\mathfrak{S}(\mathfrak{F}_1), \cdots, \mathfrak{S}(\mathfrak{F}_k), \mathfrak{S}(\mathfrak{G})$, respectively and $\mathfrak{S}$ obeys R, then derive B from $A_1, \cdots A_k$."

Since an individual axiom is a special case of an axiom schema, we shall define a schematic system as one given by a finite number of axiom schemata and a finite number of schematic rules of inference. It is clear that a large majority of existing systems in the literature are schematic systems in the sense just described.

3. Two substitution lemmas. Given a proof in a schematic system (which we, for convenience, imagine written in a tree form) by the analysis of this proof we understand a corresponding tree of remarks explaining, for each formula, whether it is an axiom and under which schema, and if derived by a rule, by which rule. By an analysis we shall mean here a tree of such remarks, not necessarily associated with any (possible) proof. Since there are only finitely many analyses of length k, questions regarding proofs of length k can be reduced to questions regarding proofs with a particular analysis $\mathfrak{A}$. The following lemma enables us to dispense with the informal notion of analysis in favour of a syntactic object.

Lemma A. *Given an analysis* $\mathfrak{A}$, *we can effectively find formulae* $\mathfrak{F}_1, \cdots, \mathfrak{F}_m$; $\mathfrak{G}_1, \cdots, \mathfrak{G}_m, \mathfrak{H}$ *with a finite set* R *of restrictions, such that the formula* A *has a*

proof with analysis $\mathfrak{A}$ *iff there is a substitution* $\mathfrak{S}$ *obeying* R *such that* $\mathfrak{S}(\mathcal{F}_i) = \mathfrak{S}(\mathcal{G}_i)$ $(i = 1, \cdots, m)$, $\mathfrak{S}(\mathcal{H}) = A$.

Moreover, the sequence $\mathfrak{S}(\mathcal{F}_1), \cdots, \mathfrak{S}(\mathcal{F}_m), A$, *is the required proof.*

Proof. By induction on k = length of $\mathfrak{A}$.

(a) $k = 1$. Then the analysis reduces to an axiom schema, $m = 0$.

(b) $k > 1$. Let the last step of $\mathfrak{A}$ consist of applying the rule $(\mathcal{L}_1, \cdots, \mathcal{L}_l, \mathcal{M}, R_1)$ to certain previously derived formulae.

Let the component analyses of these previous formulae have sequences $\mathcal{F}_1^1, \cdots, \mathcal{F}_m^1; \mathcal{G}_1^1, \cdots, \mathcal{G}_m^1; \mathcal{H}_1; \cdots, \mathcal{F}_1^l, \cdots; \mathcal{H}_l$ associated with them. We assume that all metasymbols in these different groups have been renamed so that there are no common ones, among different groups or with the $\mathcal{L}_j, \mathcal{M}$. Then the sequence for the analysis A will be $\mathcal{F}_1^1, \cdots, \mathcal{F}_m^1, \mathcal{H}_1, \mathcal{F}_1^2, \cdots, \cdots, \mathcal{H}_l; \mathcal{G}_1^1, \cdots, \mathcal{G}_m^1, \mathcal{L}_1, \mathcal{G}_1^2, \cdots, \mathcal{L}_l; \mathcal{M}$. The restrictions are obtained by putting together all the different restrictions.

Suppose there exists a substitution $\mathfrak{S}$ for this sequence, i.e. such that $\mathfrak{S}(\mathcal{F}_j^i) = \mathfrak{S}(\mathcal{G}_j^i)$, $\mathfrak{S}(\mathcal{H}_i) = \mathfrak{S}(\mathcal{L}_i)$ and $\mathfrak{S}(\mathcal{M}) = A$.

Then by induction hypothesis, each $\mathfrak{S}(\mathcal{H}_i)$ will be provable with the corresponding subproof and, moreover, $\mathfrak{S}(\mathcal{M}) = A$ will be provable from the $\mathfrak{S}(\mathcal{L}_j)$ by the given rule. But $\mathfrak{S}(\mathcal{H}_i) = \mathfrak{S}(\mathcal{L}_i)$. This shows there is a proof as required.

Conversely suppose there is a proof as required. Then each of the premises in the last rule will be provable with the corresponding subproof, and the last formula A provable with the last rule. Hence there will exist substitutions $\mathfrak{S}_1, \cdots, \mathfrak{S}_l, \mathfrak{S}'$ for all these. Since the metavariables have all been renamed to avoid conflicts, we can combine $\mathfrak{S}_1, \cdots, \mathfrak{S}_l, \mathfrak{S}'$ into one substitution $\mathfrak{S}$ as required. Q.E.D.

Notation. In the following, PA will mean one of the usual schematic systems of Peano arithmetic with S, $+$, $\cdot$ and the full induction schema, PA^* will mean the corresponding system with $+$, $\cdot$ replaced by ternary predicates A, M and axioms saying that these represent functions. If T is either of these two systems, then T_l will mean the system with induction confined to formulae of logical complexity $\leq l$. (Here logical complexity is the number of logical symbols.) For *any* theory T, $\vdash_T^k A$ will mean A is provable in T with $\leq k$ applications of rules of inference. (PA, PA^* are of equal strength, but proofs in PA^* will often be longer.) Presburger arithmetic will mean arithmetic with S, $+$, 0 but without multiplication. It is known [Pr] that PA (and hence also PA^*) is complete with respect to closed formulae in which multiplication does not appear.

Lemma B. *Let* $\mathcal{F}_1, \cdots, \mathcal{F}_m, \mathcal{G}_1, \cdots, \mathcal{G}_l, A_1(x), \cdots, A_p(x), R$ *be such that* $\mathcal{F}_1, \cdots, \mathcal{F}_m, \mathcal{G}_1, \cdots, \mathcal{G}_l$ *are formulae of* PA^*, $A_1(x), \cdots, A_p(x)$ *are*

regular formulae of PA, $m = l + p$, and R is a set of restrictions. Then there is a formula $B(x)$ of Presburger arithmetic such that, for all n, $B(\underline{n})$ is equivalent to the proposition, "there is a substitution $\mathfrak{S}$ obeying R such that $\mathfrak{S}(\mathcal{F}_i) = \mathfrak{S}(\mathcal{G}_i)$ for $i \leq l$ and $\mathfrak{S}(\mathcal{F}_{l+i}) = A_i(\underline{n})$ for $i \leq p$."*

Proof. The first part of the argument applies to all schematic systems with O, S as symbols. The last few steps will apply only to PA^*. Fix n and denote $A_i(\underline{n})$ by the expression $\mathcal{G}_{l+i}$. Then we need to find an $\mathfrak{S}$ obeying R such that $\mathfrak{S}(\mathcal{F}_i) = \mathfrak{S}(\mathcal{G}_i)$ is a regular formula of PA^* for $i \leq m$. We first show how to reduce this to the same problem but for the case when the $\mathcal{F}_i$, $\mathcal{G}_i$ are all atomic.

If $x_1, \cdots, x_{n'}$ include all the variables and $u_1, \cdots, u_m$ include all the metavariables occurring in the $\mathcal{F}_i, \mathcal{G}_i, R$, then we can assume without loss of generality that the $\mathfrak{S}(u_j)$ are all among $x_1, \cdots, x_{n'}, \cdots, x_{n'+m}$. The metavariables are thus eliminated.

Suppose $\mathcal{F}_1 = (\mathcal{F}_1' \ \& \ \mathcal{F}_1'')$. If $\mathcal{G}_1$ is not atomic and a substitution $\mathfrak{S}$ exists then $\mathcal{G}_1$ must have the form $(\mathcal{G}_1' \ \& \ \mathcal{G}_1'')$. Moreover, $\mathfrak{S}(\mathcal{F}_1) = \mathfrak{S}(\mathcal{G}_1)$ iff $\mathfrak{S}(\mathcal{F}_1') = \mathfrak{S}(\mathcal{G}_1')$ and $\mathfrak{S}(\mathcal{F}_1'') = \mathfrak{S}(\mathcal{G}_1'')$. Thus we get a correspondence between the subformulae of the $\mathcal{F}_i$, $\mathcal{G}_i$ and by taking minimal subformulae, we can assume that one side, say $\mathcal{F}_i$, is always atomic.

Let $u = \Pi\, 3^{c_i}$ where c_i = number of logical symbols in $\mathcal{G}_i$. If $u = 1$ then the $\mathcal{G}_i$ are all atomic. Consider minimal relations $P \leq Q$, $P \sim Q$ on the predicate variables such that $\leq$ is transitive, $\sim$ is an equivalence relation and $P \leq Q \ \& \ Q \leq P \leftrightarrow P \sim Q$. Moreover, if P occurs in $\mathcal{F}_i$ and Q occurs in $\mathcal{G}_i$ then $Q \leq P$; $Q \sim P$ if $\mathcal{G}_i$ is atomic. It is decidable if such relations exist and if they do not, clearly $\mathfrak{S}$ cannot exist, otherwise we could take $P \leq Q$ to mean the number of logical symbols in $\mathfrak{S}(P) \leq$ the number of logical symbols in $\mathfrak{S}(Q)$.

Suppose $u > 1$. Then there exists a P such that P is maximal in $\leq$, P occurs in $\mathcal{F}_i$, $\mathcal{G}_i$ is not atomic.

Case 1. $\mathcal{G}_i$ is of the form $\mathcal{G}_i' \rightarrow \mathcal{G}_i''$. Replace P and every predicate symbol equivalent to it by the formula $P' \rightarrow P''$ where P', P'' are two new predicate variables. Replace the pair $\mathcal{F}_i = P(-)$, $\mathcal{G}_i = \mathcal{G}_i'(-) \rightarrow \mathcal{G}_i''(-)$ by the two pairs $P'(-)$, $\mathcal{G}_i'(-)$ and $P''(-)$, $\mathcal{G}_i''(-)$. Similarly for predicate variables equivalent to P. The restrictions on P are easily translated in terms of restrictions on P', P'' etc. and u decreases. (If we cannot carry out this procedure because of an implication corresponding, say, to a conjunction, then $\mathfrak{S}$ cannot exist.)

All truth functional combinations are handled similarly.

Case 2. $\mathcal{G}_i$ is of the form $(\forall x)\mathcal{G}_i'$. The reduction is similar, but the condition "σ is free for y in P" becomes "y is not free in P" or "x does

not occur in σ''' if $y \neq x$. The condition "σ is free for x in P" is dropped, etc.

After a finite number of steps we get $u = 1$. The $\mathcal{G}_i$ are all atomic.

Now we can also assume without loss of generality that the $\mathcal{S}(\mathcal{F}_i)$, $\mathcal{S}(\mathcal{G}_i)$ are all essentially atomic. For let $x_1, \cdots, x_n$ be all the variables occurring in R. If there exists a substitution $\mathcal{S}$, we can define $\mathcal{S}'(P)$ = the leftmost atomic subformula of $\mathcal{S}(P)$ preceded by all the quantifiers $(\forall x_i)$, $(\exists x_i)$, $i = 1, \cdots, n$, in whose scope it falls. Then $\mathcal{S}'$ is a solution if $\mathcal{S}$ is.

We can also assume that we know the predicate symbols involved. For to each pair $\mathcal{F}_i = P(-)$, $\mathcal{G}_i = F(-)$, we can assume that the predicate symbol for the predicate variable P *is* F. To all predicate variables not covered by this consideration, a fixed regular formula A can be assigned without loss of generality. Thus we can assume for each predicate variable P that

$$\mathcal{S}(P(y_1, \cdots, y_k)) = (Q_1 x_1) \cdots (Q_p x_p) F_P(\theta_1(y_1, \cdots, y_k), \cdots, \theta_q(y_1, \cdots, y_k))$$

where the Q_i are quantifiers, F_P is known, and the θ_i are certain terms depending on the y_i. Given two such (not obviously inequivalent) formulae, they will be equal iff the corresponding terms are equal.

The argument so far applied to arbitrary schematic systems containing S and 0. The remainder of the argument (below) applies only to PA^*.

An atomic formula in PA^* must be of the form (i) $\theta = \theta'$, (ii) $A(\theta, \theta', \theta'')$ or (iii) $M(\theta, \theta', \theta'')$ where $\theta, \theta', \theta''$ are of the form $S^q 0$ or $S^q x$ where x is a variable. Moreover, the possible variables can be restricted to a finite set of possibilities.

Thus a substitution is given completely by specifying (a) for each F_P whether it is $=$, A or M and for each θ whether it is $S^q 0$ or $S^q x$ and (b) specifying the values q_i where $\theta_i = S^{q_i} 0$ or $S^{q_i} x$ or the term variable $t_i = S^{q_i} 0$ or $S^{q_i} x$.

Now, part (a) consists of choosing one among finitely many possibilities. For each of these possibilities, the condition for $\mathcal{S}$ to give $\mathcal{S}(\mathcal{F}_i) = \mathcal{S}(\mathcal{G}_i)$ reduces to the various numbers q_i satisfying certain equations in Presburger arithmetic. Thus if we consider all possible ways in which $\mathcal{S}$ can exist for a particular n, we get an equivalence: $\mathcal{S}$ exists iff $B_1(\underline{n}) \vee \cdots \vee B_r(\underline{n})$ where each B_i is a formula in Presburger arithmetic. Now take $B(x)$ to be $B_1(x) \vee \cdots \vee B_r(x)$. This proves Lemma B. Q.E.D.

4. Applications to length of proofs.

Theorem 1. (a) *It is uniformly decidable in k, A if $\vdash^k_{PA^*} A$ holds or not.*

(b) *Let $B(x)$ be a formula of PA^*, $k \in N$. Then the set $\{n \mid \vdash^k_{PA^*} B(\underline{n})\}$ is a finite union of arithmetic (linear) progressions.*

Proof. (a) is an immediate consequence of Lemmas A, B and the fact that Presburger arithmetic is decidable. To see (b) we notice the following. It follows from Lemmas A and B that there is a formula $B'(x)$ of Presburger arithmetic such that $\vdash^k_{PA^*} B(\underline{n})$ iff $B'(\underline{n})$ is true. However, by [GS], the set $\{n \mid B'(\underline{n}) \text{ is true}\}$ is semilinear, i.e. a finite union of arithmetic progressions. Q.E.D.

Theorem 2. *Let T be PA or PA^*, $k, k' \in N$. Then there exists a number l depending only on k, k' such that, for every formula A of complexity $\leq k'$, $\vdash^k_T A$ iff $\vdash^k_{T_l} A$. Moreover, l can be found effectively from k, k'.*

Proof. We confine ourselves to a particular analysis $\mathfrak{A}$ of k lines and investigate the existence of substitutions for the sequence $\langle \mathcal{F}_1, \cdots, \mathcal{F}_m, \mathcal{H}, \mathcal{G}_1, \cdots, \mathcal{G}_m A, R\rangle$ where $\mathcal{F}_1, \cdots, \mathcal{F}_m, \mathcal{G}_1, \cdots, \mathcal{G}_m, \mathcal{H}$ is the sequence provided by Lemma A. Since $c(A) \leq k'$, there are only finitely many ways in which A can be decomposed into atomic formulae. The rest of the argument is quite similar to that in Lemma B.

(In fact suppose the maximum complexity of any formula occuring as axiom, axiom schema or in a schematic rule of inference, is α. Then the complexity of any $\mathcal{F}_1$, $\mathcal{G}_i$ or $\mathcal{H}$ is at most α. Since $m = k - 1$, the initial value of u is $u_0 = 3^{\alpha(2k-1)}3^{k'}$. Now the analysis of Lemma B reduces the value of u until it becomes 1. If the maximum complexity $m(u)$ of any formula at a certain stage in this reduction was x, then the maximum complexity at a preceding stage could not have been greater than $2x + 1$. Now $m(1) = k$ since the images can be taken to be essentially atomic, and $m(u + 1) \leq 2m(u) + 1$. We immediately see that $l = m(u_0) \leq 3^{u_0}$.)

Theorem 3.(2) $\vdash_{PA^*} (\forall x)A(x)$ *iff there is a k such that* $(\forall n) \vdash^k_{PA^*} A(\underline{n})$.

Proof. One implication is trivial. A proof of $(\forall x)A(x)$ of l lines gives uniform proofs of $A(\underline{n})$ for all n, of $l + 2$ lines.

For the converse, we note that the arguments of Theorems 1 and 2 can be formalized in PA^*. Thus suppose we have

$$(\forall n) \vdash^k_{PA^*} A(\underline{n}).$$

Then for the corresponding formula $B(x)$ of Presburger arithmetic, $(\forall x)B(x)$ is true and hence $\vdash_{PA^*} (\forall x)B(x)$. Combining this with (formal versions of) Theorems 1 and 2, we get

$$\vdash_{PA^*} \text{“}(\forall n) \vdash_{PA^*_l} A(\underline{n})\text{”}.$$

---

(2) This result (for PA) was originally conjectured by Kreisel, to whom I am also indebted for continuing encouragement.

However, by [KW], a truth definition for PA^*_l can be given within PA^*. Thus we get $\vdash_{PA^*} (\forall x)A(x)$. Q.E.D.

Theorem 4. *Let T be one of the usual formalisations of analysis; f any function from N to N. Then there exists a Theorem A of PA^* and a number n such that $\vdash^n_T A$ holds but $\vdash^k_{PA^*} A$ does not hold where $k = f(n)$.*

Proof. Let the consistency of PA^* be expressed as a formula $(\forall x)B(x)$. This formula has a proof in T of, say, l steps. Take $n = l + 2$, then for every m, $\vdash^n_T B(\underline{m})$. However, $(\forall m)\vdash^k_{PA^*} B(\underline{m})$ would give $\vdash_{PA^*} (\forall x)B(x)$. Hence $(\exists m) \neg \vdash^k_{PA^*} B(\underline{m})$. Take A to be $B(\underline{m})$. Q.E.D.

This result, of course, will hold for much weaker systems than analysis.

We do not know if Theorems 1–4 hold for PA. The problem, of course, is in proving Lemma B, since atomic formulae of PA can be much more complex than those of PA^*.

REFERENCES

[GS] S. Ginsburg and E. Spanier, *Semigroups, Presburger formulas, and languages*, Pacific J. Math. 16 (1966), 285–296. MR 32 #9172.

[KW] G. Kreisel and H. Wang, *Some applications of formalized consistency proofs. I, II*, Fund. Math. 42 (1955), 101–110; ibid. 45 (1958), 334–335. MR 17, 447; MR 20 #4483.

[Pa_1] R. Parikh, *A decidability result for first order systems*, J. Symbolic Logic 30 (1965), 269. (abstract)

[Pa_2] ———, *Some results on lengths of proofs*, Notices Amer. Math. Soc. 13 (1966), 487. Abstract #66T–255.

[Pa_3] ———, *On context-free languages*, J. Assoc. Comput. Mach. 13 (1966), 570–581. MR 34 #8901.

[Pa_4] ———, *Existence and feasibility in arithmetic*, J. Symbolic Logic 36 (1971), 494–508.

[Pr] M. Presburger, *Über die Vollständigkeit eines gewissen Systems der Arithmetic ganzer Zahlen*, Comptes-rendus du I congrès des mathématiciens de pays Slaves, Warsaw, 1929, 1930, pp. 92–101, 395.

[R] D. Richardson, *Some theorems with short proofs* (to appear).

DEPARTMENT OF MATHEMATICS, BOSTON UNIVERSITY, BOSTON, MASSACHUSETTS 02215