

A FORMALISATION OF THE ARITHMETIC OF
TRANSFINITE ORDINALS IN A MULTISUCCESSOR EQUATION
CALCULUS

by

H.P. Williams

Thesis submitted for the degree of
Doctor of Philosophy at the University of Leicester.

1968

UMI Number: U308360

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI U308360

Published by ProQuest LLC 2015. Copyright in the Dissertation held by the Author.
Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against
unauthorized copying under Title 17, United States Code.



ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

X752999/32

Thesis
512.81 (WIL)

358082

20.10.69



To Eileen

Acknowledgement

The preparation of this thesis was supervised by Professor R.L. Goodstein who has been extremely generous with both his time and encouragement. He has helped in many ways. In particular his knowledge has always provided inspiration when it was most needed. The author would like to express his deep thanks.

The author would also like to thank the Science Research Council who provided financial support for this research.

CONTENTS

	<u>Page</u>
Acknowledgement	
Introduction	1
Chapter I. The Arithmetic of the Ordinal Numbers Less than ω^ω .	
1. The Initial Functions.	4
2. Definitions by Primitive Recursion.	5
3. Rules of Inference.	6
4. Addition.	9
5. The Degree Function.	11
6. Multiplication.	12
7. Exponentiation.	19
8. The Component Functions.	23
9. The Sum Function.	24
10. Cantor's Normal Form Theorem.	26
11. The Left Successor Functions.	37
12. Predecessor Functions.	44
13. Subtraction.	46
14. Double Recursion.	50
15. The Key Equation.	51
16. The Difference Function.	59
17. Induction Schemata.	60
18. Results requiring the Doubly Recursive Uniqueness Rule.	64
19. The Absorption Laws.	67
20. Order Relations.	67

21. Results and Schemata involving Equality and Inequality Relations.	72
22. The Propositional Calculus.	75
23. Extensions of the Formalisation to Ordinals greater than ω^ω .	78
Chapter II. A Reduction of the Primitive Recursive Arithmetic of the Ordinals less than ω^ω to the Primitive Recursive Arithmetic of the Natural Numbers.	79
Chapter III. The Consistency of the Formalisation of the Primitive Recursive Arithmetic of the Ordinals less than ω^ω .	87

INTRODUCTION

The arithmetic of the transfinite ordinal numbers is usually developed semantically from a set theory. An ordinal number is the order type of a well ordered set. The functions on ordinal numbers result from combining these sets in different ways. In order to avoid the dependence of this arithmetic on the axioms of set theory a syntactic development is given here of part of this arithmetic. The arithmetic of the ordinal numbers less than ω^ω is developed as a multisuccessor arithmetic.

The first attempt at a syntactic formalisation of the arithmetic of the natural numbers was made by Dedekind from what have become known as Peano's Postulates. Here the notion of a successor function which increases a number by 1 is accepted as primitive. It seems interesting to examine the system which would result from generalising the arithmetic of the natural numbers by accepting as primitive more than one successor function. Starting from 0 a greater variety of numbers could be defined. By placing certain restrictions on the results of combining those successor functions a number of different systems can be developed. One such system has been studied extensively by Vučković and Partis. Here the results of applying the successor functions in different orders are identified. The resulting system is a generalisation of the arithmetic of the natural numbers which preserves many of its properties such as the

commutativity of addition and multiplication. A multisuccessor arithmetic with a different restriction on the successor functions is studied here. The successor functions dominate one another in the sense that the application of a particular successor function followed by another successor function, higher in the hierarchy, has the same effect as the application of only the second successor function. As with Vučković's system this multisuccessor arithmetic will be developed formally as an equation calculus. The axioms will be primitive recursive function definitions together with two axioms involving the combination of successor functions. Four rules of inference will be given for deducing equations from other equations. This system can be readily interpreted as ordinal arithmetic for ordinals less than ω^ω . As with Vučković's system it is a generalisation of the primitive recursive arithmetic of the natural numbers.

In Chapter I the arithmetic of the system is formally developed. The chapter is divided into numbered sections and the results in each section are numbered using a decimal notation. Some of the functions used are indexed by the natural numbers. It is necessary to appeal to certain results and methods of the arithmetic of the natural numbers when manipulating these indices. The arithmetic of the natural numbers, which is used, is accepted and not formally developed. It has already been developed by Goodstein in an equation calculus which could be regarded as a restriction of the system presented here with only the index 0 allowed.

In certain cases the hypotheses of the schemata in the system are only applicable when the indices of functions in the hypotheses are 0. These schemata are then applied to give the limited conclusion of equality between two functions only when their variables are restricted to the natural numbers.

In Chapter II it is shown that there is a $(1,1)$ correspondence between the primitive recursive functions in this multisuccessor system and the primitive recursive functions of the natural numbers which corresponds to a certain $(1,1)$ coding of the ordinals in this system into the natural numbers.

A proof of the consistency of the system developed here is given in Chapter III. This proof follows the same lines as that given by Goodstein for his equation calculus formalisation of the primitive recursive arithmetic of the natural numbers.

CHAPTER I

THE ARITHMETIC OF THE ORDINAL NUMBERS LESS THAN ω^ω .

1. All functions in this system are developed from certain initial functions. These are:

- (i) the identity function $I(x) = x$ which always takes a value equal to the value of its argument.
- (ii) the zero function $N(x) = 0$ which always takes a value equal to zero.
- (iii) a countably infinite number of successor functions
 S_0, S_1, S_2, \dots

The identity and the zero function are used implicitly in the system. The function S_0 behaves in the same way as the function S in the arithmetic of the natural numbers, it increases a number by 1. The functions S_μ (for $\mu > 0$) increase a number to the smallest multiple of ω^μ greater than that number. Therefore $S_\mu 0$ is interpreted as ω^μ with ω^0 being understood to be 1.

The successor functions are restricted by two axioms. These are:

- A $S_\mu S_\nu = S_\mu$ for $\mu > \nu$
- B $S_a S_b \dots S_q = S_{a'} S_{b'} \dots S_{q'}$

with $a \leq b \leq \dots \leq q$ and $a' \leq b' \leq \dots \leq q'$ if and only if

$a = a', b = b', \dots, q = q'.$

Axiom A is what causes this system to differ from the multisuccessor arithmetic developed by Vučković and Partis. Instead of axiom A they give the axiom $S_\mu S_\nu = S_\nu S_\mu$. The resulting arithmetic is quite different and possesses many properties such as commutativity of addition and multiplication which are not found in ordinal arithmetic. Nor is their system totally ordered as is this system. Axiom B enables inequality between two different ordinals to be proved.

2. A function $F(x, y)$ is defined by primitive recursion from previously defined functions $a(x)$ and $b_\mu(x, y, z)$ in the following way

$$F(x, 0) = a(x)$$

$$F(x, S_\mu y) = b_\mu(x, y, F(x, y))$$

The second equality stands for an infinite number of equations, one for each value of the finite index μ . The functions $b_\mu(x, y, z)$ must be related by the following identity imposed by axiom A for this to constitute a proper definition by primitive recursion.

$$C \quad b_\mu(x, S_\nu y, b_\nu(x, y, z)) = b_\mu(x, y, z) \quad \text{for } \nu < \mu.$$

Functions are also defined from previously defined functions by substitution. Starting from the initial functions the class of all functions which can be derived by substitution and primitive recursion will be called the primitive recursive functions.

3. The rules of inference are the following schemata

$$\text{Sb}_1 \quad \frac{F(x) = G(x)}{F(A) = G(A)}$$

$$\text{Sb}_2 \quad \frac{A = B}{F(A) = F(B)}$$

$$\begin{array}{c} \text{T} \quad A = B \\ \\ A = C \\ \hline B = C \end{array}$$

and the primitive recursive uniqueness rule

$$\text{U} \quad \frac{F(S_\mu x) = H_\mu(x, F(x)) \text{ for all } \mu}{F(x) = H^x F(0)}$$

F, G, H_μ are primitive recursive functions and A, B, C primitive recursive terms. The class of primitive recursive terms is the smallest class containing 0, all symbols for variables and $F(t)$ if F is a primitive recursive function and t is a term. The function $H^x t$ is defined by the following primitive recursion.

$$\begin{array}{l} H^0 t = t \\ H^{S_\mu x} t = H_\mu(x, H^x t) \end{array}$$

It is not necessary to stipulate that the functions H_μ satisfy the consistency condition C for this is already guaranteed by $F(x)$ being a primitive recursive function.

A number of auxiliary schemata will now be proved. First the following result is proved.

$$3.1 \quad x = x$$

From the defining equations for addition (which follow) $x + 0 = x$.

Taking A to be $x + 0$ and B and C to be x schema T gives the result. Applying Sb_1 to 3.1 gives $A = A$. Therefore taking C as A, from schema T the following schema is obtained.

$$K \quad \frac{A = B}{B = A}$$

The following is a more useful form of U.

$$U_1 \quad \begin{array}{l} f(0) = g(0) \\ f(S_\mu x) = H_\mu(x, f(x)) \\ g(S_\mu x) = H_\mu(x, g(x)) \end{array} \quad \text{for all } \mu$$

$$f(x) = g(x)$$

U_1 is proved equivalent to U. First suppose U_1 holds and the hypotheses of U hold. By the definition of $H^x t$, $H^0 F(0) = F(0)$, $H^{S^x} F(0) = H_\mu(x, H^x F(0))$. Taking $F(x)$ as $f(x)$ and $g(x)$ as $H^x F(0)$ the hypotheses of U_1 are satisfied. Therefore

$F(x) = g(x) = H^x F(0)$ which is the conclusion of U . Hence

$$U_1 \Rightarrow U$$

Now suppose U holds and the hypotheses of U_1 hold. Taking in turn $f(x)$ and $g(x)$ as $F(x)$, U gives $f(x) = H^x f(0)$ and $g(x) = H^x g(0)$. But $f(0) = g(0)$. Therefore $H^x f(0) = H^x g(0)$ by Sb_2 . Applying K and T gives $f(x) = g(x)$ which is the conclusion of U_1 . Hence

$$U \Rightarrow U_1.$$

Therefore U and U_1 are equivalent schemata.

A particular instance of schema U_1 is frequently used and will therefore be stated as a separate schema. I and J are indexing sets of natural numbers. $I \cup J = \mathbb{Z}$ the set of all natural numbers, $I \cap J = \emptyset$.

$$\begin{array}{lcl}
 & f(0) = g(0) & \\
 U_2 & f(S_\mu x) = g(S_\mu x) \text{ for } \mu \in I & \\
 & \left. \begin{array}{l} f(S_\mu x) = M_\mu f(x) \\ g(S_\mu x) = M_\mu g(x) \end{array} \right\} \text{ for } \mu \in J & \\
 & \hline
 & f(x) = g(x) &
 \end{array}$$

This follows from U_1 . For suppose the hypotheses of U_2 hold. Define

$H_\mu(x, y) = g(S_\mu x)$ for $\mu \in I$. Then $g(S_\mu x) = H_\mu(x, g(x))$ and $f(S_\mu x) = H_\mu(x, f(x))$ for $\mu \in I$ and $H_\mu(x, y) = M_\mu(y)$ for $\mu \in J$.

The conclusion of U_2 follows by U_1 .

FUNCTION DEFINITIONS

A number of elementary functions are now introduced using primitive recursion and certain results in ordinal arithmetic concerning them are proved.

4. Addition

This is defined by the following recursions.

$$a + 0 = a, \quad a + S_{\mu} b = S_{\mu}(a + b) \quad \text{for all } \mu$$

It must be verified that the consistency condition C is satisfied.

This condition will clearly be satisfied if the result of replacing S_{μ} by $S_{\mu} S_{\nu}$ where $\nu < \mu$ in the left hand side of the defining equations, and applying this definition twice, yields an expression which can be shown to be equal to the original expression on the right hand side of the defining equation. Applying this procedure to the above definition gives

$$\begin{aligned} a + S_{\mu} S_{\nu} b &= S_{\mu}(a + S_{\nu} b) \\ &= S_{\mu} S_{\nu}(a + b) \\ &= S_{\mu}(a + b) \quad \text{by axiom A since } \nu < \mu \end{aligned}$$

Hence the definition of addition is consistent.

The following result is proved

$$4.1 \quad 0 + a = a$$

Proof. $0 + 0 = 0$ from the first equation in the definition of addition.

$0 + S_\mu a = S_\mu(0 + a)$ from the second equation in the definition of addition.

Taking $f(a) = 0 + a$, $g(a) = a$, $\mathbf{I} = \mathbf{Z}$ and $\mathbf{J} = \phi$ ^{$M_\mu = S_\mu$} the result follows from U_2 .

$$4.2 \quad S_\mu a = a + \omega^\mu$$

Proof. $a + \omega^\mu = a + S_\mu 0$

$$= S_\mu(a + 0)$$

$$= S_\mu a$$

This result gives the intuitive interpretation which is to be placed on the successor functions S_μ . The operation S_μ applied to an ordinal results in addition of ω^μ on the right.

$$4.3 \quad (a + b) + c = a + (b + c)$$

i.e. addition is associative

Proof. $(a + b) + 0 = a + b$

$$= a + (b + 0)$$

$$(a + b) + S_\mu c = S_\mu[(a + b) + c]$$

$$a + (b + S_\mu c) = a + S_\mu(b + c)$$

$$= S_\mu[a + (b + c)]$$

The result follows from U_2 taking $f(c) = (a + b) + c$, $g(c) = a + (b + c)$, $\mathbf{I} = \phi$, $\mathbf{J} = \mathbf{Z}$ and $M_\mu(x) = S_\mu(x)$.

The associative law also holds for the arithmetic of the natural numbers. However, as is well known, not all results in the arithmetic of the natural numbers generalize to transfinite ordinal arithmetic. In particular this arithmetic is not commutative with respect to addition i.e. it is possible to choose ordinals such that $a + b \neq b + a$. As an example consider $1 + \omega$ and $\omega + 1$.

$$\begin{aligned}
 1 + \omega &= S_0 0 + S_1 0 \\
 &= S_1 (S_0 0 + 0) \\
 &= S_1 S_0 0 \\
 &= S_1 0 \quad \text{by axiom A} \\
 \omega + 1 &= S_1 0 + S_0 0 \\
 &= S_0 (S_1 0 + 0) \\
 &= S_0 S_1 0
 \end{aligned}$$

$S_1 0$ and $S_0 S_1 0$ are not equal by axiom B.

5. The Degree Function

The indices of the successor functions S_μ always have finite values. In order to make definitions involving these functions it is necessary to use part of the arithmetic of the natural numbers in combining these indices with other finite numbers. The function $\text{Max}(m, n)$ in the arithmetic of the natural numbers will be taken as defined and used in such a way. The degree function is defined from this function by the following recursion.

$$d(0) = 0$$

$$d(S_{\mu} a) = \text{Max}(d(a), \mu)$$

The consistency condition is satisfied since

$$\begin{aligned} d(S_{\mu} S_{\nu} a) &= \text{Max}(d(S_{\nu} a), \mu) \\ &= \text{Max}(\text{Max}(d(a), \nu), \mu) \\ &= \text{Max}(d(a), \mu) \quad \text{if } \mu > \nu. \end{aligned}$$

Although the degree function is defined on ordinals it only takes values among the natural numbers.

$$5.1 \quad d(\omega^{\mu}) = \mu$$

Proof.

$$\begin{aligned} \omega^{\mu} &= S_{\mu} 0 \\ d(S_{\mu} 0) &= \text{Max}(d(0), \mu) \\ &= \text{Max}(0, \mu) \\ &= \mu \end{aligned}$$

6. Multiplication

First $a \cdot \omega^{\mu}$ is defined by the equations

$$\begin{aligned} 0 \cdot \omega^{\mu} &= 0 \\ S_{\nu} a \cdot \omega^{\mu} &= \omega^{d(S_{\nu} a) + \mu} \end{aligned}$$

$a \cdot b$ is then defined by $a \cdot 0 = 0$

$$a \cdot S_0 b = a \cdot b + a$$

$$a \cdot S_{\mu} b = a \cdot b + a \cdot \omega^{\mu} \quad \text{for } \mu > 0$$

To prove the definition of $a \cdot b$ consistent it is first necessary to prove two results.

$$6.1 \quad \omega^\nu + \omega^\mu = \omega^\mu \quad \text{if } \mu > \nu$$

Proof.

$$\begin{aligned}
 \omega^\nu + \omega^\mu &= S_\nu 0 + S_\mu 0 \\
 &= S_\mu (S_\nu 0 + 0) \\
 &= S_\mu S_\nu 0 \\
 &= S_\mu 0 \quad \text{by axiom A} \\
 &= \omega^\mu
 \end{aligned}$$

$$6.2 \quad a \cdot \omega^\nu + a \cdot \omega^\mu = a \cdot \omega^\mu \quad \text{if } \mu > \nu$$

Proof.

$$\begin{aligned}
 S_\lambda a \cdot \omega^\nu + S_\lambda a \cdot \omega^\mu &= \omega^{d(a)+\nu} + \omega^{d(a)+\mu} \\
 &= \omega^{d(a)+\mu} \quad \text{by 6.1 if } \mu > \nu
 \end{aligned}$$

and $0 \cdot \omega^\nu + 0 \cdot \omega^\mu = S_\lambda a \cdot \omega^\mu = 0 \cdot \omega^\mu$

The consistency of the definition of multiplication can now be proved

since

$$\begin{aligned}
 a \cdot S_\mu S_\nu b &= a \cdot S_\nu b + a \cdot \omega^\mu \\
 &= (a \cdot b + a \cdot \omega^\nu) + a \cdot \omega^\mu \\
 &= a \cdot b + (a \cdot \omega^\nu + a \cdot \omega^\mu) \\
 &= a \cdot b + a \cdot \omega^\mu \quad \text{by 6.2 if } \mu > \nu
 \end{aligned}$$

$$6.3 \quad 0 \cdot a = 0$$

Proof.

$$0 \cdot 0 = 0$$

$$0 \cdot S_0 a = 0 \cdot a + 0$$

$$= 0 \cdot a$$

$$0 \cdot S_\mu a = 0 \cdot a + 0 \cdot \omega^\mu \quad \text{for } \mu > 0$$

$$= 0.a + 0$$

$$= 0.a$$

The result follows from U_2 taking $f(a) = 0.a$, $g(a) = 0$, $I = \phi$ and $J = Z$. M_μ is the identity function.

$$6.4 \quad a.1 = a$$

Proof. $a.1 = a.S_0 0$

$$a.S_0 0 = a.0 + a$$

$$= 0 + a$$

$$= a$$

$$6.5 \quad 1.\omega^\mu = \omega^\mu$$

Proof. $1.\omega^\mu = S_0 0, \omega^\mu$

$$S_0 0.\omega^\mu = \omega^{\text{Max}(d(0), 0) + \mu}$$

$$= \omega^\mu$$

$$6.6 \quad 1.a = a$$

Proof. $1.0 = 0$

$$1.S_\mu a = 1.a + 1.\omega^\mu$$

$$= 1.a + \omega^\mu \quad \text{by 6.5}$$

$$= S_\mu (1.a)$$

$$S_\mu a = S_\mu a$$

The result follows from U_2 taking $f(a) = 1.a$, $g(a) = a$,

$I = \phi$ and $J = Z$. M_μ is S_μ .

$$6.7 \quad a.(b + c) = a.b + a.c$$

i.e. the left distributive law holds.

Proof. $a.(b + 0) = a.b$

$$a.b + a.0 = a.b + 0$$

$$= a.b$$

$$a.(b + S_\mu c) = a.S_\mu(b + c)$$

$$= a.(b + c) + a.\omega^\mu$$

$$a.b + a.S_\mu c = a.b + (a.c + a.\omega^\mu)$$

$$= (a.b + a.c) + a.\omega^\mu \quad \text{by 4.3}$$

The result follows by U_2 taking $f(a) = a.(b + c)$, $g(a) = a.b + a.c$,

$I = \phi$, $J = \mathbb{Z}$ and $M_\mu(x) = x + a.\omega^\mu$.

The right distributive law does not hold in ordinal arithmetic as is shown by the following example.

$$(\omega + 1).2 = S_0 S_1 0 . S_0 S_0 0$$

$$= S_0 S_1 0 . S_0 0 + S_0 S_1 0$$

$$= (S_0 S_1 0 . 0 + S_0 S_1 0) + S_0 S_1 0$$

$$= (0 + S_0 S_1 0) + S_0 S_1 0$$

$$= S_0 S_1 0 + S_0 S_1 0$$

$$= S_0 (S_0 S_1 0 + S_1 0)$$

$$= S_0 S_1 (S_0 S_1 0 + 0)$$

$$= S_0 S_1 S_0 S_1 0$$

$$= S_0 S_1 S_1 0 \quad \text{by axiom A}$$

$$\begin{aligned}
\omega \cdot 2 + 2 &= S_1 0 \cdot S_0 S_0 0 + S_0 S_0 0 \\
&= (S_1 0 \cdot S_0 0 + S_1 0) + S_0 S_0 0 \\
&= [(S_1 0 \cdot 0 + S_1 0) + S_1 0] + S_0 S_0 0 \\
&= (S_1 0 + S_1 0) + S_0 S_0 0 \\
&= S_1 (S_1 0 + 0) + S_0 S_0 0 \\
&= S_1 S_1 0 + S_0 S_0 0 \\
&= S_0 (S_1 S_1 0 + S_0 0) \\
&= S_0 S_0 (S_1 S_1 0 + 0) \\
&= S_0 S_0 S_1 S_1 0
\end{aligned}$$

$S_0 S_1 S_1 0$ and $S_0 S_0 S_1 S_1 0$ are not equal by axiom B.

Before proving the associativity of multiplication the following, less general, result is proved.

$$6.8 \quad a \cdot (b \cdot \omega^\mu) = (a \cdot b) \cdot \omega^\mu$$

Proof.

$$a \cdot (0 \cdot \omega^\mu) = a \cdot 0$$

$$= 0$$

$$(a \cdot 0) \cdot \omega^\mu = 0 \cdot \omega^\mu$$

$$= 0$$

$$a \cdot (S_\nu b \cdot \omega^\mu) = a \cdot \omega^d(S_\nu b) + \mu$$

$$(a \cdot S_\nu b) \cdot \omega^\mu = (a \cdot b + a \cdot \omega^\nu) \cdot \omega^\mu$$

It is necessary to prove $a \cdot \omega^d(S_\nu b) + \mu = (a \cdot b + a \cdot \omega^\nu) \cdot \omega^\mu$

$$\begin{aligned}
0 \cdot \omega \quad d(S_\nu b) + \mu &= 0 \\
(0 \cdot b + 0 \cdot \omega^\nu) \cdot \omega^\mu &= (0 + 0) \cdot \omega^\mu \\
&= 0 \cdot \omega^\mu \\
&= 0 \\
S_\lambda a \cdot \omega \quad d(S_\nu b) + \mu &= \omega \quad d(S_\lambda a) + d(S_\nu b) + \mu \\
(S_\lambda a \cdot b + S_\lambda a \cdot \omega^\nu) \cdot \omega^\mu &= (S_\lambda a \cdot b + \omega \quad d(S_\lambda a) + \nu) \cdot \omega^\mu \\
&= [S_{d(S_\lambda a)} + \nu(S_\lambda a \cdot b)] \cdot \omega^\mu \\
&= \omega \quad d(S_{d(S_\lambda a)} + \nu(S_\lambda a \cdot b)) + \mu \\
&= \omega \quad \text{Max}(d(S_\lambda a \cdot b), d(S_\lambda a) + \nu) + \mu
\end{aligned}$$

It remains to show

$$d(S_\lambda a) + d(S_\nu b) + \mu = \text{Max}(d(S_\lambda a \cdot b), d(S_\lambda a) + \nu) + \mu$$

$$d(S_\lambda a) + d(S_\nu 0) = d(S_\lambda a) + \nu$$

$$\text{Max}(d(S_\lambda a \cdot 0), d(S_\lambda a) + \nu) = \text{Max}(d(0), d(S_\lambda a) + \nu)$$

$$= \text{Max}(0, d(S_\lambda a) + \nu)$$

$$= d(S_\lambda a) + \nu$$

$$\text{Max}(d(S_\lambda a \cdot S_\delta b), d(S_\lambda a) + \nu) = \text{Max}(d(S_\lambda a) + d(S_\delta b), d(S_\lambda a) + \nu)$$

$$= d(S_\lambda a) + \text{Max}(d(S_\delta b), \nu)$$

$$= d(S_\lambda a) + d(S_\nu S_\delta b)$$

The result $a \cdot \omega \quad d(S_\nu a) + \mu = (a \cdot b + a \cdot \omega^\nu) \cdot \omega^\mu$

now follows by U_2 putting $f(a) = a \cdot \omega \quad d(S_\nu b) + \mu$, $g(a) = (a \cdot b + a \cdot \omega^\nu) \cdot \omega^\mu$,

$I = z$ and $J = \phi$.

The result 6.8 now follows from U_2 putting $f(b) = a.(b.\omega^\mu)$,
 $g(b) = (a.b).\omega^\mu$, $I = Z$ and $J = \phi$.

$$6.9 \quad a.(b.c) = (a.b).c$$

i.e. multiplication is associative

Proof.

$$a.(b.0) = a.0$$

$$= 0$$

$$(a.b).0 = 0$$

$$a.(b.S_\mu c) = a.(b.c + b.\omega^\mu)$$

$$= a.(b.c) + a.(b.\omega^\mu)$$

$$(a.b).S_\mu c = (a.b).c + (a.b).\omega^\mu$$

$$= (a.b).c + a.(b.\omega^\mu) \text{ by 6.8}$$

The result follows by U_2 putting $f(c) = a.(b.c)$, $g(c) = (a.b).c$,
 $I = \phi$, $J = Z$ and $M_\mu(x) = x + a.(b.\omega^\mu)$.

Multiplication is not commutative for transfinite ordinals as it is
for natural numbers. This is shown by the following example.

$$2.\omega = S_0 S_0 0.\omega$$

$$S_0 S_0 0.\omega = \omega^{\text{Max}(d(S_0 0), 0) + 1}$$

$$= \omega^{\text{Max}(\text{Max}(d(0), 0), 0) + 1}$$

$$= \omega$$

$$= S_1 0$$

$$\begin{aligned}
\omega.2 &= S_1 0 . S_0 S_0 0 \\
&= S_1 0 . S_0 0 + S_1 0 \\
&= S_1 0 . 0 + S_1 0 + S_1 0 \\
&= 0 + S_1 0 + S_1 0 \\
&= S_1 0 + S_1 0 \\
&= S_1 (S_1 0 + 0) \\
&= S_1 S_1 0
\end{aligned}$$

$S_1 0$ and $S_1 S_1 0$ are not equal by axiom B.

7. Exponentiation

Since this formalisation only concerns ordinals less than ω^ω a realistic definition of exponentiation for transfinite exponents cannot be given. The definition is therefore by a primitive recursion on the exponent involving only the successor function S_0 . This makes the definition only effective for finite exponents. 0^n is defined first by the recursion

$$\begin{aligned}
0^0 &= 1 \\
0^{S_0 n} &= 0
\end{aligned}$$

$(S_\mu a)^n$ is then defined by the recursion

$$\begin{aligned}
(S_\mu a)^0 &= 1 \\
(S_\mu a)^{S_0 n} &= (S_\mu a)^n . (S_\mu a)
\end{aligned}$$

Since recursion only involves S_0 no consistency condition arises.

$$7.1 \quad a^0 = 1$$

Proof. $0^0 = 1$

$$(S_{\mu} a)^0 = 1$$

The result follows by U_2 taking $f(a) = a^0$, $g(a) = 1$, $I = Z$ and $J = \phi$.

$$7.2 \quad a^1 = a$$

Proof. $a^1 = a^{S_0 0}$

$$= a^0 \cdot a$$

$$= 1 \cdot a$$

$$= a$$

$$7.3 \quad a^{n+m} = a^n \cdot a^m$$

Proof. This will be proved first for $a = 0$ and then for $S_{\nu} a$ in place of a .

$$0^{n+0} = 0^n$$

$$0^n \cdot 0^0 = 0^n \cdot 1$$

$$= 0^n$$

$$0^{n+S_0 m} = 0^{S_0 (n+m)}$$

$$= 0^{n+m} \cdot 0$$

$$= 0$$

$$0^n \cdot 0^{S_0 m} = 0^n \cdot 0$$

$$= 0$$

Hence $0^{n+m} = 0^n \cdot 0^m$ by U_2 taking $f(m) = 0^{n+m}$, $g(m) = 0^n$, 0^m ,
 $I = \{0\}$ and $J = \phi$ and restricting the hypotheses of the schema to
the case $\mu = 0$. Such a restriction in the hypotheses will be allowed
when the variable involved in the recursion can only take finite values.

$$\begin{aligned}
(S_\nu a)^{n+0} &= (S_\nu a)^n \\
(S_\nu a)^n \cdot (S_\nu a)^0 &= (S_\nu a)^n \cdot 1 \\
&= (S_\nu a)^n \\
(S_\nu a)^{n+s_0 m} &= (S_\nu a)^{s_0 (n+m)} \\
&= (S_\nu a)^{n+m} \cdot (S_\nu a) \\
(S_\nu a)^n \cdot (S_\nu a)^{s_0 m} &= (S_\nu a)^n [(S_\nu a)^m \cdot S_\nu a] \\
&= [(S_\nu a)^n \cdot (S_\nu a)^m] \cdot S_\nu a
\end{aligned}$$

Hence $(S_\nu a)^{n+m} = (S_\nu a)^n \cdot (S_\nu a)^m$ by U_2 taking $f(m) = (S_\nu a)^{n+m}$,
 $g(m) = (S_\nu a)^n \cdot (S_\nu a)^m$, $I = \phi$ $J = \{0\}$ and $M_0(x) = x \cdot S_\nu a$ and
restricting the hypotheses of the schema to the case $\mu = 0$. The
final result therefore holds by U_2 taking $f(a) = a^{n+m}$,
 $g(a) = a^n \cdot a^m$, $I = \mathbb{Z}$ and $J = \phi$.

$$74 \quad a^n \cdot m = (a^n)^m$$

Proof.
$$\begin{aligned}
a^n \cdot 0 &= a^0 \\
&= 1
\end{aligned}$$

$$\begin{aligned}
(a^n)^0 &= 1 \\
a^n \cdot s_0 m &= a^{n \cdot m + n} \\
&= a^{n \cdot m}, a^n \\
(a^n)^{s_0 m} &= (a^n)^m \cdot a^n
\end{aligned}$$

The result follows by U_2 taking $f(m) = a^{n \cdot m}$, $g(m) = (a^n)^m$, $I = \phi$, $J = \{0\}$ and $M_0(x) = x \cdot a^n$ and restricting the hypotheses of the schema to the case $\mu = 0$.

Up to now the expression ω^μ has been used as a name for $S_\mu 0$. It must be proved that this agrees with the exponentiation of ω to the finite index μ . In order not to cause confusion in the proof of this when ω^μ is considered as the name for $S_\mu 0$ it will be written $\omega^\underline{\mu}$.

$$\begin{aligned}
\omega^0 &= 1 \\
&= S_0 0 \\
&= \omega^{\underline{0}} \\
\omega^{S_0 n} &= \omega^n \cdot \omega \\
&= S_n 0 \cdot \omega \\
&= \omega^{\underline{\text{Max}(d(0), n) + 1}} \\
&= \omega^{\underline{n+1}} \\
&= \omega^{\underline{S_0 n}}
\end{aligned}$$

The result therefore follows by U_2 taking $f(n) = \omega^n$, $g(n) = \omega^{\underline{n}}$,

$I = \{0\}$, $J = \phi$ and restricting the hypotheses of the schema to the case $\mu = 0$.

The identity $a^n \cdot b^n = (a \cdot b)^n$ which holds for the arithmetic of the natural numbers does not hold when a and b can take values among the transfinite ordinals. This is shown by the following example

$$\begin{aligned}
 \omega^2 \cdot (\omega + 1)^2 &= \omega^2 \cdot (\omega + 1)^{S_0 S_0 0} \\
 &= \omega^2 \cdot (\omega + 1)^{S_0 0} \cdot (\omega + 1) \\
 &= \omega^2 \cdot (\omega + 1) \cdot (\omega + 1) \\
 &= \omega^2 \cdot (\omega + 1) \omega + \omega^2 \cdot (\omega + 1) \cdot 1 \\
 &= (\omega^3 + \omega^2) \cdot \omega + (\omega^3 + \omega^2) \\
 &= \omega^4 + \omega^3 + \omega^2 \\
 &= S_2 S_3 S_4 0 \\
 (\omega \cdot (\omega + 1))^2 &= (\omega^2 + \omega)^2 \\
 &= (\omega^2 + \omega)^{S_0 S_0 0} \\
 &= (\omega^2 + \omega)^{S_0 0} \cdot (\omega^2 + \omega) \\
 &= (\omega^2 + \omega) \cdot (\omega^2 + \omega) \\
 &= (\omega^2 + \omega) \omega^2 + (\omega^2 + \omega) \cdot \omega \\
 &= \omega^4 + \omega^3 \\
 &= S_3 S_4 0
 \end{aligned}$$

$S_2 S_3 S_4 0$ is not equal to $S_3 S_4 0$ by axiom B.

8. The Component Functions

These functions are denoted by C_μ and are defined by the following recursions

$$\begin{aligned}
C_{\mu}(0) &= 0 \\
C_{\mu}(S_{\nu} a) &= C_{\mu}(a) && \text{if } \mu > \nu \\
C_{\mu}(S_{\mu} a) &= S_0 C_{\mu}(a) \\
C_{\mu}(S_{\nu} a) &= 0 && \text{if } \mu < \nu
\end{aligned}$$

These definitions obey the consistency condition since

$$\begin{aligned}
C_{\mu}(S_{\nu} S_{\lambda} a) &= C_{\mu}(S_{\lambda} a) && \text{if } \mu > \nu \\
&= C_{\mu}(a) && \text{if } \mu > \nu > \lambda \\
C_{\mu}(S_{\mu} S_{\lambda} a) &= S_0 C_{\mu}(S_{\lambda} a) \\
&= S_0 C_{\mu}(a) && \text{if } \mu > \lambda \\
C_{\mu}(S_{\nu} S_{\lambda} a) &= 0 && \text{if } \mu < \nu
\end{aligned}$$

Since C_{μ} is defined by primitive recursion from 0 and S_0 it can only take finite values. The intuitive interpretation of the component functions will become apparent later.

9. The Sum Function

For a function f there will be a corresponding sum function denoted by Σ_f . If f is a function of two arguments the summation will be understood to be over the first argument. Therefore for the function $f(x,y)$, Σ_f will be defined by the following recursion.

$$\begin{aligned}
\Sigma_f(0,b) &= f(0,b) \\
\Sigma_f(S_0 a,b) &= f(S_0 a,b) + \Sigma_f(a,b) \\
\Sigma_f(S_{\mu} a,b) &= 0 \quad \text{for } \mu > 0
\end{aligned}$$

This definition is easily seen to be consistent for

$$\Sigma_f(S_\mu S_\nu a, b) = 0 \quad \text{if } \mu > \nu \geq 0$$

In order that the function Σ_f can have transfinite ordinal numbers for its arguments the successor functions S_μ for $\mu > 0$ have been included in the definition. This makes the definition somewhat artificial when Σ_f is considered as representing a sum of values of $f(a, b)$.

In the applications which are made of the sum function, however, the argument a will only take finite values. The above recursion clearly does not give a definition of infinite sums of ordinal numbers. Indeed no such consistent definition is possible in this system. This is shown by the following argument. Suppose $\Sigma_f(x)$ is a function which represents the sum $f(0) + f(1) + \dots + f(x)$. Clearly $\Sigma_f(0) = f(0)$.

$\Sigma_f(S_\mu a) = H_\mu(a, \Sigma_f(a))$ where $H_\mu(x, y)$ is a primitive recursive function.

Case (i) Let $f(x) = 1$ for all x .

Then $\Sigma_f(\omega) = \Sigma_f(S_1 0) = H_1(0, \Sigma_f(0)) = H_1(0, 1)$. The sum $f(0) + f(1) + \dots + f(\omega)$ is equal (in intuitive ordinal arithmetic) to $\omega + 1$.

Case (ii) Let f be defined by the following recursion.

$$f(0) = 1$$

$$f(S_\mu a) = \omega \quad \text{for all } \mu$$

Then $\Sigma_f(\omega) = \Sigma_f(S_1 0) = H_1(0, \Sigma_f(0)) = H_1(0, 1)$. The sum $f(0) + f(1) + \dots + f(\omega)$ is equal (in intuitive ordinal arithmetic) to $\omega^2 + \omega$.

But $\omega + 1$ and $\omega^2 + \omega$ are different ordinals and cannot both be equal to $H_1(0, 1)$.

In the definition of the sum function successive additions are made on the left. Such a definition is clearly different from one in which successive additions are made on the right, since addition is not commutative. The former definition is given in order to simplify an important application of this function.

10. Cantor's Normal Form Theorem

$$a = \sum_h (d(a), a) \quad \text{where} \quad h(m, a) = \omega^m \cdot C_m(a).$$

The first argument of h can only take values among the natural numbers. \sum_h is defined since $d(a)$ is substituted for its first argument and $d(a)$ always takes finite values. Before this theorem is proved a number of other results are required.

$$10.1 \quad \omega^\nu \cdot C_\nu(a) + \omega^\mu = \omega^\mu \quad \text{if } \nu < \mu$$

Proof. $\omega^\nu \cdot C_\nu(0) + \omega^\mu = \omega^\nu \cdot 0 + \omega^\mu$

$$= 0 + \omega^\mu$$

$$= \omega^\mu$$

$$\omega^\nu \cdot C_\nu(S_\lambda a) + \omega^\mu = \omega^\nu \cdot C_\nu(a) + \omega^\mu \quad \text{if } \nu > \lambda$$

$$\omega^\nu \cdot C_\nu(S_\nu a) + \omega^\mu = \omega^\nu \cdot S_0 C_\nu(a) + \omega^\mu$$

$$= (\omega^\nu \cdot C_\nu(a) + \omega^\nu) + \omega^\mu$$

$$= \omega^\nu \cdot C_\nu(a) + \omega^\mu$$

$$\omega^\nu \cdot C_\nu(S_\lambda a) + \omega^\mu = \omega^\nu \cdot 0 + \omega^\mu \quad \text{if } \lambda > \nu$$

$$= 0 + \omega^\mu$$

$$= \omega^\mu$$

The result follows by U_2 taking $f(a) = \omega^\nu \cdot C_\nu(a) + \omega^\mu$,

$g(a) = \omega^\mu$, $I = \{i: i > \nu\}$, $J = \{i: 0 \leq i \leq \nu\}$ and M_λ as the identity function.

$$10.2 \quad a + \omega^\lambda = \omega^\lambda \cdot C_\lambda(a) + \omega^\lambda \quad \text{if } \lambda \geq d(a)$$

PROOF. $0 + \omega^\lambda = \omega^\lambda$

$$\begin{aligned} \omega^\lambda \cdot C_\lambda(0) + \omega^\lambda &= \omega^\lambda \cdot 0 + \omega^\lambda \\ &= \omega^\lambda \end{aligned}$$

$$\begin{aligned} S_\nu a + \omega^\lambda &= S_\lambda S_\nu a \\ &= S_\lambda a \quad \text{if } \lambda > \nu \\ &= a + \omega^\lambda \end{aligned}$$

$$\omega^\lambda \cdot C_\lambda(S_\nu a) + \omega^\lambda = \omega^\lambda \cdot C_\lambda(a) + \omega^\lambda$$

$$S_\lambda a + \omega^\lambda = (a + \omega^\lambda) + \omega^\lambda$$

$$\begin{aligned} \omega^\lambda \cdot C_\lambda(S_\lambda a) + \omega^\lambda &= \omega^\lambda \cdot S_0 C_\lambda(a) + \omega^\lambda \\ &= (\omega^\lambda \cdot C_\lambda(a) + \omega^\lambda) + \omega^\lambda \end{aligned}$$

If $\nu > \lambda$ $d(S_\nu a) > \lambda$.

The result follows by U_2 taking $f(a) = a + \omega^\lambda$, $g(a) = \omega^\lambda \cdot C_\lambda(a) + \omega^\lambda$, $I = \emptyset$, $J = \{i: 0 \leq i \leq \lambda\}$, $M_\mu = I$ for $\mu < \lambda$, and $M_\mu(x) = \frac{\omega^\lambda}{S_\lambda x}$ for $\mu = \lambda$. The restriction of the values of μ in the hypotheses of U_2 limits the conclusion to the cases where $\lambda \geq d(a)$.

$$10.3 \quad \Sigma_h(\lambda, S_\mu a) = 0 \quad \text{where } h(m, a) = \omega^m \cdot C_m(a) \text{ and } \lambda < \mu$$

PROOF. $\Sigma_h(0, S_\mu a) = h(0, S_\mu a)$

$$= \omega^0 \cdot C_0(S_\mu a)$$

$$= \omega^0 \cdot 0 \quad \text{since } \mu > 0$$

$$= 0$$

$$\begin{aligned}
\Sigma_h(S_0\lambda, S_\mu a) &= h(S_0\lambda, S_\mu a) + \Sigma_h(\lambda, S_\mu a) \\
&= \omega^{S_0\lambda} \cdot C_{S_0\lambda}(S_\mu a) + \Sigma_h(\lambda, S_\mu a) \\
&= \omega^{S_0\lambda} \cdot 0 + \Sigma_h(\lambda, S_\mu a) \quad \text{since } S_0\lambda < \mu \\
&= 0 + \Sigma_h(\lambda, S_\mu a) \\
&= \Sigma_h(\lambda, S_\mu a)
\end{aligned}$$

The result follows by U_2 taking $f(\lambda) = \Sigma_h(\lambda, S_\mu a)$, $g(\lambda) = 0$, $I = \phi$, $J = \{0\}$ and M_0 the identity function.

A new function $h'(x, y) = h(x + \mu + 1, y)$ is defined.

$$10.4 \quad \Sigma_h(x, y) = \Sigma_{h'}(x - \mu - 1, y) + \Sigma_h(\mu, y) \quad \text{if } x > \mu.$$

PROOF. When $x = 0$ the result holds vacuously.

$$\Sigma_h(S_0x, y) = h(S_0x, y) + \Sigma_h(x, y)$$

$$\begin{aligned}
\Sigma_{h'}(S_0x - \mu - 1, y) + \Sigma_h(\mu, y) &= \Sigma_{h'}(x - \mu, y) + \Sigma_h(\mu, y) \\
&= \Sigma_{h'}(S_0(x - \mu - 1), y) + \Sigma_h(\mu, y) \\
&= h'(S_0(x - \mu - 1), y) + \Sigma_{h'}(x - \mu - 1, y) \\
&\quad + \Sigma_h(\mu, y) \\
&= h'(S_0x - \mu - 1, y) + \Sigma_{h'}(x - \mu - 1, y) \\
&\quad + \Sigma_h(\mu, y)
\end{aligned}$$

$$\begin{aligned}
&= h(S_0 x, y) + \sum_h (x - \mu - 1, y) \\
&\quad + \sum_h (\mu, y)
\end{aligned}$$

The result holds by U_2 taking $f(x) = \sum_h (x, y)$,

$$\begin{aligned}
g(x) &= \sum_h (x - \mu - 1, y) + \sum_h (\mu, y), \quad I = \phi, \quad J = \{0\} \quad \text{and} \quad M_0(z) = \\
&= h(S_0 x, y) + z,
\end{aligned}$$

$$10.5 \quad \sum_h (\lambda, a) + \omega^\mu = \omega^\mu \quad \text{if } \mu > \lambda$$

$$\begin{aligned}
\text{PROOF.} \quad \sum_h (0, a) + \omega^\mu &= h(0, a) + \omega^\mu \\
&= \omega^0 \cdot C_0(a) + \omega^\mu \\
&= \omega^\mu \quad \text{since } \mu > 0 \\
\sum_h (S_0 \lambda, a) + \omega^\mu &= h(S_0 \lambda, a) + \sum_h (\lambda, a) + \omega^\mu \\
\omega^\mu &= \omega^{S_0 \lambda} \cdot C_{S_0 \lambda}(a) + \omega^\mu \quad \text{if } S_0 \lambda < \mu \\
&= h(S_0 \lambda, a) + \omega^\mu
\end{aligned}$$

The result follows by U_2 taking $f(\lambda) = \sum_h (\lambda, a) + \omega^\mu$, $g(\lambda) = \omega^\mu$,

$$I = \phi, \quad J = \{0\} \quad \text{and} \quad M_0(x) = h(S_0 \lambda, a) + x.$$

$$10.6 \quad \sum_h (\lambda, S_\mu a) = \sum_h (\lambda, a)$$

PROOF.

$$\begin{aligned}
\sum_h (0, S_\mu a) &= h'(0, S_\mu a) \\
&= h(\mu+1, S_\mu a) \\
&= \omega^{\mu+1} \cdot C_{\mu+1}(S_\mu a) \\
&= \omega^{\mu+1} \cdot C_{\mu+1}(S_\mu a) \\
&= h(\mu+1, a)
\end{aligned}$$

$$= h'(0, a)$$

$$= \Sigma_h(0, a)$$

$$\Sigma_h(S_0\lambda, S_\mu a) = h'(S_0\lambda, S_\mu a) + \Sigma_h(\lambda, S_\mu a)$$

$$= h(S_0\lambda + \mu + 1, S_\mu a) + \Sigma_h(\lambda, S_\mu a)$$

$$= \omega^{S_0\lambda + \mu + 1} \cdot C_{S_0\lambda + \mu + 1}(S_\mu a) + \Sigma_h(\lambda, S_\mu a)$$

$$= \omega^{S_0\lambda + \mu + 1} \cdot C_{S_0\lambda + \mu + 1}(a) + \Sigma_h(\lambda, S_\mu a)$$

$$= h(S_0\lambda + \mu + 1, a) + \Sigma_h(\lambda, S_\mu a)$$

$$= h'(S_0\lambda, a) + \Sigma_h(\lambda, S_\mu a)$$

$$\Sigma_h(S_0\lambda, a) = h'(S_0\lambda, a) + \Sigma_h(\lambda, a)$$

The result follows by U_2 taking $f(\lambda) = \Sigma_h(\lambda, S_\mu a)$,

$g(\lambda) = \Sigma_h(\lambda, a)$, $I = \phi$, $J = \{0\}$ and $M_0(x) = h'(S_0\lambda, a) + x$.

PROOF of Cantor's Normal Form Theorem.

Let $g(a) = \Sigma_h(d(a), a)$ where $h(m, a) = \omega^m \cdot C_m(a)$.

$$g(0) = \Sigma_h(d(0), 0)$$

$$= \Sigma_h(0, 0)$$

$$= h(0, 0)$$

$$= \omega^0 \cdot C_0(0)$$

$$= \omega^0 \cdot 0$$

$$= 0$$

$$\begin{aligned} g(S_\mu a) &= \Sigma_h(d(S_\mu a), S_\mu a) \\ &= \Sigma_h(\text{Max}(d(a), \mu), S_\mu a) \end{aligned}$$

Case (i) $\mu \geq d(a)$

$$g(S_\mu a) = \Sigma_h(\mu, S_\mu a)$$

$$g(S_0 a) = \Sigma_h(0, S_0 a)$$

$$= h(0, S_0 a)$$

$$= \omega^0 \cdot C_0(S_0 a)$$

$$= \omega^0 \cdot S_0 C_\bullet(a)$$

For $\mu > 0$

$$g(S_\mu a) = \Sigma_h(S_0(\mu-1), S_\mu a)$$

$$= h(S_0(\mu-1), S_\mu a) + \Sigma_h(\mu-1, S_\mu a)$$

$$= h(\mu, S_\mu a) \quad \text{by 10.3}$$

$$= \omega^\mu \cdot C_\mu(S_\mu a)$$

$$= \omega^\mu \cdot S_0 C_\mu(a)$$

Hence for all $\mu \geq d(a)$

$$g(S_\mu a) = \omega^\mu \cdot S_0 C_\mu(a)$$

$$= \omega^\mu \cdot C_\mu(a) + \omega^\mu$$

$$= a + \omega^\mu \quad \text{by 10.2}$$

$$= S_{\mu} a$$

Case (ii) $\mu < d(a)$

$$\begin{aligned} g(S_{\mu} a) &= \Sigma_h(d(a), S_{\mu} a) \\ &= \Sigma_h(d(a) - \mu - 1, S_{\mu} a) + \Sigma_h(\mu, S_{\mu} a) \quad \text{by 10.4} \\ \Sigma_h(0, S_{\bullet} a) &= h(0, S_0 a) \\ &= \omega^0 \cdot C_0(S_0 a) \\ &= \omega^0 \cdot S_0 C_0(a) \\ &= \omega^0 \cdot C_0(a) + \omega^0 \end{aligned}$$

For $\mu > 0$

$$\begin{aligned} \Sigma_h(\mu, S_{\mu} a) &= \Sigma_h(S_0(\mu-1), S_{\mu} a) \\ &= h(S_0(\mu-1), S_{\mu} a) + \Sigma_h(\mu-1, S_{\mu} a) \\ &= h(\mu, S_{\mu} a) \quad \text{by 10.3} \\ &= \omega^{\mu} \cdot C_{\mu}(S_{\mu} a) \\ &= \omega^{\mu} \cdot S_0 C_{\mu}(a) \\ &= \omega^{\mu} \cdot C_{\mu}(a) + \omega^{\mu} \end{aligned}$$

Hence for all μ

$$\Sigma_h(\mu, S_{\mu} a) = \omega^{\mu} \cdot C_{\mu}(a) + \omega^{\mu}$$

Therefore

$$g(S_{\mu} a) = \Sigma_h(d(a) - \mu - 1, S_{\mu} a) + \omega^{\mu} \cdot C_{\mu}(a) + \omega^{\mu}$$

$$\begin{aligned}\Sigma_h(0, a) + \omega^0 &= h(0, a) + \omega^0 \\ &= \omega^0 \cdot C_0(a) + \omega^0\end{aligned}$$

For $\mu > 0$

$$\begin{aligned}\Sigma_h(\mu, a) + \omega^\mu &= \Sigma_h(S_0(\mu-1), a) + \omega^\mu \\ &= h(S_0(\mu-1), a) + \Sigma_h(\mu-1, a) + \omega^\mu \\ &= h(\mu, a) + \omega^\mu \quad \text{by 10.5} \\ &= \omega^\mu \cdot C_\mu(a) + \omega^\mu\end{aligned}$$

Hence for all $\mu < d(a)$

$$\omega^\mu \cdot C_\mu(a) + \omega^\mu = \Sigma_h(\mu, a) + \omega^\mu$$

Therefore

$$\begin{aligned}g(S_\mu a) &= \Sigma_h(d(a) - \mu - 1, S_\mu a) + \Sigma_h(\mu, a) + \omega^\mu \\ &= \Sigma_h(d(a) - \mu - 1, a) + \Sigma_h(\mu, a) + \omega^\mu \quad \text{by 10.6} \\ &= \Sigma_h(d(a), a) + \omega^\mu \quad \text{by 10.4} \\ &= S_\mu g(a)\end{aligned}$$

Therefore

$$\begin{aligned}g(S_\mu a) &= S_\mu a & \text{if } \mu \geq d(a) \\ g(S_\mu a) &= S_\mu g(a) & \text{if } \mu < d(a)\end{aligned}$$

Taking the subtraction function $\dot{-}$ as defined on the natural numbers

$$g(S_\mu a) = [1 \dot{-} (d(a) \dot{-} \mu)] \cdot S_\mu a + [1 \dot{-} (1 \dot{-} (d(a) \dot{-} \mu))] \cdot S_\mu g(a)$$

the result follows by U_1 taking

$$H_\mu(x,y) = [1 \dot{-} (d(a) \dot{-} \mu)] \cdot S_\mu x + [1 \dot{-} (1 \dot{-} (d(a) \dot{-} \mu))] \cdot S_\mu y$$

Since the degree function and the component functions only take values among the natural numbers Cantor's Normal Form Theorem shows that any ordinal a in this system (i.e. less than ω^ω) can be expressed uniquely in the form

$$a = \omega^{\alpha_1} \cdot a_1 + \omega^{\alpha_2} \cdot a_2 + \dots + \omega^{\alpha_k} \cdot a_k$$

where a_1, a_2, \dots, a_k are natural numbers and $\alpha_1, \alpha_2, \dots, \alpha_k$ is a decreasing sequence of natural numbers.

Denote a preceded by a string of n successor functions S_μ by $S_\mu^{(n)} a$. $S_\mu^{(0)} a$ will be taken as a . The following result is proved.

$$10.7 \quad \omega^\mu \cdot n = S_\mu^{(n)} 0$$

PROOF

$$\begin{aligned} \omega^\mu \cdot 0 &= 0 \\ S_\mu^{(0)} 0 &= 0 \\ \omega^\mu \cdot S_0 n &= \omega^\mu \cdot n + \omega^\mu \\ &= S_\mu(\omega^\mu \cdot n) \\ S_\mu^{(S_0 n)} 0 &= S_\mu^{(n+1)} 0 \\ &= S_\mu S_\mu^{(n)} 0 \end{aligned}$$

The result follows by U_2 taking $f(n) = \omega^\mu \cdot n$, $g(n) = S_\mu^{(n)} 0$,

$I = \emptyset$, $J = \{0\}$ and $M_0 = S_\mu$.

Hence if an ordinal a is given the above representation in

Cantor's Normal Form a can also be expressed in the form

$$a = S_{\alpha_1}^{(a_1)} 0 + S_{\alpha_2}^{(a_2)} 0 \dots S_{\alpha_k}^{(a_k)} 0$$

Using the defining equations for addition a can be expressed in the form

$$a = S_{\alpha_k}^{(a_k)} S_{\alpha_{k-1}}^{(a_{k-1})} \dots S_{\alpha_1}^{(a_1)} 0.$$

Hence Cantor's Normal Form Theorem gives a proof within the system that any ordinal in the system can be uniquely expressed as 0 preceded by a string of successor functions if the indices of the successor functions are in ascending order.

Computation with ordinals written in normal form (as done by, for example, Sierpinski) can be performed algorithmically if the expressions are converted into strings of successor functions and successive applications made of axiom A and the defining equations for the appropriate functions. Examples are given of an addition and a multiplication carried out in this way.

$$\begin{aligned} (\omega^3 + \omega^2 \cdot 2 + \omega + 3) + (\omega^2 + 1) &= S_0 S_0 S_0 S_1 S_2 S_2 S_3 0 + S_0 S_2 0 \\ &= S_0 (S_0 S_0 S_0 S_1 S_2 S_2 S_3 0 + S_2 0) \text{ def. of add.} \\ &= S_0 (S_2 (S_0 S_0 S_0 S_1 S_2 S_2 S_3 0 + 0)) \text{ " " "} \\ &= S_0 S_2 S_0 S_0 S_0 S_1 S_2 S_2 S_3 0 \text{ " " "} \\ &= S_0 S_2 S_2 S_2 S_3 0 \text{ axiom A} \\ &= \omega^3 + \omega^2 \cdot 3 + 1 \end{aligned}$$

$$\begin{aligned}
(\omega^2 + \omega \cdot 3) \cdot (\omega^3 + 1) &= S_1 S_1 S_1 S_2 0 \cdot S_0 S_3 0 \\
&= S_1 S_1 S_1 S_2 0 \cdot S_3 0 + S_1 S_1 S_1 S_2 0 && \text{def. of mult.} \\
&= S_1 S_1 S_1 S_2 0 \cdot 0 + S_1 S_1 S_1 S_2 0 \omega^3 \\
&\quad + S_1 S_1 S_1 S_2 0 && \text{" " "} \\
&= \omega^5 + S_1 S_1 S_1 S_2 0 && \text{" " "} \\
&= S_5 0 + S_1 S_1 S_1 S_2 0 \\
&= S_1 (S_5 0 + S_1 S_1 S_2 0) && \text{" " "} \\
&= S_1 S_1 (S_5 0 + S_1 S_2 0) && \text{" " "} \\
&= S_1 S_1 S_1 (S_5 0 + S_2 0) && \text{" " "} \\
&= S_1 S_1 S_1 S_2 (S_5 0 + 0) \\
&= S_1 S_1 S_1 S_2 S_5 0 && \text{def. of add.} \\
&= \omega^5 + \omega^2 + \omega \cdot 3
\end{aligned}$$

11. The Left Successor Functions

There is a countable infinity of these functions and they are denoted by T_μ and defined by the following recursions.

$$\begin{aligned} T_\mu 0 &= S_\mu 0 \\ T_\mu S_\nu a &= S_\nu T_\mu a \end{aligned}$$

These definitions are consistent for

$$\begin{aligned} T_\mu S_\nu S_\lambda a &= S_\nu T_\mu S_\lambda a \\ &= S_\nu S_\lambda T_\mu a \\ &= S_\nu T_\mu a \quad \text{if } \nu > \lambda \end{aligned}$$

The following analogous result to axiom A is proved

$$A' \quad T_\nu T_\mu = T_\mu \quad \text{if } \mu > \nu$$

PROOF

$$\begin{aligned} T_\nu T_\mu 0 &= T_\nu S_\mu 0 \\ &= S_\mu T_\nu 0 \\ &= S_\mu S_\nu 0 \quad \text{by axiom A} \\ &= S_\mu 0 \\ &= T_\mu 0 \\ T_\nu T_\mu S_\lambda a &= T_\nu S_\lambda T_\mu a \\ &= S_\lambda T_\nu T_\mu a \\ T_\mu S_\lambda a &= S_\lambda T_\mu a \end{aligned}$$

The result follows by U_2 taking $f(a) = T_\nu T_\mu a$, $g(a) = T_\mu a$,

$I = \phi$, $J = Z$ and $M_\lambda = S_\lambda$.

$$11.1 \quad T_\mu a = \omega^\mu + a$$

PROOF $T_\mu 0 = S_\mu 0$

$$\omega^\mu + 0 = \omega^\mu$$

$$T_\mu S_\nu a = S_\nu T_\mu a$$

$$\omega^\mu + S_\nu a = S_\nu (\omega^\mu + a)$$

The result follows by U_2 taking $f(a) = T_\mu a$, $g(a) = \omega^\mu + a$, $I = \phi$ and $M_\nu = S_\nu$. This result shows that the function T_μ is to be interpreted as addition by ω^μ on the left. The analogy between this function and S_μ is clear.

Function definitions using T_μ in place of S_μ .

Suppose $a(x)$ and $b_\mu(x, y, z)$ are primitive recursive functions and $F(x, y)$ is a function satisfying the following equations

$$F(x, 0) = a(x)$$

$$F(x, T_\mu y) = b_\mu(x, y, F(x, y)).$$

In addition the following condition holds on the functions b_μ .

$$C' \quad b_\nu(x, T_\mu y, b_\mu(x, y, z)) = b_\mu(x, y, z) \text{ if } \nu < \mu.$$

This condition is a consistency condition imposed by A' . Do these equations define $F(x, y)$ and necessitate its being primitive recursive? The

answer to this question is in the affirmative. In the same way that it follows from Cantor's Normal Form Theorem that any ordinal a can be expressed in the form

$$a = S_{\alpha_k}^{(a_k)} S_{\alpha_{k-1}}^{(a_{k-1})} \dots S_{\alpha_1}^{(a_1)} 0$$

it also follows that this ordinal can be expressed in the form

$$a = T_{\alpha_1}^{(a_1)} T_{\alpha_2}^{(a_2)} \dots T_{\alpha_k}^{(a_k)} 0$$

It therefore follows that by repeated applications of the above equations which are satisfied by $F(x,y)$ the value of $F(x,y)$ can be calculated. Hence these equations give a definition of $F(x,y)$. The consistency of this definition is guaranteed by the function b_μ satisfying condition C' . It remains to show that this definition makes $F(x,y)$ primitive recursive.

THEOREM. If $a(x)$ and $b_\mu(x,y,z)$ are primitive recursive functions and $F(x,y)$ a function which satisfies the equations

$$F(x,0)' = a(x)$$

$$F(x, T_\mu y) = b_\mu(x, y, F(x, y))$$

where the functions b_μ satisfy the condition C' then $F(x,y)$ is primitive recursive.

PROOF. The function $G_m^\mu(a,b,c)$ is introduced and defined by the following recursion.

$$G_0^\mu(a,b,c) = c$$

$$G_{S_0 m}^{\mu}(a, b, c) = b_{\mu}(a, \omega^{\mu} \cdot m + b, G_m^{\mu}(a, b, c))$$

μ and m are restricted to the natural numbers,

The following result is now proved.

$$G_m^{\mu}(a, b, F(a, b)) = F(a, \omega^{\mu} \cdot m + b)$$

$$G_0^{\mu}(a, b, F(a, b)) = F(a, b)$$

$$F(a, \omega^{\mu} \cdot 0 + b) = F(a, b)$$

$$G_{S_0 m}^{\mu}(a, b, F(a, b)) = b_{\mu}(a, \omega^{\mu} \cdot m + b, G_m^{\mu}(a, b, F(a, b)))$$

$$F(a, \omega^{\mu} \cdot S_0 m + b) = F(a, \omega^{\mu}(1 + m) + b) \quad \text{since } m \text{ is finite}$$

$$= F(a, \omega^{\mu} + (\omega^{\mu} \cdot m + b))$$

$$= F(a, T_{\mu}(\omega^{\mu} \cdot m + b))$$

$$= b_{\mu}(a, \omega^{\mu} \cdot m + b, F(a, \omega^{\mu} \cdot m + b))$$

The result follows by V, taking $f(m) = G_m^{\mu}(a, b, F(a, b))$,

$g(m) = F(a, \omega^{\mu} \cdot m + b)$ and $H_0(x, y) = b_{\mu}(a, \omega^{\mu} \cdot x + b, y)$. The theorem

will now be proved by induction on the degree of the second argument

of $F(x, y)$. Consider $F(a, S_{\nu} b)$.

If $d(b) = 0$ b is finite and $S_0 b = T_0 b$.

Therefore $F(a, S_0 b) = F(a, T_0 b)$

$$= b_0(a, b, F(a, b))$$

For $\nu > 0$ $S_{\nu} b = S_{\nu} 0$ by axiom A

$$= T_{\nu} 0$$

$$\begin{aligned} \text{Therefore } F(a, S_{\nu} b) &= F(a, T_{\nu} 0) \\ &= b_{\nu}(a, b, F(a, 0)) \end{aligned}$$

Hence for $d(b) = 0$ $F(a, S_{\nu} b)$ is defined in terms of a, b and $F(a, 0)$ by a primitive recursive function. If $d(b) > 0$ $d(b) = n + 1$, then $b = \sum_h(n + 1, b)$ where $h(m, a) = \omega^m \cdot C_m(a)$

$$\begin{aligned} &= h(n + 1, b) + \sum_h(n, b) \\ &= \omega^{n+1} \cdot C_{n+1}(b) + \sum_h(n, b) \\ S_{\nu} b &= (\omega^{n+1} \cdot C_{n+1}(b) + \sum_h(n, b)) + \omega^{\nu} \\ &= \omega^{n+1} \cdot C_{n+1}(b) + S_{\nu} \sum_h(n, b) \\ F(a, S_{\nu} b) &= G_{C_{n+1}}^{n+1}(b)(a, S_{\nu} \sum_h(n, b), F(a, S_{\nu} \sum_h(n, b))) \end{aligned}$$

$\sum_h(n, b)$ is of degree n and therefore by the inductive assumption $F(a, S_{\nu} \sum_h(n, b))$ is defined in terms of $a, \sum_h(n, b)$ and $f(a, \sum_h(n, b))$ by a primitive recursive function. Hence $F(a, S_{\nu} b)$ is defined in terms of a, b and $F(a, \bar{b})$ by a primitive recursive function.

The consistency of this definition is guaranteed by the consistency equations C' satisfied by the functions b_{μ} .

This theorem enables primitive recursive functions to be defined by recursions using T_{μ} instead of S_{μ} . For example addition could be defined by the following equations

$$0 + b = b$$

$$11.2 \quad T_{\mu} a + b = T_{\mu} (a + b)$$

PROOF The first equation has already been proved.

For the second equation

$$\begin{aligned} T_{\mu} a + 0 &= T_{\mu} a \\ T_{\mu} (a + 0) &= T_{\mu} a \\ T_{\mu} a + S_{\nu} b &= S_{\nu} (T_{\mu} a + b) \\ T_{\mu} (a + S_{\nu} b) &= T_{\mu} S_{\nu} (a + b) \\ &= S_{\nu} T_{\mu} (a + b) \end{aligned}$$

The result follows by U_2 taking $f(b) = T_{\mu} a + b$, $g(b) = T_{\mu} (a + b)$,

$I = \phi$, $J = \mathbb{Z}$ and $M_{\nu} = S_{\nu}$.

An analogous uniqueness rule to U_1 is now proved.

$$\begin{aligned} f(0) &= g(0) \\ U_1 \quad f(T_{\mu} a) &= H_{\mu}(a, f(a)) \\ g(T_{\mu} a) &= H_{\mu}(a, g(a)) \\ \hline f(a) &= g(a) \end{aligned}$$

Taking $b_{\mu}(x, y, z)$ as $H_{\mu}(y, z)$ in the proof of theorem 1

$$f(S_0 a) = H_0(a, f(a)) \quad \text{if } \mu(a) = 0$$

$$f(S_{\nu} a) = H_{\nu}(a, f(0)) \quad \text{if } \nu > 0$$

$$g(S_0 a) = H_0(a, g(a))$$

$$g(S_{\nu} a) = H_{\nu}(a, f(0)) \quad "$$

$$= H_{\nu}(a, g(0))$$

$$f(S_{\nu} a) = G_{C_{d(a)}(a)}^{d(a)}(S_{\nu} \Sigma_h(d(a)-1, a), f(S_{\nu} \Sigma_h(d(a)-1, a)))$$

$$g(S_{\nu} a) = G_{C_{d(a)}(a)}^{d(a)}(S_{\nu} \Sigma_h(d(a)-1, a), g(S_{\nu} \Sigma_h(d(a)-1, a)))$$

For $d(a) = 0$ the conclusion of U_1' holds by applying U_1 with its hypotheses restricted to $\mu = 0$. The general conclusion of U_1' therefore holds by induction on the degree of a .

As with schema U_1 there is a particular instance of U_1' which is frequently used. I and J are indexing sets of natural numbers.

$$I \cup J = \mathbb{Z}, \quad I \cap J = \emptyset.$$

$$\begin{aligned} f(0) &= g(0) \\ f(T_{\mu} x) &= g(T_{\mu} x) \quad \text{for } \mu \in I \\ f(T_{\mu} x) &= M_{\mu} f(x) \\ g(T_{\mu} x) &= M_{\mu} g(x) \quad \text{for } \mu \in J \\ \hline f(x) &= g(x) \end{aligned}$$

The proof of this schema follows the proof of U_2 .

The following result provides a further connection between S_{μ} and T_{μ} .

$$11.3 \quad a + T_{\mu} b = S_{\mu} a + b$$

PROOF

$$\begin{aligned} a + T_{\mu} b &= a + (\omega^{\mu} + b) \\ &= (a + \omega^{\mu}) + b \\ &= S_{\mu} a + b \end{aligned}$$

This result is the generalisation in this system of the result $a + Sb = Sa + b$ proved by Goodstein and used in the proof of the commutativity of addition in the arithmetic of the natural numbers. When this multisuccessor system is restricted to the natural numbers the functions S_0 and T_0 become identical. Therefore any identity in this system involving functions T_{μ} and S_{μ} becomes an identity in the arithmetic of the natural numbers by substituting the symbol S for T_{μ} and S_{μ} whenever they occur.

12. Predecessor Functions

There are a countable infinity of these functions and they are denoted by P_μ . They are defined by primitive recursions which use the functions T_μ instead of S_μ .

$$P_\mu 0 = 0$$

$$P_\mu T_\nu a = P_\mu a \quad \text{if } \mu > \nu$$

$$P_\mu T_\mu a = a$$

$$P_\mu T_\nu a = T_\nu a \quad \text{if } \mu < \nu$$

These definitions are consistent. To prove consistency it will be sufficient to adopt an analogous procedure to that adopted in the case of successor functions S_μ . Replace T_ν by $T_\lambda T_\nu$, where $\lambda < \nu$, on the left hand side of the defining equations and apply the definition twice. For the predecessor functions suppose

$$(i) \quad \mu > \nu > \lambda$$

$$\begin{aligned} P_\mu T_\lambda T_\nu a &= P_\mu T_\nu a \\ &= P_\mu a \end{aligned}$$

$$(ii) \quad \mu = \nu > \lambda$$

$$\begin{aligned} P_\mu T_\lambda T_\nu a &= P_\mu T_\nu a \\ &= P_\mu T_\mu a \\ &= a \end{aligned}$$

(iii) $\nu > \mu > \lambda$

$$\begin{aligned} P_{\mu} T_{\lambda} T_{\nu} a &= P_{\mu} T_{\nu} a \\ &= T_{\nu} a \end{aligned}$$

(iv) $\nu > \lambda = \mu$

$$\begin{aligned} P_{\mu} T_{\lambda} T_{\nu} a &= P_{\mu} T_{\mu} T_{\nu} a \\ &= T_{\nu} a \end{aligned}$$

(v) $\nu > \lambda > \mu$

$$\begin{aligned} P_{\mu} T_{\lambda} T_{\nu} a &= T_{\lambda} T_{\nu} a \\ &= T_{\nu} a \end{aligned}$$

12.1 $P_{\mu} P_{\nu} = P_{\mu}$ if $\mu > \nu$

PROOF. $P_{\mu} P_{\nu} 0 = P_{\mu} 0 = 0$

Case (i) $\mu > \nu > \lambda$

$$\begin{aligned} P_{\mu} P_{\nu} T_{\lambda} a &= P_{\mu} P_{\nu} a \\ P_{\mu} T_{\lambda} a &= P_{\mu} a \end{aligned}$$

Case (ii) $\mu > \nu = \lambda$

$$\begin{aligned} P_{\mu} P_{\nu} T_{\lambda} a &= P_{\mu} P_{\nu} T_{\nu} a \\ &= P_{\mu} a \end{aligned}$$

$$P_{\mu} T_{\lambda} a = P_{\mu} a$$

Case (iii) $\mu > \lambda > \nu$

$$\begin{aligned} P_{\mu} P_{\nu} T_{\lambda} a &= P_{\mu} T_{\lambda} a \\ &= P_{\mu} a \end{aligned}$$

$$P_{\mu} T_{\lambda} a = P_{\mu} a$$

Case (iv) $\mu = \lambda > \nu$

$$\begin{aligned} P_{\mu} P_{\nu} T_{\lambda} a &= P_{\mu} T_{\lambda} a \\ &= P_{\mu} T_{\mu} a \\ &= a \end{aligned}$$

$$\begin{aligned} P_{\mu} T_{\lambda} a &= P_{\mu} T_{\mu} a \\ &= a \end{aligned}$$

Case (v) $\lambda > \mu > \nu$

$$\begin{aligned} P_{\mu} P_{\nu} T_{\lambda} a &= P_{\mu} T_{\lambda} a \\ &= T_{\lambda} a \end{aligned}$$

$$P_{\mu} T_{\lambda} a = T_{\lambda} a$$

The result follows by U_2' taking $f(a) = P_{\mu} P_{\nu} a$, $g(a) = P_{\mu} a$, $I = \{i: i \geq \nu\}$, $J = \{i: i < \nu\}$ and M_{λ} the identity function.

13. Subtraction

This is defined using the predecessor functions by the following equations.

$$\begin{aligned} a \dot{-} 0 &= a \\ a \dot{-} S_{\mu} b &= P_{\mu} (a \dot{-} b). \end{aligned}$$

The definition is consistent for

$$\begin{aligned}
 a \dot{-} S_{\mu} S_{\nu} b &= P_{\mu} (a \dot{-} S_{\nu} b) \\
 &= P_{\mu} P_{\nu} (a \dot{-} b) \\
 &= P_{\mu} (a \dot{-} b) \quad \text{if } \mu > \nu.
 \end{aligned}$$

The subtraction defined here is not the only possible primitive recursive subtraction. It does, however, behave in many ways as the inverse to addition as is shown in the following results. In particular the important key equation $a + (b \dot{-} a) = b + (a \dot{-} b)$ holds with this form of subtraction but does not with other subtractions. This subtraction does, however, lack certain properties which are associated with the function when defined on the natural numbers. For example the identity $(a + 1) \dot{-} 1 = a$ does not hold as is shown by the following example.

$$\begin{aligned}
 (\omega + 1) \dot{-} 1 &= T_1 T_0 0 - S_0 0 \\
 &\equiv P_0 T_1 T_0 0 \\
 &= T_1 T_0 0 \\
 &= \omega + 1
 \end{aligned}$$

The definition of subtraction gives a connection between a subtraction of $S_{\mu} b$ and a subtraction of b . The following result connects a subtraction of $T_{\mu} b$ and a subtraction of b .

$$13.1 \quad a \dot{-} T_{\mu} b = P_{\mu} a \dot{-} b$$

PROOF. $a \dot{-} T_{\mu} 0 = a \dot{-} S_{\mu} 0$

$$\begin{aligned}
&= P_{\mu}(a \dot{-} 0) \\
&= P_{\mu} a \\
P_{\mu} a \dot{-} 0 &= P_{\mu} a \\
a \dot{-} T_{\mu} S_{\nu} b &= a \dot{-} S_{\nu} T_{\mu} b \\
&= P_{\nu}(a \dot{-} T_{\mu} b) \\
P_{\mu} a \dot{-} S_{\nu} b &= P_{\nu}(P_{\mu} a \dot{-} b)
\end{aligned}$$

The result follows by U_2 taking $f(b) = a \dot{-} T_{\mu} b$, $g(b) = P_{\mu} a \dot{-} b$,
 $I = \{\phi\}$, $J = Z$ and $M_{\nu} = P_{\nu}$.

$$13.2 \quad T_{\mu} a \dot{-} T_{\mu} b = a \dot{-} b$$

PROOF.
$$T_{\mu} a \dot{-} T_{\mu} b = P_{\mu} T_{\mu} a \dot{-} b \quad \text{by 13.1}$$

$$= a \dot{-} b$$

$$13.3 \quad (a + b) \dot{-} (a + c) = b \dot{-} c$$

PROOF
$$(0 + b) \dot{-} (0 + c) = b \dot{-} c$$

$$\begin{aligned}
(T_{\mu} a + b) \dot{-} (T_{\mu} a + c) &= T_{\mu}(a + b) \dot{-} T_{\mu}(a + c) \\
&= (a + b) \dot{-} (a + c) \quad \text{by 13.2}
\end{aligned}$$

The result follows by U_2 taking $f(a) = (a + b) \dot{-} (a + c)$,
 $g(a) = b \dot{-} c$, $I = Z$ and $J = \phi$ and $M_{\mu} = I$.

As particular examples of 13.3 the following results are noted.

$$13.4 \quad (a + b) \dot{-} a = b$$

$$13.5 \quad a \dot{-} (a + b) = 0$$

$$13.6 \quad 0 \dot{-} a = 0$$

$$13.7 \quad a \dot{-} a = 0$$

The corresponding equation to 13.3, $(b + a) \dot{-} (c + a) = b \dot{-} c$ does not hold as is shown by the following example

$$\begin{aligned}
 (\omega + 1) \dot{-} (2 + 1) &= T_1 T_0 0 - S_0 S_0 S_0 0 \\
 &= P_0 P_0 P_0 T_1 T_0 0 \\
 &= T_1 T_0 0 \\
 &= \omega + 1 \\
 \omega \dot{-} 2 &= T_1 0 - S_0 S_0 0 \\
 &= P_0 P_0 T_1 0 \\
 &= T_1 0 \\
 &= \omega
 \end{aligned}$$

13.8 $a \dot{-} (b + c) = (a \dot{-} b) \dot{-} c$

PROOF.

$$a \dot{-} (b + 0) = a \dot{-} b$$

$$(a \dot{-} b) \dot{-} 0 = a \dot{-} b$$

$$\begin{aligned}
 a \dot{-} (b + S_\mu c) &= a \dot{-} S_\mu (b + c) \\
 &= P_\mu (a \dot{-} (b + c))
 \end{aligned}$$

$$(a \dot{-} b) \dot{-} S_\mu c = P_\mu ((a \dot{-} b) \dot{-} c)$$

The result follows by U_2 taking $f(c) = a \dot{-} (b + c)$, $g(c) = (a \dot{-} b) \dot{-} c$,

$I = \phi$, $J = Z$ and $M_\mu = P_\mu$.

13.9 $a.(1 \dot{-} a) = 0$

PROOF.

$$\begin{aligned}
 0.(1 \dot{-} 0) &= 0.1 \\
 &= 0
 \end{aligned}$$

$$T_\mu a.(1 \dot{-} T_\mu a) = T_\mu a.(P_\mu T_0 0 \dot{-} a)$$

$$P_0 T_0 0 \equiv 0$$

$$\begin{aligned} P_\mu T_0 0 &= P_\mu 0 && \text{if } \mu > 0 \\ &= 0 \end{aligned}$$

$$\begin{aligned} \text{Hence } T_\mu a.(P_\mu S_0 0 \dot{-} a) &= T_\mu a.(0 \dot{-} a) && \text{for all } \mu \\ &= T_\mu a.0 && \text{by 13.6} \\ &= 0 \end{aligned}$$

The result follows by U_2 taking $f(a) = a.(1 \dot{-} a)$, $g(a) = 0$,

$I = Z$ and $J = \phi$.

$$13.10 \quad (1 \dot{-} a).a = 0$$

PROOF. $(1 \dot{-} 0).0 = 0$

$$\begin{aligned} (1 \dot{-} T_\mu a).T_\mu a &= (P_\mu T_0 0 \dot{-} a).T_\mu a \\ &= 0.T_\mu a \\ &= 0. \end{aligned}$$

The result follows by U_2 taking $f(a) = (1 \dot{-} a).a$, $g(a) = 0$,

$I = Z$ and $J = \phi$.

14 Double Recursion

A function is said to be defined by double recursion from the functions $a(x)$, $b(y)$ and $C_\mu(x,y,z)$ using the left successor functions T_μ if it satisfies the following equations

$$\begin{aligned} F(x, 0) &= a(x) \\ F(0, T_\mu y) &= b(T_\mu y) \\ F(T_\mu x, T_\mu y) &= C_\mu(x, y, F(x, y)) \end{aligned}$$

where the functions C_μ satisfy the following consistency conditions

imposed by A' .

$$D' \quad C_v(T_\mu x, T_\mu y, C_\mu(x, y, z)) = C_\mu(x, y, z) \quad \text{for } \mu > v$$

It might be supposed that the above equations are inadequate as a definition of $F(x, y)$ since there is no equation expressing $F(T_\mu x, T_\nu y)$, for $\mu \neq \nu$, in terms of $F(s, t)$ where either s is smaller than $T_\mu x$ or t is smaller than $T_\nu y$ or both. Such an equation can however, be deduced from the above equations using A' . Consider $F(T_\mu x, T_\nu y)$ where $\mu \neq \nu$. Suppose $\mu > \nu$, then $F(T_\mu x, T_\nu y) = F(T_\nu T_\mu x, T_\nu y) = b_\nu(T_\mu x, T_\nu y, F(T_\mu x, y))$. A similar argument applies if $\mu < \nu$.

Definitions can be made by double recursions using the successor functions S_μ instead of T_μ . Such definitions are not, however, so simple since it is necessary to give separate equations giving expressions for $F(S_\mu x, S_\nu y)$ when $\mu > \nu$ and $\mu = \nu$ and $\mu < \nu$. This necessitates complicated consistency conditions on the functions in terms of which $F(x, y)$ is defined. No use will be made of this latter type of definition and it will not, therefore, be discussed further.

15. The Key Equation.

The equation $a + (b \dot{-} a) = b + (a \dot{-} b)$ holds in this system. As in the systems of Goodstein and Vučković this equation assumes

great importance since it enables a difference function $[a,b]$ to be defined which has value zero if and only if a and b are equal. Goodstein proves this equation using a doubly recursive uniqueness rule and later manages to give a rather more difficult proof using the primitive recursive uniqueness rule. Vučković's proof of the key equation also uses a doubly recursive uniqueness rule. A proof using the primitive recursive uniqueness rule was later found by Partis. In the system given here a very simple proof of the key equation is presented using a doubly recursive uniqueness rule. Besides simplicity this proof has the virtue of showing intuitively that this equation holds for ordinals less than ω^ω . Such a proof cannot, however, be admitted in the formal development of the system since a doubly recursive uniqueness rule has not been given as one of the inference schema nor has it yet been proved to be a valid schema. Once the key equation has been accepted a doubly recursive uniqueness rule can be proved. It would therefore seem that in this system as in that of Goodstein there is a certain equivalence between the key equation and a doubly recursive uniqueness rule. A formal proof of the key equation will be given here using Cantor's Normal Form Theorem. A doubly recursive uniqueness rule will be formally stated when it is proved. The proof given now of the key equation simply shows that $a + (b \dot{-} a)$ and $b + (a \dot{-} b)$ satisfy the same introductory equations when regarded as doubly recursive functions.

Proof of $a + (b \dot{-} a) = b + (a \dot{-} b)$ using a doubly recursive uniqueness rule.

Let $f(a,b) = a + (b \dot{-} a)$, $g(a,b) = b + (a \dot{-} b)$.

$$f(a,0) = a + (0 \dot{-} a)$$

$$= a + 0$$

$$= a$$

$$g(a,0) = 0 + (a \dot{-} 0)$$

$$= 0 + a$$

$$= a$$

$$f(0, T_\mu b) = 0 + (T_\mu b \dot{-} 0)$$

$$= 0 + T_\mu b$$

$$= T_\mu b$$

$$g(0, T_\mu b) = T_\mu b + (0 \dot{-} T_\mu b)$$

$$= T_\mu b + 0$$

$$= T_\mu b$$

$$f(T_\mu a, T_\mu b) = T_\mu a + (T_\mu b \dot{-} T_\mu a)$$

$$= T_\mu a + (b \dot{-} a)$$

$$= T_\mu [a + (b \dot{-} a)]$$

$$= T_\mu g(a,b)$$

$$g(T_\mu a, T_\mu b) = T_\mu b + (T_\mu a \dot{-} T_\mu b)$$

$$= T_\mu b + (a \dot{-} b)$$

$$= T_\mu [b + (a \dot{-} b)]$$

$$= T_\mu g(a,b)$$

PROOF of $a + (b \dot{-} a) = b + (a \dot{-} b)$ using Cantor's Normal Form Theorem.

By Cantor's Normal Form Theorem a and b can be expressed in the following forms.

$$a = S_{\alpha_k}^{(a_k)} S_{\alpha_{k-1}}^{(a_{k-1})} \dots S_{\alpha_1}^{(a_1)} 0$$

$$= T_{\alpha_1}^{(a_1)} T_{\alpha_2}^{(a_2)} \dots T_{\alpha_k}^{(a_k)} 0$$

$$b = S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_1}^{(b_1)} 0$$

$$= T_{\beta_1}^{(b_1)} T_{\beta_2}^{(b_2)} \dots T_{\beta_l}^{(b_l)} 0$$

where α, β, a, b are all natural numbers $\alpha_k < \alpha_{k-1} < \dots$

$< \alpha_1, \beta_l < \beta_{l-1} < \dots < \beta_1$ and a_l and b_l are non-zero.

$$b \dot{-} a = T_{\beta_1}^{(b_1)} T_{\beta_2}^{(b_2)} \dots T_{\beta_l}^{(b_l)} 0 \dot{-} S_{\alpha_k}^{(a_k)} S_{\alpha_{k-1}}^{(a_{k-1})} \dots S_{\alpha_1}^{(a_1)} 0$$

$$= P_{\alpha_k}^{(a_k)} P_{\alpha_{k-1}}^{(a_{k-1})} \dots P_{\alpha_1}^{(a_1)} T_{\beta_1}^{(b_1)} T_{\beta_2}^{(b_2)} \dots T_{\beta_l}^{(b_l)} 0$$

Case (i) $a = b$

$$b \dot{-} a = 0$$

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

Case (ii) $\beta_1 = \alpha_1, \beta_2 = \alpha_2, \dots, \beta_{l-1} = \alpha_{l-1}, \beta_l = \alpha_l$

$$b_1 = a_1, b_2 = a_2, \dots, b_{l-1} = a_{l-1}, b_l < a_l$$

$$1 \leq i \leq \min(k, l)$$

$$b \dot{-} a = P_{\alpha_k}^{(a_k)} \dots P_{\alpha_{l+1}}^{(a_{l+1})} P_{\alpha_l}^{(a_l)} T_{\beta_l}^{(b_l)} T_{\beta_{l+1}}^{(b_{l+1})} \dots T_{\beta_l}^{(b_l)} 0$$

by successive applications of the defining equations for P^μ .

$$= P_{\alpha_k}^{(a_k)} \dots P_{\alpha_{l+1}}^{(a_{l+1})} P_{\alpha_l}^{(a_l - b_l)} T_{\beta_{l+1}}^{(b_{l+1})} \dots T_{\beta_l}^{(b_l)} 0$$

$$= 0 \text{ since } a_l - b_l > 0 \text{ and } \alpha_l > \beta_{l+1} > \beta_{l+2} > \dots > \beta_l$$

Hence $a + (b \dot{-} a) = a$

Case (iii) $\beta_1 = \alpha_1, \beta_2 = \alpha_2, \dots, \beta_{l-1} = \alpha_{l-1}, \beta_l = \alpha_l$

$$b_1 = a_1, b_2 = a_2, \dots, b_{l-1} = a_{l-1}, b_l > a_l$$

$$b \dot{-} a = P_{\alpha_k}^{(a_k)} \dots P_{\alpha_{l+1}}^{(a_{l+1})} P_{\alpha_l}^{(a_l)} T_{\beta_l}^{(b_l)} T_{\beta_{l+1}}^{(b_{l+1})} \dots T_{\beta_l}^{(b_l)} 0$$

$$= P_{\alpha_k}^{(a_k)} \dots P_{\alpha_{l+1}}^{(a_{l+1})} T_{\beta_l}^{(b_l - a_l)} T_{\beta_{l+1}}^{(b_{l+1})} \dots T_{\beta_l}^{(b_l)} 0$$

$$= T_{\beta_l}^{(b_l - a_l)} T_{\beta_{l+1}}^{(b_{l+1})} \dots T_{\beta_l}^{(b_l)} 0$$

$$\text{since } b_l - a_l > 0 \text{ and } \beta_l > \alpha_{l+1} > \alpha_{l+2} > \dots > \alpha_k$$

$$= S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_l}^{(b_l - a_l)} 0$$

Hence

$$a + (b \dot{-} a) = S_{\alpha_k}^{(a_k)} S_{\alpha_{k-1}}^{(a_{k-1})} \dots S_{\alpha_1}^{(a_1)} 0 + S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_l}^{(b_l - a_l)} 0$$

$$= S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_l}^{(b_l - a_l)} S_{\alpha_k}^{(a_k)} S_{\alpha_{k-1}}^{(a_{k-1})} \dots S_{\alpha_1}^{(a_1)} 0$$

$$= S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_l}^{(b_l - a_l)} S_{\alpha_l}^{(a_l)} S_{\alpha_{l-1}}^{(a_{l-1})} \dots S_{\alpha_1}^{(a_1)} 0$$

by axiom A since $\alpha_k < \alpha_{k-1} < \dots < \alpha_l = \beta_l$

$$= S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_l}^{(b_l)} \dots S_{\beta_1}^{(b_1)} 0$$

since $\alpha_1 = \beta_1, \alpha_2 = \beta_2, \dots, \alpha_{l-1} = \beta_{l-1}, \alpha_l = \beta_l$

$a_1 = b_1, a_2 = b_2, \dots, a_{l-1} = b_{l-1}.$

$$= b$$

Case (iv) $\beta_1 = \alpha_1, \beta_2 = \alpha_2, \dots, \beta_{l-1} = \alpha_{l-1}, \beta_l < \alpha_l$

$b_1 = a_1, b_2 = a_2, \dots, b_{l-1} = a_{l-1}.$

$$\begin{aligned} b \dot{-} a &= P_{\alpha_k}^{(a_k)} \dots P_{\alpha_l}^{(a_l)} T_{\beta_l}^{(b_l)} \dots T_{\beta_l}^{(b_l)} 0 \\ &= P_{\alpha_k}^{(a_k)} \dots P_{\alpha_l}^{(a_l)} 0 \end{aligned}$$

since $\alpha_l > \beta_l \gg \beta_{l+1} > \dots > \beta_l$

$$= 0$$

Hence $a + (b \dot{-} a) = a.$

Case (v) $\beta_1 = \alpha_1, \beta_2 = \alpha_2, \dots, \beta_{l-1} = \alpha_{l-1}, \beta_l > \alpha_l$

$b_1 = a_1, b_2 = a_2, \dots, b_{l-1} = a_{l-1}$

$$\begin{aligned} b \dot{-} a &= P_{\alpha_k}^{(a_k)} \dots P_{\alpha_l}^{(a_l)} T_{\beta_l}^{(b_l)} \dots T_{\beta_l}^{(b_l)} 0 \\ &= T_{\beta_l}^{(b_l)} T_{\beta_{l+1}}^{(b_{l+1})} \dots T_{\beta_l}^{(b_l)} 0 \end{aligned}$$

$$\begin{aligned} & \text{since } \beta_l > \alpha_l > \alpha_{l+1} > \dots > \alpha_k \\ & = S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_1}^{(b_1)} 0 \end{aligned}$$

Hence

$$\begin{aligned} a + (b \dot{-} a) &= S_{\alpha_k}^{(\alpha_k)} S_{\alpha_{k-1}}^{(\alpha_{k-1})} \dots S_{\alpha_1}^{(\alpha_1)} 0 + S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_1}^{(b_1)} 0 \\ &= S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_1}^{(b_1)} S_{\alpha_k}^{(\alpha_k)} S_{\alpha_{k-1}}^{(\alpha_{k-1})} \dots S_{\alpha_1}^{(\alpha_1)} 0 \\ &= S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_1}^{(b_1)} S_{\alpha_{l-1}}^{(\alpha_{l-1})} S_{\alpha_{l-2}}^{(\alpha_{l-2})} \dots S_{\alpha_1}^{(\alpha_1)} 0 \\ &\text{by axiom A since } \beta_l > \alpha_l > \alpha_{l+1} > \dots > \alpha_k \\ &= S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_1}^{(b_1)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_1}^{(b_1)} 0 \\ &\text{since } \alpha_1 = \beta_1, \alpha_2 = \beta_2, \dots, \alpha_{l-1} = \beta_{l-1} \\ &\quad \alpha_l = b_l, \alpha_{l+1} = b_{l+1}, \dots, \alpha_{l-1} = b_{l-1} \\ &= b. \end{aligned}$$

Since the representations of a and b as strings of successor functions as given are unique these five cases exhaust all possibilities. The value of $b + (a \dot{-} b)$ will now be considered for each of these cases.

Case (i) $a = b$

$$a \dot{-} b = 0$$

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

$$= a$$

Case (ii)

Since the conditions in this case are the same as the conditions in case (iii) if a and b are interchanged the value of $b + (a \dot{-} b)$ will be the same as the value of $a + (b \dot{-} a)$ in case (iii) interchanged i.e. a .

Case (iii)

Since the conditions in this case are the same as the conditions in case (ii) if a and b are interchanged the value of $b + (a \dot{-} b)$ will be the same as the value of $a + (b \dot{-} a)$ in case (ii) interchanged i.e. b .

Case (iv)

Since the conditions in this case are the same as the conditions in case (v) if a and b are interchanged the value of $b + (a \dot{-} b)$ will be the same as the value of $a + (b \dot{-} a)$ in case (v) interchanged i.e. a .

Case (v)

Since the conditions in this case are the same as the conditions in case (iv) if a and b are interchanged the value of $b + (a \dot{-} b)$ will be same as the value of $a + (b \dot{-} a)$ in case (iv) interchanged i.e. b .

Hence $a + (b \dot{-} a)$ and $b + (a \dot{-} b)$ are equal in all cases.

In fact they are always equal to either a or b . This fact will be made use of later in the definition of ordering relations.

16. The Difference Function.

This is defined by

$$|a, b| = (a \dot{-} b) + (b \dot{-} a).$$

The following schema is proved.

$$\underline{|A, B| = 0}$$

$$A = B$$

$$\begin{aligned} \text{PROOF. } B \dot{-} A &= [(A \dot{-} B) + (B \dot{-} A)] \dot{-} (A \dot{-} B) \\ &= |A, B| \dot{-} (A \dot{-} B) \\ &= 0 \dot{-} (A \dot{-} B) \quad \text{if the hypothesis holds} \\ &= 0 \end{aligned}$$

$$\begin{aligned} \text{Hence } A \dot{-} B &= (A \dot{-} B) + 0 \\ &= (A \dot{-} B) + (B \dot{-} A) \\ &= |A, B| \\ &= 0 \end{aligned}$$

$$\begin{aligned} \text{Therefore } A + (B \dot{-} A) &= A + 0 \\ &= A \end{aligned}$$

$$\begin{aligned} B + (A \dot{-} B) &= B + 0 \\ &= B \end{aligned}$$

$$A + (B - A) = B + (A \dot{-} B) \quad \text{by the key equation}$$

$$\text{Hence } A = B$$

The implication in this schema clearly holds the other way round for if $A = B$, $(A \dot{-} B) + (B \dot{-} A) = 0 + 0 = 0$. Therefore any equation $F = G$ is provable in this system if and only if the equation

$|F, G| = 0$ is also provable. In this sense these two equations may be said to be equivalent. Any equation in this system may therefore be replaced by an equivalent equation where the right hand side is zero.

17. Induction Schemata

If the proposition P is represented in this equation calculus by the equation $p(x) = 0$ and the proposition Q by the equation $q(x) = 0$ then the proposition $P \rightarrow Q$ will be defined by the equation $(1 \dot{-} p(x))q(x) = 0$. This definition is justified since if $p(x) = 0$ then the equation gives $q(x) = 0$.

The following induction schema

$$\frac{P(0), P(x) \rightarrow P(S_{\mu}x) \text{ for all } \mu}{P(x)}$$

is represented in this system by the schema

$$I_2' \quad \frac{p(0) = 0, (1 \dot{-} p(x))p(S_{\mu}x) = 0 \text{ for all } \mu}{P(x) = 0}.$$

This is a valid schema in this system.

PROOF. Define $q(x)$ by

$$\begin{aligned} q(0) &= 1 \\ q(S_{\mu}a) &= q(a)(1 - p(a)) \end{aligned}$$

This definition is consistent for

$$\begin{aligned} q(S_{\mu}S_{\nu}a) &= q(S_{\nu}a)(1 \dot{-} p(S_{\nu}a)) \\ &= q(a)(1 \dot{-} p(a))(1 \dot{-} p(S_{\nu}a)) \end{aligned}$$

$$\begin{aligned}
&= q(a)\{(1 \dot{-} p(a)) \dot{-} (1 \dot{-} p(a))p(S_\nu a)\} \\
&= q(a)(1 - p(a)) \quad \text{by the hypothesis of the schema.}
\end{aligned}$$

This holds whether $\nu < \mu$ or not. Hence $q(S_\mu a) = 1$ by U_2 taking $f(a) = q(S_\mu a)$, $g(a) = 1$, $I = \phi$, $J = Z$ and M_ν as the identity function. Therefore

$$\begin{aligned}
q(a)(1 \dot{-} p(a)) &= 1 \\
q(a)(1 \dot{-} p(a))p(a) &= p(a) \quad \text{by 13.10}
\end{aligned}$$

Hence $p(a) = 0$.

There is an analogous schema to I_1 using the left successor functions

$$I_1' \quad \frac{P(0) = 0, (1 \dot{-} p(x))p(T_\mu x) = 0 \text{ for all } \mu}{p(x) = 0}$$

PROOF. Define $q(0) = 1$

$$q(T_\mu a) = q(a)(1 \dot{-} p(a))$$

This definition is consistent for

$$\begin{aligned}
q(T_\nu T_\mu a) &= q(T_\mu a)(1 \dot{-} p(T_\mu a)) \\
&= q(a)(1 \dot{-} p(a))(1 \dot{-} p(T_\mu a)) \\
&= q(a)(1 \dot{-} p(a)) \dot{-} q(a)(1 \dot{-} p(a))p(T_\mu a) \\
&= q(a)(1 - p(a)) \quad \text{by the hypothesis of the schema.}
\end{aligned}$$

Since this is true whether $\nu < \mu$ or not $q(T_\mu a) = 1$ by U_2'

taking $f(a) = q(T_\mu a)$, $g(a) = 1$, $I = \phi$, $J = Z$ and M_ν as the identity function.

Therefore

$$q(a)(1 \dot{-} p(a)) = 1$$

$$q(a)(1 \dot{-} p(a))p(a) = p(a) \quad \text{by 13.10}$$

Hence $p(a) = 0$

$$I_2 \frac{f(a,0) = 0, f(0,T_\mu b) = 0, \{f(a,b) = 0\} \rightarrow \{f(T_\mu a, T_\mu b) = 0\} \text{ for all } \mu}{f(a,b) = 0}$$

Before proving this schema two less general schemata will be proved.

$$\frac{f(a,0) = 0, \{f(a,b) = 0\} \rightarrow \{f(T_\mu a, T_\mu b) = 0\} \text{ for all } \mu}{f(c + a, c) = 0}$$

PROOF. Take $p(c) = f(c + a, c)$. Then

$$p(0) = f(a,0)$$

$$= 0 \quad \text{by the hypotheses of the schema}$$

$$P(T_\mu c) = f(T_\mu c + a, T_\mu c)$$

$$= f(T_\mu(c + a), T_\mu c)$$

$$\text{Hence } (1 \dot{-} p(c))p(T_\mu c) = 0 \quad \text{by the hypotheses of the schema.}$$

$$\text{Therefore } p(c) = 0 \quad \text{by } I'_1$$

$$\text{Hence } f(c + a, c) = 0$$

$$\frac{f(a,0) = 0, f(0,T_\mu b) = 0, \{f(a,b) = 0\} \rightarrow \{f(T_\mu a, T_\mu b) = 0\} \text{ for all } \mu}{f(c, c + b) = 0}$$

PROOF Take $p(c) = f(c, c + b)$. Since $f(a, 0) = 0$, $f(0, 0) = 0$.

Also $f(0, T_\mu b) = 0$. Therefore $f(0, b) = 0$

i.e. $p(0) = 0$

$$\begin{aligned} p(T_\mu c) &= f(T_\mu c, T_\mu c + b) \\ &= f(T_\mu c, T_\mu(c + b)) \end{aligned}$$

Hence $(1 \dot{=} p(c))p(T_\mu c) = 0$ by the hypotheses of the schema

Therefore $p(c) = 0$ by I_1^1 .

Hence $f(c, c+b) = 0$

PROOF. of schema I_2 .

As in the proof of the key equation suppose

$$a = S_{\alpha_k}^{(a_k)} S_{\alpha_{k-1}}^{(a_{k-1})} \dots S_{\alpha_1}^{(a_1)} 0$$

$$b = S_{\beta_l}^{(b_l)} S_{\beta_{l-1}}^{(b_{l-1})} \dots S_{\beta_1}^{(b_1)} 0$$

In cases (i), (ii) and (iv) $b + (a \dot{=} b) = a$.

Therefore $f(a, b) = f(b + (a \dot{=} b), b)$.

If the hypotheses of I_2 are satisfied so are the hypotheses of the first of the above two schemata.

Hence $f(b + (a \dot{=} b), b) = 0$

Therefore $f(a, b) = 0$

In cases (iii) and (v) $a + (b \dot{=} a) = b$

Therefore $f(a, b) = f(a, a + (b \dot{=} a))$

If the hypotheses of I_2 are satisfied so are the hypotheses of the second of the above two schemata.

Hence $f(a, a + (b \dot{-} a)) = 0$

Therefore $f(a, b) = 0$

The doubly recursive uniqueness rule is now stated and proved.

$$\begin{array}{l}
 V_1 \quad f(a, 0) = g(a, 0) \\
 \quad f(0, T_\mu b) = g(0, T_\mu b) \\
 \quad f(T_\mu a, T_\mu b) = H_\mu(a, b, f(a, b)) \\
 \quad g(T_\mu a, T_\mu b) = H_\mu(a, b, g(a, b)) \\
 \hline
 \quad f(a, b) = g(a, b)
 \end{array}$$

PROOF. Define $\psi(a, b) = |f(a, b), g(a, b)|$. From the hypotheses of V_1 the following equations result.

$$\begin{array}{l}
 \psi(a, 0) = 0 \\
 \psi(0, T_\mu b) = 0 \\
 \{\psi(a, b) = 0\} \rightarrow \{\psi(T_\mu a, T_\mu b) = 0\}
 \end{array}$$

Therefore $\psi(a, b) = 0$ by I_2 .

Hence $f(a, b) = g(a, b)$

18 A number of proofs which require the doubly recursive uniqueness rule are now given

$$18.1 \quad a.(b \dot{-} c) = a.b \dot{-} a.c$$

i.e. subtraction is distributive with respect to multiplication on the left

$$\begin{array}{l}
 \text{PROOF} \quad a.(b \dot{-} 0) = a.b \\
 \quad a.b \dot{-} a.0 = a.b \dot{-} 0
 \end{array}$$

$$\begin{aligned}
&= a.b \\
a.(0 \dot{-} T_{\mu} c) &= a.0 \\
&= 0 \\
a.0 \dot{-} a.T_{\mu} c &= 0 \dot{-} a.T_{\mu} c \\
&= 0 \\
a.(T_{\mu} b \dot{-} T_{\mu} c) &= a.(b \dot{-} c) \\
a.T_{\mu} b \dot{-} a.T_{\mu} c &= a.(w^{\mu} + b) \dot{-} a.(w^{\mu} + c) \\
&= (a.w^{\mu} + a.b) \dot{-} (a.w^{\mu} + a.c) \\
&= a.b \dot{-} a.c
\end{aligned}$$

The result follows from V_1 taking $f(b,c) = a.(b \dot{-} c)$, $g(b,c) = a.b \dot{-} ac$ and $H_{\mu}(x,y,z) = z$. Subtraction is not, however, distributive with respect to multiplication on the right as is shown by the following example.

$$\begin{aligned}
(2 \dot{-} 1).w &= (T_0 T_0 0 \dot{-} S_0 0).w \\
&= P_0 T_0 T_0 0, w \\
&= T_0 0.w \\
&= S_0 0.w \\
&= w \\
2.w \dot{-} 1.w &= S_0 S_0 0.w - S_0 0.w \\
&= w \dot{-} w \\
&= 0
\end{aligned}$$

$$18.2 \quad (a - b).(b - a) = 0$$

PROOF
$$(a \dot{-} 0).(0 \dot{-} a) = a.0$$

$$= 0$$

$$(0 \dot{-} T_{\mu} b) \cdot (T_{\mu} b \dot{-} 0) = 0 \cdot T_{\mu} b \\ = 0$$

$$(T_{\mu} a \dot{-} T_{\mu} b) \cdot (T_{\mu} b \dot{-} T_{\mu} a) = (a \dot{-} b) \cdot (b \dot{-} a)$$

The result follows from V_1 taking $f(a,b) = (a \dot{-} b) \cdot (b \dot{-} a)$,
 $g(a,b) = 0$ and $H_{\mu}(x, y, z) = z$.

$$18.3 \quad (a \dot{-} b) = (a \dot{-} b) \dot{-} (b \dot{-} a)$$

PROOF $(a \dot{-} 0) \dot{-} (0 \dot{-} a) = (a \dot{-} 0) \dot{-} 0 \\ = a \dot{-} 0$

$$0 \dot{-} T_{\mu} b = 0$$

$$(0 \dot{-} T_{\mu} b) \dot{-} (T_{\mu} b \dot{-} 0) = 0 \dot{-} T_{\mu} b \\ = 0$$

$$T_{\mu} a \dot{-} T_{\mu} b = a \dot{-} b$$

$$(T_{\mu} a \dot{-} T_{\mu} b) \dot{-} (T_{\mu} b \dot{-} T_{\mu} a) = (a \dot{-} b) \dot{-} (b \dot{-} a)$$

The result follows by V_1 taking $f(a,b) = a \dot{-} b$,

$$g(a,b) = (a \dot{-} b) \dot{-} (b \dot{-} a) \text{ and } H_{\mu}(x,y,z) = z.$$

$$18.4 \quad (a + b) \dot{-} c = [(a \dot{-} c) + b] \dot{-} (c \dot{-} a)$$

PROOF. $(a + b) \dot{-} 0 = a + b$

$$[(a \dot{-} 0) + b] \dot{-} (0 \dot{-} a) = (a + b) \dot{-} 0 \\ = a + b$$

$$(0 + b) \dot{-} T_{\mu} c = b \dot{-} T_{\mu} c$$

$$[(0 \dot{-} T_{\mu} c) + b] \dot{-} (T_{\mu} c \dot{-} 0) = b \dot{-} T_{\mu} c$$

$$(T_{\mu} a + b) \dot{-} T_{\mu} c = T_{\mu}(a + b) \dot{-} T_{\mu} c$$

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

$$[(T_\mu a \dot{-} T_\mu c) + b] \dot{-} (T_\mu c \dot{-} T_\mu a) = [(a \dot{-} c) + b] \dot{-} (c \dot{-} a)$$

The result follows by V_1 taking $f(a, c) = (a + b) \dot{-} c$,

$$g(a, c) = [(a \dot{-} c) + b] \dot{-} (c \dot{-} a) \text{ and } H_\mu(x, y, z) = z$$

19. The Absorption Laws.

$$19.1 \quad b + a = a \quad \text{if} \quad d(b) < d(a)$$

PROOF. If $a = 0$ $d(a) = 0$ and the result holds vacuously.

$$b + S_\mu a = S_\mu(a + b)$$

The result holds by U_2 taking $f(a) = b + a$, $g(a) = a$, $I = \phi$,

$J = \mathbb{Z}$ and M_μ as S_μ .

$$19.2 \quad a \dot{-} b = a \quad \text{if} \quad d(b) < d(a)$$

$$\text{PROOF.} \quad a \dot{-} 0 = a$$

$$a \dot{-} T_\mu b = P_\mu a \dot{-} b$$

If $\mu \geq d(a)$ the result holds vacuously. If $\mu < d(a)$ $P_\mu a = a$. Hence

$$a \dot{-} T_\mu b = a \dot{-} b$$

The result follows by U_2 taking $f(a) = a \dot{-} b$, $g(a) = a$, $I = \phi$,

$J = \mathbb{Z}$ and M_μ as the identity function.

20. The Order Relations

The relation $a \leq b$ will be defined by the equation $a + (b \dot{-} a) = b$.

This relation is reflexive, antisymmetric and transitive as is shown by the following results.

$$20.1 \quad a \leq a$$

PROOF $a + (a \dot{-} a) = a + 0$
 $= a$

20.2 $\underline{a \leq b, b \leq a}$
 $a = b$

PROOF $a + (b \dot{-} a) = b$ by the hypotheses of the schema
 $b + (a \dot{-} b) = a$ by the hypotheses of the schema

But $a + (b \dot{-} a) = b + (a \dot{-} b)$

Hence $a = b$

20.3 $\underline{a \leq b, b \leq c}$
 $a \leq c$

PROOF $a + (b \dot{-} a) = b$ by the hypotheses of the schema
 $b + (c \dot{-} b) = c$ by the hypotheses of the schema
 $a + (c \dot{-} a) = a + [(b + (c \dot{-} b)) \dot{-} a]$
 $= a + [(a + (b \dot{-} a) + (c \dot{-} b)) \dot{-} a]$
 $= a + (b \dot{-} a) + (c \dot{-} b)$
 $= b + (c \dot{-} b)$
 $= c$

It must be verified that this definition of the relation \leq corresponds to the usual notion of ordering among the ordinals. Suppose a and b are represented in Cantor's Normal Form by

$$a = \omega^{\alpha_1} \cdot a_1 + \omega^{\alpha_2} \cdot a_2 + \dots + \omega^{\alpha_k} \cdot a_k$$

$$b = \omega^{\beta_1} \cdot b_1 + \omega^{\beta_2} \cdot b_2 + \dots + \omega^{\beta_l} \cdot b_l$$

a and b may then also be represented as the strings of successor functions given in the proof of the key equation. In this proof the conditions in cases (i), (iii) and (v) clearly correspond to the usual notion $a \leq b$. In each of these cases it has been proved $a + (b \dot{-} a) = b$. Conversely if $a + (b \dot{-} a) \neq b$, $a + (b \dot{-} a) = a$ again by the proof of the key equation. Hence $b + (a \dot{-} b) = a$. Therefore $b \leq a$ and unless $a = b$ $a \not\leq b$ by the usual notion of ordinal inequality. Hence the definition of \leq here defined faithfully represents the usually understood notion.

It follows from the definition of \leq and the key-equation that the expression $a + (b \dot{-} a)$ represents the maximum of a and b . This is also the case in Goodstein's system for the natural numbers. In Vučković's system the relation $a + (b \dot{-} a) = b$ partially orders the structure and the expression $a + (b \dot{-} a)$ represents the least upper bound of a and b when the structure is considered as a lattice. In both these systems the equation $a \dot{-} (a \dot{-} b) = b \dot{-} (b \dot{-} a)$ holds. This is analogous to the key-equation. In Goodstein's system the expression $a \dot{-} (a \dot{-} b)$ represents the minimum of a and b and the relation $a \dot{-} (a \dot{-} b) = a$ provides another definition of $a \leq b$. In Vučković's system this relation is the same as the partial order referred to above and the expression $a \dot{-} (a \dot{-} b)$ represents the greatest lower bound when the structure is considered as a lattice. Rather curiously in the system presented here there is no such obvious interpretation for the expression $a \dot{-} (a \dot{-} b)$ and the relation $a \dot{-} (a \dot{-} b) = a$.

The equation $a \dot{-} (a \dot{-} b) = b \dot{-} (b \dot{-} a)$ does not hold as is shown by the following example.

$$\begin{aligned}
 (\omega + 1) \dot{-} [(\omega + 1) \dot{-} \omega] &= (\omega + 1) \dot{-} P_1 T_1 T_0 0 \\
 &= (\omega + 1) \dot{-} T_0 0 \\
 &= P_0 T_1 T_0 0 \dot{-} 0 \\
 &= T_1 T_0 0 \\
 &= \omega + 1 \\
 \omega \dot{-} [\omega \dot{-} (\omega + 1)] &= \omega \dot{-} [\omega \dot{-} S_0 S_1 0] \\
 &= \omega \dot{-} P_0 P_1 T_1 0 \\
 &= \omega \dot{-} P_0 0 \\
 &= \omega \dot{-} 0 \\
 &= \omega
 \end{aligned}$$

This example also shows that $a \dot{-} (a \dot{-} b) = a$ cannot represent the relation $a \leq b$ since $(\omega + 1) \dot{-} [(\omega + 1) \dot{-} \omega] = \omega + 1$ and $\omega + 1 \not\leq \omega$.

The relation $a < b$ is defined by the equation for $S_0 a \leq b$.

This relation is ~~ir~~reflexive, asymmetric and transitive as is shown by the following results

$$204 \quad a < a$$

PROOF. Suppose $a < a$. Then $S_0 a \leq a$. Hence

$$\begin{aligned}
 S_0 a + (a \dot{-} S_0 a) &= S_0 a + P_0 (a \dot{-} a) \\
 &= S_0 a + P_0 0 \\
 &= S_0 a
 \end{aligned}$$

If $S_0 a = a$ $S_0 a \dot{-} a = 0$. Hence $0 = S_0 0$ which is not true by axiom B.

Therefore $a \not\leq a$.

$$20.5 \quad \frac{a < b}{b \not\leq a}$$

PROOF $S_0a + (b \dot{-} S_0a) = b$ by the hypothesis

$$\begin{aligned} S_0b + (a \dot{-} S_0b) &= a + (S_0b \dot{-} a) \\ &= a + [S_0(S_0a + (b \dot{-} S_0a)) \dot{-} a] \\ &= a + [(a + 1 + S_0(b \dot{-} S_0a)) \dot{-} a] \\ &= a + 1 + S_0(b \dot{-} S_0a) \\ &= a + S_0(1 + (b \dot{-} S_0a)) \end{aligned}$$

$$\text{If } a + S_0(1 + (b \dot{-} S_0a)) = a$$

$$S_0(1 + (b \dot{-} S_0a)) = 0$$

Hence $S_00 = 0$ which is not true by axiom B. Therefore $b \not\leq a$

$$20.6 \quad \frac{a < b, b < c}{a < c}$$

PROOF $S_0a + (b \dot{-} S_0a) = b$ by the hypotheses

$S_0b + (c \dot{-} S_0b) = c$ by the hypotheses

$$\begin{aligned} S_0a + (c \dot{-} S_0a) &= S_0a + [(S_0b + (c \dot{-} S_0b)) \dot{-} S_0a] \\ &= S_0a + [(S_0(S_0a + (b \dot{-} S_0a)) + (c \dot{-} S_0b)) \dot{-} S_0a] \\ &= S_0a + [(S_0a + S_0(b \dot{-} S_0a) + (c \dot{-} S_0b)) \dot{-} S_0a] \\ &= S_0a + S_0(b \dot{-} S_0a) + (c \dot{-} S_0b) \\ &= S_0(S_0a + (b \dot{-} S_0a)) + (c \dot{-} S_0b) \\ &= S_0b + (c \dot{-} S_0b) \\ &= c \end{aligned}$$

Hence $a < c$.

It is not yet possible to show that the relation $a \leq b$ is equivalent to the relation $(a < b \text{ or } a = b)$ since the logical connective "or" has not been defined in this system. It can, however, be shown that both $a = b$ and $a < b$ imply the relation $a \leq b$. The first implication follows from the reflexivity of \leq . The second implication is formally stated as

$$20.7 \quad \frac{a < b}{a \leq b}$$

PROOF. $S_0a + (b \dot{-} S_0a) = b$ by the hypothesis

$$\begin{aligned} a + (b \dot{-} a) &= a + [(S_0a + (b \dot{-} S_0a)) \dot{-} a] \\ &= a + [(a + 1 + (b \dot{-} S_0a)) \dot{-} a] \\ &= a + 1 + (b \dot{-} S_0a) \\ &= S_0a + (b \dot{-} S_0a) \\ &= b \end{aligned}$$

21. A number of results and schemata involving the equality and inequality relations will now be proved. For convenience the notation $A \vdash B$ will be used for schemata instead of the previously used notation.

$$21.1 \quad b \leq c \vdash a + b \leq a + c$$

PROOF If $b + (c \dot{-} b) = c$

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

$$\text{If } (a + b) + ((a + c) \dot{-} (a + b)) = a + c$$

$$[(a + b) + ((a + c) \dot{-} (a + b))] \dot{-} a = (a + c) \dot{-} a$$

$$\text{Hence } b + (c \dot{-} b) = c$$

The following result is a particular instance of this schema

$$21.2 \quad a \leq a + b$$

$$a + b = a + c \vdash b = c$$

PROOF If $a + b = a + c$

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

Hence $b = c$

The implication the other way is obvious

The following schema is a particular instance of this schema

$$21.3 \quad a = a + b \vdash b = 0$$

$$21.4 \quad a + b < a + c \vdash b < c$$

PROOF If $S_0(a + b) + [(a + c) \dot{-} S_0(a + b)] = a + c$

$$[(a + b + 1) + ((a + c) \dot{-} (a + b + 1))] \dot{-} a = (a + c) \dot{-} a$$

Hence $(b + 1) + (c \dot{-} (b + 1)) = c$

That is $S_0 b + (c \dot{-} S_0 b) = c$

If $S_0 b + (c - S_0 b) = c$

$$(a + S_0 b) + ((a + c) \dot{-} (a + S_0 b)) = a + c$$

Therefore $S_0(a + b) + ((a + c) - S_0(a + b)) = a + c$

The following is a particular instance of this schema

$$21.5 \quad 0 < b \vdash a < a + b$$

$$21.6 \quad b \leq c \vdash ab \leq ac$$

PROOF If $b + (c \dot{-} b) = c$

$$a[b + (c \dot{-} b)] = ac$$

$$ab + a(c \dot{-} b) = ac$$

$$ab + (ac \dot{-} ab) = ac$$

The following result is a particular instance of this schema

$$21.7 \quad 0 < b \vdash a \leq ab$$

$$21.8 \quad a^2 = 0 \vdash a = 0$$

PROOF If $a^2 = 0$, $a \dot{-} a^2 = a$

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

$$a = 0$$

$$21.9 \quad 0 < b, ab = 0 \vdash a = 0$$

PROOF If $1 + (b \dot{-} 1) = b$

$$a[1 + (b \dot{-} 1)] = ab$$

$$= 0$$

Hence $a + (ab \dot{-} a) = 0$

$$a + (ab \dot{-} a) = a + (0 \dot{-} a) \text{ by the hypothesis}$$

$$= a$$

Therefore $a = 0$

$$21.10 \quad 0 < a, ab = 0 \vdash b = 0$$

PROOF If $ab = 0$, $baba = 0$

Therefore $(ba)^2 = 0$

Hence $ba = 0$

Therefore $b = 0$ by 21.9

$$21.11 \quad 0 < a, \quad ab \leq ac \vdash b \leq c$$

PROOF If $ab + (ac \dot{-} ab) = ac$

$$[ab + (ac \dot{-} ab)] \dot{-} ac = 0$$

$$a[(b + (c \dot{-} b)) \dot{-} c] = 0$$

Hence $(b + (c \dot{-} b)) \dot{-} c = 0$ by 21.10

$$ac \dot{-} [ab + (ac \dot{-} ab)] = 0$$

$$a[c \dot{-} (b + (c \dot{-} b))] = 0$$

Hence $c \dot{-} (b + (c \dot{-} b)) = 0$

Therefore $|b + (c \dot{-} b), c| = 0$

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

$$21.12 \quad 0 < a, \quad ab = ac \vdash b = c$$

PROOF $ab \dot{-} ac = 0$ by the hypotheses

$$a(b \dot{-} c) = 0$$

Hence $b \dot{-} c = 0$ by 21.10

$$ac \dot{-} ab = 0 \quad \text{by the hypotheses}$$

$$a(c \dot{-} b) = 0$$

Hence $c \dot{-} b = 0$ by 21.10

Therefore $|b, c| = 0$

Hence $b = c$

22. The Propositional Calculus

In the system presented here no appeal has been made to the rules of logic. As with the primitive recursive arithmetic of the natural numbers

certain rules of logic may be deduced from the arithmetic of the system,
This is now demonstrated.

The propositional calculus can be developed from the primitive connectives
 \sim (negation), \rightarrow (implication) and the following axiom schemas

- (1) $P \rightarrow (Q \rightarrow P)$
- (2) $(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$
- (3) $(\sim Q \rightarrow \sim P) \rightarrow ((\sim Q \rightarrow P) \rightarrow Q)$

The only rule of inference is Modus ponens.

$$\frac{P \quad P \rightarrow Q}{Q}$$

In this equation calculus all propositions take the form of equations.

The propositions, the logic of which will be considered, will be
propositional functions $f(x) = g(x)$. Using the difference function
such propositional functions may be considered in the form $p(x) = 0$.
Implication between two propositions $p(x) = 0$ and $q(x) = 0$ has
already been defined by the equation

$$(1 \dot{=} p(x)) \cdot q(x) = 0.$$

The negation of a proposition $p(x) = 0$ is defined by the equation.

$$1 \dot{=} p(x) = 0$$

To show that the rules of the propositional calculus operate among
propositional functions it will be sufficient to show that the equations

corresponding to the above axioms hold and that modus ponens is a valid schema in this system. The axioms will be proved with variables for the propositional functions. The substitution schema Sb_1 allows these variables to be replaced by the predicates of propositional functions.

$$22.1 \quad (1 \dot{=} a) \cdot (1 \dot{=} b) \cdot a = 0$$

PROOF $(1 \dot{=} 0) \cdot (1 \dot{=} b) \cdot 0 = 0$

$$\begin{aligned} (1 \dot{=} T_\mu a) \cdot (1 \dot{=} b) \cdot T_\mu a &= (P_\mu T_0 0 \dot{=} a) \cdot (1 \dot{=} b) \cdot T_\mu a \\ &= (0 \dot{=} a) \cdot (1 \dot{=} b) \cdot T_\mu a \\ &= 0 \end{aligned}$$

$$22.2 \quad [1 \dot{=} ((1 \dot{=} a) \cdot (1 \dot{=} b) \cdot c)] \cdot (1 \dot{=} (1 \dot{=} a) \cdot b) \cdot (1 \dot{=} a) \cdot c = 0$$

PROOF $[1 \dot{=} ((1 \dot{=} 0) \cdot (1 \dot{=} b) \cdot c)] \cdot (1 \dot{=} (1 \dot{=} 0) \cdot b) \cdot (1 \dot{=} 0) \cdot c$

$$\begin{aligned} &= (1 \dot{=} (1 \dot{=} b) \cdot c) \cdot (1 \dot{=} b) \cdot c \\ &= 0 \quad \text{by } 13.10 \end{aligned}$$

$$\begin{aligned} &[1 \dot{=} ((1 \dot{=} T_\mu a) \cdot (1 \dot{=} b) \cdot c)] \cdot (1 \dot{=} (1 \dot{=} T_\mu a) \cdot b) \cdot (1 \dot{=} T_\mu a) \cdot c \\ &= [1 \dot{=} ((P_\mu T_0 0 \dot{=} a) \cdot (1 \dot{=} b) \cdot c)] \cdot (1 \dot{=} (P_\mu T_0 0 \dot{=} a) \cdot b) \cdot (P_\mu T_0 0 \dot{=} a) \cdot c \\ &= 0 \end{aligned}$$

$$22.3 \quad [1 \dot{=} (1 \dot{=} (1 \dot{=} b)) \cdot (1 \dot{=} a)] \cdot [1 \dot{=} (1 \dot{=} (1 \dot{=} b)) \cdot a] \cdot b = 0$$

PROOF $[1 \dot{=} (1 \dot{=} (1 \dot{=} 0)) \cdot (1 \dot{=} a)] \cdot [1 \dot{=} (1 \dot{=} (1 \dot{=} 0)) \cdot a] \cdot 0 = 0$

$$\begin{aligned} &[1 \dot{=} (1 \dot{=} (1 \dot{=} T_\mu b)) \cdot (1 \dot{=} a)] \cdot [1 \dot{=} (1 \dot{=} (1 \dot{=} T_\mu b)) \cdot a] \cdot T_\mu b \\ &= (1 \dot{=} (1 \dot{=} a)) \cdot (1 \dot{=} a) \cdot T_\mu b \\ &= 0 \quad \text{by } 13.10 \end{aligned}$$

Modus ponens follows from the schema

$$\begin{array}{c} x = 0 \\ \hline (1 \dot{=} x) \cdot y = 0 \\ \hline y = 0 \end{array}$$

the validity of which follows by substituting 0 for x in the second hypothesis giving $y = 0$.

As explained before it is not possible to give a realistic definition of infinite sums in this system. Nor is it possible to give a realistic definition of infinite products. It is not therefore possible to define the bounded quantifiers A^p_x and E^p_x which are defined in Goodstein's system. The logic of propositional functions which can be derived within this system is therefore limited to propositional functions with free variables.

23. Extensions of the formalisation to ordinals greater than ω^ω

The ordinals less than ω^ω can be represented using successor functions indexed by the natural numbers. In the development of the arithmetic it is necessary to use some of the arithmetic of the natural numbers used in the indexing. By taking more successor functions and using indices extending into transfinite ordinals it is possible to extend this formalisation to ordinals greater than ω^ω . It is necessary, however, to use some of the arithmetic of the indexing transfinite ordinals. If the preceding formalisation of ordinals less than ω^ω is accepted it is then possible to consider successor functions indexed by such ordinals and to formalise ordinal arithmetic for ordinals less than ω^{ω^ω} . This procedure can of course be repeated and formalisations up to any ordinal less than the first epsilon number produced.

CHAPTER II

A REDUCTION OF THE PRIMITIVE RECURSIVE ARITHMETIC OF THE ORDINALS LESS THAN ω^ω TO THE PRIMITIVE RECURSIVE ARITHMETIC OF THE NATURAL NUMBERS.

When an ordinal less than ω^ω is expressed in Cantor's Normal Form the coefficients of the powers of ω are natural numbers. Every such ordinal may therefore be represented uniquely as a sequence of natural numbers and conversely any sequence of natural numbers represents some such ordinal in this coding. As is well known in the primitive recursive arithmetic of the natural numbers there exist $(1,1)$ mappings of the class of sequences of natural numbers onto the class of natural numbers. It is therefore possible to map the class of ordinals less than ω^ω $(1,1)$ onto the class of natural numbers by considering the sequences which represent them. This correspondence between the ordinals in the system and the natural numbers defines a correspondence between functions on those ordinals and functions on the natural numbers. The question naturally arises as to what is the class of functions on the natural numbers which corresponds to the class of primitive recursive functions in the multisuccessor system for the ordinals. It is shown here that this class is the class of primitive recursive functions on the natural numbers. Therefore the arithmetic described in the previous chapter could be derived from the primitive recursive arithmetic of the natural numbers using a suitable coding. Before this result is obtained a number of subsidiary results and definitions are required. Some of these results relate to the primitive recursive arithmetic of the natural numbers and are

derived in Goodstein and Péter.

THEOREM Any primitive recursive function in the single successor system for the natural numbers can be extended to a primitive recursive function in the multisuccessor system. The extension of f will be denoted by f^* .

PROOF. The theorem is true for the initial functions I , N and S by defining

$$I^*(0) = 0$$

$$I^*(S_0 a) = S I^*(a)$$

$$I^*(S_\mu a) = 0 \quad \text{for } \mu > 0$$

$$N^*(a) = 0$$

$$S^*(0) = 1$$

$$S^*(S_0 a) = S_0 S^*(a)$$

$$S^*(S_\mu a) = 0 \quad \text{for } \mu > 0$$

These definitions are clearly consistent and when I^* , N^* and S^* are restricted to the natural numbers they are the functions I , N and S .

It will now be shown that defining new functions by primitive recursion and substitution preserves this property.

Suppose that $f(x, y)$ is defined by primitive recursion from the functions $a(x)$ and $b(x, y, z)$ so that

$$f(x, 0) = a(x)$$

$$f(x, Sy) = b(x, y, f(x, y))$$

and that the theorem holds for $a(x)$ and $b(x, y, z)$. $f^*(x, y)$ can be defined by the following recursion

$$\begin{aligned}
f^*(x, 0) &= a^*(x) \\
f^*(x, S_0 y) &= b^*(x, y, f^*(x, y)) \\
f^*(x, S_\mu y) &= 0 \quad \text{for } \mu > 0
\end{aligned}$$

This definition is clearly consistent.

Suppose that $f(x_1, x_2, \dots, x_n)$ is defined by substitution from the functions $a(x_1, x_2, \dots, x_m)$ and $b_i(x_1, x_2, \dots, x_n)$ for $i = 1, 2, \dots, m$ so that

$$\begin{aligned}
f(x_1, x_2, \dots, x_n) &= a(b_1(x_1, x_2, \dots, x_n), b_2(x_1, x_2, \dots, x_n), \\
&\quad \dots, b_m(x_1, x_2, \dots, x_n))
\end{aligned}$$

and that the theorem holds for $a(x_1, x_2, \dots, x_m)$ and $b_i(x_1, x_2, \dots, x_n)$.

$f^*(x_1, x_2, \dots, x_n)$ can be defined by

$$\begin{aligned}
f^*(x_1, x_2, \dots, x_n) &= a^*(b^*_1(x_1, x_2, \dots, x_n), b^*_2(x_1, x_2, \dots, x_n), \\
&\quad \dots, b^*_m(x_1, x_2, \dots, x_n))
\end{aligned}$$

The theorem therefore holds for all primitive recursive functions.

DEFINITION. A primitive recursive $(1,1)$ mapping from the class of sequences of natural numbers onto the class of natural numbers will be defined by the following primitive recursive functions if they satisfy the following conditions

$$\begin{aligned}
[j_k(a_0, a_1, \dots, a_k)]_i &= a_i \quad \text{for } 0 \leq i \leq k, \quad k = 0, 1, 2 \text{ etc} \\
&= 0 \quad \text{for } k > i.
\end{aligned}$$

$$j_{D(a)}((a)_0, (a)_1, \dots, (a)_{D(a)}) = a$$

$$j_{k+1}(a_0, a_1, \dots, a_k, 0) = j_k(a_0, a_1, \dots, a_k)$$

The function j_k maps a sequence of $k+1$ numbers to a single number and the

function $()_i$ picks out the $(i + 1)$ st member of the sequence corresponding to a number. The third condition means that any sequence can be regarded as a sequence of numbers followed by an unlimited sequence of zeros. $D(a)$ is a primitive recursive function such that $D(a) + 1$ gives the number of terms in the sequence corresponding to a up to the last non-zero term.

It is well known that primitive recursive functions satisfying these conditions exist. For example if p_0, p_1, \dots are the successive prime numbers the primitive recursive functions defining the following correspondence satisfy the conditions.

$$(a_0, a_1, a_2, \dots, a_k) \longleftrightarrow p_0^{a_0} p_1^{a_1} \dots p_k^{a_k} - 1$$

A $(1,1)$ mapping from the ordinals to the natural numbers is defined by the following function.

$$G(\alpha) = j_{d(\alpha)}^*(C_0(\alpha), C_1(\alpha), \dots, C_{d(\alpha)}(\alpha))$$

This function is clearly a primitive recursive function in the multisuccessor system.

The inverse mapping from the natural numbers to the ordinals is defined by the following function

$$H(x) = \sum_{h^*} (D(x), x) \text{ where } h(x, y) = \omega^x \cdot (y)_x$$

This function is primitive recursive in the multisuccessor system.

DEFINITION. A function on the ordinals, which when restricted to the natural numbers, always takes values among the natural numbers will be said to be regular.

THEOREM. The restriction of a primitive recursive regular function to the natural numbers is a primitive recursive function in the single successor system. The restriction of a function f will be denoted by f' .

PROOF. Suppose $f(x,y)$ is a regular function and is defined by primitive recursion from the primitive recursive functions $a(x)$ and $b_{\mu}(x,y,z)$ by

$$f(x,0) = a(x)$$

$$f(x, S_{\mu}y) = b_{\mu}(x, y, f(x,y))$$

$b_0(x,y,z)$ is not necessarily a regular function but $b_0(x,y,f(x,y))$ takes values among the natural numbers when x and y do since $f(x,y)$ is regular. Therefore b_0 may be replaced by C_0b_0 and the definitions will remain unchanged for finite x and y . Although $a(x)$ is regular it will be replaced by $C_0a(x)$. For convenience b_0 and a will now denote these new regular functions. The restriction of $f(x,y)$ can now be defined in the single successor system by the following recursion.

$$f'(x,0) = a'(x)$$

$$f'(x, Sy) = b'_0(x,y,f'(x,y))$$

It is necessary to verify that if F is an initial function in the multisuccessor system the restriction of C_0F is primitive recursive in the single successor system. I_{ord} and N_{ord} will denote the identity and zero functions in the multisuccessor system and I_{Nat} and N_{Nat} the same functions in the single successor system.

$$(C_0 I_{Ord})' = I_{Nat}$$

$$(C_0 N_{Ord})' = N_{Nat}$$

$$(C_0 S_0)' = S$$

$$(C_0 S_\mu)' = N_{Nat} \text{ for } \mu > 0.$$

Suppose $f(x_1, x_2, \dots, x_n)$ is defined by substitution from $a(x_1, x_2, \dots, x_m)$ and $b_i(x_1, x_2, \dots, x_n)$ for $i = 1, 2, \dots, m$ by

$$f(x_1, x_2, \dots, x_n) = a(b_1(x_1, x_2, \dots, x_n), b_2(x_1, x_2, \dots, x_n), \dots, b_m(x_1, x_2, \dots, x_n))$$

and that $f(x_1, x_2, \dots, x_n)$ is regular. Define new functions

c and e_i by

$$c(x_1, x_2, \dots, x_m) = a(Hx_1, Hx_2, \dots, Hx_m)$$

$$e_i(x_1, x_2, \dots, x_n) = Gb_i(x_1, x_2, \dots, x_n)$$

Since G and H are inverse functions

$$f(x_1, x_2, \dots, x_n) = c(e_1(x_1, x_2, \dots, x_n), e_2(x_1, x_2, \dots, x_n), \dots, e_m(x_1, x_2, \dots, x_n))$$

If a and b_i are primitive recursive functions so are c and e_i .

Clearly e_i is regular. c is not necessarily regular but when it takes finite values it will be the same as the function $C_0 c$. The function c will therefore be now taken to stand for $C_0 c$ and the definition will be unchanged. The restriction of f may therefore be defined by

$$f'(x_1, x_2, \dots, x_n) = c'(e_1'(x_1, x_2, \dots, x_n), e_2'(x_1, x_2, \dots, x_n), \dots, e_m'(x_1, x_2, \dots, x_n))$$

Hence if c' and e_i' are primitive recursive in the single successor system so is f' . It remains to show that if F is an initial function in the multisuccessor system the restrictions of C_0FH and GF are primitive recursive in the single successor system.

$$(C_0I_{Ord}H)'(x) = (x)_0$$

$$(C_0N_{Ord}H)'(x) = N_{Nat}(x)$$

$$(C_0S_0H)'(x) = S[(x)_\bullet]$$

$$(C_0S_\mu H)'(x) = N_{Nat}(x) \quad \text{for } \mu > 0$$

$$(GI_{Ord})'(x) = j_0(x)$$

$$(GN_{Ord})'(x) = j_0(0)$$

$$(GS_0)'(x) = j_0(Sx)$$

$$(GS_\mu)'(x) = j_\mu(0, 0, \dots, 1) \quad \text{for } \mu > 0.$$

THEOREM. Given a primitive recursive $(1,1)$ mapping from the class of sequences of natural numbers onto the class of natural numbers a $(1,1)$ correspondence can be defined between the ordinals less than ω^ω and the natural numbers. A $(1,1)$ mapping can be defined from the class of primitive recursive functions in the multisuccessor system for those ordinals onto the class of primitive recursive functions in the single successor system for the natural numbers which preserves this correspondence.

PROOF. Suppose $F(x)$ is a primitive recursive function in the multisuccessor system for the ordinals. Consider the function $GFH(x)$.

This is clearly regular and primitive recursive. Define $f(x)$ to be the restriction of this function to the natural numbers. $f(x)$ is therefore primitive recursive in the single successor system and preserves the correspondence between the ordinals less than ω^ω and the natural numbers.

Suppose $f(x)$ is a primitive recursive function in the single successor system for the natural numbers. Then $f(x)$ can be extended to a primitive recursive function $f^*(x)$ in the multisuccessor system for the ordinals. Define

$$F(x) = Hf^*G(x)$$

$F(x)$ is clearly primitive recursive in the multisuccessor system and preserves the correspondence between the ordinals less than ω^ω and the natural numbers.

The generalisation of these results to functions of more than one variable is obvious.

CHAPTER III

THE CONSISTENCY OF THE FORMALISATION OF THE PRIMITIVE RECURSIVE ARITHMETIC OF THE ORDINALS LESS THAN ω^ω .

In this chapter a meta-argument will be used to show that this system is consistent in the following sense. If $p = q$ is a provable equation in this formalisation where p and q are ordinals then they are the same ordinal.

DEFINITION. An equation $F = G$ is said to be verifiable only if F and G are the same ordinal or the substitution of ordinals for the variables in F and G always reduces F and G to the same ordinal.

It is therefore sufficient to show that only verifiable equations are provable.

It will first be shown that, when the variables are replaced by ordinals, the sign of any primitive recursive function is eliminable. This is obviously true for the initial functions $I(x)$ and $N(x)$. It is also true for the initial functions $S_\mu(x)$ since the appearance of "+" in the name of ordinals such as $\omega + 1$ need only be regarded as constituting part of the name for $\omega + 1$. A new symbolism could be found in which such a sign did not appear. This property of the signs being eliminable is preserved under substitution. If $f(x,y)$, $g(x,y)$ and $h(x,y)$ are eliminable then for any given set of ordinals M, N there are unique ordinals U, V, W such that the equations

$$g(M, N) = U, \quad h(M, N) = V \quad \text{and} \quad f(U, V) = W$$

are provable. For the function $\phi(x,y)$ defined by

$$\phi(x,y) = f(g(x,y), h(x,y))$$

the equation

$$\phi(M,N) = W$$

is provable for one, and only one, W corresponding to the given pair M,N . Hence $\phi(x,y)$ is eliminable. This result clearly generalises to substitutions involving functions of more than two variables.

The property is also preserved under primitive recursions. Suppose $f(x,y)$ is defined by the following equations

$$f(x,0) = a(x)$$

$$f(x, S_{\mu} y) = b_{\mu}(x, y, f(x, y))$$

where the functions $b_{\mu}(x, y, z)$ obey the consistency condition C.

Consider two ordinals A and B . B can be expressed at $S_{\alpha_0}^{a_0} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0$

where $\alpha_0 < \alpha_1 < \dots < \alpha_m$ and a_i are non-zero natural numbers.

If $a(x)$ and $b_{\mu}(x, y, z)$ are eliminable there are ordinals. $\forall i, j$ such that it can be proved in turn that

$$a(A) = V_{m,0}, \quad b_{\alpha_m}(A, 0, V_{m,0}) = V_{m,1}, \quad b_{\alpha_m}(A, S_{\alpha_m} 0, V_{m,1}) = V_{m,2}, \dots,$$

$$b_{\alpha_m}(A, S_{\alpha_m}^{a_m} 0, V_{m,a_m-1}) = V_{m,a_m}, \quad b_{\alpha_{m-1}}(A, S_{\alpha_{m-1}} S_{\alpha_m}^{a_m} 0, V_{m,a_m}) = V_{m-1,1}, \dots,$$

$$b_{\alpha_0}(A, B, V_{0,a_0-1}) = V_{0,a_0}.$$

Hence it can be proved that $f(A,B) = V_{0,a_0}$. It must be shown that

V_{0,a_0} is unique. Suppose that this is not so and that it can also be

proved that $f(A, B) = W_{o, a_o} \cdot f(A, B)$ can be evaluated in a number of ways since

$$S_{\alpha_o}^{a_o} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0 = S_{\alpha_o} S_{\beta_o}^{b_o} S_{\beta_1}^{b_1} S_{\beta_n}^{b_n} S_{\alpha_o}^{a_o-1} S_{\alpha_1}^{a_1} \dots S_{\alpha_n}^{a_n} 0$$

for any $\beta_i < \alpha_o$ by axiom A. Suppose V_{o, a_o} is derived from

$f(A, S_{\beta_o}^{b_o} S_{\beta_1}^{b_1} \dots S_{\beta_n}^{b_n} S_{\alpha_o}^{a_o-1} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0)$. Then making $f(A, S_{\beta_o}^{b_o} S_{\beta_1}^{b_1} \dots S_{\beta_n}^{b_n} S_{\alpha_o}^{a_o-1}$

$$S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0) = Y_{o, a_o-1}$$

$$V_{o, n_o} = b_{\alpha_o} (A, S_{\alpha_o}^{a_o-1} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0, V_{o, a_o-1}) \text{ and}$$

$$W_{o, n_o} = b_{\alpha_o} (A, S_{\beta_o}^{b_o} S_{\beta_1}^{b_1} \dots S_{\beta_n}^{b_n} S_{\alpha_o}^{a_o-1} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0, Y_{o, a_o-1})$$

$$Y_{o, a_o-1} = b_{\beta_o} (A, S_{\beta_o}^{b_o-1} S_{\beta_1}^{b_1} \dots S_{\beta_n}^{b_n} S_{\alpha_o}^{a_o-1} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0, Y_{o, a_1-1, o, b_o-1})$$

where $Y_{o, a_o-1, o, b_o-1} = f(A, S_{\beta_o}^{b_o-1} S_{\beta_1}^{b_1} \dots S_{\beta_n}^{b_n} S_{\alpha_o}^{a_o-1} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0)$

Applying the condition C which holds between the functions b_μ since

$$\beta_o < \alpha_o.$$

$$W_{o, n_o} = b_{\alpha_o} (A, S_{\beta_o}^{b_o-1} S_{\beta_1}^{b_1} \dots S_{\beta_n}^{b_n} S_{\alpha_o}^{a_o-1} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0, Y_{o, a_o-1, o, b_o-1})$$

This condition can be applied repeatedly since $\beta_i < \alpha_o$,

giving

$$W_{o, n_o} = b_{\alpha_o} (A, S_{\alpha_o}^{a_o-1} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0, Y_{o, a_o-1, n, o})$$

$$Y_{o, a_o-1, n, o} = f(A, S_{\alpha_o}^{a_o-1} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0)$$

Defining W_{0,a_0-1} as $Y_{0,a_0-1,n,0}$ it becomes necessary to prove that V_{0,a_0-1} and W_{0,a_0-1} are not equal. Proceeding as before it becomes necessary to successively prove $V_{0,a_0-2}, \dots, V_{0,0}, V_{1,a_1}, \dots, V_{m,0}$ not equal to $W_{0,a_0-2}, \dots, W_{0,0}, W_{1,a_1}, \dots, W_{m,0}$. But $V_{m,0} = a(A)$ and $W_{m,0} = a(A)$ and since $a(x)$ is eliminable $V_{m,0} = W_{m,0}$. Therefore V_{0,a_0} is unique and so $f(x,y)$ is eliminable.

The substitution of an ordinal for x in the equation $x = x$ yields a verifiable equation. It is now shown that the rules of inference yield verifiable equations from verifiable equations. Sb_1 and T obviously do so. For Sb_2 two cases must be considered. Firstly if A and B are two ordinals and $A = B$ is verifiable then A and B are the same ordinal and $F(A) = F(B)$ is verifiable. Secondly if A and B are functions then since $A = B$ by hypothesis the result of substituting the same ordinal for the free variables in A and B yields the same ordinal and so substituting ordinals for the free variables in $F(A)$ and $F(B)$ the same ordinal is obtained. Hence $F(A) = F(B)$ is verifiable.

Finally it must be shown that if the equation $F = G$ is proved by the primitive recursive uniqueness rule it must be a verifiable equation.

Suppose

$$F(x,0) = a(x), F(x, S_{\mu} y) = b_{\mu}(x, y, F(x, y))$$

$$G(x,0) = a(x), G(x, S_{\mu} y) = b_{\mu}(x, y, G(x, y))$$

are all verifiable equations. Consider two ordinals A and B such that

$$B = S_{\alpha_0}^{a_0} S_{\alpha_1}^{a_1} \dots S_{\alpha_m}^{a_m} 0$$

where $\alpha_0 < \alpha_1 < \dots < \alpha_m$ and a_i are natural numbers. Let the values of

$$F(A, 0), F(A, S_{\alpha_m} 0), F(A, S_{\alpha_m}^2 0), \dots, F(A, S_{\alpha_m}^{a_m} 0),$$

$$F(A, S_{\alpha_{m-1}} S_{\alpha_m}^{a_m} 0), \dots, F(A, B) \text{ and}$$

$$G(A, 0), G(A, S_{\alpha_m} 0), G(A, S_{\alpha_m}^2 0), \dots, G(A, S_{\alpha_m}^{a_m} 0),$$

$$G(A, S_{\alpha_{m-1}} S_{\alpha_m}^{a_m} 0), \dots, G(A, B) \text{ be}$$

$$V_{m,0}, V_{m,1}, V_{m,2}, \dots, V_{m,a_m}, V_{m-1,1}, \dots, V_{0,a_0}$$

and $W_{m,0}, W_{m,1}, W_{m,2}, \dots, W_{m,a_m}, W_{m-1,1}, \dots, W_{0,a_0}$. It can be successively proved that $V_{m,0} = W_{m,0}$ since both are equal to $a(A)$ and

$$V_{m,1} = b_{\alpha_m}(A, S_{\alpha_m} 0, V_{m,0}) = b_{\alpha_m}(A, S_{\alpha_m} 0, W_{m,0}) = W_{m,1}$$

$$V_{m,2} = b_{\alpha_m}(A, S_{\alpha_m}^2 0, V_{m,1}) = b_{\alpha_m}(A, S_{\alpha_m}^2 0, W_{m,1}) = W_{m,2}$$

$$\cdot \quad \cdot$$

$$\cdot \quad \cdot$$

$$\cdot \quad \cdot$$

$$V_{0,a_0} = b_{\alpha_0}(A, B, V_{0,a_0-1}) = b_{\alpha_0}(A, B, W_{0,a_0-1}) = W_{0,a_0}$$

Therefore the equation $F = G$ is verifiable.

BIBLIOGRAPHY

- R. Dedekind, Essays on the theory of numbers, Chicago, (1901)
- R.L. Goodstein, Recursive number theory, Amsterdam, (1957)
- M.T. Partis, Commutative partially ordered recursive arithmetics,
Mathematica Scandinavica 13, (1963) 199-216
- R. Péter, Recursive functions , New York, (1967)
- W. Sierpinski, Cardinal and Ordinal numbers, Warsaw (1958)
- V. Vučković, Partially ordered recursive arithmetics,
Mathematica Scandinavica 7, (1959) 306-320.
- H.P. Williams, A Formalisation of the Arithmetic of the Ordinals less than ω^ω . (To appear in the Notre Dame Journal of Formal Logic).

The synthesis of logical nets consisting of NOR units

By H. P. Williams*

This paper describes an algorithm for synthesising a logical net consisting of NOR units. Starting with a logical function presented as a truth table the function is converted into a succession of NOR statements. A simplifying procedure is used which, while not always resulting in the minimum number of NOR units, produces an economical solution. Details are given of how this algorithm can be programmed for automatic computation.

(First received November 1967)

In the construction of electronic and fluidic circuits it is often necessary to construct a logical net to perform some given logical function. These nets are often synthesised from NOR units. The NOR unit acting on two inputs, A and B , performs the function $\overline{A \vee B}$ written in Boolean algebra. This is a 'universal function' in the sense that any function in Boolean algebra can be constructed by using successive applications of this function only. Hence the advantage of using NOR units in a logical net is that no other type of logical unit is needed.

A logical net to perform some prescribed logical function can usually be constructed in many different ways. Clearly it will usually be desirable to construct such a net using as small a number of components as possible, in this case NOR units. An algorithm is described which, starting with a logical function presented as a truth table, converts the function to an expression composed only of NOR statements. Simplifications are performed which result in the use of an economical number of NOR units. This algorithm has been programmed for automatic computation.

Description of the algorithm

The method is based on successive applications of operations described by Quine (1955). First the function under consideration is presented as a truth table. The truth table is always written in the way shown below using 0 to signify 'false' and 1 to signify 'true'. The rows represent successive numbers written in binary form. Table 1 gives an example of a function F of three arguments A, B, C .

Table 1

A	B	C	F
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Stage 1. Delete the rows of the truth table which correspond to the function having value 1. In the example these are rows 1, 7 and 8.

Stage 2. Simplify the remaining portion of the truth table using the following three operations based on those of Quine.

- (i) If any two rows differ only in one column, in one row the entry being 0 and in the other 1, delete one of the rows and delete the entry in the other row. In the example after performing this operation on rows 2 and 4 the result would be the single row 0 - 1.

This operation is based on the logical equivalence,

$$\overline{X} \cdot \phi \vee X \cdot \phi \equiv \phi$$

- (ii) If one row completely contains another row except for a difference in one column, where one entry is 0 and the other entry is 1, delete this entry in the longer row. For example in the following two rows the first entry in the second row would be deleted.

$$\begin{array}{c} 0 - 1 \\ 1 0 1 \end{array}$$

This operation is based on the logical equivalence

$$X \vee \overline{X} \phi = X \vee \phi$$

- (iii) If one row completely contains another delete the longer row. For example in the following two rows the second row would be deleted.

$$\begin{array}{c} 0 - 1 \\ 0 0 1 \end{array}$$

This operation is based on the logical equivalence

$$X \vee X \cdot \phi \equiv X$$

Each pair of rows is examined in turn and operations (i), (ii) or (iii) performed if possible. If one of the operations is performed the comparison of all the rows is repeated. After completion of this stage the function can be represented as a negation of a disjunction of the complete sum of prime implicants. In the example in Table 1 the result is

$$\overline{A} \cdot C \vee \overline{A} \cdot B \vee A \cdot \overline{B} \vee \overline{B} \cdot C$$

* Department of Mathematics, The University, Leicester.

Stage 3. Examine the resulting rows of the simplified truth table for a row containing only a 1.

Case (i). If such a row exists the input represented by the column of this single entry is an input to the last NOR unit in the net. The logical function can now be considered in the form

$$\overline{X \vee \phi}$$

where X is the input which has just been considered and ϕ is the rest of the function under the negation. The function can also be written in the form

$$\text{NOR}(X, \phi)$$

showing more clearly that X is an input to the last NOR unit. The other input to this NOR unit must be a net performing the logical function ϕ . After deleting the row of the simplified truth table containing the single entry 1, if no rows of the truth table remain then this NOR unit has no other inputs. If only one row remains and this consists of only an entry 1, the column of this entry gives the other input to the NOR unit. Otherwise the remainder of the truth table is expanded into the standard form. This can be done by comparing the entries in each row of the remainder of the truth table with the corresponding entries in each possible row of the standard truth table. Where these corresponding entries are equal the row of the standard truth table is retained. For example if the remainder of the truth table consisted of the single row $-0-$, on comparison with the standard truth table shown in Table 1 it can be seen that the second column in rows 1, 2, 5 and 6 is 0. Hence these rows are retained and the row $-0-$ has been expanded into the four rows:

0 0 0
0 0 1
1 0 0
1 0 1

These rows are now deleted from the standard truth table such as Table 1. The remaining truth table is now simplified as in stage 2 and the whole procedure repeated producing a logical net for the function ϕ which connects onto the last NOR unit.

Case (ii). If no row containing only a 1 exists then none of the external inputs goes to the last NOR unit. This is the case in the example where the function has been expressed in the form

$$\overline{\bar{A} \cdot C \vee \bar{A} \cdot B \vee A \cdot \bar{B} \vee \bar{B} \cdot C}$$

In this case the rows of the simplified truth table are split up into two sections if possible so the function can be considered in the form

$$\overline{\phi \vee \psi}$$

or alternatively in the form

$$\text{NOR}(\phi, \psi).$$

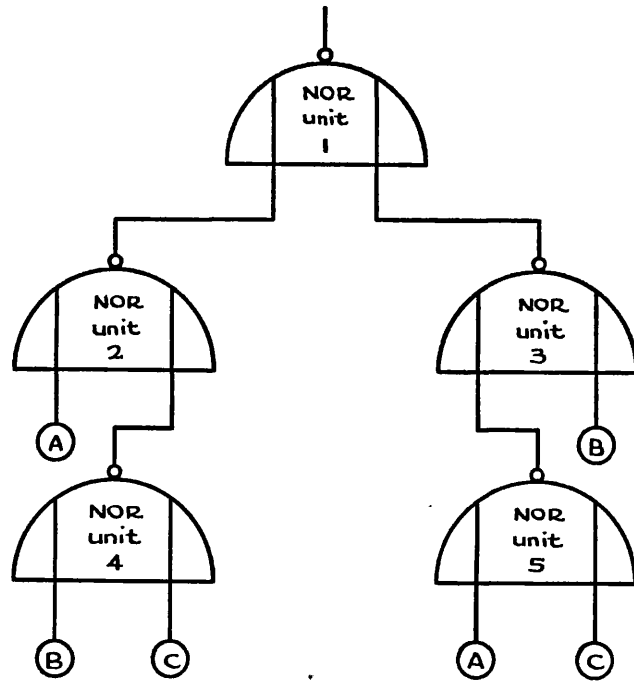


Fig. 1

The inputs to the last NOR unit must therefore be logical nets representing the functions ϕ and ψ . These functions are considered separately. Each section is therefore considered one at a time. The rows of the first section are expanded as in case (i) above. These rows are then deleted from the standard truth table which is then simplified as in stage 2, and the whole procedure is repeated producing a logical net for the function ϕ which is connected to the last NOR unit. The function ψ is considered in a similar manner. If it is not possible to split the rows of the simplified truth table into two sections, i.e. we have only one row left, one of the inputs to the last NOR unit is left blank and this single row considered as the other section and treated as before.

After repeating these procedures a sufficient number of times the whole function is represented as a net of NOR units.

The example given above is now considered in detail. After stage 1 and stage 2 have been performed for the first time the resulting truth table is

0 - 1
0 1 -
1 0 -
- 0 1

This shows that the function can be represented in the form

$$\overline{\bar{A} \cdot C \vee \bar{A} \cdot B \vee A \cdot \bar{B} \vee \bar{B} \cdot C}$$

Since no rows have only a 1 as entry NOR unit 1 as shown in Fig. 1 has no external inputs. The inputs are

Logical nets of NOR units

logical nets representing the functions ϕ and ψ where

$$\phi = \bar{A} \cdot C \vee \bar{A} \cdot B$$

$$\psi = A \cdot \bar{B} \vee \bar{B} \cdot C$$

The function ϕ is represented by the first section of the truth table which is

0 - 1
0 1 -

These rows are expanded to give the following rows

0 0 1
0 1 1
0 1 0

When these rows are deleted from the standard truth table and the resulting truth table simplified the result is

- 0 0
1 - -

This shows that NOR unit 2 has A as an input. The first row of this truth table is expanded and the rows deleted from the standard truth table. After simplification the result is

- - 1
- 1 -

This shows that NOR unit 4 has two external inputs, B and C , and that no more NOR units connect into NOR unit 4.

The function ψ is now considered. This is represented by the second section of the first truth table which is

1 0 -
- 0 1

When these rows are expanded and deleted from the standard truth table, after simplification the following truth table results:

0 - 0
- 1 -

This shows that NOR unit 3 has B as an input. The first row of the truth table is expanded and deleted from the standard truth table. After simplification the following truth table results:

- - 1
1 - -

This shows that NOR unit 5 has two external inputs A and C , and that no more NOR units connect into NOR unit 5. The net is therefore completed.

It is clearly not often practical to synthesise logical nets by performing these procedures manually. Using a computer, however, the synthesis can be performed very rapidly. The initial data for such a computation need only be a number specifying the number of inputs being considered (in the example this number is 3) and the numbers of the rows of the standard truth table corre-

sponding to the function being considered having value 1. This algorithm has been programmed and details of this are now given.

Programming the algorithm for computation

In order to compute a net it was found convenient to consider a maximum net in which two NOR units connect to each NOR unit in the net. This net is made sufficiently large that any possible net would be a proper part of it. Each NOR unit in the maximum net is numbered in a standard way. This serves as a useful framework. A cycle of the algorithm is performed for each NOR unit in the final net. After the completion of each cycle the computation moves on to consider a NOR unit with a higher number, or if this particular branch of the network has been completed it goes back to a lower number on the branch and then ascends to a higher number on another branch.

It is necessary to store certain numerical arrays. The main arrays are now described.

(i) An array consisting of 0s and 1s such as Table 1 where each row represents a successive number in binary form. For a computation of a net with n external inputs this array would have dimensions $n \times 2^n$. At each cycle in the algorithm certain rows of this table are 'deleted' by overwriting with other figures and the remainder of the table simplified using the three operations described.

(ii) Each NOR unit in the net can be regarded as the last NOR unit in some subnet performing a certain logical function. Therefore, associated with each NOR unit there must be a representation for this logical function. This is done by means of an array listing the numbers of the rows of the standard truth table which correspond to the function having value 1. Since the rows of the standard truth table are successive binary numbers the numbers of the rows can easily be computed. As there is a one-dimensional array associated with the number of each NOR unit the total array is two-dimensional.

(iii) There can be up to two external inputs to each NOR unit. These external inputs are numbered. Associating these two numbers with the number of each NOR unit gives a two-dimensional array.

(iv) One of the dimensions of the array (ii) will vary with the number of each NOR unit considered. Associating this dimension with the number of each NOR unit gives a one-dimensional array.

The program was written in FORTRAN IV and run on an IBM 360 computer with a core storage of 64K. It was found convenient to limit the program to synthesising nets with up to 8 external inputs, i.e. dealing with logical functions of up to 8 variables. Large amounts of core storage would have been used if all the arrays had been stored in core. Array (ii) was therefore stored by writing each row of it as a record on a magnetic disc. Since it was only necessary to read a record for each NOR unit and to write up to two records for each

Logical nets of NOR units

NOR unit the extra time taken was small. To deal with functions of many more than 8 variables would probably have necessitated also writing array (i) on disc.

After compilation the amount of time taken for execution of the program was quite short, not being more than ten minutes for a net with 8 external inputs, and

very much shorter for nets with a lesser number of external inputs.

Acknowledgement

The author would like to thank Mr. Brian Foster of IBM for help in writing the program.

Reference

QUINE, W. V. (1955). 'A way to simplify truth functions', *American Math. Monthly*, Vol. 62, No. 9, pp. 627-31.

ABSTRACT

A Formalisation of the Arithmetic of Transfinite Ordinals in a Multisuccessor Equation Calculus.

This thesis presents a syntactic development of the arithmetic of ordinal numbers less than ω^ω . This is done by means of an Equation calculus where all statements are given in the form of equations. There are rules of inference for deriving one equation from another. Certain functions, including a countably infinite number of successor functions S_μ , are taken as primitive. New functions are defined by substitution and primitive recursion starting with the primitive functions. Such definitions constitute some of the axioms of the system. The only other axioms are two rules concerning the combination of successor functions. Fundamental for this development is the axiom $S_\mu S_\nu = S_\mu$ for $\mu > \nu$.

In this system a multisuccessor arithmetic is developed in which it is possible to prove many of the familiar results concerning transfinite ordinal numbers. In particular the associativity of addition and multiplication as well as multiplication being left distributive with respect to addition are proved. It is shown that each ordinal in the system can be represented in Cantor's Normal Form. An ordinal subtraction is defined and a number of results involving this are proved. It is shown that this subtraction is, in a number of respects, an inverse to addition. In particular the key-equation $a + (b \div a) = b + (a \div b)$ is proved. As in Professor Goodstein's formalisation of the primitive recursive arithmetic of the natural numbers this equation is important as it allows a difference function $|a, b|$ to be defined for which a zero value is equivalent to equality of the arguments. Inequality relations are defined and some results concerning them proved.

In Chapter II it is shown, using a suitable coding, that this arithmetic can be reduced to the primitive recursive arithmetic of the natural numbers.

Chapter III gives a meta-proof of the consistency of the system.

Also submitted with this thesis is a paper "The Synthesis of Logical Nets consisting of NOR units" which is the result of work on a logical problem which was done at the same time as work for the thesis.