Notes on the decidability of addition and the Frobenius map for polynomials and rational functions

Dimitra Chompitaki, Manos Kamarianakis and Thanases Pheidas
University of Crete, Department of Mathematics & Applied Mathematics
d.hobitaki@gmail.com, kamarianakis@uoc.gr, pheidas@uoc.gr

Abstract

Let p be a prime number, $\mathbb{F}_p$ a finite field with p elements, F an algebraic extension of $\mathbb{F}_p$ and z a variable. We consider the structure of addition and the Frobenius map (i.e., $x \mapsto x^p$) in the polynomial rings $F[z]$ and in fields $F(z)$ of rational functions. We prove that any question about $F[z]$ in the structure of addition and Frobenius map may be effectively reduced to questions about the similar structure of the field F. Furthermore, we provide an example which shows that a fact which is true for addition and the Frobenius map in the polynomial rings $F[z]$ fails to be true in $F(z)$. As a consequence, certain methods used to prove model completeness for polynomials do not suffice to prove model completeness for similar structures for fields of rational functions $F(z)$, a problem that remains open even for $F = \mathbb{F}_p$.

Keywords: Decidability; Model completeness; Frobenius map; Polynomial rings; Rational functions

2020 Mathematics Subject Classification: Primary 03B25, 12L05
Secondary 03C10, 03C60, 13A35, 13L05

1 Introduction

Let p be a prime number, $\mathbb{F}_p$ a finite field with p elements, F an algebraic extension of $\mathbb{F}_p$ and z a variable. We consider the structure of addition and the Frobenius map $x \mapsto x^p$ in the polynomial rings $F[z]$ of z over F, and in fields $\mathbb{F}_p(z)$ and $F(z)$ of rational functions of z over $\mathbb{F}_p$ and F respectively. The theory of a structure is *decidable* if there is an algorithm which, given any first order sentence, decides whether that is true or false in the structure; it is called *undecidable* otherwise. Another relevant notion is the *model completeness* of a theory; one way to define model completeness is to say that any formula is equivalent to an existential formula, i.e., one in which all quantifiers are at the beginning and are existential.

In [3], [8], [2] and [11] it was proved that the theory of $F(z)$ as a field, with z being a constant-symbol of the language, is undecidable. In [10] and [18] it was proved that even the existential theory of any $\mathbb{F}_p(z)$ is undecidable. It is therefore natural to ask questions of decidability for substructures of the ring-structure of subrings of $F(z)$. For results of this kind, the reader may consult [9], [16], [17], [7], [1] and [6] as well as the surveys [12], [14], [15] and [5]. For the Model Theory of the Frobenius map see [4] and the bibliographies therein.

Let $\mathcal{L}_p$ be the language $\mathcal{L}_p := \{=, +, x \mapsto x^p, 0, 1\}$ and $\mathcal{L}_p(z) := \mathcal{L}_p \cup \{x \mapsto zx, x \in F\}$. Let $\mathcal{L}_p(z)^e$ be the extension of $\mathcal{L}_p(z)$ by the predicate symbols P_σ, one for each formula σ of $\mathcal{L}_p$. We interpret the symbols of $\mathcal{L}_p(z)$ in the obvious way (for details see [13]), and we interpret $P_\sigma(\alpha)$, where α is a tuple of variables ranging over F, as '$\sigma(\alpha)$ holds true over F'. We assume that all the free variables of the formula σ are among the tuple of variables α.

In [13] it was proved that:

Theorem 1.1. *Assume that F is a perfect field of characteristic $p > 0$. Then:*

1. *The $\mathcal{L}_p(z)^e$-theory of $F[z]$ is model complete i.e., for every $\mathcal{L}_p(z)^e$-formula $\phi(x_1, \ldots, x_n)$ there exists an existential $\mathcal{L}_p(z)^e$-formula $\phi_0(x_1, \ldots, x_n)$ such that*

$$F[z] \models \forall x_1, \ldots, x_n[\phi(x_1, \ldots, x_n) \leftrightarrow \phi_0(x_1, \ldots, x_n)]$$

2. *In addition, assume that F is a countable and recursive field. Then, with notation of 1, there is an algorithm which to any ϕ associates ϕ_0.*

From Theorem 1.1 it follows, in a straightforward way, that:

Corollary 1.2. *The $\mathcal{L}_p(z)^e$-theory of a ring $F[z]$ is model complete if the theory of F in the language $\mathcal{L}_p$ is model complete.*

In this work we prove a stronger result:

Theorem 1.3. *There is an effective procedure which, to any given $\mathcal{L}_p(z)^e$-sentence ϕ associates an $\mathcal{L}_p$-sentence τ, such that ϕ is true in $F[z]$ if and only if τ is true in F - considered as a model of $\mathcal{L}_p$. If ϕ is an existential sentence, then the sentence τ that is produced is the same for all fields F, i.e., τ depends on p and ϕ but not on F.*

This provides an example of a positive answer to a question by Leonard Lipshitz: *"For subtheories of the algebraic structure of a ring of polynomials $F[z]$ and rational functions $F(z)$, identify those for which there is an 'effective translation' of every sentence over the structure to an equivalent sentence over the field F, and, possibly, a sentence over some simple structure, e.g., a group".*

Moreover, Theorem 1.3 provides an alternative proof of the decidability of the $\mathcal{L}_p(z)^e$-theory of $F[z]$ for fields F with a decidable $\mathcal{L}_p$-theory, and it also has the advantage of uniformity across all algebraic fields F of the same characteristic. Furthermore, the theorem does not assume that the field F is recursive, which is, by itself, a strengthening of the

Corollary 1.2. In future work, we intend to pursue this advantage in order to examine relative problems in Algebra and Model Theory.

It is natural to wish to extend the methods used to prove Theorem 1.1 to the fields of rational functions $F(z)$, as the question of decidability of the $\mathcal{L}_p(z)^e$-theories of such fields remains an open problem. To this end, we prove in Section 4 that the techniques used for the polynomial ring $F[z]$ cannot be naively applied for $F(z)$. This is caused by a crucial property required for the methods shown in [13] not being valid in the case studied. Specifically, we prove in Theorem 1.5 that, the kernel of strongly normalized additive polynomials (defined below) might be infinite over function fields, as opposed to the case of polynomials, where they are necessarily finite.

The polynomial terms of the language $\mathcal{L}_p(z)$ with a 'zero constant term' are additive polynomials. An *additive* polynomial f is a polynomial of the form

$$f(x_0, \ldots, x_{m-1}) = \sum_n f_n(x_n), \tag{1.1}$$

where each $f_n(x_n)$ is a polynomial of the variable x_n of the form $f_n(x_n) = \sum_i a_{n,i} x_n^{p^i}$ and i takes values in a finite subset of $\mathbb{N} \cup \{0\}$. The additive polynomial f is called *strongly normalized* if its coefficients are in $\mathbb{F}_p[z]$, the degrees of f with respect to each of its variables is the same, p^s, for some $s \in \mathbb{N}$, and the degrees of its leading coefficients $a_{n,s}$, $0 \leq n \leq m-1$, are pairwise inequivalent modulo p^s.

In [13], the authors develop an algorithm that reduces questions regarding the solvability of arbitrary additive polynomials to similar questions for strongly normalized polynomials.

An immediate consequence of Lemmas 3.1 and 3.2 of [13] is the following proposition, which is a crucial property for the proof of Theorem 1.1.

Proposition 1.4. *The heights (i.e., maxima of degrees) of the elements of the inverse image $\{x \in (F[z])^m \mid f(x) = u\}$ of a (multivariate) additive strongly normalized polynomial f over $F[z]$ have a bound, which can be effectively computed from f and the height of u.*

In a subsequent paper, the authors intend to show the similar result for rings that are generated over $\mathbb{F}_p[z]$ by the inverses of finitely many irreducible polynomials.

We ask the following:

Question. *Let $f(x) \in \mathbb{F}_p[z]$ be a strongly normalized additive polynomial of the variables of the tuple $x = (x_1, \ldots, x_m)$. Is the set $K_f := \{x \in (\mathbb{F}_p(z))^m \mid f(x) = 0\}$ necessarily finite?*

We will give a negative answer in Section 4, by providing a counterexample in each positive characteristic. More precisely, let p be a prime number and consider the additive polynomial

$$f_p(x_0, \ldots, x_{p-1}) = x_0^p + \cdots + z^k x_k^p + \cdots + z^{p-1} x_{p-1}^p - x_{p-1}. \tag{1.2}$$

Observe that f_p is strongly normalized. In Section 4 we prove:

Theorem 1.5. *Let Q be an irreducible monic polynomial of $\mathbb{F}_p[z]$. Then the equation*

$$f_p(x_0, \ldots, x_{p-1}) = 0 \tag{1.3}$$

has a non-zero solution $X := (X_0, \ldots, X_{p-1})$ *such that, for each* $n \in \{0, \ldots, p-1\}$*, we have* $X_n \in \mathbb{F}_p[z, \frac{1}{Q}]$ *and* X_n *has only simple affine poles and positive order at infinity.*

This has the following consequence. Let R be a subring of $\mathbb{F}_p(z)$ containing $\mathbb{F}_p[z]$ and infinitely many inverses of polynomials in $\mathbb{F}_p[z]$, i.e., $\mathbb{F}_p[z] \subset R \subset \mathbb{F}_p(z)$. Then, Theorem 1.5 implies that there are strongly normalized additive polynomials f with an infinite number of zeros. Therefore, the strategy of [13] in order to prove model completeness or decidability of the $\mathcal{L}_p(z)^e$-theory of such R does not suffice and new methods are required.

Some open problems that we consider important, for future work, in relation to the above are:

1. Let F be a field with a decidable (or model complete) $\mathcal{L}_p$-theory such that $\mathbb{F}_p \subset F \subset \tilde{\mathbb{F}}_p$, where $\tilde{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$. Does it follow that the existential $\mathcal{L}_p(z)^e$-theory of $F(z)$ is decidable? Model complete? What about the similar question asked of subrings of $F(z)$ containing $F[z]$?

2. The derivative in $\mathbb{F}_p(z)$ (and any extension $F(z)$ of $\mathbb{F}_p(z)$ if F is perfect) is existentially definable (see [13]). Let D denote the derivative with respect to z and $\mathcal{L}_D := \{+, D, 0, 1, x \mapsto zx\}$. It follows that the theory of $\mathbb{F}_p[z]$ (respectively, any $F[z]$ with F algebraic over $\mathbb{F}_p$) in the language $\mathcal{L}_D$ is decidable if the ring-theory of F is decidable. Is it model complete?

2 Existential Formulas

In [13, p. 1009], the authors show that any existential formula of $\mathcal{L}_p(z)^e$ is equivalent to either a quantifier free formula or a disjunction of formulas of the form:

$$\phi(u, \{v_j\}_{j\in J}) \ : \ \chi \wedge \exists x, \alpha \ [\alpha \in F \wedge \psi(x, \alpha)], \tag{2.1}$$

where χ is a quantifier free formula and

$$\psi(x, \alpha) \ : \ f(x) + H(\alpha) = u \wedge_{j\in J} e_j(x) + G_j(\alpha) \neq v_j \wedge P_\sigma(\alpha), \tag{2.2}$$

under the conventions:

- $x = (x_1, \ldots, x_m)$ is a tuple of variables.
- α is a tuple of variables ranging over F (denoted by $\alpha \in F$ in (2.1)), each of them distinct from each variable of x.
- f and each e_j are additive polynomials in some of the variables of x.
- H and each G_j are additive polynomials in some of the variables of α.

- u and each v_j are terms of $\mathcal{L}_p(z)$. No variables among those of x or α occur in u or any of the v_j.

- The predicate symbol $P_\sigma(\alpha)$ may have more variables than those of α occurring in it.

The above equivalence is a direct consequence of the following two facts.

- Since the system $\{x = 0 \wedge y = 0\}$ is equivalent to $x^p + zy^p = 0$, a system of equations can be substituted by a single equation.

- Since $x \notin F$ is equivalent to $\{\exists a \in F \exists b \in F[z] : x = a + zb \wedge b \neq 0\}$, we may substitute relations of the form $x \notin F$ by systems of relations in which $\notin$ does not appear.

3 Proof of Theorem 1.3

Let ϕ_0 be a given sentence of $\mathcal{L}_p(z)^e$. By Theorem 1 of [13], it follows that ϕ_0 is equivalent to an existential formula of the form ϕ, as shown in (2.1). We may assume that ϕ is a sentence[1]. This means that the terms u and v_j are elements of $F[z]$. In [13, Lemmas 3.3 and 3.4], the authors show that there exists a suitable and effective change of variables (denoted as *proper transformations* in [13, p. 1015]), after which we may assume, without loss of generality, that the additive polynomial f is strongly normalized. Re-enumerate the variables of x so that $x = (x_1, \ldots, x_k, x_{k+1}, \ldots, x_m)$ and $x_{k+1}, \ldots, x_m$ are exactly the variables of x which occur in f with non-zero highest degree coefficient. Then, by Lemma 3.2 of [13], for any value $\tilde{x}$ of the tuple x which is a solution of the equation $f + H = u$, the degrees of $\tilde{x}_{k+1}, \ldots, \tilde{x}_m$ are effectively bounded, hence, the variables $x_{k+1}, \ldots, x_m$ may be substituted by (existentially quantified) variables that range over F. Therefore, we may assume that the sentence ϕ has no equations. Moreover, determining the truth of ϕ amounts to the solvability of the system of inequalities $e_j + G_j \neq v_j$ together with P_σ. Clearly, because $F[z]$ is an infinite domain, all inequalities in which some of the variables $x_1, \ldots, x_k$ occur with a non-zero coefficient may be satisfied simultaneously. Each of the inequalities in which none of the variables $x_1, \ldots, x_k$ occurs, is clearly equivalent to a formula of the form $P_\omega(\beta)$.

Hence, ϕ is equivalent to a formula of the form $\exists \beta\ [\beta \in F \wedge\ P_\omega(\beta)]$, for some formula $\omega(\beta)$ of $\mathcal{L}_p$; the proof is now complete.

[1] Let T be a theory of a language L, ψ and $\omega(y)$ be formulas of L such that y is a tuple of variables which are free in ω but not occur in ψ. Assume that $T \models \psi \leftrightarrow \omega(y)$. Let t be any tuple of terms of L, with size as large as that of the tuple y. Then it follows that $T \models \psi \leftrightarrow \omega(t)$.

In our case this means that if ϕ is not a sentence, we may substitute each free variable of ϕ by 0 and obtain an existential sentence equivalent to ϕ. We are indebted to Russell Miller for pointing this to us.

4 Infinite kernels of additive polynomials

Let $\tilde{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$ and $\gamma \in \tilde{\mathbb{F}}_p$. The proof of Theorem 1.5 is based on the identity

$$\frac{1}{z+\gamma} = \frac{(z+\gamma)^{p-1}}{(z+\gamma)^p} = \frac{1}{(z+\gamma)^p} \sum_{n=0}^{p-1} \binom{p-1}{n} \gamma^{p-1-n} z^n, \tag{4.1}$$

which one may view as writing $\frac{1}{z+\gamma}$ on the basis $\{1, z, z^2, \ldots, z^{p-1}\}$, considering $\tilde{\mathbb{F}}_p(z)$ as a vector space over the field $\tilde{\mathbb{F}}_p(z^p)$.

Proof of Theorem 1.5. We will find a solution $\tilde{x} := (\tilde{x}_1, \ldots, \tilde{x}_p)$ for the equation $f_p(x) = 0$, where $f_p(x)$ is defined in (1.2). Indeed, if we set $\lambda_n := \binom{p-1}{n}\gamma^{p-1-n}$ in 4.1, we obtain a solution $\tilde{x} = (\frac{\mu_0}{z+\gamma}, \frac{\mu_1}{z+\gamma} \ldots, \frac{\mu_{p-1}}{z+\gamma})$, where $\mu_n^p = \lambda_n$, for $0 \leq n \leq p-1$. This already proves the analogue of Theorem 1.5 if $\tilde{\mathbb{F}}_p$ were in place of $\mathbb{F}_p$, since every irreducible element of $\tilde{\mathbb{F}}_p[z]$ has degree 1. Now consider a zero γ of Q and write $K = \mathbb{F}_p(\gamma)$. From the Theory of Finite Fields we know that K is a Galois extension of $\mathbb{F}_p$. Let Θ be its Galois group and $\theta(\gamma)$ denote the conjugates of γ under the action of $\theta \in \Theta$ - similarly for $\tilde{x}_n$ and $\theta(\tilde{x}_n)$. Then observe that $\theta(\tilde{x}) := (\theta(\tilde{x}_0), \ldots, \theta(\tilde{x}_{p-1}))$ is also a solution of $f_p = 0$ and, by the additivity of f_p, so is $X := \sum_{\theta\in\Theta} \theta(\tilde{x})$ - addition is meant component-wise. Clearly, X is invariant under the action of Θ, so we have that, writing $X := (X_1, X_2, \ldots, X_{p-1})$ each X_n is an element of $\mathbb{F}_p(z)$. Observe that, for each n we have $X_n = \sum_{\theta\in\Theta} \frac{\theta(\mu_n)}{z+\theta(\gamma)}$.

Initially, we prove that X is not identically equal to 0. Indeed, $X_{p-1} = \sum_{\theta\in\Theta} \frac{1}{z+\theta(\gamma)}$ can not be equal to the zero function, because the extension of fields K over $\mathbb{F}_p$ is a separable one, hence the various $\theta(\gamma)$ are pairwise distinct.

Clearly, all poles of each X_n are zeros of Q, and each one has multiplicity equal to one, since K is algebraic and therefore separable over $\mathbb{F}_p$. Moreover, the order at infinity of each term $\frac{\theta(\lambda_n)}{z+\theta(\gamma)}$ is positive, hence the order of each X_n at infinity is positive (including the possibility of *infinite*, i.e., the possibility that some $X_n = 0$). $\square$

Note: It is obvious how to generalise the results of Theorem 1.5 for any field F instead of $\mathbb{F}_p$.

Acknowledgments

This research work was supported from Greek and European Union resources, through the National Strategic Reference Framework (NSRF 2014-2020), under the call "Support for researchers with emphasis on young researchers (EDBM103)" and the funded project "Problems of Diophantine Nature in Logic and Number Theory" with code MIS 5048407.

Some of the problems of this project were initiated in discussions with faculty at the University of Concepción, Chile, during a visit by the first and the third authors from the University of Crete within a European Union Erasmus+ cooperation project. The hospitality of U. of Concepción is greatly appreciated.

Finally, we would like to thank the editor and the anonymous reviewers for their valuable remarks that led to a more reader-friendly presentation of the paper.

References

[1] L. Cerda-Romero and C. Martinez-Ranero, "The diophantine problem for addition and divisibility for subrings of rational functions over finite fields," *Proyecciones*, vol. 39, no. 3, pp. 721–736, 2020.

[2] G. L. Cherlin, "Undecidability of rational function fields in nonzero characteristic," in *Logic Colloquium '82*, ser. Studies in Logic and the Foundations of Mathematics, G. Lolli, G. Longo, and A. Marcja, Eds. Elsevier, 1984, vol. 112, pp. 85–95.

[3] Y. Ershov, "Undecidability of certain fields," *Dokl. Akad. Nauk SSSR*, vol. 161, pp. 27–29, 1965.

[4] E. Hrushovski, "The elementary theory of the frobenius automorphisms," *arXiv math/0406514*, 2004.

[5] J. Koenigsmann, "Decidability in local and global fields," in *Proceedings of the International Congress of Mathematicians (ICM 2018)*. World Scientific Publishers, 2018, pp. 45–59.

[6] C. Martinez-Ranero, J. Utreras, and X. Vidaux, "Existential decidability for addition and divisibility in holomorphy subrings of global fields," *arXiv 2010.14024*, 2020.

[7] G. Onay, "$\mathbb{F}_p((x))$ is decidable as a module over the ring of additive polynomials," *arXiv 1806.03123*, 2018.

[8] Y. G. Penzin, "The undecidability of fields of rational functions over fields of characteristic 2," *Algebra and Logic*, vol. 12, pp. 205–210, 1973.

[9] T. Pheidas, "The diophantine problem for addition and divisibility in polynomial rings (decidability, undecidability)," Ph.D. dissertation, Purdue University, 1985.

[10] ——, "Hilbert's tenth problem for fields of rational functions over finite fields," *Inventiones mathematicae*, vol. 103, no. 1, pp. 1–8, 1991.

[11] ——, "Endomorphisms of elliptic curves and undecidability in function fields of positive characteristic," *Journal of Algebra*, vol. 273, no. 1, pp. 395–411, 2004.

[12] T. Pheidas and K. Zahidi, "Undecidability of existential theories of rings and fields: a survey," *Contemporary mathematics - American Mathematical Society*, vol. 270, pp. 49–105, 2000.

[13] ——, "Elimination theory for addition and the Frobenius map in polynomial rings," *Journal of Symbolic Logic*, vol. 69, no. 4, pp. 1006–1026, 2004.

[14] ——, "Decision problems in algebra and analogues of hilbert's tenth problem," in *Model theory with Applications to Algebra and Analysis*. Cambridge University Press, 2008, pp. 207–236.

[15] B. Poonen, "Undecidability in number theory," *Notices of the American Mathematical Society*, vol. 55, pp. 344–350, 03 2008.

[16] A. Shlapentokh, "Hilbert's tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic," *Transactions of the American Mathematical Society*, vol. 333, no. 1, pp. 275–298, 1992.

[17] A. Sirokofrkich, "On an exponential predicate in polynomials over finite fields," *Proceedings of the American Mathematical Society*, vol. 138, no. 7, pp. 2569–2583, 2010.

[18] C. Videla, "Hilbert's tenth problem for rational function fields in characteristic 2," *Proceedings of the American Mathematical Society*, vol. 120, no. 1, pp. 249–253, 1994.