TSUKUBA J. MATH.
Vol. 2 (1978). 69–73

# A NOTE ON A FORMALIZED ARITHMETIC WITH FUNCTION SYMBOLS $'$ AND $+$.

By

Tsuyoshi YUKAMI

## Introduction.

Let $\mathfrak{L}_0$ be the first order language with function symbols $'$, $+$ and the equality symbol $=$. By $\mathfrak{L}$ we denote the first order language obtained from $\mathfrak{L}_0$ by adding a ternary predicate symbol $P$. The theory in $\mathfrak{L}$ with the following axioms and axiom schemata is signified by $\mathfrak{N}$.

(N- 1) $\forall x\neg(x'=0)$.

(N- 2) $\forall x\forall y(x'=y'\supset x=y)$.

(N- 3) $\forall x(x+0=x)$.

(N- 4) $\forall y\forall y(x+y'=(x+y)')$.

(N- 5) $\forall xP(x, 0, 0)$.

(N- 6) $\forall x\forall y\forall z\{P(x, y, z)\supset P(x, y', z+x)\}$.

(N- 7) $\forall x\forall y\forall z\forall w\{(P(x, y, z)\wedge P(x, y, w))\supset z=w\}$.

(N- 8) $\forall x(x=x)$.

(N- 9) $\forall x\forall y\{x=y\supset(\mathfrak{A}(x)\supset\mathfrak{A}(y))\}$.

(N-10) $\{\mathfrak{A}(0)\wedge\forall x((\mathfrak{A}(x)\supset\mathfrak{A}(x'))\}\supset\forall x\mathfrak{A}(x)$.

(N-11) $s=t$, where $s=t$ is valid.

For a term $t$, $\mathrm{b}(t)$ means the number of occurrences of bound varibles in $t$. For a formula $\mathfrak{A}$, $\mathrm{b}(\mathfrak{A})$ is defined inductively as follows. 1. $\mathrm{b}(r=s)=\max(\mathrm{b}(r), \mathrm{b}(s))$. 2. $\mathrm{b}(P(r, s, t))=\max(\mathrm{b}(r), \mathrm{b}(s), \mathrm{b}(t))$. 3. $\mathrm{b}(\neg\mathfrak{A})=\mathrm{b}(\mathfrak{A})$. 4. $\mathrm{b}(\mathfrak{A}\wedge\mathfrak{B})=\mathrm{b}(\mathfrak{A}\vee\mathfrak{B})=\max(\mathrm{b}(\mathfrak{A}), \mathrm{b}(\mathfrak{B}))$. 5. $\mathrm{b}(\forall x\mathfrak{A})=\mathrm{b}(\exists x\mathfrak{A})=\mathrm{b}(\mathfrak{A})$.

In [3] we proved that:

*For any formula $\mathfrak{A}(a)$ of $\mathfrak{L}$; if there is a number $m$ such that, for any natural number $n$, there exists a proof $\mathfrak{P}$ of $\mathfrak{A}(\bar{n})$ in $\mathfrak{N}$ with the following properties (1) and (2), then $\forall x\mathfrak{A}(x)$ is provable in $\mathfrak{N}$.*

*(1) The length of $\mathfrak{P}$ is less than $m$.*

*(2) For any induction schema $\mathfrak{B}$ in $\mathfrak{P}$ which is not a formula of $\mathfrak{L}_0$, $\mathrm{b}(\mathfrak{B})\leq m$.*

The purpose of this paper is to prove the following theorem.

THEOREM. *There are a formula $\mathfrak{A}(a)$ and a natural number $M$ such that: (a)*

Received January 28, 1978

$\forall x\mathfrak{A}(x)$ *is not provable in* $\mathfrak{N}$. (*b*) *For any natural number* $n$, $\mathfrak{A}(\bar{n})$ *is provable in* $\mathfrak{N}$ *with length* $\leq M$.

We devote § 2 to proving the theorem. In § 1 we prepare for the proof.

The author wishes to thank Dr. T. Uesu and Dr. M. Fukuyama, on whose advices the author could simplify both the form of the formula $\mathfrak{A}(a)$ mentioned in the theorem and the related arguments.

§ 2. **Preparations for § 2.**

LEMMA 1. *If* $m\cdot n=k$, *then* $P(\bar{m}, \bar{n}, \bar{k})$ *is provable in* $\mathfrak{N}$ *with length 13.*

PROOF. Using (N-5) and (N-6), we can prove (1-1) and (1-2) with length $\leq 5$.

(1- 1) $P(\bar{m}, 0, 0)$.

(1- 2) $P(\bar{m}, a, \overbrace{a+\cdots+a}^{m})\supset P(\bar{m}, a', \overbrace{a+\cdots+a}^{m}+\bar{m})$.

By (N-11), (1-3), (1-4) and (1-5) are axioms.

(1- 3) $0=\overbrace{0+\cdots+0}^{m}$.

(1- 4) $\overbrace{a+\cdots+a}^{m}+\bar{m}=\overbrace{a'+\cdots+a'}^{m}$.

(1- 5) $\overbrace{\bar{n}+\cdots+\bar{n}}^{m}=\bar{k}$.

Using equality axioms with (1-1), (1-2), (1-3) and (1-4), we can deduce (1-6) with length 10.

(1- 6) $P(\bar{m}, 0, 0+\cdots+0)\land\forall x(P(\bar{m}, x, x+\cdots+x)\supset P(\bar{m},x', x'+\cdots+x'))$.

From (1-6) with an iduction axiom, (1-7) is provable with lenght 11.

(1- 7) $\forall xP(\bar{m}, x, x+\cdots+x)$.

Hence we can deduce (1-8) with lenght 13 from (1-5) and (1-7).

(1- 8) $P(\bar{m}, \bar{n}, \bar{k})$.

LEMMA 2. *If* $m+n=k$ *and* $n\neq 0$, *then* $\bar{k}\neq\bar{m}$ *is provable in* $\mathfrak{N}$ *with length* 25.

PROOF. By (N-11), (1-9) is an axiom.

(1- 9) $\bar{k}=\bar{m}+\bar{n}$.

The following formula is provable with length 17.

(1-10) $\forall x\forall y(x+y=x\supset y=0)$.

We can deduce (1-11) with length 21 from (1-9) and (1-10) with equality axioms.

(1-11) $\bar{k}=\bar{m}\supset\bar{n}=0$.

Hence (1-12) is provable with length 25 from (1-11) with the axiom (N-1). (Note that $n\neq 0$.)

(1-12) $\neg(\bar{k}=\bar{m})$.

We define *E-formulas* inductively in the following manner. 1. Formulas of the forms $r=s$, $r\neq s$ and $P(r, s, t)$ are E-formulas. 2. If $\mathfrak{A}$ and $\mathfrak{B}$ are E-formulas, then so are $\mathfrak{A}\wedge\mathfrak{B}$ and $\mathfrak{A}\vee\mathfrak{B}$. 3. If $\mathfrak{A}$ is an E-formula, then so is $\exists x\mathfrak{A}$.

LEMMA 3. *Let $\mathfrak{A}(a_1, \cdots, a_\nu)$ be an E-formula. Assume that every free variable of $\mathfrak{A}(a_1, \cdots, a_\nu)$ is among $a_1, \cdots, a_\nu$. Then there is a natural number M such that: for any natural numbers $n_1, \cdots, n_\nu$, if $\mathfrak{A}(\bar{n}_1, \cdots, \bar{n}_\nu)$ is true, then $\mathfrak{A}(\bar{n}_1, \cdots, \bar{n}_\nu)$ is provable in $\mathfrak{N}$ with length $\leq M$.*

Lemma 3 is easily proved by the induction corresponding to the inductive difinition of E-formulas. We use Lemma 1 and Lemma 2 in the basis step of the proof.

Let $\mathfrak{F}(a,b,c)$ be

$$\exists x[P(b+c, b+c+1, x)\wedge a+a=x+c+c].$$

By formalizing the ordinary informal proof that the function

$$J(x, y) = \frac{(x+y)(x+y+1)}{2}+y$$

is a one-to-one function from $\omega^2$ onto $\omega$, we can prove

(1-13) $\mathfrak{F}(a, b, c)\wedge\mathfrak{F}(a, d, e)\rightarrow b=d\wedge c=e$,

(1-14) $\forall x\forall y\exists z\mathfrak{F}(z, x, y)$

and

(1-15) $\forall x\exists y\exists z\mathfrak{F}(x, y, z)$.

We define E-formulas $\mathfrak{F}_\nu(a, b_1, \cdots, b_{\nu+1})$ by induction on $\nu$: 1. $\mathfrak{F}_0(a, b_1)=a=b_1$. 2. $\mathfrak{F}_1(a, b_1, b_2)=\mathfrak{F}(a, b_1, b_2)$. 3. $\mathfrak{F}_{\nu+1}(a, b_1, b_2, \cdots, b_{\nu+1}, b_{\nu+2})=\exists x[\mathfrak{F}_\nu(a, b_1, \cdots, b_\nu, x)\wedge \mathfrak{F}(x, b_{\nu+1}, b_{\nu+2})]$.

Using (1-13), (1-14) and (1-15), we can prove by induction on $\nu$,

(1-16) $\mathfrak{F}_\nu(a, b_1, \cdots, b_{\nu+1})\wedge\mathfrak{F}_\nu(a, c_1, \cdots, c_{\nu+1})\rightarrow b_1=c_1\wedge\cdots\wedge b_{\nu+1}=c_{\nu+1}$,

(1-17) $\forall x_1\cdots\forall x_{\nu+1}\exists y\mathfrak{F}_\nu(y, x_1, \cdots, x_{\nu+1})$

and

(1-18) $\forall x\exists y_1\cdots\exists y_{\nu+1}\mathfrak{F}_\nu(x, y_1, \cdots, y_{\nu+1})$.

REMARK. In connection with the definition of E-formulas, we state the following lemma. But it is superfluous for our purpose. It is proved by formalizing the proof of the theorem 1 in §6 of the chapter 2 of [2].

LEMMA 4. *Let $\mathfrak{S}(a, b, c)$ be the standard formula which expresses the primitive recursive predicate '$a=b^c$'. There is an E-formula $\mathfrak{H}(a, b, c)$ such that $\mathfrak{S}(a, b, c)\equiv\mathfrak{H}(a, b, c)$ is provable in $\mathfrak{N}$.*

## §2. Proof of the theorem.

2.1 Let $T(x)$ be a recursively enumerable predicate which is not recursive. By [1], there are polynomials $f(x, y_1, \cdots, y_\nu)$ and $g(x, y_1, \cdots, y_\nu)$ with natural number coefficients such that:

(*) $T(x)\leftrightarrow\forall y_1\cdots\forall y_\nu(f(x, y_1, \cdots, y_\nu)=g(x, y_1, \cdots, y_\nu))$.

We can find an E-formula $\mathfrak{T}(x, y_1, \cdots, y_\nu)$ which expresses naturally $f(x, y_1,\cdots,y_\nu)$

$=g(x, y_1, \cdots, y_\nu)$. There is a primitive recursive function $\phi(x)$ such that

$$\phi(n) = \ulcorner \exists y_1 \cdots \exists y_\nu \mathfrak{T}(\bar{n}, y_1, \cdots, y_\nu) \urcorner.$$

2.2 To deduce a contradiction, we assume that, for any natural number $n$, $\exists y_1 \cdots \exists y_\nu \mathfrak{T}(\bar{n}, y_1, \cdots, y_\nu)$ or its negation is provable in $\mathfrak{N}$.

Then

(**) $\bigwedge x \bigvee y \{[\mathrm{Proof}_{\mathfrak{N}}((y)_0, \phi(x)) \ \& \ (y)_1 = 0]$ or $[\mathrm{Proof}_{\mathfrak{N}}((y)_0, Neg(\phi(x))) \ \& \ (y)_1 = 1]\}$,

where $\mathrm{Proof}_{\mathfrak{N}}$ is the proof predicate for $\mathfrak{N}$, and $Neg$ is a function such that $Neg(\ulcorner \mathfrak{A} \urcorner) = \ulcorner \neg \mathfrak{A} \urcorner$ for any formula $\mathfrak{A}$.

We define

$$\psi(n) = (\mu y \{[\mathrm{Proof}_{\mathfrak{N}}((y)_0, \phi(n)) \ \& \ (y)_1 = 0] \text{ or } [\mathrm{Proof}_{\mathfrak{N}}((y)_0, Neg(\phi(n))) \ \& \ (y)_1 = 1]\})_1.$$

From (**) and recursiveness of predicate $Proof_{\mathfrak{N}}$ and function $Neg$, we can conclude that:

(***) $\psi(n)$ is recursive.

Furthermore we can conclude (****) by the following arguments (a) and (b).

(****) $\bigwedge x (T(x) \leftrightarrow \psi(x) = 0)$.

(a) Assume $T(n)$. By (*), $\exists y_1 \cdots \exists y_\nu \mathfrak{T}(\bar{n}, y_1, \cdots, y_\nu)$ is true.
Because $\mathfrak{T}(\bar{n}, y_1, \cdots, y_\nu)$ is an E-formula,

(*****) $\bigvee y \, \mathrm{Proof}_{\mathfrak{N}}(y, \phi(n))$.

From the consistency of $\mathfrak{N}$.

(******) $\sim \bigvee y \, \mathrm{Proof}_{\mathfrak{N}}(y, Neg(\phi(n)))$.

We can obtain the conclusion that $\psi(n) = 0$ from (*****), (******) and the difinition of $\psi(n)$.

(b) Conversely assume $\psi(n) = 0$. Then, by the difinition of $\psi(n)$, $\bigvee y \, \mathrm{Proof}_{\mathfrak{N}}(y, \phi(n))$. Because every provable formula in $\mathfrak{N}$ is valid, $\exists y_1 \cdots \exists y_\nu \mathfrak{T}(\bar{n}, y_1, \cdots, y_\nu)$ is true. Hence, by (*), $T(n)$.

We can deduce a contradiction from (***), (****) and the hypothesis that $T(x)$ is not recursive. Hence we can obtain the conclusion that:

(*******) For some $m$, $\exists y_1 \cdots \exists y_\nu \mathfrak{T}(\bar{m}, y_1, \cdots, y_\nu)$ and its negation are not provable in $\mathfrak{N}$. Furthermore $\exists y_1 \cdots \exists y_\nu \mathfrak{T}(\bar{m}, y_1, \cdots, y_\nu)$ is false, because $\exists y_1 \cdots \exists y_\nu \mathfrak{T}(\bar{m}, y_1, \cdots, y_\nu)$ is an E-formula.

2.3 We can find an E-formula $\mathfrak{U}(y_1, \cdots, y_\nu)$ which expresses naturally $f(m, y_1, \cdots, y_\nu) \neq g(m, y_1, \cdots, y_\nu)$ and for which

(2-1) $\mathfrak{U}(y_1, \cdots, y_\nu) \equiv \neg \mathfrak{T}(\bar{m}, y_1, \cdots, y_\nu)$

is provable.

By $\mathfrak{A}(a)$, we denote the following formula:

$$\exists y_1 \cdots \exists y_\nu \{\mathfrak{F}_{\nu-1}(a, y_1, \cdots, y_\nu) \wedge \mathfrak{U}(y_1, \cdots, y_\nu)\}.$$

Note that $\mathfrak{A}(a)$ is an E-formula. In the remainder of this paper, we shall prove that $\mathfrak{A}(a)$ has the two properties in the theorem.

2.3.1 Because of (*******) with (1-18) and (2-1), $\mathfrak{A}(\bar{n})$ is true for any natural number $n$. Hence, by Lemma 3, we can conclude that: there is a natural number $M$ such that, for any natural number $n$, $\mathfrak{A}(\bar{n})$ is provable with length $\leq M$.

2.3.2 Using (1-16), (1-17) and (1-18), we can prove

(2-2) $\forall x \mathfrak{A}(x) \supset \forall y_1 \cdots \forall y_\nu \mathfrak{U}(y_1, \cdots, y_\nu)$.

From (2-1) and (2-2), we can deduce

(2-3) $\forall x \mathfrak{A}(x) \supset \neg \exists y_1 \cdots \exists y_\nu \mathfrak{T}(\bar{m}, y_1, \cdots, y_\nu)$.

Hence, from (*******) and (2-3), we can conclude that $\forall x \mathfrak{A}(x)$ is not provable.

## References


[1] Ju. V. Matijasevič, Enumerable sets are diophantine, Soviet Math. Dokl., 11 (1970), 354-358.

[2] G. Takeuti, The mathematical logic-the word problem (Japanese), Tokyo, 1973.

[3] T. Yukami, A theorem on the formalized aritmetic with function symbols ′ and +, this journal, **1** (1977), 195-211.



Institute of Mathematics
The University of Tsukuba
Ibaraki, 300-31, Japan