Preprint, Institute of Mathematics, AS CR, Prague. 2007-12-15

Theories very close to PA where Kreisel's Conjecture is false.

Pavel Hrubeš*

June 14, 2006

Abstract

We give four examples of theories in which Kreisel Conjecture is false: 1) the theory $PA(-)$ obtained by adding a function symbol minus, '$-$', to the language of PA, and the axiom $\forall x \forall y \forall z\ (x - y = z) \equiv (x = y + z \vee (x < y \wedge z = 0))$; 2) the theory $\mathcal{Z}$ of integers; 3) the theory $PA(q)$ obtained by adding a function symbol q (of arity ≥ 1) to PA, assuming nothing about q; 4) the theory $PA(N)$ containing a unary predicate $N(x)$ meaning *'x is a natural number'*. In Section 6 we suggest a counterexample to the so called Sharpened Kreisel Conjecture.

1 Introduction.

Kreisel's Conjecture (KC) is the following assertion (as quoted by Friedman [1975]):

Let $\forall n\ \psi(n)$ be a universal sentence of PA. Then if there is some k s.t. for every n $\psi(\overline{n})$ is provable in PA in k steps then $\forall n\ \psi(n)$ is provable in PA.

Similarly, we could formulate KC for any formal system S related to arithmetic. The peculiarity of KC lies in the fact that it depends not so much on the logical strength of S, i.e., on how many propositions are provable in S, but on the length of proofs in S and, in particular, on the structure of terms in S. So far, it has been shown that for some theories obtained by weakening[1] of PA, KC is true. Parikh[1978] has shown that KC is true in the theory obtained by replacing the binary function symbols for multiplication and addition by ternary predicates in PA; the result has been extended by Miyatake[1980] to the case where also $+$ is present as a function symbol. Baaz and Pudlák[1993] proved KC for the theory $I\Sigma_1$.[2] Krajíček and Pudlák[1988] proved that KC holds for any finitely axiomatised theory. On the other hand, we can find trivial examples of theories where KC is false, e.g., one obtained by adding every instance of an undecidable Π_1-sentence as an axiom. Yukami[1978] has shown, using the Matyasievich theorem, that KC is false when we add to PA all the true equations of the form $\overline{n} \cdot \overline{m} = \overline{n \cdot m}$. The theories that we are going to present will be more

* *Mathematical Institute, Academy of Sciences of the Czech Republic, Prague, Czech republic*

[1] In the sense of having longer proofs.

[2] However, only with the scheme of minimum and the axioms of identity.

natural: the system $PA(-)$ differs from PA only in containing an additional function symbol, minus, which denotes a function definable by a formula already in PA. The theory $\mathcal{Z}$ has exactly the same language as PA but it is a natural axiomatisation of the theory of integers. We will show that in those systems we can find k s.t. every sentence of the form $\overline{n} \cdot \overline{m} = \overline{n \cdot m}$ is provable in k steps, which implies that KC is false (as follows from Yukami's argument). The systems $PA(q)$ and $PA(N)$ will be obtained by weakening the systems $PA(-)$ and $\mathcal{Z}$ respectively. Here, KC will be disproved without determining such an upper bound for multiplication, i.e., without bounding proof lengths of the equation $\overline{n} \cdot \overline{m} = \overline{n \cdot m}$.

I thank my supervisor Pavel Pudlák for his help and patience.

General notions:

1) PA will denote the usual Peano arithmetic.

2) Let T be a theory, ψ a formula and k a number. Then

$$T \vdash_k \psi$$

states that ψ is provable in T in k steps.

3) We assume that PA is formalised using *the schemes of identity*, i.e., infinitely many axioms

$$x = y \rightarrow t(z/x) = t(z/y)$$

for every term of PA and

$$x = y \rightarrow (\psi(z/x) \equiv \psi(z/y))$$

for every formula of PA.

On the other hand, for the purposes of our construction it would be sufficient to axiomatise identity with the finite list of axioms of the type $x = y \rightarrow S(x) = S(y)$, and similarly for the other function and predicate symbols. The reason is that an important fragment of the identity schema is derivable from the scheme of induction in a fixed number of steps. The scheme of induction over a language L is the scheme

$$IND: \qquad (\psi(z/0) \wedge \forall x \psi(z/x) \rightarrow \psi(z/S(x))) \rightarrow \forall z \psi(z),$$

where ψ is a formula of the language L. The weak identity scheme over L will be the scheme

$$WID: \qquad x = 0 \rightarrow t(z/x) = t(z/0),$$
$$x = 0 \rightarrow \psi(z/x) \equiv \psi(z/0),$$

where t and ψ is a term resp. a formula of L.

Observation: *Let L be a language containing the language of PA. There is $k \in \omega$ s.t. every instance of WID over L is provable in k steps in PA with induction over L.*

`Proof.` The formula $\psi(x) := x = 0 \rightarrow t(x) = t(0)$ is proved by induction. If $x = 0$, $\psi(0)$ is $0 = 0 \rightarrow t(0) = t(0)$. This is provable in a bounded number of

steps, since $t(0) = t(0)$ is obtained by substitution to the formula $x = x$. Since $PA \vdash \neg(S(x) = 0)$, then $\psi(S(x))$ is provable in a bounded number of steps, and hence also $\psi(x) \to \psi(S(x))$. QED

In order to obtain the full identity scheme, it would be sufficient to replace induction by a stronger version

$$IND' : \qquad (\psi(z,z) \wedge \forall x \geq z\ \psi(z,x) \to \psi(z,S(x))) \to \forall x \geq z \psi(z,x).$$

However, it can be shown that the constructions of this paper require only the weak scheme WID.

4) We shall be dealing with terms recursively defined by a given rule. Those terms will be denoted Q^n, $Q^n_m, \ldots$ where the indices range over natural numbers. For example, $S^n(0)$ will denote the term $S(S(\ldots S(0)))$ where the S's occur n times (this term will be also denoted by $\overline{n}$). If $\psi(Q^n)$ is a formula containing the depicted recursive term then

$$T \vdash_b \psi(Q^n)$$

is an abbreviation for the statement *'there exists k such that for every n, $T \vdash_k \psi(Q^n)$'*. Similarly for a greater number of terms possibly with a greater number of indices. As an example we state the following important lemma (see Yukami [1984]):

Lemma 1 *$PA \vdash_b S^n(y) + x = S^n(y + x)$ and hence $PA \vdash_b x + S^n(y) = S^n(x + y)$.*

Proof. Let $\psi(y,x)$ denote the formula $S^n(y) + x = S^n(y + x)$. The proof is carried in PA by induction. If $x = 0$ then $\psi(y,0) = S^n(y) + 0 = S^n(y + 0)$ and clearly $PA \vdash_b \psi(y,0)$. It can also be shown that $PA \vdash_b \psi(y,x) \to \psi(y,S(x))$. For assume $\psi(y,x)$. Then we have $S^n(y) + S(x) = S(S^n(y) + x) = S(S^n(y + x)) = S^n(S(y + x)) = S^n(y + S(x))$ and hence also $\psi(y,S(x))$. QED

The following can be obtained from Yukami [1978] and so we just sketch the proof:

Theorem 2 *Let T be a consistent recursively axiomatised theory which contains the language of PA and extends PA. Assume that there is $k \in \omega$ s.t. for every $n, m \in \omega$ the formula*

$$\overline{n} \cdot \overline{m} = \overline{n \cdot m}$$

is provable in T in k steps. Then KC is false in T.

Proof. By the Matyasievich theorem we can find terms of PA, $t_1(x, y_1, \ldots y_l)$ and $t_2(x, y_1, \ldots y_l)$ s.t. the formula

$$\psi(x) := \forall x \exists y_1, \ldots \exists y_l\ t_1(x, y_1, \ldots y_l) = t_1(x, y_1, \ldots y_l)$$

is true and undecidable in T. From Lemma 1 every equation of the form $\overline{n} + \overline{m} = \overline{n + m}$ is provable in a bounded number of steps. This, together with the assumption of the theorem, gives an upper bound for the proofs of the instances $\psi(\overline{n})$. QED

2 The theory $PA(-)$

The theory $PA(-)$ is obtained by adding to PA a new binary function symbol '$-$' and the axiom

$$\forall x \forall y \forall z \ (x - y = z) \equiv (x = y + z \vee (x < y \wedge z = 0)),$$

and extending the scheme of induction to the language of $PA(-)$. We are going to prove the following theorem:

Theorem 3 *There exists a $k \in \omega$ such that for every n, m $PA(-) \vdash_k S^n(0) \cdot S^m(0) = S^{n \cdot m}(0)$, or shortly*

$$PA(-) \vdash_b S^n(0) \cdot S^m(0) = S^{n \cdot m}(0)$$

Corollary *There is a number k and a formula $\psi(x)$ in the language of PA such that for every n $PA(-) \vdash_k \psi(S^n(0))$ but $PA(-) \nvdash \forall x \ \psi(x)$.*

The point of the construction is the following. For a large term T we are sometimes able to decide in a small number of steps whether it is equal to zero or one, as will be seen below. For example, let $T(z)$ denote the term

$$(\ldots((z \cdot \overline{1}) \cdot \overline{1})\ldots) \cdot \overline{1}).$$

Then we can prove the following propositions in a bounded number of steps: $z = 0 \equiv T(z) = 0$, $z = 1 \equiv T(z) = 1$.[3] The information whether a term equals zero or not does not seem very useful. It may become so if we have a term $q(x, y)$ s.t. $q(x, y) = 0$ iff $x \neq y$. For then if we show that $q(t_1, t_2) \neq 0$, in a small number of steps, then we also have $t_1 = t_2$ in a small number of steps. Minus, as introduced here, enables us to find a term with such a property.

Let the expression $t_1 \triangle t_2$ be an abbreviation for $((t_1 - t_2) + (t_2 - t_1))$. We observe the following:

Lemma 4 *The following is provable in $PA(-)$:*

1. $(x + z) \triangle (y + z) = x \triangle y$,
2. $(x \triangle y = 0) \equiv (x = y)$,
3. $(\overline{1} - (x \triangle y) = 0) \equiv (x \neq y)$.

Let $T^n_m(x)$ denote the term

$$S^m(0) \cdot S^n(x) \triangle S^{n \cdot m}(S^m(0) \cdot x).$$

We will show that $PA(-) \vdash_b \overline{1} - T^n_m(0) \neq 0$, which immediately implies $PA(-) \vdash_b S^m(0) \cdot S^n(0) = S^{n \cdot m}(0)$.

[3] However, in PA we are unable to prove even $z > 2 \to T(z) > 2$, or even $\forall z T(z) = z$ in a bounded number of steps. In $PA(-)$ this becomes easily provable.

Definition 1 *1. Let t, t_1, t_2 be terms. Then $t[t_1/t_2]$ will denote the term obtained by replacing all the occurrences of t_1 in t by t_2.*

2. We shall write $t_1 \sim t_2$, if the terms t_1 and t_2 are identical.

Lemma 5 *1. $PA(-) \vdash_b S^m(0) \cdot S(x) = S^m(S^m(0) \cdot x)$.*

2. $T^n_m(S(x))[S^m(0) \cdot S(x)/S^m(S^m(0) \cdot x)] \sim T^{n+1}_m(x)$, for every n.

3. $PA(-) \vdash_b \forall x\, T^n_m(x) = T^n_m(0)$ and hence $PA(-) \vdash_b T^n_m(0) \neq 0 \to \forall x T^n_m(x) \neq 0$.

`Proof.` 1 With the use of Lemma 1 we obtain $S^m(0) \cdot S(x) = S^m(0) \cdot x + S^m(0) = S^m(S^m(0) \cdot x + 0) = S^m(S^m(0) \cdot x)$.

2 By inspection.

3 It is sufficient to prove $T^n_m(S(x)) = T^n_m(x)$ in a bounded numbers of steps, the statement then follows by induction. The following equivalences are proved in a bounded number of steps by the use of Lemma 1 and the statement 1.

$$\begin{aligned}
T^n_m(S(x)) = \quad & S^m(0) \cdot S^n(S(x)) && \triangle \quad S^{n\cdot m}(S^m(0) \cdot S(x)) \\
= \quad & S^m(0) \cdot S(S^n(x)) && \triangle \quad S^{n\cdot m}(S^m(S^m(0) \cdot x)) \\
= \quad & (S^m(0) \cdot S^n(x) + S^m(0)) && \triangle \quad S^{n\cdot m}(S^m(S^m(0) \cdot x)) \\
= \quad & (S^m(0) \cdot S^n(x) + S^m(0)) && \triangle \quad S^{n\cdot m}(S^m(S^m(0) \cdot x) + 0) \\
= \quad & (S^m(0) \cdot S^n(x) + S^m(0)) && \triangle \quad (S^{n\cdot m}(S^m(0) \cdot x) + S^m(0))
\end{aligned}$$

By Lemma 4 part 1 we conclude

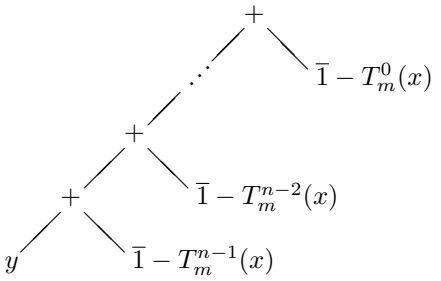
$$T^n_m(S(x)) \quad = \quad S^n(x) \cdot S^m(0) \triangle S^{n\cdot m}(S^m(0) \cdot x)$$

`QED`

Lemma 6 *Let t, t_1, t_2 be terms. Then the implication $t_1 = t_2 \to t = t[t_1/t_2]$ is provable in $PA(-)$ in three steps.*

`Proof.` Let z be a variable not occurring in t and let $t' := t[t_1/z]$. Let x_1, x_2 be variables not occurring in t'. The implication $x_1 = x_2 \to t'[z/x_1] = t'[z/x_2]$ is an axiom of identity. Applying substitutions x_1/t_1 and x_2/t_2 we obtain $t_1 = t_2 \to t'[z/t_1] = t'[z/t_2]$. But $t'(z/t_1) \sim t$ and $t'(z/t_2) \sim t[t_1/t_2]$. `QED`

Let $Q^n_m(y, x)$ denote the term



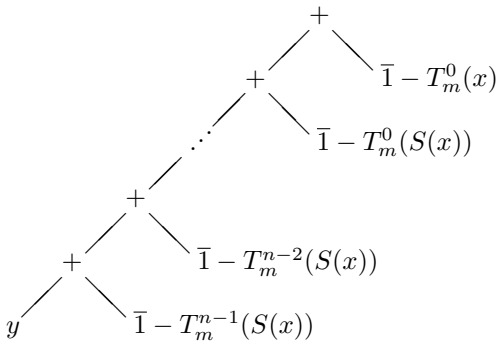
Lemma 7 *$PA(-) \vdash_b Q^n_m(y + (\overline{1} - T^n_m(x)), x) = Q^n_m(y, S(x)) + (\overline{1} - T^0_m)$ and hence $PA(-) \vdash_b Q^n_m(y + (\overline{1} - T^n_m(x)), x) = Q^n_m(y, S(x)) + \overline{1}$*

`Proof.` Let t_1 be the term $S^m(0) \cdot S(x)$ and t_2 be the term $S^m(S^m(0) \cdot x)$. Let us show that

$$(Q^n_m(y, S(x)) + (\overline{1} - T^0_m))[t_1/t_2] \ \sim \ Q^n_m(y + (\overline{1} - T^n_m(x)), x).$$

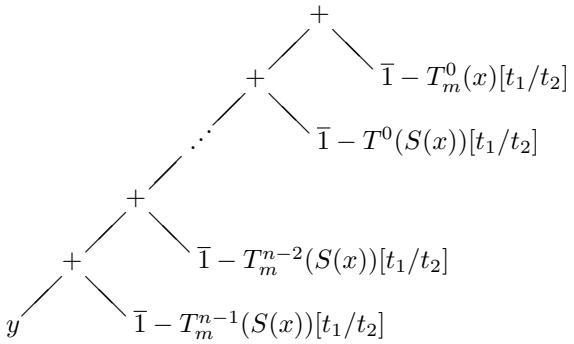
We have

$Q^n_m(y, S(x)) + (\overline{1} - T^0_m)$ $\sim$



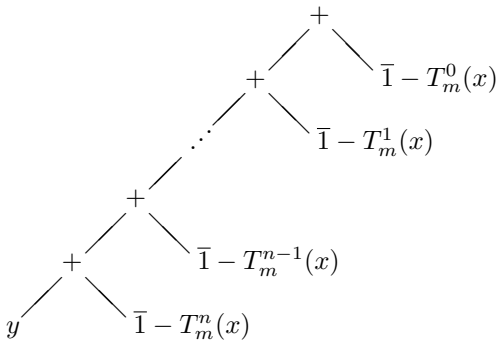
Hence

$(Q^n_m(y, S(x)) + (\overline{1} - T^0_m))[t_1/t_2]$ $\sim$



But $T^0_m(x)$ does not contain t_1 and by Lemma 5 $T^k_m(S(x))[t_1/t_2] \sim T^{k+1}_m(x)$. Therefore

$(Q^n_m(y, S(x)) + (\overline{1} - T^0_m))[t_1/t_2]$ $\sim$



which is the term $Q^n_m(y + (\overline{1} - T^n_m(x)), x)$.

By the previous Lemma and Lemma 5, part 4, we obtain

$$PA(-) \vdash_b (Q^n_m(y, S(x)) + (\overline{1} - T^0_m))[t_1/t_2] = Q^n_m(y, S(x)) + (\overline{1} - T^0_m)$$

and therefore

$$PA(-) \vdash_b Q^n_m(y + (\overline{1} - T^n_m(x)), x) = Q^n_m(y, S(x)) + (\overline{1} - T^0_m(x))$$

The other part of the proposition follows from the fact that $PA(-) \vdash_b T^0_m(x) = 0$. QED

Proof of Theorem 3: We reason in $PA(-)$. Assume that $S^m(0) \cdot S^n(0) \neq S^{m \cdot n}(0)$. Then by Lemma 5 for every x, $T^n_m(x) \neq 0$. Then, by Lemma 4, part 3, $\overline{1} - T^n_m(x) = 0$ for every x. The previous lemma then gives the equality

$$(\star) \qquad Q(y, x) = Q(y, S(x)) + \overline{1}.$$

Let $y := 0$. By induction we can prove that for every z,

$$(\star\star) \qquad Q(0, 0) = Q(0, z) + z.$$

If $z = 0$ we have $Q(0, 0) = Q(0, 0) + 0$ which is true. Assume that the statement holds for z, i.e., $Q(0, 0) = Q(0, z) + z$. From $(\star)$ we have $Q(0, z) = Q(0, S(z)) + \overline{1}$ and hence $Q(0, 0) = Q(0, S(z)) + \overline{1} + z = Q(0, S(z)) + S(z)$.

But the proposition $(\star\star)$ implies that $Q(0, 0) \geq z$ for every z, which is impossible. QED

3 The theory $PA(q)$

Let q be a function symbol of arity ≥ 1. The theory $PA(q)$ will be the theory obtained by adding the symbol q to the language of PA and extending the scheme of induction to the language of $PA(q)$. Hence the only axioms describing the properties of q in $PA(q)$ are those given in the induction and the identity schemes.

Theorem 8 *There is a number k and a formula $\psi(x)$ in the language of $PA(q)$ such that for every n $PA(q) \vdash_k \psi(S^n(0))$ but $PA(q) \nvdash \forall x\ \psi(x)$.*

Proof. Assume that q is a binary function. The sentence

$$\forall x \forall y \forall z\ (q(x, y) = z) \equiv (x = y + z \vee (x < y \wedge z = 0))$$

will be denoted as $SUBTR[q]$. As in Theorem 2 we can find a formula $\psi'(x)$ in the language of PA such that $\forall x\ \psi(x)$ is not provable in PA (and hence in $PA(q)$), but the instances are provable in a bounded number of steps, if we have an upper bound on proof-lengths for the equations $\overline{n} \cdot \overline{m} = \overline{n \cdot m}$. Let $\psi(x)$ be the formula

$$SUBTR[q] \rightarrow \psi'(x)$$

In every instance of the formula we can assume $SUBTR[q]$ and use q in place of minus as in the previous section. Hence we obtain $PA(q) \vdash_b \psi(S^n(0))$. The sentence

$\forall x\ \psi(x)$ is not provable in $PA(q)$, since $PA(q)$ is a conservative extension of PA and the formula $SUBTR[q]$ is satisfiable (i.e., every model of PA can be expanded to the model of $PA(q) + SUBTR[q]$).

If q has an arity bigger than two, we can use the term $q(x, y, 0, \ldots 0)$ instead.

Assume that q is a unary function symbol. In PA we have a binary term OP coding pairs of natural numbers. The previous argument can be applied to the term $q(OP(x, y))$. QED

4 The theory of integers

The function minus, as introduced in section 2, is quite different from the functions definable by terms in PA. Not only it is not increasing but it is also very 'discontinuous'. Note that with minus we have definitions by cases on terms: if we have functions f_1, f_2, g_1, g_2 defined by terms then we also have a term in $PA(-)$ which defines the function h such that $h(x) = f_1(x)$, if $g_1(x) \leq g_2(x)$, and $h(x) = f_2(x)$ otherwise.[4] We defined minus in this way because we wanted to have a theory with the same universe as PA. However, this property of minus is not essential in the proof of Theorem 3. We will now show that a similar argument can be applied to the theory of integers, where minus is definable in the natural way.

The theory of integers, $\mathcal{Z}$, is the theory with constant 0, function symbols $S, +, \cdot$ and predicates $<, \leq, =$. The axioms are the following (we take the leisure to write $x > y$ ($\geq y$) instead of $y < x$ ($\leq x$) and abbreviate the bounded quantifiers in the usual way):

$Q1$: $\forall x \forall y (S(x) = S(y)) \rightarrow x = y$

$Q3'$: $\forall x \exists y\ S(y) = x$

$Q4$: $\forall x\ x + 0 = x$

$Q5$: $\forall x \forall y\ x + S(y) = S(x + y)$

$Q6$: $\forall x\ x \cdot 0 = 0$

$Q7$: $\forall x \forall y\ x \cdot S(y) = x \cdot y + x$

$R8$: $\forall x < 0 \exists y > 0\ x + y = 0$

$D9$: $\forall x \forall y\ x \leq y \equiv x < y \vee x = y$

$L10$: $\forall x \geq 0\ S(x) > 0$

$L11$: $\forall x\ x < 0 \equiv \neg(x \geq 0))$

$L12$: $\forall x \forall y\ (x < y \equiv \exists z > 0\ y = x + z)$

and the scheme of induction

[4] Observe that $h(x) = f_1(x)(1 - (g_1(x) - g_2(x))) + f_2(x)(1 - ((g_2(x) + 1) - g_1(x)))$.

IND: $((\psi(0) \wedge (\forall x \geq 0\ \psi(x) \rightarrow \psi(S(x))) \rightarrow \forall x \geq 0\ \psi(x)$

The axioms Q1 -Q7 determine the behavior of $S, +$ and $\cdot$; they are the axioms of PA except for the modified axiom $Q3'$. $R8$ is the key axiom relating positive and negative numbers. $D9$ is a definition of $\leq$. The axioms $L10$-$L11$ can be equivalently replaced by axioms asserting that $<$ is a linear ordering and that $x < S(x)$. The motivation for choosing our axiomatisation is the following: axioms preceding $L12$, except for the definition $D9$, use the relations $<, \leq$ only in the context $x < 0$, $x \leq 0$ etc., i.e., we employ only the property 'to be a positive (non-negative) number'. The axiom $L10$ asserts that the successor of a non-negative number is positive, the axiom $L11$ says that every number is either positive or non-positive and not both. It is just the last axiom which determines the exact properties of $<$. Note that there is no function symbol for minus in $\mathcal{Z}$ and that the scheme of induction applies only to positive numbers.

Lemma 9 *Let ψ be a formula in the language of $\mathcal{Z}$. Then the following are provable in $\mathcal{Z}$:*

IND1 $((\psi(0) \wedge (\forall x \geq 0\ \psi(x) \rightarrow \psi(S(x)) \wedge (\forall x < 0\ \psi(S(x)) \rightarrow \psi(x))) \rightarrow \forall x \psi(x)$

IND2 $((\psi(0) \wedge (\forall x \psi(x) \equiv \psi(S(x))) \rightarrow \forall x \psi(x)$

`Proof.` It is sufficient to prove part one, the other follows immediately. Reason within $\mathcal{Z}$. Assume that i) $\psi(0)$, ii) $(\forall x \geq 0\ \psi(x) \rightarrow \psi(S(x))$ and iii) $\forall x < 0\ \psi(S(x)) \rightarrow \psi(x)$. From i), ii) and IND we obtain $\forall x \geq 0\ \psi(x)$. By $L11$ it is sufficient to show that $\forall x < 0\ \psi(x)$. The following can be easily proved by induction (and the axioms $Q4$, $Q5$):

Claim. $\forall x \forall y \geq 0\ x + S(y) = S(x) + y$

Let $\psi'(x)$ be the formula

$$\forall z < 0\ z + x = 0 \rightarrow \psi(z),$$

where z does not occur freely in ψ. Let us show that $\forall x \geq 0\ \psi'(x)$. If $x = 0$ then for every z if $z + x = 0$ then $z = 0$, the antecedent is not satisfied and the statement holds. Assume that $\psi(x)$ is true for $x \geq 0$. Let us show that $\psi(Sx)$ is true. Let $z < 0$ be such that $z + S(x) = 0$. Then $S(z) + x = 0$ and, by the inductive assumption, we have $\psi(S(z))$ (more exactly, if $S(z) \geq 0$ we have $\psi(S(z))$ from the first part of the proposition and we use the inductive assumption in the case $S(z) < 0$) . From iii) we have $\psi(z)$. Hence $\psi'(S(x))$ is true and therefore also $\forall x \geq 0\ \psi'(x)$. This, together with axiom $R8$, gives $\forall x < 0\ \psi(x)$. `QED`

The following proposition serves mainly to convince the reader of the soundness of the system $\mathcal{Z}$.

Proposition 10 *The following formulae are provable in $\mathcal{Z}$:*

1. *i) $x \neq S(x)$, ii) $x+y = y+x$, iii) $(x+y)+z = x+(y+z)$, iv) $y+z = x+z \equiv y = x$, v) $x \cdot (y+z) = x \cdot y + x \cdot z$, vi) $x \cdot y = y \cdot x$, vii) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$*

2. *i)* $\forall x \forall y \exists! z\ x = y + z$, *ii)* $\forall x \geq 0 \forall y \geq 0\ x + y \geq 0$, *iii)* $\forall x \leq 0 \forall y \leq 0\ x + y \leq 0$

3. *i)* $\neg x < x$, *ii)* $x < y \vee y < x \vee x = y$, *iii)* $(x < y) \wedge (y < z) \rightarrow (x < z)$, *iv)* $\neg(x < y \wedge y < x)$

4. *i)* $\forall x \forall y (x > 0 \wedge y > 0 \vee x < 0 \wedge y < 0) \rightarrow x \cdot y > 0$, *ii)* $x \cdot x \geq x$.

5. $\exists! z \forall x\ x \cdot z + x = 0$

`Proof.` For 1 proceed as in PA but use IND2 where appropriate. We will prove part ii), the rest is similar. (In order to prove i) note that the statement $S(0) \neq 0$ follows from $L10$ and $L11$.) Let us first prove that for all x, $0 + x = x$. Let $\psi(x)$ be the formula $0 + x = x$. If $x = 0$ the formula holds because of $Q4$. Let us show that $\psi(x)$ iff $\psi(S(x))$, for every x. Assume $\psi(x)$. Then $0 + S(x) = S(0 + x) = S(x)$ and $\psi(S(x))$ holds. Assume $\psi(S(x))$. Then $0 + S(x) = S(x)$ and so $S(0 + x) = S(x)$. By $Q1$ we have $0 + x = x$ and $\psi(x)$ holds. By IND2 we then obtain $\forall x \psi(x)$. Let now $\psi(x)$ be the formula $\forall y\ x + y = y + x$. If $x = 0$, the formula holds as shown. As in the previous case we can prove that $\psi(x)$ iff $\psi(S(x))$, for every x and hence $\forall x \psi(x)$ holds.

2 The first proposition is straightforward, the second one requires the axiom $L10$. The next one uses the axiom $L11$.

3 If $x < x$ then there is $z > 0$ such that $x = x + z$. But then $(x = x + 0 = x + z)$ and by 1, iv) we have $z = 0$. But that is impossible, by axiom $L11$. The rest follows from the statements already proved.

4 Easy.

5 Let z_0 be such that $S(z_0) = 0$. Then $x \cdot S(z_0) = 0$. But $x \cdot S(z_0) = x \cdot z_0 + x$. If on the other hand $x \cdot z + x = 0$ for every x then also $S(0) \cdot z + S(0) = 0$ and hence $S(0) \cdot S(z) = 0$. But $S(0) \cdot S(z) = S(z)$ and hence $S(z) = 0$. Therefore $z = z_0$. `QED`

We are now going to prove the following theorem:

Theorem 11 *There is k such that for every n, m $\mathcal{Z} \vdash_k S^n(0) \cdot S^m(0) = S^{n \cdot m}(0)$, or shortly*

$$\mathcal{Z} \vdash_b S^n(0) \cdot S^m(0) = S^{n \cdot m}(0)$$

Corollary *There is a number k and a formula $\psi(x)$ in the language of $\mathcal{Z}$ such that for every n $\mathcal{Z} \vdash_k \psi(S^n(0))$ but $\mathcal{Z} \nvdash \forall x \geq 0\ \psi(x)$.*

Lemma 12 *Let T be a theory such that $\exists z \psi(z)$ is provable in T. Let T' be the extension of T with a new constant symbol c and the axiom $\psi(c)$. Then*

1. *There exists a function $p : \omega \rightarrow \omega$ with the following property: if ξ is a formula in the language of T such that $T' \vdash_k \xi$ then $T \vdash_{p(k)} \xi$*

2. *Hence if S is a set of formulae in the language of T and $k \in \omega$ is such that $T' \vdash_k \xi$ for every $\xi \in S$ then there is $j \in \omega$ s.t. $T \vdash_j \xi$, for every $\xi \in S$.*

`Proof.` The first part is easy and the other follows. `QED`

The lemma shows that we can, without significantly shortening the proofs, extend the language of $\mathcal{Z}$ by new constant symbols. We shall thus work in the system $\mathcal{Z}$(-1) obtained by adding a new constant -1 to the language of $\mathcal{Z}$ together with the axiom

$$\forall x\ x \cdot (\text{-}1) + x = 0$$

Definition 2 *1. The expression $t_1 - t_2$ will be an abbreviation for $t_1 + (\text{-}1).t_2$*

2. The expression $t_1 \oplus t_2$ will be an abbreviation for $t_1 \cdot t_1 + t_2 \cdot t_2$.

Lemma 13 *The following formulae are provable in $\mathcal{Z}$:*

1. $(x + z) - (x + z) = x - y$
2. $x - y = 0 \ \equiv \ x = y$
3. $(0 \oplus 0) = 0.$
4. $(x \oplus y) \geq 0$
5. $x \neq 0 \rightarrow (y \oplus x > y).$

`Proof.` 1-3 are easy.
4 and 5 follow from Proposition 10, part 4. `QED`

Let $T^n_m(x)$ denote the term

$$S^m(0) \cdot S^n(x) - S^{n \cdot m}(S^m(0) \cdot x).$$

We will show that $\mathcal{Z} \vdash_b T^n_m(0) = 0$, which immediately implies $\mathcal{Z} \vdash_b S^m(0) \cdot S^n(0) = S^{n \cdot m}(0)$.

The proof proceeds similarly to that one in section 2.

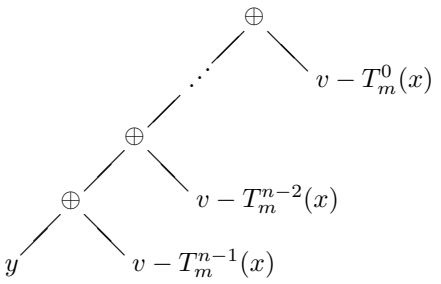
Lemma 14 *1. $\mathcal{Z} \vdash_b S^m(0) \cdot S(x) = S^m(S^m(0) \cdot x)$*

2. $T^n_m(S(x))[S^m(0) \cdot S(x)/S^m(S^m(0) \cdot x)] \ \sim \ T^{n+1}_m(x)$, for every n.

3. $\mathcal{Z} \vdash_b \forall x\ T^n_m(x) = T^n_m(0).$

`Proof.` As in Lemma 5 `QED`

Let $Q^n_m(y,v,x)$ denote the term



The following is proved as in Lemma 7:

Lemma 15 *$\mathcal{Z} \vdash_b Q(y \oplus (v - T^n_m(x)), v, x) = Q(y, v, S(x)) \oplus (v - T^0_m)$ and hence $\mathcal{Z} \vdash_b Q(y \oplus (v - T^n_m(x)), v, x) = Q(y, v, S(x)) \oplus v$*

Proof of Theorem 9: We reason in $\mathcal{Z}$. Assume that $S^m(0) \cdot S^n(0) \neq S^{m \cdot n}(0)$. Therefore $T^n_m(0) \neq 0$. Let $v_0 := T^n_m(0)$. We have $v_0 - T^n_m(0) = 0$ and $v_0 \neq 0$. By Lemma 13 part 3, $v_0 - T^n_m(x) = 0$ for every x.

The previous lemma then gives

$$Q(y \oplus 0, v_0, x) = Q(y, v_0, S(x)) \oplus v_0.$$

Let $y := 0$. Then we obtain (Lemma 13, part 3)

$$(\star) \qquad Q(0, v_0, x) = Q(0, v_0, S(x)) \oplus v_0.$$

By induction with respect to z we can prove that for every $z \geq 0$ and for every x

$$Q(0, v_0, x) \geq z.$$

If $z = 0$, the proposition follows from Lemma 13, part 4 (since $Q(0, v_0, x)$ has the form $t_1 \oplus t_2$.) Assume the statement holds for $z \geq 0$. From $(\star)$ and Lemma 13, part 5, and the fact that $v_0 \neq 0$ we have $Q(0, v_0, x) > Q(0, v_0, S(x))$. By the inductive assumption $Q(0, v_0, x) \geq z$ for every x and hence $Q(0, v_0, S(x)) \geq z$. Hence $Q(0, v_0, x) > Q(0, v_0, S(x))$ implies $Q(0, v_0, x) > z$ and $Q(0, v_0, x) \geq S(z)$. But that is impossible.

`QED`

5 The theory $PA(N)$

Let $N(x)$ be a unary predicate. The expressions $\forall x \in N\ \psi(x)$, $\exists x \in N\ \psi(x)$ will abbreviate the formulae $\forall x\ N(x) \rightarrow \psi(x)$, $\exists x\ N(x) \wedge \psi(x)$ respectively. Let ψ be a formula of PA. Then *the relativisation* of ψ will be the formula obtained by replacing the quantifiers $\forall x$, $\exists x$ by $\forall x \in N$, $\exists x \in N$ respectively. The theory $PA(N)$ will be the

theory obtained by adding the unary predicate N to the language of PA, its axioms - besides induction - will be the relativisations of axioms of PA, and the induction being replaced by the scheme

$$(\psi(0) \wedge (\forall x \in N\ (\psi(x) \rightarrow \psi(S(x)) \rightarrow \forall x \in N\ \psi(x),$$

where ψ is any formula of $PA(N)$.

The intended meaning of the predicate N is *'is a natural number'*. We see that PA is equivalent (meaning mutually interpretable conserving the length of proofs) to the theory $PA(N)$ plus the axiom $\forall x\ N(x)$. At the same time the theory $PA(N)$ can be extended to a theory equivalent to $\mathcal{Z}$, by adding only a finite number of axioms. This fact is used in the following theorem.

Theorem 16 *There is a formula $\psi(x)$ in the language of $PA(N)$ and a number k such that for every n, $PA(N) \vdash_k \psi(S^n(0))$ but $PA(N) \nvdash \forall x \in N\ \psi(x)$.*

`Proof.` The proof is similar to the proof of Theorem 9. Let κ denote the sentence obtained by the conjunction of the axioms of $\mathcal{Z}$, apart from induction, and the sentence $\forall x\ N(x) \equiv x \geq 0$. Let $\psi'(x)$ be as in Theorem 9 and let $\psi(x)$ denote the formula

$$\kappa \rightarrow \psi'(x).$$

The theory $PA(N) + \kappa$ is equivalent to $\mathcal{Z}$. This is true even in the sense of conserving the lengths of proofs: the lengths of proofs in $\mathcal{Z}$ and $PA(N) + \kappa$ differ at most by a constant. As shown above $\mathcal{Z} \vdash_b \psi'(S^n(0))$ and hence there is a k such that for every n, $PA(N) \vdash_k \psi(S^n(0))$. The formula $\forall x \in N(x)\ \psi(x)$ is not provable in $PA(N)$, for $PA(N)$ is conservative over PA. `QED`

6 Modifications of KC.

Let us recall the proposition

$$SUBTR[q] \rightarrow \psi'(x)$$

of Theorem 8, and let us substitute a binary term t of PA for q. Using the assumption $SUBTR[t]$, the instances of the formula

$$\psi(x) := SUBTR[t] \rightarrow \psi'(x)$$

can be proved in a bounded number of steps. On the other hand, since t is a term of PA, we can also prove $\neg SUBTR[t]$ in PA and hence also $\forall x \psi(x)$ is provable in PA. But we must notice that the proof of $SUBTR[t] \rightarrow \psi'(x)$ is very dissimilar from the proofs of its instances: we prove the instances using the assumption $SUBTR[t]$ but we prove the generalization by proving $\neg SUBTR[t]$. This observation does not contradict KC but it goes very strongly against its spirit: the motivation for believing KC is that we can somehow transform the proofs of the instances to the proof of the

generalization. But at least in a naive reading of the phrase 'transformation of the proof' this is not the case.

The same observation applies to the so called Sharpened Kreisel's Conjecture (SKC). SKC asserts, roughly (see, e.g., Krajíček and Pudlák [1988]), that if $\psi(\overline{n})$ can be proved by a short proof for a large n then the proof can be transformed to the proof of the proposition *'the numbers satisfying ψ contain an (infinite) arithmetical sequence'*. Depending again on the charitability of the reading of the phrase 'to be transformed', we can give a counterexample to SKC. For take the formula

$$\psi(x) := SUBTR[t] \to \exists z x = z \cdot z.$$

Using the assumption $SUBTR[t]$ the formula can be proved for every n which is a square in a bounded number of steps. Since $\neg SUBTR[t]$ is provable then $\forall x \psi(x)$ is also provable, and hence also the sentence *'the numbers satisfying ψ contain an arithmetical sequence'*. However, this proof is 'very different' from the proof of $\psi(\overline{n})$, for a square n. The gap between the proofs of the instances and the proof of the generalization would stand out more clearly if we managed to show that formulae of the form $\neg SUBTR[t]$ cannot be proved in PA in a bounded number of steps. For then the instances of $\psi(x)$ would be proved in k steps regardless to the t chosen but the proof of the generalization would have an arbitrary length, as determined by the particular t.

Conjecture. For every $k \in \omega$ there exists a binary term t of PA s.t. $\nvdash_k \neg SUBTR[t]$.

Corollary 1. There exists $k \in \omega$ s.t. for every $j \in \omega$ there exists a formula $\psi(x)$ s.t. the set $\{n \in \omega, \vdash_k \psi(\overline{n})\}$ is infinite but the set $\{n \in \omega, \vdash_j \psi(\overline{n})\}$ does not contain an arithmetical sequence.

'`Proof`' Let $\phi(x)$ be the formula $\exists z\ x = z \cdot z$. There exists $k \in \omega$ s.t. for every binary term t and every square number n, $\vdash_k SUBTR[t] \to \phi(\overline{n})$, and $\vdash_k SUBTR[t] \to \neg\phi(\overline{n})$, if n is not a square. For a given $j \in \omega$ there exists, by the Conjecture, a binary term t s.t. $\nvdash_{k+j+5} \neg SUBTR[t]$. Let

$$\psi(x) := SUBTR[t] \to \phi(x).$$

Then $\{n \in \omega, \vdash_k \psi(\overline{n})\}$ is infinite. Assume that the set $\{n \in \omega, \vdash_j \psi(\overline{n})\}$ contains an arithmetical sequence. Then there exists a number n which is not a square s.t. $\vdash_j \psi(\overline{n})$, i.e.

$$\vdash_j SUBTR[t] \to \phi(\overline{n}).$$

On the other hand, since n is not a square, we have

$$\vdash_k SUBTR[t] \to \neg\phi(\overline{n}).$$

This altogether gives $\vdash_{k+j+5} \neg SUBTR[t]$, contrary to our assumption. '`QED`'

Corollary 2. There exists $k \in \omega$ s.t. for every $j \in \omega$ there exists a formula $\psi(x)$ s.t. $\nvdash_j \forall x \psi(x)$ but $\vdash_k \psi(\overline{n})$ for every $n \in \omega$.

'`Proof`' Let $t_1, t_2, \ldots$ be a sequence of terms s.t. $\nvdash_i \neg SUBTR[t_i]$. Let $Proof(x, y)$ be an arithmetical translation of the proposition that the formula with Gödel number y

has a proof with x proof lines in PA. Let T_i be the theory $PA+\neg Proof(\bar{i}, \ulcorner \neg SUBTR[t_i] \urcorner)$. Let us have a sequence of Π_0-formulas $\phi_1(x), \phi_2(x), \ldots$ s.t. $\forall x \phi_i(x)$ is undecidable in T_i. Furthermore, we can bound the complexity of the formulas in such a way that there exists $k \in \omega$ s.t. for every n and every i if $\phi_i(\overline{n})$ is true then $PA \vdash_k SUBTR[t_i] \rightarrow \phi_i(\overline{n})$, and $PA \vdash_k SUBTR[t_i] \rightarrow \neg\phi_i(\overline{n})$ otherwise. Since the argument of Theorem 3 can be formalised in PA, we can also assume that for the given k we have

$$PA \vdash \forall x(\neg\phi_i(x) \rightarrow Proof(\overline{k}, \ulcorner SUBTR[t_i] \rightarrow \neg\phi_i(x) \urcorner))$$

Let $\psi_i(x) := SUBTR[t_i] \rightarrow \phi_i(x)$. Then for every $n \in \omega$, $PA \vdash_k \psi_i(\overline{n})$. Assume that there exists $j \in \omega$ s.t. for every i $PA \vdash_j \forall x \psi_i(x)$. Let $i > k + j + 6$. There exists a model $\mathcal{N}$ of T_i and $n \in \mathcal{N}$ s.t. $\mathcal{N} \models \neg\phi_i(n)$. Hence

$$\mathcal{N} \models Proof(\overline{k}, \ulcorner SUBTR[t_i] \rightarrow \neg\phi_i(\overline{n}) \urcorner).$$

From the assumption that $PA \vdash_j \forall x \psi_i(x)$ we have also

$$\mathcal{N} \models Proof(\overline{j+1}, \ulcorner SUBTR[t_i] \rightarrow \phi_i(\overline{n}) \urcorner).$$

But this altogether gives

$$\mathcal{N} \models Proof(\overline{k+j+6}, \ulcorner \neg SUBTR[t_i] \urcorner),$$

which contradicts the fact that $\mathcal{N} \models T_i$. 'QED'

The latter corollary violates the idea of transforming the proofs of the instances to the proof of the generalization, while the first is a refutation of SKC. However, we must note that the Conjecture takes its plausibility from the same intuitions as KC itself. For it seems that for a sufficiently large and chaotic term we cannot prove in a small number of steps that it does not have the property $SUBTR$. The assumption is a special case of the following general problem. Let us again have the theory $PA(q)$, where q can have arity ≥ 0. We may ask what is the relationship between a formula $\psi[q]$ in the language of $PA(q)$ and the formulae $\psi[t]$ obtained by replacing q by a term t of PA of the same arity. Clearly, it can happen that $\psi[q]$ is not provable in $PA(q)$ while $\psi[t]$ can be proved in PA for every term t (of adequate arity). On the other hand, by the same intuitions that lead us to believing KC we expect that if such a situation occurs then the proofs of $\psi[t]$ must use some specific properties of t and thus have lengths which depends on the complexity of t. If q has arity $n \geq 0$, we can formulate an *n-modified Kreisel's Conjecture:*

MKC$_n$ Let $k \in \omega$. Assume that for every n-ary term t of PA the formula $\psi[t]$ is provable in PA in k steps. Then the formula $\psi[q]$ is provable in $PA(q)$.

All the instances of MKC$_n$ for $n > 0$ are equivalent. If $n = 0$, the assertion is equivalent to the proposition (which may be called *'The Very Weak Kreisel's Conjecture'*):

VWKC Let $k \in \omega$. Assume that for every constant term C of PA the formula $\psi(C)$ is provable in PA in k steps. Then the formula $\forall x \psi(x)$ is provable in PA.

The VWKC immediately follows from KC. And it seems very straightforward: it seems enough to take for C a sufficiently large and chaotic term. But this is not the case. It can be shown that true equations of the form $C = 0$, $\neg(C = 0)$, $C = 1$, $\neg(C = 1)$, for a constant term C, can be proved for even 'very large' and 'very chaotic' terms in a bounded number of steps. (This is somewhat surprising, for all our previous constructions were based on symmetric terms.) Hence we cannot easily rule out the alternative that all true equations of the form $C = 0$, $\neg(C = 0)$, $C = 1$, $\neg(C = 1)$ can be proved in a bounded number of steps. This would imply that also the formulae $\neg SUBTR[t]$ can be proved in PA in a bounded number of steps, for binary t (note that necessary conditions for $SUBTR[t]$ are i) $t(1,0) \neq 0$ and ii) $t(1,1) = 0$). Hence also our assumption and the conjectures MKC_n, $n > 0$, would be false.

We are here facing a dichotomy, none of whose parts is very favourable for KC: if MKC_1 is true, then the Corollary 1 of our Conjecture frustrates the concept of 'transforming instances to the generalization'. If, on the other hand, MKC_1 is false then it makes our reasons for believing KC even more doubtful: for KC and MKC_1 take their plausibility from essentially the same source.

7 Is KC true?

We have met two kinds of systems in this paper: one in which we have an upper bound on multiplication and therefore KC is false, and the other where KC is false for a different reason. The following questions therefore do not need to have the same answers: *i) is there an upper bound for multiplication in PA? ii) is KC false in PA?* If we are allowed to guess, if not to conjecture, then the answer to i) is *'no'* and to ii) *'yes'*. The reason why we believe that no upper bound for multiplication can be found in PA is roughly this: for a large term t, all the tricks we have tried have helped us to prove in a bounded number of steps only whether $t = 0, \neq 0, = 1, \neq 1$, or some general and not very useful property of t. The point of our preceding construction is that using '-' we convert the apparently useless information $t \neq 0$ to the proposition $t_1 = t_2$, for some useful t_1 and t_2. But if we have only terms which provably define increasing functions then the information whether $t = 0, \neq 0, = 1, \neq 1$ is indeed useless. On the other hand, we believe that KC is very likely to be false. Leaving aside the alternative that in PA the upper bound for multiplication can in fact be found, we see that the systems $PA(q)$ and $PA(N)$ are very close to PA, the system $PA(N)$ being almost indiscernible from PA. Second, the examples of Section 6 go strongly against the spirit of KC and they could perhaps be converted to a counterexample. Our current inability to find a counterexample may follow merely from our combined inability to determine the lengths of proofs of instances $\psi(\overline{n})$ and our lack of techniques for proving the undecidability of $\forall n\ \psi(n)$.

If, after all, KC is true then our result shows that the proof must concentrate on the specific properties of PA. In the proof it must be relevant that the functions definable by terms in PA are provably increasing, polynomial etc. We cannot hope for a proof that would work independently on the function symbols used, and thus we cannot hope to solve KC by some clever general argument.

We would like to end with a list of problems apparently easier than KC but which could help us understand the function of terms, and perhaps to solve KC itself.

Problem 1. In this paper, we have used the schemes of identity (which, as noted in the Introduction, can be replaced by the induction scheme). Can we find a 'natural' extension of PA where KC is false, if only the axioms of identity and the minimum-element scheme are used?

Problem 2. Find a set of true equations on terms with a fixed number of variables (ideally, constant terms) which cannot be proved in a bounded number of steps. For example, the instances of commutativity of large sums or products.

Problem 3. Prove or disprove the so called Very Weak Kreisel's Conjecture of Section 6.

References

[1] Friedman, H.: One hundred and two problems in mathematical logic. The Journal of Symbolic Logic, 40, 113-129 (1975)

[2] Baaz, M., Pudlák, P.: Kreisel's conjecture for $L\exists_1$. Arithmetic, Proof Theory, and Computation Complexity, Papers from the Conference Held in Prague, July 2-5, 1991, New York: Oxford University Press, 30-60 (1993)

[3] Krajíček, J., Pudlák, P.: The number of proof lines and the size of proofs in first order logic. Arch. Math. Logic 27, 69-84 (1988)

[4] Miyatake, T.: On the lengths of proofs in formal systems. Tsukuba Journal of Mathematics 4, 115-125 (1980)

[5] Parikh, R.: Some results on the length of proofs.TAMS 177,29-36 (1973)

[6] Yukami, T.: A note on a formalized arithmetic with function symbols and +. Tsukuba Journal of Mathematics 7, 69-73 (1978)

[7] Yukami, T.: Some results on speed-up. Ann.Jap.Assoc.Philos.Sci.,Vol.6,195-205 (1984)