Decidability of theories of polynomials

Alla Sirokofskich
University of Crete

June 18, 2009

1 Basic notions
- Few words on notation
- Generalization of diophantine equation

2 Some facts about decidability
- Several tools for proving decidability
- A list with known results

3 Analogue of Presburger Arithmetic

4 Analogue of Semenov's result

Few words on notation

- R to be considered any integral domain i.e. commutative ring with one, without zero divisors.
- $t_1, \ldots, t_n$ are transcendental over R, i.e., for $i = 1, \ldots, n$, t_i is not a root of any polynomial with coefficients from R.
- $R[t_1, \ldots, t_n]$ is the polynomial ring in n variables over R.
- For $n = 1$, we simply write $R[t]$.
- $\mathbb{F}_q$ is a finite field, with $q = p^n$, where p is a prime number.
- $\mathbb{F}_q^*$ stands for $\mathbb{F}_q - \{0\}$ and $(\mathbb{F}_q[t])^*$ stands for $\mathbb{F}_q[t] - \{0\}$.
- By $\mathbb{N}$ we denote the set of positive integers and let $\mathbb{N}_0$ be $\mathbb{N} \cup \{0\}$.

Generalization of diophantine equation

1. A diophantine equation over R is an equation of the form $P(x_1, \ldots, x_m) = 0$, where P is a polynomial over R.
2. Note that we need to have the proper symbols (constants and functions) in order to talk about polynomials in our language. We will see later the exact details on this fact.

Several tools for proving decidability

1. Elimination of quantifiers, i.e., each first-order formula of L is equivalent to a quantifier-free formula.
2. Model completeness, i.e., each first-order formula in the language of the structure is equivalent to an existential formula.
3. Reduction of given problem to some known decidable problem.

A list with known results for $\mathbb{Z}$

1. Motivation: Undecidability of the ring-theory of the rational integers (Matijasevich, Davis, Putnam, Robinson, 1970)
2. L. Lipshitz (1978) proved that the existential theory of $\mathbb{Z}$ in the language of addition and divisibility is decidable. the full first order theory is undecidable),
3. L. Lipshitz (1978) proved that the full first order theory of $\mathbb{Z}$ in the language of addition and divisibility is undecidable.
4. J. Denef (1978) showed that the existential theory of $A[t]$ is undecidable, if A is an integral domain.
5. A. Semenov (1982, 1984)proved that the elementary theory of addition and the function $n \longrightarrow 2^n$ over $\mathbb{Z}$ is decidable.

Known results for polynomials

1. Th. Pheidas (Ph D. Thesis) proved that the existential theory for polynomials in one variable over a field is decidable.
2. Th. Pheidas (Ph.D. Thesis) proved that the existential theory for polynomials in two variables over a field is undecidable.
3. Th. Pheidas and K. Zahidi (2004) showed that the theory of the structure $(\mathbb{F}_q[t]; +; x \longrightarrow x^p; f_t; 0, 1)$ is model complete and therefore decidable, where $x \longrightarrow x^p$ is the Frobenius function.

Our working language

Definition

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

where

$D_<(\omega_1, \omega_2)$ *stands for "deg* $\omega_1 <$ *deg* ω_2*",*

$D_n(\omega)$ *stands for "*$n|$*deg* ω*",*

$|_\alpha(\omega)$ *stands for "* $\exists x(x \cdot \alpha = \omega)$*".*

Proposition

Every existential formula of L is equivalent to a finite disjunction of formulas of the form

$$\sigma(\bar{\omega}) : \ \sigma_0 \wedge \ \exists \bar{x} = (x_1, \ldots, x_n)$$

$$\sigma_1 \wedge \sigma_2 \wedge \sigma_3 \wedge \sigma_4$$

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

$$\sigma_1(\bar{x}, \bar{\omega}) : \ \bigwedge_i \ f_i(\bar{x}) = h_i(\bar{\omega}) \ , \tag{1}$$

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

$$\sigma_3(\bar{x}, \bar{\omega}) : \ \bigwedge_\lambda \ |_{c_\lambda}(\chi_\lambda(\bar{x}, \bar{\omega})) \ , \tag{3}$$

$$\sigma_4(\bar{x}, \bar{\omega}) : \ \bigwedge \ D_{n_\xi}(g_\xi(\bar{x}, \bar{\omega})) \ , \tag{4}$$

Definition

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 $dc(X + Y) > dc(X + Z)$.

Facts about the depth of the cancellation

Let

$$a_1 x = \sum_{i \leq k} u_i t^i, \qquad \omega_1 = \sum_{i \leq k} v_i t^i, \qquad \omega_2 = \sum_{i \leq k} w_i t^i,$$

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 $a_1 x + \omega_1$ is $\lambda_1 - 1$ and thus $dc(a_1 x + \omega_1) = k - \lambda_1 + 1$. Note that in case $\lambda_1 = 0$, then $a_1 x = -\omega_1$ and the degree of $a_1 x + \omega_1$ is $-\infty$.
Assume that $dc(a_1 x + \omega_1) > 0$. Consider any ω_2 with the properties $\deg(a_1 x) = \deg(\omega_2)$ and $dc(a_1 x + \omega_1) < dc(a_1 x + \omega_2)$. 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 $dc(a_1 x + \omega_1) > dc(\omega_2 + (-\omega_1))$. Thus $\deg(a_1 x + \omega_1) < \deg(\omega_2 - \omega_1)$

Facts for the relation of the form $D_<(a_1x + \omega_1, a_2x + \omega_2)$

Lemma

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) $D_=(a_1x + \omega_2, \omega_2) \wedge D_=(a_1x, \omega_2) \wedge D_<(\omega_1, \omega_2)$.

Lemma

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) $D_<(a_1x + \omega_1, \omega_1) \wedge D_=(a_1x, \omega_1) \wedge D_=(a_1x, \omega_2) \wedge D_{<_k}(a_1x + \omega_1, \omega_2 - \omega_1)$.

Lemma

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) $D_=(a_1x, \omega_2) \wedge D_=(\omega_1, \omega_2) \wedge D_=(a_1x + \omega_1, \omega_2 - \omega_1) \wedge \left[\bigvee_{i=1}^{k-1} D_=(a_1x + \omega_2, t^i(\omega_2 - \omega_1))\right]$.

Lemma

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

Proposition (Separation)

Consider σ as given in first proposition 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 $\bar{\omega}$,

$$\tilde{\sigma_1}(z, \bar{\omega}) : \bigwedge_i\ z = \tilde{h_i}(\bar{\omega})\ , \tag{5}$$

$$\tilde{\sigma_2}(z, \bar{\omega}) : \bigwedge_\rho\ D_<(z, \tilde{\pi}_{2,\rho}(\bar{\omega})) \wedge D_<(\tilde{\pi'}_{1,\rho}(\bar{\omega}), z), \tag{6}$$

$$\tilde{\sigma_3}(z) : \bigwedge_\lambda\ |_{c_\lambda}(\tilde{\chi}_\lambda(z))\ , \tag{7}$$

$$\tilde{\sigma_4}(z) : \bigwedge_\xi\ D_{n_\xi}(z) \tag{8}$$

Result I

Theorem

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

Extending our working language

$$L_Q = \{+, \mathbf{c}_1, \ldots, \mathbf{c}_q, t, f_t\} \cup \{Q_{\bar{a},m} : \ \bar{a} \in ((\mathbb{F}_q[t])^*)^{<\mathbb{N}}, m \in \mathbb{N}\} \cup$$

$$\cup \{|_a : \ a \in (\mathbb{F}_q[t])^*\} \cup \ \{D_<\} \cup \{D_n : n \in \mathbb{N}\} \cup \{C_{\bar{a}} : \ \bar{a} \in ((\mathbb{F}_q[t])^*)^{<\mathbb{N}}\}$$

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

$$\exists \bar{y} = (y_1, \ldots, y_n)$$

$$[a_1 y_1 + \cdots + a_n y_n = \omega \wedge \bigwedge_{j=1,\ldots,n} y_j \in \{t^{ms} : \ s \in \mathbb{N}_0\} \wedge$$

$$\bigwedge_{j=1,\ldots,n-1} \deg(a_j y_j) < \deg(a_{j+1} y_{j+1})] \ .$$

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

$$\exists \bar{y} = (y_1, \ldots, y_n) \ [\deg(a_1 y_1 + \cdots + a_n y_n + \omega) < \deg(a_1 y_1) \wedge$$

$$\bigwedge_{j=1,\ldots,n} y_j \in \{t^s : \ s \in \mathbb{N}_0\} \wedge \deg(a_n y_n) = \deg(\omega) \wedge$$

$$\bigwedge_{j=1,\ldots,n-1} \deg(a_j y_j) < \deg(a_{j+1} y_{j+1})] \ .$$

Properties of two basic predicates

Lemma

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 $k = 1$.

Lemma

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

Lemma

Every existential formula of L_Q is equivalent to a finite disjunction of formulas of the form

$$\sigma(\bar{\omega}) : \ \sigma_0 \wedge \exists \bar{x} = (x_1, \ldots, x_n) \, \exists \bar{y} = (y_1, \ldots y_m) \, (\sigma_1 \wedge \sigma_3 \wedge \sigma_4 \wedge \sigma_5 \wedge \sigma_6) \quad (9)$$

where σ_0 is a quantifier-free formula with parameters $\bar{\omega}$, and $\sigma_1,\ldots,\sigma_6$ have the following forms:

$$\sigma_1(\bar{x},\bar{y},\bar{\omega}) : \bigwedge_i \ f_i(\bar{x}) + g_i(\bar{y}) = h_i(\bar{\omega}) \ , \tag{10}$$

$$\sigma_3(\bar{y}) : \bigwedge_{j=1}^{m} P(y_j), \tag{11}$$

$$\sigma_4(\bar{x},\bar{y},\bar{\omega}) : \bigwedge_\rho \ D_<(\pi_\rho(\bar{x},\bar{y},\bar{\omega}), \pi'_\rho(\bar{x},\bar{y},\bar{\omega})) \ , \tag{12}$$

$$\sigma_5(\bar{x},\bar{y},\bar{\omega}) : \bigwedge_\lambda \ |_{c_\lambda} (\chi_\lambda(\bar{x},\bar{y},\bar{\omega})) \ , \tag{13}$$

$$\sigma_6(\bar{x},\bar{\omega}) : \bigwedge_\xi \ D_{n_\xi}(\chi'_\xi(\bar{x},\bar{\omega})) \ , \tag{14}$$

First step towards decidability

Lemma

Every formula σ of L_Q is equivalent over $\mathbb{F}_q[t]$ to a finite disjunction of formulas of the form

$$\varphi(\bar{\omega}) : \ \varphi_0 \wedge \exists \bar{y}(\varphi_1 \wedge \varphi_3 \wedge \varphi_4 \wedge \varphi_5 \wedge \varphi_6) \tag{15}$$

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

$$\varphi_1(\bar{y}, \bar{\omega}) : \bigwedge_i \ g_i(\bar{y}) = h_i(\bar{\omega}) \ , \tag{16}$$

$$\varphi_3(\bar{y}) : \bigwedge_{j=1}^{m} P(y_j) \tag{17}$$

$$\varphi_4(\bar{y}, \bar{\omega}) : \bigwedge_\rho \ D_<(\pi_{1,\rho}(\bar{y}) + \pi_{2,\rho}(\bar{\omega}), \pi'_{1,\rho}(\bar{y}) + \pi'_{2,\rho}(\bar{\omega})) \ , \tag{18}$$

$$\varphi_5(\bar{y}, \bar{\omega}) : \bigwedge_\lambda \ |_{c_\lambda} \left(\chi_{1,\lambda}(\bar{y}) + \chi_{2,\lambda}(\bar{\omega})\right) \ , \tag{19}$$

$$\varphi_6(\bar{y}, \bar{\omega}) : \bigwedge_\xi \ D_{n_\xi}(\chi'_{1,\xi}(\bar{y}) + \chi'_{2,\xi}(\bar{\omega})) \ , \tag{20}$$

An observation

Lemma

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* $t\not| c$. *Then for every* $l\geq k$ *there is a solution* y' *of* $c|ay+b$, *where* y' *is a power of* t *and* $\deg(y')>l$.

Lemma

In the conclusion of last lemma the formula of type φ_5 *can be omitted.*

model-completness

Proposition

Every formula φ which is as in the last lemma 9 is equivalent to a disjunction of formulas of the form

$$\varphi'_0 \wedge \forall \bar{y}\ [\varphi_1(\bar{y}, \bar{\omega}) \wedge \varphi'_4(\bar{y}, \bar{\omega}) \wedge \varphi_3(\bar{y}) \rightarrow \exists \bar{z}[\varphi_3(\bar{z}) \wedge \varphi_4(\bar{y}, \bar{z}, \bar{\omega}) \wedge \varphi_6(\bar{y}, \bar{z}, \bar{\omega})]] \tag{21}$$

Proposition

Every formula ψ of the form

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

where φ_3, φ_4 and φ_6 are as in the conclusion of the last lemma, is equivalent to some quantifier-free L_Q-formula.

Result II

Given an existential formula as in Lemma 9, it is equivalent to a universal formula.

Theorem

The ring theory in L_Q is model complete, therefore it is decidable.

Corollary

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