

RESTRICTED SET-THEORETICAL DEFINITIONS IN ARITHMETIC

RAPHAEL M. ROBINSON

1. Introduction. Addition of natural numbers is defined recursively in terms of successor by the formulas $a+0=a$, $a+b'=(a+b)'$. This recursive definition may be replaced by the explicit *set-theoretical definition*

$$a + b = c \leftrightarrow (\wedge M) \{ (0, a) \in M \wedge (\wedge x, y) [(x, y) \in M \rightarrow (x', y') \in M] \rightarrow (b, c) \in M \}.$$

Notice that sets of ordered pairs of natural numbers are used in this definition.

Here and throughout this paper the logical symbols \wedge (and), \vee (or), \rightarrow (if \dots then \dots), \leftrightarrow (if and only if), \wedge (for every), and \vee (there exists) are used; negation does not occur explicitly. The concepts just mentioned, together with identity, are considered as the logical notions.

On the other hand, it is known that it is not possible to give an explicit *arithmetical definition* of addition in terms of successor, that is, a definition using only the concepts of logic, and excluding the concepts of set theory. In fact, from a formula containing (besides parentheses and variables ranging over the natural numbers) only logical symbols and the symbol for successor, we can eliminate all quantifiers, if we allow the symbol 0 to be introduced.¹ From this, it follows that the only sets of natural numbers which are definable are the finite sets and their complements. In particular, the set of even numbers is not definable. It is then clear that addition also is not definable in this way.

Alfred Tarski has proposed (in lectures) consideration of an intermediate type of definition, in which sets of natural numbers but no other sets are allowed. Thus we will have variables a, b, c, \dots which represent natural numbers, and variables A, B, C, \dots which repre-

Presented to the Society, August 24, 1956; received by the editors, December 1, 1956.

¹ The method of elimination of quantifiers was discussed, in the related case in which addition is the only operation, by M. Presburger, *Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, Comptes-rendus du I Congrès des Mathématiciens des Pays Slaves, Warsaw, 1929, pp. 92-101, 395. He showed that arithmetic based on addition and not using set theory is decidable, and that multiplication is not definable in the theory. The argument in the case required here is much simpler than Presburger's.

sent sets of natural numbers. The term restricted set theory will refer to the use of just these types of variables. A definition using such variables will be called a *restricted set-theoretical definition*. As examples of definitions of this type, we may give

$$a < b \leftrightarrow (\forall A)[b \in A \wedge (\wedge x)(x \in A \rightarrow x' \in A) \wedge a \notin A]$$

and

$$a \equiv 0 \pmod{2} \leftrightarrow (\wedge A)[0 \in A \wedge (\wedge x)(x \in A \rightarrow x'' \in A) \rightarrow a \in A].$$

Specifically, Tarski has proposed the following two problems.

PROBLEM 1. Is it possible to give a restricted set-theoretical definition of addition of natural numbers in terms of successor?

PROBLEM 2. Is there a decision method for the arithmetic of natural numbers based on the notion of successor and using restricted set theory?

A positive solution to the first problem would lead to a negative solution to the second. For in terms of addition, we may define divisibility by the formula

$$a \mid b \leftrightarrow (\wedge A)[0 \in A \wedge (\wedge x)(x \in A \rightarrow x + a \in A) \rightarrow b \in A].$$

Since, as pointed out by Tarski, multiplication is arithmetically definable in terms of addition and divisibility,² we can then also define multiplication, and hence, by the method of Gödel, all recursive functions. Thus the arithmetic of natural numbers, with the operation of addition and using restricted set theory, is undecidable. It follows that if there is a restricted set-theoretical definition of addition in terms of successor, then also the arithmetic of natural numbers with the operation of successor and using restricted set theory would be undecidable.

A variant of the problems proposed by Tarski is obtained by using not variables A, B, C, \dots representing arbitrary sets of natural numbers, but instead variables $\alpha, \beta, \gamma, \dots$ representing finite sets of natural numbers.³ Every definition of this new type can be transformed into a definition of the previous type, since finite (that is, bounded) sets can be defined using the set variables A, B, C, \dots . It also appears to be possible to replace definitions involving $A, B,$

² The definitions may be found, for example, on page 146 of R. M. Robinson, *Undecidable rings*, Trans. Amer. Math. Soc. vol. 70 (1951) pp. 137-159.

³ (*Added in proof.*) I have learned that A. Ehrenfeucht has proved that the arithmetical theory of the addition of ordinals is decidable, and that R. L. Vaught has shown how this result may be used to give a positive solution to the modified Problem 2 and hence a negative solution to the modified Problem 1. However, the problems as first stated remain open.

C, \dots by definitions involving $\alpha, \beta, \gamma, \dots$. At least, this is easily seen to be the case for all the definitions used in this paper. For example, we see that

$$a < b \leftrightarrow (\forall \alpha)[a \in \alpha \wedge (\bigwedge x)(x' \in \alpha \rightarrow x \in \alpha) \wedge b \notin \alpha].$$

However, I have not found a general procedure.

2. Definitions of addition. We shall prove two independent theorems relating to the definability of addition. However, both theorems fall short of yielding a positive solution to Problem 1 or a negative solution to Problem 2.

THEOREM 1. *It is possible to give a restricted set-theoretical definition of addition in a certain model of the arithmetic of natural numbers in terms of the successor operation on natural numbers.*

PROOF. The model in question will have as elements exactly the finite sets of natural numbers. These can be put into one-to-one correspondence with the natural numbers by letting the set $\alpha = \{a_1, a_2, \dots, a_n\}$, where a_1, a_2, \dots, a_n are distinct natural numbers, correspond to the number

$$N(\alpha) = 2^{a_1} + 2^{a_2} + \dots + 2^{a_n}.$$

We wish to define an operation \oplus so that $N(\alpha \oplus \beta) = N(\alpha) + N(\beta)$.

Notice that if $N(\alpha)$ is written in binary notation, then α is the set of positions in which the digit 1 occurs. Now in adding two numbers in binary notation, there will be a carry-over to position a if and only if there is a position of lower rank where the two numbers agree, and in the last such position t both numbers contain the digit 1. Taking this carry-over into account, we see that

$$\begin{aligned} a \in \alpha \oplus \beta &\leftrightarrow (\bigwedge x)[x \leq a \rightarrow (x \in \alpha \leftrightarrow x \in \beta)] \\ &\vee (\forall t)\{t < a \wedge (\bigwedge x)[t < x < a \rightarrow (x \in \alpha \leftrightarrow x \in \beta)] \\ &\wedge ([t \in \alpha \wedge t \in \beta \wedge (a \in \alpha \leftrightarrow a \in \beta)] \\ &\vee [t \notin \alpha \wedge t \notin \beta \wedge (a \in \alpha \leftrightarrow a \notin \beta)])\}. \end{aligned}$$

The inequalities here may be eliminated, by using one of the definitions given in §1.

REMARK. This definition of addition in a model of the arithmetic of natural numbers does not yield a negative solution to Problem 2, as a positive solution to Problem 1 (definition of addition for the natural numbers themselves) would. However, if we could define both addition and multiplication in some model, then the undecidability of the theory would follow.

THEOREM 2. *It is possible to give a restricted set-theoretical definition of addition of natural numbers in terms of the operations of successor and double. That is, the binary operation $x+y$ is definable in terms of two special cases, $x' = x+1$ and $2x = x+x$.*

PROOF. The proof depends on the use of a suitable correspondence between all ordered pairs of natural numbers and some natural numbers. We shall use the pairing function

$$J(x, y) = 2^x(2y + 3).$$

Clearly,

$$J(x, y) = J(a, b) \leftrightarrow x = a \wedge y = b.$$

It is immaterial that $J(x, y)$ does not assume all natural numbers as values.

We shall be interested, for each natural number n , in the three sets $P(n)$, $Q(n)$, $R(n)$ defined by

$$\begin{aligned} z \in P(n) &\leftrightarrow (\forall y)[z = J(n, y)], \\ z \in Q(n) &\leftrightarrow (\forall x)[z = J(x, n)], \\ z \in R(n) &\leftrightarrow (\forall x, y)[z = J(x, y) \wedge x + y = n]. \end{aligned}$$

We also use the relations S and T defined by

$$\begin{aligned} uSv &\leftrightarrow (\forall x, y)[u = J(x, y) \wedge v = J(x', y)], \\ uTv &\leftrightarrow (\forall x, y)[u = J(x, y) \wedge v = J(x, y')]. \end{aligned}$$

We shall show that all of these, and finally also $J(x, y)$ and $x+y$, are definable in terms of successor and double, using restricted set-theoretical definitions.

We may in fact use the following definitions:

$$\begin{aligned} z \in Q(n) &\leftrightarrow (\wedge A)[2n + 3 \in A \wedge (\wedge u)(u \in A \rightarrow 2u \in A) \rightarrow z \in A], \\ uSv &\leftrightarrow (\forall n)[u \in Q(n)] \wedge v = 2u, \\ uTv &\leftrightarrow (\forall n)[u \in Q(n) \wedge v \in Q(n')] \wedge u < v < 2u, \\ z \in R(n) &\leftrightarrow (\wedge A)\{2n + 3 \in A \\ &\quad \wedge (\wedge u, v, w)[uSv \wedge uTv \wedge w \in A \rightarrow v \in A]\} \rightarrow z \in A\}, \\ z \in P(n) &\leftrightarrow (\wedge A)\{(\forall u)[u \in Q(0) \wedge u \in R(n) \wedge u \in A] \\ &\quad \wedge (\wedge u, v)[u \in A \wedge uTv \rightarrow v \in A]\} \rightarrow z \in A\}. \end{aligned}$$

As before, we can eliminate inequalities, and we can also eliminate the symbol 0. We can now define the pairing function $J(x, y)$ by the formula

$$z = J(x, y) \leftrightarrow z \in P(x) \wedge z \in Q(y).$$

Addition may be defined by translating the set-theoretical definition given at the beginning of the paper into the form

$$a + b = c \leftrightarrow (\wedge A) \{ J(0, a) \in A \wedge (\wedge x, y) [J(x, y) \in A \rightarrow J(x', y') \in A] \rightarrow J(b, c) \in A \} .$$

However, in terms of the above defined sets and functions, we can also use the simpler definition

$$a + b = c \leftrightarrow J(a, b) \in R(c).$$

We may also eliminate $J(a, b)$, and write this in the form

$$a + b = c \leftrightarrow (\forall z) [z \in P(a) \wedge z \in Q(b) \wedge z \in R(c)].$$

COROLLARY. *The arithmetic of natural numbers, based on the operations successor and double, and using restricted set theory, is undecidable.*

REMARK. By way of contrast to Theorem 2, it is easily seen that it is not possible to define addition arithmetically in terms of successor and double. The argument is a simple modification of Presburger's (see Footnote 1). Indeed, elimination of quantifiers is possible if we introduce the symbols $0, 1, 2, \dots$ and the congruences $x \equiv a \pmod{2^b}$ for $a = 0, 1, 2, \dots$ and $b = 0, 1, 2, \dots$. It is then seen that the congruence $x \equiv 0 \pmod{3}$, for example, is not expressible, and hence that addition is not definable.

Also, by the result of Presburger, the corollary is clearly false if no set theory is used, since the two given operations are special cases of addition.

REMARK. We do not know whether the doubling operation can be omitted from either Theorem 2 or the corollary; these are exactly Tarski's two problems. On the other hand, the successor operation clearly cannot be omitted from Theorem 2, since the system of natural numbers with only the doubling operation admits nontrivial automorphisms, whereas the system with addition does not. With regard to the corollary, if the theory with successor alone turns out to be undecidable, then the theory with double alone will be also, since models of the former theory may be constructed in the latter.