Notre Dame Journal of Formal Logic
Volume VI, Number 3, July 1965

THE SUBSTITUTION SCHEMA IN RECURSIVE ARITHMETIC

R. D. LEE

In his paper *Logic Free Formalisations of Recursive Arithmetic* [1] R. L. Goodstein presents a formalisation of primitive recursive arithmetic in which the only axioms are explicit and recursive function definitions, and the rules of inference are the schemata

$$(\mathbf{Sb_1}) \qquad \frac{F(x) = G(x)}{F(A) = G(A)}$$

$$(\mathbf{Sb_2}) \qquad \frac{A = B}{F(A) = F(B)}$$

$$(\mathbf{T}) \qquad A = B$$

$$\frac{A = C}{B = C}$$

where $F(x)$, $G(x)$ are recursive functions and A,B,C are recursive terms, and the primitive recursive uniqueness rule

$$(\mathbf{U}) \qquad \frac{F(Sx) = H(x,F(x))}{F(x) = H^x F(0)}$$

where the iterative function $H^x t$ is defined by the primitive recursion $H^0 t = t$, $H^{Sx} t = H(x,H^x t)$; in **U**, F may contain additional parameters.

In the same paper it is shown that the schema **U** may be replaced by

$$(\mathbf{E}) \qquad \frac{F(0) = 0 \quad F(Sx) = F(x)}{F(x) = 0}$$

if we take as axioms

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

and, in place of the introductory equations for the predecessor function,

$$(P) \qquad Sa \dot{-} Sb = a \dot{-} b$$

This system is referred to as $\mathbf{R_1}$.

Received November 6, 1964

The purpose of this paper is to present another formalisation, **R***, which also weakens **U** and yet avoids taking A as an axiom.

The rules of inference of **R*** are $\mathbf{Sb}_1$, $\mathbf{Sb}_2$, **T** and

$$(\mathbf{E}_1) \qquad \frac{F(Sx) = F(x)}{F(x) = F(0)}$$

$$(\mathbf{E}_3)^{\dagger} \qquad \frac{F(0) = G(0)}{\dfrac{F(Sx) = G(Sx)}{F(x) = G(x)}}$$

In place of the recursive definitions of addition we have the axioms

$$(A_1)\ a + 0 = a \qquad (A_2)\ a + (b + c) = (a + b) + c.$$

and for subtraction, we have the recursive definitions of predecessor and difference

$$(S_1)\ 0 \dot{-} 1 = 0;\ (S_2)\ Sa \dot{-} 1 = a;\ (S_3)\ a \dot{-} 0 = a;\ (S_4)\ a \dot{-} Sb = (a \dot{-} b) \dot{-} 1;$$

and the axiom

$$(S_5)\ (a \dot{-} b) \dot{-} 1 = (a \dot{-} 1) \dot{-} b$$

We have also the recursive definition of multiplication

$$(M_1)\ a \cdot 0 = 0 \qquad (M_2)\ a \cdot Sb = a \cdot b + a.$$

Exactly as in [1] we may prove the following results

$$(\mathbf{K}) \qquad \frac{A = B}{B = A}$$

and $Sa \dot{-} Sb = a \dot{-} b$, $a \dot{-} a = 0$, $0 \dot{-} a = 0$, $(a + b) \dot{-} b = a$, $(a + n) \dot{-} (b + n) = a \dot{-} b$, $n \dot{-} (b + n) = 0$.

We now derive the schema,

$$(\mathbf{U}_2) \qquad \frac{F(Sx) = SF(x)}{F(x) = F(0) + x}$$

(I am indebted to R. L. Goodstein for the following proof). Write $G(x) = F(0) + x$, then $G(Sx) = SG(x)$ and $G(0) = F(0)$. Using these two results and $F(Sx) = SF(x)$ we deduce $F(x) = G(x)$ for if $L(x) = F(x \dot{-} 1) + \{1 \dot{-} (1 \dot{-} x)\}$, then $L(0) = F(0)$ and $L(Sx) = SF(x) = F(Sx)$ so that, by $\mathbf{E}_6$, $L(x) = F(x)$. Therefore

$$F(x) = F(x \dot{-} 1) + \{1 \dot{-} (1 \dot{-} x)\}$$

Let $\phi(n,x)$ be defined by

$$\phi(0, x) = 0 \qquad \phi(Sn,x) = \{1 \dot{-} (1 \dot{-} (x \dot{-} n))\} + \phi(n,x)$$

then

$$\begin{aligned} F(x \dot{-} n) + \phi(n,x) &= \{F(x \dot{-} Sn) + [1 \dot{-} (1 \dot{-} (x \dot{-} n))]\} + \phi(n,x) \\ &= F(x \dot{-} Sn) + \phi(Sn,x) \end{aligned}$$

†Retaining the notation of [1].

Using $\mathbf{E}_1$

$$F(x \dot{-} n) + \phi(n, x) = F(x \dot{-} 0) + \phi(0, x) = F(x)$$

Whence taking $n = x$

$$F(0) + \phi(x,x) = F(x)$$

Similarly

$$G(0) + \phi(x,x) = G(x)$$

Hence

$$F(x) = G(x)$$
$$F(x) = F(0) + x.$$

We now use $\mathbf{U}_2$ to prove

$$0 + a = a.$$

Write $F(a) = a$, then $F(Sa) = SF(a)$. Hence using $\mathbf{U}_2$ and **K**, $0 + a = a$. Similarly using $\mathbf{U}_2$ we may prove $a + Sb = Sa + b$, $a + b = b + a$, $(a + b) \dot{-} a = b$ and exactly as in [1]

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

Now from $\mathbf{E}_1$, **E** follows immediately and hence we have postulated or derived all the axioms and rules of inference of system $\mathbf{R}_1$, given in [1]. Hence the sufficiency of **R*** for the construction of primitive recursive arithmetic follows from the sufficiency of $\mathbf{R}_1$, which is proved in [1]. In fact we can reduce the axiom system **R*** by postulating only certain *special* cases of $\mathbf{Sb}_2$. The special cases are

$(\mathbf{Sb}_{21})$ $\dfrac{A = B}{x+A = x+B}$ $\quad$ $(\mathbf{Sb}_{22})$ $\dfrac{A = B}{A \dot{-} x = B \dot{-} x}$ $\quad$ $(\mathbf{Sb}_{23})$ $\dfrac{A = B}{x \dot{-} A = x \dot{-} B}$

$(\mathbf{Sb}_{24})$ $\dfrac{A = B}{F(A) = F(B)}$

where in $\mathbf{Sb}_{24}$ $A = B$ is restricted to one of the initial equations $A_1, A_2, S_1, S_2, S_3, S_4, S_5, M_1, M_2$, or is any recursive or explicit function definition. For $F(0 \dot{-} Sx))$ $F((0 \dot{-} x) \dot{-} 1) = F((0 \dot{-} 1) \dot{-} x) = F(0 \dot{-} x)$ using $\mathbf{Sb}_{24}$ for the equations $a \dot{-} Sb = (a \dot{-} b) \dot{-} 1$, $(a \dot{-} b) \dot{-} 1 = (a \dot{-} 1) \dot{-} b$, $0 \dot{-} 1 = 0$, and **Sb**, to substitute 0 for x and x for b. Now writing $G(x) = F(0 \dot{-} x)$, we have proved $G(Sx) = G(x)$ and hence from $\mathbf{U}_1$, $G(x) = G(0)$
therefore

0.1 $\qquad F(0 \dot{-} x) = F(0)$

Similarly $F(Sx \dot{-} Sx) = F((Sx \dot{-} x) \dot{-} 1) = F((Sx \dot{-} 1) \dot{-} x) = F(x \dot{-} x)$ and hence by $\mathbf{U}_1$

0.2 $\qquad F(x \dot{-} x) = F(0).$

The proofs of the results in the first part of this paper up to and including the proof of $a + (b \dot{-} a) = b + (a \dot{-} b)$ use only the above special cases of $\mathbf{Sb}_2$ and 0.1 and 0.2.

Using $a + b = b + a$ and $\mathbf{Sb}_{21}$ we have

$$(\mathbf{Sb}_{25}) \qquad \frac{A = B}{A+x = B+x}$$

Following the proof, as given in [1], of the sufficiency of $\mathbf{R}_1$ (and therefore of $\mathbf{R}^*$, since in $\mathbf{R}^*$ we have derived or postulated all the axioms and rules of $\mathbf{R}_1$), we may derive the schema

$$(\mathbf{A}) \qquad \frac{A \dot{-} B = 0,\ B \dot{-} A = 0}{A = B}$$

The schema

$$(\mathbf{Sb}_{26}) \qquad \frac{A = B}{Ax = Bx}$$

is now proved as follows

Using $\mathbf{Sb}_{24}$, $A.Sx \dot{-} B.Sx = A.Sx \dot{-} B.x + B = A.x + A \dot{-} B.x + B$. Assuming $A = B$, from $\mathbf{Sb}_{21}$, $z + A = z + B$, and hence from $\mathbf{Sb}_1$, $B.x + A = B.x + B$. Therefore using $\mathbf{Sb}_{23}$, $z \dot{-} (B.x + B) = z \dot{-} (B.x + A)$ and hence from $\mathbf{Sb}_1$ $(A.x + A) \dot{-} (B.x + B) = (A.x + A) \dot{-} (B.x + A)$; but from a previous result $(A.x + A) \dot{-} (B.x + A) = A.x \dot{-} B.x$
Hence

$$A.Sx \dot{-} B.Sx = A.x \dot{-} B.x$$

Using $\mathbf{E}_1$,

$$A.x \dot{-} B.x = 0.$$

Similarly

$$B.x \dot{-} A.x = 0.$$

Hence, by **A**.

$$A.x = B.x.$$

Exactly as in [1], we may now prove $Sa.b = a.b + b$, $0.a = 0$ and $a.b = b.a$. The schema

$$(\mathbf{Sb}_{27}) \qquad \frac{A = B}{xA = xB}$$

follows from $a.b = b.a$ and $\mathbf{Sb}_{26}$.

Apart from the special cases of $\mathbf{Sb}_2$ which are axioms or have been derived the only application of $\mathbf{Sb}_2$ in the proof of the sufficiency of $\mathbf{R}^*$ occurs in the proof of the substitution theorem, in the form

$$\frac{x + (y \dot{-} x) = y + (x \dot{-} y)}{F(x + (y \dot{-} x)) = F(y + (x \dot{-} y))}$$

I shall give an alternative proof of the substitution theorem which avoids use of this result.

THE SUBSTITUTION THEOREM

$$x = y \rightarrow F(x) = F(y)$$

All primitive recursive functions can be obtained by substitution and recursion according to the schema $F(0) = 0\ F(Sx) = H(F(x))$, from the initial functions $u + v$, $u \dot{-} v$, $Rt(u)$, where $Rt(0) = 0$, $Rt(Sx) = Rt(x) + [1 \dot{-} p(x,Rt(x))]$ and $p(x,y) = (Sy)^2 \dot{-} Sx$.

It suffices therefore to prove that the substitution theorem holds for these initial functions and is preserved under substitution and the given recursion. From the original proof of the substitution theorem given in [1], we have

$$(1 \dot{-} |x,y|)F(x + (y \dot{-} x)) = (1 \dot{-} |x,y|)F(x)$$
$$(1 \dot{-} |x,y|)F(y + (x \dot{-} y)) = (1 \dot{-} |x,y|)F(y)$$

In the case of $F(z) = z + a$ we have

$$(1 \dot{-} |x,y|)((x + (y \dot{-} x)) + a) = (1 \dot{-} |x,y|)(x + a)$$
$$(1 \dot{-} |x,y|)((y + (x \dot{-} y)) + a) = (1 \dot{-} |x,y|)(y + a)$$

But from $\mathbf{Sb}_{25}$ and $x + (y \dot{-} x) = y + (x \dot{-} y)$, $[x + (y \dot{-} x)] + a = [y + (x \dot{-} y)] + a$ and hence from $\mathbf{Sb}_{27}$

$$(1 \dot{-} |x,y|)[(x + (y \dot{-} x)) + a] = (1 \dot{-} |x,y|)[(y + (x \dot{-} y)) + a]$$

Hence

$$(1 \dot{-} |x,y|)(x + a) = (1 \dot{-} |x,y|)(y + a)$$

Thus we have derived the substitution for the function $F(z) = z + a$.

In the way, using $\mathbf{Sb}_{21}$, $\mathbf{Sb}_{22}$, $\mathbf{Sb}_{23}$, $\mathbf{Sb}_{25}$, $\mathbf{Sb}_{27}$, we may obtain the substitution theorem for the initial functions $u + v$, $u \dot{-} v$, $u.v$.

In the following proof of the substitution theorem for the function $Rt(x)$, I shall use theorems of the proportional calculus, which may easily be proved by deriving their corresponding equations in recursive arithmetic. The theorems concerned are

(1) $(x = x') \rightarrow (Sx = Sx')$

(2) $(y = y') \rightarrow (Sy)^2 = (Sy')^2$

(3) $((x = x') \,\&\, (y = y')) \rightarrow (Sy)^2 \dot{-} Sx = (Sy')^2 \dot{-} Sx'$

(4) $(x=x') \,\&\, (Rt(x) = Rt(x')) \rightarrow p(x,Rt(x)) = p(x',Rt(x'))$

(5) $(x=x') \,\&\, (Rt(x) = Rt(x')) \rightarrow Rt(x) + (1 \dot{-} p(x,Rt(x))) = Rt(x') + (1 \dot{-} p(x',Rt(x')))$

(6) $(x=x') \,\&\, (Rt(x) = Rt(x')) \rightarrow Rt(Sx) = Rt(Sx')$

We now prove

$$((x = x') \rightarrow Rt(x) = Rt(x')) \rightarrow (Sx = Sx' \rightarrow Rt(Sx) = Rt(Sx'))$$

with a,b,c standing for $|x,x'|$ (and hence for $|Sx,Sx'|$, $|Rt(x), Rt(x')|$, $|Rt(Sx), Rt(x')|$ respectively), we require to prove

(7) $(1 \dot{-} (1 \dot{-} a)b)(1 \dot{-} a)c = 0$.

From (6)

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

so that

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

Hence

$$(1 \dot{-} a)c \dot{-} b\,(1 \dot{-} a)c = 0$$

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

(8) $$(1 \dot{-} a)c(1 \dot{-} b) = 0.$$

Hence

(9) $$\begin{aligned}(1 \dot{-} (1 \dot{-} a)b)\,(1 \dot{-} a)c &= (1 \dot{-} a)c \dot{-} (1 \dot{-} a)(1 \dot{-} a)bc \\ &= (1 \dot{-} a)c \dot{-} (1 \dot{-} a)bc \\ &= (1 \dot{-} a)c(1 \dot{-} b) \\ &= 0\end{aligned}$$

from (8). Therefore

(10) $$(x = x' \rightarrow Rt(x) = Rt(x')) \rightarrow (Sx = Sx' \rightarrow Rt(Sx) = Rt(Sx'))$$

Now define $P(x,x') = (1 \dot{-} |x,x'|)\,|\,Rt(x), Rt(x')|$
Then, from (9),

$$P(x,x') = 0 \rightarrow P(Sx, Sx') = 0.$$

But, from $\mathbf{E}_3$,

$$P(x,0) = (1 \dot{-} x)|Rt(x), Rt(0)| = 0.$$

Similarly

$$P(0,x') = 0.$$

Hence, by $\mathbf{I}_2$,

$$P(x,x') = 0.$$
$$(x = x') \rightarrow \{Rt(x) = Rtx'\}$$

We have now proved the substitution theorem for all the initial functions.

Now suppose the substitution theorem holds for the particular functions f,g, i.e.

(11) $$x = y \rightarrow f(x) = f(y)$$

and

(12) $$x = y \rightarrow g(x) = g(y).$$

From $\mathbf{Sb}_1$ and (11) we have

(13) $$g(x) = g(y) \rightarrow f(g(x)) = f(g(y)).$$

We now use the schema

(14) $$\begin{array}{l} p \to q \\ \underline{q \to r} \\ p \to r \end{array}$$

which may be proved by a consideration of the corresponding equations in recursive arithmetic.

Hence from (12), (13),

$$x = y \to f(g(x)) = f(g(y))$$

i.e. the substitution theorem is preserved under composition.

Now consider $\phi(x)$ defined by the recursion $\phi(0) = 0$, $\phi(Sx) = H(\phi(x))$ and suppose the substitution theorem holds for H.

Define $P(x,y) = (1 \dot{-} |x,y|)|\phi(x), \phi(y)|$. Then, using $\mathbf{E}_3$

(15) $$P(x,0) = (1 \dot{-} x)|\phi(x), \phi(0)| = 0$$

and

(16) $$P(0,Sy) = 0.$$

We now derive the result

$$(a = a') \to \{(b = b') \to (a = b \to a' = b')\}.$$

As we observed above

$$(1 \dot{-} |x,y|)F(x + (y \dot{-} x)) = (1 \dot{-} |x,y|)F(x)$$

and so with $F(x) = |x,t|$

$$(1 \dot{-} |x,y|)|x + (y \dot{-} x),t| = (1 \dot{-} |x,y|)|x,t|.$$

Similarly

$$(1 \dot{-} |x,y|)|y + (x \dot{-} y), t| = (1 \dot{-} |x,y|)|y,t|$$

Using $x + (y \dot{-} x) = y + (x \dot{-} y)$, and the given special cases of $\mathbf{Sb}_2$ we obtain

$$(1 \dot{-} |x,y|)|x + (y \dot{-} x), t| = (1 \dot{-} |x,y|)|y + (x \dot{-} y),t|.$$

Hence

(17) $$(1 \dot{-} |x,y|)|x,t| = (1 \dot{-} |x,y|)|y,t|$$

Now using (17) and rearranging factors

$$\begin{aligned}(1 \dot{-} |a,a'|)(1 \dot{-} |b,b'|)(1 \dot{-} |a,b|)|a',b'| &= (1 \dot{-} |b,b'|)(1 \dot{-} |a,a'|) \\ &\quad (1 \dot{-} |a,b|)|a,b| \\ &= 0.\end{aligned}$$

Hence

(18) $$a = a' \to \{b = b' \to (a = b \to a' = b')\}.$$

Replacing a,a',b,b' by $H(\phi(x)), \phi(Sx), H(\phi(y)), \phi(Sy)$ respectively

$$H(\phi(x)) = \phi(Sx) \to \{H(\phi(y)) = \phi(Sy) \to (H(\phi(x)) = H(\phi(y)) \to \phi(Sx) = \phi(Sy))\}$$

From the definition of ϕ, using modus ponens twice

$$H(\phi(x)) = H(\phi(y)) \rightarrow \phi(Sx) = \phi(Sy)$$

Using the substitution theorem for H,

$$\phi(x) = \phi(y) \rightarrow H(\phi(x)) = H(\phi(y))$$

and hence by schema (14)

(19) $\quad \phi(x) = \phi(y) \rightarrow \phi(Sx) = \phi(Sy).$

We now prove

(20) $\quad P(x,y) = 0 \rightarrow P(Sx,Sy) = 0.$

With a, b, c standing for $|x,y|$, $|\phi(x), \phi(y)|$, $|\phi(Sx), \phi(Sy)|$ respectively there is represented by the equation

(21) $\quad (1 \dot{-} (1 \dot{-} a)b)\,(1 \dot{-} a)c = 0$

With $f(a)$ standing for the left hand side, $f(Sa) = 0$ and $f(0) = (1 \dot{-} b)c = 0$ from (19) and hence, using E_3 $f(a) = 0$.

Now using I_2 with conditions satisfied by (15), (16), (20), we obtain

$$x = y \rightarrow \phi(x) = \phi(y)$$

Hence the substitution theorem is preserved under the given recursion and thus it holds for all recursive functions.

My thanks are due to Professor R. L. Goodstein for help and encouragement in the preparation of this paper.

REFERENCE

[1] R. L. Goodstein, Logic-free formalisation of recursive arithmetic. *Math. Scand*, 2(1954). 247-261.

University of Leicester
Leicester, England