

## ON AN EXPONENTIAL PREDICATE IN POLYNOMIALS OVER FINITE FIELDS

ALLA SIROKOFSKICH

(Communicated by Julia Knight)

ABSTRACT. We show that the theory of the set of polynomials in  $\mathbb{F}_q[t]$ , where  $\mathbb{F}_q$  is a finite field, in a language including addition and a predicate for the relation “ $x$  is a power of  $t$ ” is model-complete and therefore decidable.

### 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  $\mathbb{F}_q$ , while  $\mathbb{F}_q^*$  stands for  $\mathbb{F}_q - \{0\}$  and  $(\mathbb{F}_q[t])^*$  stands for  $\mathbb{F}_q[t] - \{0\}$ . We denote by  $\mathbb{N}$  the set of positive integers and let  $\mathbb{N}_0$  be  $\mathbb{N} \cup \{0\}$ .

We investigate the theory of the structure  $\mathcal{P}_q = (\mathbb{F}_q[t]; +; P; f_t; \mathbf{c}_1, \dots, \mathbf{c}_q; D_<)$ , where  $+$  denotes regular addition,  $t$  is a transcendental element over  $\mathbb{F}_q$ ,  $\mathbf{c}_1, \dots, \mathbf{c}_q$  are constant symbols for each element of  $\mathbb{F}_q$ ,  $P$  is a one-place predicate for the relation “ $P(x)$  if and only if  $x$  is a power of  $t$ ”,  $D_<$  is a two-place predicate for the relation “ $D_<(x, y)$  if and only if the degree of  $x$  is less than the degree of  $y$ ” and  $f_t$  is a one-placed functional symbol interpreted by  $f_t(x) = tx$  (in other words, we allow multiplication by  $t$ ). For simplicity we use 0 instead of  $\mathbf{c}_1$ , where 0 is interpreted in the usual way.

We show that the first-order theory of this structure is model-complete. This means that each first-order formula in the language of the structure is equivalent to an existential formula, i.e. a formula which consists of a finite sequence of existential quantifiers followed by a formula without quantifiers. We obtain as a consequence that the first-order theory of this structure is decidable, that is, there is an algorithm which, given any formula, decides whether it is true or not. This gives a partial answer to the open question stated by Th. Pheidas, which is open problem (1) in the list below.

Since Goedel’s Incompleteness Theorem 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  $A[t]$  in 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 showed in [2] and [3] that the existential theory of  $A[t]$  is undecidable. Both of these results are actually stronger: In  $A[t]$  one can

---

Received by the editors May 6, 2009, and, in revised form, October 19, 2009.

2000 *Mathematics Subject Classification*. Primary 03C10, 03B25, 12L05.

This work was supported by the Trimester Program on Diophantine Equations, January–April 2009, at the Hausdorff Research Institute for Mathematics, Bonn, Germany.

interpret the rational integers; thus any polynomial ring encodes recursively all the difficulties associated with number theory. In consequence, decidability can be a property of theories weaker, only, than the ring theory of  $A[t]$ . The situation is analogous to that of 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 due to L. Lipshitz in [4], that the existential theory of  $\mathbb{Z}$  in the language of addition and divisibility is decidable (but the full first-order theory is undecidable), and to A. Semenov in [11] and [10], that the elementary theory of addition and the function  $n \rightarrow 2^n$  over  $\mathbb{Z}$  is decidable.

Other general elimination results for rings of polynomials include the following: Th. Pheidas showed in his Ph.D. thesis that the existential theory of  $(\mathbb{F}_q[t]; +; |; f_t; 0, 1)$  is decidable (where  $|$  denotes divisibility) but that the analogous problem for polynomials in two variables has an undecidable existential theory. Th. Pheidas and K. Zahidi showed that the theory of the structure  $(\mathbb{F}_q[t]; +; x \rightarrow x^p; f_t; 0, 1)$  is model-complete and therefore decidable (here  $x \rightarrow x^p$  is the Frobenius function). For surveys on decidability of rings the reader may consult [5], [6], [7] and [8].

Our intention is to prove that the structure  $\mathcal{P}_q$  has reasonable elimination properties and is decidable. We prove a stronger result. In Definition 2.1 we define a set of predicates  $Q_{\bar{a}, m}$  (where  $\bar{a}$  are tuples of elements of  $\mathbb{F}_q[t]$  and  $m \in \mathbb{N}$ ) such that  $Q_{1,1} \Leftrightarrow P$ . With the help of the auxiliary predicates  $C_{\bar{a}}$  (see Definition 2.1) we prove:

**Theorem 1.1.** *The theory of the structure  $\mathcal{A}_Q = (\mathbb{F}_q[t]; +; \mathbf{c}_1, \dots, \mathbf{c}_q; f_t; \{Q_{\bar{a}, m} : \bar{a} \in ((\mathbb{F}_q[t])^*)^k, k, m \in \mathbb{N}\}; \{I_a : a \in (\mathbb{F}_q[t])^*\}; D_{<}; \{D_n : n \in \mathbb{N}\}; \{C_{\bar{a}} : \bar{a} \in ((\mathbb{F}_q[t])^*)^k : k \in \mathbb{N}\})$  is model-complete and decidable. Moreover, there is a primitive recursive algorithm which, given any first-order formula of  $\mathcal{A}_Q$ , produces an equivalent existential formula.*

We obtain the following as a corollary:

**Theorem 1.2.** *The theory of the structure  $\mathcal{P}_q$  is model-complete and decidable.*

Our approach to proving Theorem 1.2 is the following: In [12] we proved an analogue of the decidability of Presburger Arithmetic (the theory of the rational integers with addition, inequality and, for each fixed integer  $n$ , the relation  $n|x$ ) for a ring of polynomials over a finite field; in our situation the language has predicates for addition, divisibility by fixed elements and inequality of degrees, and we show that the resulting structure admits an effective elimination of quantifiers (every formula is equivalent to a quantifier-free formula). In Section 2 we extend our language by adding new relations. In the new language we are able to characterize in a simple way all existential formulae (Lemma 2.6). This characterization allows us to show that an existential formula is equivalent to a universal one. Model-completeness follows. Since  $\mathbb{F}_q[t]$  is a recursively enumerable structure, it follows from a classic argument from logic that the theory of  $\mathcal{P}_q$  is decidable.

We give the argument: Let  $\sigma$  be a sentence of  $\mathcal{P}_q$ . Then it is equivalent to an existential formula of  $\mathcal{P}_q$ , say  $\psi_1$ . Similarly  $\neg\sigma$  is equivalent to an existential formula of  $\mathcal{P}_q$ , say  $\psi_2$ . Thus the set of all sentences which are true in  $\mathcal{P}_q$  is a recursively enumerable set and its complement is also a recursively enumerable set. A well known theorem in the theory of computation (see for instance [1]) states the following:

**Theorem 1.3.** *A set  $A$  is recursive if and only if  $A$  and its complement are both recursively enumerable.*

Hence the theory of  $\mathcal{P}_q$  is decidable.

**A list of open problems.**

- (1) (Th. Pheidas) Is the theory of the structure  $(\mathbb{F}_q[t]; +; P; f_t; \mathbf{c}_1, \dots, \mathbf{c}_q; D_<; x \rightarrow x^p; \{ |_a \}_{a \in (\mathbb{F}_q[t])^*})$  decidable?
- (2) It is possible that our methods can be extended to the case of recursive algebraic extensions of  $\mathbb{F}_p$  instead of  $\mathbb{F}_q$ , but not to polynomial rings  $A[t]$  with  $A$  containing elements transcendental over the prime subfield. This is because we use the fact that all finite extensions of  $\mathbb{F}_q$  have cyclic Galois groups. Is there a corresponding lemma about such rings, analogous to Lemma 3.1, which will modify the algorithm for these rings?
- (3) For the same reason mentioned above, our methods are inadequate for showing a similar result in characteristic zero. Again, is there a lemma similar to Lemma 3.1 for polynomial rings over a field with characteristic zero?

2. AN ENRICHMENT FOR  $(\mathbb{F}_q[t]; +; |_a; P; f_t; 0, 1)$

A few words on notation: by  $\wedge, \vee, \neg$  we mean the usual logical connectives,  $\deg x$  stands for the degree of the polynomial  $x$ , and  $((\mathbb{F}_q[t])^*)^{<\mathbb{N}}$  is the set of finite sequences of elements of  $(\mathbb{F}_q[t])^*$ . In what follows, addition, multiplication and degree are meant in  $\mathbb{F}_q[t]$ .

We start by augmenting the language of the structure  $\mathcal{P}_q$  to a language  $L_Q$ .

**Definition 2.1.** Let  $q$  and  $t$  be given. We define the language

$$L_Q = \{+, \mathbf{c}_1, \dots, \mathbf{c}_q, t, f_t\} \cup \{Q_{\bar{a}, m} : \bar{a} \in ((\mathbb{F}_q[t])^*)^{<\mathbb{N}}, m \in \mathbb{N}\} \\ \cup \{ |_a : a \in (\mathbb{F}_q[t])^* \} \cup \{D_<\} \cup \{D_n : n \in \mathbb{N}\} \cup \{C_{\bar{a}} : \bar{a} \in ((\mathbb{F}_q[t])^*)^{<\mathbb{N}}\}$$

where:

- $\mathbf{c}_1, \dots, \mathbf{c}_q$  are constant symbols for each element of  $\mathbb{F}_q$ .
- For each  $n, m \in \mathbb{N}$  and for each  $\bar{a} = (a_1, \dots, a_n) \in ((\mathbb{F}_q[t])^*)^n$  the predicate  $Q_{\bar{a}, m}(\omega)$  stands for

$$\exists \bar{y} = (y_1, \dots, y_n) \\ [a_1 y_1 + \dots + a_n y_n = \omega \wedge \bigwedge_{j=1, \dots, n} y_j \in \{t^{m_s} : s \in \mathbb{N}_0\} \\ \wedge \bigwedge_{j=1, \dots, n-1} \deg(a_j y_j) < \deg(a_{j+1} y_{j+1})].$$

- For each  $n \in \mathbb{N}$  and for each  $\bar{a} = (a_1, \dots, a_n) \in ((\mathbb{F}_q[t])^*)^n$  the predicate  $C_{\bar{a}}(\omega)$  stands for

$$\exists \bar{y} = (y_1, \dots, y_n) \\ [\deg(a_1 y_1 + \dots + a_n y_n + \omega) < \deg(a_1 y_1) \wedge \bigwedge_{j=1, \dots, n} y_j \in \{t^s : s \in \mathbb{N}_0\} \wedge \deg(a_n y_n) \\ = \deg(\omega) \wedge \bigwedge_{j=1, \dots, n-1} \deg(a_j y_j) < \deg(a_{j+1} y_{j+1})].$$

- For any  $\omega_1, \omega_2 \in \mathbb{F}_q[t]$ ,  $D_<(\omega_1, \omega_2)$  stands for “ $\deg \omega_1 < \deg \omega_2$ ”.
- For given  $a \in \mathbb{F}_q[t]$ ,  $|_a(\omega)$  stands for “ $\exists x(x \cdot a = \omega)$ ”.
- For given  $n \in \mathbb{N}$ ,  $D_n(\omega)$  stands for “ $n | \deg \omega$ ”.

It is easy to check that the relations of the language  $L_Q$  can be defined by formulae of  $\{+; |_a; P; f_i; \mathbf{c}_1, \dots, \mathbf{c}_q; t, D_<\}$  and that  $P(x) \Leftrightarrow Q_{1,1}(x)$ . Thus, for brevity in our proofs, we may use the predicate  $P$  when needed.

We start with some properties of the predicate  $Q_{\bar{a},m}(\omega)$  which we will need later.

*Remark 1.* Given  $\bar{a} = (a_1, \dots, a_n)$  such that  $a_i \in \mathbb{F}_q^*$  for all  $i$ ,  $\omega$  can be written uniquely as a sum  $\sum_i a_i y_i$ , where  $y_i$  are powers of  $t$ ; i.e., given  $(a_1, \dots, a_{n_1}) \in (\mathbb{F}_q^*)^{n_1}$  and  $(b_1, \dots, b_{n_2}) \in (\mathbb{F}_q^*)^{n_2}$  such that

$$\begin{aligned} \omega &= \sum_{i \leq n_1} a_i y_i \wedge \bigwedge_i D_<(a_i y_i, a_{i+1} y_{i+1}) \bigwedge_i P(y_i), \\ \omega &= \sum_{i \leq n_2} b_i y'_i \wedge \bigwedge_i D_<(b_i y'_i, b_{i+1} y'_{i+1}) \bigwedge_i P(y'_i), \end{aligned}$$

we have that  $n_1 = n_2$ ,  $y_i = y'_i$  and  $a_i = b_i$ . The unique number  $n$  in the expansion of  $\omega$  will be called *length*. In this case, i.e., for  $\bar{a} \in (\mathbb{F}_q^*)^n$ ,  $\neg Q_{\bar{a},m}(\omega)$  is equivalent to a finite disjunction of existential formulae, which actually says that  $\omega$  has length other than  $n$ , or it has the same length but either has different coefficients or the degree of some  $y_i$  is not divisible by  $m$ .

This uniqueness does not always hold for arbitrary  $\bar{a} \in \mathbb{F}_q^n[t]$ . In our next lemma we show that there is a reduction of  $Q_{\bar{a},m}(\omega)$  to a universal existential formula in  $L_Q$ , where each relation  $Q_{\bar{b}}$  has coefficients  $b_i$  in  $\mathbb{F}_q$ .

**Lemma 2.2.** *Let  $\bar{a} \in ((\mathbb{F}_q[t])^*)^n$  and  $m \in \mathbb{N}$ . Then the formula  $Q_{\bar{a},m}(\omega)$  is equivalent to a universal formula in  $L_Q$  such that each relation symbol  $Q_{\bar{b},k}$  that occurs in it has the properties that the components of  $\bar{b}$  are in  $\mathbb{F}_q^*$  and that  $k = 1$ .*

*Proof.* Suppose that for  $1 \leq i \leq n$ ,  $a_i = \sum_j b_{ij} t^j \in \mathbb{F}_q[t]$  with  $b_{ij} \in \mathbb{F}_q^*$  and denote by  $K$  the set of pairs of indices  $(i, j)$  for which  $b_{ij} \neq 0$ . Let  $y_1, \dots, y_n$  be variables and let  $m \in \mathbb{N}$ . We consider a formula

$$\psi_\tau(\omega, \bar{y}) : \omega = a_1 y_1 + \dots + a_n y_n \wedge \bigwedge_i P(y_i) \wedge \bigwedge_i D_m(y_i) \wedge \theta \wedge \tau$$

where  $\theta$  is a quantifier-free  $L_Q$ -formula which does not contain any occurrence of the relation symbol  $Q$  and  $\tau$  is a set of conditions of the forms

- $\deg(t^j y_i) < \deg(t^h y_k)$ , where  $(i, j), (k, h) \in K$
- $\deg(t^j y_i) = \deg(t^h y_k)$ , where  $(i, j), (k, h) \in K$

that impose a linear ordering on the degrees of the terms of the set  $\{t^j y_i : b_{ij} \neq 0\}$  which implies  $\bigwedge_i D_<(a_i y_i, a_{i+1} y_{i+1})$ . We claim that  $\exists \bar{y} \psi_\tau(\omega, \bar{y})$  is equivalent to a universal formula in  $L_Q$  such that each relation symbol  $Q_{\bar{b},k}$  that occurs in it has the properties that the components of  $\bar{b}$  are in  $\mathbb{F}_q^*$  and that  $k = 1$ . We will work by induction on  $n$ . The case of  $n = 1$  follows from the fact that if there exists some  $y_1 \in \mathbb{F}_q[t]$  such that  $\omega = \sum_j b_{1j} t^j y_1 \wedge P(y_1)$ , then such  $y_1$  is unique and the corresponding  $K$  is strictly ordered. Therefore  $\exists y_1 \psi_\tau(\omega, y_1)$  is equivalent to

$$Q_{\bar{b},1}(\omega) \wedge \forall y_1 [\omega = \sum_j b_{1j} t^j y_1 \wedge P(y_1) \wedge \tau \rightarrow D_m(y_1) \wedge \theta],$$

where  $\bar{b}$  has as its components the  $b_{1j}, (1, j) \in K$ , ordered by the magnitude of  $j$ .

We proceed with the induction step. In the case where  $\tau$  contains a condition of the form  $\deg(t^j y_i) = \deg(t^h y_k)$ ,  $\psi(\omega, \bar{y})$  is equivalent to the conjunction of the formula  $y_i = t^{h-j} y_k$  and the formula that results from replacing in  $\psi_\tau(\omega, \bar{y})$  the variable  $y_i$  by the expression  $t^{h-j} y_k$  (clearing denominators if necessary). Then the result follows from the hypothesis of the induction. Hence, from now on we assume that  $\tau$  contains only conditions of the form  $\deg(t^j y_i) < \deg(t^h y_k)$ ; hence the degrees of the set  $\{t^j y_i : b_{ij} \neq 0\}$  are assumed to be strictly ordered. Consider the variables  $y_{ij}$  which are related to the variables of  $\bar{y}$  by  $y_{ij} = t^j y_i$ , for  $(i, j) \in K$ ; consider the formula

$$S : \bigwedge_{(i,j),(i,k) \in K} (t^k y_{ij} = t^j y_{ik}) \wedge \bigwedge_{(i,j) \in K} m | (\deg(y_{ij}) - j),$$

which is implied by the definition of the  $y_{ij}$  (one may need to clear denominators in  $S$  in order to make it an  $L_Q$ -formula). Solve for the variables  $y_1, \dots, y_n$  in terms of the variables  $y_{ij}$  (there can be more than one way of doing this; choose any of those), and replace each occurrence of each variable  $y_i$  in  $\psi_\tau(\omega, \bar{y})$  by the corresponding expression in the variables  $y_{ij}$  only to obtain a formula  $\bar{\psi}_\tau(\omega, \{y_{ij}\}_{(i,j) \in K})$ .

It is now obvious that  $\exists \bar{y} \psi_\tau(\omega, \bar{y})$  and  $\exists \{y_{ij}\}_{(i,j) \in K} [\bar{\psi}_\tau(\omega, \{y_{ij}\}_{(i,j) \in K}) \wedge S]$  are equivalent formulae.

Observe that the formula  $\bar{\psi}_\tau(\omega, \{y_{ij}\}_{(i,j) \in K})$  has the same form as  $\psi_\tau(\omega, \bar{y})$  except that

- a) the new coefficients  $a_i$  are elements of  $\mathbb{F}_q^*$  and
- b) the degrees of the new terms are strictly ordered (by  $\tau$ ).

By our remarks before the lemma, if there are  $y_{ij}$  such that  $\bar{\psi}_\tau(\omega, \{y_{ij}\}_{(i,j) \in K})$  holds true, then they are unique. It then follows that

$$\begin{aligned} & \exists \{y_{ij}\}_{(i,j) \in K} [\bar{\psi}_\tau(\omega, \{y_{ij}\}_{(i,j) \in K}) \wedge S] \\ & \iff Q_{\bar{b},1} \wedge \forall \{y_{ij}\}_{(i,j) \in K} [\omega = \sum_{(i,j) \in K} b_{ij} y_{ij} \wedge \bigwedge_{(i,j) \in K} P(y_{ij}) \wedge \tau \rightarrow S \wedge \theta], \end{aligned}$$

where  $\bar{b}$  has as its components the  $b_{ij}, (i, j) \in K$ , ordered according to the corresponding ordering on  $y_{ij}, (i, j) \in K$ , by  $\tau$ . Let  $T$  be the set of all linear orderings  $\tau$  on the degrees of the terms of the set  $\{t^j y_i : (i, j) \in K\}$  which implies  $\bigwedge_i D_{<}(a_i y_i, a_{i+1} y_{i+1})$ .

The statement of Lemma 2.2 follows from the fact that  $Q_{\bar{a},m}(\omega)$  is equivalent to the formula  $\bigvee_{\tau \in T} \exists \bar{y} \psi_\tau(\omega, \bar{y})$ . □

For simplicity we define  $D_=(\omega_1, \omega_2) : D_{<}(\omega_1, t\omega_2) \wedge D_{<}(\omega_2, t\omega_1)$  and

$$D_{<k}(\omega_1, \omega_2) : D_{<}(t^{k-1}\omega_1, \omega_2), \quad k \in \mathbb{N}.$$

Next we obtain a similar result for the predicate  $C_{\bar{a}}(\omega)$ .

**Lemma 2.3.** *Let  $\bar{a} = (a_1, \dots, a_n) \in ((\mathbb{F}_q[t])^*)^n$ . Then the formula  $\neg C_{\bar{a}}(\omega)$  is equivalent to an existential formula in  $L_Q$ .*

*Proof.* Let  $\bar{a} = (a_1, \dots, a_n) \in (\mathbb{F}_q[t] \setminus \{0\})^n$  and  $\omega \in \mathbb{F}_q[t]$ . We define  $a_0 = a_{n+1} = 0$ .

*Claim.* The formula  $\chi_{\bar{a}}(\omega)$

$$\exists \bar{y} = (y_1, \dots, y_n) \left[ \bigwedge_{j=1}^n P(y_j) \wedge \deg(a_n y_n) = \deg(\omega) \wedge \bigwedge_{j=1}^{n-1} \deg(a_j y_j) < \deg(a_{j+1} y_{j+1}) \right]$$

is equivalent to the quantifier-free formula

$$Cnd_{\bar{a}}(\omega) : D_{<}(a_n, t\omega) \wedge D_{<}(t^0 a_{n-1}, \omega) \wedge \dots \wedge D_{<}(t^{n-2} a_1, \omega).$$

*Proof of the claim.* Assume that there are  $y_j \in \{t^s : s \in \mathbb{N}_0\}$  such that  $\deg(a_0 y_0) < \dots < \deg(a_n y_n) = \deg(\omega)$ . This implies that  $\deg(a_n) \leq \deg(\omega)$  and  $\deg(a_{n-i}) <_i \deg(\omega)$ , for all  $i = 1, \dots, n$ ; i.e.,  $Cnd_{\bar{a}}(\omega)$  holds.

Conversely, assume that  $Cnd_{\bar{a}}(\omega)$  holds. For each  $j = 1, \dots, n$  define  $y_j = t^{\deg(\omega) - n + j - \deg(a_j)}$ . Then it is easy to check that these  $y_j$  evaluate  $\chi_{\bar{a}}(\omega)$ . Note that this is not always a unique evaluation.  $\square$

We proceed with the proof of Lemma 2.3. In Figure 1 we illustrate the cases that arise if  $Cnd_{\bar{a}}(\omega)$  holds. The figure can be viewed as a directed finite tree of vertices (formulae) with the edges being implications among formulae.

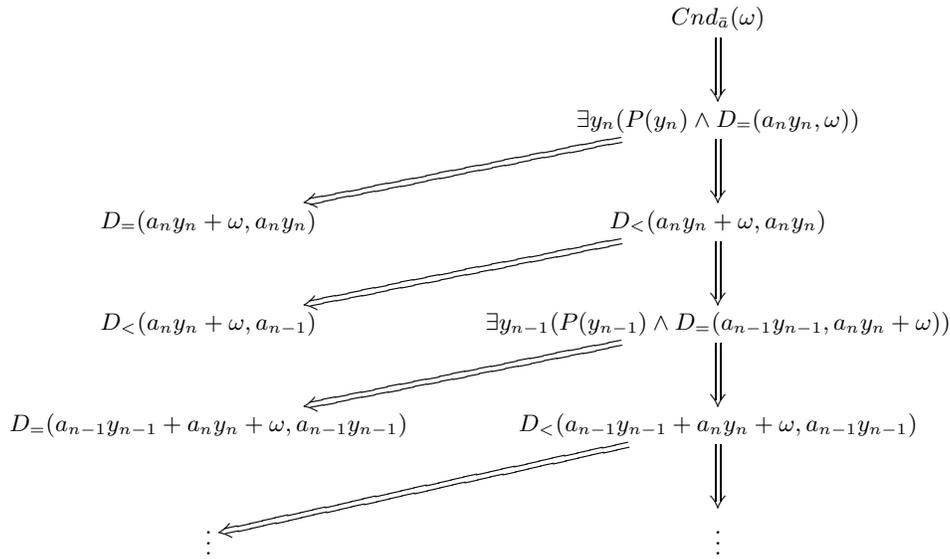


FIGURE 1.  $Cnd_{\bar{a}}(\omega)$

Due to the claim and the analysis of Figure 1, we have that  $\neg C_{\bar{a}}(\omega)$  holds if and only if either  $\neg Cnd_{\bar{a}}(\omega)$  holds or the left leaf of some level holds on the binary tree of Figure 1. Thus  $\neg C_{\bar{a}}(\omega)$  is equivalent to

$$\neg Cnd_{\bar{a}}(\omega) \vee \exists \bar{y} = (y_0, \dots, y_{n+1}) \left[ \bigwedge_{j=0}^{n+1} P(y_j) \wedge \left( \bigvee_{i_0=1}^n [h_{i_0}(\bar{y}, \omega) \wedge \bigwedge_{i=i_0}^n \psi_i(\bar{y}, \omega)] \right) \right],$$

where  $h_{i_0}(\bar{y}, \omega)$  is the formula  $D_{<}(a_{i_0} y_{i_0} + \dots + a_n y_n + \omega, a_{i_0-1}) \vee D_{=}(a_{i_0} y_{i_0} + \dots + a_n y_n, a_{i_0} y_{i_0})$  and the formula  $\psi_i(\bar{y}, \omega)$  is  $D_{=}(a_i y_i, a_{i+1} y_{i+1} + \dots + a_n y_n + \omega) \wedge D_{<}(a_i y_i + \dots + a_n y_n + \omega, a_i y_i)$ .  $\square$

We continue by giving a first description of an arbitrary existential formula in the language  $L_Q$ .

**Lemma 2.4.** *Every existential formula of  $L_Q$  is equivalent to a finite disjunction of formulae of the form*

$$(1) \quad \sigma(\bar{\omega}) : \sigma_0 \wedge \exists \bar{x} = (x_1, \dots, x_n) \exists \bar{y} = (y_1, \dots, y_m) (\sigma_1 \wedge \sigma_3 \wedge \sigma_4 \wedge \sigma_5 \wedge \sigma_6)$$

where  $\sigma_0$  is a quantifier-free formula with parameters  $\bar{\omega}$  and  $\sigma_1, \dots, \sigma_6$  have the following forms:

$$(2) \quad \sigma_1(\bar{x}, \bar{y}, \bar{\omega}) : \bigwedge_i f_i(\bar{x}) + g_i(\bar{y}) = h_i(\bar{\omega}) ,$$

$$(3) \quad \sigma_3(\bar{y}) : \bigwedge_{j=1}^m P(y_j),$$

$$(4) \quad \sigma_4(\bar{x}, \bar{y}, \bar{\omega}) : \bigwedge_{\rho} D_{<}(\pi_{\rho}(\bar{x}, \bar{y}, \bar{\omega}), \pi'_{\rho}(\bar{x}, \bar{y}, \bar{\omega})) ,$$

$$(5) \quad \sigma_5(\bar{x}, \bar{y}, \bar{\omega}) : \bigwedge_{\lambda} |_{c_{\lambda}} (\chi_{\lambda}(\bar{x}, \bar{y}, \bar{\omega})) ,$$

$$(6) \quad \sigma_6(\bar{x}, \bar{\omega}) : \bigwedge_{\xi} D_{n_{\xi}}(\chi'_{\xi}(\bar{x}, \bar{\omega})) ,$$

where  $\omega_1, \dots, \omega_s$  are all the free (i.e. non-quantified) variables of  $\sigma$  and  $\bar{\omega} = (\omega_1, \dots, \omega_s)$ ; each index  $i, \rho, \lambda, \xi$  ranges over a finite set; each  $c_{\lambda}$  is a fixed element of  $\mathbb{F}_q[t]$ ; each of  $f_i, g_i, h_i, \pi_{\rho}, \pi'_{\rho}, \chi_{\lambda}, \chi'_{\xi}$  is a degree-one polynomial of the indicated variables over  $\mathbb{F}_q[t]$ ; and each of  $f_i, g_i$  is a homogeneous polynomial.

*Proof.* It is obvious that given an existential formula  $\varphi(\bar{\omega}) = \exists \bar{x} \psi(\bar{x}, \bar{\omega})$  with free variables only among those of  $\bar{\omega}$  and with  $\psi$  quantifier-free, the open formula  $\psi(\bar{x}, \bar{\omega})$  can be written equivalently as a boolean combination of atomic formulae of the following forms:

$$D_{<}(\pi_1(\bar{x}, \bar{\omega}), \pi_2(\bar{x}, \bar{\omega})), \quad c|\pi(\bar{x}, \bar{\omega}), \quad D_n(\pi(\bar{x}, \bar{\omega})), \\ Q_{\bar{a}, m}(\pi(\bar{x}, \bar{\omega})), \quad C_{\bar{a}}(\pi(\bar{x}, \bar{\omega})), \quad \pi(\bar{x}, \bar{\omega}) = 0,$$

where  $\pi, \pi_1$  and  $\pi_2$  are degree-one polynomials of the indicated variables,  $c \in (\mathbb{F}_q[t])^*$  and  $\bar{a} = (a_1, \dots, a_n) \in ((\mathbb{F}_q[t])^*)^n$ . The details of the proof of this fact are easy and are left to the reader.

Therefore, in order to prove the lemma, it suffices to show that the negation of an atomic formula of each of the first four kinds is equivalent to a positive (i.e. without negations) boolean combination of formulae of the forms of  $\sigma_1, \dots, \sigma_6$ . We have:

- $\pi(\bar{x}, \bar{\omega}) \neq 0$  is equivalent to  $D_{<}(0, \pi(\bar{x}, \bar{\omega})) \vee \bigvee_{b \in \mathbb{F}_q^*} \pi(\bar{x}, \bar{\omega}) = b$ .
- $\neg D_{<}(\pi_1, \pi_2)$  is equivalent to  $D_{<}(\pi_2, \pi_1) \vee [D_{<}(\pi_1, t\pi_2) \wedge D_{<}(\pi_2, t\pi_1)]$ .
- $c \nmid \pi(\bar{x}, \bar{\omega})$  is equivalent to  $\bigvee_{\deg(r) < \deg(c), r \neq 0} c|\pi + r$ .
- $\neg D_n(\pi)$  is equivalent to  $\bigvee_{m < n, m \neq 0} D_n(\pi t^m)$ .
- $\neg Q_{\bar{a}, m}(\pi)$ , according to Lemma 2.2, is equivalent to a positive existential formula of  $L_Q$ .
- $\neg C_{\bar{a}}(\pi)$ , according to Lemma 2.3, is equivalent to a positive existential formula of  $L_Q$ .  $\square$

In [12] we proved the elimination of quantifiers in the sub-language

$$L_0 = \{+, 0, 1, t, f_t\} \cup \{ |a : a \in \mathbb{F}_q[t] \} \cup \{D_{<}\} \cup \{D_n : n \in \mathbb{N}\};$$

that is, we proved:

**Proposition 2.5.** *Every formula of  $L_0$  is equivalent to a quantifier-free formula of  $L_0$ .*

Our next step is to eliminate the existentially quantified variables  $\bar{x}$  from the formulas  $\sigma$  in the conclusion of Lemma 2.4, so the existential quantifier is applied only to variables that are declared to be powers of  $t$ .

**Lemma 2.6.** *Every existential formula  $\sigma$  of  $L_Q$  is equivalent to a finite disjunction of formulae of the form*

$$(7) \quad \varphi(\bar{\omega}) : \varphi_0 \wedge \exists \bar{y} (\varphi_1 \wedge \varphi_3 \wedge \varphi_4 \wedge \varphi_5 \wedge \varphi_6)$$

where  $\varphi_0(\bar{\omega})$  is a quantifier-free formula and the  $\varphi_1, \dots, \varphi_6$  have the following forms:

$$(8) \quad \varphi_1(\bar{y}, \bar{\omega}) : \bigwedge_i g_i(\bar{y}) = h_i(\bar{\omega}),$$

$$(9) \quad \varphi_3(\bar{y}) : \bigwedge_{j=1}^m P(y_j),$$

$$(10) \quad \varphi_4(\bar{y}, \bar{\omega}) : \bigwedge_{\rho} D_{<}(\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega}), \pi'_{1,\rho}(\bar{y}) + \pi'_{2,\rho}(\bar{\omega})),$$

$$(11) \quad \varphi_5(\bar{y}, \bar{\omega}) : \bigwedge_{\lambda} |_{c_\lambda} (\chi_{1,\lambda}(\bar{y}) + \chi_{2,\lambda}(\bar{\omega})),$$

$$(12) \quad \varphi_6(\bar{y}, \bar{\omega}) : \bigwedge_{\xi} D_{n_\xi}(\chi'_{1,\xi}(\bar{y}) + \chi'_{2,\xi}(\bar{\omega})),$$

where  $\bar{y} = (y_1, \dots, y_m)$ ,  $\omega_1, \dots, \omega_s$  are all the free (i.e. non-quantified) variables of  $\sigma$  and  $\bar{\omega} = (\omega_1, \dots, \omega_s)$ ; each index  $i, \rho, \lambda, \xi$  ranges over a finite set; each  $c_\lambda$  is a fixed element of  $\mathbb{F}_q[t]$ ; each of  $g_i, h_i, \pi_{1,\rho}, \pi_{2,\rho}, \pi'_{1,\rho}, \pi'_{2,\rho}, \chi_{1,\lambda}, \chi_{2,\lambda}, \chi'_{1,\xi}, \chi'_{2,\xi}$  is a degree-one polynomial of the indicated variables over  $\mathbb{F}_q[t]$ ; and each of  $g_i, \pi_{1,\rho}, \pi'_{1,\rho}, \chi_{1,\lambda}, \chi'_{1,\xi}$  is a homogeneous polynomial.

*Proof.* We may assume that  $\sigma$  is of the form given in the conclusion of Lemma 2.4. Our goal is to eliminate all the existentially quantified variables which are not declared to be a power of  $t$ . Note that  $\sigma$  is equivalent to  $\sigma_0 \wedge \exists \bar{y} = (y_1, \dots, y_m) [\sigma_3 \wedge \exists \bar{x} = (x_1, \dots, x_n) (\sigma_1 \wedge \sigma_4 \wedge \sigma_5 \wedge \sigma_6)]$ . The formula  $\psi(\bar{y}, \bar{\omega}) : \exists \bar{x} (\sigma_1 \wedge \sigma_4 \wedge \sigma_5 \wedge \sigma_6)$  is a formula in the sub-language  $L_0 = \{+, 0, 1, t, f_t\} \cup \{ |a : a \in \mathbb{F}_q[t] \} \cup \{D_{<}\} \cup \{D_n : n \in \mathbb{N}\}$ .

Thus, according to Proposition 2.5,  $\psi(\bar{y}, \bar{\omega})$  is equivalent to a quantifier-free formula in the language  $L_0$  and therefore in  $L$ .  $\square$

### 3. MODEL-COMPLETENESS OF $\mathbb{F}_q[t]$ IN $L_Q$

In this section we shall prove that any existential formula of  $L_Q$  is equivalent to a universal formula. This will complete the claim of Theorem 1.2 on model-completeness. In order to prove this, we first show that the formula of type  $\varphi_5$  can be omitted. Then we list several remarks which aim to show how to separate the variables appearing in  $\varphi$  (as given in Lemma 2.6) into two categories. The

first category contains those variables which postulate uniqueness and the second category contains variables that can be eliminated.

At this point we state the following lemma, which is a known result from the theory of finite fields.

**Lemma 3.1.** *Let  $a(t) \in \mathbb{F}_q[t]$  with  $t \nmid a(t)$ . Then there is some  $m \in \mathbb{N}$  such that  $a(t)|t^m - 1$ .*

*Proof.* If  $a(t)$  is irreducible and  $t$  does not divide  $a$  in  $\mathbb{F}_q[t]$ , then the ring  $\mathbb{F}_q[t]/(a)$  is a finite field and the image of  $t$  under the natural morphism in that field is not the 0 element. Hence the image of  $t$ , as an element of the multiplicative group of that field, has finite order, say  $r$ . Then  $a(t)|t^r - 1$ .

Now let  $a(t) \in \mathbb{F}_q[t]$  with  $t \nmid a(t)$  and let  $a(t) = a_1^{r_1}(t) \dots a_k^{r_k}(t)$  where  $a_i(t)$  are irreducible polynomials. Thus  $a_i(t)|t^{k_i} - t$  for some finite and non-zero  $k_i$ . It follows that  $a(t)|t^{\prod_i k_i} - 1$ . □

**Lemma 3.2.** *Assume that  $c|ay + b$  holds for some  $y = t^k$ , for some  $k \in \mathbb{N}_0$ , where  $a, b, c \in \mathbb{F}_q[t]$  and  $t \nmid c$ . Then for every  $l \geq k$  there is a solution  $y'$  of  $c|ay + b$ , where  $y'$  is a power of  $t$  and  $\deg(y') > l$ .*

*Proof.* Given that  $t \nmid c$ , there is some  $n > 0$  such that  $c|t^n - 1$  (due to Lemma 3.1), i.e.,  $t^n \equiv 1 \pmod{c}$ . Thus

$$c|ay + b \iff at^k \equiv -b \pmod{c} \iff at^k t^n \equiv -b \pmod{c} \iff c|ayt^n + b.$$

Therefore, we obtain another solution  $y' = yt^n$ , which is a power of  $t$  and with  $\deg(y') > \deg(y)$ . □

**Lemma 3.3.** *In the conclusion of Lemma 2.6 the formula of type  $\varphi_5$  can be omitted.*

*Proof.* It is enough to show that the formula

$$\psi(y) : c|ay + b \wedge P(y),$$

with  $a, b, c \in \mathbb{F}_q[t]$ , is equivalent to a quantifier-free formula with every relation that contains the variable  $y$  belonging to  $L \setminus \{ |_a : a \in \mathbb{F}_q[t] \}$ . Let  $c = c_1 t^v$ , with  $t \nmid c_1$ . Consider the following cases:

*Case 1.*  $v = 0$ . Then according to Lemma 3.2 there are either no solutions or infinitely many solutions. In any case, it is enough to test  $y = t^i$ , with  $i < n$ , where  $n$  is the smallest positive integer as given in the conclusion of Lemma 3.1, i.e.,  $t^n \equiv 1 \pmod{c}$ . Thus  $\psi(y)$  is equivalent to

$$P(y) \wedge \bigvee_{0 \leq i \leq n-1} [D_n(t^{n-i}y) \wedge c|at^i + b].$$

*Case 2.*  $v \neq 0$  and  $t^v \nmid b$ . Then there are finitely many possible solutions and  $\psi(y)$  is equivalent to

$$\bigvee_{0 \leq i \leq v-1} [y = t^i \wedge c|at^i + b].$$

*Case 3.*  $v \neq 0$  and  $t^v | b$ . Let  $a = a_1 t^\mu$  and  $b = b_1 t^v$ , where  $\mu$  is the maximal power of  $t$  that divides  $a$  and is less than or equal to  $v$ . Thus  $\psi(y)$  is equivalent to

$$c_1 | a_1 y + b_1 \wedge P(y) \wedge D_{<}(t^{v-\mu}, ty).$$

Given that  $t \nmid c_1$ , we consider the smallest  $n_1 \in \mathbb{N}$  from the conclusion of Lemma 3.1 such that  $t^{n_1} \equiv 1 \pmod{c_1}$ . Therefore  $\psi(y)$  is equivalent to

$$P(y) \wedge D_{<}(t^{v-\mu}, ty) \wedge \bigvee_{0 \leq i \leq n_1-1} [D_{n_1}(t^{n_1-i}y) \wedge c_1 | a_1 t^i + b_1].$$

We establish a technical fact which will be crucial in what follows.

**Proposition 3.4.** *Assume that  $a_j \in (\mathbb{F}_q[t])^*$  and that  $Q_{\bar{a},m}(\omega)$  holds with  $\bar{a} = (a_1, \dots, a_n)$ . Then there is a unique  $\bar{y} = (y_1, \dots, y_n)$  such that*

$$\begin{aligned} [a_1 y_1 + \dots + a_n y_n = \omega \wedge \bigwedge_{j=1, \dots, n} y_j \in \{t^{ms} : s \in \mathbb{N}_0\} \\ \wedge \bigwedge_{j=1, \dots, n-1} \deg(a_j y_j) < \deg(a_{j+1} y_{j+1})]. \end{aligned}$$

*Proof.* Assume that  $\bar{y} = (y_1, \dots, y_n)$  is such that

$$\begin{aligned} [a_1 y_1 + \dots + a_n y_n = \omega \wedge \bigwedge_{j=1, \dots, n} y_j \in \{t^{ms} : s \in \mathbb{N}_0\} \\ \wedge \bigwedge_{j=1, \dots, n-1} \deg(a_j y_j) < \deg(a_{j+1} y_{j+1})] \end{aligned}$$

and the same for  $\bar{y}' = (y'_1, \dots, y'_n)$ . Then  $\deg(a_n y_n) = \deg(a_1 y_1 + \dots + a_n y_n) = \deg(a_1 y'_1 + \dots + a_n y'_n) = \deg(a_n y'_n)$ . So  $\deg(y_n) = \deg(y'_n)$  and hence  $y_n = y'_n$ . The conclusion follows by induction on  $n$ .  $\square$

*Remarks.* Throughout the remarks of the next few paragraphs we consider a relation  $R$  over  $\mathbb{F}_q[t]$  defined by a formula  $\exists y \varphi$  which is as in the conclusion of Lemma 2.6 but with the sub-formula  $\varphi_5$  omitted. We will transform  $\varphi$  into an equivalent formula (i.e. a definition of  $R$  as well) with a concrete form.

1. **H1:** We let  $K$  be a set of terms of the form  $ay_i$ , where  $a \in (\mathbb{F}_q[t])^*$  and  $y_i$  is a variable, with the following property: each of the terms  $g_i, \pi_{1,\rho}, \pi'_{1,\rho}, \chi'_{1,\xi}$  mentioned in the conclusion of Lemma 2.6 is a sum of elements of  $K$ . Let  $\Omega$  be a set of the terms  $h_i, \pi_{2,\rho}, \pi'_{2,\rho}, \chi'_{2,\xi}$  mentioned in the conclusion of Lemma 2.6.
2. Assume that the formula  $\varphi_4$  implies a formula equivalent to the formula  $D_{=}(ay_i, by_j)$  for some terms  $ay_i$  and  $by_j$  of  $K$ , with  $i \neq j$ . This implies
  - (I)  $y_i = t^{\deg(b)-\deg(a)} y_j$  if  $\deg(a) \leq \deg(b)$  and
  - (II)  $y_i = t^{\deg(a)-\deg(b)} y_j$  otherwise.

Hence we can replace  $y_i$  by terms which involve only the remaining variables and obtain a new definition of the relation  $R$  with fewer variables. Thus, taking a disjunction over all strict orderings of the degrees of the elements of  $K$ , we can assume that the formula  $\varphi_4$  implies a strict ordering of the terms of  $K$ . In a similar manner we augment the latter ordering to a linear ordering of the set  $K \cup \Omega$ . Now observe that this ordering implies that the degree of each of the terms  $g_i, \pi_{1,\rho}, \pi'_{1,\rho}, \chi'_{1,\xi}$  mentioned in the conclusion of Lemma 2.6 is equal to the degree of a specific element of  $K$  (recall that each  $y_i$  is assumed to be a power of  $t$ ). Note that the ordering on the degrees of terms of  $K \cup \Omega$  need not be strict.

Next, we observe that if the ordering of degrees of elements of  $K$  implies  $\deg(ay_i) < \deg(by_j) < \deg(cy_i)$ , then we obtain as a conclusion that the

possible values of  $\deg(y_j)$  are in the (finite) set  $\{\deg(y_i) + \deg(a) - \deg(b) + 1, \dots, \deg(y_i) + \deg(c) - \deg(b) - 1\}$ , which again allows elimination of the variable  $y_j$ , as above. Taking a disjunction over the possible cases we can assume without loss of generality that this situation does not occur. We re-enumerate the variables of  $y$  in accordance with the ordering of  $K$ . We replace the formula  $\varphi_4$  in  $\varphi$  by a formula  $\varphi_4 \wedge \varphi'_4$ , where  $\varphi'_4$  states the above-mentioned ordering of  $K \cup \Omega$ , i.e.

**H2:** *The formula  $\varphi'_4$  is*

$$\bigwedge_{i=1}^{m-1} D_{<}(a_i y_i, a_{i+1} y_{i+1}) \wedge \bigwedge_k D_{<}(b_k y_k, \omega_k) \wedge \bigwedge_r D_{<}(\omega'_r, c_r y_r) \wedge \bigwedge_\ell D_{=}(\omega''_\ell, d_\ell y_\ell)$$

where  $a_i, b_k, c_r, d_\ell \in (\mathbb{F}_q[t])^*$  and  $\omega_k, \omega'_r, \omega''_\ell \in \Omega$  and  $\varphi_4 \wedge \varphi'_4$  imply a linear ordering  $\tau$  of the degrees of elements of  $K \cup \Omega$  whose restriction to the degrees of elements of  $K$  is a strict ordering.

3. A variable  $y_i$  whose degree, according to  $\tau$ , is bounded above by the degree of a linear combination of terms in  $\Omega$  will be called *bounded*; otherwise, it will be called *unbounded*.

Observe that an upper bound for the degree of a variable  $y_i$  is implied by each equation in which  $y_i$  occurs: The degree of the right-hand side of such an equation is an upper bound because there are no cancellations among the highest-degree terms of the elements of  $K$  which occur on the left-hand side. Thus we may assume, without loss of generality,

**H3:** *Every variable that occurs in an equation (in  $\varphi_1$ ) with non-zero coefficient is bounded.*

4. Next, assume that  $e_m y_m$  is the element of  $K$  of highest degree and assume that  $y_m$  is an unbounded variable. It is obvious that  $y_m$  cannot occur in an atomic formula of the form  $D_{<}(a y_m, \dots)$  (with  $y_m$  occurring on the left). Let  $a' y_m$  be the term that occurs in  $\chi'_{1,\xi}(\bar{y})$  with  $a' \neq 0$ . Then we have that  $D_{n_\xi}(\chi'_{1,\xi}(\bar{y}) + \chi'_{2,\xi}(\bar{\omega}))$  is equivalent to  $D_{n_\xi}(a' y_m)$ . Therefore  $y_m$  occurs only in atomic formulae of the forms  $P(y_m)$ ,  $D_{<}(\dots, a y_m)$  and  $D_{n_\xi}(a y_m)$ . Let  $D_{n_{\xi_1}}(a_1 y_m), \dots, D_{n_{\xi_f}}(a_f y_m)$  be all the atomic formulae of the form  $D_{n_\xi}(a y_m)$  in which  $y_m$  occurs.

If there is  $\bar{y}_m$  such that

$$(13) \quad D_{n_{\xi_1}}(a_1 y_m) \wedge \dots \wedge D_{n_{\xi_f}}(a_f y_m)$$

is true for  $y_m = \bar{y}_m$ , then  $D_{n_{\xi_1}}(a_1 y_m) \wedge \dots \wedge D_{n_{\xi_f}}(a_f y_m) \wedge P(y_m) \wedge D_{<}(\dots, a y_m)$  is true for  $y_m = \tilde{y}_m$ , for some  $\tilde{y}_m$  of sufficiently large degree. Hence the formula that results from  $\varphi$  by deleting all atomic formulae in which  $y_m$  occurs with non-zero coefficient is equivalent to  $\varphi$ .

In the case (13) has no solution, the formula  $\varphi$  is not satisfiable.

Hence we assume:

**H4:** *Every variable that occurs in  $\varphi$  is bounded.*

5. With notation as in the conclusion of Lemma 2.6, we augment  $K \cup \Omega$  by the set  $N$  which consists of the terms  $\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega})$ ,  $\pi'_{1,\rho}(\bar{y}) + \pi'_{2,\rho}(\bar{\omega})$ , and  $\chi'_{1,\xi}(\bar{y}) + \chi'_{2,\xi}(\bar{\omega})$  that occur in the formulae  $\varphi_4$  and  $\varphi_6$ . We take a disjunction over all possible extensions of the ordering  $\tau$  to a linear ordering of the set of degrees of elements of the set  $K \cup \Omega \cup N$ . So from now on we assume:

**H5:** *The ordering  $\tau$  implies a linear ordering of the degrees of the elements of the set  $K \cup \Omega \cup N$ .*

6. Now observe that for any term  $d$  the formula  $D_{n_1}(d) \wedge D_{n_2}(d)$  is equivalent (over  $\mathbb{F}_q[t]$ ) to the formula  $D_{\text{lcm}(n_1, n_2)}(d)$ , where  $\text{lcm}(n_1, n_2)$  stands for the least common multiple of  $n_1$  and  $n_2$ . Moreover, for any term  $d$ ,  $D_1(d)$  holds trivially. So we assume:

**H6:** *For each term  $d \in K \cup \Omega \cup N$  there is exactly one relation of the form  $D_n(d)$ .*

7. Consider  $\tau$  to be a linear ordering of the degrees of the elements of the set  $K \cup \Omega \cup N$  as defined above. With notation as in the conclusion of Lemma 2.6, let  $\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega}) \in N$ . Note that  $\pi_{1,\rho}(\bar{y}) = a_1y_{i_1} + \dots + a_ry_{i_r}$ , for some  $a_jy_{i_j} \in K$ , with  $\deg(a_jy_{i_j}) < \deg(a_{j+1}y_{i_{j+1}})$  for all  $j = 1, \dots, r - 1$ . Consider the following cases:

(a) If  $\deg(a_ry_{i_r}) \neq \deg(\pi_{2,\rho}(\bar{\omega}))$ , then we remove  $\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega})$  from  $N$  and replace  $\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega})$  in  $\varphi$  by the one of  $a_ry_{i_r}$  and  $\pi_{2,\rho}(\bar{\omega})$  whose degree is bigger.

(b) If  $\deg(\pi_{1,\rho}(\bar{y})) = \deg(\pi_{2,\rho}(\bar{\omega}))$ , then there are the following cases:

(b<sub>1</sub>) There is no cancellation of highest-degree terms, i.e.,  $\deg(\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega})) = \deg(\pi_{2,\rho}(\bar{\omega}))$ . Then modify  $\varphi_4$  by replacing each occurrence of  $\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega})$  by  $\pi_{2,\rho}(\bar{\omega})$ , remove  $\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega})$  from  $N$  and add to  $\varphi_4$  the atomic formula  $D_{=(a_ry_{i_r}, \pi_{2,\rho})} \wedge D_{=(a_ry_{i_r} + \pi_{2,\rho}, \pi_{2,\rho})}$ .

(b<sub>2</sub>) Let  $\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega}) = 0$ . Then replace  $\varphi_1$  by  $\varphi_1 \wedge \pi_{1,\rho}(\bar{y}) = -\pi_{2,\rho}(\bar{\omega})$  and modify  $\varphi_4$  by replacing each occurrence of  $\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega})$  by 0.

(b<sub>3</sub>) Let  $\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega}) \neq 0$ . From the assumptions we have made in this remark, there is  $\beta \in \{0, 1, \dots, r - 1\}$  such that

$$\deg(a_\beta y_{i_\beta}) < \deg(\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega})) < \deg(a_{\beta+1}y_{i_{\beta+1}}),$$

where  $a_0y_{j_0} = 0$ . Then modify  $\varphi_4$  by replacing each occurrence of  $\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega})$  by  $a_{\beta+1}y_{i_{\beta+1}} + \dots + a_ry_{i_r} + \pi_{2,\rho}(\bar{\omega})$ .

Similarly, we repeat the above procedure for all  $\pi'_{1,\rho}(\bar{y}) + \pi'_{2,\rho}(\bar{\omega}), \chi'_{1,\xi}(\bar{y}) + \chi'_{2,\xi}(\bar{\omega}) \in N$  with notation as in the conclusion of Lemma 2.6.

**H7:** *Each element of  $N$  is of the form  $a_1y_1 + \dots + a_ny_n + \omega$ , for some  $a_iy_i \in K$  and  $\omega \in \Omega$  such that the relation  $C_{(a_1, \dots, a_n)}(\omega)$  holds.*

8. Now we change the notation as follows: We rewrite the variables of  $\bar{y}$  as  $(\bar{y}, \bar{z})$ , where  $\bar{y} = (y_1 \dots, y_\ell)$  and  $\bar{z} = (z_1, \dots, z_{m-\ell})$ , in such a way that:

- Each variable  $y_i$  occurs (with non-zero coefficient  $a$ ) in an equation (of  $\varphi_1$ ) or in some element of the set  $N$ , or  $D_{=(ay_i, \omega)}$  holds for some  $\omega \in \Omega$ .
- No variable  $z_j$  occurs in  $\varphi_1$  or in any element of the set  $N$ , nor does any atomic subformula of the form  $D_{=(az_i, \omega)}$  occur for any  $\omega \in \Omega$ .

**Proposition 3.5.** *Let  $a_1, \dots, a_n \in \mathbb{F}_q[t]$ . Consider a formula  $\psi_n(y_1, \dots, y_n, \omega)$  of the form*

$$(14) \quad D_{<}(a_1y_1 + \dots + a_ny_n + \omega, a_1y_1) \wedge \bigwedge_{i=1}^n P(y_i) \wedge \bigwedge_{i=1}^{n-1} D_{<}(a_iy_i, a_{i+1}y_{i+1}) \wedge D_{=(a_ny_n, \omega)}.$$

*Given  $\omega$ , if there are some  $y_1, \dots, y_n \in \mathbb{F}_q[t]$  which satisfy  $\psi_n$ , then they are unique.*

*Proof.* Let  $a_1, \dots, a_n, \omega \in \mathbb{F}_q[t]$ . Consider any  $y_1, \dots, y_n, y'_1, \dots, y'_n \in \mathbb{F}_q[t]$  such that the formula  $\psi_n(y_1, \dots, y_n, \omega) \wedge \psi_n(y'_1, \dots, y'_n, \omega)$  holds true. Therefore  $\deg(a_n y_n) = \deg(\omega) = \deg(a_n y'_n)$  and  $P(y_n) \wedge P(y'_n)$ . Thus  $y_n = y'_n$  and  $\psi_n(y_1, \dots, y_n, \omega)$  is equivalent to  $\psi_{n-1}(y_1, \dots, y_{n-1}, \omega + y_n)$ . The conclusion follows by induction on  $n$ .  $\square$

**Lemma 3.6.** *Every formula  $\varphi$  which is as in the conclusion of Lemma 2.6 is equivalent to a disjunction of formulae of the form*

$$(15) \quad \varphi'_0 \wedge \forall \bar{y} [\varphi_1(\bar{y}, \bar{\omega}) \wedge \varphi'_4(\bar{y}, \bar{\omega}) \wedge \varphi_3(\bar{y}) \rightarrow \exists \bar{z} [\varphi_3(\bar{z}) \wedge \varphi_4(\bar{y}, \bar{z}, \bar{\omega}) \wedge \varphi_6(\bar{y}, \bar{z}, \bar{\omega})]]]$$

where  $\varphi'_0$  is a quantifier-free formula,  $\varphi'_4$  is as given in **H2** and  $\varphi_1, \dots, \varphi_6$  are as in the conclusion of Lemma 2.6 but with the variables  $\bar{y}$  replaced by the tuple  $(\bar{y}, \bar{z})$  (with the same convention on  $z$  as in the last paragraph before Proposition 3.5).

*Proof.* Let  $\psi_1(x)$  and  $\psi_2(x)$  be formulae (of any language) with free variables among those of  $x$  ( $x$  is a tuple of variables). Assume that whenever  $\psi_1(x)$  is satisfied by some  $x = a$ , this value of  $x$  is unique (i.e. no other value satisfies  $\psi_1$ ). Then

$$\exists x [\psi_1(x) \wedge \psi_2(x)] \text{ is equivalent to } [\exists x \psi_1(x) \wedge \forall x (\psi_1(x) \rightarrow \psi_2(x))]$$

(the verification of this trivial fact is left to the reader). Therefore, in order to prove the lemma it suffices to show that whenever there is a  $\bar{y}$  such that  $\varphi_1(\bar{y}, \bar{\omega}) \wedge \varphi_4(\bar{y}, \bar{\omega}) \wedge \varphi_3(\bar{y})$  holds true, that  $\bar{y}$  is unique. The uniqueness of  $\bar{y}$  follows from Propositions 3.4 and 3.5, while the existence of  $\bar{y}$  is implied by  $\varphi'_0$ , which is the following quantifier-free formula of  $L_Q$ :

$$\varphi_0 \wedge \bigwedge_{(\bar{a}, \bar{\omega}) \in \bar{N}} Q_{\bar{a}}(\bar{\omega}) \wedge \bigwedge_{(\bar{a}, \bar{\omega}) \in \bar{\Phi}_1} D_{\bar{a}}(\bar{\omega}),$$

where

$$\begin{aligned} \bar{N} &= \{((a_1, \dots, a_n), \bar{\omega}) : n \in \mathbb{N} \text{ and there are some variables } y_{i_1}, \dots, y_{i_n} \\ &\quad \text{and a polynomial } \pi \text{ such that } a_1 y_{i_1} + \dots + a_n y_{i_n} + \pi(\bar{\omega}) \in N\}, \\ \bar{\Phi}_1 &= \{((a_1, \dots, a_n), \bar{\omega}) : n \in \mathbb{N} \text{ and there are some variables } y_{i_1}, \dots, y_{i_n} \\ &\quad \text{and a polynomial } h \text{ such that } a_1 y_{i_1} + \dots + a_n y_{i_n} = h(\bar{\omega}) \\ &\quad \text{is a sub-formula of } \varphi_1\}. \end{aligned} \quad \square$$

*Remark 9.* Consider the following formula  $S(\omega_1, \omega_2, z_1, \dots, z_\zeta)$ :

$$\begin{aligned} \deg(\omega_1) < \deg(a_{1,1} z_1) < \dots < \deg(a_{1,r_1} z_1) < \dots < \deg(a_{\zeta,r_\zeta} z_\zeta) < \deg(\omega_2) \wedge \\ &\bigwedge_{i,j} D_{n_{i,j}}(a_{i,j} z_i) \wedge \bigwedge_i P(z_i). \end{aligned}$$

We define the *size* between two consecutive terms of the sequence  $S$  as follows:

$$(16) \quad size(s_j, s_{j+1}) = \begin{cases} n_{1,1} - \text{rem}(\deg(s_j), n_{1,1}) & \text{if } s_j = \omega_1, \\ \deg(a_{i,k+1}) - \deg(a_{i,k}) & \text{if } s_j = a_{i,k} z_i \text{ and } s_{j+1} = a_{i,k+1} z_i \text{ for some } i, \\ 1 & \text{if } s_{j+1} = \omega_2, \\ n_{i+1,1} - \text{rem}(\deg(\omega_1) + \sum_{i=1}^j size(s_{i-1}, s_i), n_{j+1}) & \text{if } s_j = a_{i,k} z_i \text{ and } s_{j+1} = a_{i+1,1} z_{i+1}. \end{cases}$$

Define the size of  $S$  to be the sum of  $size(s_j, s_{j+1})$  over all  $j$ , i.e.,

$$size(S) = \sum_j size(s_j, s_{j+1}).$$

The key point in this notion is that  $size$  actually describes the least difference of powers that terms should have, in order to satisfy restrictions on degrees. Thus  $\exists z_1, \dots, z_n S(\omega_1, \omega_2, z_1, \dots, z_n)$  is equivalent to an open formula which says that every system

$$\bigwedge_j a_{i,j} + X_i \equiv 0 \pmod{n_{i,j}}$$

has a solution and  $\deg(\omega_1 t^{size(S)}) < \deg(\omega_2)$ .

**Lemma 3.7.** *Every formula  $\psi$  of the form*

$$\exists \bar{z} = (z_1, \dots, z_\zeta) [\varphi_3(\bar{z}) \wedge \varphi_4(\bar{z}, \bar{\omega}) \wedge \varphi_6(\bar{z}, \bar{\omega})]$$

where  $\varphi_3$ ,  $\varphi_4$  and  $\varphi_6$  are as in the conclusion of Lemma 2.6 is equivalent to some quantifier-free  $L_Q$ -formula.

*Proof.* According to Remark 8, the formula  $\varphi_4$  is equivalent to a formula of the form  $\varphi'_4$  as given in **H2** but with the relation  $D_-$  omitted. By **H4** there are some  $\omega_1, \dots, \omega_\gamma \in \Omega \cup \{0\}$  such that  $\varphi_3(\bar{z}) \wedge \varphi'_4(\bar{z}, \bar{\omega}) \wedge \varphi_6(\bar{z}, \bar{\omega})$  is interpreted as a sequence of the form  $(s_j)_{0 \leq j \leq r}$ , with the following properties:

- $s_r = \omega_\gamma \neq 0$ ;
- for all  $j < r$ ; each  $s_j$  is either an element of  $\{\omega_1, \dots, \omega_{\gamma-1}\}$  or of the form  $az_i \in K$ ,
- for all  $j < r$ ,  $\deg(s_j) < \deg(s_{j+1})$ .

Note that for the reasons pointed out in Remark 2, for every variable  $z_i$  that appears in the sequence there are unique  $j, j'$  such that  $s_j, s_{j'}$  are consecutive elements of  $\{\omega_1, \dots, \omega_\gamma\}$  and  $\deg(s_j) < \deg(az_i) < \deg(s_{j'})$ . According to **H6**, for each  $s_i$  there is a unique  $n_i \in \mathbb{N}$  such that  $D_{n_i}(s_i)$  holds. Therefore, there is some  $\bar{z}$  which satisfies  $\varphi_3(\bar{z}) \wedge \varphi'_4(\bar{z}, \bar{\omega}) \wedge \varphi_6(\bar{z}, \bar{\omega})$  if and only if the difference in degrees of  $\omega_i$  and  $\omega_{i+1}$  is big enough and the corresponding systems of divisibility have a solution, as described in Remark 9.  $\square$

**Proposition 3.8.** *An existential formula as given in Lemma 2.6 is equivalent to a universal formula.*

*Proof.* Let  $\sigma$  be in a form given in Lemma 2.6. Combining the two basic results, Lemmas 3.6 and 3.7, we deduce the main result of this section.  $\square$

As a corollary of Proposition 3.8 we obtain the main theorem.

**Theorem 3.9.** *The ring theory in  $L_Q$  is model-complete and therefore decidable.*

**Corollary 3.10.** *The theory  $(\mathbb{F}_q[t]; +; |; P; f_t; 0, 1, t)$  is decidable.*

#### ACKNOWLEDGMENTS

The author would like to thank Th. Pheidas for the enlightening discussions and the referee for helpful suggestions concerning this work.

## REFERENCES

- [1] M. Davis, R. Sigal, and E. J. Weyuker, *Computability, Complexity, and Languages: Fundamentals of Theoretical Computer Science (2nd ed.)*, Academic Press Professional, Inc. (1994). MR1257183 (94j:03001)
- [2] J. Denef, *The diophantine problem for polynomial rings and fields of rational functions*, Transactions of the American Mathematical Society **242** (1978), 391-399. MR0491583 (58:10809)
- [3] J. Denef, *The diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium '78, North Holland (1984), 131-145. MR567668 (81h:03090)
- [4] L. Lipshitz, *The diophantine problem for addition and divisibility*, Transactions of the American Mathematical Society **235** (1978), 271-283. MR0469886 (57:9666)
- [5] T. Pheidas and K. Zahidi, *Undecidability of existential theories of rings and fields: A survey*, Contemporary Mathematics, 270, Amer. Math. Soc. (2000), 49-106. MR1802009 (2002a:03085)
- [6] T. Pheidas and K. Zahidi, *Elimination theory for addition and the Frobenius map in polynomial rings*, Journal of Symbolic Logic **69**, no. 4 (2004), 1006-1026. MR2135654 (2006c:03020)
- [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, 350, Cambridge University Press (2008), 207-236. MR2446305 (2009e:03006)
- [8] B. Poonen, *Undecidability in number theory*, Notices of the American Mathematical Society **55** (2008), no. 3, 344-350. MR2382821 (2008m:11238)
- [9] R. Robinson, *Undecidable rings*, Transactions of the American Mathematical Society **70** (1951), 137-159. MR0041081 (12:791b)
- [10] A. Semenov, *On the definability of arithmetic in its fragments*, Soviet Math. Dokl. **25** (1982), 300-303. MR647548 (84a:03074)
- [11] A. Semenov, *Logical theories of one-place functions on the set of natural numbers*, Math. USSR Izvestija **22** (1984), 587-618.
- [12] A. Sirokofskich, *Decidability of Sub-theories of Polynomials over a Finite Field*, Mathematical Theory and Computational Practice, Lecture Notes in Computer Science, 5635, Springer (2009), 437-446.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CRETE, 714 09 HERAKLION, GREECE  
E-mail address: [asirokof@math.uoc.gr](mailto:asirokof@math.uoc.gr)