Introduction

Patrick Cégielski
LACL, EA 4219
Université Paris-Est Créteil
IUT de Sénart-Fontainebleau
route forestière Hurtault
F-77300 Fontainebleau (France)
patrick.cegielski@univ-paris-est.fr

The field of Weak arithmetics is application of logical methods to Number Theory. The most famous results are: undecidability of elementary arithmetic (in contrast with elementary geometry [46, 47], there is no computer program to determine whether an arithmetical sentence is true [8]); and the negative answer to the Hilbert’s tenth problem (there is no general algorithm to decide whether a diophantine equation with integer coefficients has a solution in integers [11, 25, 12, 26]).

Number Theory is free to use any method to obtain results concerning natural integers. The adjective ‘weak’ in weak arithmetics refers to restrictions used in this topic. First of all, weak arithmetics specify its object of study: it is not a vague ‘study of natural integers’ but a study of the first order structure \( \langle \mathbb{N}, +, \times \rangle \), where \( \mathbb{N} \) is the set of natural integers 0, 1, 2,..., + denotes addition, and \( \times \) denotes multiplication*. In fact, we study expansions by definitions of this structure and substructures of such expansions. Because \( \mathbb{N} \) is not well defined in the universe of sets, we also study non standard models of \( \langle \mathbb{N}, +, \times \rangle \), more precisely of \( Th(\mathbb{N}, +, \times) \), where ‘Th’ means theory in a formal sense.

* See, for instance, [27, 16, 15] for an introduction to mathematical logic and its vocabulary.
2 Studies in Weak Arithmetics

As well as we are interested in nonstandard models of $Th(A)$, where $A$ is a substructure of an expansion by definitions of $\langle \mathbb{N}, +, \times \rangle$ or $Th(A)$ is a theory given by a set of axioms (satisfied in the standard structure $\langle \mathbb{N}, +, \times \rangle$).

Secondly, weak arithmetics also impose a restriction on the studied properties. We do not consider ill defined properties but only well defined logical sentences: first-order sentences and second-order sentences, or more precisely for the second ones monadic second-order sentences or weak monadic second-order sentences. The origin of this restriction comes from set theory. After the axiomatization of set theory by Zermelo [55], Henri Poincaré criticized the explanation given by Zermelo of the notion of ‘defined property’ implied in the axiom of separation [31]. In 1922, Fraenkel and Skolem proposed, independently, a more precise definition [19, 43]; nowadays we prefer to use the second one: to employ a formal first-order language and to consider a ‘defined property’ to be a property that can be expressed by a first-order formula (an idea inspired by Hermann Weyl [53]). First-order formulas have a long history: introduced in the second part of the nineteenth century, essentially by Gotlob Frege, they were formally defined by Skolem in the above-cited paper.

**Definition 1.** Let denote by $L(PA)$ the first-order logical language whose proper symbols are an unary function symbol $S$, two binary function symbols $+$ and $\times$, and a constant symbol 0.

**Terms** of $L(PA)$ are defined recursively:
1) A variable $x_0, x_1, x_2, \ldots$ is a term.
2) 0 is a term.
3) If $s$ and $t$ are terms, so are $Ss$, $(s + t)$, and $(s \times t)$.

**Primitive formulas** of $L(PA)$ are $t = s$, where $t$ and $s$ are terms.

**Formulas** of $L(PA)$ are defined recursively:
1) Primitive formulas are formulas.
2) If $\phi$ and $\psi$ are formulas then $\phi \land \psi$, $\phi \lor \psi$, $\phi \rightarrow \psi$, and $\neg \phi$ are formulas.
3) If $x$ is a variable and $\phi$ is a formula then $\forall x \phi$ and $\exists x \phi$ are formulas.

A **sentence** is a formula without free variables. Every sentence of $L(PA)$ is either true or false in the structure $\langle \mathbb{N}, +, \times \rangle$. However, the undecidability of elementary arithmetic amounts to the nonexistence of a general algorithm to decide whether a given sentence is true in $\langle \mathbb{N}, +, \times \rangle$. 
One of the topics of weak arithmetics is to try to axiomatize the theory of some arithmetical structure, i.e., to find a set of sentences (true in this structure) whose deductions are exactly the sentences true in this structure. Dedekind [13] and Peano [29] showed that $Th_1(\langle \mathbb{N}, +, \times \rangle)$ is axiomatizable for an ill-defined logic $L$ (a sort of but not exactly second-order logic). Gödel proved that $Th_1(\langle \mathbb{N}, +, \times \rangle)$ is not first-order axiomatizable [20]. Inspired by Dedekind and Peano’s axiomatization, Skolem defined a first-order theory whose axioms are all true in $\langle \mathbb{N}, +, \times \rangle$, but is not an axiomatization of $Th_1(\langle \mathbb{N}, +, \times \rangle)$, for Gödel proved that $Th_1(\langle \mathbb{N}, +, \times \rangle)$ is not first-order axiomatizable [20].

**Definition 2.** The **first-order Peano arithmetic** is the first-order theory in the language $L(PA)$ whose proper axioms are:

- $\forall x (Sx \neq 0)$;
- $\forall x, \forall y (Sx = Sy \Rightarrow x = y)$;
- $\forall x (x + 0 = x)$;
- $\forall x, \forall y [x + Sy = S(x + y)]$;
- $\forall x (x.0 = 0)$;
- $\forall x, \forall y [x.Sy = x.y + x]$;
- For each formula $\phi(x, \vec{y})$ of $L(PA)$, we have:
  $$\forall \vec{y} [[\phi(0, \vec{y}) \land \forall x [\phi(x, \vec{y}) \rightarrow \phi(Sx, \vec{y})]] \rightarrow \forall x \phi(x, \vec{y})].$$

The last item is a schema of axioms (induction axiom schema) hence the number of axioms is infinite. Indeed, it is proved that this theory is not finitely axiomatizable.

Many works in weak arithmetics concern axiomatizability of the first-order theory of substructures of an expansion of $\langle \mathbb{N}, +, \times \rangle$, e.g. $Th_1(\langle \mathbb{N}, S \rangle)$ [24], $Th_1(\langle \mathbb{N}, + \rangle)$ (Presburger arithmetic [33, 16]), $Th_1(\langle \mathbb{N}, \times \rangle)$ (Skolem arithmetic [3, 4, 5, 45]), and $Th_1(\langle \mathbb{N}, | \rangle)$, where $|$ is the divisibility relation (which is finitely axiomatizable [6, 7]).

In a second topic, the goal is to determine whether a well-defined logical theory of a substructure of an expansion of $\langle \mathbb{N}, +, \times \rangle$ is decidable, i.e. to determine the existence of an algorithm to decide whether a general sentence of this theory is true. Church has shown $Th_1(\langle \mathbb{N}, +, \times \rangle)$ is undecidable. In contrast, $Th_1(\langle N, + \rangle)$ (Presburger arithmetic [33, 16]), $Th_1(\langle N, \times \rangle)$ (Skolem arithmetic [44, 28, 5, 45]), $Th_1(\langle N, | \rangle)$ (natural lattice theory), or monadic second-order theory of $\langle \mathbb{N}, S, 0 \rangle$ (Büchi arithmetic [1, 41]) are decidable. The best overall reference on undecidability problem is [17, 21].
A third topic involves determining the complexity of decidable theories. For instance $Th_1(\mathbb{N}, +)$ has complexity of order $2^{2^n}$ (double exponential), i.e. there are constants $c, c'$ such that i. every sentence $\phi$ of the given language of size $\leq n$ can be decided in at most $2^{2^n}$ steps, and ii. for any decision procedure there are, for infinitely many $n$, sentences of size $\leq n$ which require more than $2^{2^n}$ steps of the procedure to be decided. The lower complexity for $Th_1(\mathbb{N}, \times)$ has been shown to be of order $2^{2^{2^n}}$ (triple exponential) [18]. The analog for undecidable theories, to determine the corresponding Turing degrees, is not an alive topic.

We have seen first-order Peano Arithmetic has an infinite number of axioms, due to the schema of induction. A very active fourth topic of weak arithmetics is interested in variants of the schema of induction, searching equivalence of such variants with other variants or consequences of this variant. Many variants are known for the full first-order Peano arithmetic. Peano Arithmetic contains an induction axiom for each first-order formula $\phi$. But, what happens if we restrict formulas $\phi$ to belong to a given well defined set of formulas? A lot of such sets of formulas have been considered in the literature: either natural subsets of the set of first-order formulas characterized by their logical structure, either set of formulas characterizing a given property in the standard model. Certainly the most famous of this second sort of sets are the sets of $\Sigma_n$ and $\Pi_n$ sentences and the sets defined by Samuel Buss [2] to characterize NP and P.

Algorithms are fundamental in Number Theory. A fifth topic of weak arithmetic aims to find out which algorithms are expressible in certain restricted programming language. For instance Loic COLSON has shown [9] that the “best” algorithm to obtain the minimum of two natural integers (to decrease one then the other until one of the integers is zero) is not expressible in many natural functional programming languages.

There exist other topics in weak arithmetics but this description of the domain is sufficient to give an idea of its subject and the methods involved. Classical books on weak arithmetics are [30, 11, 41, 18, 2, 45, 21, 23, 22, 26]. Another survey on weak arithmetics is [35].

The European researches on weak arithmetics (mainly in Armenia, Belgium, Czech Republic, Federation of Russia, France, Great Britain, Greece, Israel, Italy, Poland, Portugal, Slovakia, Spain, Tunisia, Ukraine) have had their annual conference since 1990, called JAF.
Introduction

(French acronym for “Journées sur les Arithmétiques Faibles”) or, equivalently, Weak Arithmetics Days. The original name, due to the fact that the first issues were held in France, has not been changed until now. The first issue was held in École Normale Supérieure de Lyon in June 1990, the twenty-eighth issue at University Paris-Est Créteil, campus of Fontainebleau, in June 2009. Some records on JAF are maintained at

http://lacl.univ-paris12.fr/jaf/


We have begun this introduction by recalling the result of Tarski on decidability of elementary geometry. This result is equivalent to the decidability of the first-order theory of the structure \( \langle \mathbb{R}, +, \times \rangle \), where \( \mathbb{R} \) is the set of real numbers, axiomatized as theory of real closed fields. Tarski also asked the question of the decidability of the first-order theory of the structure \( \langle \mathbb{R}, +, \times, \exp \rangle \), where \( \exp \) is the exponential function. There exist a lot of results related to this still open problem. In 1964, Shepherdson [40] axiomatized the theory of the integral part \( \langle \mathbb{N}, +, \times \rangle \) of a real closed field \( \langle \mathbb{R}, +, \times \rangle \): it coincides with the theory of discrete unitary commutative semi-ring satisfying \( IE_0 \) (schema of induction restricted to quantifier free formulas). In chapter one, Sedki Boughattas and Jean-Pierre Ressayre explain the beautiful results they have obtained on integral parts \( \langle \mathbb{N}, +, \times \rangle \) of a real exponential field \( \langle \mathbb{R}, +, \times, \exp \rangle \). The careful reader has noted integral part is not unique.

We have given above the definition of formulas and sentences in the first-order language of Peano Arithmetic. Every formula is logically equivalent to a formula under prenex form

\[
Q_1 y_1 Q_2 y_2 \cdots Q_n y_p \theta(y_1, \ldots, y_p; x_1, \ldots, x_m)
\]

where \( Q_i \) are quantifiers (\( \forall \) or \( \exists \)) and \( \theta \) is an open formula, i.e. a formula without quantifiers. Such a prenex formula is a \( \Pi_n \)-formula if there are \( n \) groups for quantifiers: the first ones (including \( Q_1 \)) are universal quantifiers \( \forall \), the following are existential quantifiers, then universal quantifiers, ending by a \( n \)-th group. Such a prenex formula is a \( \Sigma_n \)-formula if there are \( n \) groups for quantifiers beginning with a group of
existential quantifiers. We have already mentioned the interest in studying the so-called fragments of first-order Peano Arithmetic. That is to say, subtheories of Peano Arithmetic obtained by imposing a restriction on the formulas for which the induction schema (or some other related number-theoretic principle) is postulated. Notably, $\text{I}^\Sigma_n$, $\text{I}^\Pi_n$, $\text{I}^{\Sigma_n^-}$, and $\text{I}^{\Pi_n^-}$ denote, respectively, the induction schema restricted to $\Sigma_n$ formulas, $\Pi_n$ formulas, $\Sigma_n$ sentences, and $\Pi_n$ sentences. These theories, fragments of Peano Arithmetic PA, are objects of a very lively active topic of weak arithmetics. In chapter two, Andrés CORDÓN-FRANCO, Alejandro FERNÁNDEZ-MARGARIT, and Francisco-Félix LARA-MARTÍN study a number of conservation results for $\text{I}^{\Pi_n^-}$. The reference list cites some previous papers on this topic.

Often the organizers of JAF ask for a survey on methods which may be applied to, but are not necessarily directly connected to, weak arithmetic. In chapter three, Anuj DAWAR and Bjarki HOLM present the class of tools, called games, used in finite model theory. They begin with the classical Ehrenfeucht-Fraïssé games, and then explain why other games are needed (pebble, counting, and bijection games) and introduce a new type of model-comparaison games. Not only they give the original reasons for introducing a new type of games (related to logical expression of PTIME) but they also motivate these games through a problem close to weak arithmetics: the inability of logics to express a basic problem in linear algebra, namely, to determine whether a system of linear equations over a fixed finite field has a solution.

The sets of natural numbers defined by a formula $\phi(x)$ of $L(\text{PA})$ are called arithmetics. The study of subsets of $\mathbb{N}$ defined by various sets of formulas constitutes an active field. For example, the relation $<$ is first-order definable in $(\mathbb{N}, +, \times)$; hence a new sort of quantifiers (bounded quantifiers) are introduced: $(\forall x)_{\leq y} \ldots$ stands for $\forall x \ (x \leq y \to \ldots)$ and $(\exists x)_{\leq y} \ldots$ for $\exists x \ (x \leq y \land \ldots)$. Rudimentary relations are defined by formulas using bounded quantifiers instead regular quantifiers. The class of rudimentary relations has been studied for a long time but several old open problems remain. In chapter four, Henri-Alex ESBELIN proves the constant $e$ (basis for neperian logarithm) and $\pi$ (= 3.14159...) have rudimentary approximations.

Quine [34] has shown that the theory of formal languages is in a sense a field of weak arithmetics, because the first-order theory of the set of words over a finite alphabet with concatenation is equivalent to the first-order Peano Arithmetic. Finite words were generalized to infinite words (more precisely, to denumerable words $a_0a_1 \ldots a_n \ldots$) by Büchi.
to prove the decidability of monadic second-order theory of $< \mathbb{N}, S, 0 >$, then to bi-infinite words $(\ldots a_{-m} \ldots a_1 a_0 a_1 \ldots a_n \ldots)$ and more recently to pictures, i.e. infinite words in two dimensions. Olivier Finkel proves in chapter five some undecidability results on pictures and shows that some properties on pictures depend on the universe of sets, that is to say, those properties are neither provable nor refutable in ZFC.

The study of restricted classes of algorithms and the expression of these algorithms in such and such programming language is a growing topic of Theoretical Computer Science. Possible applications of this topic to arithmetical problems constitute a growing field of weak arithmetics. In chapter six, David Michel and Pierre Valarcher define the class APRA of primitive recursive algorithms (related to primitive recursive functions) and show that there exists a functional programming language that simulates in a sufficiently nice manner all algorithms of APRA. Applications to the challenging case of GCD are also given.

It is well known in weak arithmetics that some arithmetical properties depend on the underlying universe of sets (indeed, as we have already mentioned, a result of this kind appears in Olivier Finkel’s contribution to these proceedings). For arithmetic, the axiom of infinity of set theory is fundamental. In chapter seven, Eugenio Omodeo, Alberto Policriti, and Alexandru Tomescu study the logical complexity of this axiom in some variants of set theory without the axiom of foundation.

We have already mentioned the relationship between weak arithmetics and the theory of words defined over a finite alphabet. The theory of words is the study of the structures $\langle A^*, \cdot, = \rangle$, where $A$ is a non empty finite set, called alphabet, $A^*$ is the set of words $a_1 a_2 \ldots a_n$ over this alphabet, the binary operation ‘.’ stands for concatenation and ‘=’ is interpreted as set equality: two words $a_1 a_2 \ldots a_n$ and $b_1 b_2 \ldots b_m$ are equal if $m = n$, $b_1 = a_1$, ..., $b_n = a_n$. The theory of traces is the study of structures $\langle A^*, \cdot, \equiv \rangle$ with a different interpretation of equality: there exists a subset $R$ of $A \times A$ (the set of elements that commute) such that if $(a, b) \in R$ (with $a \neq b$) then $ab \equiv ba$ and, more generally, $\sigma ab \tau \equiv \sigma ba \tau$ for every words $\sigma, \tau$. As usual, if we want to make explicit the set $R$, we shall write $\equiv_R$ to denote the equality relation $\equiv$. The theory of traces is a growing field of Theoretical Computer Science because a trace is a representation of events in parallelism: a word is a sequential list of tasks; the tasks $a$ and $b$ commute if they may be executed in parallel [14]. A classical problem on words is to search the best algorithm to determine if a word $p$ (the pattern) is a factor of a word $t$ (the text), i.e. if there exist words $\sigma$ and $\tau$ such that $t = \sigma p \tau$. 
We may generalize this problem where letters of $p = p_1 \ldots p_k$ appear in the text, in the same order but not consecutively with a constraint on the difference of location between the last letter and the first letter (the problem is trivial without this constraint). In chapter eight, Karine Shahbazyan and Yuri Shoukourian study the generalization of this last problem to traces.

References


10 Studies in Weak Arithmetics


[32] Poincaré, Henri, Dernières pensées, Flammarion, 1913 and several reeditions. Electronic version:
http://www.ac-nancy-metz.fr/enseign/philo/textesph/


Studies in Weak Arithmetics


