Kreisel's Conjecture with minimality principle

Pavel Hrubeš*

November 9, 2008

Abstract

We prove that Kreisel's Conjecture is true, if Peano arithmetic is axiomatised using minimality principle and axioms of identity (theory PA_M). The result is independent on the choice of language of PA_M. We also show that if infinitely many instances of $A(x)$ are provable in a bounded number of steps in PA_M then there exists $k \in \omega$ s.t. $PA_M \vdash \forall x > \overline{k}\ A(x)$. The results imply that PA_M does not prove scheme of induction or identity schemes in a bounded number of steps.

1 Introduction.

Kreisel's Conjecture (KC) is the following assertion:

Let $A(x)$ be a formula of PA with one free variable. Assume that there exists $c \in \omega$ s.t. for every n $A(\overline{n})$ is provable in PA in c steps. Then $\forall x A(x)$ is provable in PA.

The peculiarity of KC is that it is very sensitive to the way PA is axiomatised[1]. One natural axiomatisation, which we shall denote PA_I, is to formalise PA using the *scheme of induction*

$$A(0) \wedge \forall x(A(x) \to A(S(x))) \to \forall x A(x),$$

and to axiomatise "=" by *identity schemes* of the form

$$x = y \to t(x) = t(y),$$

where t is an arbitrary term of PA. However, this does not yet settle the question. Multiplication and addition can be formalised either as binary function symbols or as ternary predicates. It was shown in [6] and [5] that KC is true in the theory $PA_I(S, +)$, where S and $+$ are present as function symbols, and $\cdot$ is axiomatised as a predicate. On the other hand, KC is false in the theory

*Written in Prague, Institute of Mathematics, with support from grant 1AA1019401. Completed at Institute for Advanced Study, NSF grant CCF 0832797.

[1] Kreisel's conjecture, as presented in [1] refers to PA axiomatised by identity axioms and the scheme of induction. However, this seems purely accidental.

$PA_I(S,+,\cdot,-)$ where $-$ is a function symbol for subtraction (see [3]). The most interesting case, where exactly the function symbols $S,+,\cdot$ are present, is an open problem.

In this paper, we consider a different axiomatisation of PA, the theory PA_M. Instead of the scheme of induction, we take *minimality principle*

$$\exists x A(x) \rightarrow \exists x (A(x) \wedge \forall y < x \neg A(y)),$$

and identity will be finitely axiomatised using *identity axioms* of the form

$$x = y \rightarrow S(x) = S(y),$$

for the function symbols of PA. We will show that KC is true in PA_M (A weaker result in this direction was given in [2] for minimality principle restricted to Σ_1-formulas.) The good news is that the result does not depend on the choice of the language: we can add any finite number of function symbols and axioms to PA_M and KC is still valid (see Theorem 12).

The sensitivity of KC to the axiomatisation of PA diminishes its attractiveness as a mathematical problem. However, it reveals an interesting question of the role of functions symbols in proofs; and our inability to solve KC reveals how little we understand that role. An intuition behind KC is that if we prove a formula $A(\overline{n})$ for a large n in a small number of steps then the proof cannot take advantage of the specific structure of $\overline{n}$. This intuition is in general false. In PA_I we can prove for every even natural number that it is even, in a bounded number of steps (see [7]), and if we are given a sufficiently rich term structure than we can prove that n is a square number, for n being a square number (see [3]). None of those phenomena occur in the theory PA_M. Hence PA_M can teach us little about the theory PA_I. PA_M is rather a natural example of a theory where our intuitions *do* work. In PA_M, KC is true, we cannot prove that a number is even in a bounded number of steps, and more generally, if many instances of $A(x)$ are provable in a small number of steps then the set of numbers satisfying A contains an infinite interval.

2 The system PA_M

Predicate logic

As the system of predicate logic we take a system of propositional calculus plus the *generalisation rule*

$$\frac{B \rightarrow A(x)}{B \rightarrow \forall x A(x)},$$

and the *substitution axiom*

$$\forall x A(x) \rightarrow A(t),$$

B not containing free x and t being substitutible for x in $A(x)$. For simplicity, we assume that the only rule of propositional logic is modus ponens. Identity $=$ is not taken as a logical symbol.

Robinson's arithmetic and Identity axioms

Q will denote a particular finite axiomatisation of Robinson's arithmetic, a theory in the language $<, =, 0, S, +, \cdot$. As we do not work in predicate calculus with identity, the axiomatisation of "=" is a part of Q. The standard way is to formalise "=" using *identity axioms*, i.e., to have axioms stating that = is an equivalence, plus finitely many axioms of the form

$$\forall x, y \; x = y \rightarrow S(x) = S(y)$$

for the symbols of Q. However, the relevant fact is that Q is axiomatised in a finite way.

PA_M and minimality principle

PA_M is a theory in the language $<, =, 0, S, +, \cdot$. The axioms are the axioms of Q plus *minimality principle*

$$\exists x A(x) \rightarrow \exists x (A(x) \wedge \forall y < x \neg A(y)),$$

where A is a formula of PA_M and y is substitutible for x in $A(x)$.

Notation

Let t be term and a A a formula not containing function symbols. We write

$$t = t(x_1, \dots x_n), \qquad \text{resp.} \qquad A = A(x_1, \dots x_n)$$

if t resp. A contains exactly the variables $x_1, \dots x_n$, and for every $i, j = 1, \dots n$, $i < j$ implies that there exists an occurrence of x_i which precedes all the occurrences of x_j in t resp. A, where t resp. A is understood as a string ordered from left to right.

For a formula A, we write

$$A = A(t_1, \dots t_n),$$

if there exists a formula $B = B(x_1, \dots x_n)$ which does not contain any function symbol, and

$$A = B(x_1/t_1, \dots x_n/t_n).$$

In this case, we say that the terms $t_1, \dots t_n$ *occur in* A. Note that the term $SS(0)$ occurs in the formula $x = SS(0)$, whereas $S(0)$ does not.

3 Characteristic set of equations of a proof

Let S be a proof in PA_M. We shall now define R_S, the *characteristic set of equations of* S. The idea is to treat terms in S as completely uninterpreted function symbols, and we ask what information are we given about the function symbols in the proof S.

For every term s which occurs in a formula in S, or it has been substituted somewhere in S, we introduce a new n-ary function symbol f_s, where n is the number of variables occurring in s. We shall say that f_s *represents* s in R_S. For a formula A in S let us add to R_S equations in the following manner:

1. if A is an axiom of propositional logic, or has been obtained be a generalisation rule, or by means of modus ponens, add nothing.

2. If A is a substitution axiom of the form

$$\forall x B(s_1(x), \dots s_n(x)) \to B(s_1(s), \dots s_n(s)),$$

where $s_i(x) = s_i(\overline{z_i}, x, \overline{z_i}')$, $s = s(\overline{z})$ and $s_i(s) = s_i(s)(\overline{y_i})$, we add to R_S the equations

$$f_{s_i(s)}(\overline{y_i}) = f_{s_i}(\overline{z_i}, f_s(\overline{z}), \overline{z_i}'), \qquad \text{for } i = 1, \dots n.$$

3. if A is an axiom of Q containing the terms $s_i = s_i(\overline{x_i}), i = 1, \dots n$, we add to R_S the equations

$$f_{s_i}(\overline{x_i}) = s_i(\overline{x_i}), \qquad \text{for } i = 1, \dots n.$$

4. If A is an instance of the minimality principle of the form

$$\exists x B(s_1(x), \dots s_n(x)) \to \exists x (B(s_1(x), \dots s_n(x)) \wedge \forall_{y<x} \neg B(s_1(y), \dots s_n(y))),$$

where $s_i(x) = s_i(\overline{z_i}, x, \overline{z_i}')$ and $s_i(y) = s_i(\overline{y_i})$, we add the equations

$$f_{s_i(y)}(\overline{y_i}) = f_{s_i(x)}(\overline{z_i}, y, \overline{z_i}'), \qquad \text{for } i = 1, \dots n.$$

4 The theory $PA_M(\mathcal{F})$

Let $\mathcal{F}$ be a list of function symbols not occurring in PA_M. The theory $PA_M(\mathcal{F})$ is obtained by adding the function symbols $\mathcal{F}$ to the language of PA_M, and extending the minimality principle to the language of $PA_M(\mathcal{F})$. We *do not* add the identity axioms for the symbols in $\mathcal{F}$. We do not have axioms of the form

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

for $f \in \mathcal{F}$.

Convention and definition. *In this paper, we denote the terms of $PA_M(\mathcal{F})$ by $t_1, t_2, \dots,$ and the terms of PA_M by $s_1, s_2, \dots.$ $\mathcal{T}$ will denote the set of closed terms of $PA_M(\mathcal{F})$. Let $\mathcal{T}_0 \subset \mathcal{T}$ be the set of closed terms of the form $f(t_1, \dots t_n)$, where $f \in \mathcal{F}$. The elements of $\mathcal{T}_0$ will be denoted by $\lambda_1, \lambda_2, \dots.$*

The key connection between $PA_M(\mathcal{F})$ and the characteristic set of equations is given in the following proposition. πR_S is an abbreviation for the conjunction of universal closures of the equations in R_S.

Proposition 1 *Let S be a PA_M proof of the formula $A(s_1, \dots s_n)$, where $s_i = s_i(\overline{x_i}), i = 1, \dots n$. Let R_S be the characteristic set of equations of S. Then*

$$PA_M(\mathcal{F}) \vdash \pi R_S \to A(f_{s_1}(\overline{x_1}), \dots f_{s_n}(\overline{x_n})).$$

`Proof.` Let $S = A_1, \dots A_k$. For a formula A_i, let $A_i^\star$ be the formula obtained by replacing terms $s = s(\overline{x})$ occurring in A_i by $f_s(\overline{x})$. It is sufficient to prove that every $A_i^\star$ is provable in $PA_M(\mathcal{F})$ from πR_S. First note the following:

Claim. *Let A be a formula s.t. the variable x occurs in A only in the context $s(x)$. Let t_1 and t_2 be $PA_M(\mathcal{F})$ terms with the same variables $\overline{y}$. Then*

$$PA_M(\mathcal{F}) \vdash \forall \overline{y}(t_1 = t_2) \to (A(x/t_1) \equiv A(x/t_2)).$$

The Claim is proved easily by induction with respect to the complexity of A; for atomic formulas we use identity axioms for PA_M function symbols.

Let us use the Claim to prove the proposition. If A_i is an axiom of propositional logic then $A_i^\star$ is also an axiom of propositional logic. Similarly if A_i has been obtained by means of generalisation rule or modus ponens.

Assume that

$$A_i = A_i(s_1(\overline{x}), \dots s_n(\overline{x_n}))$$

is an axiom of Q. Then

$$A_i^\star = A_i(f_{s_1}(\overline{x}), \dots f_{s_n}(\overline{x_n})).$$

By the condition (3) of the definition of R_S and the Claim we have

$$PA_M(\mathcal{F}) \vdash \pi R_S \to A_i^\star \equiv A_i.$$

Since A_i is an axiom of Robinson arithmetic, then it is an axiom of $PA_M(\mathcal{F})$, and $PA_M(\mathcal{F}) \vdash \pi R_S \to A_i^\star$.

Assume that A_i is an instance of a substitution axiom of the form

$$\forall x B(x) \to B(s),$$

where B is as in part (2) of the definition of R_S. Then $A_i^\star = \forall x B(x)^\star \to B(s)^\star$. $B(x)^\star$ is the formula

$$B(f_{s_1}(\overline{z_1}, x, \overline{z_1}'), \dots f_{s_n}(\overline{z_n}, x, \overline{z_n}'))$$

and $B(s)^\star$ is the formula

$$B(f_{s_1(s)}(\overline{y_1}), \dots f_{s_n(s)}(\overline{y_n})).$$

Since the term $s(\overline{z})$ is substitutable for x in $B(x)$ then $f_s(\overline{z})$ is substitutible for x in $B(x)^\star$. Hence

$$\forall x B(x)^\star \to B(f_{s_1}(\overline{z_1}, f_s(\overline{z}), \overline{z_1}'), \dots f_{s_n}(\overline{z_n}, f_s(\overline{z}), \overline{z_n}'))$$

is an instance of the substitution axiom. By the Claim and part (2) of the definition of R_S, the formula

$$B(f_{s_1}(\overline{z_1}, f_s(\overline{z}), \overline{z_1}'), \ldots f_{s_n}(\overline{z_n}, f_s(\overline{z}), \overline{z_n}')) \equiv B(f_{s_1(s)}(\overline{y_1}), \ldots f_{s_n(s)}(\overline{y_n}))$$

is provable in $PA_M(\mathcal{F})$ from πR_S. Therefore

$$PA_M(\mathcal{F}) \vdash \pi R_S \rightarrow (\forall x B(x)^\star \rightarrow B(s)^\star).$$

If A_i is an instance of the minimality principle, the proof is similar. QED

5 Models of $PA_M(\mathcal{F})$

By means of Proposition 1 one can transform the question about bounded-length provability in PA_M to that of provability in $PA_M(\mathcal{F})$. Fortunately, it is not difficult to construct models of $PA_M(\mathcal{F})$, which makes the latter question easier.

For a model M and a predicate symbol P, P_M denotes the relation defined by P in M. Similarly $[\alpha]_M$ is the function defined by α in M, for α being a function symbol.

Let $\mathcal{N}$ be a model of PA_M. We would like to "expand" the model to a model of $PA_M(\mathcal{F})$. By a suitable coding, we can define the set of closed terms $\mathcal{T}$ and the set $\mathcal{T}_0 \subseteq \mathcal{T}$ inside $\mathcal{N}$. (I.e., $\mathcal{T}$ and $\mathcal{T}_0$ contain non-standard elements, if $\mathcal{N}$ is non-standard.) We extend the Convention above to terms defined in $\mathcal{N}$. The universe of our new model will be the set of closed terms $\mathcal{T}$. Let σ be a function from $\mathcal{T}_0$ to $\mathcal{N}$ definable in $\mathcal{N}$. Inside $\mathcal{N}$ we can (uniquely) extend it to the function $\sigma^\star : \mathcal{T} \rightarrow \mathcal{N}$ in the following manner:

1. $\sigma^\star(0) := [0]_\mathcal{N}$, $\sigma^\star(\lambda) := \sigma(\lambda)$, and
2. $\sigma^\star(St) := [S]_\mathcal{N}(\sigma^\star(t))$, $\sigma^\star(t_1 + t_2) := \sigma^\star(t_1)[+]_\mathcal{N}\sigma^\star(t_2)$, and $\sigma^\star(t_1 \cdot t_2) := \sigma^\star(t_1)[\cdot]_\mathcal{N}\sigma^\star(t_2)$.

We will use the function $\sigma^\star$ to define the model $\mathcal{N}_\sigma$. On $\mathcal{T}$ we define the identity $=_{\mathcal{N}_\sigma}$ by the condition

$$t_1 =_{\mathcal{N}_\sigma} t_2 \equiv \sigma^\star(t_1) =_\mathcal{N} \sigma^\star(t_2).$$

$<_{\mathcal{N}_\sigma}$ is defined as

$$t_1 <_{\mathcal{N}_\sigma} t_2 \equiv \sigma^\star(t_1) <_\mathcal{N} \sigma^\star(t_2).$$

The function symbols will be interpreted in $\mathcal{N}_\sigma$ as follows: if α is an n-ary function symbol of $PA_M(\mathcal{F})$ then $[\alpha]_{\mathcal{N}_\sigma}$ is the function which to $t_1, \ldots t_n \in \mathcal{T}$ assigns the term $\alpha(t_1, \ldots t_n) \in \mathcal{T}$.

The model $\mathcal{N}_\sigma$ is the set $\mathcal{T}$ with $=, <$ interpreted by the relations $=_{\mathcal{N}_\sigma}, <_{\mathcal{N}_\sigma}$, and the $PA_M(\mathcal{F})$ function symbols interpreted as $[0]_{\mathcal{N}_\sigma}, [S]_{\mathcal{N}_\sigma}, [+]_{\mathcal{N}_\sigma}, [\cdot]_{\mathcal{N}_\sigma}$, and $[f]_{\mathcal{N}_\sigma}, f \in \mathcal{F}$.

Proposition 2 *Let $\mathcal{N}$ be a model of PA_M. Let $\sigma : \mathcal{T}_0 \to \mathcal{N}$ be definable in $\mathcal{N}$. Then $\mathcal{N}_\sigma$ is a model of $PA_M(\mathcal{F})$. The PA_M part of $\mathcal{N}_\sigma$ is elementary equivalent to $\mathcal{N}$.*

`Proof.` Axioms of Robinson arithmetic and the identity axioms for PA_M function symbols are satisfied by the definition of $\mathcal{N}_\sigma$. Take, for example, the axiom

$$\forall x, y \;\; x + S(y) = S(x + y).$$

In order to prove that it is true in $\mathcal{N}_\sigma$, we must show that for every $t_1, t_2 \in \mathcal{T}$

$$t_1[+]_{\mathcal{N}_\sigma}[S]_{\mathcal{N}_\sigma}(t_2) =_{\mathcal{N}_\sigma} [S]_{\mathcal{N}_\sigma}(t_1[+]_{\mathcal{N}_\sigma}t_2).$$

From the definition of $[S]_{\mathcal{N}_\sigma}$ and $[+]_{\mathcal{N}_\sigma}$, this is equivalent to

$$t_1 + S(t_2) =_{\mathcal{N}_\sigma} S(t_1 + t_2),$$

where the equivalence is between elements of $\mathcal{T}$. From the definition of $=_{\mathcal{N}_\sigma}$, this is equivalent to

$$\sigma^\star(t_1 + S(t_2)) =_{\mathcal{N}} \sigma^\star(S(t_1 + t_2)).$$

From the definition of $\sigma^\star$, this is equivalent to

$$\sigma^\star(t_1)[+]_{\mathcal{N}}[S]_{\mathcal{N}}(\sigma^\star(t_2)) =_{\mathcal{N}} [S]_{\mathcal{N}}(\sigma^\star(t_1)[+]_{\mathcal{N}}\sigma^\star(t_2)),$$

which is true in $\mathcal{N}$, since $\mathcal{N}$ is a model of Robinson arithmetic.

The minimality principle is satisfied, for it was satisfied in the original model and the construction is defined inside $\mathcal{N}$.

PA_M-part of $\mathcal{N}_\sigma$ is isomorphic to $\mathcal{N}$, if $\mathcal{N}_\sigma$ is factorised with respect to $=_{\mathcal{N}_\sigma}$.
`QED`

Identity axioms and the scheme of induction are not in general true in $\mathcal{N}_\sigma$. To show that the identity axioms are not true, take the sentence

$$f(0) = f(0 + 0).$$

The sentence can be false in a model of $PA_M(\mathcal{F})$, for we can choose the value of $\sigma(f(0))$ and $\sigma(f(0 + 0))$ in an arbitrary way. Hence also the formula

$$x = 0 \to f(x) = f(0)$$

is not valid in models of $PA_M(\mathcal{F})$. On the other hand, the formula can be proved by induction with respect to x, and hence the scheme of induction is not valid in models of $PA_M(\mathcal{F})$.

6 Solving R_S in models of $PA_M(\mathcal{F})$

Let R be the characteristic set of equations of a PA_M proof. Let $\mathcal{N}$ be a model of PA_M. We shall now argue inside the model $\mathcal{N}$.

Let R' be the set of equations obtained from R by taking all possible substitutions of terms from $\mathcal{T}$ into R. More exactly, R' contains the equations

$$t(t_1, \dots t_n) = t'(t_1, \dots t_n),$$

for $t(x_1, \dots x_n) = t'(x_1, \dots x_n) \in R$ and $t_1, \dots t_n \in \mathcal{T}$.

The general form of an equations in R' is

$$\lambda = s(\overline{\lambda'}).$$

Inside $\mathcal{N}$, we define $R^\star$ as the smallest set of equations with the following properties:

1. $R' \subseteq R^\star$,
2. i) $\lambda = \lambda \in R^\star$ for every $\lambda \in \mathcal{T}_0$, ii) if $t_1 = t_2 \in R^\star$ then $t_2 = t_1 \in R^\star$, and iii) if $t_1 = t_2, t_2 = t_3 \in R^\star$ then $t_1 = t_3 \in R^\star$
3. if $t = s(t_1, \dots, t_i, t', t_{i+1} \dots t_n) \in R^\star$ and $t' = s'(t'_1, \dots t'_m) \in R^\star$ then
$$t = s(t_1, \dots, t_i, s'(t'_1, \dots t'_m), t_{i+1}, \dots t_n) \in R^\star$$
(we allow the case that s' is a variable),
4. if $s(t_1, \dots, t_n) = s(t'_1, \dots, t'_n) \in R^\star$ then
$$t_1 = t'_1 \in R^\star, \dots t_n = t'_n \in R^\star.$$

The general form of the equations in $R^\star$ is

$$s(\overline{\lambda}) = s'(\overline{\lambda'})$$

On $\mathcal{T}_0$ we define the relations $\sim$ and $\prec$ as follows:

1. $\lambda_1 \sim \lambda_2$ iff $\lambda_1 = \lambda_2 \in R^\star$,
2. $\lambda' \prec \lambda$ iff there exists s s.t. $\lambda = s(\lambda_1, \dots, \lambda_i, \lambda', \lambda_{i+1}, \dots \lambda_n) \in R^\star$. We require that s is not a variable.

For a term t of $PA_M(\mathcal{F})$ let $t^\star$ denote the PA_M term obtained by replacing the function symbols f_s by s. To be exact, i) $0^\star := 0$, ii) $(s(t_1, \dots t_2))^\star := s(t_1^\star, \dots t_n^\star)$, and iii) $(f_s(t_1, \dots t_2))^\star := s(t_1^\star, \dots t_n^\star)$. The following Lemma is simple but important:

Lemma 3 *1. If $t_1 = t_2 \in R^\star$ then $t_1^\star$ and $t_2^\star$ are the same terms.*

2. *If* $\lambda_1 \prec \lambda_2$ *then* $\lambda_1^\star$ *is a proper subterm of* $\lambda_2^\star$.

3. *Let* α *resp.* α' *be* PA_M *function symbols of arities* i *resp* i' *(so* $i, i' \leq 2$*) and let*
$$\alpha(t_1, \dots t_i) = \alpha'(t'_1, \dots t'_{i'}) \in R^\star.$$
Then $i = i'$, α *and* α' *are the same function symbols, and* $R^\star$ *contains the equations*
$$t_1 = t'_1, \dots t_i = t'_i.$$

`Proof.` Parts (1) and (2) follow from the definition of $R^\star$.

(3). That α and α' are the same follows from part (1). That
$$t_1 = t'_1 \in R^\star, \dots t_i = t'_i \in R^\star$$
follows from (4) of the definition of $R^\star$. `QED`

Lemma 4 *1.* $\sim$ *is an equivalence on* $\mathcal{T}$ *and it is a congruence w.r. to* $\prec$, *i.e., if* $\lambda_1 \sim \lambda'_1, \lambda_2 \sim \lambda'_2$ *and* $\lambda_1 \prec \lambda_2$ *then* $\lambda'_1 \prec \lambda'_2$.

2. $\prec$ *is transitive and antireflexive. Moreover, every descending chain in* $\prec$ *is finite (in the sense of* $\mathcal{N}$*).*

`Proof.` That $\sim$ is an equivalence follows from the condition (2) in the definition of $R^\star$. That $\sim$ is a congruence w.r. to $\prec$ follows from conditions (2) and (3). For if $R^\star$ contains the equations $\lambda_1 = \lambda'_1, \lambda_2 = \lambda'_2$ and the equation
$$\lambda_2 = s(\overline{\lambda}, \lambda_1, \overline{\lambda'}),$$
then it also contains the equation
$$\lambda'_2 = s(\overline{\lambda}, \lambda'_1, \overline{\lambda'}).$$
Transitivity of $\prec$ follows from (3) of the definition.

Antireflexivity and finite chain property follow from Lemma 3, part (2). If $\lambda \prec \lambda$ then $\lambda^\star$ is a proper subterm of itself, which is impossible, and if there exists an infinite decreasing $\prec$-chain then there exists a term with an infinite number of subterms (in the sense of $\mathcal{N}$). `QED`

1. $\lambda \in \mathcal{T}_0$ will be called *trivial*, if $R^\star$ contains the equation $\lambda = s$, for a PA_M term s.

2. λ is an *atom*, if it is $\prec$-minimal and non-trivial.

3. *A basis* $\mathcal{B} \subseteq \mathcal{T}_0$ is a set of atoms s.t. every $\sim$-equivalence class on $\mathcal{T}_0$ which contains an atom contains exactly one element from $\mathcal{B}$ (i.e., it is a set of representatives of $\sim$-classes of equivalence restricted to atoms).

Lemma 5 *1. A basis $\mathcal{B}$ exists.*

2. *If $R^\star$ contains an equation*

$$s(b_1, \dots b_n) = s'(b'_1, \dots b'_{n'}),$$

where $b_1, \dots b_n, b'_1, \dots b'_{n'}$ are in $\mathcal{B}$ then $n = n'$, b_i and b'_i are the same terms for every $i = 1, \dots n$, and the terms $s(x_1, \dots x_n)$ and $s'(x_1, \dots x_n)$ are the same.

3. *For every $\lambda \in \mathcal{T}_0$ there exists a unique s s.t. the equation $\lambda = s(\bar{b})$ is in $R^\star$, where $\bar{b} \in \mathcal{B}$. $s(\bar{b})$ will be called* the expression of λ in $\mathcal{B}$

`Proof.` (1) is trivial.

(2). *The depth* of a term s will be the length of the longest branch in s, if s is understood as a tree. s has depth zero, if s is a variable or the constant 0. The proof is by induction with respect to the sum of depths of s and s'.

If both s and s' have depth zero then the equation has one of the following forms: i) $0 = 0$, ii) $b = b'$, iii) $b = 0$, iv) $0 = b'$. i) and ii) agree with the statement of the lemma, since ii) is possible only if b and b' are the same terms (no different elements of $\mathcal{B}$ are $\sim$-equivalent). iii) and iv) are impossible, for otherwise b and b' would be trivial.

The alternative that s has depth zero and s' does not, or vice versa, is impossible. For then the equation has the form i) $b = s'(\overline{b'})$, or ii) $0 = s'(\overline{b'})$. i) contradicts the assumption that b is an atom and ii) contradicts Lemma 3.

If both s and s' have depth > 0 then, by (3) of Lemma 3, there is a PA_M function symbol α s.t. $s(b_1, \dots b_n)$ is the term $\alpha(s_1(\bar{b}_1), \dots s_i(\bar{b}_i))$ and $s'(b'_1, \dots b'_{n'})$ is the term $\alpha(s'_1(\bar{b}_1)', \dots s'_i(\bar{b}'_1))$, with $i \leq 2$. By the condition (4) of the definition of $R^\star$, $R^\star$ contains the equations

$$s_k(\bar{b}_k) = s'_k(\bar{b}'_k), \qquad k = 1, \dots i$$

The statement then follows from the inductive assumption.

(3). That every term can be thus expressed follows from the finite chain property. If λ is $\prec$-minimal then either it is trivial and $\lambda = s \in R^\star$ for some s, or it is non-trivial and $\lambda = b \in R^\star$ for some $b \in \mathcal{B}$. If λ is not minimal, use the finite chain property. Uniqueness is a consequence of part (2). `QED`

In the following Proposition, we use an expression like $\mathcal{N}_\sigma \models t_1 = t_2$, where $t_1, t_2 \in \mathcal{T}$. This requires an explanation since t_1 and t_2 can be nonstandard. However, by the definition of $\mathcal{N}_\sigma$, $\mathcal{N}_\sigma \models t_1 = t_2$, is equivalent to $\sigma^\star(t_1) = \sigma^\star(t_2)$, which is meaningful inside $\mathcal{N}$.

Proposition 6 *Let σ_0 be a function from $\mathcal{B}$ to $\mathcal{N}$. Then it can be extended to a function $\sigma : \mathcal{T}_0 \to \mathcal{N}$ s.t.*

$$\mathcal{N}_\sigma \models R^\star, \qquad \textit{and hence} \qquad \mathcal{N}_\sigma \models \pi R.$$

Proof. For $\lambda \in \mathcal{T}_0$, let $s(b_1, \dots, b_n)$ be its expression in terms of $\mathcal{B}$. We define σ by the condition

$$\sigma(\lambda) := [s](\sigma_0(b_1), \dots, \sigma_0(b_n)),$$

where $[s]$ stands for the function defined by s in $\mathcal{N}$.

Let us have $s(\lambda_1, \dots \lambda_n) = s'(\lambda'_1, \dots \lambda'_m)$ in $R^\star$. We must show that

$$(1) \qquad s(\lambda_1, \dots \lambda_n) =_{\mathcal{N}_\sigma} s'(\lambda'_1, \dots \lambda'_m)).$$

Let $\lambda_i = s_i(\bar{b}_i)$ resp. $\lambda'_i = s'_i(\bar{b}'_i)$ be the expression of $\lambda_i, i = 1, \dots n$, resp. $\lambda'_i, i = 1, \dots m$, in terms of $\mathcal{B}$. Let $\sigma^\star$ be as in the definition of $\mathcal{N}_\sigma$. Then (1) is equivalent to

$$\sigma^\star(s(\lambda_1, \dots \lambda_n)) =_{\mathcal{N}} \sigma^\star(s'(\lambda'_1, \dots \lambda'_m))).$$

By the definition of $\sigma^\star$, this is equivalent to

$$[s](\sigma(\lambda_1), \dots \sigma(\lambda_n)) =_{\mathcal{N}} [s'](\sigma(\lambda'_1), \dots \sigma(\lambda'_m))),$$

which is in turn equivalent to (2):

$$[s]([s_1](\sigma_0(\bar{b}_1)), \dots [s_n](\sigma_0((\bar{b}_n))) = [s]'([s'_1](\sigma_0((\bar{b}'_1)), \dots [s'_m](\sigma_0((\bar{b}'_m))).$$

From the definition of $R^\star$, the equation

$$s(s_1(\bar{b}_1), \dots s_n(\bar{b}_n)) = s'(s'_1(\bar{b}'_1), \dots s'_m(\bar{b}'_m))$$

is in $R^\star$ But, from part (2) of Lemma 5 the equation is then trivial and hence (2) is true. QED

7 The proof of KC

Lemma 7 *Let $\mathcal{A}$ be an infinite set of formulas. Assume that the formulas contain exactly k terms, they have a bounded number of variables and that there exists $c \in \omega$ s.t. every A in $\mathcal{A}$ is provable in c steps. Then there exists a (finite) set of equations R and an infinite $\mathcal{C} \subseteq \mathcal{A}$ s.t. every $A \in \mathcal{C}$ has a proof with the characteristic set of equations R. Moreover, if $A = A(s_1^A, \dots s_k^A)$ then s_i^A is represented by the function symbol f_i in R, for every $A \in \mathcal{C}$ and $i = 1, \dots k$.*

Proof. If formulas in $\mathcal{A}$ contain a bounded number of terms and variables, and can be proved in a bounded number of steps, then there exists $c^\star$ s.t. the formulas can be proved in c steps using at most $c^\star$ terms, and the terms are of arity at most $c^\star$. However, there are only finitely many characteristic sets of equations for such proofs (ignoring renaming of the function symbols), and hence there exists an infinite subset of $\mathcal{A}$ sharing the same characteristic set R. Similarly for the "moreover" part. QED

Lemma 8 *Let $A_1(s_1)$ and $A_2(s_2)$ be formulas s.t. the terms s_1 and s_2 are different constant terms. Assume that the formulas have proofs with the same characteristic set of equations R where s_1 and s_2 are represented by the same (constant) function symbol f. Let $\mathcal{N}$ be a model of PA_M, let $R^\star$ and a basis $\mathcal{B}$ be defined in $\mathcal{N}$. Let $s(\bar{b})$ be the expression of f in $\mathcal{B}$. Then f is non-trivial, i.e., $R^\star$ does not contain an equation of the form $f = s$.*

`Proof.` Assume the contrary. Than we have an equation $f = s$ in $R^\star$ for a PA_M term s. By Lemma 3, part (1), this implies that s_1 and s_2 are the same terms. `QED`

Theorem 9 *Kreisel's conjecture is true in PA_M.*

`Proof.` Let $A(x)$ be a formula of PA_M with one free variable x. Without loss of generality we can assume that the only term in A which contains x is x itself. (Otherwise take the formula $\exists y\ y = x \wedge A(y)$). We write A as $A(x, s_1, \dots s_j)$, where $s_1 = s_1(\overline{x_1}), \dots s_j = s_j(\overline{x_j})$ are the other terms occurring in A. Assume that for every $n \in \omega$ the formula $A(\overline{n})$ is provable in PA_M in c steps. Let us show that $\forall x A(x)$ is true in every model of PA_M.

By Lemma 7 there exist n, m, $n \neq m$ s.t. the formulas $A(\overline{n})$, $A(\overline{m})$ are provable by means of the same characteristic set of equations R, where $\overline{n}$ and $\overline{m}$ are represented by the same constant function symbol f. We can assume that R contains also the equations

$$f_{s_i}(\overline{x_i}) = s_i(\overline{x_i}), \qquad i = 1, \dots j.$$

Let $\mathcal{F}$ be the set of new function symbols occurring in R. Let $\mathcal{N}$ be a model of PA_M. We construct the set $R^\star$ and a basis $\mathcal{B}$, inside $\mathcal{N}$. Let $s(\bar{b})$ be the expression of f in terms of $\mathcal{B}$. By Lemma 8, the term f is non-trivial. Hence there exists $k \leq m, n$ s.t. $s(\bar{b})$ has the form $S^k(b)$, and so $R^\star$ contains the equation

$$f = S^k(b), \qquad b \in \mathcal{B}.$$

In particular, k is a standard number. Assume that there is $\eta \in \mathcal{N}$ s.t. $A(\eta)$ is false. Than η is non-standard, since the standard instances of $A(x)$ are true. Let us define the function $\sigma_0 : \mathcal{B} \to \mathcal{N}$ by $\sigma_0(b) := \eta - k$, and $\sigma(b') = 0$, if b' is different from b. By Proposition 6, σ_0 can be extended to $\sigma : \mathcal{T}_0 \to \mathcal{N}$ in such a way that

$$\mathcal{N}_\sigma \models \pi R.$$

Since $\mathcal{N}_\sigma \models R^\star$ then

$$\mathcal{N}_\sigma \models f = S^k(b)$$

and

$$\mathcal{N}_\sigma \models f = \eta,$$

from the definition of σ_0. Hence $N_\sigma \models A(f, f_{s_1}, \dots f_{s_j})$ iff $\mathcal{N} \models A(\eta, s_1, \dots s_j)$ and therefore

$$N_\sigma \not\models A(f, f_{s_1}, \dots f_{s_j}).$$

This contradicts the Proposition 1. `QED`

8 Applications and generalisations

If we axiomatise PA as PA_I, i.e., using the scheme of induction and schemes of identity, many unexpected propositions can be proved in a bounded number of steps. A nice example is the formula Even(x),

$$\exists y \; x = y + y,$$

asserting that x is even. For every even $n \in \omega$ Even($\overline{n}$) can be proved in a bounded number of steps. The reason is that every formula of the form

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

can be proved in a bounded number of steps. Hence there exists a formula $A(x)$ s.t.

1. the set $X := \{n \in \omega; N \models A(\overline{n})\}$ is infinite but X does not contain an infinite interval, and
2. there exists c s.t. for every $n \in X$, $A(\overline{n})$ is provable in c steps in PA_I.[2].

The following proposition shows that in PA_M such a situation is impossible. If we prove infinitely many instances of A in a bounded number of steps then A provably contains an infinite interval. Hence PA_M is quite a simple-minded theory, from the number of proof-lines perspective. It does not play tricks and it fulfils our expectations.

Note that the assumption "X is infinite" can be replaced by the assumption "X is large".

Theorem 10 *Let $A(x)$ be a formula of PA_M. Assume that there exists $c \in \omega$ and an infinite set $X \subseteq \omega$ s.t. for every $n \in X$ $A(\overline{n})$ is provable in c steps. Then there exists $k \in \omega$ s.t. $PA_M \vdash \forall x > \overline{k} A(x)$.*

`Proof.` Assume that $A(x)$ is as in the proof of Theorem 9. By Lemma 7 there exist n, m, $n < m$ s.t. the formulas $A(\overline{n})$ and $A(\overline{m})$ are provable by proofs with the same characteristic set of equations R. We can assume that R contains also the equations

$$f_{s_i}(\overline{x_i}) = s_i(\overline{x_i}), \qquad i = 1, \dots j$$

and that $\overline{n}$ and $\overline{m}$ are represented by the same constant function symbol f in R. Let $\mathcal{F}$ be the set of new function symbols occurring in R.

Let $\mathcal{N}$ be a model of PA_M. Let us show that

$$\mathcal{N} \models \forall x > \overline{m} A(x).$$

[2]Whether one can find an A with the property (2), s.t. X does not contain even an infinite arithmetical sequence is an interesting, and open, problem (see [4]).

We construct the set $R^\star$ and a basis $\mathcal{B}$, inside $\mathcal{N}$. As in Theorem 11 we can show that $R^\star$ contains the equation

$$f = S^k(b), \qquad b \in \mathcal{B},$$

for some $k \leq m$. Let $\eta \in \mathcal{N}$, $\eta > m$ be given. Let us define the function $\sigma_0 : \mathcal{B} \to \mathcal{N}$ by $\sigma_0(b) := \eta - k$ (η is bigger than k), and $\sigma(b') = 0$, if b' is different from b. By Proposition 6, σ_0 can be extended to $\sigma : \mathcal{T}_0 \to \mathcal{N}$ in such a way that

$$\mathcal{N}_\sigma \models \pi R$$

and hence $\mathcal{N}_\sigma \models A(f, f_{s_1}, \ldots f_{s_j})$, by Proposition 1. Hence also

$$\mathcal{N} \models A(\eta),$$

since $\mathcal{N}_\sigma \models f = \eta$, and the PA_M parts of $\mathcal{N}$ and $\mathcal{N}_\sigma$ are elementary equivalent.
QED

Corollary *The formulas Even*$(\overline{2n})$*,* $S^n(0) + S^m(0) = S^{n+m}(0)$ *and* $S^n(0) \cdot S^m(0) = S^{n \cdot m}(0)$ *are not provable in* PA_M *in a bounded number of steps.*

Proof. The assertion for Even$(2n)$ follows directly from the theorem. If $S^n(0) + S^m(0) = S^{n+m}(0)$ was provable in a bounded number of steps then also Even$(\overline{2n})$ would be. Similarly for the formula $S^n(0) \cdot S^m(0) = S^{n \cdot m}(0)$.
QED

The following proposition illustrates the fact that identity schemes are not provable in PA_M in a bounded number of steps.

Proposition 11 *There is no* $c \in \omega$ *s.t. for every* $n \in \omega$

$$S^n(0) = S^n(0+0)$$

is provable in PA_M *in* c *steps.*

Proof. Assume the contrary. Then by Lemma 7 there exist n, m, $n \neq m$ s.t. the formulas $S^n(0) = S^n(0+0)$ and $S^m(0) = S^m(0+0)$ are provable by proofs with the same characteristic set of equations R, where $S^n(0)$ and $S^m(0)$ are represented by a constant f_1 and $S^n(0+0)$, $S^m(0+0)$ by f_2 in R. Let $\mathcal{F}$ be the set of new function symbols occurring in R.

Let us work in the standard model N. We construct the set $R^\star$ and a basis $\mathcal{B}$. Let $s_1(\bar{b}_1)$ and $s_2(\bar{b}_2)$ be the expressions of f_1 and f_2, respectively, in terms of $\mathcal{B}$. The terms f_1 and f_2 are non-trivial. By Lemma 3, part (1), $s_1(\bar{b}_1)$ has the form

$$S^k(b_1), \qquad k \leq m, n, b_1 \in \mathcal{B}$$

and $s_2(\bar{b}_2)$ has the form

$$S^i(b_2), \qquad i \leq m, n, b_2 \in \mathcal{B},$$

where b_2 is different from b_1. Let $c_1, c_2 \in \omega$ be such that $c_1 + k \neq c_2 + i$. Let us define the function $\sigma_0 : \mathcal{B} \to N$ as follows: $\sigma_0(b_1) = c_1, \sigma_0(b_2) = c_2$ and $\sigma_0(b) = 0$ otherwise. Let us extend σ_0 to $\sigma : \mathcal{T}_0 \to N$ by means of Proposition 6. Let us have the model N_σ. As in Theorem 9, we obtain

$$N_\sigma \models \pi R,$$

and

$$N_\sigma \not\models f_1 = f_2,$$

which contradicts the Proposition 1. QED

Corollary *There is no c s.t. every instance of the identity scheme is provable in PA_M with c lines. There is no c s.t. every instance of the scheme of induction is provable in PA_M with c lines.*

Proof. The first statement is an immediate consequence of the theorem. The second follows from the fact that $x = 0 \to S^n(0) = S^n(x)$ can be proved in a bounded number of steps, by means of the induction scheme. QED

As we have mentioned in the Introduction, validity of KC in PA_I depends on the function symbols present in the axiomatisation. In PA_M this is again not the case, as we state in the last theorem.

Let L be the language $=, <, 0, S, \cdot, \alpha_1, \dots \alpha_k$, where $\alpha_1, \dots \alpha_k$ are new function or predicate symbols. Let $PA_M(L) \supseteq PA_M$ be the theory obtained by extending the minimality principle and the identity axioms to the language L. A theory T in L will be called a *simple extension of PA_M*, if T is an extension of $PA_M(L)$ by finitely many axioms.

Theorem 12 *Let T be a simple extension of PA_M. Then KC is true in T. I.e., for any formula $A(x)$ of T if there exists c s.t. for any $n \in \omega$, $A(\overline{n})$ is provable in T in c steps then $T \vdash \forall x A(x)$.*

Proof. If T is inconsistent, the statement is immediate. For a consistent T, we can see that the proof of KC for PA_M does not use any specific properties of the language of PA, or the particular axiomatisation of Q, as long as it is finite. QED

References

[1] Friedman, H.: One hundred and two problems in mathematical logic. 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] Hrubeš, P.: Theories very close to PA where Kreisel's Conjecture is false. Journal of Symbolic Logic 2, vol.1, no. 6, 123 - 137 (2007)

[4] 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)

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

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

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

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