REPORTS ON MATHEMATICAL LOGIC
42 (2007), 145–151

Kamila BENDOV'A

A WEAK ESSENTIALLY UNDECIDABLE THEORY

1. Introduction

Peano arithmetic PA is surely the most well known axiomatic arithmetic, essentially incomplete (Gödel's incompleteness theorem) and hence essentially undecidable. There is an extensive literature on fragments of PA sharing these properties; among them classical theories Q (finitely axiomatizable) and still weaker R, both presented in [8]. For newer development see e.g. Krajíček's book [3]. Most of these theories have the same language as PA with the operations of successor, addition and multiplication, predicates $=$ and $\leq$ and constant for zero. Whereas it is known that there is a complete and decidable theory of addition and ordering of natural numbers [4, 5] and of the ordering of natural numbers [7], the theory of multiplication and order of natural numbers is not decidable, even not arithmetical [6]. In this paper we offer an axiomatic theory of multiplication and ordering which is sound (true in the standard model $\mathbf{N}$ of natural numbers), is Σ_1 complete and contains the theory R, hence is essentially incomplete and essentially undecidable.

Received 28 August 2006

For simplicity we shall formulate the theory as a theory of *positive* natural numbers, without zero. This could be of course routinely transformed for a theory with zero.

Definition 1 MO is the first order theory with equality, the ordering predicate $<$, constant $\underline{1}$ and the binary function symbol $*$ of multiplication. The axioms are as follows:

(1) The axioms stating that the operation $*$ is commutative, associative and $\underline{1}$ is its unit element: $x * \underline{1} = x$.

(2) The axioms stating that $<$ is a linear discrete order with the smallest element $\underline{1}$ and no largest element. Thus the unary operation S of successor is introduced by definition.

(3) $\underline{2} * S(x) = S(S(\underline{2} * x))$

(4) $(x < y) \Rightarrow (x * z < y * z)$

(5) $(x < y \,\&\, x * z \leq y * w) \Rightarrow (x * S(z) < y * S(w))$

(6) $(\forall x, y)(\exists! z) R(x, y, z)$ where $R(x, y, z)$ is the formula $S(z * z * S(x * y)) = S(x * z) * S(y * z)$ (formula of Julia Robinson [6]).

$\underline{n}$ stands for the $(n-1)$-th successor of $\underline{1}$, SS...S($\underline{1}$).

Lemma 1 *The standard model* $\mathbf{N}^+$ *of positive natural numbers is a model of* MO

Proof. This is evident for all axioms except the last one; J. Robinson proved in [6] that the formula $R(x, y, z)$ defines the relation $z = x + y$ in the standard model $\mathbf{N}$ and hence in $\mathbf{N}^+$. □

2. Proving the bookkeeping axioms

Theorem 1 *MO proves the bookkeeping axiom schema* $\underline{m} * \underline{n} = \underline{m \cdot n}$ *for each* $m, n = 1, 2, \ldots$

The rest of the section elaborates a proof.

Remark 1 $MO \vdash \underline{1} * \underline{m} = \underline{m} = \underline{1 \cdot m}$, thus $MO \vdash \underline{m} * \underline{1} = \underline{m \cdot 1}$, in particular, $MO \vdash \underline{2} * \underline{1} = \underline{2 \cdot 1}$

Lemma 2 $MO \vdash \underline{2} * \underline{k} = \underline{2 \cdot k}$, *thus* $MO \vdash \underline{2k+1} = S(\underline{2} * \underline{k})$

Proof. For $k = 1$ see above; assume the validity for k. Then MO proves $\underline{2(k+1)} = \underline{2k+2} = SS(\underline{2k}) = SS(2*k) = 2*S(k) = 2*(\underline{k+1})$. (We used axiom (3).) □

From now on we assume $m \geq 3$, $n \geq 2$ and validity of the bookkeeping axiom for $(i < m, j \leq n+1)$ and for $(i \leq m, j \leq n)$. We prove the axiom for $(m, n+1)$. This is our *induction step.* Due to the (provable) commutativity of $*$ this gives full validity of the bookkeeping schema.

Lemma 3 *The induction step holds for m even.*

Proof. Let $m = 2i$, then $MO \vdash \underline{m} = \underline{2} * \underline{i}$ by Lemma 2. Then MO proves $\underline{m}*(\underline{n+1}) = \underline{2i}*(\underline{n+1}) = \underline{2}*(\underline{n+1})*\underline{i} = \underline{2}*\underline{(n+1)i} = \underline{2i(n+1)} = \underline{m(n+1)}$ (using the induction assumption for $(i, n+1)$ and Lemma 2). □

Lemma 4 *The induction step holds for $(n+1)$ even.*

Proof. Let $(n+1) = 2k$, thus $MO \vdash \underline{n+1} = \underline{2} * \underline{k}$. Prove in MO: $\underline{m} * (\underline{n+1}) = \underline{m} * \underline{2} * \underline{k} = 2 * (\underline{km}) = \underline{2km} = \underline{m(n+1)}$. □

Lemma 5 *In the case of both m and $(n+1)$ being odd we claim*

$$MO \vdash \underline{m(n+1)-1} < \underline{m} * \underline{n+1} < \underline{m(n+1)+1},$$

which gives $MO \vdash \underline{m} * (\underline{n+1}) = \underline{m(n+1)}$.

Proof. Assume $n = 2k$, $m = 2i+1$. Let x^{+k} stand for $S \dots S(x)$, k copies of S. Finally let $w = n+1$. Reason in MO. Observe

$$\underline{m} * \underline{k} = \underline{mk} = \underline{(2i+1)k} = \underline{2ik+k} = \underline{(2ik)}^{+k},$$

Analogously

$$\underline{m} * (\underline{k+1}) = \underline{(2i+1)(k+1)} = (\underline{2i(k+1)})^{+k+1} = (\underline{2i.k'})^{+k+1}$$

Now $\underline{2} * \underline{k} * \underline{wi} = \underline{w} * \underline{2ki}$ (by induction assumption) and $\underline{2k} < \underline{w}$; thus by axiom (5),

$$\underline{2k} * S(\underline{wi}) < \underline{w} * S(\underline{2ki})$$

and by iterative use of Axiom (5),

$$\underline{2k} * (\underline{wi})^{+k} < \underline{w} * (\underline{2ki})^{+k}.$$

Now $(\underline{2ki})^{+k} = \underline{(2i+1)k} = \underline{m} * \underline{k}$, thus

$$\underline{2} * \underline{k} * (\underline{wi})^{+k} < \underline{w} * \underline{m} * \underline{k}$$

and by cancellation (which is an obvious consequence of the axiom (4)),

$$\underline{2((n+1)i+k)} = 2 * (\underline{wi})^{+k} < (\underline{n+1}) * \underline{m}.$$

Now, outside MO, compute

$$(n+1) \cdot m = (n+1)(2i+1) = (n+1)2i + 2k + 1 = 2((n+1)i+k) + 1,$$

which with the last preceding computation gives

$$(*) \qquad MO \vdash \underline{(n+1)m - 1} < (\underline{n+1}) * \underline{m}.$$

To get second inequality, recall $w = 2k+1 = n+1, m = 2i+1$ write k' for $k+1$ and compute in MO :

$$\begin{aligned} S(\underline{w}) = SS(\underline{2k}) &= SS(\underline{2} * \underline{k}) = 2 * S(\underline{k}) = 2 * k'; \\ \underline{w} * \underline{2k'} * \underline{i} &= S(\underline{w}) * \underline{w} * \underline{i}, \\ \underline{w} * \underline{2k'i} &= S(\underline{w}) * \underline{wi} \text{ and } \underline{w} < S(\underline{w}), \text{ thus} \\ \underline{w} * (\underline{k'.2i})^{+k+1} &< S(\underline{w}) * (wi)^{+k+1} \end{aligned}$$

Now since (outside MO) $2ik' + (k+1) = (2i+1)(k+1) = m.k'$ we get $MO \vdash \underline{w} * \underline{m} * \underline{k'} < \underline{2} * \underline{k'} * (\underline{wi})^{+k+1}$; cancel getting
$MO \vdash \underline{w} * \underline{m} < \underline{2} * (\underline{wi})^{+k+1} = 2(\underline{wi+k+1})$.
But $2(wi+k+1) = 2wi+2k+2 = 2wi+w+1 = w(2i+1)+1 = (n+1)m+1$, which gives the second inequality:

$$(*) \qquad MO \vdash \underline{(n+1)} * \underline{m} < \underline{(n+1)m+1}.$$

This completes the proof. □

3. Σ_1-completeness and essential incompleteness

It follows from the axiom on discrete ordering with first element 1 and no last element that each model of MO contains an initial segment of the order type of (positive) natural numbers and this segment with the order and successor of the model is isomorphic to positive natural numbers with order and successor. Now the validity of bookkeeping axioms in the model guarantees that the isomorphism preserves also multiplication. Also the isomorphism yields the validity of the following axiom (schema) in each model and hence its provability in MO:

Lemma 6 *For each positive natural numbers MO proves*

$$x \leq \underline{n} \equiv (x = \underline{1} \vee x = \underline{2} \vee \cdots \vee x = \underline{n}).$$

Denote it by (*).

Definition 2 Σ_0-formulas of MO are built from atomic formulas of MO using connectives and bounded quantifiers $(\exists x \leq y), (\forall x \leq y)$ (as usual). Σ_1-formulas are formulas of the form $(\exists x)\varphi$ where φ is a bounded formula.

Theorem 2 *(Σ_1-completeness.) For each Σ_1-formula $\varphi(x, \ldots, y)$ and each $m, \ldots, n \in N^+$, the formula $\varphi(\underline{m}, \ldots, \underline{n})$ is true in $\mathbf{N}^+$ iff it is provable in MO.*

Proof. The proof is fully analogous to the proof of [2] 1.8 (using the bookkeeping theorem and the preceding lemma). □

.

Definition 3 In MO define the new operation $\oplus$ by $z = x \oplus y \equiv R(x, y, z)$.

Lemma 7 *MO proves the bookkeeping axioms for $\oplus$, namely $\underline{m} \oplus \underline{n} = \underline{m+n}$, for all positive natural m, n.*

Proof. This follows immediately from the Σ_1-completeness since the defining formula $R(x, y, z)$ is (open and hence) Σ_1. □

Lemma 8 *The arithmetic R is a subtheory of MO (with addition defined as above).*

Proof. Recall that the arithmetic R has as axioms the bookkeeping axioms for addition and multiplication, the formula (*) from Lemma 6, $\neg(\underline{n} = \underline{m})$ for $n \neq m$, $\neg(\underline{n} \leq \underline{m})$ for $n > m$ and, finally, $x \leq \underline{n} \vee \underline{n} \leq x$ for each $n \in N^+$. We have proved the bookkeeping axioms for multiplication and we defined addition and we know that (*) is provable. The provability of the remaining axioms is clear from the observation that the axioms are true in each model of MO (speaking on its initial segment isomorphic to N^+). □

Theorem 3 *(Main theorem.) MO with the defined addition is essentially incomplete and hence essentially undecidable.*

Proof. Immediate from the preceding lemma. □

To conclude let us stress once more that the language of our theory MO consists of multiplication and ordering; the operations of successor and addition are introduced by definitions and may be considered to be just a sort of abbreviation. This appears to make our result on essential incompleteness interesting. (Cf. also [1].)

References

[1] K. Bendová, *On ordering and multiplication of natural numbers*, Arch. Math. Logic 40 (2001), pp. 19–23.

[2] P. Hájek and P. Pudlák, Metamathematics of first-order arithmetic, Springer-Verlag 1993.

[3] J. Krajíček, Bounded arithmetic,propositional logic and complexity theory, Cambridge Univ. Press 1995.

[4] M. Presburger, *Über die Vollständigkeit eines gewissen Systems der Arithmetik der ganzen Zahlen, in dem die Addition als einzige Operation hervortritt*, Cempter Rendus du 1. Congres des Mathematiciens des pays Slaves, Warszawa 129, pp. 92–101.

[5] M.O. Rabin, Decidable theories. In: Handbook of Mathematical Logic (Barwise, ed.) North Holland P.C. 1977.

[6] J. Robinson, *Definability and decisin problems in arithmetic*, Journ. Symb. Log. 14 (1949), pp. 98–114.

[7] T. Skolem, *Über einige Satzfunktionen in der Arithmetik*, V. A. Skr. I, No 7, (1930) pp. 1–28 (reprinted in J. Fenstad, editor, Selected Works in Logic, pp. 281–306, Universitetsforlaget, Oslo, 1970).

[8] A. Tarski, A. Mostowski, and R.M. Robinson, Undecidable theories. North Holland P.C. 1953.

Prague, Czech Republic