Annals of Pure and Applied Logic 163 (2012) 615–619

Contents lists available at SciVerse ScienceDirect

Annals of Pure and Applied Logic

journal homepage: www.elsevier.com/locate/apal

Decidability questions for a ring of Laurent polynomials

Alla Sirokofskich

Department of Mathematics, University of Crete, 714 09 Heraklion, Greece

ARTICLE INFO

Article history:
Available online 23 July 2011

MSC:
03B25
03C10
11U05

Keywords:
Decidability
Existential theory
Laurent polynomials

ABSTRACT

We prove that the additive structure of the ring of Laurent polynomials augmented by the predicate symbol P, where $P(x)$ if and only if x is a power of t, is decidable. We also prove that the first-order theory of the previous structure together with the relation $|_t$, where $x\,|_t\,y$ if and only if $\exists s \in \mathbb{Z}\; y = x \cdot t^s$, is undecidable.

1. Introduction

It is well known that the additive theory of a polynomial ring over a finite field is decidable (for a concrete result of this type see, for example, [20]). On the other hand, the full ring theory with its additive and multiplicative structure is undecidable (cf. [16]); even the positive-existential theory is undecidable (cf. [4,13], the first in the ring language augmented by a symbol for the variable of the polynomials and the second without such a constant, but with a predicate for the transcendental elements of the ring). In the light of the similarity of common properties of these rings with 'analogous' properties of the ring $\mathbb{Z}$ of rational integers, those results are an analogue of the decidability of Presburger Arithmetic (the additive structure of $\mathbb{Z}$ as an ordered ring, cf. for example [5,1]) and the undecidability of the ring theory of $\mathbb{Z}$ (which is an immediate consequence of Gödel's Incompleteness Theorem, cf. [6]) or, the very much sharper negative answer to Hilbert's tenth problem (cf. [2,8]), i.e. the undecidability of the positive-existential theory of $\mathbb{Z}$. It is therefore of interest to examine sub-theories of the theory of such a polynomial ring, from the point of view of decidability. The literature on the subject is not large, but it seems reasonable to ask questions similar, at least in terms of appearance, to questions that have been asked over the ring of integers $\mathbb{Z}$. Apart from the possible independent interest of the results in this line of investigation, the methods used can then be transferred, occasionally, to answer the initial questions over $\mathbb{Z}$.

In this paper, we deal with sub-theories of the rings $\mathbb{F}_q[t]$ and $\mathbb{F}_q[t, t^{-1}]$ ($\mathbb{F}_q$ is a finite field with q elements and t is a variable). These rings may be considered as 'similar' to the rings $\mathbb{Z}$ and $\mathbb{Z}[\frac{1}{\ell}]$, respectively, where ℓ is a prime number. All our structures will contain addition and constant symbols and operation to represent any element of $\mathbb{F}_q[t]$. The additional structure that we will impose is of two sorts: first, we will consider the relation (property) P that stands for the powers of t (the resulting structures are analogues of the structures $\mathbf{Z}_P = [\mathbb{Z}; +, \{\ell^n\}_{n\in\mathbb{N}}; 0, 1]$ and $\mathbf{Z}_{\ell^{-1},P} = [\mathbb{Z}[\frac{1}{\ell}]; +, \{\ell^n\}_{n\in\mathbb{Z}}; 0, 1]$, respectively). Second, we will consider, instead of P, the relation $|_t$ which is defined by

$$x|_t y \text{ if and only if } \exists s \in \mathbb{Z}\; y = x \cdot t^s$$

E-mail address: asirokof@math.uoc.gr.

0168-0072/$ – see front matter
doi:10.1016/j.apal.2011.06.015

(the resulting structures are analogues of the structures $\mathbf{Z}_{|_\ell} = [\mathbb{Z}; +, |_\ell; 0, 1]$ and $\mathbf{Z}_{\ell^{-1},|_\ell} = [\mathbb{Z}[\frac{1}{\ell}]; +, |_\ell; \mathbf{0}, \mathbf{1}]$, respectively, where $|_p$ is defined similarly as $|_t$, with t replaced by ℓ). So we define the structures

$$\mathcal{F}_{q,t,P} = [\mathbb{F}_q[t]; +, \{t^n\}_{n\in\mathbb{N}}; 0, 1, t, f_t],$$
$$\mathcal{F}_{q,t,t^{-1},P} = [\mathbb{F}_q[t, t^{-1}]; +, \{t^n\}_{n\in\mathbb{Z}}; 0, 1, t, f_t],$$
$$\mathcal{F}_{q,t,|_t} = [\mathbb{F}_q[t]; +, |_t; 0, 1, t, f_t]$$

and

$$\mathcal{F}_{q,t,t^{-1},|_t} = [\mathbb{F}_q[t, t^{-1}]; +, |_t; 0, 1, t, f_t]$$

where f_t is a one placed functional symbol interpreted by $f_t(x) = tx$ (in other words, we allow multiplication by t) and $|_t$ is as above.

The known results are as follows.

(1) The first-order theory of $\mathbf{Z}_P$ is decidable (see [18] by Semenov). In [3] Delon showed the undecidability of the first-order theory of $\mathbf{Z}_{2^{-1},P,f} = [\mathbb{Z}[\frac{1}{2}]; +, \{2^n\}_{n\in\mathbb{Z}}; 0, 1; f]$, where f is a binary function interpreted by the restriction of the multiplication to $2^{\mathbb{Z}} \times \mathbb{Z}[\frac{1}{2}]$. The decidability or undecidability of $\mathbf{Z}_{\ell^{-1},P}$ remains an open problem.
(2) The first-order theory of $\mathcal{F}_{q,t,P}$ is decidable (see [20] by the author). We give a positive answer (decidability) for the existential theory of $\mathcal{F}_{q,t,t^{-1},P}$ in the first part of the present paper.
(3) The first-order theory of $\mathbf{Z}_{|_\ell}$ is undecidable (see [12] by Pheidas). The similar question for $\mathbf{Z}_{\ell^{-1},|_\ell}$ is an open problem.
(4) Consider the structure $[\mathbb{Z}; +, |_\ell, >; 0, 1]$, i.e., the structure which results from $\mathbf{Z}_{|_\ell}$ with the additional relation of inequality. We note that the positive-existential theory of this structure is undecidable (see [10,14]). However, the decidability of the positive-existential theory of $\mathbf{Z}_{|_\ell}$ is still an open question, and the same is true for $\mathbf{Z}_{\ell^{-1},|_\ell}$.
(5) In the second part of the present paper we show that the first-order theory of each of $\mathcal{F}_{q,t,|_t}$ and $\mathcal{F}_{q,t,t^{-1},|_t}$ is undecidable. The similar questions about the positive-existential theories are both open problems.

Obviously all questions, intermediate to the above, are open. We note that some of those questions have important implications in other problems. For example, if it turns out that the structure of addition and $|_\ell$ over an order of a quadratic number field (instead of $\mathbb{Z}$) has an undecidable positive-existential theory then it will follow that an analogue to Hilbert's tenth problem for the field $\tilde{\mathbb{F}}_p(t)$, of rational functions in the variable t, with coefficients in an algebraic closure $\tilde{\mathbb{F}}_p$ of the finite field $\mathbb{F}_p$, has a negative answer (undecidability); for the details see [12], for a discussion of this structure see also [11]. For a survey of the status of problems related to Hilbert's tenth problem see [14,15,19].

By $\mathbb{N}$ we denote the set of positive integers and by $\mathbb{N}_0$ the set of non-negative integers.

We will work in the following languages (sets of symbols).

Definition 1. (I) We define

$$L_1 = \{+, 0, 1, \mathbf{c_3}, \ldots, \mathbf{c_{q-1}}, f_t, P\}$$

and we will consider the models $\mathbb{F}_q[t]$ and $\mathbb{F}_q[t, t^{-1}]$ of L_1, adopting the following conventions:

(i) The constant symbols 0 and 1 will be interpreted by the neutral elements of addition and multiplication, respectively; the constant symbols $\mathbf{c}_3, \ldots, \mathbf{c}_{q-1}$ will represent the remaining elements of $\mathbb{F}_q$. The constant symbol t stands for the variable t and t^{-1} stands for the inverse of t.

(iii) The unary function symbol f_t stands for the function $x \mapsto tx$.

(iv) Whenever L_1 is interpreted in $\mathbb{F}_q[t, t^{-1}]$, we will assume without noting that L_1 contains the symbol t^{-1} for the inverse of the variable t and for the unary function symbol $f_{t^{-1}}$ for the function $x \mapsto t^{-1}x$ (notice that both t and f_t are quantifier-free definable in the initial language L_1).

(v) The unary predicate P is interpreted by

$$P(\omega) \text{ stands for } \text{“}\exists k \in \mathbb{Z}(\omega = t^k)\text{”}$$

where k ranges in $\mathbb{N}_0$ in the case of $\mathbb{F}_q[t]$ and in $\mathbb{Z}$ in the case of $\mathbb{F}_q[t, t^{-1}]$.

(II) We define the language L_2 by

$$L_2 = \{+, f_t, f_{t^{-1}}, |_t, 0, 1, \mathbf{c_3}, \ldots, \mathbf{c_{q-1}}, \}$$

and we will consider the models $\mathbb{F}_q[t]$ and $\mathbb{F}_q[t, t^{-1}]$ of L_2, adopting the same conventions as for L_1, together with the following:

The binary relation $x|_t y$ is defined by

$$\exists s\, x \cdot t^s = y$$

where s ranges in $\mathbb{N}_0$ in the case of $\mathbb{F}_q[t]$ and in $\mathbb{Z}$ in the case of $\mathbb{F}_q[t, t^{-1}]$.

Note that the predicate P is definable in L_2, as $P(x) \iff 1|_t x$. Therefore, for brevity, we will use $P(x)$ when needed, even when we work with the language L_2.