ISRAEL JOURNAL OF MATHEMATICS, Vol. 39, No. 3, 1981

THE COMPLETENESS OF PEANO MULTIPLICATION

BY

MARK E. NADEL[†]

ABSTRACT

It is shown that the set of all theorems of Peano Arithmetic which mention only multiplication is a complete theory in the corresponding restricted language. The notion of a complete decidable covering of a theory is introduced.

§0. By Peano Addition (usually called Presburger Arithmetic) we mean the set of all theorems of Peano Arithmetic which do not mention multiplication. By Complete Addition we mean the complete theory of $(\omega, +)$, the natural numbers with addition. Presburger [10] gave a quantifier elimination for Peano Arithmetic in a language augmented by some basic definable relations. This showed that Peano Addition was decidable, complete, and hence the same as Complete Addition.

Let us now define Peano Multiplication and Complete multiplication in an analogous way. The best known proof of the decidability of Peano Multiplication originated with Mostowski [8]. His method of proof was a precursor of what is today usually called the Feferman–Vaught Method [4]. The idea is basically this. The set of positive integers with multiplication is isomorphic to the weak direct product of countably many copies of the non-negative integers. To see this, think of the nth coordinate of an element of the direct sum as representing the exponent of the nth prime in the prime decomposition. Now, the decidability of the multiplicative system is obtained from the decidability of Complete Addition and the decidability of the theory of the Boolean algebra of all finite and co-finite subsets of ω, together with the ideal of finite sets [cf. 11]. In an earlier paper [12] Skolem had suggested a quantifier elimination for complete multiplication and gave what we would call today a proof by example.

[†] The author was partially supported by N.S.F. Grant No. MC578-02224.
Received February 25, 1980 and in revised form February 18, 1981

It would only seem natural to investigate whether the situation for multiplication is analogous to that for addition. Is Peano Multiplication complete, or alternatively, is Peano Multiplication the same as Complete Multiplication? If not, is Peano Multiplication at least decidable? The first question seems especially appropriate in view of the recent renewed interest in sentences undecidable in Peano Arithmetic [cf. 9].

In our review of the literature, though we found numerous references to the decidability of Complete Multiplication, we found little or no mention of the problem for Peano Multiplication and most of what we did find seemed confused. For example, as was pointed out to us after we completed the work on this paper, it is stated in [5] that Peano Multiplication is complete, and Malcev [7] is cited as a reference. However Malcev [7], which is concerned with a more general question of giving a quantifier elimination for "locally free algebras", deals only with non-associative algebras and so does not apply to the present context.

The following is the main result of the present paper and gives an affirmative answer to the questions stated above.

THEOREM. *Peano Multiplication is complete and hence decidable.*

This result was discovered independently by P. Cegielski whose proof involves a direct quantifier elimination for Peano multiplication, and so differs considerably from the more "model theoretic" proof presented herein. Even though our proof is quite short, it still follows by noticing the few properties of arithmetic we actually use, that only a small amount of induction is really needed.

An arbitrary model of Peano Multiplication, nor even the multiplicative semigroup of a model of Peano Arithmetic, need not be a weak direct product, though, in the latter case it would appear to be a weak direct product from the viewpoint of the model of Peano Arithmetic. This, of course, raises the possibility of trying to formalize the Skolem–Mostowki argument within Peano Arithmetic and in such a way obtain a proof of the Theorem. The approach we will adopt, which appears to be simpler and perhaps more intuitive, will be to work purely externally. We will need to make use of the completeness of Peano Addition rather than the decidability of Complete Addition.

We should like to express our gratitude to Y. Gurevich, V. Harnick, H. J. Keisler, J. Knight, L. Lipshitz, M. Rabin, S. Shelah, C. Smorynski and R. Vaught for conversations relating to the preparation of this paper, and to the University of Bar Ilan where much of the preparation took place.

§**1.** In proving the Theorem we will use the continuum hypothesis. Of course, since the continuum hypothesis holds in L, the universe of constructible sèts, and since the completeness of Peano Multiplication is absolute between L and the real universe, the dependence of the proof upon the continuum hypothesis is only virtual.

Throughout this paper we will use the term *saturated model* to denote a $\aleph_1$-saturated model of cardinality $\aleph_1$. The continuum hypothesis guarantees the existence of saturated models. Even without the continuum hypothesis, a complete theory T can have, up to isomorphism, at most one saturated model. In particular if L and L' are alphabets with $L \subset L'$ and T and T' are theories in L and L' respectively such that $T \subset T'$ and T is complete, then the reduct of a saturated model of T' to L must be the unique saturated model of T. On the other hand, a saturated model of T can always be "expanded" to a saturated model of T'. We will establish the Theorem by proving

LEMMA. *Let* $\langle A, +, \cdot \rangle$ *and* $\langle B, +, \cdot \rangle$ *be saturated models of Peano Arithmetic. Then,* $\langle A, \cdot \rangle \equiv \langle B, \cdot \rangle$.

Then, since any saturated model of Peano Multiplication can be expanded to a saturated model of Peano Arithmetic, it follows that Peano Multiplication has a unique saturated model, and so is complete.

§**2.** Before beginning the proof of the Lemma in earnest, we familiarize ourselves with the basic structure of a model $\langle A, \cdot \rangle$ where $\langle A, +, \cdot \rangle \models P$. Though much of what we say here would hold as well for arbitrary models of Peano Multiplication, in this special context a clearer picture can be painted. We will use familiar terms, such as prime, without explicitly defining them in the formalism of Peano Multiplication or Peano Arithmetic, but such definitions can be easily formulated. Of course, there will be, for example, non-standard primes in a non-standard model.

The first thing to notice is that each non-zero element a has a prime decomposition. Specifically, we can associate with each non-zero element a a function d_a from the set P of all primes of A into A, where for each $p \in P$ $d_a(p)$ is the highest power of p that divides a. It is easy to prove in Peano Arithmetic, using mathematical induction, that such a power exists and is unique. In fact, the function $d_a(p)$ of both a and p is definable in $\langle A, +, \cdot \rangle$.

Moreover, the prime decomposition determines the element, i.e. if $d_a = d_b$, then $a = b$. To see this, suppose a is the least element such that for some $b > a$, $d_a = d_b$. Then, using the division algorithm, there is x, and $y < a$, such that

$b = xa + y$. It is now easy to check using some simple theorems of Peano Arithmetic that $d_y = d_b$, contradicting the minimality of a.

Next, the familiar rule for adding exponents will guarantee that $d_{a\cdot b}(p) = d_a(p) + d_b(p)$, where the $+$ comes from $\langle A, +\rangle$. Now, since Peano Addition is complete, if $\langle A, +, \cdot\rangle$ is saturated, $\langle A, +\rangle$ is uniquely determined. Thus, once we have the prime decompositions, multiplication will be determined.

Finally, later we will make use of the following simple fact which is easily proved in Peano Arithmetic.

(*) Let $p_0, \cdots, p_{n-1}$ be primes and $a_0, \cdots, a_{n-1}$ arbitrary elements. There is some element f such that for each $i < n$, $d_f(p_i) = a_i$.

§3. We now prove the Lemma. For the remainder of this section $\langle A, +, \cdot\rangle$ and $\langle B, +, \cdot\rangle$ will denote saturated models of Peano Arithmetic. We will actually show $\langle A, \cdot\rangle \equiv_{\infty\omega} \langle B, \cdot\rangle$. We first introduce the terminology necessary to describe the back and forth relation.

First, for $a_0, \cdots, a_{n-1} \in A$, $b_0, \cdots, b_{n-1} \in B$, we write $(a_0, \cdots, a_{n-1}) \equiv (b_0, \cdots, b_{n-1})$ iff $(A, +, a_0, \cdots, a_{n-1}) \equiv (B, +, b_0, \cdots, b_{n-1})$. We could, of course, replace $\equiv$ with $\cong$. For future reference we let $\langle \psi_i^n(x_0, \cdots, x_{n-1}) : i \in \omega\rangle$ be a list of all the basic formulas in the n-variables $x_0, \cdots, x_{n-1}$ given by the Presburger quantifier elimination. For this purpose we now assume our models have constants for 0 and 1, which are definable in the structures anyway. Finally, for $a \in A$, we let P_a be the set of primes of A dividing a.

We are now prepared to define the candidate for a back and forth relation. If $f_0, \cdots, f_{n-1} \in A$, $g_0, \cdots, g_{n-1} \in B$, we write

$$(f_0, \cdots, f_{n-1}) \sim (g_0, \cdots, g_{n-1})$$

iff there is a bijection α from the primes of A onto the primes of B such that for each prime p of A,

$$(d_{f_0}(p), \cdots, d_{f_{n-1}}(p)) \equiv (d_{g_0}(\alpha(p)), \cdots, d_{g_{n-1}}(\alpha(p))).$$

Stated slightly differently, given $f_0, \cdots, f_{n-1}$ in A, we associate with each prime p of A the "Presburger n-type" of $(d_{f_0}(p), \cdots, d_{f_{n-1}}(p))$. Then $(f_0, \cdots, f_{n-1}) \sim (g_0, \cdots, g_{n-1})$ iff each n-tuple gives rise to the same number of the same "Presburger n-types". Since we are dealing with saturated models, each such type will be realized either some finite number of times or $\aleph_1$ many times. It is of importance to note that we need only pay attention to the relation between the highest powers of the same prime, and need not compare powers of different primes. It is not difficult to see that the mapping taking f_i to g_i for $i < n$ will be a partial isomorphism from $\langle A, \cdot\rangle$ to $\langle B, \cdot\rangle$.

We now need to show that if $f_0, \cdots, f_{n-1}, f_n \in A$, $g_0, \cdots, g_{n-1} \in B$ and $(f_0, \cdots, f_{n-1}) \sim (g_0, \cdots, g_{n-1})$, then there is some $g_n \in B$ such that $(f_0, \cdots, f_{n-1}, f_n) \sim (g_0, \cdots, g_{n-1}, g_n)$. In order to help find such a g_n we introduce notation for certain formulas. For each $l, m, n \in \omega$ and $s \in {}^l2$ we choose a formula $\theta^n_{s,m}(x_0, \cdots, x_{n-1})$ of the language of Peano Arithmetic which expresses "there are at least m primes p such that for all $k < l$,

$$\psi^n_k(d_{x_0}(p), \cdots, d_{x_{n-1}}(p)) \qquad \text{iff} \quad s(k) = 1."$$

We leave the precise formulation of $\theta^n_{s,m}$ to the reader. Then, relying on the saturation of $\langle A, +, \cdot \rangle$ and $\langle B, +, \cdot \rangle$ we can see that

(1) If $f_0, \cdots, f_{n-1} \in A$, $g_0, \cdots, g_{n-1} \in B$, then $(f_0, \cdots, f_{n-1}) \sim (g_0, \cdots, g_{n-1})$ iff for all s and m, $\langle A, +, \cdot \rangle \models \theta^n_{s,m}(f_0, \cdots, f_{n-1})$ iff $\langle B, +, \cdot \rangle \models \theta^n_{s,m}(g_0, \cdots, g_{n-1})$.

This follows since the formulas $\theta^n_{s,m}$ will determine how many realizations there are of each "Presburger n-type."

We may now consider the following type τ over $g_0, \cdots, g_{n-1}$ consisting of the formulas

(i) $\theta^{n+1}_{s,m}(g_0, \cdots, g_{n-1}, x_n)$ such that $\langle A, +, \cdot \rangle \models \theta^{n+1}_{s,m}(f_0, \cdots, f_{n-1}, f_n)$ and

(ii) $\neg\, \theta^{n+1}_{s,m}(g_0, \cdots, g_{n-1}, x_n)$ such that $\langle A, +, \cdot \rangle \models \neg\, \theta^{n+1}_{s,m}(f_0, \cdots, f_{n-1}, f_n)$.

Since $(f_0, \cdots, f_{n-1}) \sim (g_0, \cdots, g_{n-1})$, each individual "Presburger $(n+1)$-type" is consistent and hence realized since $\langle A, + \rangle \cong \langle B, + \rangle$. Then, by (*) τ is finitely consistent, and so realized in $\langle B, +, \cdot \rangle$ since it is saturated. Then, by (1) above, $(f_0, \cdots, f_n) \sim (g_0, \cdots, g_n)$. Notice that though we do not necessarily preserve the same map from the primes of A onto those of B, this is not required. This finishes the proof.

Now looking back at our proof we see it is possible to extract a quantifier elimination. Using the Presburger quantifier elimination we first see how the relation $\sim$ could have been expressed purely in terms of multiplication.

At the urging of the referee we give some indication of how this may be done. We assume the reader is familiar with the Presburger quantifier elimination in terms of congruences. In order to make our formulas more easily understandable, we employ expressions such as "$x = 1$", "x is a prime", or "$x \mid y$", i.e. x divides y, which we assume the reader can easily translate into the language of multiplication.

First we define a formula $h(x, p, y)$ to say that p is a prime and x is the highest power of p dividing y.

$$h(x, p, y) \equiv_{\mathrm{Df}} p \text{ is a prime } \& \ \forall z [z \mid x \rightarrow$$
$$(p \mid z \vee z = 1)] \ \& \ p \circ x \nmid y.$$

We next define for $n \in \omega$ and $i < n$ a formula $\delta_i^n(a, b, p)$ which expresses $d_a(p) \equiv d_b(p) + i \pmod{n}$.

$$\delta_i^n(a, b, p) \equiv_{\mathrm{Df}} \forall x_1 x_2 [(h(x_1, p, a) \ \&$$

$$h(x_2, p, b)) \to \bigvee_{k, l < n, |k-l| = i} \exists u, v$$

$$[x_1 = \underbrace{u \circ \cdots \circ u}_{n \text{ times}} \circ \underbrace{p \circ \cdots \circ p}_{k \text{ times}} \ \& \ x_2 = \underbrace{v \circ \cdots \circ v}_{n \text{ times}} \circ \underbrace{p \circ \cdots \circ p}_{l \text{ times}}])].$$

Then, it follows that $(a_1, \cdots, a_n) \sim (b_1, \cdots, b_m)$ iff for each $l_1, \cdots, l_m$, $k_1, \cdots, k_m$, m, n and j in ω, and $i < n$,

$$\exists \geqq j_p \delta_i^n(a_1^{l_1} \circ \cdots \circ a_m^{l_m}, a_1^{k_1} \circ \cdots \circ a_m^{k_m})$$

$$\text{iff } \exists \geqq j_p \delta_i^n(b_1^{l_1} \circ \cdots \circ b_m^{l_m}, b_1^{k_1} \circ \cdots \circ b_m^{k_m}).$$

Thus, we see that the complete type in the language of multiplication of any finite tuple of elements is completely determined by formulas of the form just described. Now, using a standard compactness argument it follows that each formula of the language of multiplication is equivalent in PM to some (finite) Boolean combination of these formulas.

§4. In this final section we briefly introduce a general notion prompted by the example of Peano Arithmetic. Peano Arithmetic is, as we all know, an incomplete and undecidable theory. Nonetheless, each model $\langle A, +, \cdot \rangle$ of Peano Arithmetic can be split into two parts, $\langle A, + \rangle$ and $\langle A, \cdot \rangle$, where $\langle A, + \rangle$ is a model of Peano Addition, a complete decidable theory, and $\langle A, \cdot \rangle$ is a model of Peano Multiplication, also a complete decidable theory. Moreover, Peano Arithmetic even has a model, viz., the standard model $\langle \omega, +, \cdot \rangle$, such that both $\langle \omega, + \rangle$ and $\langle \omega, \cdot \rangle$ are decidable, i.e. have recursive complete diagrams for some appropriate arithmetization. We wish to abstract this situation and generalize it so that the splitting need not be simply by reducts.

In order to do this we will need to employ the notion of an interpretation of one alphabet into another. For our purposes, by an *interpretation* α from an alphabet $\mathscr{L}$ into an alphabet $\mathscr{L}'$, written $\alpha : L \to L'$, we mean a mapping that assigns to each symbol of $\mathscr{L}$ a quantifier free expression of $\mathscr{L}'$ of the appropriate type, e.g. a 3-place relation symbol would be sent to a quantifier free formula with 3 free variables, while a 2-place function symbol would be sent to a term with 2 free variables. For the present we will assume all alphabets finite. Given $\alpha : \mathscr{L} \to \mathscr{L}'$ and an $\mathscr{L}'$-structure $\mathscr{M}$, we can define, in a fairly obvious way, the associated $\mathscr{L}$-structure $\mathscr{M}^{-\alpha}$ obtained from $\mathscr{M}$ by using α. If $\mathscr{M}$ is recursive, i.e.

has a recursive atomic diagram for some arithmetization, then $\mathcal{M}^{-\alpha}$ is easily seen to be recursive.

Before proceeding to the next definition, we should like to emphasize that we do not regard it as being necessarily in its final form. It is quite likely that further investigation may lead to some modification. Nevertheless, the present discussion should remain meaningful under foreseeable modifications.

Definition. Let T be a theory in the alphabet $\mathcal{L}$. By a *complete decidable covering of* T we mean a collection of complete decidable theories $T_1, \cdots, T_n$ in disjoint alphabets $\mathcal{L}_1 = \{R_1^1, \cdots\}, \cdots, \mathcal{L}_n = \{R_1^n, \cdots\}$ and an interpretation $\alpha : \mathcal{L} \to \cup \cdots \cup \mathcal{L}_n$ and interpretations $\alpha_i : \mathcal{L}_i \to \mathcal{L}$, for $i = 1, \cdots, n$ such that

(i) for each model $\mathcal{M}$ of T there are models $\langle N, R_1^1 \cdots \rangle \models T_1, \cdots, \langle N, R_1^n, \cdots \rangle \models T_n$ such that

$$\langle N, R_1^1, \cdots, \cdots, R_1^n, \cdots \rangle^{-\alpha} \cong \mathcal{M};$$

(ii) there is some model $\mathcal{M}$ of $T_1 \cup \cdots \cup T_n$ such that $\mathcal{M}^{-\alpha} \models T$ and $\mathcal{M} \restriction \mathcal{L}_i$ is decidable for each $i = 1, \cdots, n$.

We now proceed immediately to a concrete example. For T we will take the theory ZF + $\neg$ Infinity, consisting of the axioms of ZF with the negation of the axiom of infinity, rather than the axiom of infinity itself. The alphabet $\mathcal{L}$ consists, of course, of the binary relation symbol $\in$. This theory T is easily seen to be incomplete and undecidable since Peano Arithmetic can be interpeted within it. One may regard $\langle \mathrm{HF}, \in \rangle$, where HF is the set of hereditarily finite sets, as the standard model of T.

We will now cover T with two complete theories T_1 and T_2. T_1 will be in the alphabet $\mathcal{L}_1$ consisting of a single unary function symbol which we denote by $\boldsymbol{F}$. Specifically, T_1 will be the complete theory of $\langle \mathrm{HF}, \{\ \ \}\rangle$ where $\{\ \ \}$ denotes the operation of taking the singleton of a set. T_2 will be in the alphabet $\mathcal{L}_2$ consisting of the single binary relation symbol $\boldsymbol{R}$. Specifically, T_2 will be the complete theory of $\langle \mathrm{HF}, \subseteq \rangle$. For the interpretation we take $\alpha(\in) = R(F(\ \ ),\ \ )$. The idea is, of course, that $x \in y$ iff $\{x\} \subseteq y$.

We must now verify that T_1, T_2 and α give a complete decidable covering of T. To that end, let $\langle A, E \rangle \models T$. Consider the associated models $\langle A, \{\ \ \}\rangle$ and $\langle A, \subseteq \rangle$ where $\{\ \ \}$ and $\subseteq$ are defined within $\langle A, E \rangle$ as usual. We must show first that these structures are models of T_1 and T_2, respectively. We consider the two separately. First, suppose A is countable. Then, it is not difficult to see that $\langle A, \{\ \ \}\rangle$ is isomorphic to the positive integers with the function that assigns to each number its square. [It may be surprising at first how little of E remains when we look only at $\{\ \}$.] Consequently, $\langle A, \{\ \}\rangle \cong \langle \mathrm{HF}, \{\ \}\rangle$ and so $\langle A, \{\ \}\rangle \models T_1$. In particular, T_1 must be nothing but the theorems of T that can be written using only the defined symbol "$\{\ \}$", and as such must be decidable, since it is complete.

We will handle $\langle A, \subseteq\rangle$ indirectly. We observe first that $\langle A, \subseteq\rangle$ is always an infinite atomic distributive lattice. The theory of such lattices is known to be complete [cf. 2]. This can alternatively be obtained from the completeness of the theory of infinite atomic Boolean algebras with a unary predicate which forms a non-principal prime ideal.

Now, to verify (ii) we will use the fact that $\langle \omega, \cdot\rangle$ is decidable. It is quite easy to see this since in $(\omega, \cdot)$ each element, and, in fact, each finite tuple of elements can be described up to automorphism by a single formula. We claim that $\langle \mathrm{HF}, \{\ \}\rangle$ and $\langle \mathrm{HF}, \subseteq\rangle$ are each decidable. The first follows since, as we observed above, $\langle \mathrm{HF}, \{\ \}\rangle$ is isomorphic to $\omega\backslash\{0\}$ with the squaring function and 0 and the squaring function are definable in $\langle \omega, \cdot\rangle$. The second follows by a similar argument. Call a positive integer *square free* if it is not divisible by any square. Then, $\langle \mathrm{HF}, \subseteq\rangle$ is easily seen to be isomorphic to the set of square free positive integers with the relation of divisibility. Again, both the class of square-free positive integers and the relation of divisibility are definable in $\langle \omega, \cdot\rangle$.

The case in which a theory has a complete decidable covering is certainly the exceptional one. For example, if T is any extension of Peano Arithmetic inconsistent with Complete Arithmetic, then T has no recursive model (actually, even the additive part alone cannot be recursive) and so (ii) in the definition could never be satisfied. This last result is due to Tennenbaum, (cf. [2]) and follows quite easily from the main result of [6]. The same applies to any "set theory" T inconsistent with the complete theory of $\langle \mathrm{HF}, \in\rangle$, in particular, ZF itself.

As we have seen, the property of a theory T having a complete decidable covering lies between the properties of T being complete decidable and T having a recursive model. The three properties are strictly different. We have also seen examples that show that a theory with a complete decidable covering need not be decidable. Conversely, a decidable theory need not have a complete decidable covering. A decidable theory such as the theory of Abelian groups cannot have a complete decidable covering since it has finite models of different sizes.

The next step in this program, which we will not undertake here, is the introduction of a weaker notion of decidable covering in which completeness is not required. It would then be of interest to see whether certain important theories, e.g., group theory or field theory, had decidable coverings. The hope would be that using these notions of coverings, in addition to the notions of completeness and decidability, particular theories could be viewed in a more enlightening way.

References

1. P. Cegielski, *Theorie elementaire de la multiplication des entiers naturel*, Doctoral dissertation, University Pierre et Marie Curie, Paris 6, 1980.

2. A. Ehrenfeucht and G. Kreisel, *Strong models for Arithmetic*, Bull. Acad. Polon. Sci. **14** (1966), 107–110.

3. Yu. Ershov, *Decidability of relatively complemented distributive lattices and the theory of filters*, Algebra i Logika **3** (1964), 17–38.

4. S. Feferman and R. Vaught, *First order properties of products of algebraic systems*, Fund. Math. **47** (1959), 57–102.

5. D. Jensen and A. Ehrenfeucht, *Some problems in elementary arithmetics*, Fund. Math. **92** (1976), 223–245.

6. L. Lipshitz and M. Nadel, *The additive structure of models of arithmetic*, Proc. Amer. Math. Soc. **68** (3) (1978), 331-336.

7. A. Malcev, *Axiomatizable classes of locally free algebras of various types*, in chapter 23, *The Metamathematics of Algebraic Systems*, North-Holland, 1971.

8. A. Mostowski, *On direct products of theories*, J. Symbolic Logic **17** (1952), 1–31.

9. J. Paris and L. Harrington, *A mathematical incompleteness in Peano Arithmetic*, in *Handbook of Mathematical Logic*, North-Holland, 1977.

10. M. Presburger, *Uber die vollstandigkeit eines gewissen Systems der Arithmetic ganzer zahlen, in welchen die Addition als einzige Operation hervortritt*, Comptes-rendus du I Congres de Mathematiciens des Pays Slaves, Warsaw, 1929, pp. 92–101.

11. T. Skolem, *Untersuchungen uber die Axiome des Klassenkalkuls und uber die "Productations und Summationsprobeleme", welche gewissen Klassen von Aussagen betreffen*, 1919; reprinted in *Selected Works in Logic*, Scandinavian University Books, 1970.

12. T. Skolem, *Uber einige Salzfunktionen in der Arithmetik*, V. A. Skr. **1** (7) (1930), 1–28.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF NOTRE DAME
NOTRE DAME, IN 46556 USA