Decidability results of subtheories of polynomial rings and formal power series

Dimitra Chompitaki

University of Crete, Greece
Department of Mathematics and Applied Mathematics

July 2024, Panhellenic Logic Symposium

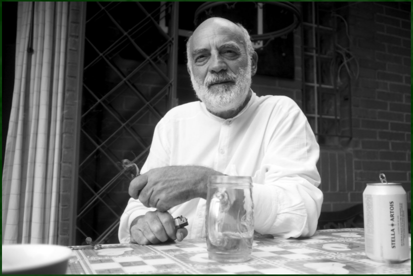
Hilbert's Tenth Problem (HTP)

- HTP asks for an algorithm to determine the solvability in integers of Diophantine equations over $\mathbb{Z}$, i.e, of polynomials with integer coefficients (1900)
- Y. Matiyasevich, M. Davis, H. Putnam, J. Robinson provided a negative answer to HTP (1970)
- The positive existential theory of the $\mathcal{L}_r = \{=, 0, 1, +, \cdot\}$ structure for integers is undecidable.

Extensions of Hilbert's Tenth Problem (HTP)

- A number of similar problems have been solved over other domains of mathematical interest.
- Some others remain open. HTP for the field of rational numbers is a (or the) major open problem of this area.

A phrase of Thanases Pheidas



" We are studying problems of decidability and undecidability, roughly speaking, trying to find where is the limit between what a computer can or can not do."

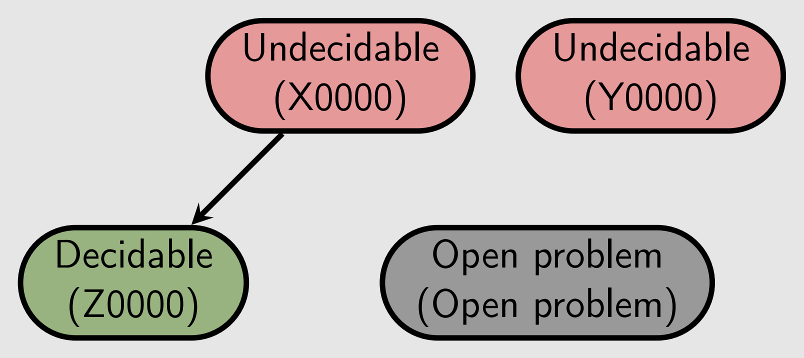
A story about Thanases Pheidas

At a glance

We will present:

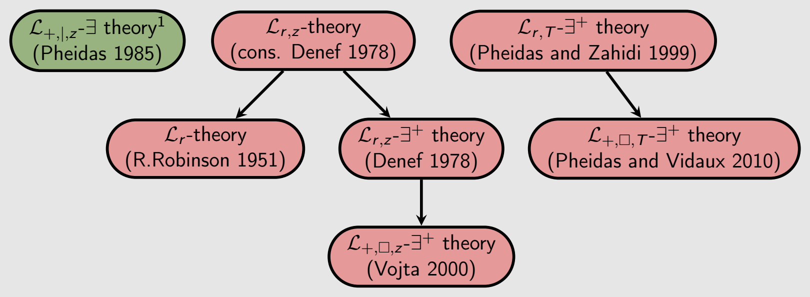
- Known decidability and undecidability results for theories of the ring-structures for commonly used domains:
  - Polynomial Rings
  - Formal Power Series
- New results:
  - Focus on the structure of addition and localized divisibility in polynomial rings and the corresponding rings of formal power series and inter relations.

Legend



Undecidable
(X0000)
Undecidable
(Y0000)
Decidable
(Z0000)
Open problem
(Open problem)

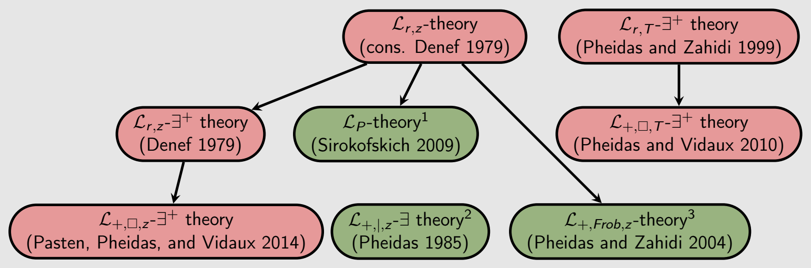
For $\mathcal{F}[z]$, $char(\mathcal{F}) = 0$



- $\mathcal{L}_r = \{=, 0, 1, +, \cdot\}$
- $\mathcal{L}_{r,z} = \mathcal{L}_r \cup \{z\}$
- $\mathcal{L}_{r,T} = \mathcal{L}_r \cup \{T(x)\}$, where $T(x)$: "x is not a constant"
- $\mathcal{L}_{+,|} = \{=, 0, 1, +, |\}$, $\mathcal{L}_{+,|,z} = \mathcal{L}_{+,|} \cup \{z\}$
- $\mathcal{L}_{+,\square,z} = \mathcal{L}_{+,z} \cup \{x \text{ is square}\}$, $\mathcal{L}_{+,\square,T} = \mathcal{L}_{+,T} \cup \{x \text{ is square}\}$

[1] Iff the existential $\mathcal{L}_r$-theory of $\mathcal{F}$ is decidable

For $\mathcal{F}[z]$, $char(\mathcal{F}) > 0$



- $\mathcal{L}_{+,Frob,z} = \{=, 0, 1, z, +, x \mapsto x^p, x \mapsto xz\}$
- $\mathcal{L}_P = \mathcal{L}_{+,z} \cup \{P(\omega)\}$, where $P(\omega)$: ω is a power of z

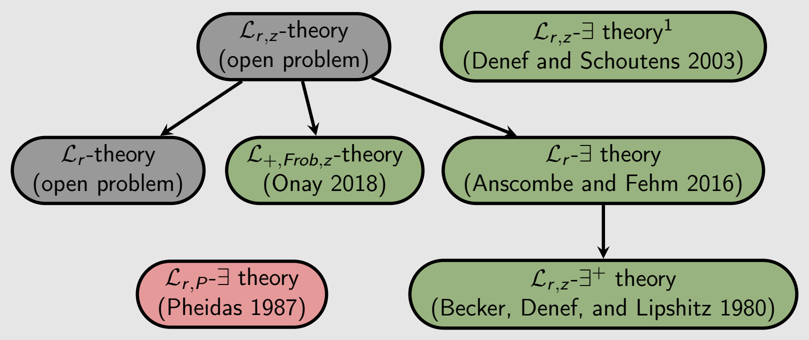
[1] For finite fields
[2] Iff the existential $\mathcal{L}_r$-theory of $\mathcal{F}$ is decidable
[3] For perfect fields

For $\mathcal{F}[[z]]$, $char(\mathcal{F}) = 0$, $\mathcal{F}$: a field with decidable theory

$\mathcal{L}_r$-theory[1]
(Kochen 1975,
Weispfenning 1984)

[1] Kochen 1975 first proved the decidability result under the continuum hypothesis, whereas Weispfenning 1984 provided an algorithm.

For $\mathcal{F}[[z]]$, $\mathcal{F}$: finite field



- $\mathcal{L}_{r,P} = \mathcal{L}_r \cup \{P\}$, where $P(\omega)$: ω is a power of z

[1] Follows from resolution of singularities in positive characteristic

Other useful resources (further reading)

Surveys:

- (Pheidas and Zahidi 2000): Undecidability of existential theories of rings and fields: a survey
- (Shlapentokh 2006): Diophantine classes and extensions to global fields
- (Pheidas and Zahidi 2008): Model theory with applications to algebra and analysis
- (Poonen 2008): Undecidability in number theory
- (Koenigsmann 2018): Decidability in local and global fields

Addition and divisibility in FPS

Consider the language $\mathcal{L}_{+,|} = \{=, +, |, x \mapsto zx, 0, 1, z\}$.

$a \mid b \Leftrightarrow \exists c : b = ca \Leftrightarrow ord(a) \leq ord(b)$.

Produce a quantifier elimination that works as far as possible for power series ($\mathcal{F}[[z]]$), over any field of any characteristic.

Addition and divisibility in FPS: language

- $\mathcal{L}_{+,|} = \{=, +, |, x \mapsto zx, 0, 1, z\}$.
- Atomic formulas in $\mathcal{L}_{+,|}$:
  - $f(\bar{x}) = 0$, where f is a linear polynomial, $\bar{x}$ a vector of variables.
  - $g(\bar{x}) \mid h(\bar{x})$, where g, h are linear polynomials, $\bar{x}$ a vector of variables.
- $\alpha_0 + \sum_{j=1}^{m} \alpha_j x_j$ is a linear polynomial, where x_j are independent variables over $\mathcal{F}[z]$ and $a_j \in \mathcal{F}[z]$.

Addition and divisibility in FPS: a method of quantifier elimination

- The general case:

$$\exists \bar{x} : \phi(\bar{x})$$

  where

$$\phi(\bar{x}) = \bigwedge \phi_i(\bar{x})$$

  where each $\phi_i(\bar{x})$ is an atomic formula, or the negation of an atomic formula, and $\bar{x}$ is a vector of variables.
- The most interesting case deals with formulas of the form:

$$\exists x : \bigwedge (a_i x + b_i) \mid (c_i x + d_i)$$

  where x a single variable, $a_i, c_i \in \mathcal{F}[z]$, $b_i, d_i \in \mathcal{F}[[z]]$.

Systems of divisibilities

- Generic system of divisibilities:

$$\Sigma_{|} = \bigwedge_{i=1}^{n} (a_i x + b_i) \mid (c_i x + d_i)$$

- Simplified system of divisibilities:

$$\Sigma_{|}^{*} = \bigwedge_{i=1}^{m} ((x + e_i) \mid f_i) \bigwedge_{i=m+1}^{n} (f_i \mid (x + e_i))$$

Theorem 1

For any generic system of divisibilities $\Sigma_|$, there exists a simplified system of divisibilities $\Sigma_|^*$ such that:

1. There is a primitive recursive function J_0 such that for any x that is a solution of $\Sigma_|$, $J_0(x)$ is a solution for $\Sigma_|^*$
2. There is a primitive recursive function J_0^* such that for any x that is a solution of $\Sigma_|^*$, $J_0^*(x)$ is a solution for $\Sigma_|$

Proposition

Given a simplified system of divisibilities $\Sigma_{|}^{*}$, the quantifier $\exists$ can be eliminated from the following statement:
$\exists x \in \mathcal{F}[[z]] : \Sigma_{|}^{*}$.

Addition and divisibility in FPS: notation

- trunc(a, n): a function that keeps the first n coefficients of a:
  - $a = \sum_{j=0}^{\infty} \alpha_j z^j$
  - $\mathrm{trunc}(a, n) = \sum_{j=0}^{n} \alpha_j z^j$

Basic idea for quantifier elimination (1/3)

- Consider the divisibility: $(x + e) \mid f$

x

x_0	x_1	x_2	x_3	x_4	$\ldots$

e

e_0	e_1	e_2	e_3	e_4	$\ldots$

$x + e$

$x_0 + e_0$	$x_1 + e_1$	$x_2 + e_2$	$x_3 + e_3$	$x_4 + e_4$	$\ldots$

f

0	0	0	0	$\neq 0$	$\ldots$

- $ord(f) = 4$
- In order for $ord(x + e) \leq 4$, it should be the case that: $x_i \neq -e_i$ for some $i \leq 4$, i.e:

$$\text{trunc}(x, ord(f)) \neq -\text{trunc}(e, ord(f))$$

Basic idea for quantifier elimination (2/3)

- Consider the divisibility: $f \mid (x + e)$

x

x_0	x_1	x_2	x_3	x_4	...

e

e_0	e_1	e_2	e_3	e_4	...

$x + e$

$x_0 + e_0$	$x_1 + e_1$	$x_2 + e_2$	$x_3 + e_3$	$x_4 + e_4$	...

f

0	0	0	0	$\neq 0$	...

- $ord(f) = 4$
- In order for $4 \leq ord(x + e)$, it should be the case that: $x_i = -e_i$ for all $i < 4$, i.e:

$$\text{trunc}(x, ord(f) - 1) = -\text{trunc}(e, ord(f) - 1)$$

Basic idea for quantifier elimination (3/3)

- In summary, for the system

$$\Sigma_{|}^{*} = \bigwedge_{i=1}^{m}((x + e_i) \mid f_i) \bigwedge_{i=m+1}^{n} (f_i \mid (x + e_i))$$

  to have a solution, we require that there exists x such that:
  - $\mathrm{trunc}(x, ord(f_i)) \neq -\mathrm{trunc}(e_i, ord(f_i))$, for $1 \leq i \leq m$
  - $\mathrm{trunc}(x, ord(f_i) - 1) = -\mathrm{trunc}(e_i, ord(f_i) - 1)$, for $m < i \leq n$
- From there it is easy to define conditions under which such a x exists (quantifier elimination).

Theorem 1

There exists a recursive function J_1, such that for any system of divisibilities $\Sigma_|$, we have:

$$\exists x \in \mathcal{F}[[z]] : \Sigma_|$$

if and only if

$$\exists x \in \mathcal{F}[z] : \Sigma_| \text{ with } \deg(x) \leq J_1(\Sigma_|).$$

Theorem 2

For each formula ϕ of the language of $\mathcal{L}_{+,|}$ there is a quantifier-free formula ϕ' such that ϕ, ϕ' are equivalent over almost all rings $\mathcal{F}_p[[z]]$.

References I

- Anscombe, Sylvy and Arno Fehm (2016). "The existential theory of equicharacteristic henselian valued fields". In: *Algebra and Number Theory* 10.3, pp. 665 –683.
- Becker, J., J. Denef, and L. Lipshitz (1980). "Further remarks on the elementary theory of formal power series rings". In: *Model Theory of Algebra and Arithmetic*. Ed. by Leszek Pacholski, Jedrzej Wierzejewski, and Alec J. Wilkie. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1–9.
- Denef, J. (1978). "The Diophantine problem for polynomial rings and fields of rational functions". In: *Transactions of the American Mathematical Society* 242, pp. 391–399.

References II

- Denef, J. (1979). "The Diophantine Problem for Polynomial Rings of Positive Characteristic". In: *Logic Colloquium '78*. Ed. by Maurice Boffa, Dirkvan Dalen, and Kenneth Mcaloon. Vol. 97. Studies in Logic and the Foundations of Mathematics. Elsevier, pp. 131–145.
- Denef, Jan and Hans Schoutens (Sept. 2003). "On the Decidability of the Existential Theory of $F_p[[t]]$". In: pp. 43–60.
- Kochen, S. (1975). "The model theory of local fields". In: *Proceedings of the International Summer Institute and Logic Colloquium*, pp. 385–425.
- Koenigsmann, Jochen (2018). "Decidability in local and global fields". In: *Proceedings of the International Congress of Mathematicians (ICM 2018)*, pp. 45–59.

References III

- Onay, Gönenç (June 2018). "$\mathbf{F}_p((X))$ is decidable as a module over the ring of additive polynomials". In: *arXiv.org*. arXiv: 1806.03123v2 [math.LO].
- Pasten, Hector, Thanases Pheidas, and Xavier Vidaux (2014). "Uniform existential interpretation of Arithmetic in rings of functions of positive characteristic". In: *Inventiones Mathematicae* 196.2, pp. 453–484.
- Pheidas, T and Karim Zahidi (2000). "Undecidability of existential theories of rings and fields: a survey". In: *Contemporary mathematics - American Mathematical Society* 270, pp. 49–105. issn: 1098-3627.
- Pheidas, Thanases (1985). "The Diophantine problem for addition and divisibility in polynomial rings (decidability, undecidability)". In: *PhD Dissertation, Purdue University*.

References IV

- Pheidas, Thanases (1987). “An Undecidability Result for Power Series Rings of Positive Characteristic. II”. In: *Proceedings of the American Mathematical Society* 100.3, pp. 526–530.
- Pheidas, Thanases and Xavier Vidaux (2010). “The analogue of Buchi’s problem for rational functions; Errata”. In: *Journal of the London Mathematical Society* 82, pp. 273–278.
- Pheidas, Thanases and Karim Zahidi (1999). “Undecidable existential theories of polynomial rings and function fields”. eng. In: *Communications in Algebra* 27.10, pp. 4993–5010. issn: 0092-7872.
- — (2004). “Elimination theory for addition and the Frobenius map in polynomial rings”. In: *Journal of Symbolic Logic* 69.4, pp. 1006–1026.

References V

Pheidas, Thanases and Karim Zahidi (2008). "Analogues of Hilbert's tenth problem". In: *Model theory with Applications to Algebra and Analysis*. London Math Society Lecture Note Series 2.

Poonen, Bjorn (Mar. 2008). "Undecidability in number theory". In: *Notices of the American Mathematical Society* 55.

Robinson, Raphael M. (1951). "Arithmetical definability of field elements". In: *J. Symbolic Logic* 16.02, pp. 125–126. issn: 0022-4812.

Shlapentokh, Alexandra (2006). *Diophantine Classes and Extensions to Global Fields*. Ed. by Cambridge University Press. isbn: 9780521833608.

References VI

Sirokofskich, Alla (2009). "Decidability of Sub-theories of Polynomials over a Finite Field". In: *Mathematical Theory and Computational Practice*. Ed. by Klaus Ambos-Spies, Benedikt Löwe, and Wolfgang Merkle. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 437–446. isbn: 978-3-642-03073-4.

Vojta, P. (2000). "Diagonal quadratic forms and Hilbert's Tenth Problem". In: *Contemporary Mathematics* 270, pp. 261–274.

Weispfenning, Volker (1984). "Quantifier elimination and decision procedures for valued fields". In: *Models and Sets*. Ed. by Gert H. Müller and Michael M. Richter. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 419–472.

Moments of Thanases Pheidas with his students in UOC

Moments of Thanases Pheidas with his students in UOC

Moments of Thanases Pheidas with his students in UOC

Panhellenic Logic Symposium in Anogeia, 2019