Commentationes Mathematicae Universitatis Carolinae

Jiří Ivánek

The non-axiomatizability of the observational predicate calculus (generalized Trachtenbrot's theorems)

Commentationes Mathematicae Universitatis Carolinae, Vol. 18 (1977), No. 1, 41--57

Persistent URL: `http://dml.cz/dmlcz/105747`

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE

18,1 (1977)

THE NON-AXIOMATIZABILITY OF THE OBSERVATIONAL PREDICATE CALCULUS (GENERALIZED TRACHTENBROT'S THEOREMS)

Jiří IVÁNEK, Praha

Abstract: The observational predicate calculus (OPC) differs from the classical predicate calculus by restricting of the semantics only to finite structures. The following theorem is proved: Any OPC with at least one at least binary predicate is non-axiomatizable. The result is strengthened in various ways.

Key words: Predicate calculus, finite models, non-axiomatizability.

AMS: 02B10 Ref. Ž.: 2.663.2

Introduction. By the observational predicate calculus (OPC) we mean the predicate calculus with the usual syntax (predicates, function symbols, connectives, classical quantifiers; no equality predicate) but with the semantics modified by allowing only finite models.

B.A. Trachtenbrot constructed in [7],[8] a particular OPC with a finite number of predicates which is not (recursively) axiomatizable and the set of all non-tautologies of which (i.e. sentences negation of which has a finite model) is not separable from the set of all classical tautologies.

We generalize these results as follows:

Let L be a language containing at least one at least binary predicate. Then

(1) The set Taut(OPC) of all observational tautologies in L (i.e. the set of all sentences in L valid in all finite structures for L) is not recursively enumerable.

(2) If Taut(CPC) is the set of all classical tautologies in L (i.e. the set of all sentences in L valid in all structures for L) then Taut(CPC) and the complement of Taut(OPC) are effectively recursively inseparable.

(3) There is a primitive recursive function f associating with each (index of) a recursively enumerable theory T sound for OPC an observational tautology f(T), which is a $\forall\exists\forall\exists$-formula and is not provable from T.

We use a method of proof (suggested by P. Hájek) based on the Matiasevič's theorem ([3],[4]) about diophantine expression of recursively enumerable sets.

§ 1. <u>The theory of natural sets.</u> The theory of natural sets (TNS) has a single binary predicate letter $\in$ and no function letters and individual constants.

1.1. <u>Definition</u>.

$x \equiv y$ ... $(\forall u)(u \in x \longleftrightarrow u \in y)$ (equality)

$x \subseteq y$ ... $(\forall u)(u \in x \longrightarrow u \in y)$ (inclusion)

$\underline{O}(x)$ ... $(\forall u) \neg u \in x$ (empty set)

$S(x,y,z)$ ... $(\forall u)(u \in z \longleftrightarrow (u \in x \vee u \equiv y))$ (generalized successor)

The <u>theory of natural sets</u> has the following two axioms:

Axiom of Extensionality.

$(\forall x,y,z)\ (x \equiv y \longrightarrow (x \in z \longleftrightarrow y \in z))$.

Axiom of Strong Completeness.

$(\exists u)O(u)\ \&\ (\forall x,y,v)((x \subseteq v\ \&\ y \in v) \longrightarrow (\exists z)S(x,y,z))$.

1.2. Lemma. For any n

$$TNS \models (u_1 \in x \,\&\, \dots \,\&\, u_n \in x) \rightarrow (\exists y)(\forall u)(u \in y \leftrightarrow$$
$$\leftrightarrow (u \equiv u_1 \vee \dots \vee u \equiv u_n)).$$

1.3. Remark. In the observational predicate calculus the Axiom of Strong Completeness is (semantically) equivalent to the axiom

$$(\forall y,z)(y \in z \rightarrow (\exists x)(\neg y \in x \,\&\, S(x,y,z))).$$

1.4. Auxiliary definition. Let R be a binary relation on a class M, $a,b \in M$. We denote

$Ext_R(a) = \{c \in M;\ c\ R\ a\}$ (R-extension)

$a =_R b \Longleftrightarrow Ext_R(a) = Ext_R(b)$ (R-equality)

$a \subseteq_R b \Longleftrightarrow Ext_R(a) \subseteq Ext_R(b)$ (R-inclusion)

A subclass M' of a class M is called R-complete if $d \in M'$ implies $Ext_R(d) \subseteq M'$.

1.5. Convention. By the symbol $\underline{M}$ we shall always denote a binary relational structure $\langle M, e \rangle$.

Investigating models of TNS we shall restrict ouselves (by the Axiom of Extensionality) only to structures $\underline{M}$ with the property: $a =_e b \Longleftrightarrow a = b$ for all $a,b \in M$.

1.6. Example. Let $s_0 = \{\emptyset\}$, $s_{i+1} = s_i \cup \{a \cup \{b\};\ a,b \in s_i\}$,

$HF = \bigcup_{i=0}^{\infty} s_i$ (the class of all hereditarily finite sets).

$\underline{HF} = \langle HF, \in \rangle$ is a model of TNS; in addition, for any i $\underline{s}_i = \langle s_i, \in \rangle$ is a finite model of TNS.

1.7. Definition. A natural set is a finite model $\underline{M}$ of TNS such that the relation e is well-founded on the set M.

1.8. Example. For any i, $\underline{s}_i$ is a natural set.

1.9. Lemma. For any natural set $\underline{M}$ there exists a unique hereditarily finite $\in$-complete $\subseteq$-complete set $\widetilde{M}$ such that $\langle \widetilde{M}, \in \rangle$ is isomorphic with $\underline{M}$.

Proof. By the Isomorphism Theorem (Theorem 15B in [2]).

1.10. Definition. (Natural numbers.)

$N(x) \ldots \underline{O}(x) \vee ((\exists u)(u \in x \ \& \ \underline{O}(u)) \ \& \ (\forall v)(v \in x \longrightarrow$

$\longrightarrow (\exists w)(S(v,c,w) \ \& \ v \mp w \ \& \ (w \in x \vee w \equiv x))))$ (x is zero or x contains zero and for any element v of x the successor w of v exists and either w is an element of x or w equals to x)

$\underline{n}(x) \ldots N(x) \ \& \ (\exists u_1, \ldots, u_n)(\underset{i \neq j}{\&} \ u_i \mp u_j \ \& \ (\forall u)(u \in x \longleftrightarrow$

$\longleftrightarrow (u \equiv u_1 \vee \ldots \vee u \equiv u_n)))$. (x is the standard natural number n)

1.11. Lemma. For any $m,n \geq 1$

(i) $\models \underline{n}(x) \longleftrightarrow (\exists x_0, \ldots, x_{n-1})(\underline{O}(x_0) \ \& \ \ldots$

$\ldots \ \& \ \underline{n-1}(x_{n-1}) \& (\forall u)(u \in x \longleftrightarrow (u \equiv x_0 \vee \ldots \vee u \equiv x_{n-1})))$,

(ii) $\models (\underline{m}(x) \ \& \ \underline{m}(y)) \longrightarrow x \equiv y$,

$\models (\underline{m}(x) \ \& \ \underline{m+n}(y)) \longrightarrow x \in y$.

Proof. Let $\underline{M} \models n[a]$ for some $\underline{M}$, $a \in M$. Using the definition of the predicate N and the trivial assertion

$\models (\underline{i}(v) \ \& \ S(v,v,q) \ \& \ v \mp w) \longrightarrow \underline{i+1}(w)$ (for all i)

we successively construct an e-chain $a_0, a_1, \ldots \in M$ such that $\underline{M} \models \underline{i}[a_i]$ as long as possible. But, a contains exactly n e-different e-elements, hence this construction must be finished on the n-th step: a_0 e a,..., a_{n-1} e a, $a_n =_e a$. This implies (i). One can prove (ii) from (i) by induction.

1.12. Lemma. Let $M \models N[a]$. If for all n $\underline{M} \not\models \underline{n}[a]$, then there is an e-chain $a_0, a_1, \dots, a_n, \dots$ such that for each n we have a_n e a and $\underline{M} \models \underline{n}[a_n]$.

Proof. It is enough to repeat the construction of the proof of the Lemma 1.11, in this case this construction cannot be finished after a finite number of steps.

1.13. Lemma. Let $\underline{M} = \langle M, e \rangle$, and let M' be an e-complete part of M, $\underline{M}' = \langle M', e \restriction M' \rangle$. If for some p

$\underline{M}' \models (\exists x)\underline{p}(x)$

then for each $m \leq p$

$a \in M,\ \underline{M} \models \underline{m}[a] \Longleftrightarrow a \in M',\ \underline{M}' \models \underline{m}[a]$.

Proof. The implication " $\Longleftarrow$ " is obvious.

" $\Longrightarrow$ " Let $\underline{M} \models \underline{m}[a]$. There is a $b \in M'$ such that $\underline{M}' \models \underline{p}[b]$, hence (by " $\Longleftarrow$ ") $\underline{M} \models \underline{p}[b]$. By Lemma 1.11 (ii) we have a e b or $a =_e b$. Since M' is e-complete, we have $a \in M'$ and $a \subseteq_e b$. Finally, by Lemma 1.11 (ii) we obtain $\underline{M}' \models \underline{m}[a]$.

1.14. Definition.

$P(x,y)$ ... $(\forall u)(u \varepsilon y \leftrightarrow u \subseteq x)$ (power)

$Z(x)$... $(\exists y_1, \dots, y_6)(P(x,y_1) \,\&\, P(y_1,y_2) \,\&\, \dots \,\&\, P(y_5,y_6))$ (arithmetical securedness)

1.15. Lemma. For any $n \geq 1$

$TNS \models (Z(x) \,\&\, y \subseteq x \,\&\, (\exists u_1, \dots, u_n)(\forall u)(u \varepsilon y \leftrightarrow (u \equiv u_1 \vee \vee \dots \vee u \equiv u_n))) \longrightarrow Z(y)$.

Proof. It suffices to use repeatedly Lemma 1.2.

1.16. Definition. A natural set $\underline{M}' = \langle M', e' \rangle$ is said to be a securing set for a natural number p in a structure $\underline{M} = \langle M, e \rangle$ if

(1) $\underline{M}'$ is a substructure of $\underline{M}$ (i.e. $e' = e \restriction M'$),

(2) M' is an e-complete part of M,

(3) $M' \models (\exists x)(\underline{p}(x) \,\&\, Z(x))$.

1.17. Example. Denote $\exp(n) = 2^n$, $\exp^{i+1}(n) = \exp(\exp^i(n))$. Then $\underline{s}_{\exp^6(p)}$ is a securing set for p in $\underline{HF}$.

1.18. Theorem. Let M be a model of the theory of natural sets and let $\underline{M} \models N[a] \,\&\, Z[a]$.

(i) If $\underline{M} \models \underline{p}[a]$ for some p, then there exists a natural set $\underline{M}'$ which is a securing set for p in $\underline{M}$.

(ii) If $\underline{M} \not\models \underline{p}[a]$ for all p, then for each p there exists a natural set $\underline{M}_p$ which is a securing set for p in $\underline{M}$.

Proof. (i) By the definition of the predicate Z there are $q_1,\dots,q_6 \in M$ such that

$\underline{M} \models P[a,q_1] \,\&\, P[q_1,q_2] \,\&\, \dots \,\&\, P[q_5,q_6]$.

Since by Lemma 1.11 $Ext_e(a)$ is e-complete, it follows that $a \subseteq_e q_1$ and $Ext_e(q_1)$ is e-complete,..., $Ext_e(q_6)$ is e-complete. Let $M' = Ext_{\subseteq_e}(q_6)$, $\underline{M}' = \langle M', e \upharpoonright M' \rangle$.

$\underline{M}'$ is a finite model of TNS, because M' is a finite e-complete and $\subseteq_e$-complete part of a model of TNS. If $b_1, b_2, \dots$ is a descending e-chain in $\underline{M}'$, then clearly $b_8, b_9, \dots \in Ext_e(a)$; therefore, by Lemma 1.11 there is a $k \leq p + 8$ such that $\underline{M} \models \underline{0}[b_k]$. Hence every descending e-chain in M' is finite. Thus the relation e is well-founded on M'.

Finally one can verify

$\underline{M}' \models \underline{p}[a] \,\&\, Z[a]$,

since M' is e-complete and $a, q_1, \dots, q_6 \in M'$.

(ii) This is a consequence of Lemma 1.12, Lemma 1.15 and part (i) of the present theorem.

§ 2. Polynomial formulas. We show how to express polynomials by means of some particular formulas using the notion of securing sets.

2.1. Definition.

$U(x,y,z)$ .. $(\forall u)(u \in z \longleftrightarrow (u \in x \vee u \in y))$ (z is the union of x and y)

$D(x,y,z)$.. $(\exists v,z_1,z_2,z_3)(\underline{O}(v)$ & $S(v,x,z_1)$ & $S(z_1,y,z_2)$ & & $S(v,z_1,z_3)$ & $S(z_3,z_2,z))$ (z is the ordered pair of x and y)

$K(x,y,z)$ .. $(\forall u)(u \in z \longleftrightarrow (\exists v,w)$ $(v \in x$ & $w \in y$ & $D(v,w,u)))$ (z is the cartesian product of x and y)

$F(x,y,f)$ .. $(\exists z)(K(x,y,z)$ & $f \subseteq z$ & $(\forall v)(v \in x \longrightarrow$ $\longrightarrow (\exists w,u)(w \in y$ & $u \in f$ & $D(v,w,u)))$ & $(\forall w)(w \in y \longrightarrow$ $\longrightarrow (\exists v,u)(v \in x$ & $u \in f$ & $D(v,w,u)))$ & $(\forall v,v',w,w',u,u')$ $((u \in f$ & $u' \in f$ & $D(v,w,u)$ & $D(v',w',u')) \longrightarrow$ $\longrightarrow ((v \equiv v' \vee w \equiv w') \longrightarrow u \equiv u'))$ (f is a bijection between x and y)

$\dot{+}(x,y,z)$ .. $N(x)$ & $N(y)$ & $N(z)$ & $(\exists u,v,w,x',y',z',f)$ $(\underline{O}(u)$ & $S(u,u,v)$ & $S(u,v,w)$ & $K(v,x,x')$ & $K(w,y,y')$ & & $U(x',y',z')$ & $F(z',z,f))$ (addition; z is equinumerous with the union of disjoint copies of x and y)

$\dot{\cdot}(x,y,z)$ .. $N(x)$ & $N(y)$ & $N(z)$ & $(\exists z',f)(K(x,y,z')$ & & $F(z',z,f))$ (multiplication; z is equinumerous with the cartesian product of x and y).

2.2. Example. For any natural numbers m_1,m_2,m

$\underline{HF} \models \dot{+}[m_1,m_2,m] \Longleftrightarrow m_1 + m_2 = m$

$\underline{HF} \models \dot{\cdot}[m_1,m_2,m] \Longleftrightarrow m_1 \; m_2 = m$

The following lemma explains the role of securing sets in our construction of arithmetic.

2.3. Lemma. Let a natural set $\underline{M}'$ be a securing set for p in $\underline{M}$. If for some $a_1, a_2, a \in M$, $m_1, m_2, m \leq p$ we have $\underline{M} \models \underline{m}_1[a_1] \,\&\, \underline{m}_2[a_2] \,\&\, \underline{m}[a]$ then $a_1, a_2, a \in M'$ and

(i) $\underline{M} \models \dot{+}[a_1, a_2, a] \Longleftrightarrow \underline{M}' \models \dot{+}[a_1, a_2, a] \Longleftrightarrow m_1 + m_2 = m$,

(ii) $\underline{M} \models \dot{\cdot}[a_1, a_2, a] \Longleftrightarrow \underline{M}' \models \dot{\cdot}[a_1, a_2, a] \Longleftrightarrow m_1 \cdot m_2 = m$.

Proof. We prove (ii); one can prove (i) analogously. First, by Lemma 1.13 we have $a_1, a_2, a \in M'$ and $\underline{M}' \models \underline{m}_1[a_1] \,\&\, \underline{m}_2[a_2] \,\&\, \underline{m}[a]$. Now, we prove the first equivalence of (ii). Since $\underline{M}'$ is a securing set for p in $\underline{M}$, there are $b, q_1, \ldots, q_6 \in M'$ such that

$\underline{M}' \models \underline{p}[b] \,\&\, P[b, q_1] \,\&\, P[q_1, q_2] \,\&\, \ldots \,\&\, P[q_5, q_6]$.

If $\underline{M} \models \dot{\cdot}[a_1, a_2, a]$, then for some $a', f, g \in M$

$\underline{M} \models K[a_1, a_2, a'] \,\&\, F[a', a, f] \,\&\, K[a', a, g]$.

Since, $a_1 \subseteq_e b$, $a_2 \subseteq_e b$, we have $a' \subseteq_e q_2$ (and $a \subseteq_e b \subseteq_e q_2$); thus $f \subseteq_e q_4$ and $g \subseteq_e q_4$. If follows $a', f, g \in M'$ and

$\underline{M}' \models K[a_1, a_2, a'] \,\&\, F[a', a, f] \,\&\, K[a', a, g]$

since M' is $\subseteq_e$-complete and the quantifiers in the definitions of the predicates K, F are bounded. Similarly the converse implication holds.

By Lemma 1.9 there exists a uniquely determined hereditarily finite $\in$-complete $\subseteq$-complete set $\widetilde{M}$ such that $\langle \widetilde{M}, \in \rangle$ is isomorphic with $\underline{M}'$ (by means of some mapping f). It is easy to verify the following by induction:

$\underline{M}' \models \underline{i}[c] \Longleftrightarrow f(c) = i \in \widetilde{M}$ (for any $c \in M'$, $i = 0, 1, \ldots$).

Hence $\underline{M}' \models \dot{\cdot}[a_1, a_2, a] \Longleftrightarrow \underline{\widetilde{M}} \models \dot{\cdot}[m_1, m_2, m]$.

Finally, $\underline{\widetilde{M}}$ is a securing set for p in $\underline{HF}$, hence by the first equivalence of the assertion (ii) (which has been proved) and Example 2.2

$\underline{\widetilde{M}} \models \dot{-}[m_1,m_2,m] \Longleftrightarrow \underline{HF} \models \dot{-}[m_1,m_2,m] \Longleftrightarrow m_1 \cdot m_2 = m.$

2.4. Definition. We define (by induction) polynomial formulas with j + 2 free variables and their values - functions of j + 1 arguments on natural numbers:

(1) The following formulas

$\underline{O}(x_0,\dots,x_j,x)\dots N(x_0)$ & ... & $N(x_j)$ & $N(x)$ & $\underline{O}(x)$,

$\underline{1}(x_0,\dots,x_j,x)\dots N(x_0)$ & ... & $N(x_j)$ & $N(x)$ & $\underline{1}(x)$,

$\underline{I}_i(x_0,\dots,x_j,x)\dots N(x_0)$ & ... & $N(x_j)$ & $N(x)$ & $x \equiv x_i$

are initial polynomial formulas with values

$O(m_0,\dots,m_j) = 0$, $1(m_0,\dots,m_j) = 1$, $I_i(m_0,\dots,m_j) = m_i$ $(i = 0,1,\dots,j)$ respectively.

(2) Let π, φ be polynomial formulas with values P, Q, respectively. Then the following formulas

$\pi \oplus \varphi\ (x_0,\dots,x_j,x)..(\exists y,z)((y \varepsilon x \vee y \equiv x)\ \&\ (z \varepsilon x \vee z \equiv x)\ \&$
$\&\ \dot{+}(y,z,x)\ \&\ \pi\ (x_0,\dots,x_j,y)\ \&\ \varphi\ (x_0,\dots,x_j,z)$

$\pi \odot \varphi\ (x_0,\dots,x_j,x)..(\exists y,z)((y \varepsilon x \vee y \equiv x)\ \&\ (z \varepsilon x \vee z \equiv x)\ \&$
$\&\ \dot{-}(y,z,x)\ \&\ \pi\ (x_0,\dots,x_j,y)\ \&\ \varphi\ (x_0,\dots,x_j,z)$

are polynomial formulas with values

$P \oplus Q(m_0,\dots,m_j) = P(m_0,\dots,m_j) + Q(m_0,\dots,m_j)$,

$P \odot Q(m_0,\dots,m_j) = P(m_0,\dots,m_j) \cdot Q(m_0,\dots,m_j)$,

respectively.

(3) Each polynomial formula can be obtained from the initial polynomial formulas (1) by finite number of uses the rule (2).

2.5. Lemma. (i) If π is a polynomial formula with j + 2 free variables, then its value is a polynomial of j + 1 arguments on natural numbers.

(ii) For any polynomial P of j + 1 arguments on natural numbers there exist (many) polynomial formulas with j + 2 free variables such that their values are P.

Proof. Polynomials of j + 1 arguments on natural numbers are exactly those functions which can be obtained from the functions $0,1,I_0,\dots,I_j$ (see 2.4 (1)) by finite number of additions $\oplus$ and multiplications $\odot$ (see 2.4 (2)).

2.6. Example. If a polynomial formula π has a polynomial P as its value, then for all natural numbers $m_0,\dots,m_j,m$ we have

$\underline{\underline{HF}} \models \pi [m_0,\dots,m_j,m] \Longleftrightarrow P(m_0,m..,m_j) = m.$

2.7. Theorem. Let a natural set $\underline{M}'$ be a securing set for p in $\underline{M}$. If for some $a_0,\dots,a_j,a \in M$, $m_0,\dots,m_j,m \leq p$ we have

$\underline{M} \models \underline{m}_0 [a_0] \ \& \ \dots \ \& \ \underline{m}_j [a_j] \ \& \ \underline{m} [a]$

then $a_0,\dots,a_j,a \in M'$ and for each polynomial formula π with a value P

$\underline{M} \models \pi [a_0,\dots,a_j,a] \Longleftrightarrow \underline{M}' \models \pi [a_0,\dots,a_j,a] \Longleftrightarrow$
$\Longleftrightarrow P(m_0,\dots,m_j) = m.$

Proof. For the initial polynomial formulas the theorem trivially holds. By Lemma 2.3 the rule (2) of Definition 2.4 does not lead out of the class of polynomial formulas satisfying the theorem.

§ 3. Generalized Trachtenbrot's theorems.

3.1. Lemma (Matiasevič [3],[4]). If a set R of natural numbers is recursively enumerable, then there exist j and polynomials P, Q of j + 1 arguments on natural numbers (with natural coefficients) such that $k \in R \Longleftrightarrow P(k,m_1,\dots,m_j) = Q(k,m_1,\dots,m_j)$ for some $m_1,\dots,m_j$.

3.2. Notation. For any finite language L of the predicate calculus we denote

$Sent_L$ ... the set of all sentences (i.e. closed formulas) in L

$Taut_L(CPC)$ ... the set of all classical tautologies in L

$Taut_L(OPC)$ ... the set of all observational tautologies in L (i.e. all sentences which are true in every finite structure for the language L)

3.3. Theorem. If any finite language L of predicate calculus contains at least one at least binary predicate, then $Sent_L - Taut_L(OPC)$ and $Taut_L(CPC)$ are effectively inseparable recursively enumerable sets.

Proof. Let A, B be some effectively inseparable recursively enumerable sets of natural numbers (see Rogers [5], Th. XII, § 7.8), let a partial recursive function g realize their effective inseparability.

Assume we have a recursive sequence $\{\varphi_k;\ k = 0,1,\dots\}$ of sentences of the language L such that

(a) $k \in A \Longrightarrow \varphi_k \in Sent_L - Taut_L(OPC)$,

(b) $k \in B \Longrightarrow \varphi_k \in Taut_L(CPC)$.

Denote by W_t recursively enumerable set with the index t, by h a primitive recursive function such that h(t) is an index of the recursively enumerable set $\{k;\ \varphi_k \in W_t\}$, i.e. $W_{h(t)} = \{k;\ \varphi_k \in W_t\}$.

If for any disjoint sets W_u, W_v

$Sent_L - Taut_L(OPC) \subseteq W_u$, $Taut_L(CPC) \subseteq W_v$,
then by (a),(b) we have

$A \subseteq W_{h(u)}$, $B \subseteq W_{h(v)}$;

therefore $g(h(u),h(v)) \notin W_{h(u)} \cup W_{h(v)}$ which implies

$\varphi_{g(h(u),h(v))} \notin W_u \cup W_v$.

Hence, $Sent_L - Taut_L(OPC)$ and $Taut_L(CPC)$ are effectively inseparable sets by means of the partial recursive function

$f(u,v) = \varphi_{g(h(u),h(v))}$.

Now, we use Matiasevič's theorem, the theory of natural sets and polynomial formulas to construct formulas φ_k with the desired properties (a),(b).

By Lemma 3.1 there are polynomials P_A, Q_A of i + 1 arguments and P_B, Q_B of j + 1 arguments on natural numbers (with natural coefficients) such that

$k \in A \Longleftrightarrow P_A(k,m_1,\dots,m_i) = Q_A(k,m_1,\dots,m_i)$ for some $m_1,\dots,m_i$

$k \in B \Longleftrightarrow P_B(k,n_1,\dots,n_j) = Q_B(k,n_1,\dots,n_j)$ for some $n_1,\dots,n_j$

Choose (by Lemma 2.5) polynomial formulas π_A, $\wp_A$, π_B, $\wp_B$ with values P_A,Q_A,P_B,Q_B, respectively, and denote

$\alpha_k \dots (\exists x_0,\dots,x_i,x)(Z(x_0) \,\&\, \dots \,\&\, Z(x_i) \,\&\, Z(x) \,\&\, \underline{k}(x_0) \,\&$
$\& \,\pi_A(x_0,\dots,x_i,x) \,\&\, \wp_A(x_0,\dots,x_i,x))$

$\beta_k \dots (\exists y_0,\dots,y_j,y)(Z(y_0) \,\&\, \dots \,\&\, Z(y_1) \,\&\, Z(y) \,\&\, \underline{k}(y_0) \,\&$
$\& \,\pi_B(y_0,\dots,y_j,y) \,\&\, \wp_B(y_0,\dots,y_j,y))$

$\varphi_k \dots TNS \longrightarrow (\alpha_k \longrightarrow \beta_k)$.

Since the language L contains at least one at least binary predicate, we can assume that $\varphi_k \in Sent_L$. We wish to show (a),(b).

(a) If $k \in A$, then there exist $m_1,\dots,m_i,m$ such that $P_A(k,m_1,\dots,m_i) = m = Q_A(k,m_1,\dots,m_i)$.

By Example 1.17 there is a natural set s which is a securing set for $m' = \max(k, m_1, \ldots, m_i, m)$ in $\underline{HF}$. By Theorem 2.7

$\underline{s} \models \pi_A [k, m_1, \ldots, m_i, m] \ \& \ \rho_A [k, m_1, \ldots, m_i, m]$

hence $\underline{s} \models$ TNS & α_k.

Assume $\underline{s} \models \beta_k$, i.e. for some $b_o, \ldots, b_j, b \in S$ we have

$\underline{s} \models Z[b_o] \ \& \ \ldots \ \& \ Z[b_j] \ \& \ Z[b] \ \& \ \underline{k}[b_o] \ \&$
$\quad \& \ \pi_B [b_o, \ldots, b_j, b] \ \& \ \rho_B [b_o, \ldots, b_j, b]$.

Since s is finite, there exist $n_1, \ldots, n_j, n$ such that

$\underline{s} \models \underline{n}_1 [b_1] \ \& \ \ldots \ \& \ \underline{n}_j [b_j] \ \& \ \underline{n} [b]$.

Hence, by Theorem 2.7,

$P_B(k, n_1, \ldots, n_j) = n = Q_B(k, n_1, \ldots, n_j)$

which contradicts $k \notin B$.

(b) If $k \in B$, then there exist $n_1, \ldots, n_j, n$ such that $P_B(k, n_1, \ldots, n_j) = n = Q_B(k, n_1, \ldots, n_j)$.

Let $\underline{M}$ be a model of TNS and α_k. Then for some $a_o, \ldots, a_i$, $a \in M$

$\underline{M} \models Z[a_o] \ \& \ \ldots \ \& \ Z[a_i] \ \& \ Z[a] \ \& \ \underline{k}[a_o] \ \&$
$\quad \& \ \pi_A [a_o, \ldots, a_i, a] \ \& \ \rho_A [a_o, \ldots, a_i, a]$.

Assume $\underline{M} \models \underline{m}_1 [a_1] \ \& \ \ldots \ \& \ \underline{m}_i [a_i] \ \& \ \underline{m} [a]$

for some natural numbers $m_1, \ldots, m_i, m$.

Hence, by Theorem 1.18 (i), there exists a natural set $\underline{M}'$ which is a securing set for $m' = \max(k, m_1, \ldots, m_i, m)$ in $\underline{M}$, therefore, by Theorem 2.7,

$P_A(k, m_1, \ldots, m_i) = m = Q_A(k, m_1, \ldots, m_i)$

which contradicts $k \notin A$.

Thus, there is an $a' \in \{a_1, \ldots, a_i, a\}$ such that

$\underline{M} \models N[a'] \ \& \ Z[a']$ and $\underline{M} \not\models \underline{p}[a']$ for all p.

Hence, by Theorem 1.18 (ii), there exists a natural set $\underline{M}_p$ which is a securing set for $p = \max(k,n_1,\dots,n_j,n)$ in $\underline{M}$, and, by Lemma 1.12, there are $b_0,\dots,b_j,b \in \underline{M}$ such that

$\underline{M} \models \underline{k}[b_0] \& \underline{n}_1[b_1] \& \dots \& \underline{n}_j[b_j] \& \underline{n}[b]$.

Therefore, by Theorem 2.7

$\underline{M} \models \pi_B[b_0,\dots,b_j,b] \& \varphi_B[b_0,\dots,b_j,b]$,

i.e. $\underline{M}$ is a model of β_k.

3.4. Corollary. The observational predicate calculus with at least one at least binary predicate is not axiomatizable (i.e. the set of all its tautologies is not recursively enumerable). Consequently, the calculus in question is not decidable.

Now we shall consider complexity of formulas defined by means of the number of alternating blocks of quantifiers.

3.5. Notation. Let Fml_L be a class of all formulas of a language L. For any $F,C,D \subseteq Fml_L$ we denote

$EqF = \{\psi \in FmL_L;$ there is $\varphi \in F$ such that $\psi \leftrightarrow \varphi$ is a classical tautology$\}$,

$\forall C = Eq\{(\forall x_1,\dots,x_i)\gamma \; ; \; \gamma \in C, i = 1,2,\dots\}$,

$\neg C = Eq\{\neg\gamma \; ; \; \gamma \in C\}$,

$C \rightarrow D = Eq\{\gamma \rightarrow \delta \; ; \; \gamma \in C, \delta \in D\}$,

and analogously $\exists C$, $C \& D$, $C \vee D$, $C \leftrightarrow D$.

3.6. Definition. We construct (by induction) classes A_n, E_n $(n = 0,1,\dots)$:

$A_0 = E_0 = B = Eq\{\beta \in Fml_L; \beta$ is an open formula$\}$,

$A_{n+1} = \forall E_n$, $E_{n+1} = \exists A_n$ (notice $Fml_L = \bigcup_{n=0}^{\infty}(A_n \cup E_n)$).

We also use the following notation:

$\underbrace{AEA\dots}_{n\text{-times}}B$ for the class A_n, $\underbrace{AEA\dots}_{n\text{-times}}$-formula for its elements, and analogously for E_n.

3.7. Lemma. (1) TNS is an AEA-formula.

(2) Z(x) is an EAE-formula.

(3) N(x, n(x) (n = 0,1,...) are AEA-formulas.

(4) $\dot{+}(x,y,z)$, $\dot{\cdot}(x,y,z)$ are EAEA-formulas.

(5) Polynomial formulas are EAEA-formulas.

Proof. Proofs of all points are routine by using usual prenex operations; for example we prove (3):

The most complex subformula of N(x)

$(\forall v)(v \varepsilon x \longrightarrow (\exists w)(S(v,v,w) \mathbin{\&} v \dot{\neq} w \mathbin{\&} (w \varepsilon x \vee w \equiv x)))$

is an element of the class of formulas

$\forall(B \longrightarrow (\exists (AB \mathbin{\&} (\neg AB) \mathbin{\&} (B \vee AB)))) = \forall(B \longrightarrow EAB) = AEAB.$

The predicate $\underline{n}(x)$ is equivalent with the formula

$N(x) \mathbin{\&} (\exists u_1,\ldots,u_n)(\mathop{\&}_{i \neq j} u_i \dot{\neq} u_j \mathbin{\&} u_1 \varepsilon x \mathbin{\&} \ldots \mathbin{\&} u_n \varepsilon x \mathbin{\&}$
$\mathbin{\&} (\forall u)(u \varepsilon x \longrightarrow (u \equiv u_1 \vee \ldots \vee u \equiv u_n)))$

which is an element of the class of formulas

$AEAB \mathbin{\&} (\exists (EB \mathbin{\&} B \mathbin{\&} (\forall (B \longrightarrow AB)))) = AEAB \mathbin{\&} (\exists (EB \mathbin{\&} AB)) =$
$= AEAB \mathbin{\&} EAB = AEAB.$

3.8. Theorem. If a finite language L contains at least one at least binary predicate, then there exists a primitive recursive function f_L such that, for any index t of any recursively enumerable theory T in the observational predicate calculus with the language L such that $T \subseteq Taut_L OPC)$, $f_L(t)$ is an AEAE-formula and $f_L(t) \in Taut_L(OPC) - T$.

Proof. Assume we have a recursive sequence $\{\psi_k; k = 0,1,\ldots\}$ of sentences of the language L such that

$k \in W_k \Longleftrightarrow \psi_k \in Sent_L - Taut_L(OPC)$

for every recursive enumerable set W_k with an index k. There is a primitive recursive function h such that

$W_{h(t)} = \{k;\ \psi_k \in W_t\}$ for all $t = 0,1,\ldots$.

Hence

$$\psi_{h(t)} \in W_t \Longleftrightarrow h(t) \in W_{h(t)} \Longleftrightarrow \psi_{h(t)} \in Sent_L - Taut_L(OPC)$$

therefore, if $W_t \subseteq Taut_L(OPC)$ then $\psi_{h(t)} \in Taut_L(OPC) - W_t$.

Now we construct formulas ψ_k. Since $K = \{k;\ k \in W_k\}$ is a recursively enumerable set of natural numbers, there are (by Theorem 3.1), polynomials P, Q of i + 1 arguments such that

$k \in K \Longleftrightarrow P(k,m\ ,\ldots,m_i) = Q(k,m_1,\ldots,m_i)$ for some $m_1,\ldots,m_i$.

Choose (by Lemma 2.5) polynomial formulas π, ϱ with values P, Q, respectively, and denote

$$\varkappa_k \ldots (\exists x_0,\ldots,x_i,x)(Z(x_0) \mathbin{\&} \ldots \mathbin{\&} Z(x_i) \mathbin{\&} Z(x) \mathbin{\&} \underline{k}(x_0) \mathbin{\&}$$
$$\mathbin{\&} \pi(x_0,\ldots,x_i,x) \mathbin{\&} \varrho(x_0,\ldots,x_i,x),$$

$$\psi_k \ldots TNS \longrightarrow \neg \varkappa_k$$

It is easy to prove, similarly as in the proof of Theorem 3.3,

$k \in K \Longleftrightarrow \psi_k$ $Sent_L - Taut_L(OPC)$.

Finally, by Lemma 3.7, $\varkappa_k$ is EAEA-formula, therefore $\psi_k \in AEAB \longrightarrow (\neg EAEAB) = AEAEB$.

3.9. Remark. After [1] had been completed I was informed by P. Hájek that Professor D. Scott had proved the result 3.4 using different methods; Scott's proof has not been published.

R e f e r e n c e s

[1] IVÁNEK J.: O neaxiomatizovatelnosti observačního predikátového počtu (Master thesis, Charles University 1976).

[2] JECH T.J.: Lectures in Set Theory with Particular Emphasis on the Method of Forcing, Lecture Notes in Mathematics 217, Springer-Verlag 1971 (Russian translation: Moskva 1973).

[3] MATIASEVIČ J.V.: Diofantovost perečislimych množestv, Doklady AN SSSR (1970), 279-282.

[4] MATIASEVIČ J.V.: Diofantovo predstavlenie perečislimych predikatov, Izvestija AN SSSR, Serija matematičeskaja 35(1971), 3-30.

[5] ROGERS H.: Theory of recursive functions and effective computability, McGraw-Hill Book Company, 1967 (Russian translation: Moskva 1972).

[6] SHOENFIELD J.R.: Mathematical Logic, Addison-Wesley Publishing Company, 1967 (Russian translation: Moskva, 1975).

[7] TRACHTENBROT B.A.: Nevozmožnost algorifma dlja problemy razrešimosti na koněčnych klassach, Doklady AN SSSR 70(1950), 569-572.

[8] TRACHTENBROT B.A.: O rekursivnoj otdělimosti, Doklady AN SSSR 88(1953), 953-956.

Vysoká škola ekonomická
Katedra matematiky
Nám. G. Klimenta, 13000 Praha
Československo

(Oblatum 30.8. 1976)