Uniform Existential Interpretation of Arithmetic in Rings of Functions of Positive Characteristic

Hector Pasten
Queen's University, Canada
and
Thanases Pheidas
University of Crete and Institute of Applied and Computational Mathematics, Foundation of Research and Technology, Greece
and
Xavier Vidaux
Universidad de Concepción, Chile

It is known that a system of Diophantine equations has a complex solution if and only if it has a solution modulo *infinitely many* primes. Since there is an algorithm to solve the former problem, there is also an algorithm to decide the latter. By deeper work due to Ax Ax it is also known that there is an algorithm to decide whether a system of Diophantine equations has a solution modulo *every* prime. In this work we show that the situation is completely different if we replace the fields $\mathbb{F}_p$ by rings of functions of positive characteristic and consider analogous Diophantine problems. For example, we show that the following (five) problems are undecidable:

Problems: Decide whether or not a system of Diophantine equations in the unknowns $x_1, \ldots, x_n$ together with conditions of the form "x_i is non-constant", for some of the unknowns x_i, has a solution in $\mathbb{F}_p[z]$ for

1. some prime p,
2. all primes p,
3. infinitely many primes p,
4. all but possibly a finite number of primes p, or
5. all primes p of the form $6k + 5$ (say).

We work in a class Ω, each element of which is a structure over a fixed language $\mathcal{L}$. We ask the question: "Is there an algorithm which, given any (existential) sentence of $\mathcal{L}$, determines whether the sentence is true in some (or all, or infinitely many, or almost all) elements of Ω?" In the cases that we will consider the answer is 'No'. We call results of this type *uniform* undecidability results.

Notation.

$\mathcal{L}_{\text{rings}}$ the language of rings.

Consider subrings of fields of rational functions $F(z)$, where F is a field, as structures over the following languages:

$\mathcal{L}_z = \mathcal{L}_{\text{rings}} \cup \{z\}$ where z is a constant symbol,

$\mathcal{L}_T = \mathcal{L}_{\text{rings}} \cup \{T\}$ where T is interpreted as the set of non-constant functions, and $\mathcal{L}_{z,\text{ord}} = \mathcal{L}_z \cup \{\text{ord}\}$ where ord is interpreted as the valuation ring at 0.

Some of our main results are:

Theorem 0.1. *First order arithmetic is uniformly positive-existentially interpretable in the class of*

1. *polynomial rings of positive characteristic over the language $\mathcal{L}_T$, with one parameter interpreted (in each structure of the class) as any non-constant element,*
2. *polynomial rings of positive characteristic over the language $\mathcal{L}_z$, without parameters, and*
3. *fields of rational functions of positive characteristic over the language $\mathcal{L}_{z,\text{ord}}$, without parameters.*

Our results for languages that extend $\mathcal{L}_z$ hold also for large classes of (subrings of) function fields of positive characteristic of bounded genus.

A major intermediate result of independent importance:
Fact: The relation
$$\exists s \in \mathbb{Z}\ y = x^{p^s}$$
is definable over each field $F(z)$ (of rational functions over a field of 'constants' F of characteristic p) in the language $\mathcal{L}_T$ *uniformly for all fields F and all characteristics which are greater than 20.*

This follows from previous work on $F(z)$-rational points of a class of varieties defined by Büchi. These are affine varieties, in variables $x_1, \ldots, x_M$ which are given by
$$x_{n+2}^2 - 2x_{n+1}^2 + x_n^2 = 2 \text{ for } \ n = 0, \ldots, M-2\ .$$

Quiz: Obviously there are the solutions $x_n = x + n$ for any $x \in F(z)$. Can you find any more in such a uniform manner (i.e. regardless of F and regardless of how large M is) for any fixed positive odd characteristic p? (They exist!)

To appear in Inventiones Mathematicae.

This work was developed as part of the first author's thesis at Universidad de Concepción (Chile). It was supported by the third author's Chilean research project Fondecyt 1090233. During the revision of this work, the first author was partially supported by an Ontario Graduate Scholarship, and the second author was supported by the Conicyt Program 'Atracción de Capital Humano Avanzado' 80112001.