Definability, decidability, complexity

Patrick Cegielski

LITP, Institut Blaise Pascal, Université Paris 12, IUT de Fontainebleau,
Route Hurtault, 77300 Fontainebleu, France

E-mail: cep@litp.ibp.fr

We survey how the definability problem in first-order logic was born and the relations between this problem and the question of decidability of logical theories. We also show present connections between definability and the important theoretical problems of computational complexity.

1. Definability

1.1. WHAT IS A DEFINITION?

1.1.1. Historical remarks

1.1.1.1. Definitions as a shortcut

When someone uses a word whose meaning is unkown to us, our first reaction, if we dare, is to ask for a definition of the underlying concept. The notion of *definition* is very widespread.

It can happen that we misuse a definition, with vicious circles as the result. For instance, the favorite quotation of Quine[1] is a definition of a "bachelor" as an "unmarried man" and an "unmarried man" as a "bachelor" [58].

Aristotle was the first to teach that it is not possible to define each word. It is necessary to distinguish between *primitive terms* and *defined terms*, with an analogy between *theorem* and *axioms*.

Pascal clarified this argumentation with many details in *De l'esprit géométrique et de l'art de persuader* (around 1657, published in 1728).

The Polish logician Lesniewski first explicited rules for the definition process in mathematical logic (see Suppes [78, Chap. 8]).

Nowadays, these definitions appear as an introduction to new symbols, or a shortcut, popularised by Bourbaki [4] in 1954:

[1] The occurrence of a name is also a reference which does not always appear with a ref. no. in the text itself, but which is given in the list of references.

> *The exclusive use of assemblies would lead to insuperable difficulties both for the printer and for the reader. For this reason, current texts use abbreviating symbols (notably words of ordinary speech) which do not belong to formal mathematics. The introduction of such symbols is the object of* definitions. *Their use* is not indispensable to the theory, *and can often lead to confusion which only a certain familiarity with the subject will enable the reader to avoid.*

1.1.1.2. Implicit definition

A definition as a shortcut does not pose any problem when it is *explicit*. Nevertheless, for many reasons, *implicit definitions* appeared. Gergonne [21] pointed out this problem in 1818. Let us consider two sorts of implicit definitions.

Fibonacci [19] defined his famous sequence $(f_n)_{n \in \mathbb{N}}$ in 1202 by

$$f_0 = 1, \ \ f_1 = 1, \ \ f_{n+2} = f_{n+1} + f_n .$$

Actually, he wrote:

> *How many pairs of rabbits will be produced in a year, beginning with a single pair, if in every month each pair bears a new pair which becomes productive from the second month on?*

and Girard [22] solved the problem in the above form in 1634. This definition is not explicit because the terms of the sequence to be defined appear in the left and right members. Dedekind [18] was the first to justify this *recursive definition* in 1888 (*The Nature and Meaning of Numbers*, § 124 and following). In fact, he justified *primitive recursive definitions*; Ackermann [1] and then Péter [53] introduced other forms of recursive definitions (complete, simultaneous, multiple, etc.).

Frege studied *definitions by abstraction* in 1884 (*Foundations of Arithmetic*, § 63–69). The *definition* of a concept is *by abstraction* when this concept is the common characteristic of several things. The original problem is to define *cardinality* of a set as the common characteristic of equipotent sets. Frege introduces the notion of *equivalence relation* and *equivalence class*, and identifies "common characteristic" with equivalence class. For instance, he clarifies in this way the notion of *direction* of straight lines in geometry, where the equivalence relation is the relation of parallelism and a direction is just an equivalence class. It is interesting to note that Frege makes such a definition clear, but does not solve the original problem because it is not possible to define cardinality with this method since the set of all sets does not exist (Russell's Paradox [72]).

1.1.1.3. Definition with limited vocabularly

The problem of presenting mathematical theories with a minimum of undefined terms and axioms greatly interested Peano's school. To reduce the total number of definitions and axioms, members of this school used unusual undefined terms and tried to find a definition for usual notions. This is not an easy task; moreover, the existence of such a definition is not assured. In 1889, for instance, Peano [51] based his treatment of Euclidean geometry upon primitive terms: "point", "betweenness" (a ternary relation) and "distance". In 1899, Pieri [54] employed two primitive terms: "point" and "motion".

In a certain way, this paper relates the formalisation and the explicitation of definitions with limited vocabulary in a general setting.

1.1.1.4. Definability in first-order logic

Tarski gave definitions of definability in 1931 and 1935 [80, 82]. He identified *primitive terms* as a more elaborate notion of a *first-order logical language*; in particular, *proper symbols* represent classical "primitive terms". He defined *definability in a theory*, completed by *definability in a structure* in 1948 [84].

1.1.2. Definition

In what follows, we suppose an acquaintance with basic notions of mathematical logic (cf., for instance, Mendelson [45]).

Let L be a logical first-order language, S a symbol (symbol of individual constant, function symbol or predicate) and $L^* = L \cup \{S\}$.

DEFINITION 1

Let $\mathcal{M}$ be an L-structure with domain M.

(1) We say that an element a of M is *definable in the stucture* $\mathcal{M}$ if and only if there exists an L-formula ϕ with one free variable such that

$$(\mathcal{M}, a) \models x = a \leftrightarrow \phi(x).$$

(2) We say that an n-ary *function* f over M is *definable in the structure* $\mathcal{M}$ if and only if there exists an L-formula ϕ with $n+1$ free variables such that

$$(\mathcal{M}, f) \models y = f(x_1,\ldots,x_n) \leftrightarrow \phi(x_1.\ldots.x_n, y).$$

(3) We say that an n-ary *relation* R over M is *definable in the structure* M if and only if there exists an L-formula ϕ with n free variables such that

$$(\mathcal{M}, R) \models R(x_1,\ldots,x_n) \leftrightarrow \phi(x_1,\ldots,x_n).$$

DEFINITION 2

Let T be a logical first-order theory in the language L^*.

(1) We say that a *symbol of individual constant* S is (*provably L-*) *definable in the theory* T if and only if there exists an L-formula ϕ with one free variable which verifies
$$T \vdash x = S \leftrightarrow \phi(x).$$

(2) The n-ary *function symbol* S is said to be *definable in the theory* T if and only if there exists an L-formula ϕ with $n+1$ free variables which verifies
$$T \vdash y = S(x_1,\ldots,x_n) \leftrightarrow \phi(x_1,\ldots,x_n, y).$$

(3) The n-ary *predicate* S is said to be *definable in the theory* T if and only if there exists an L-formula ϕ with n free variables which verifies
$$T \vdash S(x_1,\ldots,x_n) \leftrightarrow \phi(x_1,\ldots,x_n).$$

Notation

We denote by $Th(\mathcal{M})$ the theory of the $\mathcal{L}$-structure $\mathcal{M}$, that is the set of all sentences of L which are true in $\mathcal{M}$. We observe the following fact: *S is definable in the structure $\mathcal{M}$ if and only if S is definable in the theory $Th(\mathcal{M}, S)$.*

1.2. HOW TO PROVE DEFINABILITY?

Theoretically speaking, it is very easy: it is sufficient to exhibit a suitable formula ϕ.

Practically, it varies from easy to very difficult and open problems.

Examples (or exercises for courageous or motivated readers)

(1) (*Easy*) Define 0 in $(\mathbb{N}, +, =)$.

(2) (*Less easy*) Define $\leq$ in $(\mathbb{Z}, +, \times, =)$.

(3) (*Difficult*) Define the exponentiation function $(x, y) \to x^y$ in $(\mathbb{N}, +, \times, =)$.

(4) (*Really hard*) Define $\mathbb{N}$ in $(\mathbb{Q}, +, \times, =)$.

(5) (*Open problem*) Is the divisibility relation $\mid$ definable in $(\mathbb{N}, S, \perp, =)$? (As usual, $\mid$ is the divisibility relation, S is the *successor function* defined by $Sx = x + 1$, and $\perp$ is the coprimeness relation).

Answers

(1) 0 is definable by the formula $x = x + x$.

(2) We use Lagrange's famous theorem (*every integer is a sum of four squares*) to define $x \leq y$ as $\exists u, v, w, t\ (y = x + u^2 + v^2 + w^2 + t^2)$.

(3) Gödel [23] established this result in 1931 by using his famous *beta function* $\beta : \mathbb{N}^3 \to \mathbb{N}$ such that $\beta(x, y, z) = x \bmod 1 + (z+1)xy$ is the remainder in Euclidean division of x by $1 + (z+1)xy$. It is not difficult to see that this beta function is definable in $(\mathbb{N}, +, \times, =)$. The beta function verifies the following fundamental property: for every finite sequence $a_0, \ldots, a_n$ of natural numbers, u and v exist such that for $i \in [0, n]$, we have $\beta(u, v, i) = a_i$.
This property allows the following to be proved: if g is a binary function definable in $(\mathbb{N}, +, \times, =)$, then for every natural number a, the function f defined by primitive recursion without a parameter

$$\begin{cases} f(0) = a, \\ f(x+1) = g(x, f(x)), \end{cases}$$

is also definable in $(\mathbb{N}, +, \times, =)$. It is precisely definable as follows:

$$\begin{aligned} y = f(x) \leftrightarrow \exists u \exists v[\beta(u, v, 0) = a \ \wedge \ \beta(u, v, x) = y \ \wedge \\ \forall t < x \forall r \forall s[[\beta(u, v, t) = r \ \wedge \ \beta(u, v, t+1) = s] \to s = g(t, r)]], \end{aligned}$$

in other words, $\langle u, v \rangle$ is a code for the tuple $\langle f(0), f(1), \ldots, f(x) \rangle$, i.e. for a history of the computation of $f(x)$.
Then exponentiation is definable as usual from its recursive definition $x^0 = 1$ and $x^{y+1} = x^y \times x$.

(4) (*Hints*) Robinson [69] established this result is 1949. She introduced a (mysterious) relation between rational numbers, now denoted by $JR(a, b, k)$, which asserts that some particular quadratic form has a solution. Actually, $JR(a, b, k)$ is

$$\exists x, y, z[2 + a \times b \times k^2 + b \times z^2 = x^2 + a \times y^2].$$

She shows that a rational k is an integer if and only if

$$\forall a, b[[JR(a, b, 0) \ \wedge \ \forall m[JR(a, b, m) \to JR(a, b, m+1)]] \to JR(a, b, k)].$$

Her difficult and technical proof uses the quadratic reciprocity law of Gauss together with Minkowski–Hasse's theorem on rational quadratic forms (hence p-adic numbers) and Dirichlet's theorem on primes in an arithmetical progression.
Positive integers are defined as in example 2.

(5) In subsection 3.2, we shall see that, according to Wood's work [95], open problem 5 turns out to be equivalent to some conjecture of the theory of numbers.

1.3. HOW CAN WE PROVE UNDEFINABILITY?

1.3.1. Padoa's method [49]

The following proposition justifies this method, analogous to the model theoretical method to prove independence of axioms. Padoa [49] introduced this method in 1900. Tarski [81,82] in 1934 and 1935, and independently McKinsey [44] in 1935, have proved the proposition in well-defined contexts.

PROPOSITION 1

If a theory T^* in the language $L^* = L \cup \{S\}$ admits two models $\mathcal{M}$ and $\mathcal{N}$ so that

$$\begin{array}{lll} |\mathcal{M}| = |\mathcal{N}| & & \text{[same domain]} \\ \sigma^{\mathcal{M}} = \sigma^{\mathcal{N}} & \text{for } \sigma \in L & \text{[same interpretation for primitive symbols]} \\ S^{\mathcal{M}} \neq S^{\mathcal{N}} & & \text{[different interpretation for examined symbol } S\text{]} \end{array}$$

then S is not definable in the theory T^*.

Example

An order relation $\leq$ is not definable in the theory of commutative fields. Indeed, consider $(\mathbb{Q}[\sqrt{2}], \oplus, \otimes, =)$, where $\mathbb{Q}[\sqrt{2}] = \{a + b.\sqrt{2}/a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$, addition $\oplus$ and multiplication $\otimes$ being restrictions of addition and multiplication on $\mathbb{R}$. We can define two orders that are comparable with $\oplus$ and $\otimes$, namely the order $\leq$ induced by natural order on $\mathbb{R}$ and the order $\prec$ defined by

$$a + b.\sqrt{2} \prec c + d.\sqrt{2} \quad \text{if and only if } a - b.\sqrt{2} \leq c - d.\sqrt{2}.$$

Note

Beth [3] has proved a converse of this proposition in 1953, i.e.:

Let T^* be a theory in the language $L^* = L \cup \{S\}$. If for every model $\mathcal{M}$ and $\mathcal{N}$ of T^* such that

$$|\mathcal{M}| = |\mathcal{N}|, \ \sigma^{\mathcal{M}} = \sigma^{\mathcal{N}} \quad \text{for all } \sigma \in L,$$

we have $S^{\mathcal{M}} = S^{\mathcal{N}}$, then S is definable in the theory T^*.

A more classical (but equivalent) statement of this theorem is:

Let T^* and T be two theories within the respective language L^* and L (with $L^* = L \cup \{S\}$) so that T^* is an extension of T. If every model of T has at most an expansion which is a model of T^*, then S is T^*-definable.

The hypothesis of both theorems is expressed by saying that S is *implicitly definable in* T^*.

The proof of Beth's theorem is difficult (see, for instance, Monk [47] for a simpler proof given by Craig [15] in 1957). *But we do not know any historical examples of constant S definable thanks to this theorem.*

However, Beth's theorem gives a method that can be used to obtain *nonstandard* models. For instance, Beth remarks that there exists an "addition" + and two different "multiplications" $\times_1$ and $\times_2$ so that the structures $(\mathbb{N}, +, \times_1, =)$ and $(\mathbb{N}, +, \times_2, =)$ are both models of $Th(\mathbb{N}, +, \times, =)$. These multiplcations cannot be explicitly determined; this is the purpose of a famous result from Tennebaum [91], improved by McAloon [43].

1.3.2. Svenonius' method [79]

This method, based on the following proposition 2, is in fact a variation of Padoa's method.

PROPOSITION 2

If a theory T admits a model $\mathcal{M}$ with an L-automorphism which is not an S-homomorphism, then the constant S is not definable in T.

It is important to notice that such an L-automorphism is not necessarily definable.

Examples

(1) The usual order relation $\leq$ is not definable in the multiplicative structure $(\mathbb{N}, \cdot)$: consider the function which exchanges exponents of prime numbers 2 and 3 in the factorisation of a natural number in prime factors.

(2) The usual order $\leq$ is definable in the additive structure $(\mathbb{N}, +, =)$ from the following equivalence: $x \leq y \Leftrightarrow \exists z\, (x + z = y)$. We have seen that $\leq$ is definable in the integer structure $(\mathbb{Z}, +, \cdot, =)$. But $\leq$ *is not definable in the substructure* $(\mathbb{Z}, +, =)$: it is sufficient to consider the additive automorphism f defined by $f(x) = -x$ which does not respect the order relation.

(3) (Richard [62]) Multiplication of natural numbers is not definable from the divisibility relation alone, i.e. in the structure $(\mathbb{N}, |, =)$. It is not possible to find a suitable automorphism of the standard model, but we can find some in nonstandard models. Let $(M, S_M, +_M, x_M, =)$ be a nonstandard model of the complete arithmetic, i.e. the theory $Th(\mathbb{N}, S, +, x, =)$. Consider the function f so defined:

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ 2^a \cdot b & \text{if } x = 2^a \cdot b \text{ where } a \in \mathbb{N} \text{ and } b \text{ is odd}, \\ 2^{a-1} \cdot b & \text{if } x = 2^a \cdot b \text{ where } a \notin \mathbb{N} \text{ and } b \text{ is odd}. \end{cases}$$

Then f is a $|$-automorphism but does not preserve multiplication.

Note

We observe that Svenonius' method allows us to prove simply that the order relation is not definable in the theory of ordered commutative fields. We take the above example and function f on $\mathbb{Q}[\sqrt{2}]$ defined by: $f(a + b.\sqrt{2}) = a - b.\sqrt{2}$.

In fact, I have never heard of any concrete case where Padova's method is suitable, but Svenonius' method is not suitable.

1.3.3. Elimination of quantifiers

DEFINITION 3

We say that a (logical first-order) theory T within the language L *admits elimination of quantifiers* if and only if for every formula θ there exists an open formula (i.e. without occurrence of any quantifier) ϕ such that: $T \vdash \theta \leftrightarrow \phi$.

Application

If a theory T admits elimination of quantifiers and if the language L is simple enough, then it is possible to characterize the relations which are definable in the theory T.

Example (Langford [35])

The theory $Th(\mathbb{N}, S, 0, \leq)$ admits elimination of quantifiers. Thus, a subset A of $\mathbb{N}$ is definable in the structure $(\mathbb{N}, S, 0, \leq)$ (or $(\mathbb{N}, \leq)$) if and only if A ıs finite or cofinite (i.e. its complement $\mathbb{N} \backslash A$ is finite): a formula is equivalent to a Boolean combination of "$x \leq n$" or "$x \geq n$", where n is a natural number. In particular, the subset $2 \cdot \mathbb{N}$ of even numbers is not definable and consequently addition is not definable in this structure.

1.3.4. Decidability

Method

If $\mathcal{M}$ is an L-structure such that the theory $Th(\mathcal{M})$ is decidable and the theory $Th(\mathcal{M}, S)$ is not decidable, then S is not definable in $\mathcal{M}$.

Examples

(1) Presburger [57] proved in 1929 that the theory of addition of natural numbers, i.e. $Th(\mathbb{N}, +, =)$, is decidable. Church [14] and Turing [92] proved in 1936 that the theory $Th(\mathbb{N}, +, \times, =)$ is not decidable, hence *multiplication is not definable in* $(\mathbb{N}, +, =)$.

(2) Skolem [75] showed in 1930 that the theory of multiplication of natural numbers, i.e. $Th(\mathbb{N}, \times, =)$, is decidable, hence *addition is not definable in* $(\mathbb{N}, \times, =)$.

(3) Tarski [84,85] proved in 1929 (published in 1948) that the theory of real-closed fields is the theory $Th(\mathbb{R}, +, \cdot, \leq)$ and is decidable, hence *the subset* $\mathbb{N}$ *is not definable in the structure* $(\mathbb{R}, +, \cdot, \leq)$.

(4) Goodstein [25] in 1975 used the undecidability of Diophantine equations (see section 3.1) and the decidability of equations of a special form to show that the positive difference $x \dot{-} y$ [$= \sup(0, x - y)$] is not a member of the class of functions generated by composition from the four functions $x + y$, $x \cdot y$, $1 \dot{-} x$ and $x - 1$.

1.3.5. Diagonalisation

The method of diagonalisation was first invented and applied by Cantor [7] in 1891 to prove that the set $\mathbb{R}$ is not denumerable. Its applications may be very tricky.

Example

The set of *arithmetical theorems* is the set of true sentences of the structure $(\mathbb{N}, S, +, \times, =)$. We may consider this set as a formal language (note the difference to a logical language) Λ on the alphabet:

$$\Sigma = \{v, {}_0, {}_1, \neg, \wedge, \vee, \forall, \exists, (,), S, +, \times, =\},$$

with variables v_n written as the concatenation of v and the binary expansion of n (using ${}_0$ and ${}_1$).

Let Σ^+ be the set of nonempty words over Σ and let $ng : \Sigma^+ \to \mathbb{N}^*$ any reasonable surjective map such as the usual *Gödel numbering*[2].

Let A be the subset of $\mathbb{N}$ defined by $\{ng(\theta)/\theta$ is an arithmetical theorem$\}$.

[2] Let $g : \Sigma \to \mathbb{N}^*$ be such that

$$g(v) = 1,\ g(0) = 2,\ g(1) = 3,\ g(\neg) = 4, g(\wedge) = 5,\ g(\vee) = 6,\ g(\forall) = 7,\ g(\exists) = 8,$$
$$g() = 9,\ g() = 10,\ g(S) = 11,\ g(+) = 12,\ g(\times) = 13,\ g(=) = 14,$$

and let $ng : \Sigma^+ \to \mathbb{N}^*$ be so that

$$ng(w_1 \ldots w_n) = p_1^{g(w_1)} \times \ldots \times p_n^{g(w_n)},$$

where p_i is the ith prime number and $p_0 = 2$ (*Gödel numbering*).

THEOREM (Gödel [24], Tarski [83])

The subset A is not definable in the structure $(\mathbb{N}, S, +, \times, =)$.

Proof

The main idea is to use an argument of diagonalisation. Set

$B = \{n \in \mathbb{N}/n$ is the Gödel numbering of a unary $\{S, +, \times, =\}$-formula $\phi(x)$ and $\phi(n)$ is an arithmetical theorem$\}$.

It is easy to prove that the set

$\{n \in \mathbb{N}/n$ is the Gödel numbering of a unary $\{S, +, \times, =\}$-formula $\phi(x)\}$

is definable in the structure $(\mathbb{N}, S, \times, =)$. Suppose that A is definable. Then B is also definable. So there exists a unary $\{S, +, \times, =\}$-formula $\varphi(x)$ so that

$$n \in B \Leftrightarrow \neg\varphi(n) \text{ is an arithmetical theorem.}$$

We shall see below the interest in considering a negative formula.

Let m be the Gödel numbering of the formula $\varphi(x)$. If $\varphi(m)$ is an arithmetical theorem, then $m \in B$, hence $\neg\varphi(m)$ is also an arithmetical theorem, a contradiction. If $\neg\varphi(m)$ is an arithmetical theorem, then $\varphi(m)$ is not an arithmetical theorem, hence $m \notin B$, so $\varphi(m)$ is not an arithmetical theorem, contradicting the fact that the theory $Th(\mathbb{N}, S, +, \times, =)$ is complete.

The contradictions show that A is not definable. □

1.3.6. Complexity

Principle

This method is an improvement on those mentioned in section 1.3.4. Let us replace the *decidable/undecidable* dichotomy by *easy/hard*. Let $\mathcal{M}$ be an L-structure so that the theory $Th(\mathcal{M})$ has complexity measure m and the theory $Th(\mathcal{M}, S)$ has complexity measure m' greater than m. If no extension by definition of $\mathcal{M}$ can have the complexity measure m', then S is not definable in $\mathcal{M}$.

Example (Cegielski et al [13])

The binary relation *SUPEQUI* of equipotency between sets of prime divisors of positive integers is not definable within the divisibility lattice of positive integers.

This theorem is proved using the following lemmas:

(1) $Th(\mathbb{N}, +, =)$ can be emulated in $Th(\mathbb{N}, \mid, SUPEQUI, =)$;

(2) *Th*($\mathbb{N}$, +, =) has a complexity of at least *ATIME-ALT*($2^{2^{cn}}$, n), while *Th*($\mathbb{N}$, $|$, =) has a complexity of at most *ATIME-ALT*(2^{cn^3}, n).

We remind the reader of some complexity notions which are useful to appreciate this example. Concerning these questions of complexity, we take as a reference the book by Bovet and Crescenzi published in 1994 [5]. It seems that the most adequate model of a theoretical machine for measuring complexities of logical theories is the *alternating Turing machine.* It allows, in particular, the exact complexity class of a given logical theory to be obtained.

An *alternating Turing machine* (abbreviated to *ATM*) is a generalization of the well-known nondeterministic Turing machine (abbreviated to *NDM*), where each state is an ordered pair (q', $\forall$) or (q'', $\exists$). We say that the quantifier C is the *color* of the ordered pair (q, C). A *tree of computations* and a *subtree of a tree of computations* have the same definitions as in the *NDM* case. Every vertex of such a subtree of labeled 1 or 0 in the following way: first of all, every leaf (of this subtree) is labeled 1 if and only if this leaf is accepting; secondly, any interior node (of this subtree including the root) is labeled 1 if and only if either its color in $\exists$ and one of its sons is labeled 1 or its color is $\forall$ and all of its sons are labeled 1. A *subtree* is *accepting* if and only if its root is labeled 1.

Let T and A be mappings from $\mathbb{N}$ to $\mathbb{N}$. Let $|w|$ be the length of the word w of a given formal language. A formal language A belongs to the complexity class *ATIME-ALT*($T(n)$, $A(n)$) if and only if there exists an *ATM* recognizing Λ such that, for every w in Λ, there exists an accepting subtree with depth at most $T(|w|)$ and such that every path linking the root to an accepting leaf presents at most $A(|w|)$ alternations of colors.

Now take a (decidable) theory T within a logical language L. Its associated *formal language* Λ is the set of words in the alphabet $\{v, {}_{0,1}, \neg, \wedge, \vee, \forall, \exists, (\,,), =\} \cup L$ which are the theorems of T. It must be emphasized that *numerating* of variables v_1, v_1, v_{10},... is given by their binary expansion. We say that T belongs to the complexity class *ATIME-ALT*($T(n)$, $A(n)$) if and only if Λ does.

2. Definability and decidability

2.1. IMPORTANCE OF DECIDABILITY

Hilbert raises the supreme question: are mathematics decidable? Actually, Hilbert has raised this problem, his tenth, for Diophantine equations in 1900 [30]. The French logician Herbrand did not hesitate to call this problem the "fundamental problem of mathematics" in 1931 [29].

There are two difficulties in answering Hilbert's question. The first problem is to know what mathematics is. The second problem is to carefully define what a decidable class of problems (or a decidable theory) is.

Reflections by logicians such as Frege, Peano, Russell, Skolem and Hilbert have given answers to the first question. In fact, mathematics is a certain logical first-order theory; perhaps the Zermelo–Fraenkel set theory with some supplementary axioms. The French group of mathematicians known as Bourbaki popularized this idea. Of course, for the working mathematician, mathematics remains rather a naive logical second-order theory than a formalized first-order logical theory, but the formalized point of view is necessary for studies on mathematics itself.

Turing [92] answered the second question in 1936 by defining his famous model of abstract machines. His answer is somehow universal according to the so-called Church thesis [14] claiming that every notion of computability is reducible to Turing's machines.

In 1936, Church and Turing proved that mathematics is not decidable.

Still, this does not close the problem. We have an essentially unique method to prove that a theory is undecidable, while to prove decidability methods are as old as mathematics. Hence, it is important to continue to bring out special theories on specific domains and to see if they are decidable or not.

2.2. ESSENTIAL UNDECIDABILITY

At this step of the paper, we know only undecidable theory. How can we prove the undecidability of other theories? Essentially, this can be done thanks to a particular theory Q and to the notion of *essential undecidability* due to Tarski in 1949.

DEFINITION 4

Let T and T^* be (logical first-order) theories within respective languages L and L^*.

A *suitable formula* for a constant S of L^* is a formula ϕ^S of L with, respectively, one free variable if S is an individual constant, $n + 1$ free variables if S is an n-ary function symbol f, and n free variables if S is an n-ary predicate R.

Let be given suitable formulas for every constant of L^* and a formula $N(x)$ for the domain. The *translation* of a formula θ of L^* is the formula $trans(\theta)$ of L obtained by replacing every constant S of L^* by ϕ^S and every quantification by a quantification relative to N.

The theory T^* is *definable in the theory* T if such a translation of T^* in T exists such that for every sentence θ of L^*, if $T^* \vdash \theta$ then $T \vdash trans(\theta)$.

DEFINITION 5

A theory T^* within language L^* is *essentially undecidable* iff every theory T' within this language L^* extension of T^* is inconsistent or undecidable.

Fact

If a theory T^* is essentially undecidable, then every theory T in which T^* is definable is undecidable.

Important note

Essentially undecidable is different from *undecidable*. The theory of fields is undecidable but not essentially undecidable. This is so because the theory of real-closed fields is decidable (Tarski, 1929, published in 1948 [85]).

PROPOSITION 3 (Rosser [71])

Peano arithmetic *PA* is essentially undecidable.

COROLLARY

Zermelo set theory Z and the theory of the structure $(\mathbb{Z}, +, \times, =)$ are (essentially) undecidable.

Proof

It is well-known that *PA* is definable in Z. Since $\leq$ is definable in $Th(\mathbb{Z}, +, \times, =)$, Peano arithmetic is also definable in this theory. □

The theory *PA* is too special to obtain many results of undecidability. The following result is an improvement of proposition 3.

DEFINITION 6

The *theory Q* is the theory with language $(S, +, \times, 0, =)$ with the following axioms:

(1) $\forall x[Sx \neq 0]$; (2) $\forall x, y[Sx = Sy \rightarrow x = y]$;

(3) $\forall x[x \neq 0 \rightarrow \exists y[x = Sy]]$; (4) $\forall x[x + 0 = x]$;

(5) $\forall x, y[x + Sy = S(x + y)]$; (6) $\forall x[x \times 0 = 0]$;

(7) $\forall x, y[x \times Sy = x \times y + x]$.

Note

The theory Q is a finitely axiomatized theory, without induction axioms.

PROPOSITION 4 (Robinson [70])

The theory Q is essentially undecidable.

COROLLARY

The theories of rings, of commutative rings and of ordered rings are undecidable.

Proof

The theory Q is easily definable in the theory of discreted ordered rings (i.e. there exists an element 1 so that: $\forall x[0 \leq x \leq 1 \rightarrow [x = 0 \vee x = 1]]$): it is sufficient to lay $x \geq 0$ for $N(x)$ and $x + 1$ for Sx. Hence, this theory is undecidable. The undecidability of the former theories follows, because a finite set of axioms is sufficient to obtain the latter theory. Let us suppose, for instance, that the theory of rings is decidable. Let $A_1, \ldots, A_n$ be the axioms to add to this theory to obtain the theory of discreted ordered rings. A sentence θ is a theorem of the theory of discreted ordered rings if and only if $(A_1 \wedge \ldots \wedge A_n) \rightarrow \theta$ is a theorem of the theory of rings. Hence, the theory of discreted ordered rings would be decidable, a contradiction. □

2.3. DEFINABILITY HUNTERS

Introduction

Previous results have induced many people to try to find languages L such that structure $(\mathbb{N}, S, +, \times, =)$ is definable in $(\mathbb{N}, L)$. Tarski and Robinson are the most prominent names. Richard in France and Woods in England (now in his native country Australia) are their most important successors.

We give some samples of their results.

PROPOSITION 5 (Tarski, in Robinson [69])

Theories of $(\mathbb{N}, \leq, \times)$ and $(\mathbb{N}, S, \times, =)$ are undecidable.

Proof

It is sufficient to define the addition. This is obtained by observing that for $a, b \neq 0$, we have

$$c = a + b \Leftrightarrow (1 + a \times c) \times (1 + b \times c) = 1 + c^2 \times (1 + a \times b). \qquad \square$$

PROPOSITION 6 (Robinson [69])

Theories of $(\mathbb{N}, S, |, =)$ and $(\mathbb{Q}, +, \times, =)$ are undecidable.

Proof

The second result is a consequence of section 1.2, example 4. For the first result, using proposition 5, it is sufficient to define the multiplication. This is obtained by proving that for $a, b \neq 0$, we have

$$c = a \times b \Leftrightarrow [\forall x(a|x \wedge b|x \wedge c|x) \vee \forall x, y, m((a \perp x \wedge b \perp y \wedge c \perp x \wedge$$
$$c \perp y \wedge x \perp y \wedge a \times x \equiv -1[m] \wedge b \times y \equiv -1[m]) \Rightarrow x \times y \times c \equiv 1[m])],$$

where $x \perp y$ and $x \equiv y[z]$, respectively, means x and y are coprime and x is congruent to y modulo z. It is interesting to note that the proof uses Dirichlet's theorem, ensuring the existence of primes in an arithmetical progression. □

COROLLARY

The theories of fields, of commutative fields and of ordered fields are undecidable.

Proof

Let $Nat(x)$ be Robinson's formula defining $\mathbb{N}$ in $(\mathbb{Q}, +, \times, =)$ (example 4 of section 1.2). We define a theory T in the language $(S, +, \times, \leq, 0)$ with

- axioms for ordered commutative fields;
- axioms for Q restricted to Nat, for instance, $\forall x[Nat(x) \rightarrow Sx \neq 0]$.

This theory is consistent because $(\mathbb{Q}, +1, +, \times, \leq, 0)$ is a model. This theory is undecidable because the theory Q is essentially undecidable. If a theory is decidable, then a theory obtained by adding a *finite* set of axioms is also decidable (see the proof of the corollary of proposition 4). Hence, the cited theories are undecidable. □

Note

All the above undecidable theories have a language with at least two proper symbols.

PROPOSITION 7 (Pabion and Richard [48], Richard [60], Richard [66, chap. IV])

The theories of structures $(\mathbb{N}, \exp, =)$, $(\mathbb{N}, \beta, =)$, $(\mathbb{N}, (x)_y \neq 0, =)$ are undecidable, where exp denotes the exponentiation function $\exp(x, y) = x^y$, and the symbol β denotes the ternary beta function of Gödel, and $(x)_y$ denotes the p_y-adic valuation of x.

Proof

For the first result, we use the following properties:

$$z = x + y \Leftrightarrow \forall t[\exp(t, z) = \exp(\exp(t, x), y)],$$

$$z = x \times y \Leftrightarrow \forall t\, \forall u[\exp(t, \exp(u, z)) = \exp(\exp(t, \exp(u, x)), \exp(u, y))]. \qquad □$$

PROPOSITION 8 (Woods [95])

The functions + and × and the identity relation = are definable in the structure $(\mathbb{N}, <, \perp)$.

PROPOSITION 9 (Richard [61])

The predicate $\mathbb{P}$ of being a prime is definable in the structure without an identity relation $(\mathbb{N}, S, \perp)$.

Richard has obtained many other results. (His main papers are listed in the references below.)

2.4. EMULATION AND ISOMORPHIC RE-INTERPRETATION

We have seen that a good method to prove the undecidability of a theory is to define an essentially undecidable theory within. Richard [60] generalized in 1981 this method with his notion of an *isomorphic re-interpretation property*, and later, in 1992 (published in 1996), Cegielski et al. [13] with the notion of *emulation*.

DEFINITION 7

A *structure* $(A, c_1, \ldots, c_n)$ is *emulatable in a structure* $\mathcal{M}$, with domain M, iff there exists a structure $(B, d_1, \ldots, d_n, \equiv)$ isomorphic to $(A, c_1, \ldots, c_n, =)$, where B is a subset of M, $\equiv$ a binary relation on A, and $B, d_1, \ldots, d_n, \equiv$ are $\mathcal{M}$-definable.

A *structure* $\mathcal{M}$ *has the isomorphic re-interpretation property* if the structure $(\mathbb{N}, +, \times, =)$ is emulatable in $\mathcal{M}$.

Note

If a structure with undecidable theory is emulatable in a structure $\mathcal{M}$, then $Th(\mathcal{M})$ is undecidable. In particular, $Th(\mathcal{M})$ is undecidable if $\mathcal{M}$ has the isomorphic re-interpretation property.

Richard used the isomorphic re-interpretation property to prove that many structures $\mathcal{M}$ with domain $\mathbb{N}$ have an undecidable theory (see Richard [63,65,68]); in particular, structures for which it is an open problem (related to Erdös–Wood's conjecture, stated below) to know if + and × are definable in $\mathcal{M}$. In fact, the isomorphic re-interpretation property does not imply definability of + and ×:

PROPOSITION 10 (Cegielski and Richard [12] and Cegielski et al. [13])

Let π be the canonical enumeration of prime numbers: $\pi(0) = 2$, $\pi(1) = 3$, $\pi(2) = 5$, $\pi(3) = 7$, $\pi(4) = 11, \ldots$. Let $\tilde{\pi}$ be the following enumeration: $\tilde{\pi}(0) = 5$, $\tilde{\pi}(1) = 7$, $\tilde{\pi}(2) = 3$, $\tilde{\pi}(3) = 2$, $\tilde{\pi}(x) = \pi(x)$ for every $x \geq 4$. The structure $(\mathrm{N}, \tilde{\pi}, \times, =)$ has the isomorphic re-interpretation property but + is not definable in this structure.

3. Definability and number theory

It is not rare that connections exists between new problems in theoretical computer science and old conjectures in number theory. Here, we speak of two such connections, namely about the famous Hilbert's tenth problem and about some open problems in number theory.

3.1. THE SOLUTION OF HILBERT'S TENTH PROBLEM

3.1.1. The problem

Hilbert's tenth problem appears in the famous list which Hilbert [30] gave in his 1900 address before the Second International Congress of Mathematicians.

Many problems in number theory do have the form of a *Diophantine equation*

$$P(x_1,\ldots,x_n) = Q(x_1,\ldots,x_n)$$

to solve, where P and Q are polynomials with non-negative integer coefficients, and solutions are n-tuples $\langle x_1,\ldots,x_n\rangle$ of non-negative integers.

It is easy to solve such an equation if P and Q are of degree one, by using the Euclidean Algorithm, the Bézout identity, and the Chinese Remainder Theorem. An algorithm to solve a Diophantine equation when P and Q are degree two exists, but the proof is very difficult; we have Legendre and Gauss to thank for solving, at the beginning of the nineteenth century, the case $n = 2$, and Siegel [73] for the general case in 1972. The case $n = 2$ with polynomials P and Q of respective degrees 3 and 2 has been studied extensively; it is related to *elliptic curves*; we do not know (in 1996) if an algorithm exists for this case.

The famous *last theorem of Fermat* is a particular (a priori schema of) such problems, namely to solve $x^n + y^n = z^n$ for a given natural number n.

Hilbert's tenth problem asks for an algorithm to determine whether or not a given Diophantine equation has a solution. Matiyasevich [37] proved in 1970 that *there is no such algorithm*. Hence, he negatively answers the tenth Hilbert question by positively solving a problem of definability.

3.1.2. Solution of the initial problem

Introduction

The problem is solved in three steps. The first one is to define what a *decidable set* (of positive integers) is. The second step is to find an undecidable set W. The third step is to prove that if Hilbert's tenth problem were decidable, then W would be decidable.

Apprehension of the notion of a decidable set

Many mathematicians proposed in the same year (1936) a definition of the notion of a *decidable set*. These definitions are equivalent. The reference is a definition by Turing's machine. Nowadays, the clearest definition uses the notion of a computer program: a *set A* is *decidable* if, and only if, a program P exists with an input n of integer type output of which is "yes" if $n \in A$ and "no" is $n \notin A$.

Existence of an undecidable set

Turing [92] proves in 1936 the existence of an undeciable set by an argument of diagonalisation. A result of the famous 1931 paper by Gödel [23] can be seen as a relation between undecidable sets and sets definable in $\mathbb{N}$ by a certain type of formulas of the language of Peano arithmetic.

DEFINITION 8

(1) The *language of Peano arithmetic* is the first-order logical language $L(PA)$, proper symbols of which are $S, +, \times, 0, \leq$, where S is a unary functional symbol, + and × binary functional symbols, 0 an individual constant symbol and $\leq$ a binary predicate.

(2) The set of Δ_0-*formulas* is recursively defined by

- atomic formulas are Δ_0-formulas;
- Boolean combinations of Δ_0-formulas are Δ_0-formulas;
- *bounded quantifications* of Δ_0-formulas are Δ_0-formulas, i.e. if ϕ is a Δ_0-formula, then $(\forall x \leq y)\ \phi$ and $(\exists x \leq y)\ \phi$ are Δ_0-formulas.

(3) For $n \in \mathbb{N}^*$, a Σ_n-*formula* (respectively, Π_n-*formula*) is of the form

$$\exists x_1\ \forall x_2\ \exists x_3 \ldots Q_n x_n \phi \quad [\text{respectively, } \forall x_1\ \exists x_2\ \forall x_3 \ldots Q_n x_n \phi],$$

where matrix ϕ is a Δ_0-formula, and Q_i the convenient quantifier according to the parity of n.

Note

Every $L(PA)$-formula is PA-equivalent to a Σ_n-formula and to a Π_p-formula for some $n, p \in \mathbb{N}$.

PROPOSITION 11 (Gödel [23])

A subset A of $\mathbb{N}$ is decidable if and only if there are a unary Σ_1-formula $\phi(x)$ and a unary Π_1-formula $\varphi(x)$ such that

$$x \in A \Leftrightarrow \phi(x) \Leftrightarrow \varphi(x).$$

PROPOSITION 12 (Turing [92])

There is a subset W of $\mathbb{N}$ such that

(1) W is not decidable;

(2) there is a Σ_1-formula $\phi(x)$ such that: $x \in W \Leftrightarrow \phi(x)$.

The last condition is expressed by saying that W is a recursively enumerable set.

Third step

Diophantine formulas are the special case of Σ_1-formulas where the matrix is not a Δ_0-formula but a polynomial formula. The works of Robinson, Putnam and Davis culminated in Matiyasevich's theorem (known as the *MDRP theorem* to insist on the four contributors).

DEFINITION 9

An n-ary *polynomial formula* has the following form:

$$P(x_1,\ldots,x_n) = Q(x_1,\ldots,x_n),$$

with $P, Q \in \mathbb{N}[X_1,\ldots,X_n]$.

An n-ary *Diophantine formula* has the following form:

$$\exists x_{n+1} \ldots \exists x_p \; \phi(x_1,\ldots,x_n, x_{n+1},\ldots,x_p),$$

where ϕ is a polynomial formula.

PROPOSITION 12 (MDRP's theorem (1970); Matiyasevich [38])

Every Σ_1-formula is equivalent to a Diophantine formula.

Proof

Davis [17] presented a very clear proof of this theorem in his 1973 paper. The book published in 1993 by Matiyasevich [41] gives several proofs of the main theorem and of many improvements. □

COROLLARY

Hilbert's tenth problem is undecidable.

Proof

Proposition 13 ensures there is a polynomial formula ϕ such that

$$x \in W \Leftrightarrow \exists x_1 \ldots \exists x_p \; \phi(x_1,\ldots,x_p, x).$$

If Hilbert's tenth problem is decidable, then for any integer n we can decide if $\phi(x_1,\ldots,x_p, n)$ admits an integer solution or not; hence, the membership of n to W is decidable. But this contradicts proposition 12. □

3.1.3. New problems

Introduction

MDRP's theorem does not solve a classical problem of definability. Indeed, we are here searching for a definition with an $\mathfrak{I}$-formula and not with an $L(PA)$-formula, $\mathfrak{I}$ being a subclass of $L(PA)$-formulas.

This leads to a very interesting generalization of the classical problem of definability. We shall again see the interest of this generalization for the study of computational complexity in section 4. We give the formal definition, for instance, in the case of a relation definable in a structure.

DEFINITION 10

Let $\mathcal{M}$ and $\mathfrak{I}$ be, respectively, an L-structure with domain M and a subclass of the set of L-formulas. We say that an n-ary *relation* R over M is *$\mathfrak{I}$-definable in the structure* $\mathcal{M}$ if and only if there exists a formula ϕ in the class $\mathfrak{I}$ with n free variables such that

$$(\mathcal{M}, R) \models R(x_1,\ldots,x_n) \Leftrightarrow \phi(x_1,\ldots,x_n).$$

The main result to solve the Hilbert tenth problem is to prove that every arithmetical relation which is Σ_1-definable is also Diophantine-definable. Speculative problems arise about the complexity of universal Diophantine relations. The book by Matiyasevich [41] contains an excellent survey of results for these problems.

A first measure of complexity: degree of the polynomial prefix

The *degree* of a Diophantine equation is the maximum of the degree of the two polynomials occurring in the formula.

PROPOSITION 14

There is no algorithm to determine whether or not a given Diophantine equation of degree 4 has a solution.

Proof

It is a consequence of the corollary of MDRP's theorem and of the following result of Skolem [76]: every Diophantine formula is arithmetically equivalent to a Diophantine equation with the same set of free variables and a degree 4 polynomial prefix. Indeed, the number of bound variables increases. Section 1.2 of Matiyasevich [41] contains a complete proof. □

As we have already said, there exists an algorithm for degree 2 (Siegel [73]) and it is an open problem for degree 3.

A second measure of complexity: number of unknowns

The *number of unknowns* of a Diophantine formula is the number of quantifiers or, equivalently, the number of bound variables.

PROPOSITION 15

There is no algorithm to determine whether or not a given Diophantine equation with 9 unknowns has a solution.

Proof

Matiyasevich [38] proves the analog of this theorem for about 200 unknowns. Matiyasevich and Robinson [42] improve this result to 13 unknowns. The bound of 9 unknowns was announced by Matiyasevich [39] and presented with full details by Jones [31]. □

Both measures

Jones [31] gives the following couples $\langle n, p\rangle$, with degree n and p unknowns, for undecidability:

$$\langle 4,58\rangle, \langle 8,38\rangle, \langle 12,32\rangle, \langle 16,29\rangle, \langle 20,28\rangle, \langle 24,26\rangle, \langle 28,25\rangle, \langle 36,24\rangle, \langle 96,21\rangle, \langle 2668,19\rangle,$$

$$\langle 2\times 10^5, 14\rangle, \langle 6.6\times 10^{43}, 13\rangle, \langle 1.3\times 10^{44}, 12\rangle, \langle 4.6\times 10^{44}, 11\rangle,$$

$$\langle 8.6\times 10^{44}, 10\rangle, \langle 1.6\times 10^{45}, 9\rangle.$$

Polynomial representation of prime numbers

An easy by-product of the MDRP theorem is the existence of some polynomial with integer coefficients $P(x_1,\ldots,x_n)$ such that $P(\mathbb{N}^n) \cap \mathbb{N}$ is exactly the set of (positive) prime numbers. A classical Euler proposition ensures this polynomial has a negative value for some natural number values.

Many researchers were interested in knowing how few variables are sufficient in such a polynomial representing primes. The first upper bound of 24 variables was obtained by Matiyasevich [38]; the bound was reduced to 21 variables in the appendix to the English translation. Later, the bound was further reduced to 12 variables by Wada [94] and by Jones et al. [32]. The present record is 10 variables, achieved by Matiyasevich [40], then Jones [31].

3.2. ERDÖS-WOODS' CONJECTURE

Robinson [69] proved in 1949 that the theory of $(\mathbb{N}, S, |, =)$ is undecidable. She asks many related questions: is PA axiomatizable in the language $\{S, |, =\}$ in a natural number? Is $Th(\mathbb{N}, S, \perp, =)$ decidable? Is the divisibility $|$ definable in $(\mathbb{N}, S, \perp, =)$?

We have seen how Woods and Richard have answered the second question. I have given a response to the first question (Cegielski [10, chap. V]). Let us see how Woods has answered the third question.

The problem of characterizing a number by its prime divisors and those of its successors (a universally bounded number of successors) interested Zsigmondy (1892), Størmer (1897), Birkhoff and Vandiver (1904), and Erdös (1980). Guy [27] gave in 1981 the following denomination, where $\mathbb{P}$ is the set of prime numbers:

EW (Erdös–Woods' conjecture)

$$\exists k \in \mathbb{N}, \forall x, y \in \mathbb{N}[x = y \Leftrightarrow (\forall i < k)(\forall p \in \mathbb{P})[p | x + i \Leftrightarrow p | y + i]].$$

Woods [95] showed in 1981 a surprising relation between this conjecture and definability.

PROPOSITION 16

We have the following equivalences:

(EW) $\Leftrightarrow$ Divisibility relation $|$ is definable in the structure $(\mathbb{N}, S, \perp, =)$
$\Leftrightarrow$ Identity relation $=$ is definable in the structure $(\mathbb{N}, S, \perp)$.

(EW) remains a conjecture, but we have many related results, for instance:

PROPOSITION 17 (Grigorieff and Richard [26])

The identity relation $=$ and the multiplication $\times$ are definable in the structure $(\mathbb{N}, S, \perp, R)$, where R is any of the following functions or relations:

- the relation x *is a quadratic residue of prime number* p;
- the relation y *is a power of* x;
- the multiplication $(p, x) \mapsto p \times x$ restricted to prime numbers p and natural numbers x;
- or the addition $(p, x) \mapsto p + x$ *restricted* to prime numbers p and natural numbers x.

4. Definability and complexity

Buss [6] initiated in 1985 a new way to deal with great computational complexity problems (like the famous problem $P \overset{?}{=} NP$). He reduces these problems to problems of definability in weak arithmetics.

We shall begin with some more classical notions.

4.1. AN ARITHMETICAL HIERARCHY

Turing machines are well known. Subsets of $\mathbb{N}$ are identified through formal languages, for instance in unary alphabet $\{1\}$.

DEFINITION 11

Let A be a subset of $\mathbb{N}$.

We say that A is Σ_1 (or *recursively enumerable*) if and only if it is accepted by a Turing machine.

For $n \in \mathbb{N}^*$, a subset A is Σ_{n+1} if and only if it is accepted by a Turing machine with an oracle which is a Σ_n-subset.

A subset A is Π_n iff its complement $\mathbb{N} \setminus A$ is Σ_n.

A subset A is Δ_n iff it is both Σ_n and Π_n.

PROPOSITION 18 (negation theorem; Church [14])

A subset A of $\mathbb{N}$ is decidable (i.e. recursive) if and only if both A and its complement $\bar{A}$ are recursively enumerable.

PROPOSITION 19 (Kleene [33])

We have the following strict inclusions for $n \in \mathbb{N}^*$:

$$\Delta_n \subset \Sigma_n \subset \Delta_{n+1}; \ \Delta_n \subset \Pi_n \subset \Delta_{n+1}.$$

PROPOSITION 20 (Post [56])

A subset A of $\mathbb{N}$ is Σ_n (respectively, Π_n) if and only if it is definable by a Σ_n-formula (respectively, a Π_n-formula).

4.2. A POLYNOMIAL HIERARCHY

DEFINITION 12

Let C be a class of subsets of $\mathbb{N}$. We say a subset A of $\mathbb{N}$ belongs to the class $P(C)$ (respectively, $NP(C)$) iff A is accepted in polynomial time by a deterministic (respectively, nondeterministic) Turing machine with an oracle in C. A subset A belongs to $co\text{-}NP(C)$ iff its complement $\mathbb{N} \setminus A$ belongs to $NP(C)$.

We define

$$\begin{array}{ll} \Sigma_0^p = \Pi_0^p = \Delta_0^p = P & \text{as } P(\emptyset), \\ NP & \text{as } NP(\emptyset), \\ co\text{-}NP & \text{as } co\text{-}NP(\emptyset), \end{array}$$

$$\Sigma^p_{k+1} \qquad \text{as } NP(\Sigma^p_k),$$

$$\Delta^p_{k+1} \qquad \text{as } P(\Sigma^p_k),$$

and

$$\Pi^p_{k+1} \qquad \text{as } co\text{-}NP(\Sigma^p_k).$$

(p and P are for *polynomial*).

PROPOSITION 21 (Meyer and Stockmeyer [46])

We have the following inclusions for $k \in \mathbb{N}$:

$$\Delta^p_k \subseteq \Sigma^p_k \subseteq \Delta^p_{k+1}, \quad \Delta^p_k \subseteq \Pi^p_k \subseteq \Delta^p_{k+1}.$$

Note

These notions lead to some famous open problems in computational complexity theory, for instance: Does this (pseudo-) hierarchy collapse?

$$P \overset{?}{=} NP,$$

$$P \overset{?}{=} NP \cap co\text{-}NP.$$

DEFINITION 13

The *language of bounded arithmetic* is the first-order logical language $L(BA)$, proper symbols of which are $S, +, ., 0, \lfloor ./2 \rfloor, |.|, .\#., =, \leq$, where naturai interpretations in $\mathbb{N}$ for $\lfloor x/2 \rfloor$, $|x|$, $x \# y$ are, respectively, the *integral part* of x divided by 2, the *length of* x, i.e. $\lceil \log_2(x+1) \rceil$, and $2^{|x| \cdot |y|}$.

In this language, the *bounded quantifiers* are the classical $(\forall x \leq t)$ and $(\exists x \leq t)$, and the *sharply bounded quantifiers* are $(\forall x \leq |t|)$ and $(\exists x \leq |t|)$, where t is a term.

We define Σ^b_k*-formulas* (respectively, Π^b_k*-formulas*) with no other quantifier than bounded quantifiers, with k alternations of bounded quantifiers which are not sharply bounded quantifiers, and beginning with an existential (respectively, universal) bounded quantifier.

The b in exponential position signifies that the considered class consists of *bounded* formulas. A formal definition of Σ^b_k-formulas and Π^b_k-formulas is analogous to the above definition 7 for Σ_n-formulas and Π_n-formulas, but is more intricate.

PROPOSITION 22 (Stockmeyer [77], Wrathall [96])

A subset A of $\mathbb{N}$ is Σ^p_k (respectively Π^p_k) if and only if it is definable by a Σ^b_k-formula (respectively a Π^b_k-formula).

Note

The collapsing of the polynomial hierarchy is equivalent to a quantifier elimination. Now, this has been reduced to a logical problem studied since 1920. This gives new tools with which one can attack some of the fundamental questions of theoretical computer science. It is a field of application for definability topics.

4.3. BOUNDED ARITHMETICS

Buss introduced *bounded arithmetics*, analogous to Peano arithmetic with a richer language $L(BA)$, more basic axioms and restricted axiom schemata of induction, and studied its connections to the polynomial hierarchy.

DEFINITION 14

BASIC is a theory in language $L(BA)$ with 32 axioms, analogous to theory Q for language $L(PA)$ and setting natural relations between objects of the structure $(\mathbb{N}, L(BA))$. The choice of these axioms is not very important.

For a fixed class $\mathfrak{I}$ of formulas of $L(BA)$, the schemata of axioms denoted by $\mathfrak{I}$-*PIND* is the set of all sentences

$$[\phi(0) \wedge \forall x[\phi(\lfloor x/2 \rfloor) \Rightarrow \phi(x)]] \Rightarrow \forall x\, \phi(x),$$

where the formula ϕ belongs to $\mathfrak{I}$.

The theory S_2^i is the theory language of which is $L(BA)$ and axioms are *BASIC* and Σ_i^b-*PIND*.

The theory T_b^i is the theory language of which is $L(BA)$ and axioms are *BASIC* and Δ_b^{i+1}-*PIND*, i.e. for Σ_{i+1}^b-formulas $\phi(x)$ and $\psi(x)$, we have:

$$\forall x[\phi(x) \Leftrightarrow \neg\, \psi(x)] \Rightarrow [[\phi(0) \;\wedge \forall x[\phi(\lfloor x/2 \rfloor) \Rightarrow \phi(x)]] \Rightarrow \forall x\, \phi(x)].$$

PROPOSITION 23 (Buss [6])

(1) A function $f: \mathbb{N} \rightarrow \mathbb{N}$ is *polynomial time computable* if and only if there is a binary Σ_1^b-formula $\phi(x, y)$ and a term $t(x)$ in $L(BA)$ such that

$$S_2^1 \vdash \forall x\, \exists y \leq t(x)\, \phi(x, y),$$

$$S_2^1 \vdash \forall x\, !y\, \phi(x, y),$$

$$\forall n \in \mathbb{N}\, \phi(n, f(n)).$$

(2) If A is a Σ_i^p-subset (*defined by the formula* $\phi(x)$) and a Π_i^p-subset (*defined by the formula* $\varphi(x)$) and if

$$S_2^i \vdash \forall x[\phi(x) \leftrightarrow \varphi(x)],$$

then A is a Δ_i^p-subset.

COROLLARY

If a subset A is S_2^1-provably $NP \cap co\text{-}NP$, then it is P.

Consequences

This corollary of the Buss result provides a very promising method to prove that a set A is P. It is sufficient to prove it is both NP and $co\text{-}NP$ in some theory; practically, if we know it is both NP and $co\text{-}NP$, then the method used to prove this result certainly is not too complex and the demonstration can be formalized in such a theory.

However, up to now, no set A has been shown in P by such a method. The reason is that bounded arithmetics are still not widely developed. For instance we do not know which classical theorems of number theory are true in these weak arithmetics. The length of proof of any classical theorem increases greatly with weakness of the arithmetical theory in which this proof takes place. For instance, a proof of Dirichlet's theorem on primes in arithmetical sequences in primitive recursive arithmetic *PRA* is one hundred pages long (Cegielski [11]). Such results would help to apply Buss' theorem.

Work around Buss' theory is being developed. For instance, we have the following result:

PROPOSITION 24 (Krajíček [34])

If $T_2^0 = S_2^1$, then $\Sigma_2^p = \Pi_2^p$.

Consequence

This result gives us a promising method to show that the polynomial hierarchy collapses.

Hájek and Pudlak [28] compile analogous results of relations between provability and computational complexity in chapter 5 of their book published in 1993.

4.4. POLYNOMIAL TIME UNIFORMIZATION PROPERTY

Ressayre [59] introduced in 1990 a notion to generalize an aspect of proposition 23(2).

DEFINITION 15

An arithmetical theory (i.e. with a definable predicate to be interpreted by the set of natural integers) T has the *polynomial time uniformization property* iff for any binary relation R in NP definable in the standard model by a formula ϕ such that

$$T \vdash (\forall x)(\exists y \leq t(x))\ \phi(x, y),$$

there is a function f in P such that $\forall n \in \mathbb{N}\ \phi(n, f(n))$.

The theory S_2^1 has the polynomial time uniformization property.

PROPOSITION 25 (Ressayre [59])

A certain recursively presented subtheory *RCEI* (explicitly given) of the theory $Th(\mathbb{R}, +, \times, \leq, x \mapsto 2^x, \mathbb{N})$ has the polynomial time uniformization property.

Proof of the result uses nonstandard methods. No direct proof is known.

We are in the same situation as with Buss' result. We have a promising method, but at the present time we do not have a sufficient knowledge of the number theoretic properties of this theory to obtain concrete results in computational complexity. Just a (difficult) negative result exists: Boughattas has proved that this result does not yield factorization in polynomial time.

References

[1] W. Ackermann, Zum Hilbertschen Aufbau der reellen Zahlen, Math. Annalen 99(1928)118–133; English translation in [93] pp. 493–507.

[2] Aristotle, *Posterior Analytics*, II, 3, 90 b 9 and 91 a 12; English translation in *The Works of Aristotle*, 11 Vols., ed. W.D. Ross (Clarendon Press, Oxford, 1931); French translation by Jean Tricot, *Les Seconds Analytiques* (Vrin, 1947).

[3] E.W. Beth, On Padoa's method in the theory of definition, Koningklijke Nederlandse Akademie van Wetenschappen, *Proc. of the Section of Sciences*, Vol. 56 (1953), series A, Mathematical Sciences, pp. 330–339; also in Indagationes Mathematicae, Vol. 15, pp. 330–339.

[4] Bourbaki, *Théorie des Ensembles* (Hermann, 1954) EI 14–15; English translation *Theory of Sets* (Hermann and Addison–Wesley, 1968) p. 16.

[5] D.P. Bovet and P. Crescenzi, *Introduction to the Theory of Complexity* (Prentice–Hall, 1994) p. XI + 282.

[6] S. Buss, Studies in proof theory, *Bounded Arithmetic* (Bibliopolis, Napoli, 1986) p. 221.

[7] G. Cantor, Über eine elementare Frage der Mannigfaltigkeitslehere, *Jahresbericht der Deutschen Mathematiker-Vereinigung*, Vol. 1 (1891) pp. 75–78; also in [8], pp. 278–280.

[8] G. Cantor, *Gesammelte Abhandlungen, Mathematischen und Philosophischen Inhalts* (Springer, 1932, p. VII + 486 (reprinted: Hidesheim, Olms, 1966); (2nd ed., 1980) p. VII + 489.

[9] P. Cegielski, L'article fondateur de Julia Robinson sur la définissabilité, quarante ans après, LITP No. 90.41, Université Paris VII (1990) p. 15; also chap. VIII of [10].

[10] P. Cegielski, Thèse de doctorat d'état, LITP No. 90.77, Institut Blaise Pascal, Paris (1990) p. 310.

[11] P. Cegielski, Le théorème de Dirichlet est finitiste, LITP 92.40 (1992) p. 131.

[12] P. Cegielski and D. Richard, Indécidabilité de la théorie des entiers naturels munis d'une énumération des premiers et de la divisibilité, Compte Rend. Acad. Sci. Paris 315, Série I (1992)1431–1434.

[13] P. Cegielski, Y. Matiyasevich and D. Richard, Definability and decidability issues in extensions of the integers with the divisibility predicate, to appear in J. Symb. Logic.

[14] A. Church, An unsolvable problem of elementary number theory, Amer. J. Math. 58(1936) 345–363; reprinted in [16], pp. 88–107.

[15] W. Craig, Review of two papers by E.W. Beth and of three papers by K.J.J. Hintikka, J. Symb. Logic 22 (1957).

[16] M. Davis (ed.), *The Undecidable: Basic Papers on Undecidable Propositions, Unsolvable Problems and Computable Functions* (Raven Press, New York, 1965).

[17] M. Davis, Hilbert's tenth problem is unsolvable, Amer. Math. Monthly 80(1973)233–269; also in *Computability and Unsolvability* (2nd ed., Dover, 1982) pp. 199–235.

[18] R. Dedekind, *Was sind und was sollen die Zahlen?*, 1888 (Braunschweig, 6th ed., 1930); also in *Dedekind Gesammelte Mathematische Werke*, Vol. III (Braunschweig, 1932) pp. 335–391. English translation by W.W. Beman, The nature and meaning of numbers, in: *Essays on the Theory of Numbers* (Open Court, Chicago, 1901, reed: Dover, 1963) p. 115; French translation by J. Milner and H. Sinaceur, *Les Nombres, que sont-ils et à quoi servent-ils?*, La bibliothèque d'Ornicar? (Diffusion Seuil, s.d., 1979) p. 142.

[19] Fibonacci, in fact Leonardo Pisa, *Liber abaci* (1202), Bullettino di Bibliografia e di Storia delle Scienze Mathematiche e Fisiche (Baldassare Boncompagni, Rome, 1868–1887) 20 Vols; no English or French translation. Partial English translation by D.J. Struik, *A Source Book in Mathematics 1200–1800*, (Princeton University Press, 1969) pp. 2–3.

[20] G. Frege, *Die Grundlagen der Arithmetik* (Breslau, 1884); English translation: *The Foundations of Arithmetic* (Blackwell, Oxford, 1950); French trannslation by C. Imbert, *Les Fondements de l'Arithmétique* (Seuil, 1969, deuxième édition s.d., 1979) p. 235.

[21] J. Gergonne, Essai sur la théorie des définitions, Ann. de Math. Pures et Appliq. (1818) 1–35.

[22] A. Girard, *L'Arithmétique de Simon Stevin de Bruges* (Leyde, 1634) p. 677.

[23] K. Gödel, Über formal unentscheidbare Sätze der *Principia mathematica* und verwandter Systeme I, Monatshefte für Mathematik und Physik 38(1931)173–198; English translation in [93] and in *Collected Works*, Vol. 1 (Oxford University Press, 1986); French translation in *Le Théorème de Gödel* (Seuil, 1989) p. 184.

[24] K. Gödel, Letter to Zermelo dated 12 October 1932, edited by Grattan-Guinness in Historia Mathematica 6(1979)294–304.

[25] R.L. Goodstein, Hilbert's tenth problem and the independence of recursive difference, J. London Math. Soc., 2nd Series, 10(1975)175–176.

[26] S. Grigorieff and D. Richard, Contribution à l'étude d'une conjecture de théorie des nombres par le codage ZBV, L'Enseignement Mathématique 35(1989)125–189.

[27] R. Guy, *Unsolved Problems in Number Theory* (Springer, 1981) pp. 25–28.

[28] P. Hájek and P. Pudlak, *Metamathematics of First-Order Arithmetic* (Springer,1993) p. 460.

[29] J. Herbrand, Sur le problème fondamental de la logique mathématique, Sprawozdania z posiedzen Towarzystwa Naukowego Warszawskiego wydzial, III, 24(1931)12–56; reprinted in *Écrits Logiques*, ed. Jean van Heijenoort (P.U.F., 1968); English translation in *Logical Writings* (Reidel, 1971).

[30] D. Hilbert, Mathematische Probleme, *Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen* (1990) pp. 253–297; French translation with emendations and additions in *Compte Rendu du Deuxième Congrès Int. des Mathématiciens*, Paris, 12 August, 1900 (Gauthier-Villars, 1902) pp. 58–114, réédition GABBAY (1992); English translation in Bull. Amer. Math. Soc. 8(1902)437–479, reprinted in *Mathematical Developments Arising from Hilbert Problems*, ed. Browder, *Proc. Symposia in Pure Mathematics*, Vol. 28 (American Mathematical Society, 1976) pp. 1–34.

[31] J.P. Jones, Universal Diophantine equation, J. Symb. Logic 47(1982)549–571.

[32] J.P. Jones, D. Sato, H. Wada and D. Wiens, Diophantine representation of the set of prime numbers, Amer. Math. Monthly 83(1976)449–464.

[33] S.C. Kleene, Recursive predicates and quantifiers, Trans. Amer. Math. Soc. 53(1943)41–73; reprinted in [16] pp. 254–287.

[34] J. Krajíček, P. Pudlák and G. Takeuti, Bounded arithmetic and the polynomial hierarchy, Ann. Pure and Appl. Logic 52(1991). [Result communicated by Professor Pudlák at *Secondes Journées sur les Arithmétiques Faibles*, held at LITP, Université Paris VII, December 1990; no proceedings published to date.]

[35] C.H. Langford, Some theorems on deducibility, Ann. Math 28, 2nd Series (1926–1927) 16–40; 459–471.

[36] S. Leśniewski, Über die Definitionen der sagenannten Theorie der Deduktion, C.R. Soc. Sci. Lett. Varsovie Cl: 3(1932)289–309; *The Collected Works* (University of Notre Dame Press, 1967).

[37] Y. Matiyasevich, Diophantine representation of recursively enumerable predicates, *Actes du Congrès Int. des Mathématiciens*, Nice, 1970, Vol. 1 (Gauthier-Villars, 1971) pp. 235–238.

[38] Y. Matiyasevich, Diofantovo predstavlenie mnozhestva prostykh chisel, Dokl. Akad. Nauk SSSR 196(1971)770–773; English translation: Diophantine representation of the set of prime numbers, Sov. Math. Dokl. 12(1971)249–254.

[39] Y. Matiyasevich, Some purely mathematical results inspired by mathematical logic, *Logic, Foundations of Mathematics and Computability*, Vol. 1, *Proc. 5th Int. Congres of Logic, Methodology and Philosophy of Sciences* (Reidel, 1977) pp. 121–127.

[40] Y. Matiyasevich, Prostye chisla perechislyayutya polinomon ot 10 peremennykh, Zap. Nauchn. Sem. Leningrad Otdel. Mat. Inst. Steklov 68(1977)62–82; English translation: Primes are nonnegative values of a polynomial in 10 variables, J. Sov. Math. 15(1981)33–44.

[41] Y. Matiyasevich, *Desyataya problema Gil'berta* [in Russian] (Nauka, 1993) p. 223; English translation: *Hilbert's Tenth Problem* (MIT Press, 1993) chap. XXII and p. 264; French translation: *Le Dixième Problème de Hilbert* (Masson, 1995).

[42] Y. Matiyasevich and J. Robinson, Reduction of an arbitrary Diophantine equation to one in 13 unknowns, Acta Arithm. 27(1975)521–553.

[43] K. McAloon, On the complexity of models of arithmetic, J. Symb. Logic 47(1982)403–415.

[44] J.C.C. McKinsey, On the independence of undefined ideas, Bull. Amer. Math. Soc. 41(1935) 291–297.

[45] E. Mendelson, *Introduction to Mathematical Logic* (Van Nostrand, 1964); (2nd ed., 1979) p. VIII + 328; (Wadsworth, CA, 1987, 3rd ed.) p. X + 342.

[46] A.R. Meyer and L.J. Stockmeyer, The equivalence problem for regular expression with squaring requires exponential time, *Proc. 13th IEEE Symp. on Switching and Automata Theory* (1973) pp. 125–129.

[47] J.D. Monk, *Mathematical Logic* (Springer, 1976) p. X + 531.

[48] J.-F. Pabion and D. Richard, Synonymy and re-interpretation for some sublanguages of Peano arithmetic, in: *Open Days in Model Theory and Set Theory*, eds. W. Guzicki, W. Marek, A. Pelc and C. Rauszer, Proc. of a conference held September 1981 at Jadwisin, near Warsaw, Poland (Leeds University Press).

[49] A. Padoa, Essai d'une théorie algébrique des nombres entiers, précédé d'une introduction logique à une théorie déductive quelconque, *Bibliothèque du Congrès International de Philosophie*, Paris 1900, Vol. 3 (Armand Colin, 1901) pp. 309–365; partial English translation in [93] pp. 118–123.

[50] B. Pascal, De l'esprit géométrique et de l'art de persuader, numerous editions, for instance in *Oeuvres Complètes*, ed. Lafuma (Seuil, Paris, 1963) pp. 348–359; English translation: Provincial Letters, Pensées, Scientific Treatise, Encylopædia Britannica "Great Books of the Western World" (1952).

[51] G. Peano, *I Principii di Geometria* (Bocca, Turin, 1889) p. 40.

[52] G. Peano, Le definizioni in matematica, *Periodico di Matematiche* (1921) pp. 175–189; English translation: *Selected Works of Giuseppe Peano*, translated and edited by H.C. Kennedy (University of Toronto Press, 1973) p. XI + 249.

[53] R. Péter, *Rekursive Functionnen* (Verlag der Ungarischen Akademie der Wissenschaften, Budapest, 1951); English translation: *Recursive Functions* (Academic Press, 1967).

[54] M. Pieri, Delle geometria elementaire come sistema ipotetico-deduttivo: monografia del punto e del mote, *Memorie della Reale Accademia delle Scienze di Torino* (1899).

[55] B. Poizat, *Cours de Théorie des Modèles* (Nur al-mantiq wal-ma'rifah, Diffusion Offilib, 1985) p. 584.

[56] E.L. Post, Degrees of recursive unsolvability, Bull. Amer. Math. Soc. 54(1948)641–642.

[57] M. Presburger, Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, *Sprawozdanie z I Kongresu matematyków krajów slowiańskich, Warsawa, 1929*, Warsaw (1930) pp. 92–101; English translation and study by J. Zygmunt in History and Philosophy of Logic. 12(1991)211–233.

[58] W.V.O. Quine, Vagaries of definition, Ann. New York Acad. Sci. (1973); also in *The Ways of Paradox and Other Essays*, 2nd ed. (Harvard University Press, 1976) p. X + 335.

[59] J.-P. Ressayre, Polynomial time uniformization and nonstandard methods, *Secondes Journées sur les Arithmétiques Faibles*, LITP, Université Paris VII (1990). Also in this volume, Ann. of Math. and AI 16(1996).

[60] D. Richard, De la structure additive à la saturation des modèles de Peano et à la classification des sous-langages de l'Arithmétique, *Model Theory and Arithmetic*, eds. Berline, K. McAloon and J.-P. Ressayre, Lecture Notes in Mathematics No. 890 (Springer, 1981) pp. 270–296.

[61] D. Richard, La théorie sans égalité du successeur et de la coprimarité des entiers naturels est indécidable. Le prédicat de primarité est définissable dans le langage de cette théorie, C.R. Acad. Sci. Paris 294, série I (1982)143–145.

[62] D. Richard (1984), first publication in [9].

[63] D. Richard, The arithmetics as theories of two orders, Ann. Discr. Math. 23(1984)287–312.

[64] D. Richard, All arithmetical sets of powers of primes are first-order definable in terms of the successor function and the coprimeness predicate, Discr. Math. 53(1985)221–247.

[65] D. Richard, Answer to a problem raised by J. Robinson: The arithmetic of positive or negative integers is definable from successor and divisibility, J. Symb. Logic 50(1985)135–143.

[66] D. Richard, Définissabilité en arithmétique et méthode de codage ZBV appliquée à langages avec successuer et coprimarité, Thèse d'État, Université Lyon-I, No. 85-16 (1985).

[67] D. Richard, Equivalence of some questions in mathematical logic with some conjectures in number theory, *Number Theory and Applications*, ed. R. Mollin, NATO ASI Series, Series C: Math. Phys. Sci., Vol. 265 (1988) pp. 529–545.

[68] D. Richard, Definability in terms of the successor function and the coprimeness predicate in the set of arbitrary integers, J. Symb. Logic 54(1989)1253–1287.

[69] J. Robinson, Definability and decision problems in arithmetic, J. Symb. Logic 14(1949)98–114.

[70] R. Robinson, An essentially undecidable axiom system, *Proc. Int. Congress of Mathematics*, Vol. 1 (1950) pp. 729–730.

[71] J.B. Rosser, Extensions of some theorems of Gödel and Church, J. Symb. Logic 1(1936)87–91; reprinted in [16] pp. 230–235.

[72] B. Russel, Letter to Frege (1902), first published in [93] pp. 124–125; French translation in *Logique et Fondements des Mathématiques: Anthologie (1850–1914)*, eds. F. Rivenc and P. de Rouilhan (Payot, 1992) p. 447.

[73] C.L. Siegel, Zur Theorie der quadratischen Formen, *Nachrichten der Akademie der Wissenschaften in Göttingen II Mathematisch-Physikalische Klass* (1972) pp. 21–46.

[74] T. Skolem, Begründung der elementaren Arithmetik durch die rekurrierende Dekweise ohne Anwendung scheinbarer Veränderlichen mit unendlicem Ausdehnungsbereich, Videnskabselskabets Skrifter, I. Matematisk-naturvidenskabelig Klasse No. 6 (1923) pp. 1–38; reprinted in *Selected Works in Logic* (Universitetsforlaget, Oslo, 1970) pp. 153–188; English translation in [93] pp. 302–333.

[75] T. Skolem, Über einige satzfunktionen in der arithmetik, Videnskabselskabet i Kristiana Skriften, 1 Klasse, No. 7, Oslo (1930); reprinted in *Selected Works in Logic*, ed. J.E. Fenstad (Universitetsforlag, Oslo, 1970) pp. 281–306; French translation by C. Richard (1979).

[76] T. Skolem, Über die Nicht-charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar vieler Aussagen mit ausschliessich Zahlenvariablen, Fundamenta Mathematica 23(1934) 150–161.

[77] L.J. Stockmeyer, The polynomial-time hierarchy, Theor. Comp. Sci. 3(1977)1–22.

[78] P. Suppes, *Introduction to Logic* (Van Nostrand, 1957) p. XVIII + 312; (reed: Dover, 1993).

[79] L. Svenonius, A theorem on permutations in models, Theoria 25(1959)173–179.

[80] A. Tarski, Sur les ensembles définissables de nombres réels I, Fundamenta Mathematica 17(1931) 210–239; reprinted in [88], Vol. 1, chap. VI; [89], Vol. 1, pp. 517–548.

[81] A. Tarski, Z badán metodologicznych nad definiowalnoscą terminów, Przegl ąd filozoficzny 37(1934)438–460.

[82] A. Tarski, Einige methodologische Untersuchungen über die Definierbarkeit der Begriffe, Erkenntnis 5(1935)80–100; reprinted in [89], Vol. 3, pp. 637–659; French translation in [88], Vol. 2, chap. X; English translation in [87], pp. 296–319.

[83] A. Tarski, Der Wahrheisbegriff in den formalisierten Sprachen, Studia Philosophica 1(1936) 261–405; English translation in [87] pp. 157–278; French translation in [88] chap. VIII, pp. 159–269. [Interesting result for us in section 5, theorem 1].

[84] A. Tarski, A problem concerning the notion of definability, J. Symb. Logic. 13(1948)107–111; reprinted in [89], Vol. 3, pp. 163–170 (this is an abstract of [80], second part, unpublished).

[85] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*, 2nd Ed. (Rand Corporation, Santa Monica, 1948) p. III + 60; (Calfornia University Press, Berkeley, 1951) p. III + 63; French translation of the 1st edition (unpublished) in [88], Vol. 2, pp. 203–242.

[86] A. Tarski, On essential undecidability, J. Symb. Logic 14(1949)75–76.

[87] A. Tarski, *Logic, Semantics, Metamathematics* (Oxford University Press, 1956).

[88] A. Tarski, *Logique, Sémantique, Métamathématique 1923–1944* (Armand Colin, Paris) Vol. 1 (1972), Vol. 2 (1974).

[89] A. Tarski, *Collected Papers*, eds. Givant and McKenzie (Birkhäuser, 1986) 4 Vols.

[90] A. Tarski, A. Mostowski and R. Robinson, *Undecidable Theories* (North-Holland, 1953).

[91] S. Tennenbaum, Non-archimedean models for arithmetic, *Notices of the Amer. Math. Soc.* (1959) p. 270.

[92] A.M. Turing, On computable numbers, with an application to the Entscheidungsproblem, *Proc. London Math. Soc.* Vol. 42 (1936) pp. 230–265; erratum, ibid., Vol. 43, pp. 544–546; reprinted in [16] pp. 116–154; French translation in: A. Turing and J.-Y. Girard, *La Machine de Turing* (Seuil, 1995) pp. 47–102.

[93] J. Van Heijenoort (ed.), *From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931* (Harvard University Press, 1967; 4th printing: 1981, corrected).

[94] H. Wada, Polynomial representations of prime numbers (in Japanese), Sûgaku 27(1975) 160–161.

[95] A. Woods, Some problems in logic and number theory and their connections, Thesis, University of Manchester (1981).

[96] C. Wrathall, Complete sets and the polynomial time hierarchy, Theor. Comp. Sci. 3(1977)23–33.

[97] E. Zermelo, Untersuchungen über die Grundlagen der Mengenlehre, Math. Annal. 65, pp. 261–281; English translation: Investigations in the foundations of set theory I, in: *From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931*, ed. J. Van Heijenoort (Harvard University Press, 1967; 4th printing, 1981, corrected) pp. 199–215; French translation: Recherches sur les fondements de la théorie des ensembles, in: *Logique et Fondements des Mathématiques* (Payot, 1992) pp. 367–378.