Decidability of the theory of addition and the Frobenius map in certain rings of rational functions

13th Panhellenic Logic Symposium, Volos

Dimitra Chompitaki, Manos Kamarianakis and Thanases Pheidas

July 2022

University of Crete
Department of Mathematics & Applied Mathematics

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού,
Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Introduction

Notation

- p : a prime number
- z : a variable
- $\mathbb{F}_p$: a finite field with p elements
- $\mathbb{F}_p[z]$: the ring of polynomials of z with coefficients in $\mathbb{F}_p$
- $\mathbb{F}_p(z)$: the field of rational functions of z over $\mathbb{F}_p$
- F : a field of characteristic p
- $F(z)$: the field of rational functions of z over F

Area Overview

- The **ring theory of any field F(z) with** $\mathrm{char}(F) = p$ **is undecidable** [Ershov, 1965], [Penzin, 1973], [Cherlin, 1984], [Pheidas, 2004].
- Even the **existential ring theory of the finite field** $\mathbb{F}_p(z)$ **is undecidable** [Pheidas, 1991], [Videla, 1994].
- What about subtheories of $F(z)$?
- What about subrings of $F(z)$?

The considered ring and language

- $S := \{s_1, \ldots, s_\nu\}$, s_i: irreducible elements of $\mathbb{F}_p[z]$.
- $\mathsf{R} := \mathbb{F}_\mathsf{p}[\mathsf{z}, \mathsf{s}_1^{-1}, \ldots, \mathsf{s}_\nu^{-1}]$.
- $\mathcal{L}_{\mathsf{Frob}+} := \{=, +, \mathsf{x} \mapsto \mathsf{zx}, \mathsf{x} \mapsto \mathsf{x}^\mathsf{p}, 0, 1\}$.
  - The $\mathcal{L}_{Frob+}$-theory of $\mathbb{F}_p[z]$ is decidable [Pheidas and Zahidi, 2004].
  - The $\mathcal{L}_{Frob+}$-theory of $\mathbb{F}_p[[z]]$ is decidable [Onay, 2018].

Main Results

Main Theorem

Theorem

The $\mathcal{L}_{Frob+} \cup \{x \in F\}$-theory of R is model-complete, and thus decidable.

Our Strategy: Outline

- We start with a **generic existential formula** ϕ of $\mathcal{L}_{Frob+} \cup \{x \in F\}$, and we construct an **equivalent universal** formula.
- We generalize the strategy of [Pheidas and Zahidi, 2004] where the authors solve over $F[z]$, F a perfect field.
- **We are solving over** $R = \mathbb{F}_p[z, s_1^{-1}, \ldots, s_\nu^{-1}]$.
- New methods & tools introduced, e.g., Hasse Derivative.

Definitions (1/2)

Additive polynomial

A polynomial of the form

$$f(\bar{x}) = \sum_{i=1}^{n} f_i(x_i),$$

where $\bar{x} = (x_1, \ldots, x_n)$ and, for each i,

$$f_i(x_i) = b_i x_i^{p^{s(i)}} + \sum_{j=1}^{s(i)-1} c_{i,j} x_i^{p^{s(i)-j}},$$

with $b_i, c_{i,j} \in \mathbb{F}_p[z]$ is called **additive**.

Remark: For every $\bar{x}, \bar{y}$, it holds that $f(\bar{x} + \bar{y}) = f(\bar{x}) + f(\bar{y})$.

Example: $f(x_0, x_1) = x_0^{p^2} - x_0 + (3z + 2)x_1^p$.

Definitions (2/2)

Strongly Normalized Polynomials

An additive polynomial f is **strongly normalized** iff

- the degrees of f_i are equal and,
- the set of leading coefficients $\{b_i\}$ is linearly independent over $\mathbb{F}_p(z)$, considered as a vector space over $\mathbb{F}_p(z^{p^s})$, and
- the degrees of b_i are pair-wise inequivalent modulo p^s, where p^s is the degree of f.

Example: $f(x_0, x_1, \ldots, x_{p-1}) = x_0^p - x_0 + zx_1^p + z^2x_2^p + \cdots + z^{p-1}x_{p-1}^p$.

Existential Formulas

An **existential formula of** $\mathcal{L}_{Frob+} \cup \{x \in F\}$ is equivalent in R to a **disjunction** of formulas of the form:

$$\phi(w, \beta) : \theta(w, \beta) \wedge \exists x, \alpha[\alpha \in \mathbb{F}_p \wedge \psi(x, \alpha, w, \beta)],$$

where θ is a quantifier-free and ψ is of the form:

$$\bigwedge_{i \in I} f_i(x) + H_i(\alpha) = u_i(w, \beta) \bigwedge_{j \in J} e_j(x) + G_j(\alpha) \neq v_j(w, \beta).$$

Remark: In R, a set of equations can be substituted by one equation:

$$(a = 0 \wedge b = 0) \Leftrightarrow a^p + zb^p = 0.$$

Our Strategy: Example

Our strategy applied to an example :

$$\phi(u) : \exists x_1, x_2, x_3, a$$
$$[a \in \mathbb{F}_p \wedge f(x_1, x_2, x_3) + H(a) = u \wedge x_1 + x_3 \neq 0 \wedge x_1 - a \neq 0],$$

where

$$f(x_1, x_2, x_3) = z x_1^{p^2} + z x_2^p - x_2 + z x_3^p - x_3$$

and

$$H(a) = z^p a^p.$$

Our Strategy: Example

Our strategy applied to an example :

$$\phi(u) : \exists x_1, x_2, x_3, a$$
$$[a \in \mathbb{F}_p \wedge f(x_1, x_2, x_3) + H(a) = u \wedge x_1 + x_3 \neq 0 \wedge x_1 - a \neq 0],$$

where

$$f(x_1, x_2, x_3) = zx_1^{p^2} + zx_2^p - x_2 + zx_3^p - x_3$$

and

$$H(a) = z^p a^p.$$

Notation

$Im_{\mathbb{F}_p}(H) := \{y \in R \mid \exists \alpha \in \mathbb{F}_p \; H(\alpha) = y\}$. $Im(f) := \{y \in R \mid \exists x \in R \; f(x) = y\}$.

Our Strategy: Example II

We reduce $\phi(u)$ to the equivalent formula:

$$\omega(u) : \phi_1(u) \wedge u \in Im(f) + Im_{\mathbb{F}_p}(H),$$

where

$$\phi_1(u) : \forall w_1, w_2, w_3, \gamma$$
$$[\gamma \in \mathbb{F}_p \wedge f(w_1, w_2, w_3) + H(\gamma) = u] \rightarrow \phi_2(w_1, w_2, w_3, \gamma)$$

and

$$\phi_2(w_1, w_2, w_3, \gamma) : \exists x_1, x_2, x_3, a[a \in \mathbb{F}_p \wedge$$
$$f(x_1, x_2, x_3) + H(a) = 0 \wedge x_1 + w_1 + x_3 + w_3 \neq 0 \wedge x_1 + w_1 - a - \gamma \neq 0].$$

Our Strategy: Example II

We reduce $\phi(u)$ to the equivalent formula:

$$\omega(u) : \phi_1(u) \wedge u \in Im(f) + Im_{\mathbb{F}_p}(H),$$

where

$$\phi_1(u) : \forall w_1, w_2, w_3, \gamma$$
$$[\gamma \in \mathbb{F}_p \wedge f(w_1, w_2, w_3) + H(\gamma) = u] \rightarrow \phi_2(w_1, w_2, w_3, \gamma)$$

and

$$\phi_2(w_1, w_2, w_3, \gamma) : \exists x_1, x_2, x_3, a[a \in \mathbb{F}_p \wedge$$
$$f(x_1, x_2, x_3) + H(a) = 0 \wedge x_1 + w_1 + x_3 + w_3 \neq 0 \wedge x_1 + w_1 - a - \gamma \neq 0].$$

Theorem

The formula $u \in Im(f) + Im_{\mathbb{F}_p}(H)$ is equivalent to a universal formula.

Our Tools I

Lemma

Let $\mathbf{f}$ be **an additive polynomial** in n_0 variables, with coefficients in $\mathbb{F}_p[z]$. Then, there is a proper transformation $\xi : R^n \times \mathbb{F}_p^k \to R^{n_0}$, a **strongly normalized additive polynomial** $\tilde{f}$ in n variables ($n \leq n_o$), with coefficients in $\mathbb{F}_p[z]$ and an additive polynomial G in only $\mathbb{F}_p$-variables, each one of them distinct from the variables of $\tilde{f}$, such that:

- $f \circ \xi = \tilde{f} + G$.
- $\deg(\tilde{f}) \leq \deg(f)$.
- $\mathbf{Im(f) = Im(f) + Im_{\mathbb{F}_p}(G)}$.
- ξ and $\tilde{f}$ are effectively computable from f.

Our Strategy: Example III

Due to previous lemma,

$$\phi_2(w_1, w_2, w_3, \gamma) : \exists x_1, x_2, x_3, a[a \in \mathbb{F}_p \wedge$$
$$f(x_1, x_2, x_3) + H(a) = 0 \wedge x_1 + w_1 + x_3 + w_3 \neq 0 \wedge x_1 + w_1 - a - \gamma \neq 0].$$

is equivalent to

$$\phi_2'(w_1, w_2, w_3, \gamma) : \exists x_1, x_2, x_3, a[a \in \mathbb{F}_p \wedge$$
$$\tilde{f}(x_1, x_2, x_3) + H'(a) = 0 \wedge x_1 + w_1 + x_3 + w_3 \neq 0 \wedge x_1 + w_1 - a - \gamma \neq 0].$$

where $\tilde{f}$ is strongly normalized.

Our Tools II

Main Technical Theorem

Let $\tilde{f}$ be a normalized additive polynomial of the variables $\bar{x} = (x_1, \ldots, x_n)$, which has positive degree in all the variables. Let $u \in \mathbb{F}_p(z)$. Then the set $\{\bar{x} \in R^n \mid \tilde{f}(\bar{x}) = u\}$ is finite.

Our Tools III

Returning to the example:

$$\phi_2'(w_1, w_2, w_3, \gamma) : \exists x_1, x_2, x_3, a[a \in \mathbb{F}_p \wedge$$
$$\tilde{f}(x_1, x_2, x_3) + H'(a) = 0 \wedge x_1 + w_1 + x_3 + w_3 \neq 0 \wedge x_1 + w_1 - a - \gamma \neq 0].$$

Our Tools III

Returning to the example:

$$\phi_2'(w_1, w_2, w_3, \gamma) : \exists x_1, x_2, x_3, a[a \in \mathbb{F}_p \wedge$$
$$\tilde{f}(x_1, x_2, x_3) + H'(a) = 0 \wedge x_1 + w_1 + x_3 + w_3 \neq 0 \wedge x_1 + w_1 - a - \gamma \neq 0].$$

Due to Main Technical Theorem, x_1, x_2 and x_3 belong to a finite set $\Rightarrow$
ϕ_2 can be reduced to a quantifier-free formula!

Ongoing Research

The existential $\mathcal{L}_{Frob+}$-theory of $\mathbb{F}_p(z)$

- The analogous of the Main Technical Theorem for $\mathbb{F}_p(z)$ does not hold.
- **Counter-example:** there are infinitely many pairs $(x_1, x_2) \in \mathbb{F}_p(z)^2$ that satisfy $zx_1^2 + x_2^2 + x_1 + x_2 = 0$.
- We believe we are close to finding an alternative technique that will work.

References i

- Cherlin, G. L. (1984). **Undecidability of rational function fields in nonzero characteristic.** In Lolli, G., Longo, G., and Marcja, A., editors, *Logic Colloquium '82*, volume 112 of *Studies in Logic and the Foundations of Mathematics*, pages 85–95. Elsevier.
- Ershov, Y. (1965). **Undecidability of certain fields.**
- Onay, G. (2018). **$F_p((X))$ is decidable as a module over the ring of additive polynomials.** *arXiv.org*.
- Penzin, Y. G. (1973). **The undecidability of fields of rational functions over fields of characteristic 2.** *Algebra and Logic*, 12:205–210.

References ii

- Pheidas, T. (1991). **Hilbert's tenth problem for fields of rational functions over finite fields.** *Inventiones mathematicae*, 103(1):1–8.
- Pheidas, T. (2004). **Endomorphisms of elliptic curves and undecidability in function fields of positive characteristic.** *Journal of Algebra*, 273(1):395–411.
- Pheidas, T. and Zahidi, K. (2004). **Elimination theory for addition and the Frobenius map in polynomial rings.** *J. Symb. Log.*, 69(4):1006–1026.
- Videla, C. (1994). **Hilbert's tenth problem for rational function fields in characteristic 2.** *Proceedings of the American Mathematical Society*, 120(1):249–253.

Acknowledgments

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**.

Thank you for your attention! :)
Have a nice Covid-free Summer!