MATH. SCAND. 10 (1962), 201–216

TERNARY RECURSIVE ARITHMETIC

H. E. ROSE

1. Introduction.

Recursive arithmetics are free variable formalisations of parts of the elementary theory of natural numbers, in which the only methods of function definition are recursion and composition (that is, definition by explicit substitution). In a recent paper [1], Alonzo Church described a formalisation of recursive arithmetic in which single axioms of composition and recursion took the place of an infinity of such axioms in earlier codifications. Church's system, however, postulates axioms of the propositional calculus and of mathematical induction, and it is the object of the present paper to eliminate these axioms in the manner of Goodstein [2].

Goodstein's formulation of primitive recursive arithmetic is a free variable pure equation calculus in which all propositions take the form

$$A = B$$

where A and B are function signs. The axioms of this codification are infinite in number and consist of the recursive definitions of each function of the system. On the other hand, Church's formalisation admits the connectives of the sentential calculus, variables for propositions and variables for functions with one or two argument places and, as a consequence of this, has a finite axiom basis. Professor Goodstein suggested that we should try to find to what extent these opposed approaches may be reconciled within a single codification; the system, called Ternary Recursive Arithmetic — TRA, described in this paper is the outcome of this suggestion. Essentially, we shall show that, if we add to the primitive basis of Church's formalisation variables for functions with three argument places (and the rules for operating them), the propositional variables and the axioms and rules of the sentential calculus are redundant. The variables for functions having three argument places are introduced into TRA because it is necessary to be able to derive the properties of some three variable equations, for instance — associativity of addition,

Received December 7, 1961.

in the early stages of the development and, as the proof schemas (lab elled E and F) are stated in terms of numerical function variables, they can be applied only to functions or equations between functions. Church's system did not need this concept as its proof schemas (induction) are stated in terms of propositional variables (and there is no limit upon the number of numerical variables contained in a particular proposition).

The codification TRA presented in this paper is a slightly improved version of the one discussed briefly in [3], the main change being that only one recursion axiom is required (previously there were two). This paper is the one that was to have appeared in the Annales de l'École Normale, Paris.

2. The basis of Ternary Recursive Arithmetic.

Ternary Recursive Arithmetic is a codification of primitive recursive arithmetic as a logic-free equation calculus (that is, one in which the sentential calculus, or similar logical structure, is not taken as primitive) with function variables in which there are two basic entities — functions and terms. The functions have one, two or three argument places and are defined by recursion or composition and the terms are defined explicitly, from these functions, but have no function signs (names) attached to them. As with Church's formulation this device gives primitive recursive arithmetic without function variables a finite axiom basis.

The primitive symbols of Ternary Recursive Arithmetic are (a) infinite lists of numerical variables $a,b,c,a_1,b_1,\ldots,$ 1-function variables $f,g,h,\ldots,$ 2-function variables $f',g',h',\ldots,$ and 3-function variables $f'',g'',h'',\ldots$; (b) the constant functors s, o, i, j and k; (c) the functor connectives R, C, C', C''; (d) the numerical constant 0; (e) the connective $=$; and (f) brackets, commas and parentheses. In practice the primes $'$ and $''$ indicating the kind of function being used will be omitted as this will be obvious from the contents of the brackets following the function sign. We begin by defining the functors.

(i) A 1-*functor* is one of the following: — the constant functors s, o or i; a 1-function variable standing alone; $C''f$ where f is a 2-functor.

(ii) A 2-*functor* is one of the following: — the constant functor j; a 2-function variable standing alone; $C'pfgh$ where p is a 3-functor, f and g are 1-functors and h is a 2-functor.

(iii) A 3-*functor* is one of the following: — the constant functor k;

a 3-function variable standing alone; $Cpfgh$ where p, f, g and h are 3-functors; $Rfgh$ where f and g are 2-functors and h is a 3-functor.

A 1-*function* is a symbol of the form $f(a)$ where f is a 1-functor and a is a numerical variable, similarly a 2-*function* has the form $g(a,b)$ (g is a 2-functor) and a 3-*function* has the form $h(a,b,c)$ (h is a 3-functor). A *term* is one of the following: —

(i) the numerical constant 0,

(ii) a numerical variable standing alone,

(iii) $f(A)$ where f is a 1-functor and A is a term,

(iv) $f(A,B)$ where f is a 2-functor and A and B are terms,

(v) $f(A,B,C)$ where f is a 3-functor and A, B and C are terms.

(The italic capital letters $A,B,C,\ldots$ will always represent terms.) The expression

$$A = B,$$

where A and B are terms, is called an *equation*. This is the only way in which terms may be connected and the purpose of the system is to derive new equations from the axioms by applying the axiom schemas. The expression $A=B \vdash C=D$ is called a schema or metatheorem and states that if $A=B$ is a theorem then $C=D$ is also a theorem.

The axiom schemas of Ternary Recursive Arithmetic, labelled E, F, T, U, V and W, are as follows. ($s(a)$ will usually be written sa.)

E. $f(sa,b,c)=f(a,b,c) \vdash f(a,b,c)=f(0,b,c)$, where f is a 3-functor.

F. $f(0,b)=g(0,b)$, $f(sa,b)=C'hsif(a,b)$, $g(sa,b)=C'hsig(a,b) \vdash f(a,b)= g(a,b)$, where f and g are 2-functors, h is a 3-functor, s is the successor function and i is defined by axiom 2.

T. $A=B$, $A=C \vdash B=C$, where A, B and C are terms.

U. $A=B \vdash f(A,b,c)=f(B,b,c)$, where f is a 3-functor, A and B are terms and b and c are numerical variables.

V. If an equation involving a numerical variable $\boldsymbol{a}$ is represented by $P(\boldsymbol{a})$ and the result of replacing all occurrences of $\boldsymbol{a}$ by A (a term) in $P(\boldsymbol{a})$ is denoted by $P(A)$, then $P(\boldsymbol{a}) \vdash P(A)$. ($\boldsymbol{a}$ is a meta-variable).

W. If an equation involving a function variable $\boldsymbol{f}$ is represented by $P\boldsymbol{f}$, the result of replacing all occurrences of $\boldsymbol{f}$ by g (a functor) in $P\boldsymbol{f}$ is denoted by Pg and g belongs to the same class of functors as $\boldsymbol{f}$, then $P\boldsymbol{f} \vdash Pg$. ($\boldsymbol{f}$ is a meta-variable.)

Finally the axioms are given as follows.

1. $o(a)=0$.
2. $i(a)=a$.
3. $j(a,b)=a$.
4. $k(a,b,c)=a$.

5. $Rfgh(0,b,c)=f(b,c)$.
6. $Rfgh(sa,b,c)=g(Rfgh(a,b,c),h(a,b,c))$.
7. $Cpfgh(a,b,c)=p(f(a,b,c),g(a,b,c),h(a,b,c))$.
8. $C'pfgh(a,b)=p(f(a),g(b),h(a,b))$.
9. $C''f(a)=f(0,a)$.

In these axioms f, g, h and p are function variables.

3. The simplest properties.

In the remaining sections of this paper we shall develop TRA to the point where we can show that it is a codification of that part of primitive recursive arithmetic which does not involve function variables. The essential step in this work is the introduction of the notion of an ordered pair: that is, the definition of three functions $w(a,b)$, m_1a and m_2a having the properties

$$m_1w(a,b) = a \qquad \text{and} \qquad m_2w(a,b) = b\ .$$

Once this has been achieved we can readily show that to every primitve recursive function $f(a_1,a_2,\ldots,a_n)$ there corresponds a 1-functor f^*, belonging to TRA, such that

$$f(a_1\ a_2,\ldots,a_{n-1},a_n) = f^*\big(w\big(a_1,w(a_2,\ldots,w(a_{n-1},a_n)\ldots)\big)\big);$$

i.e. there is (at least) one term of TRA corresponding to every primitive recursive function. [This follows by a simple inductive argument which will be omitted here.]

We begin by deriving the basic properties of equality.

1. $\quad a = a.$

This is derived by taking $i(a)$ for A, a for B and a for C in axiom schema T and applying axiom 2 twice.

2. $\quad A = B \vdash B = A.$

By 1 and axiom schema V we derive $A=A$, and 2 follows by taking A for C in axiom schema T.

3. $\quad A = B,\ B = C \vdash A = C.$

Applying 2 the hypotheses give $B=A$, $B=C$ and 3 is deduced by T.

We define now some initial functions which will lead us to the new composition rules.

4. $\quad Rfjk(a,b,c) = f(b,c),$

where f is a 2-functor and j and k are defined by axioms 3 and 4. Applying axiom 6 and W we have

$$\begin{aligned} Rfjk(sa,b,c) &= j\big(Rfjk(a,b,c),k(a,b,c)\big) \\ &= Rfjk(a,b,c) \end{aligned}$$

by axiom 3, 3 and V; and hence by E

$$Rfjk(a,b,c) = Rfjk(0,b,c)$$

and theorem 4 follows by axiom 5, W and 3.

DEFINITION. $k' \rightarrow Rjjk$.

[In the expression $X \rightarrow Y$ the arrow indicates that X is an abbreviation for Y; this is simply a typographical convention.]

5. $k'(a,b,c) = b$.

Taking j for f in 4 this follows from axiom 3 by V.

6. $C'k'ofj(a,b) = f(b)$,

where f is a 1-functor and o is defined by axiom 1.
We have by axiom 8,

$$C'k'ofj(a,b) = k'\big(o(a),f(b),j(a,b)\big)$$

and 6 follows from 5 by V.

DEFINITION. $j' \rightarrow C'k'oij$.

7. $j'(a,b) = b$.

Taking i for f in 6 this follows from axiom 2 by V.

DEFINITION. $k'' \rightarrow Rj'jk$.

8. $k''(a,b,c) = c$.

This is an immediate consequence, by V, of 4 and 7.
Some variants of the axiom schemas E and U can be proved now.

E′. $f(sa,b)=f(a,b) \vdash f(a,b)=f(0,b)$,

where f is a 2-functor.

DEFINITION. $f' \rightarrow CRfjkkkk'$.

From this, we have by axiom 7, V, 4 and 3,

$$f'(a,b,c) = f(a,b)$$

and the hypothesis gives, by V and 3,

$$f'(sa,b,c) = f'(a,b,c)\,,$$

hence by E, $f'(a,b,c)=f'(0,b,c)$; applying V and 3 to this the conclusion of E′ follows.

U_1. $A=B \vdash f(a,A,b)=f(a,B,b)$,
where f is a 3-functor.
We have, by axiom 7, theorems 5 and 8, and V,

$$f(a,A,b) = Cfk'kk''(A,a,b)\ ,$$

U_1 follows from this by U, V and 3 applied to $Cfk'kk''$. By exactly similar arguments the following can also be deduced.

U_2. $A=B \vdash f(a,b,A)=f(a,b,B)$.

U'. $A=B \vdash f(A,b)=f(B,b)$.

U_1'. $A=B \vdash f(a,A)=f(a,B)$.

U''. $A=B \vdash f(A) = f(B)$.

Using the results derived so far eight new composition rules may be introduced now.

Definition. $C_{32}pfgh \rightarrow C'CCpRfjkRgjkRhjkkk''k'oij'$.

9. $C_{32}pfgh(a,b) = p\big(f(a,b),g(a,b),h(a,b)\big)$.

(a) By 4, U, U_1, U_2 and V we have

$$\begin{aligned} CpRfjkRgjkRhjk(a,b,c) &= p\big(Rfjk(a,b,c),Rgjk(a,b,c),Rhjk(a,b,c)\big) \\ &= p\big(f(b,c),g(b,c),h(b,c)\big) \end{aligned}$$

and, from this by E and V, follows

$$CpRfjkRgjkRhjk(0,b,c) = p\big(f(b,c),g(b,c),h(b,c)\big)\ .$$

(b) From axioms 3, 7 and 8, theorems 5 and 8, by V and W, we derive

$$C'Cxkk''k'oij(a,b) = Cxkk''k'\big(o(a),i(b),j(a,b)\big) = x(0,a,b)\ .$$

Hence, taking $CpRfjkRgjkRhjk$ for x in (b), 9 follows from (a) by 3.
Very similar arguments give the remaining composition rules.

Definition. $C_{23}fgh \rightarrow CRfjkkgh$.

10. $C_{23}fgh(a,b,c) = f\big(g(a,b,c),h(a,b,c)\big)$.

Definition. $C_{13}fg \rightarrow CRC'k'ofjjkkkg$.

11. $C_{13}fg(a,b,c) = f\big(g(a,b,c)\big)$.

Definition. $C_{22}fgh \rightarrow C_{32}Rfjkjgh$.

12. $C_{22}fgh(a,b) = f\big(g(a,b),h(a,b)\big)$.

Definition. $C_{12}fg \rightarrow C_{22}C'k'ofjjg$.

13. $C_{12}fg(a,b) = f\big(g(a,b)\big)$.

Definition. $C_{31}pfgh \rightarrow C''C_{32}pC'k'ofjC'k'ogjC'k'ohj$.

14. $C_{31}pfgh(a) = p\big(f(a),g(a),h(a)\big)$. [Derived by E′.]

DEFINITION. $C_{21}fgh \to C_{31}Rfjkigh$.

15. $C_{21}fgh(a) = f(g(a),h(a))$.

DEFINITION. $C_{11}fg \to C_{21}C'k'ofjig$.

16. $C_{11}fg(a) = f(g(a))$.

Definition by recursion for 2-functions is given by the

DEFINITION. $R'fgh \to C_{32}RC_{22}C'k'ofjj'jgCRhjkkkk'jj'C_{12}oj$.

We have, by 12, 7, 6; 4, 5; 11, 3, 7

(i) $C_{22}C'k'ofjj'j(b,c) = C'k'ofj(c,b) = f(b)$,
(ii) $CRhjkkkk'(a,b,c) = Rhjk(a,a,b) = h(a,b)$,
(iii) $C_{32}xjj'C_{12}oj(a,b) = x(a,b,0)$,

hence, if x stands for $RC_{22}C'k'ofjj'jgCRhjkkkk'$, by V (putting 0 for c)

$$x(0,b,0) = f(b) \qquad \text{by (i)},$$
$$x(sa,b,0) = g(x(a,b,0),h(a,b)) \qquad \text{by (ii)}.$$

Thus by (iii)

17a. $R'fgh(0,b) = f(b)$.

17b. $R'fgh(sa,b) = g(R'fgh(a,b),h(a,b))$.

Similarly 1-function recursion is given by

DEFINITION. $R''fgh \to C''C_{22}R'C_{11}fogC_{22}C'k'ohjjjj'j$.

18a. $R''fgh(0) = f(0)$.

18b. $R''fgh(sa) = g(R''fgh(a),h(a))$.

These two equations follow in a similar manner to 17a and 17b.

To end these preliminary results we derive some variants of the axiom schemas E and F.

E″. $f(sa) = f(a) \vdash f(a) = f(0)$.

This follows by applying E′ to $C_{12}fj(a,b)$ and using 3, 13 and V. The following schemas may be deduced from F by taking particular functors for h: (a) taking $C_{23}fkk'$ for h we have, by axiom 8, 5, 9, U and V, $g(sa,b)=f(sa,b)$ and so

G. $f(0,b) = g(0,b), \quad f(sa,b) = g(sa,b) \vdash f(a,b) = g(a,b)$;

(b) taking $C_{13}pk''$ for h we have, by axiom 8, 10, U and V,

F₁. $f(0,b) = g(0,b),\ f(sa,b) = p(f(a,b)),\ g(sa,b) = p(g(a,b))$
$\vdash f(a,b) = g(a,b)$;

and (c) taking $C_{22}qk''k'$ for h we have, by axioms 7 and 8, 4, 5, 8, U and V,

F$_2$. $$f(0,b) = g(0,b),\ f(sa,b) = q\big(f(a,b),b\big),\ g(sa,b) = q\big(g(a,b)b\big) \vdash f(a,b) = g(a,b)\,.$$

In a similar manner we deduce

F′. $$f(0) = g(0),\ f(sa) = p\big(a,f(a)\big),\ g(sa) = p\big(a,g(a)\big) \vdash f(a) = g(a)$$

and

G′. $$f(0) = g(0),\ f(sa) = g(sa) \vdash f(a) = g(a)\,.$$

4. Addition and modified subtraction.

We shall define now addition and modified subtraction and derive their basic properties. The derivations will be given in outline only; the schemas T, U, V and W, and the theorems 2 and 3 will be used tacitly.

For the sake of convenience we shall usually apply U (or its variants) without first explicitly stating the definition of the functor involved, it is always possible to do this in the work to come. We note also that the order of the variables in a function, f say, is now immaterial; for we may define a new function g having the same value as f but with its variables in any desired order.

We begin with the definition of the addition function $d(a,b)$.

DEFINITION. $s_1 \to C_{12}sj$.

19. $s_1(a,b) = s(a)$.

DEFINITION. $s_2 \to C_{12}sj'$.

20. $s_2(a,b) = s(b)$.

DEFINITION. $d \to R'is_1j$.

21. $d(0,b) = b$.

22. $d(sa,b) = s\big(d(a,b)\big)$.

DEFINITION. $d_1 \to C_{21}dio$.

23. $d_1(b) = d(b,0)$.

24. $d_1(b) = b$.

This is derived by F′, for, using 19 to 23 and axiom 2,

$$d_1(0) = d(0,0) = 0\,,$$
$$d_1(sb) = d(sb,0) = s\big(d(b,0)\big) = s_2\big(b,d_1(b)\big)\,,$$
$$i(0) = 0 \quad\text{and}\quad i(sb) = s_2\big(b,i(b)\big)\,.$$

DEFINITION. $d' \to C_{22}djs_2$.

25. $d'(a,b) = d(a,sb)$.

DEFINITION. $d'' \to C_{22}ds_1j'$.

26. $d''(a,b) = d(sa,b)$.

27. $d(a,sb) = d(sa,b)$.

By F_1, for by 21, 22, 25 and 26, we have

$$d'(0,b) = d(0,sb) = s(b),\ d''(0,b) = d\big(s(0),b\big) = s(b)\,,$$
$$d'(sa,b) = d(sa,sb) = s\big(d(a,sb)\big) = s\big(d'(a,b)\big) \text{ and}$$
$$d''(sa,b) = d(ssa,b) = s\big(d(sa,b)\big) = s\big(d''(a,b)\big)\,.$$

DEFINITION. $d^* \to C_{22}dj'j$.

28. $d^*(a,b) = d(b,a)$.

29. $d^*(a,b) = d(a,b)$.

We have, by 28, 21, 23 and 24,

$$d^*(0,b) = d(b,0) = b\,,$$

and, by 28, 25, 26 and 27,

$$d^*(sa,b) = d(b,sa) = d(sb,a) = s\big(d(b,a)\big) = s\big(d^*(a,b)\big)\,,$$

thus we deduce 29 by F_1 from these equations, 21 and 22.

$d(a,b)$ will now be written $a+b$, 28 and 29 give

30. $a+b = b+a$.

The predecessor function $p(a)$ and the modified subtraction function $e(a,b)$ are given by the following definitions.

DEFINITION. $p \to R''oj'i$.

31. $p(0) = 0$.

32. $p(sa) = a$.

DEFINITION. $e \to C_{22}R'iC_{12}pjjj'j$.

33. $e(a,0) = a$.

34. $e(a,sb) = p\big(e(a,b)\big)$.

These two theorems follow from the axioms, 12, 13 and 7.

DEFINITION. $f \to C_{12}pe$.

35. $f(a,b) = p\big(e(a,b)\big)$.

DEFINITION. $f' \to C_{22}eC_{12}pjj'$.

36. $f'(a,b) = e(p(a),b)$.

37. $p(e(a,b)) = e(p(a),b)$.

This is given by F_1 and 33 to 36, as

$$f(a,0) = p(e(a,0)) = p(a),\ f'(a,0) = e(p(a),0) = p(a),$$
$$f(a,sb) = p(e(a,sb)) = p(p(e(a,b))) = p(f(a,b)) \text{ and}$$
$$f'(a,sb) = e(p(a),sb) = p(e(p(a),b)) = p(f'(a,b)).$$

We shall now write 1 for $s(0)$ and $a \dot- b$ for $e(a,b)$, and we have, by 34,

38. $p(a) = a \dot- 1$,

and by 37

39. $(a \dot- 1) \dot- b = (a \dot- b) \dot- 1$.

DEFINITION. $1 \to C_{11}so$.

40. $1(a) = 1$. By E″.

41. $sa \dot- sb = a \dot- b$. By 34, 39 and 32.

42. $a \dot- a = 0$. By E″, 41 and 33.

43. $0 \dot- a = 0$. By E″ and 33.

44. $1 \dot- sa = 0$. By 41 and 43.

DEFINITION. $g \to C_{23}eC_{23}dkk''C_{23}dk'k''$.

45. $g(a,b,c) = (a+c) \dot- (b+c)$.

46. $(a+c) \dot- (b+c) = a \dot- b$. By E applied to $g(a,b,c)$, 22 and 41.

47. $(a+b) \dot- b = a$. By 46, 21 and 33.

48. $(a+b) \dot- a = b$. By 47 and 30.

49. $b \dot- (a+b) = 0$. By 46, 21 and 43.

We shall now prove $a+(b+c)=(a+b)+c$, it is not possible to derive this directly as F is not yet available for 3-functions.

50. $1+(a \dot- 1) = a+(1 \dot- a)$.

This is derived by first defining two functors h and h', so that $h(a)= 1+(a \dot- 1)$ and $h'(a)=a+(1 \dot- a)$, and then deriving $h(a)=h'(a)$ by G′ and some previously proved results.

51. $(a \dot- 1)+(b+1) = (a+(1 \dot- a))+b$. By 27 and 50.

52. $1 \dot{-} (a \dot{-} b) = 0 \vdash (a \dot{-} b) + (b + c) = a + c$.

We have by U, U_2 and 24

$$\begin{aligned} 1 \dot{-} (a \dot{-} b) = 0 \vdash (a \dot{-} b) + (b+c) &= \big((a \dot{-} b) + \big(1 \dot{-} (a \dot{-} b)\big)\big) + (b+c) \\ &= \big((a \dot{-} b) \dot{-} 1\big) + \big((b+c)+1\big) && \text{by 51 .} \\ &= (a \dot{-} sb) + (sb + c) && \text{by 34, 22 .} \end{aligned}$$

Hence, if we define $h^*(a,b,c)$ to be $(a \dot{-} b) + (b+c)$, we derive, by E, 21 and 33, $h^*(a,b,c) = a+c$ and 52 follows.

53. $a + (b+c) = (a+b) + c$.

For, by 47 and 44, $1 \dot{-} \big((sa+b) \dot{-} b\big) = 0$ and hence 52 gives

$$\big((sa+b) \dot{-} b\big) + (b+c) = (sa+b)+c$$

and, by 47, 22, 30 and U″,

$$p\big(s\big(a+(b+c)\big)\big) = p\big(s\big((a+b)+c\big)\big)$$

53 is given by 32.

Finally in this section we shall derive $a + (b \dot{-} a) = b + (a \dot{-} b)$, some subsidiary results are required first.

54. $(a \dot{-} 1) + \big(1 \dot{-} (1 \dot{-} a)\big) = a$.

For, if we define $q(a)$ to be $(a \dot{-} 1) + \big(1 \dot{-} (1 \dot{-} a)\big)$, then $q(0) = 0$ by 43 and 42, and $q(sa) = sa$ by 41 and 44 and the result follows by G′.

DEFINITION. $q' \to C_{22} dj C_{22} e j' j$.

55a. $q'(a,b) = a + (b \dot{-} a)$.

56a. $q'(a,sb) = s\big(q'(a \dot{-} 1, b)\big)$.

As $q'(0,b) = b$ (21, 33 and 55a), $q'(0,sb) = s\big(q'(0 \dot{-} 1, b)\big)$, and

$$\begin{aligned} q'(sa,sb) &= sa + (b \dot{-} a) = s\big(q'(a,b)\big) && \text{by 41 and 27} \\ &= s\big(q'(sa \dot{-} 1, b)\big) && \text{by 41 ,} \end{aligned}$$

56a is given by G.

57a. $q'(a,b) = q'(a \dot{-} 1, b \dot{-} 1) + \big(1 \dot{-} \big(1 \dot{-} (a+b)\big)\big)$.

As $q'(a,0) = a$, we have by 54 $q'(a,0) = q'(a \dot{-} 1, 0) + \big(1 \dot{-} \big(1 \dot{-} (a+0)\big)\big)$. Further, as $1 \dot{-} \big(1 \dot{-} (a+sb)\big) = 1$ (by 22 and 44), 56a gives

$$q'(a,sb) = q'(a \dot{-} 1, sb \dot{-} 1) + \big(1 \dot{-} \big(1 \dot{-} (a+sb)\big)\big) .$$

From these two equations 57a follows by G.

DEFINITION. $q^* \to RC_{12}ojdC_{13}C_{21}elC_{21}eliC_{23}dC_{23}ek'kC_{23}ek''k.$

58. $q^*(0,a,b) = 0\,.$

59. $q^*(sc,a,b) = q^*(c,a,b) + \big(1 \dot- (1 \dot- ((a \dot- c) + (b \dot- c)))\big)\,.$

60a. $q'(a \dot- c, b \dot- c) + q^*(c,a,b) = q'(a,b)\,.$

57a gives $$q'(a \dot- c, b \dot- c) + q^*(c,a,b)$$
$$= \Big[q'\big((a \dot- c) \dot- 1,\; (b \dot- c) \dot- 1\big) + \big(1 \dot- (1 \dot- ((a \dot- c) + (b \dot- c)))\big)\Big] + q^*(c,a,b)$$
$$= q'(a \dot- sc, b \dot- sc) + q^*(sc,a,b)\,,$$

and 60a now follows by E.

61a. $q'(a,b) = (a \dot- b) + q^*(b,a,b)$. By 60a as $q'(a,0) = a\,.$

DEFINITION. $q'' \to C_{22}dj'C_{22}ejj'.$

55b. $q''(a,b) = b + (a \dot- b)\,.$

Theorems 56b, 57b, 60b and 61b have the same form (and derivation) as the corresponding ones above, with the single exception that q'' replaces q' at all occurrences of q'.

62. $a + (b \dot- a) = b + (a \dot- b)$. By 61a and 61b.

5. Further theorems. The pairing function.

In this section we shall show that the basic theorems of primitive recursive arithmetic are provable in TRA and introduce and derive the properties of the pairing function $w(a,b)$. The theorems and principle definitions will be stated as before, but the derivations will only be indicated by giving a list of the main theorems upon which they depend. We begin with the modulus function.

DEFINITION. $u \to C_{22}dC_{22}ej'je.$

63. $u(a,b) = (b \dot- a) + (a \dot- b)\,.$

We shall write $|a,b|$ for $u(a,b)$.

64. $|a,0| = a$. By 33, 43.

65. $|a,b| = |b,a|$. By 30.

66. $|a,a| = 0$. By 42.

67. $|a+c, b+c| = |a,b|$. By 46.

68. $A \dot- B = 0,\; B \dot- A = 0 \vdash A = B$. By 62.

69. $|A,B| = 0 \vdash A = B$. By 63, 68.

70. $A = B \vdash |A,B| = 0$. By 42, 63.

71. $A+C = B+C \vdash A = B$. By 70, 67, 69.

H. $f(0,b,c) = g(0,b,c),\ f(sa,b,c) = f(a,b,c)+h(b,c)$,
$g(sa,b,c) = g(a,b,c)+h(b,c) \vdash f(a,b,c) = g(a,b,c)$,

where f and g are 3-functors and h is a 2-functor.

This is proved by applying E to $|f(a,b,c),\ g(a,b,c)|$, for by 67

$$|f(sa,b,c),\ g(sa,b,c)| = |f(a,b,c)+h(b,c),\ g(a,b,c)+h(b,c)|$$
$$= |f(a,b,c),\ g(a,b,c)| \ .$$

Multiplication is given by the following

DEFINITION. $m \to R'odj'$.

72. $m(0,b) = 0$.

73. $m(sa,b) = m(a,b)+b$.

We shall write $m(a,b)$ as $a \cdot b$.

74. $a\cdot 0 = 0$. By E″, 72, 73, 24 .

75. $a\cdot sb = a\cdot b+a$. By H, 30, 53, 72, 73 .

76. $a\cdot b = b\cdot a$. By H, 72–75 .

77. $a\cdot(b+c) = a\cdot b+a\cdot c$. By H, 72, 73, 30, 53 .

78. $a\cdot(b\cdot c) = (a\cdot b)\cdot c$. By H, 72, 73, 75, 76 .

79. $a\cdot(1 \dot{-} a) = 0$. By G′, 72, 74, 44 .

80. $b\cdot(1 \dot{-} a) = b \dot{-} a\cdot b$. By G, 44, 49, 75 .

81. $a\cdot(b \dot{-} 1) = a\cdot b \dot{-} a$. By G, 43, 41, 47 .

Mathematical induction is introduced by the following schema.

I. $f(0,b,c) = 0,\ \big(1 \dot{-} f(a,b,c)\big)\cdot f(sa,b,c) = 0 \vdash f(a,b,c) = 0$.

DEFINITION. $f^* \to RC_{12}ljmC_{23}eC_{13}lkf$.

This gives $f^*(0,b,c)=1$ and $f^*(sa,b,c)=f^*(a,b,c)\cdot\big(1 \dot{-} f(a,b,c)\big)$, from which we derive by E, 80 and 76 (and the hypotheses),

$$f^*(sa,b,c) = f^*(1,b,c) = 1$$

and hence

$$f^*(a,b,c)\cdot\big(f(a,b,c)\cdot(1\dot{-}f(a,b,c))\big) = f(a,b,c)\,,$$

the conclusion of I is given now by 79 and 74.

G*. $f(0,b,c) = g(0,b,c),\ f(sa,b,c) = g(sa,b,c) \vdash f(a,b,c) = g(a,b,c)\,,$

where f is a 3-functor. By I, 69 and 70.

The substitution theorem.

82. $1\dot{-}(a+b) = (1\dot{-}a)\dot{-}b.$ By G, 33, 20, 44, 43 .

83. $\big((1\dot{-}a)\dot{-}b\big)\cdot a = 0.$ By G, 33, 44 .

84. $(1\dot{-}|a,b|)\cdot\big(1\dot{-}(a\dot{-}b)\big) = (1\dot{-}|a,b|).$ By 80, 83, 82, 63 .

85. $(1\dot{-}c)\cdot f(a+c,b) = (1\dot{-}c)\cdot f(a,b)\,,$

where f is a 2-functor. By G* and 44.

86. $(1\dot{-}|a,b|)\cdot f(a,c) = (1\dot{-}|a,b|)\cdot f(b,c)\,.$

By 85 and 84 we have

$$(1\dot{-}|a,b|)\cdot f\big(a+(b\dot{-}a),c\big) = (1\dot{-}|a,b|)\cdot f(a,c)$$

and, using 65

$$(1\dot{-}|a,b|)\cdot f\big(b+(a\dot{-}b),c\big) = (1\dot{-}|a,b|)\cdot f(b,c)$$

and 86 follows by 62.

87. $|(1\dot{-}c)\cdot a,\ (1\dot{-}c)\cdot b| = (1\dot{-}c)\cdot|a,b|.$ By G*, 44 .

88. $(1\dot{-}|a,b|)\cdot|f(a,c),f(b,c)| = 0.$ By 87, 69, 86 .

86 and 88 are versions of the substitution theorem, they enable us to prove the following uniqueness rule J.

J. $f(0,b,c) = g(0,b,c),\ f(sa,b,c) = p\big(f(a,b,c),h(a,b,c)\big)\,,$
$g(sa,b,c) = p\big(g(a,b,c),h(a,b,c)\big) \vdash f(a,b,c) = g(a,b,c)\,,$

where f, g, h are 3-functors and p is a 2-functor.

We apply I to $|f(a,b,c),g(a,b,c)|$, for

$$\begin{aligned}&\big(1\dot{-}|f(a,b,c),g(a,b,c)|\big)\cdot|f(sa,b,c),g(sa,b,c)|\\ &\quad= \big(1\dot{-}|f(a,b,c),g(a,b,c)|\big)\cdot\big|p\big(f(a,b,c),h(a,b,c)\big),p\big(g(a,b,c),h(a,b,c)\big)\big|\\ &\quad= 0\end{aligned}$$

by 88, J follows from I by 69 and 70.

89. $a\dot{-}(b+c) = (a\dot{-}b)\dot{-}c.$ By J, 34, 39 .

90. $a\cdot(b\dot{-}c) = a\cdot b\dot{-}a\cdot c.$ By J, 81, 34, 89 .

91. $a \cdot |b,c| = |a \cdot b, a \cdot c|$. By 90 .

92. $(a+b) \dot{-} c = (a \dot{-} c) + \big(b \dot{-} (c \dot{-} a)\big)$.

For by 62, 53 and 89,

$$c + \big((a+b) \dot{-} c\big) = c + \Big((a \dot{-} c) + \big(b \dot{-} (c \dot{-} a)\big)\Big)$$

and 92 is given by 71.

93. $\big(1 \dot{-} (sb \dot{-} a)\big) = \big(1 \dot{-} (b \dot{-} a)\big) \dot{-} \big(1 \dot{-} (a \dot{-} b)\big)$. By 92, 89 .

94. $\big(1 \dot{-} (sb \dot{-} a)\big) \cdot (1 \dot{-} |a,b|) = 0$. By 85, 62, 64, 67, 89, 43 .

95. $(1 \dot{-} |a,b|) \cdot |f(c,a), g(b)| = (1 \dot{-} |a,b|) \cdot |f(c,b), g(b)|$. By 86, 91 .

96. $A = 0,\ (1 \dot{-} A) \cdot B = 0 \vdash B = 0$. By U, 73 .

97. $(1 \dot{-} A) \cdot B = 0,\ (1 \dot{-} B) \cdot C = 0 \vdash (1 \dot{-} A) \cdot C = 0$.

By 78, 76, 62, 77, 47 .

98. $(1 \dot{-} A) \cdot B = 0 \vdash (1 \dot{-} A \cdot C) \cdot B \cdot C = 0$. By G*, 89, 90, 43 .

We are now ready to define the pairing function $w(a,b)$.

DEFINITION. $t \to R''ods$.

99. $t(0) = 0$.

100. $t(sa) = t(a) + sa$.

DEFINITION. $w \to C_{22}dC_{12}tdj'$.

101. $w(a,b) = t(a+b) + b$.

DEFINITION. $v \to R''oC_{22}djC_{22}eC_{12}ljC_{22}uC_{12}ts_1j's$.

102. $v(0) = 0$.

103. $v(sa) = v(a) + \Big(1 \dot{-} \Big|t\big(s(v(a))\big), sa\Big|\Big)$.

(1 is defined in 40, u in 63 and s_1 in 19.)

104. $\Big(1 \dot{-} \Big|v\big(t(a)\big), a\Big|\Big) \cdot \big(1 \dot{-} (b \dot{-} a)\big) \cdot \Big|v\big(t(a)+b\big), a\Big| = 0$.

Let $F(a,b) = 0$ stand for this equation, then by 23

$$\big(1 \dot{-} F(a,b)\big) \cdot F(a,sb)$$

$$= \big(1 \dot{-} F(a,b)\big) \cdot \Big(1 \dot{-} \Big|v\big(t(a)\big), a\Big|\Big) \cdot \Big(\big(1 \dot{-} (b \dot{-} a)\big) \dot{-} \big(1 \dot{-} (a \dot{-} b)\big)\Big) \cdot$$
$$\cdot \Big|v\big(t(a)+b\big) + \Big(1 \dot{-} \Big|t\Big(s\Big(v\big(t(a)+b\big)\Big)\Big), t(a)+sb\Big|\Big), a\Big|$$
$$= \big(1 \dot{-} F(a,b)\big) \cdot \Big(1 \dot{-} \Big|v\big(t(a)\big), a\Big|\Big) \cdot \big(1 \dot{-} (sb \dot{-} a)\big) \cdot \Big|a + \big(1 \dot{-} |t(sa), t(a)+sb|\big), a\Big|$$

by 95, 98, 90, 43

$$= \big(1 \dot{-} F(a,b)\big)\cdot\big(1 \dot{-} \big|v\big(t(a)\big),a\big|\big)\cdot\big(1 \dot{-} (sb \dot{-} a)\big)\cdot\big(1 \dot{-} |a,b|\big)$$
$$= 0 \qquad \text{by 64, 67, 100 and 94}.$$

104 follows now by I and 79.

105. $\quad v\big(t(a)\big) = a$.

For by 103, 100, 95 and 66

$$\big(1 \dot{-} \big|v\big(t(a)+a\big),a\big|\big)\cdot\big|v\big(t(sa)\big),sa\big| = 0$$

and so 105 is given by I from this, 104, 97 and 102.

106. $\quad v\big(w(a,b)\big) = a+b$. By 104, 105 .

DEFINITION. $m_2 \to C_{21}eiC_{11}tv$.

107. $\quad m_2(a) = a \dot{-} t\big(v(a)\big)$.

108. $\quad m_2\big(w(a,b)\big) = b$. By 106, 47 .

DEFINITION. $m_1 \to C_{21}evm_2$.

109. $\quad m_1(a) = v(a) \dot{-} m_2(a)$.

110. $\quad m_1\big(w(a,b)\big) = a$. By 108, 106, 47 .

111. $\quad t\big(v(a)\big) \dot{-} a = 0$.

112. $\quad sa \dot{-} t\Big(s\big(v(a)\big)\Big) = 0$.

These two results are derived by considering the two cases $t\Big(s\big(v(a)\big)\Big) = sa$ (which implies $v(sa) = s\big(v(a)\big)$) and $1 \dot{-} \Big|t\Big(s\big(v(a)\big)\Big),sa\Big| = 0$ (which implies $v(sa) = v(a)$) and applying I and some theorems already proved.

113. $\quad w\big(m_1(a),m_2(a)\big) = a$. By 111, 112 .

The theorems 108, 110 and 113 show that the correspondence between numbers and pairs of numbers, defined by $w(a,b)$ is unique.

BIBLIOGRAPHY

1. A. Church, *Binary recursive arithmetic*, J. Math. Pures Appl. (9) 36 (1957), 39–55.
2. R. L. Goodstein, *Logic-free formalisations of recursive arithmetic*, Math. Scand. 2 (1954), 247–261.
3. H. E. Rose, *On the consistency and undecidability of recursive arithmetic*, Z. Math. Logik Grundlagen Math. 7 (1961), 124–135.

THE UNIVERSITY, LEEDS, ENGLAND