Decidability of Sub-theories of Polynomials over a Finite Field

Conference Paper · July 2009

DOI: 10.1007/978-3-642-03073-4_45 · Source: DBLP

Alla Sirokofskich
University of Crete

Decidability of Sub-theories of Polynomials over a Finite Field

Alla Sirokofskich

**Hausdorff Research Institute for Mathematics
Poppelsdorfer Allee 45, D-53115, Bonn, Germany

Department of Mathematics
University of Crete, 714 09 Heraklion, Greece
asirokof@math.uoc.gr

Abstract. Let $\mathbb{F}_q$ be a finite field with q elements. We produce an (effective) elimination of quantifiers for the structure of the set of polynomials, $\mathbb{F}_q[t]$, of one variable, in the language which contains symbols for addition, multiplication by t, inequalities of degrees, divisibility of degrees by a positive integer and, for each $d \in \mathbb{F}_q[t]$, a symbol for divisibility by d. We discuss the possibility of extending our results to the structure which results if one includes a predicate for the relation "x is a power of t".

1 Introduction

In what follows $\mathbb{F}_q$ is a finite field with $q = p^n$, p a prime; $\mathbb{F}_q[t]$ is the ring of polynomials over $\mathbb{F}_q$ in the variable t. By $\mathbb{N}$ we denote the set of positive integers and by $\mathbb{N}_0$ the set of non-negative integers. In what follows $+$ denotes regular addition in $\mathbb{F}_q[t]$ and f_t is a one placed functional symbol interpreted by $f_t(x) = tx$ (in other words, we allow multiplication by t). The constant symbols 0 and 1 are interpreted in the usual way. We work in the language

Definition 1.

$$L = \{+, 0, 1, f_t\} \cup \{|_\alpha : \ \alpha \in \mathbb{F}_q[t]\} \cup \ \{D_<\} \cup \{D_n : n \in \mathbb{N}\}$$

where

$$D_<(\omega_1, \omega_2) \textit{ stands for } \text{“}\textit{deg } \omega_1 < \textit{deg } \omega_2\text{”},$$

$$D_n(\omega) \textit{ stands for } \text{“}n | \textit{deg } \omega\text{”},$$

$$|_\alpha(\omega) \textit{ stands for } \text{“}\exists x (x \cdot \alpha = \omega)\text{”}.$$

** Supported by the Trimester Program on Diophantine Equations, January - April 2009

We consider the structure $\mathcal{A}$ with universe $\mathbb{F}_q[t]$ in the language L, where the symbols are interpreted as above. We show that the first-order theory of $\mathcal{A}$ admits elimination of quantifiers, i.e., each first-order formula of L is equivalent in $\mathcal{A}$ to a quantifier-free formula. The elimination is constructive. As a consequence we obtain that the first-order theory of $\mathcal{A}$ is decidable, that is, there is an algorithm which, given any formula of L, decides whether that is true or not in $\mathcal{A}$. Our main Theorem is

Theorem 1. *The theory of the structure $\mathcal{A}$ in the language L admits elimination of quantifiers and is decidable.*

Since Goedel's Incompleteness Theorem which asserts undecidability of the ring-theory of the rational integers, many researchers have investigated various rings of interest from the point of view of decidability of their theories. In [9] R. Robinson proved that the theory of a ring of polynomials $A[t]$ of the variable t in the language of rings, augmented by a symbol for t, is undecidable. Following the negative answer to 'Hilbert's Tenth Problem', Denef in [1] and [2] showed that the existential theory of $A[t]$ is undecidable, if A is a domain. In consequence, decidability can be a property of theories weaker, only, than the ring theory of $A[t]$. The situation is analogous to the ring of integers: Since no general algorithms can exist for the ring theory of $\mathbb{Z}$, one can look into sub-theories that correspond to structures on $\mathbb{Z}$ weaker than the ring structure. Two examples are: (a) (L. Lipshitz in [3]) the existential theory of $\mathbb{Z}$ in the language of addition and divisibility is decidable (but the full first order theory is undecidable), and (b) (A. Semenov in [10] and [11]) the elementary theory of addition and the function $n \to 2^n$ over $\mathbb{Z}$ is decidable. Th. Pheidas proved a result analogous to those of Lipshitz in (a) for polynomials in one variable over a field with decidable existential theory (in his Ph. D. Thesis) - but the similar problem for polynomials in two variables has an undecidable existential theory. Th. Pheidas and K. Zahidi in [6] showed that the theory of the structure $(\mathbb{F}_q[t]; +; x \to x^p; f_t; 0, 1)$ is model complete and therefore decidable ($x \to x^p$ is the Frobenius function). For surveys on relevant decidability questions and results the reader may consult [4], [5], [6], [7] and [8].

Our results provide a mild strengthening of the analogue, for polynomials over finite fields, of the decidability of 'Presburger Arithmetic' (which is, essentially, the theory of addition and order) for $\mathbb{N}$.

1.1 A List of Open Problems

1. Presently we do not have any estimate for the complexity of the decision algorithm. The existential theory of the structure $\mathcal{A}$ is already exponential and NP-hard since it contains the problem of dynamic programming over polynomials. At the moment it is unclear what the complexity of the whole theory is.
2. Does the similar problem for polynomial rings $F[t]$ have a similar answer (decidability) for any field F with a decidable theory?

2 Analogue of Presburger Arithmetic in $\mathbb{F}_q[t]$

By $\wedge, \vee, \neg$ we mean the usual logical connectives and deg x stands for the degree of the polynomial x. In what follows, addition, multiplication and degree are meant in $\mathbb{F}_q[t]$.

Consider any quantifier free formula $\psi(\bar{x})$ in L, where $\bar{x} = (x_1, \ldots, x_n)$. Then $\psi(\bar{x})$ is equivalent to a quantifier-free formula in disjunctive-normal form with literals among the following relations:

$$D_<(\omega_1, \omega_2),\ |_c(\omega),\ D_n(\omega),\ \omega = 0$$

and their negations, where $\omega, \omega_1, \omega_2$ are terms of the language L with variables among $x_1, \ldots, x_n$. The following negations can be eliminated:

- $\neg D_<(\omega_1, \omega_2)$ is equivalent to $D_<(\omega_2, \omega_1) \vee [D_<(\omega_1, t \cdot \omega_2) \wedge D_<(\omega_2, t \cdot \omega_1)]$.
- $\neg D_n(\omega)$ is equivalent to a finite disjunction of $D_n(t^i \omega)$ for $1 \leq i < n$.
- $\not|_c(\omega)$ can be replaced by

$$\bigvee_{r \neq 0, deg(r) < deg(c)} |_c(\omega + r).$$

- $\omega \neq 0$ is equivalent to $D_<(0, \omega)$, (recall that $\deg(0) = -\infty$).

This can be summarized in the next Proposition.

Proposition 1. *Every existential formula of L is equivalent to a finite disjunction of formulas of the form*

$$\sigma(\bar{\omega}):\ \sigma_0 \wedge\ \exists \bar{x} = (x_1, \ldots, x_n) \sigma_1 \wedge \sigma_2 \wedge \sigma_3 \wedge \sigma_4 \tag{1}$$

where σ_0 is an open formula with parameters $\bar{\omega} = (\omega_1, \ldots, \omega_k)$,

$$\sigma_1(\bar{x}, \bar{\omega}):\ \bigwedge_i\ f_i(\bar{x}) = h_i(\bar{\omega})\ , \tag{2}$$

$$\sigma_2(\bar{x}, \bar{\omega}):\ \bigwedge_\rho\ D_<(\pi_{1,\rho}(\bar{x}, \bar{\omega}), \pi_{2,\rho}(\bar{x}, \bar{\omega}))\ , \tag{3}$$

$$\sigma_3(\bar{x}, \bar{\omega}):\ \bigwedge_\lambda\ |_{c_\lambda}(\chi_\lambda(\bar{x}, \bar{\omega}))\ , \tag{4}$$

$$\sigma_4(\bar{x}, \bar{\omega}):\ \bigwedge_\xi\ D_{n_\xi}(g_\xi(\bar{x}, \bar{\omega}))\ , \tag{5}$$

where
each index among i, ρ, λ, ξ ranges over a finite set, $n_\xi \in \mathbb{N}$, each of f_i, h_i, $\pi_{1,\rho}$, $\pi_{2,\rho}$, χ_λ, g_ξ is a degree-one polynomial of the indicated variables over $\mathbb{F}_q[t]$, and each f_i is a homogeneous polynomial.

$D_=(X,Y)$ is an abbreviation for the formula $D_<(X,tY)\wedge D_<(Y,tX)$. Also $D_\leq(X,Y)$ stands for the formula $D_<(X,Y)\vee D_=(X,Y)$.

Definition 2. *Let $X,Y,Z\in\mathbb{F}[t]$, with $\deg(X)=\deg(Y)=\deg(Z)$. We define the depth of the cancellation in the sum $X+Y$ to be*

$$dc(X+Y)=\deg(Y)-deg(X+Y).$$

We say that X fits better into Y than into Z, if $dc(X+Y)>dc(X+Z)$.

We continue with several facts about the depth of the cancellation. Let

$$a_1x=\sum_{i\leq k}u_it^i,\qquad \omega_1=\sum_{i\leq k}v_it^i,\qquad \omega_2=\sum_{i\leq k}w_it^i,$$

with $u_i,v_i,w_i\in\mathbb{F}_q$. Assume that there is some $\lambda\leq k$ such that $u_i=-v_i$ for all $i\geq\lambda$. Let λ_1 be the least such λ. If $\lambda_1\geq 1$, then the degree of $a_1x+\omega_1$ is λ_1-1 and thus $dc(a_1x+\omega_1)=k-\lambda_1+1$. Note that in case $\lambda_1=0$, then $a_1x=-\omega_1$ and the degree of $a_1x+\omega_1$ is $-\infty$.

Assume that $dc(a_1x+\omega_1)>0$. Consider any ω_2 with the properties $\deg(a_1x)$ $=\deg(\omega_2)$ and $dc(a_1x+\omega_1)<dc(a_1x+\omega_2)$. The crucial observation is that for any i such that $\forall j\geq i(u_j=-w_j)$, we have that i should be greater than λ_1. Therefore $dc(a_1x+\omega_1)>dc(\omega_2+(-\omega_1))$. Thus $\deg(a_1x+\omega_1)<\deg(\omega_2-\omega_1)$

For the sake of completeness we list several facts for the relation of the form $D_<(a_1x+\omega_1,a_2x+\omega_2)$, where $a_i\in\mathbb{F}_q[t]\setminus\{0\}$, ω_i are parameters and x is a variable.

Lemma 1. *The relation $D_=(a_1x+\omega_1,a_1x+\omega_2)$ is equivalent to the disjunction of*

(1.1) $D_<(a_1x,\omega_1)\wedge D_<(a_1x,\omega_2)\wedge D_=(\omega_1,\omega_2)$,
(1.2) $D_<(\omega_1,a_1x)\wedge D_<(\omega_2,a_1x)$,
(1.3) $D_=(a_1x+\omega_1,\omega_1)\wedge D_=(a_1x,\omega_1)\wedge D_<(\omega_2,\omega_1)$,
(1.4) $D_=(a_1x+\omega_1,\omega_1)\wedge D_=(a_1x+\omega_2,\omega_2)\wedge D_=(a_1x,\omega_1)\wedge D_=(\omega_1,\omega_2)$,
(1.5) $D_<(a_1x+\omega_1,\omega_1)\wedge D_<(a_1x+\omega_2,\omega_2)\wedge D_\leq(\omega_1-\omega_2,a_1x+\omega_1)\wedge D_=(a_1x,\omega_1)\wedge D_=(\omega_1,\omega_2)\wedge D_\leq(\omega_1-\omega_2,a_1x+\omega_2)$,
(1.6) $D_=(a_1x+\omega_2,\omega_2)\wedge D_=(a_1x,\omega_2)\wedge D_<(\omega_1,\omega_2)$.

Proof. "$\Leftarrow$"

• Assume that (1.1) holds. Then $D_=(a_1x+\omega_1,\omega_1)$ and $D_=(a_1x+\omega_2,\omega_2)$, therefore $D_=(a_1x+\omega_1,a_1x+\omega_2)$ holds.

• Assume that (1.2) holds. Then $D_=(a_1x+\omega_1,a_1x)$ and $D_=(a_1x+\omega_2,a_1x)$, therefore $D_=(a_1x+\omega_1,a_1x+\omega_2)$ holds.

• Assume that (1.3) holds. Then $D_=(a_1x+\omega_1,a_1x)$ and $D_=(a_1x+\omega_2,a_1x)$, therefore $D_=(a_1x+\omega_1,a_1x+\omega_2)$ holds.

• Assume that (1.4) holds. Then it is obvious that $D_=(a_1x+\omega_1,a_1x+\omega_2)$ holds true.

• Assume that (1.5) holds. Following the notation given after Definition 2, let λ_1 be as defined and λ_2 be the least λ such that $u_i = -w_i$ for all $i \geq \lambda$. Note that if $\lambda_1 < \lambda_2$, then $\deg(a_1x + \omega_1) < \deg(\omega_1 - \omega_2)$ and this contradicts the assumption. Similarly if $\lambda_2 < \lambda_1$, we have that $\deg(a_1x + \omega_2) < \deg(\omega_1 - \omega_2)$ and this also contradicts the assumption. Thus $\lambda_1 = \lambda_2$, therefore we have that $D_=(a_1x + \omega_1, a_1x + \omega_2)$ holds.

• Assume that (1.6) holds. Then $D_=(a_1x + \omega_1, a_1x)$ and $D_=(a_1x + \omega_2, a_1x)$, therefore $D_=(a_1x + \omega_1, a_1x + \omega_2)$ holds.

"⇒" Assume that $D_=(a_1x + \omega_1, a_1x + \omega_2)$ holds. We examine all possible linear orderings of the set $\{a_1x, \omega_1, \omega_2\}$.

• Let $D_<(a_1x, \omega_2)$. The cases $D_=(a_1x, \omega_1)$ and $D_<(\omega_1, a_1x)$ are impossible. If $D_<(a_1x, \omega_1)$, then (1.1) holds.

• Let $D_<(\omega_2, a_1x)$. Then either $D_<(\omega_1, a_1x)$, thus (1.2) holds, or $D_=(\omega_1, a_1x)$ and $\deg(a_1x + \omega_1) = \deg(\omega_1)$ i.e., (1.3) holds.

• Let $D_=(\omega_2, a_1x)$. The case $D_<(a_1x, \omega_1)$ is impossible. If $D_<(\omega_1, a_1x)$, then (1.6) holds. If $D_=(\omega_1, a_1x)$, then we $dc(a_1x+\omega_1) = dc(a_1x+\omega_2)$. If both depths are zero, then (1.4) holds. If the depths are non-zero, then we have that $v_i = w_i$, for all $i \geq \lambda_1 = \lambda_2$. Note that v_i, w_i might be equal and for some $i < \lambda_1$, i.e., $\deg(\omega_2 - \omega_1) \leq \lambda_1 - 1 = \lambda_2 - 1$. Therefore (1.5) holds. □

Lemma 2. *For $k \in \mathbb{N}$ and $X, Y \in \mathbb{F}_q[t]$, we define $D_{<_k}(X, Y)$ to be $D_<(t^{k-1}X, Y)$. With this notation the formula $D_{<_k}(a_1x + \omega_1, a_1x + \omega_2)$ is equivalent to the disjunction of*

(2.1) $D_<(a_1x, \omega_1) \wedge D_<(a_1x, \omega_2) \wedge D_{<_k}(\omega_1, \omega_2)$,
(2.2) $D_<(\omega_1, a_1x) \wedge D_{<_k}(a_1x, \omega_2)$,
(2.3) $D_\leq(a_1x + \omega_1, \omega_1) \wedge D_=(a_1x, \omega_1) \wedge D_<(\omega_1, \omega_2) \wedge D_{<_k}(a_1x + \omega_1, \omega_2)$,
(2.4) $D_\leq(a_1x + \omega_1, \omega_1) \wedge D_=(a_1x, \omega_1) \wedge D_<(\omega_2, \omega_1) \wedge D_{<_k}(a_1x + \omega_1, \omega_1)$,
(2.5) $D_<(a_1x + \omega_1, \omega_1) \wedge D_=(a_1x, \omega_1) \wedge D_=(a_1x, \omega_2) \wedge D_{<_k}(a_1x + \omega_1, \omega_2 - \omega_1)$.

Proof. "⇐"

• Assume that (2.1) holds. Then $D_=(a_1x + \omega_1, \omega_1)$ and $D_=(a_1x + \omega_2, \omega_2)$, therefore $D_{<_k}(a_1x + \omega_1, a_1x + \omega_2)$ holds.

• Assume that (2.2) holds. Then $D_=(a_1x + \omega_1, a_1x)$, $D_<(a_1x, \omega_2)$, $k \geq 1$ and $D_=(a_1x + \omega_2, \omega_2)$, therefore $D_{<_k}(a_1x + \omega_1, a_1x + \omega_2)$ holds.

• Assume that (2.3) holds. Then for the reasons given above, we have that $D_{<_k}(a_1x + \omega_1, a_1x + \omega_2)$ holds.

• Assume that (2.4) holds. Then $D_=(a_1x+\omega_2, \omega_1)$ and $D_=(a_1x, \omega_1)$, therefore $D_{<_k}(a_1x + \omega_1, a_1x + \omega_2)$ holds.

• Assume that (2.5) holds. Then we have that there is a cancellation in the sum $a_1x + \omega_1$. Also the cancellation, if there is any, in the sum $\omega_2 + (-\omega_1)$ is smaller from the former one. Thus the cancellation (if there is) in the sum $a_1x+\omega_2$ is smaller than the cancellation in the sum $a_1x + \omega_1$. Therefore $D_{<_k}(a_1x + \omega_1, a_1x + \omega_2)$ holds.

"$\Rightarrow$" Assume that $D_{<_k}(a_1x+\omega_1, a_1x+\omega_2)$ holds.

- Let $D_<(a_1x, \omega_2)$. If $D_=(a_1x, \omega_1)$, then (2.3) holds. If $D_<(a_1x, \omega_1)$, then (2.1) holds. If $D_<(\omega_1, a_1x)$, then (2.2) holds.
- Let $D_<(\omega_2, a_1x)$. Then we must have a cancellation at least of depth k in the sum $a_1x+\omega_1$, i.e., $\deg(a_1x+\omega_1) \leq \deg(\omega_1)+k$, i.e., (2.4) holds.
- Let $D_=(\omega_2, a_1x)$. Then we must have a cancellation in the sum $a_1x+\omega_1$ of at least depth k plus the depth of cancellation in the sum $a_1x+\omega_2$, i.e., (2.5) holds. $\square$

Lemma 3. *For $k \in \mathbb{N}$ and $X, Y \in \mathbb{F}_q[t]$, we define $D_{<^k}(X,Y)$ to be $D_<(X, Yt^k)$. With this notation the formula $D_{<^k}(a_1x+\omega_1, a_1x+\omega_2)$ is equivalent to the disjunction of*

(3.1) $D_<(a_1x, \omega_2) \wedge D_{<^k}(a_1x+\omega_1, \omega_2)$,
(3.2) $D_\leq(\omega_1, a_1x) \wedge D_<(\omega_2, a_1x)$,
(3.3) $D_<(a_1x, \omega_1) \wedge D_<(\omega_2, a_1x) \wedge D_{<^k}(\omega_1, a_1x)$,
(3.4) $D_=(a_1x, \omega_2) \wedge D_<(a_1x, \omega_1) \wedge D_{<^k}(\omega_1, a_1x+\omega_2)$,
(3.5) $D_=(a_1x, \omega_2) \wedge D_<(\omega_1, a_1x) \wedge [D_{<^k}((\omega_2, a_1x+\omega_2)]$,
(4.6) $D_=(a_1x, \omega_2) \wedge D_=(\omega_1, a_1x) \wedge D_\leq(a_1x+\omega_1, a_1x+\omega_2)$,
(4.7) $D_=(a_1x, \omega_2) \wedge D_=(\omega_1, \omega_2) \wedge D_=(a_1x+\omega_1, \omega_2-\omega_1) \wedge \Big[\bigvee_{i=1}^{k-1} D_=(a_1x+\omega_2, t^i(\omega_2-\omega_1))\Big]$.

The purpose of the above Lemmas is to show that when the coefficients of x in the relation $D_<(a_1x+\omega_1, a_2x+\omega_2)$ are the same, then this relation is equivalent to a disjunction of relations of the form $D_<$, where we have at most one appearance of x in each relation $D_<$. Our next goal is to deal with the relation $D_<(a_1x+\omega_1, a_2x+\omega_2)$, where the coefficients of x are not the same.

Lemma 4. *Consider the relation $D_<(a_1x+\omega_1, a_2x+\omega_2)$, with $a_1 \neq a_2$. Then it is equivalent to the disjunction of*

(4.1) $D_<(a_1, a_2) \wedge D_{<^{k_1}}(a_1a_2x+a_2\omega_1, a_1a_2x+a_1\omega_2)$,
(4.2) $D_<(a_2, a_1) \wedge D_{<_{k_2}}(a_1a_2x+a_2\omega_1, a_1a_2x+a_1\omega_2)$,
(4.3) $D_=(a_1, a_2) \wedge D_<(a_1a_2x+a_2\omega_1, a_1a_2x+a_1\omega_2)$,

where $k_1 = \deg(a_2)-\deg(a_1)$, $k_2 = \deg(a_1)-\deg(a_2)+1$,

In order to proceed with the elimination of quantifiers, we need to prove one fact.

Proposition 2. *Consider σ as given in Proposition 1 for $n=1$ (i.e. $\bar{x}=x_1=x$). Then there are quantifier-free formulae $\tilde{\sigma}_0$, $\tilde{\sigma}_1$, $\tilde{\sigma}_2$, $\tilde{\sigma}_3$ and $\tilde{\sigma}_4$ such that*

$$\sigma_0 \wedge \ \exists x\ (\sigma_1 \wedge \sigma_2 \wedge \sigma_3 \wedge \sigma_4) \iff \bigvee (\tilde{\sigma_0} \wedge \ \exists z\ (\tilde{\sigma_1} \wedge \tilde{\sigma_2} \wedge \tilde{\sigma_3} \wedge \tilde{\sigma_4})),$$

where $\tilde{\sigma_0}$ *is a quantifier-free formula with parameters* $\bar{\omega}$*,*

$$\tilde{\sigma_1}(z,\bar{\omega}): \bigwedge_i \; z = \tilde{h_i}(\bar{\omega}) \;, \tag{6}$$

$$\tilde{\sigma_2}(z,\bar{\omega}): \bigwedge_\rho \; D_<(z,\tilde{\pi}_{2,\rho}(\bar{\omega})) \wedge D_<(\tilde{\pi'}_{1,\rho}(\bar{\omega}),z), \tag{7}$$

$$\tilde{\sigma_3}(z): \bigwedge_\lambda \; |_{c_\lambda}(\tilde{\chi}_\lambda(z)) \;, \tag{8}$$

$$\tilde{\sigma_4}(z): \bigwedge_\xi \; D_{n_\xi}(z) \tag{9}$$

where
each index among i*,* ρ*,* λ, ξ *ranges over a finite set, each of* $\tilde{h_i}, \tilde{\pi}_{2,\rho}, \tilde{\pi'}_{1,\rho}$ *is a degree-one polynomial in the parameters* $\bar{\omega}$ *over* $\mathbb{F}_q[t]$*, each of* $\tilde{\chi}_\lambda$ *is a degree-one polynomial in the variable* z *over* $\mathbb{F}_q[t]$*.*

Proof. Let σ be as in the hypothesis. We follow the notation as given in Proposition 1. According to the above Lemmas, we can assume that for every ρ in the formula σ_2, the coefficient of x is non-zero in exactly one of the polynomials $\pi_{1,\rho}, \pi_{2,\rho}$.

Consider A to be the set of all coefficients of x in σ. Let a' be the least common multiple of all coefficients of x in σ. Let a be the least element in $\mathbb{F}_q[t]$ such that $a'|a$ and $n_\xi|deg(\frac{a}{b})$, for all n_ξ given in σ_4 and for all $b \in A$. Next we modify σ in the following way.

• By multiplying suitably, we arrange the coefficient of x in the terms $f_i(x)$ to be a. Thus we may assume that $f_i(x) = ax$, for all i.

• Consider any relation of the form $|_{c_\lambda}(\chi_\lambda(x,\bar{\omega}))$ and let a_1 be the coefficient of x. Then

$$|_{c_\lambda}(\chi_\lambda(x,\bar{\omega})) \text{ if and only if } |_{\frac{a \cdot c_\lambda}{a_1}}(\frac{a}{a_1}\chi_\lambda(x,\bar{\omega})).$$

Therefore we may assume that $\chi_\lambda(x,\bar{\omega}) = ax + \chi'_\lambda(\bar{\omega})$.

• Consider any relation of the form $D_{n_\xi}(g_\xi(x,\bar{\omega}))$ and let a_1 be the coefficient of x. Then

$$D_{n_\xi}(g_\xi(x,\bar{\omega})) \text{ if and only if } D_{n_\xi}(\frac{a}{a_1}g_\xi(x,\bar{\omega})),$$

because $deg\big(\frac{a}{a_1}g_\xi(x,\bar{\omega})\big)= deg(\frac{a}{a_1}) + deg(g_\xi(x,\bar{\omega}))$ and $n_\xi|deg(\frac{a}{a_1})$ Therefore we may assume that $g_\xi(x,\bar{\omega}) = ax + g'_\xi(\bar{\omega})$.

• Consider any relation of the form $D_<(\pi_{1,\rho}(x,\bar{\omega}), \pi_{2,\rho}(x,\bar{\omega}))$. As we mentioned before, due to Lemmas 1 -4 for every ρ exactly one of the polynomials $\pi_{1,\rho}, \pi_{2,\rho}$ has a non-trivial appearance of x. Let a_1 be the non-zero coefficient of x. Then

$$D_<(\pi_{1,\rho}(x,\bar{\omega}), \pi_{2,\rho}(x,\bar{\omega})) \text{ if and only if } D_<(\frac{a}{a_1}\pi_{1,\rho}(x,\bar{\omega}), \frac{a}{a_1}\pi_{2,\rho}(x,\bar{\omega})).$$

Therefore we may assume that either $\pi_{1,\rho}(x,\bar{\omega}) = ax + \pi'_{1,\rho}(\bar{\omega})$, $\pi_{2,\rho}(x,\bar{\omega}) = \pi'_{2,\rho}(\bar{\omega})$, or $\pi_{1,\rho}(x,\bar{\omega}) = \pi'_{1,\rho}(\bar{\omega})$, $\pi_{2,\rho}(x,\bar{\omega}) = ax + \pi'_{2,\rho}(\bar{\omega})$.

We take a disjunction over all possible total orderings of the degrees of the terms $ax, ax+\pi'_{1,\rho}(\bar\omega), ax+\pi'_{2,\rho}(\bar\omega), \pi'_{1,\rho}(\bar\omega), \pi'_{2,\rho}(\bar\omega), ax+\chi'_\lambda(\bar\omega), ax+g'_\xi(\bar\omega)$ that occur in σ. Since the existential quantifier $\exists x$ distributes over $\vee$ we may assume, without loss of generality, that σ_2 implies such an ordering. Let T be a term of lowest degree (according to this ordering), in which x occurs non-trivially. Clearly, T must be of the form $ax+u(\bar\omega)$ where u is a term of L in which x does not occur. We perform the change of variables $z = ax + u$ and we substitute each occurrence of ax in the above terms by the resulting value of ax, $z-u$. We adjoin in σ_3 the divisibility $|_a(z-u)$. In detail,

- each formula of the form $ax = h_i(\bar\omega)$ is replaced by $z = \tilde h(\bar\omega)$, where $\tilde h(\bar\omega) = h_i(\bar\omega) + u(\bar\omega)$,
- each formula of the form $|_c(ax+\chi'_\lambda(\bar\omega))$ is replaced by $\bigvee_r |_c(z+r) \wedge |_c(\chi'(\bar\omega) - u(\bar\omega) - r))$, where r runs over all polynomials with degree less then deg(c),
- each formula of the form $D_<(ax+\pi'_{1,\rho}(\bar\omega), \pi'_{2,\rho}(\bar\omega)) \wedge D_<(ax+u(\bar\omega), ax+\pi'_{1,\rho}(\bar\omega))$ is replaced by $D_\le(\pi'_{1,\rho}(\bar\omega) - u(\bar\omega), z) \wedge D_<(z, \pi'_{2,\rho}(\bar\omega))$,
- each formula of the form $D_<(ax+\pi'_{1,\rho}(\bar\omega), \pi'_{2,\rho}(\bar\omega)) \wedge D_=(ax+u(\bar\omega), ax+\pi'_{1,\rho}(\bar\omega))$ is replaced by $D_<(z, \pi'_{2,\rho}(\bar\omega)) \wedge D_\le(\pi'_{1,\rho}(\bar\omega) - u(\bar\omega), z)$,
- each formula of the form $D_<(\pi'_{1,\rho}(\bar\omega), ax+\pi'_{2,\rho}(\bar\omega)) \wedge D_<(ax+u(\bar\omega), ax+\pi'_{2,\rho}(\bar\omega))$ is replaced by $D_<(z, \pi'_{2,\rho}(\bar\omega) - u(\bar\omega)) \wedge D_<(\pi'_{1,\rho}(\bar\omega), \pi'_{2,\rho}(\bar\omega)) - u(\bar\omega)$,
- each formula of the form $D_<(\pi'_{1,\rho}(\bar\omega), ax+\pi'_{2,\rho}(\bar\omega)) \wedge D_=(ax+u(\bar\omega), ax+\pi'_{2,\rho}(\bar\omega))$ is replaced by $D_<(\pi'_{1,\rho}(\bar\omega), z) \wedge D_\le(\pi'_{2,\rho}(\bar\omega) - u(\bar\omega), z)$,
- each formula of the form $D_n(ax+g'_\xi(\bar\omega)) \wedge D_<(ax+u(\bar\omega), ax+g'_\xi(\bar\omega))$ is replaced by $D_n(g'_\xi(\bar\omega) - u(\bar\omega)) \wedge D_<(z, g'_\xi(\bar\omega) - u(\bar\omega)$,
- each formula of the form $D_n(ax+g'_\xi(\bar\omega)) \wedge D_=(ax+u(\bar\omega), ax+g'_\xi(\bar\omega))$ is replaced by $D_n(z) \wedge D_\le(g'_\xi(\bar\omega) - u(\bar\omega), z)$.

This completes the proof of the separation of x from $\bar\omega$. □

We are ready to eliminate the existential quantifiers over the variables $\bar x$ in the existential formula σ of Proposition 1.

Theorem 2. *Every formula σ of L is equivalent over $\mathbb{F}_q[t]$ to an open formula of L.*

Proof. Let σ be as in Proposition 1. If σ_1 is not void (i.e. equivalent to $1 = 1$) then solve for one of the variables in terms of the remaining ones over $\mathbb{F}_q(t)$, substitute each occurrence of it by the value implied by the equations and adjoin the corresponding divisibility to σ_3 as indicated in the proof of Proposition 2. Iterate until there are no equations. Hence we assume that σ_1 is void.

According to Proposition 1 we assume that $\sigma_2 \wedge \sigma_3 \wedge \sigma_4$ has the form indicated in Proposition 2, with respect to the variable x_n.

In order to achieve the elimination of x_n, we separate the variable x_n from the rest of the variables $x_1, \dots, x_{n-1}$, by considering $x_1, \dots, x_{n-1}, \omega_1, \dots, \omega_m$ as parameters. Thus after applying Proposition 2 to σ, we may assume from the beginning that each σ_i (as given in Proposition 1) is already in separated form with $\bar{x} = x_n$ and that the coefficient of every nontrivial appearance of x_n in σ is equal to 1.

Let $x_1, \ldots, x_{n-1}$ and $\bar{\omega}$ be given. First, we observe that we may substitute the relations of σ_4 by only one divisibility $D_{n_{\xi_0}}(x_n)$, where n_{ξ_0} is the least common multiple of all n_ξ appearing in σ_4.

Case 1: There is no upper bound for the degree of x_n. Then x_n can be eliminated if and only if the conditions for the Generalized Chinese Theorem hold for σ_3.

Case 2: There is an upper bound for the degree of x_n. Now note that

$$D_<(x_n, \theta_1(x_1, ..., x_{n-1}, \bar{\omega})) \wedge D_<(x_n, \theta_2(x_1, ..., x_{n-1}, \bar{\omega})) \iff$$

$$[D_<(\theta_1(x_1, ..., x_{n-1}, \bar{\omega}), \theta_2(x_1, ..., x_{n-1}, \bar{\omega})) \wedge D_<(x_n, \theta_1(x_1, ..., x_{n-1}, \bar{\omega}))] \vee$$

$$[D_<(\theta_2(x_1, ..., x_{n-1}, \bar{\omega}), t\theta_1(x_1, ..., x_{n-1}, \bar{\omega})) \wedge D_<(x_n, \theta_2(x_1, ..., x_{n-1}, \bar{\omega}))].$$

Let $\theta_{m_2}(x_1, ..., x_{n-1}, \bar{\omega})$ be such that its degree is the least upper bound for the degree of x_n. Using the Generalized Chinese Theorem, we check if the system of divisibilities of σ_3 has some solution $x_n \in \mathbb{F}_q[t]$. If it does, then there is a solution $x_n \in \mathbb{F}_q[t]$ such that $D_{n_{\xi_0}}(x_n)$.

Case 2(a): Assume that there is no $\theta(x_1, ..., x_{n-1}, \bar{\omega})$ such that $D_<(\theta(x_1, ..., x_{n-1}, \bar{\omega}), x_n)$. Then x_n should be a constant polynomial, i.e., there is an elimination of x_n.

Case 2(b): There are $\theta_1(x_1, ..., x_{n-1}, \bar{\omega})$ and $\theta_2(x_1, ..., x_{n-1}, \bar{\omega})$ such that

$$D_<(\theta_1(x_1, ..., x_{n-1}, \bar{\omega}), x_n) \wedge D_<(x_n, \theta_2(x_1, ..., x_{n-1}, \bar{\omega})).$$

Let $\theta_{m_2}(x_1, ..., x_{n-1}, \bar{\omega})$ be as defined above and $\theta_{m_1}(x_1, ..., x_{n-1}, \bar{\omega})$ such that its degree is the least lower bound for the degree of x_n. For simplicity we denote $\theta_{m_1}(x_1, ..., x_{n-1}, \bar{\omega}), \theta_{m_2}(x_1, ..., x_{n-1}, \bar{\omega})$ by $\theta_{m_1}, \theta_{m_2}$ respectively. We repeat the previous algorithm to decide if there exists a x_n that satisfies $\sigma_3 \wedge D_{n_{\xi_0}}(x_n)$. If there is such $x_n \in \mathbb{F}_q[t]$, then let d be the least positive integer with the property: if x_n is a solution of $\sigma_3 \wedge D_{n_{\xi_0}}(x_n)$, then the next solution of $\sigma_3 \wedge D_{n_{\xi_0}}(x_n)$ is of degree $\deg(x_n) + d$. Such d exists due to the Generalized Chinese Theorem. Thus

$$\exists x_n(\sigma_2 \wedge \sigma_3 \wedge \sigma_4) \iff \bigvee_{i=0}^{d-1} [D_d(t^{d-i}\theta_{m_1}) \wedge D_<(t^{d-i}\theta_{m_1}, \theta_{m_2})].$$

Thus by induction on n we obtain the required statement of elimination. □

3 An Enrichment for $(\mathbb{F}_q[t]; +; |_a; P; f_t; 0, 1)$

We start by augmenting the language of the structure $\mathcal{A}$ to a language L_P.

Definition 3. *Let q and t be given. We define the language*

$$L_P = L \cup \{P\}$$

where the predicate $P(\omega)$ stands for "ω is a power of t".

This extension of a language L is an analogue to the extension of Presburger arithmetic by the relation "x is a power of 2", which, over $\mathbb{N}$, has a decidable theory, as mentioned in the Introduction.

Currently, we are investigating the theory of $\mathbb{F}_q[t]$ in L_P from the point of view of decidability. Our results so far indicate that this theory may be model-complete.

3.1 Acknowledgments

The author would like to thank Th. Pheidas and the referees for helpful suggestions.

References

1. J. Denef, *The diophantine problem for polynomial rings and fields of rational functions*, Transactions of the American Mathematical Society **242** (1978), 391-399.
2. J. Denef, *The diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium 78, North Holland (1984), 131-145.
3. L. Lipshitz, *The diophantine problem for addition and divisibility*, Transactions of the American Mathematical Society **235** (1978), 271-283.
4. T. Pheidas, *Extensions of Hilbert's Tenth Problem*, the Journal of Symbolic Logic **59-2** (1994), 372-397.
5. T. Pheidas and K. Zahidi, *Undecidability of existential theories of rings and fields: A survey*, Contemporary Mathematics **270** (2000), 49-106.
6. T. Pheidas and K. Zahidi, *Elimination theory for addition and the Frobenius map in polynomial rings*, the Journal of Symbolic Logic **69-4** (2004), 1006-1026.
7. T. Pheidas and K. Zahidi, *Analogues of Hilbert's tenth problem*, Model theory with Applications to Algebra and Analysis Vol. 2 (Eds. Zoe Chatzidakis, Dugald Macpherson, Anand Pillay, Alex Wilkie), London Math Soc. Lecture Note Series **Nr 350** (2008), 207-236.
8. B. Poonen, *Undecidability in Number Theory*, Notices A.M.S. **55** (2008), no 3, 344-350.
9. R. Robinson, *Undecidable rings*, Transactions of the American Mathematical Society **70** (1951), 137-159.
10. A. Semenov *Logical theories of one-place functions on the set of natural numbers*, Math. USSR Izvestija **22** (1984), 587-618.
11. A. Semenov, *On the definability of arithmetic in its fragments*, Soviet Math. Dokl. **25** (1982), 300-303.