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*

Abstract

We show that first order integer arithmetic is uniformly positive-existentially interpretable in large classes of (subrings of) function fields of positive characteristic over some languages that contain the language of rings. One of the main intermediate results is a positive existential definition (in these classes), uniform among all characteristics p, of the binary relation "$y = x^{p^s}$ or $x = y^{p^s}$ for some integer $s \geq 0$". A natural consequence of our work is that there is no algorithm to decide whether or not a system of polynomial equations over $\mathbb{Z}[z]$ has solutions in all but finitely many polynomial rings $\mathbb{F}_p[z]$. Analogous consequences are deduced for the rational function fields $\mathbb{F}_p(z)$, over languages with a predicate for the valuation ring at zero.

MSC references 03B25, 11U05, 12L05.

Keywords: Uniform Interpretability, Hilbert's Tenth Problem, Undecidability, Positive Characteristic, Polynomial Rings, Fields of Algebraic Functions, Function Fields

*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.

Contents

1 Introduction

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 (see [Nav10, p. 460]). 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 [A67] 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.

In order to state our main result, let us briefly introduce some notation. We denote by $\mathcal{L}_{\text{rings}}$ the language of rings, and we 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 (see Section 3 for more details).

Some of our main results are:

Theorem 1.1. *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 (see Theorem 4.5, Corollary 4.6 and Theorem 4.7 in Section 4).

A result relevant to ours is due to Rumely, who showed in [Rum80] that the natural numbers are uniformly interpretable in the class of global fields. Various authors have used the notion of uniform interpretability, but not in the context of positive existential theories, to the best of our knowledge. For some references and some extensions of [Rum80], see [Po07] (compare our results to the discussion in Section 6 of the latter).

From Theorem 1.1 and using standard arguments going back to Tarski, we deduce the following uniform undecidability results.

Theorem 1.2. *Consider any of the following three cases for the language $\mathcal{L}$ and the class Ω:*

1. *$\mathcal{L}$ is $\mathcal{L}_T$ and Ω is a non-empty subclass of the class of all polynomial rings $F[z]$, where F is a field of positive characteristic.*

2. *$\mathcal{L}$ is $\mathcal{L}_z$ and Ω is as in Item 1.*

3. *$\mathcal{L}$ is $\mathcal{L}_{z,\mathrm{ord}}$ and Ω is a non-empty subclass of the class of all fields of rational functions of the variable z, over a field F of positive characteristic.*

The following hold true:
a) There is no algorithm which determines whether or not any given positive-existential sentence of the language $\mathcal{L}$ is true or not in some *member of Ω.*
b) The conclusions of a) hold true if the word some *is substituted by any of the words* all, almost all *or* infinitely many *(members).*

From the point view of algebraic geometry, positive existential formulas over $\mathcal{L}_z$, when interpreted in $F(z)$, correspond to assertions concerning the existence of rational sections for families of varieties over the projective line, while over $\mathcal{L}_T$, they correspond to assertions concerning the existence of non-constant rational maps from the projective line to varieties. For polynomial rings the meanings are similar but considering instead morphisms of affine varieties.

Note that if the class Ω in Items 1 or 2 consists only of one polynomial ring, then the results above have already been proved, over $\mathcal{L}_z$ in [Den79] - or see [Dem07] for a much stronger result for polynomials over finite fields - and over $\mathcal{L}_T$ in [PZ99a]. Similar results for the case of classes consisting of one rational function field over $\mathcal{L}_{z,\mathrm{ord}}$ are proved in [Ph91] and [V94] (and even over $\mathcal{L}_z$ if the base field is finite - see also [KR92]).

One of the main tools that we develop is a positive existential definition of the relation $\mathrm{Den}_p(x,y)$, defined as "$y = x^{p^s}$ or $x = y^{p^s}$ for some natural number s" in large classes of subrings of function fields of positive characteristic p. This relation was introduced by Denef in [Den79] and has often been a crucial step to codify the integers in rings of functions of positive characteristic (see for example, by chronological order, [Ph87], [Ph91], [KR92], [Sh96], [PZ99a], [Sh00], [E03] and [ES09]). In particular, we prove:

Theorem 1.3. *There are positive-existential $\mathcal{L}_z$-formulas φ_1 and φ_2 such that, for every field F of positive characteristic p, φ_1 defines* Den_p *in $F[z]$ and φ_2 defines* Den_p *in $F(z)$.*

The relevant Theorem is 4.2 below, where we prove an analogous result for function fields of bounded genus and also for the language $\mathcal{L}_T$. The method of achieving these definitions is by utilizing the rational points on some specific varieties which come from a problem asked by J. R. Büchi (see Subsection 3.4). Note that a first order (not

existential) definition of the same relation in any function field of *fixed* odd characteristic over $\mathcal{L}_z$ can be found in [ES09][1].

Using the tool described above, the proof of Theorem 1.1 turns out to be a consequence of the following theorem which can be considered of independent interest.

Theorem 1.4. *Given a prime number p, let $|_p$ be the relation over $\mathbb{N}$ defined by "$x\ |_p\ y$ if and only if there exists an integer s such that $y = p^s x$". There exists a positive existential formula over the language $\{0, 1, +, R\}$, where R is a binary relation symbol, which is independent of p and defines multiplication in the structure $(\mathbb{N}; 0, 1, +, |_p)$.*

The relation $|_p$ was introduced by Denef in [Den79]. This result corresponds to Item 1 of Theorem 4.3 in Section 4.

With respect to Theorem 1.2, there seem to be rather few results of this kind in the literature, but there are several results on *asymptotic (un)decidability*: given a class of structures, to decide whether or not a given formula is true for all but finitely many of them. For example, in [CH03], Chatzidakis and Hrushovski prove that a certain class of differential fields, each of them separately having a decidable theory, has an asymptotic undecidable theory. On the other hand, Hrushovski [Hr06] and Macintyre [Mac] (independently) show that the class of algebraically closed fields in positive characteristic, together with the Frobenius map, is asymptotically decidable. Other results of the same flavour can be found in [AK65a, AK65b, AK66, A67].

The undecidability results that we obtain are a consequence of the undecidability of the positive existential theory of the ring of rational integers (the unsolvability of Hilbert's Tenth Problem), proved in 1970 by Y. Matijasevich, based on works M. Davis, H. Putnam and J. Robinson (see [D73], [Mat70] and [DMR74]). For general surveys on Hilbert's Tenth Problem, see [PZ99b], [Po03] and [Sh07].

Acknowledgements. The authors would like to thank Ricardo Baeza, Antonio Laface, Angus Macintyre and Thomas Scanlon for comments on a first version of this paper, and Alexander Molnar for a careful reading of the very final version of it. The authors were also benefited from discussions with Ram Murty, Alexandra Shlapentokh and Carlos Videla.

Finally, the authors would like to heartily thank the anonymous referee. Her or his comments and corrections greatly improved the quality and presentation of this work.

2 Outline of the proof

All the definitions and interpretations discussed in this section are uniform on the various parameters involved (unless specified otherwise) and positive existential.

[1]We have been informed that they now have obtained (non-uniform) positive existential such definitions over $\mathcal{L}_{z,\mathrm{ord}}$.

Let us briefly indicate the main points of the proof of Theorem 1.1. In particular, this result asserts that the semi-ring of natural numbers $(\mathbb{N}; 0, 1, +, \cdot)$ is uniformly positive-existentially interpretable in

(A) the class of positive characteristic polynomial rings $F[z]$, seen as $\mathcal{L}_T$-structures, with one parameter that stands for a non-constant polynomial, and

(B) the class of positive characteristic rational function fields $F(z)$, seen as $\mathcal{L}_{z,\mathrm{ord}}$-structures, without parameters.

(Item 2 of the Theorem is done similarly to (B), whose proof actually works for subrings of function fields.) We prove these two items separately, although their proofs have common ingredients.

The first step is of arithmetic nature. The structure $(\mathbb{N}; 0, 1, +, \cdot)$ is not well-suited to be interpreted directly in polynomial rings and rational function fields seen as $\mathcal{L}_T$ and $\mathcal{L}_{z,\mathrm{ord}}$-structures respectively. Thus, we first show (Theorem 4.3) that $(\mathbb{N}; 0, 1, +, \cdot)$ is uniformly interpreted (without any parameter) in

(C) the class of structures $\mathfrak{N}_p = (\mathbb{N}; 0, 1, +, |_p)$ for p prime, and

(D) the class of structures $\mathfrak{D}_p = (\mathbb{Z}; 0, 1, +, |, |_p, \mathbb{Z} \setminus \{-1, 0, 1\})$ for p prime.

Here, the symbol $|$ stands for the usual divisibility relation.

That the natural numbers are interpretable in $\mathfrak{N}_p$ via positive existential formulas is a known fact (see [Den79]), and our goal is to show that such an interpretation can be done by (positive existential) formulas that are independent of the prime p, so that it is uniform. Item (D) can be obtained by defining the relation $\leq$ independently of p and thus reducing to the previous case. For this we prove a result of additive number theory, Theorem 4.4, which can be of independent interest: a version of Lagrange's four squares theorem in the case of squares coprime to p, involving a uniformly bounded number of summands (independent of p).

The next fundamental step in our argument is to find a definition of the binary relation $\mathrm{Den}_p(x, y)$ defined by '$x = y^{p^s}$ or $y = x^{p^s}$ for some natural number s', which is uniform (independent of p) among all rational function fields of sufficiently large characteristic p (indeed, $p \geq 19$ is enough). This is obtained as a consequence of the existence of 'exceptional' sequences in the context of the so-called Büchi's problem in positive characteristic (see Subection 3.4). Actually this definition is uniform among all function fields of bounded genus and large enough characteristic (see Theorem 4.2 and the comments afterwards), which allows us to prove a more general version of Theorem 1.1. In each application, we are able to consider all but finitely many characteristics. For purposes of obtaining interpretations that are uniform for all primes, this is harmless as long as one can distinguish the exceptional (finitely many) cases by positive-existentially definable formulas and the interpretability result is known for the exceptional cases. Thus, for the sake of simplicity, and since the central issue of this work is uniformity, let us ignore this technicality for the rest of the present section.

The proof of (A) is as follows. We show that for p a given prime, the structure $\mathfrak{D}_p$ is uniformly interpretable (with one parameter) in the class of polynomial rings $F[z]$ of characteristic p, seen as $\mathcal{L}_T$-structures. This is achieved via the classical technique of Pell equations introduced by Denef in [Den79], following the approach of Zahidi and the second author [PZ99a]. Since the natural numbers are coded as the indices n of some pairs of solutions (x_n, y_n) of an equation of the form $X^2 - (a^2 - 1)Y^2 = 1$ for some non-constant a, this technique involves a parameter for a (which seems to be *necessary*). Nevertheless, this parameter turns out to have no impact for the consequences on uniform undecidability. Indeed, the key fact is that the formulas involved in this step actually *do not depend on* p, and therefore we can deduce (A) from (D). At this point we remark that the interpretation of $\mathfrak{D}_p$ in polynomial rings over the language $\mathcal{L}_T$ via formulas independent of p is already in [PZ99a], but this is not sufficient to obtain (A), as (D) is essential. One of the key steps is Lemma 8.3, which gives a definition (with parameters) of the relation Den_p on x-coordinates of some solutions of Pell equations. Here we could use our own definition of Den_p, which does not depend on any parameter and works in a much more general context, but this will not improve the interpretability results as the parameter is needed in the other formulas that appear in the interpretation.

The proof of (B) lies deeper. For p a given prime we show that the structure $\mathfrak{N}_p$ is uniformly interpretable in the class of rational function fields of characteristic p over the language $\mathcal{L}_{z,\mathrm{ord}}$ (and as indicated above, we can also consider function fields of bounded genus), making uniform the technique in [Ph91]. We interpret the natural numbers as the order of vanishing at $z = 0$ of nonzero rational functions without poles at $z = 0$, and then the relation $|_p$ for integers corresponds to the relation $\mathrm{Den}_p(x, y)$ for rational functions. The crucial point is that our definition of $\mathrm{Den}_p(x, y)$ is uniform on the characteristic p and works without restrictions on the field of coefficients for each characteristic, so that we can obtain (B) from (C). Non-uniform definitions of Den_p are already available in the literature in several special cases as discussed in the Introduction, but for our purposes the uniformity in the characteristic is the central issue.

The consequences on undecidability then follow (Theorem 1.2, and more generally Corollary 4.8).nonzero

3 Preliminaries

All languages considered will be first order languages with equality. The word *class* will always refer to a non-empty class of structures over a common language.

3.1 Notation

1. We consider 0 to be a natural number.

2. A language is identified with its set of constant, relation and function symbols.

3. If $\mathfrak{U}$ is a structure, we will denote by $|\mathfrak{U}|$ the underlying set of $\mathfrak{U}$.

4. If $\varphi(x_1, \ldots, x_n)$ is an $\mathcal{L}$-formula with free variables among $x_1, \ldots, x_n$, we will write $\varphi^{\mathfrak{U}}$ for its realization in the $\mathcal{L}$-structure $\mathfrak{U}$, namely,

$$\varphi^{\mathfrak{U}} = \{(x_1, \ldots, x_n) \in |\mathfrak{U}|^n \colon \mathfrak{U} \vDash \varphi(x_1, \ldots, x_n)\}.$$

   If α is a symbol of $\mathcal{L}$, we will write $\alpha^{\mathfrak{U}}$ for its interpretation in $\mathfrak{U}$.

5. We consider the following languages:

   - $\mathcal{L}_{\text{rings}} = \{0, 1, +, \cdot\}$, the language of rings.
   - $\mathcal{L}^* = \{0, 1, +\}$.

   Moreover, if $s_1, \ldots, s_n$ are relation, function or constant symbols, then we will write

   - $\mathcal{L}_{s_1,\ldots,s_n} = \mathcal{L}_{\text{rings}} \cup \{s_1, \ldots, s_n\}$, and
   - $\mathcal{L}^*_{s_1,\ldots,s_n} = \mathcal{L}^* \cup \{s_1, \ldots, s_n\}$.

6. The symbols

   - 0, 1 and z are constant symbols;
   - $+$ and $\cdot$ are binary function symbols;
   - T and ord are unary relation symbols;
   - $|$, $\neq$, R and S are binary relation symbols.

7. For each prime p, consider the following equivalence relation $|_p$ over $\mathbb{Z}$:

$$x \mid_p y \text{ if and only if there exists } s \in \mathbb{Z} \text{ such that } y = \pm x p^s.$$

   We will refer to it as *p-divisibility* and denote its restriction to the natural numbers by the same symbol.

8. Let $\mathfrak{N}_p$ be the $\mathcal{L}^*_R$-structure $(\mathbb{N}; 0, 1, +, |_p)$ and

$$\mathcal{N} = \{\mathfrak{N}_p \colon p \text{ is prime}\}.$$

9. Let $\mathfrak{D}_p$ be the $\mathcal{L}^*_{|,R,T}$-structure $(\mathbb{Z}; 0, 1, +, |, |_p, \mathbb{Z} \setminus \{-1, 0, 1\})$, where $x \mid y$ is interpreted as divisibility in the usual sense, and

$$\mathcal{D} = \{\mathfrak{D}_p \colon p \text{ is prime}\}.$$

10. If A is a commutative ring with unit and of prime positive characteristic p, let Den_p be the equivalence relation defined on A by

$$\text{Den}_p(x, y) \text{ if and only if there exists } s \in \mathbb{N} \text{ such that either } y = x^{p^s} \text{ or } x = y^{p^s},$$

    where p is the characteristic of A.

3.2 Uniform Definability

We briefly introduce the notion of uniform definability, and then give a non-trivial example to illustrate it.

Definition 3.1. *Let $\mathcal{L}$ be a first order language, let X be a non-empty proper subset of $\mathcal{L}$, and let $\mathcal{U}$ be a class of $\mathcal{L}$-structures. We will say that a symbol $\alpha \in X$ is* uniformly $\mathcal{L} \setminus X$-definable in $\mathcal{U}$*, if there exists an $\mathcal{L} \setminus X$-formula which defines the interpretation of α in each structure in $\mathcal{U}$. If moreover the formula is positive existential, then we will write* uniformly $\exists^+$-$\mathcal{L} \setminus X$-definable.

If the symbol α has the same name 'x' across its interpretations in elements of $\mathcal{U}$, we will say that 'x' is uniformly $\mathcal{L} \setminus \{\alpha\}$-definable. Also we may say that the family of interpretations of α is uniformly definable in $\mathcal{U}$ instead of saying that α is (in practice, the symbol α may be implicit, as in Lemma 5.5 for instance).

The following proposition is an immediate consequence of Theorem 4.4 (we state it only to illustrate the concept).

Proposition 3.2. *Consider the language $\{0, +, \leq, R_2\}$, where R_2 is a unary relation symbol, and the structures $\mathfrak{U}_r = (\mathbb{Z}; 0, +, \leq, P_2^r)$, where $P_2^r(x)$ stands for "x is a square and r does not divide x". The relation $\leq$ is uniformly $\exists^+$-$\{0, +, R_2\}$-definable in the class of all structures $\mathfrak{U}_r$ with $r \geq 2$.*

A highly relevant result in the direction of non-uniformity can be found in [CDM92], where it is shown that there is no formula in the language of rings that defines $\mathbb{F}_q$ in $\mathbb{F}_{q^2}$ for all but finitely many q (here q is any power of any prime).

3.3 Uniform Interpretability

We give the definition of the concept of *uniform interpretability* that we use in this work. See [Ho08, Chap. 5] for a general discussion on interpretations.

Definition 3.3. *Let $\mathcal{L}$ and $\mathcal{L}'$ be first order languages. Let $\mathfrak{M}$ be an $\mathcal{L}$-structure and $\mathcal{U}$ a class of $\mathcal{L}'$-structures. We say that $\mathfrak{M}$ is* uniformly interpretable *in $\mathcal{U}$ if there exist an $\mathcal{L}'$-formula $\varphi_{\mathcal{L}}$, and for each symbol s of $\mathcal{L}$, an $\mathcal{L}'$-formula φ_s, such that for each $\mathfrak{U}$ in $\mathcal{U}$ there is a surjective map $\theta_{\mathfrak{U}} \colon \varphi_{\mathcal{L}}^{\mathfrak{U}} \to |\mathfrak{M}|$ satisfying:*

- *$\varphi_c^{\mathfrak{U}} \subseteq \varphi_{\mathcal{L}}^{\mathfrak{U}}$ and $\theta_{\mathfrak{U}}^{-1}(c^{\mathfrak{M}}) = \varphi_c^{\mathfrak{U}}$ for each constant symbol c,*
- *$\varphi_R^{\mathfrak{U}} \subseteq (\varphi_{\mathcal{L}}^{\mathfrak{U}})^n$ and $(\theta_{\mathfrak{U}}^n)^{-1}(R^{\mathfrak{M}}) = \varphi_R^{\mathfrak{U}}$ for each n-ary relation symbol R, and*
- *$\varphi_f^{\mathfrak{U}} \subseteq (\varphi_{\mathcal{L}}^{\mathfrak{U}})^{n+1}$ and $(\theta_{\mathfrak{U}}^{n+1})^{-1}(f^{\mathfrak{M}}) = \varphi_f^{\mathfrak{U}}$ for each symbol of function of arity n (here $f^{\mathfrak{M}} \subseteq |\mathfrak{M}|^{n+1}$ is the graph of the interpretation of f in $\mathfrak{M}$).*

If needed, we will specify that $\mathfrak{M}$ is uniformly interpretable in $\mathcal{U}$ by $\Phi = \{\varphi_s\}_{s \in \mathcal{L} \cup \{\mathcal{L}\}}$ through the class $\theta_{\mathcal{U}}$ of maps $\theta_{\mathfrak{U}}$, $\mathfrak{U}$ in $\mathcal{U}$. If all formulas in Φ are positive existential then we will say that $\mathfrak{M}$ is uniformly $\exists^+$-interpretable *in $\mathcal{U}$.*

Note that if the class $\mathcal{U}$ consists of just one structure $\mathfrak{U}$, then the above definition coincides with the usual definition of interpretability.

For clarity of the exposition, let us state the following somewhat trivial consequence of Proposition 3.2, that illustrates both the concept of (uniform) interpretability and its relation to the concept of (uniform) definability.

Proposition 3.4. *Let $\mathcal{L} = \{0, +, \leq\}$ and $\mathcal{L}' = \{0, +, R_2\}$ with R_2 a unary relation symbol. Consider the $\mathcal{L}$-structure $\mathfrak{M} = (\mathbb{N}; 0, +, \leq)$ and $\mathcal{U}$ the class of $\mathcal{L}'$-structures $(\mathbb{Z}; 0, +, P_2^r)$ for $r \geq 2$ (with P_2^r as in Proposition 3.2). Then $\mathfrak{M}$ is uniformly $\exists^+$-interpretable in $\mathcal{U}$.*

The rest of this subsection is devoted to collect some observations on the concept of uniform interpretability that will be useful in the present work.

Fact 3.5. *Let $\mathcal{U}_1, \ldots, \mathcal{U}_n$ be classes of $\mathcal{L}'$-structures and let $\mathfrak{M}$ be an $\mathcal{L}$-structure. If $\mathfrak{M}$ is uniformly (positive-existentially) interpretable in each $\mathcal{U}_k$ and if there exists, for each $k = 1, \ldots, n$, a (positive-existential) $\mathcal{L}'$-formula φ_k that distinguishes the class $\mathcal{U}_k$ from the others, then $\mathfrak{M}$ is uniformly (positive-existentially) interpretable in the class $\bigcup_{k=1}^n \mathcal{U}_k$.*

In our applications we will use a sort of "transitivity" satisfied by the concept of uniform interpretability, which we now explain. Suppose that an $\mathcal{L}$-structure $\mathfrak{M}$ is uniformly interpretable in a class of $\mathcal{L}'$-structures $\mathcal{U}$ by $\Phi = \{\varphi_s\}_{s \in \mathcal{L} \cup \{\mathcal{L}\}}$, and suppose that each $\mathfrak{U} \in \mathcal{U}$ is uniformly interpretable in a class of $\mathcal{L}''$-structures $\mathcal{V}_\mathfrak{U}$ by $\Psi_\mathfrak{U} = \{\psi_{\mathfrak{U},s}\}_{s \in \mathcal{L}' \cup \{\mathcal{L}'\}}$ for some fixed language $\mathcal{L}''$. If the set of $\mathcal{L}''$-formulas $\Psi_\mathfrak{U}$ is the same for each $\mathfrak{U} \in \mathcal{U}$ then $\mathfrak{M}$ is uniformly interpretable in $\mathcal{V} = \cup_{\mathfrak{U} \in \mathcal{U}} \mathcal{V}_\mathfrak{U}$. Moreover this happens in a positive existential way if the formulas in Φ and $\Psi_\mathfrak{U}$ are positive existential. We will quote this as the *transitivity property* of uniform interpretability.

Now we proceed to discuss some applications of uniform interpretability to problems of decidability.

Once one has an interpretation of an $\mathcal{L}$-structure $\mathfrak{M}$ in an $\mathcal{L}'$-structure $\mathfrak{U}$ by a set Φ of formulas through a map $\theta_\mathfrak{U}$, it is standard to derive a (syntactic) algorithm $\mathcal{A}_\Phi$, *depending on Φ but not on $\mathfrak{U}$*, that transforms each $\mathcal{L}$-sentence F into an $\mathcal{L}'$-sentence $\mathcal{A}_\Phi(F)$, so that $\mathfrak{M} \vDash F$ if and only if $\mathfrak{U} \vDash \mathcal{A}_\Phi(F)$ (indeed, the algorithm roughly consists of replacing every symbol $s \in \mathcal{L}$ that occurs in F by the formula φ_s). Therefore, if one has a uniform interpretation of an $\mathcal{L}$-structure $\mathfrak{M}$ in a class $\mathcal{U}$ of $\mathcal{L}'$-structures by Φ, then there exists an algorithm $\mathcal{A}_\Phi$, *uniform in the sense that it depends on Φ but not on each element of $\mathcal{U}$*, that transforms each $\mathcal{L}$-sentence F into an $\mathcal{L}'$-sentence $\mathcal{A}_\Phi(F)$, so that, for each $\mathfrak{U}$ in $\mathcal{U}$, $\mathfrak{M} \vDash F$ if and only if $\mathfrak{U} \vDash \mathcal{A}_\Phi(F)$. Moreover, if Φ only consists of positive existential formulas, then the algorithm $\mathcal{A}_\Phi$ transforms positive existential sentences into positive existential sentences.

Uniform interpretability can be used to show very strong undecidability results. In the subsequent discussion, all formulas are meant to be positive existential. Suppose that an $\mathcal{L}$-structure $\mathfrak{M}$ is uniformly interpretable in a class $\mathcal{U}$ by a set of $\mathcal{L}'$-formulas Φ.

Note that the property that for each $\mathfrak{U}$ in $\mathcal{U}$, $\mathfrak{M} \vDash F$ if and only if $\mathfrak{U} \vDash \mathcal{A}_\Phi(F)$, yields the following equivalences:

$$\mathfrak{M} \vDash F \iff \text{for each } \mathfrak{U} \text{ in } \mathcal{U},\ \mathfrak{U} \vDash \mathcal{A}_\Phi(F) \iff \text{there exists } \mathfrak{U} \text{ in } \mathcal{U},\ \mathfrak{U} \vDash \mathcal{A}_\Phi(F).$$

If $\mathcal{C}$ is a non-empty collection (class) of non-empty subclasses of $\mathcal{U}$ then this implies:

$$\mathfrak{M} \vDash F \iff \text{ there exists } \mathcal{V} \text{ in } \mathcal{C} \text{ such that for each } \mathfrak{U} \text{ in } \mathcal{V},\ \mathfrak{U} \vDash \mathcal{A}_\Phi(F).$$

In particular, if there is no algorithm to decide whether or not an $\mathcal{L}$-sentence F is true in $\mathfrak{M}$, then the following problem is also undecidable:

($\star$) "Given an $\mathcal{L}'$-sentence G, decide whether or not there exists a class $\mathcal{V}$ in $\mathcal{C}$ such that every structure $\mathfrak{U}$ in $\mathcal{V}$ satisfies G."

We will refer to this phenomenon as *uniform undecidability property*.

For Item 1 of Theorem 1.1, we will need the more general concept of *uniform interpretability with parameters*. Though it is very close to Definition 3.3, we state it in the particular case we need it (namely, for one parameter) for the convenience of the reader. In the following, the notation $\mathbf{x}$ and $\mathbf{x}_s$ stand for tuples of variables.

Definition 3.6. *Let $\mathcal{L}$ and $\mathcal{L}'$ be first order languages. Let $\mathfrak{M}$ be an $\mathcal{L}$-structure and $\mathcal{U}$ a class of $\mathcal{L}'$-structures. We say that $\mathfrak{M}$ is* uniformly interpretable in $\mathcal{U}$ with one parameter α *if there exist an $\mathcal{L}'$-formula τ with one free variable, an $\mathcal{L}'$-formula $\varphi_{\mathcal{L}}(\alpha; \mathbf{x})$ and, for each symbol s of $\mathcal{L}$, an $\mathcal{L}'$-formula $\varphi_s(\alpha; \mathbf{x}_s)$, such that for each $\mathfrak{U}$ in $\mathcal{U}$ and for each $a \in \tau^{\mathfrak{U}}$, there is a surjective map $\theta_{\mathfrak{U},a} \colon \varphi_{\mathcal{L}}(a; \mathbf{x})^{\mathfrak{U}} \to |\mathfrak{M}|$ satisfying:*

- $\varphi_c(a; \mathbf{x}_c)^{\mathfrak{U}} \subseteq \varphi_{\mathcal{L}}(a; \mathbf{x})^{\mathfrak{U}}$ *and* $\theta_{\mathfrak{U},a}^{-1}(c^{\mathfrak{M}}) = \varphi_c(a; \mathbf{x}_c)^{\mathfrak{U}}$ *for each constant symbol c,*
- $\varphi_R(a; \mathbf{x}_R)^{\mathfrak{U}} \subseteq (\varphi_{\mathcal{L}}(a; \mathbf{x})^{\mathfrak{U}})^n$ *and* $(\theta_{\mathfrak{U},a}^n)^{-1}(R^{\mathfrak{M}}) = \varphi_R(a; \mathbf{x}_R)^{\mathfrak{U}}$ *for each n-ary relation symbol R, and*
- $\varphi_f(a; \mathbf{x}_f)^{\mathfrak{U}} \subseteq (\varphi_{\mathcal{L}}(a; \mathbf{x})^{\mathfrak{U}})^{n+1}$ *and* $(\theta_{\mathfrak{U},a}^{n+1})^{-1}(f^{\mathfrak{M}}) = \varphi_f(a; \mathbf{x}_f)^{\mathfrak{U}}$ *for each symbol of function of arity n.*

We may specify that $\mathfrak{M}$ is uniformly interpretable in $\mathcal{U}$ by the set of formulas $\{\varphi_s\}_{s \in \mathcal{L} \cup \{\mathcal{L}\}}$ with one parameter restricted by τ.

The remarks of this subsection can be extended in a straightforward way to our definition of uniform interpretability with parameters. The only point that requires closer attention is undecidability: the algorithm $\mathcal{A}_\Phi$ is syntactically the same except that one adds the string $\exists \alpha \tau(\alpha) \wedge$ at the beginning of the output formula.

3.4 Büchi's Problem in Positive Characteristic

In order to show that the relation Den_p is uniformly $\exists^+$-definable in several classes of structures, we need to introduce Büchi's problem. For that we consider a commutative ring A with unit having a subfield C of characteristic $p > 2$. If $M \geq 3$ is an integer, an *M-term Büchi sequence for (A, C)* is a sequence of M elements of A, not all in C, whose second difference of squares is the constant sequence $(2, \ldots, 2)$.

Büchi's Problem for Rings of Characteristic $p > 2$:
BP(A, C, M) *Is it true that for all $N \geq M$, any N-term Büchi sequence (x_n) of (A, C) satisfies*

$$x_n^2 = (x + n)^{p^s+1}, \qquad n = 1, \ldots, N,$$

for some $x \in A$ and some non-negative integer s?

Observe that in characteristic p, any sequence of the form $\left((x+n)^{\frac{p^s+1}{2}}\right)_n$ is indeed a Büchi sequence.

Notation 3.7. *If* **BP**(A, C, M) *has a positive answer for some M then we will denote by $M_0(A, C)$ the least such M and say that* **BP**(A, C) has a positive answer.

Note that $M_0(A, C)$, if it exists, is always at most the characteristic p of A (as if there exists an M-term Büchi sequence with $M > p$ then this sequence can be trivially extended into an infinite p-periodic Büchi sequence; see [PPV10]).

Definition 3.8. *Let $\mathcal{L}$ be a language extending the language of rings. A class $\mathcal{B}$ of $\mathcal{L}$-structures is an* $\mathcal{L}$-Büchi class *if there exists a constant M such that each structure A in $\mathcal{B}$ seen as a ring has a subfield C of positive characteristic satisfying:*

- **BP**(A, C) *has a positive answer with $M_0(A, C) \leq M$,*
- *if the unary predicate T belongs to $\mathcal{L}$, then T^A is the set of elements of A transcendental over C,*
- *if the constant symbol z belongs to $\mathcal{L}$, then z^A is transcendental over C,*
- *if $z \in \mathcal{L}$ and moreover the unary predicate* ord *belongs to $\mathcal{L}$, then there is a function field K of genus g with constant field C such that A is a subring of K,* ord^A *is the intersection of A with a valuation ring $\mathcal{O}_{\mathfrak{P}}$ at some prime $\mathfrak{P}$ of K, and $z^A \in A$ is a uniformizer at $\mathfrak{P}$ (hence transcendental over C). In this situation we further assume that* **BP**(K, C) *has a positive answer with $M_0(K, C) \leq M$, and that g is bounded as A ranges in $\mathcal{B}$;*
- *if z,* ord *and S are in $\mathcal{L}$ then we interpret z and* ord *as in the previous item and $S(x, y)$ as "x and y have the same order at $\mathfrak{P}$".*

The least such M is denoted by $M_0(\mathcal{B})$.

4 Results

The next proposition is one of the key technical results of our work (the proof is in Section 6).

Proposition 4.1. *For every integer $M \geq 3$, there exists a positive existential $\mathcal{L}_{\text{rings}}$-formula $\beta_M(x,y)$ with the following property: If $\mathbf{BP}(A,C)$ has a positive answer and $M_0(A,C) \leq M$ then:*

1. *if $\text{Den}_p(x,y)$ holds, then A satisfies $\beta_M(x,y)$, and*
2. *if either xy or $x+y$ is not in C, then $\text{Den}_p(x,y)$ holds if and only if A satisfies $\beta_M(x,y)$.*

With respect to the languages considered in this work, this implies:

Theorem 4.2. *For every positive integer M, there exists a positive existential $\mathcal{L}_T$-formula $\beta_M^T(x,y)$ and a positive existential $\mathcal{L}_z$-formula $\beta_M^z(x,y)$ such that:*

1. *if $\mathcal{B}$ is an $\mathcal{L}_T$-Büchi class with $M_0(\mathcal{B}) \leq M$, then $\beta_M^T(x,y)$ uniformly defines Den_p in $\mathcal{B}$, and*
2. *if $\mathcal{B}$ is an $\mathcal{L}_z$-Büchi class with $M_0(\mathcal{B}) \leq M$, then $\beta_M^z(x,y)$ uniformly defines Den_p in $\mathcal{B}$.*

Theorem 1.3 is an immediate consequence of Item 2 above. Indeed, the polynomial rings of characteristic ≥ 17 constitute a Büchi class, so we can use the results from [Den79] to cover the remaining cases (using disjunctions to construct one single formula). Similarly, the rational functions of characteristic ≥ 19 constitute a Büchi class and we can conclude by results from [Ph91, Lemma 1] and [V94, Lemma 2.3].

In the case of the language $\mathcal{L}_T$, one can actually impose much weaker hypothesis on the class $\mathcal{B}$ and define the slightly weaker relation

$$\text{Den}_p(x,y) \text{ holds, and either } x \text{ or } y \text{ is not in } C$$

instead of Den_p. Details are left to the reader (see proof of Theorem 4.2 in Section 6). However, Theorem 4.2 is enough for our purposes.

As already mentioned in Section 2, we do not really need the formula β_M^T in this work. Nevertheless, this formula (or a slight modification of it) might be used for studying interpretability problems in much wider context, such as function fields for instance. Note that over the language $\mathcal{L}_T$ the only known results are for polynomial rings in any characteristic (see [KR92] and [PZ99a] - these are undecidability results), and for complex analytic functions on the unit disk [Rub95] (a decidability result). The case of function fields is wide open, even for $\mathbb{F}_p(z)$.

Here are some known $\mathcal{L}$-Büchi classes where Theorem 4.2 applies (see [PV06] for Items 1 and 2, and [ShV11] for Item 3):

1. Any non-empty subclass of the class of one variable polynomial rings over a field of characteristic at least 17, where $\mathcal{L}$ is either $\mathcal{L}_z$ or $\mathcal{L}_T$.

2. Any non-empty subclass of the class of rational function fields over a field of characteristic at least 19, where $\mathcal{L}$ is $\mathcal{L}_z$.

3. Given an integer $g_0 \geq 0$, any non-empty subclass of the class of function fields of curves of genus $g \leq g_0$ and of positive characteristic at least $312g + 169$, where $\mathcal{L}$ is $\mathcal{L}_z$.

As far as arithmetic is concerned, we prove the following uniform interpretability results:

Theorem 4.3. *Multiplication is uniformly positive-existentially*

1. *$\mathcal{L}_R^*$-definable in $\mathcal{N} = \{(\mathbb{N}; 0, 1, +, |_p) \colon p \text{ is prime}\}$;*

2. *$\mathcal{L}_{|,R,T}^*$-definable in $\mathcal{D} = \{(\mathbb{Z}; 0, 1, +, |, |_p, \mathbb{Z} \smallsetminus \{-1, 0, 1\}) \colon p \text{ is prime}\}$.*

In particular, the semi-ring of natural numbers is uniformly $\exists^+$-interpretable in $\mathcal{N}$ and $\mathcal{D}$ without parameters.

In our approach, this theorem turns out to be essential for obtaining the uniform interpretability of arithmetic in rings of functions. Item 1 is proved in Subsection 5.2. Item 2 is proved in two different ways in Subsection 5.3. One way uses the following number-theoretical result, whose proof is given in Subsection 5.4.

Theorem 4.4. *There exists an absolute constant M such that for each integer $u \geq 2$, each non-negative integer is the sum of at most M squares of elements in*

$$C(u) = \{n \in \mathbb{Z} \colon u \nmid n\}.$$

As we shall see in the proof, one can take $M = 4599396$, which is far from being optimal, but is a bound that is independent of u. A more detailed argument, along the same lines as the proof that we will give here, can be used to show that the optimal M is less than 6000, but this is likely to be also far from optimal. Finding the optimal such M seems to be an interesting problem in additive number theory but we do not consider it in the present work.

We now turn to the results about uniform interpretability in rings of functions.

Theorem 4.5. *The semi-ring of natural numbers is uniformly $\exists^+$-interpretable without parameters in any $\mathcal{L}_{z,\mathrm{ord},\neq,S}$-Büchi class.*

In the following corollary, we specialize this theorem to some classes for which we have a positive existential uniform definition of $\neq$, ord or S.

Corollary 4.6. *The semi-ring of natural numbers is uniformly $\exists^+$-interpretable without parameters in any of the following classes:*

1. *the class of one variable polynomial rings over a field of positive characteristic over $\mathcal{L}_z$,*
2. *the class of one variable rational function fields of positive characteristic over $\mathcal{L}_{z,\mathrm{ord}}$,*
3. *the class $\mathcal{C}(g_0)$ of function fields of genus at most some g_0, whose characteristic is at least $312g + 169$, where g is the genus of the function field, over $\mathcal{L}_{z,\mathrm{ord}}$, and*
4. *the class of valuation rings of fields in $\mathcal{C}(g_0)$ over $\mathcal{L}_z$, where z is interpreted as a uniformizer of the valuation ring.*

We remark that Items 1 and 2 require results from [Den79], [Ph91] and [V94] (see the comments after Theorem 4.2 and Fact 3.5). Theorem 4.5 and Corollary 4.6 are proved in Section 7.

As far as the language $\mathcal{L}_T$ is concerned, we will prove the following in Section 8.

Theorem 4.7. *The semi-ring of natural numbers is uniformly $\exists^+$-$\mathcal{L}_T$-interpretable, with one parameter restricted by T, in the class of all polynomial rings over a field of positive characteristic, where $T(x)$ is interpreted in each structure as "x is non-constant".*

Corollary 4.8. *Let $\mathcal{L}$ be a language and let $\mathcal{U}$ be a class of $\mathcal{L}$-structures such that the conclusion of Theorems 4.5 or 4.7 hold. There is no algorithm to decide whether or not a positive existential $\mathcal{L}$-sentence is true for (for example):*

1. *some $\mathfrak{U}$ in $\mathcal{U}$;*
2. *all $\mathfrak{U}$ in $\mathcal{U}$;*
3. *infinitely many $\mathfrak{U}$ in $\mathcal{U}$ (assuming $\mathcal{U}$ to be infinite);*
4. *all but finitely many $\mathfrak{U}$ in $\mathcal{U}$ (assuming $\mathcal{U}$ to be infinite).*

This corollary follows from Theorem 4.7 and the discussion around Problem ($\star$) in Subsection 3.3. For example, one obtains Item 4 by choosing the class $\mathcal{C}$ (in the notation of Problem ($\star$)) to be the class of all cofinite subclasses of $\mathcal{U}$.

5 Uniform Definitions over the Integers

5.1 Some General Uniform Definitions in $\mathcal{N}$ and $\mathcal{D}$

In this subsection we will show that the restriction of the squaring function to the set of powers of a given prime is uniformly $\exists^+$-definable in $\mathcal{N}$ and in $\mathcal{D}$ - see Subsection 3.1, Items 7, 8, and 9.

When working with the structures $\mathfrak{N}_p$, the string '$a \leq b$' stands for $\exists c(b = a + c)$.

Notation 5.1. *For each prime number p we consider the sets:*

$$P_p^{>} = \{p^h \colon h \in \mathbb{N}\}, \qquad P_p^{\pm} = \{p^h \colon h \in \mathbb{N}\} \cup \{-p^h \colon h \in \mathbb{N}\},$$

$$P_{p,*}^{>} = \{p^h \colon h \in \mathbb{N}_{>0}\}, \text{ and } \quad P_{p,*}^{\pm} = \{p^h \colon h \in \mathbb{N}_{>0}\} \cup \{-p^h \colon h \in \mathbb{N}_{>0}\}.$$

Moreover, we consider the formulas

$$P(n) := R(1,n) \qquad \text{and} \qquad P_*^{\varepsilon}(n) := \begin{cases} R(1,n) \wedge (n \geq 2) & \text{if } \varepsilon \text{ is } > \\ R(1,n) \wedge T(n) & \text{if } \varepsilon \text{ is } \pm \ . \end{cases}$$

Note that $P(n)$ uniformly $\exists^+$-$\mathcal{L}_R^*$-defines the collection of sets $P_p^{>}$ in $\mathcal{N}$, and uniformly $\exists^+$-$\mathcal{L}_{|,R,T}^*$-defines the collection of sets $P_p^{\pm}$ in $\mathcal{D}$. Also note that $P_*^{\varepsilon}(n)$ uniformly $\exists^+$-$\mathcal{L}_R^*$-defines the collection of sets $P_{p,*}^{>}$ in $\mathcal{N}$ if ε is $>$, and uniformly $\exists^+$-$\mathcal{L}_{|,R,T}^*$-defines the collection of sets $P_{p,*}^{\pm}$ in $\mathcal{D}$ if ε is $\pm$.

Lemma 5.2. *Consider the positive existential formula*

$$\bar{\theta}_P^{\varepsilon}(m,n) \colon P_*^{\varepsilon}(m) \wedge P_*^{\varepsilon}(n) \wedge R(m-1, n-m)$$

over $\mathcal{L}_R^*$ if ε is $>$, and over $\mathcal{L}_{|,R,T}^*$ if ε is $\pm$. For each prime p, we have

1. *$\mathfrak{N}_p$ satisfies $\bar{\theta}_P^{>}$ if and only if $m, n \in P_{p,*}^{>}$ and $n = m^2$; and*
2. *$\mathfrak{D}_p$ satisfies $\bar{\theta}_P^{\pm}$ if and only if $m, n \in P_{p,*}^{\pm}$ and*
   - *either $n = m^2$,*
   - *$p = 2$ and $(m,n) \in \{(-2,-8), (2,-2), (4,-2), (4,-8)\}$, or*
   - *$p = 3$ and $(m,n) = (3,-3)$.*

Proof. We leave to the reader the verification of the implications from the right to the left. Suppose that $\bar{\theta}_P^{\varepsilon}$ is satisfied in $\mathfrak{D}_p$ or $\mathfrak{N}_p$ (depending on ε). There exist integers r, s, ℓ such that $r > 0$ and $s > 0$ and there exist ρ, σ, λ in $\{-1, 1\}$ (or $= 1$ if working in $\mathfrak{N}_p$) so that

$$m = \rho p^r, \quad n = \sigma p^s \quad \text{and} \quad n - m = \lambda p^{\ell}(m-1).$$

By direct substitution we obtain

$$\sigma p^s - \rho p^r = \lambda p^{\ell}(\rho p^r - 1)$$

and deduce that $\ell \geq \min\{r, s\} \geq 1$ because $p \nmid \rho p^r - 1$. Rearranging the previous equation we get

$$\sigma p^s = \rho\lambda p^{r+\ell} + \rho p^r - \lambda p^{\ell}. \tag{1}$$

We analyze this equation in two cases corresponding to $\lambda = \rho$ and $\lambda \neq \rho$ (note that the latter can only occur if working over $\mathfrak{D}_p$).
Case $\rho = \lambda$. We have $\lambda\rho = 1$, hence

$$\sigma p^s \geq p^{\ell+r} - |p^\ell - p^r| > 0$$

and we conclude that $\sigma = 1$. Thus Equation (1) becomes $p^s = p^{\ell+r} - \lambda(p^\ell - p^r)$ from which we deduce $\ell = r$, for otherwise the right-hand side is not a power of p (since $\ell, r \geq 1$). We obtain $p^s = p^{2r}$, that is $s = 2r$. Therefore, when $\rho = \lambda$ we have $\sigma = 1$ and $s = 2r$, which means $n = m^2$.
Case $\rho \neq \lambda$. We have $\lambda\rho = -1$ and

$$\sigma p^s \leq -p^{\ell+r} + p^\ell + p^r = 1 - (p^\ell - 1)(p^r - 1) \leq 0$$

because $\ell, r \geq 1$. Thus $\sigma = -1$ and Equation (1) becomes

$$p^s = p^{r+\ell} + \lambda(p^r + p^\ell). \tag{2}$$

We claim that $p \leq 3$. Indeed, if $p \geq 5$ then $|2\lambda| = 2 \leq (p-1)/2$ and we can look at Equation (2) as an equality between p-adic expansions with p-adic digits in the set

$$\left\{ \frac{-(p-1)}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2} \right\}.$$

We conclude that (2) cannot hold, as the right-hand side has at least two digits (because $\ell, r \geq 1$ and $0 \neq |2\lambda| \leq (p-1)/2$) while the left-hand side has only one. Therefore, if $\lambda \neq \rho$ then we have $p = 2$ or $p = 3$. We will explain the case $p = 3$ and leave the verification of the case $p = 2$ to the reader, as it involves the same kind of analysis.

With $p = 3$, Equation (2) gives $3^s = 3^{r+\ell} + \lambda(3^r + 3^\ell)$. Note that $r = \ell$, for otherwise the right-hand side would not be a power of 3. Hence we get $3^s = 3^{2r} + 2\lambda 3^r$ and in particular $s \geq r$. This leads to $3^{s-r} = 3^r + 2\lambda$, hence $3^{s-r} \equiv 2\lambda \mod 3$. From here we see that $s = r$ and $\lambda = -1$, so that $1 = 3^{s-r} = 3^r - 2$. In particular $r = s = 1$ and $\rho = 1$ (as $\rho \neq \lambda$). Recalling that $\sigma = -1$, we conclude that $(m, n) = (3, -3)$. □

Corollary 5.3. *There exists a positive existential formula*

1. *$\theta_P^>(m,n)$ that uniformly $\mathcal{L}_R^*$-defines the collection of sets $\{(p^h, p^{2h}) \colon h \in \mathbb{N}\}$ in $\mathcal{N}$ (hence squaring in $P_p^>$ is uniformly $\exists^+$-$\mathcal{L}_R^*$-definable in $\mathcal{N}$).*

2. *$\theta_P^\pm(m,n)$ that uniformly $\mathcal{L}_{|,R,T}^*$-defines the collection of sets $\{(\pm p^h, p^{2h}) \colon h \in \mathbb{N}\}$ in $\mathcal{D}$ (hence squaring in $P_p^\pm$ is uniformly $\exists^+$-$\mathcal{L}_{|,R,T}^*$-definable in $\mathcal{D}$).*

Remark 5.4. *Corollary 5.3 allows us to write in our formulas terms like a^2, a^4, a^8,... whenever a is an element of $P_p^>$, $P_{p,*}^>$, $P_p^\pm$ or $P_{p,*}^\pm$.*

5.2 Multiplication Uniformly in $\mathcal{N}$

We prove Item 1 of Theorem 4.3.

Lemma 5.5. *The collections of sets*

$$M_p = \{(n, p^a, np^a) \colon n \geq 0 \text{ and } a \geq 0\}$$

are uniformly $\exists^+$-$\mathcal{L}^*_R$-definable in $\mathcal{N}$.

Proof. Following the strategy of the second author in [Ph87, Section 2], one can show that the formula $\varphi(x, y, z)$, given by

$$R(1, y) \wedge z \geq x \wedge R(x, z) \wedge R(x + 1, z + y) \wedge R(x + y, z + y^2),$$

is true in $\mathfrak{N}_p$ if and only if $(x, y, z) \in M_p$ (the verification is not immediate, as there are many cases to consider, but it is a quite straightforward adaptation of *op. cit.*). □

The rest of the proof of Item 1 is identical to the proof of [Ph87, Lemma 3] using Lemma 5.5 instead of [Ph87, Lemma 2].

5.3 Multiplication Uniformly in $\mathcal{D}$

In this section we prove Item 2 of Theorem 4.3.

Lemma 5.6. *There is a positive existential $\mathcal{L}^*_{|,R,T}$-formula $CO(x)$ that defines uniformly the collection of sets*

$$CO_p = \{n \in \mathbb{Z} \colon p \nmid n\}$$

in $\mathcal{D}$ (hence the sets CO_p are uniformly $\exists^+$-$\mathcal{L}^*_{|,R,T}$-definable in $\mathcal{D}$).

Proof. Consider the formula

$$\exists m(P^{\pm}_*(m) \wedge n|(m - 1)).$$

If $n \in CO_p$, then we can take $m = p^{\phi(|n|)}$, since by Euler's theorem we know that $p^{\phi(|n|)}$ is congruent to 1 mod n.

Conversely, if the formula is satisfied in $\mathfrak{D}_p$, then there exists $k \in \mathbb{Z}$ such that $nk = m - 1$. Since p divides m, it does not divide n. □

The next lemma defines squaring uniformly in each CO_p.

Lemma 5.7. *The collection of sets*

$$\left\{(n, n^2) \colon n \in CO_p\right\}$$

is uniformly $\exists^+$-$\mathcal{L}^*_{|,R,T}$-definable in $\mathcal{D}$. More precisely, for any prime p we have: $n = m^2$ with $m, n \in CO_p$ if and only if $\mathfrak{D}_p$ satisfies the $\mathcal{L}^*_{|,R,T}$-formula $\theta_{CO}(m, n)$ given by

$$CO(m) \wedge CO(n) \wedge \exists a(P^{\pm}_*(a) \wedge m|(a^2 - 1) \wedge n|(a^2 - 1) \wedge (a^8 - m) \mid (a^{16} - n)).$$

Proof. If $n = m^2$ and $m, n \in CO_p$ then in particular $m, n \neq 0$ and the formula is satisfied by choosing $a = p^{\phi(n)}$, where ϕ stands for Euler's function (note that $\phi(|m|)$ divides $\phi(n)$).

Suppose that $\mathfrak{D}_p$ satisfies $\theta_{CO}(m, n)$ for some $m, n \in CO_p$. Since $a \in P^{\pm}_{p,*}$ we have $a \geq 2$. Since m and n divide $a^2 - 1$, we have $|m| < a^2$ and $|n| < a^2$. Since $a^8 - m$ divides

$$a^{16} - n = a^{16} - m^2 + m^2 - n,$$

we have:

1. $a^8 - m$ divides $m^2 - n$,
2. $|m^2 - n| < a^4 + a^2$ (since $|m| < a^2$ and $|n| < a^2$), and
3. $|a^8 - m| > a^8 - a^2$ (since $|m| < a^2$).

By Item 1, we have that either $m^2 - n = 0$ or $|a^8 - m| \leq |m^2 - n|$. For the sake of contradiction, suppose the latter is true. Then we have

$$a^8 - a^2 < |a^8 - m| \leq |m^2 - n| < a^4 + a^2.$$

Hence, since $a \geq 2$ we get

$$a^8 < a^4 + 2a^2 < a^4 + a^4 < a^8,$$

which is impossible. Therefore $m^2 = n$. □

By Lemma 5.7, we can use Theorem 4.4 to uniformly define the relation $\leq$ in $\mathcal{D}$. Therefore, Item 2 of Theorem 4.3 follows from Item 1. The proof of Theorem 4.4 is given in the next subsection. The following two lemmas give an alternative *elementary* way to conclude (though maybe in a somewhat less natural manner).

Lemma 5.8. *The collection of sets*

$$\{(x, y, z) \colon z = xy \text{ and } x \in CO_p \text{ and } y \in P^{\pm}_p\}$$

is uniformly $\exists^+$-$\mathcal{L}^*_{|,R,T}$-definable in $\mathcal{D}$. More precisely, for any integer prime p, we have: $x = mn$ with $m \in CO_p$ and $n \in P^{\pm}_p$, if and only if $\mathfrak{D}_p$ satisfies the formula

$$\rho_{CP}(m, n, x) \colon (n = -1 \wedge m = -x) \vee (n = 1 \wedge m = x) \vee \\ \left(CO(m) \wedge P^{\pm}_*(n) \wedge \exists a, b(\theta_{CO}(m, a) \wedge \theta^{\pm}_P(n, b) \wedge \theta_{CO}(m + n, a + 2x + b))\right).$$

Proof. Note that if p does not divide m and $n \in P^{\pm}_{p,*}$ then p does not divide $m + n$, and note that $(m + n)^2 = a + 2mn + b$. □

We are now ready to show that squaring is uniformly $\exists^+$-$\mathcal{L}^*_{|,R,T}$-definable in $\mathcal{D}$.

Lemma 5.9. *For any integer prime p and for any $m, n \in \mathbb{Z}$ the following holds: $n = m^2$ if and only if $\mathfrak{D}_p$ satisfies*

$$\exists a, b, u, v(P(a) \wedge P(b) \wedge CO(u) \wedge CO(v) \wedge \rho_{CP}(u, a, m) \wedge \\ \rho_{CP}(v, b, n) \wedge \theta_P^{\pm}(a, b) \wedge \theta_{CO}(u, v)).$$

Proof. Choose

$$a = p^{\mathrm{ord}_p m} \qquad \text{and} \qquad u = \frac{m}{a},$$

and do similarly for n. □

It is standard to define multiplication using squaring: for any $m, n, h \in \mathbb{Z}$ we have

$$h = m \cdot n \text{ if and only if } (m+n)^2 = m^2 + 2h + n^2.$$

Hence, multiplication is uniformly $\exists^+$-$\mathcal{L}^*_{|,R,T}$-definable in $\mathcal{D}$ and Item 2 of Theorem 4.3 follows.

5.4 Proof of Theorem 4.4

Let us recall the notion of Shnirelman density of a set of positive integers. If A is a set of positive integers, then we write $A[n] = |A \cap \{1, 2, \ldots, n\}|$. The *Shnirelman density* of A is defined by

$$\sigma(A) = \inf_{n \geq 1} \frac{A[n]}{n}.$$

Note that $0 \leq \sigma(A) \leq 1$. A fundamental property of the Shnirelman density is the following (see [Nat00, Section 11.3]).

Theorem 5.10. *For a set A of positive integers, if $1 > \delta = \sigma(A) > 0$ then every positive integer is the sum of at most g elements of A, where g depends only on δ (not on the particular set A). More precisely, one can take*

$$g = g(\delta) := 2\left(1 + \left\lfloor \frac{\log 2}{-\log(1-\delta)} \right\rfloor\right).$$

Recall that in the notation of Theorem 4.4 we have $u \geq 2$ and

$$C(u) = \{n \in \mathbb{Z} \colon u \nmid n\}.$$

Let $S(u)$ be the set of squares of elements in $C(u)$. Let A_u be the set of positive integers that can be expressed as the sum of at most 6 elements in $S(u)$, and let δ_u be the Shnirelman density of A_u (the reason for the number 6 in the definition of A_u will be clear later in the discussion). By Theorem 5.10, to prove Theorem 4.4 it suffices to give a positive lower bound δ^* for δ_u which is independent of u (one can take $M = 6g(\delta^*)$), and we devote the rest of this subsection to this end.

Let $r^{(u)}(n)$ be the number of ways to write n as the sum of 6 elements of $S(u)\cup\{0\}$, taking the order into account. Similarly, define $r(n)$ to be the number of ways to write n as a sum of 6 squares of non-negative integers, taking the order into account. Define

$$R^{(u)}(N)=\sum_{n=1}^{N} r^{(u)}(n).$$

On the one hand we have

$$\begin{aligned}
R^u(N) &= \#\left\{(x_1,\dots,x_6)\in\mathbb{N}^6\colon \sqrt{x_1^2+\cdots+x_6^2}\le N^{\frac{1}{2}} \wedge u\nmid x_i,\ \text{for } i=1,\dots,6\right\}\\
&\ge \left(\frac{u-1}{u}\right)^6 \#\left\{(x_1,\dots,x_6)\in\mathbb{N}^6\colon \sqrt{x_1^2+\cdots+x_6^2}\le N^{\frac{1}{2}}\right\}\\
&\ge \left(\frac{u-1}{u}\right)^6 \#\left\{(x_1,\dots,x_6)\in\mathbb{N}^6\colon x_i\le\sqrt{\frac{N}{6}}\ \text{for } i=1,\dots,6\right\}\\
&\ge \left(\frac{u-1}{u}\right)^6 \frac{N^3}{6^3}.
\end{aligned}$$

On the other hand, by [Nat00, Theorem 14.6] we know that $r(n)<40n^2$ if $n>0$, and hence $r^{(u)}(n)<40n^2$ (this is the reason for the number 6 in the definition of A_u). Therefore

$$R^{(u)}(N)\le\sum_{n\le N, r^{(u)}(n)\neq 0} 40n^2\le 40N^2A_u[N]$$

and we conclude that for every positive integer N

$$\frac{A_u[N]}{N}\ge\frac{1}{40\cdot 6^3}\left(\frac{u-1}{u}\right)^6\ge\frac{1}{40\cdot 6^3\cdot 2^6}$$

where we have used $u\ge 2$. This proves $\delta_u\ge 1/552960$ which is a positive lower bound independent of u, and hence the proof of Theorem 4.4 is complete.

As a side remark, using the lower bound $1/552960$ for δ_u in Theorem 5.10 and recalling the definition of A_u we see that one can take $M=4599396$ in Theorem 4.4, which is by no means intended to be optimal, but makes clear the uniformity on u.

6 The Relation "y is a p^s-th Power of x"

In this section, we prove Proposition 4.1 and Theorem 4.2. For short, we might write

$$\text{"there exists } s\in\mathbb{Z} \text{ such that } y=x^{p^s}\text{"}$$

instead of "there exists $s\in\mathbb{N}$ such that either $y=x^{p^s}$ or $x=y^{p^s}$".

Lemma 6.1. *Let A be a unitary commutative ring of prime characteristic p. Let $x, y \in A$ be such that $y = x^{p^s}$ for some non-negative integer s. Let $M \geq 2$ be an integer. Suppose that for $n = 1, \ldots, M$ the elements $x_n \in A$ satisfy*

$$x_n^2 = (x - 1 + n)^{p^s+1}.$$

We have

$$xy = x_1^2 \qquad \text{and} \qquad x + y = x_2^2 - x_1^2 - 1.$$

Proof. Let us show that the second equation holds. We have:

$$\begin{aligned} x + y &= x + x^{p^s} \\ &= x^{p^s+1} + x + x^{p^s} + 1 - x^{p^s+1} - 1 \\ &= (x+1)(x^{p^s} + 1) - x^{p^s+1} - 1 \\ &= (x+1)(x+1)^{p^s} - x^{p^s+1} - 1 \\ &= (x+1)^{p^s+1} - x^{p^s+1} - 1 \\ &= x_2^2 - x_1^2 - 1, \end{aligned}$$

which proves the lemma. □

Proof of Proposition 4.1. Suppose that Büchi's problem has a positive answer for a triple (A, C, M) and write $M_0 = M_0(A, C)$. Namely, any M-term Büchi sequence (x_n) of (A, C), with $M \geq M_0$, is of the form

$$x_n^2 = (f + n)^{p^s+1}$$

for some non-negative integer s and $f \in A$.

Consider the following formulas from the language of rings:

$$\varphi_0(x_1, \ldots, x_{M_0}, x, y) \colon \Delta^{(2)}(x_1^2, \ldots, x_{M_0}^2) = (2) \wedge xy = x_1^2 \wedge x + y = x_2^2 - x_1^2 - 1,$$

$$\varphi_1(x, y) \colon \exists x_1 \ldots \exists x_{M_0} \varphi_0(x_1, \ldots, x_{M_0}, x, y),$$

and

$$\beta_{M_0}(x, y) \colon \varphi_1(x, y) \vee \varphi_1(y, x).$$

Let us prove Item 1 of Proposition 4.1. Let $x, y \in A$ be such that $\mathrm{Den}_p(x, y)$ holds. By definition of Den_p we have $y = x^{p^s}$ for some integer s. If $s \geq 0$, taking $x_n \in A$ such that $x_n^2 = (x - 1 + n)^{p^s+1}$ the formula $\beta_{M_0}(x, y)$ is satisfied in A by Lemma 6.1. Analogously, if $s \leq 0$, then by taking $x_n^2 = (y - 1 + n)^{p^{-s}+1}$ the formula $\varphi_1(y, x)$ is true in A by Lemma 6.1.

Let us prove Item 2 of Proposition 4.1 (note that one implication comes directly from Item 1). Let $x, y \in A$ be such that A satisfies $\beta_{M_0}(x, y)$ and xy or $x + y$ is not in C. On the one hand, if xy is not in C then x_1^2 is not in C. On the other hand, if $x + y$ is not in C then $x_2^2 - x_1^2 - 1$ is not in C, hence one of x_1^2 and x_2^2 is not in C. Therefore,

the sequence $(x_1, \ldots, x_{M_0})$ is a Büchi sequence with at least one term not in C and by hypothesis, there exists $f \in A$ such that

$$x_n^2 = (f+n)^{p^s+1}$$

for some non-negative integer s. Therefore we have a system of equations in x and y

$$\begin{cases} xy = (f+1)^{p^s+1} \\ x+y = (f+2)^{p^s+1} - (f+1)^{p^s+1} - 1 \end{cases}$$

whose unique solutions are

$$(x,y) = (f+1, (f+1)^{p^s}) \qquad \text{and} \qquad (x,y) = ((f+1)^{p^s}, f+1)$$

(the verification is easy and is left to the reader). Hence either $y = x^{p^s}$ or $x = y^{p^s}$, i.e. $\mathrm{Den}_p(x,y)$ holds. □

Proof of Theorem 4.2. Within this proof, "transcendental" will always mean "transcendental over C", and "algebraic" will always mean "algebraic over C".

The positive existential formula from the language $\mathcal{L}_T = \{0, 1, +, \cdot, T\}$

$$\begin{aligned} \varphi_{\mathcal{B}}^T(x,y)\colon\ & ((T(xy) \vee T(x+y)) \wedge \beta_{M(\mathcal{B})}(x,y)) \vee \\ & \exists u \exists v ((T(uv) \vee T(u+v)) \wedge \beta_{M(\mathcal{B})}(ux, vy) \wedge \beta_{M(\mathcal{B})}(u,v)) \end{aligned}$$

uniformly defines Den_p in $\mathcal{B}$ over $\mathcal{L}_T$.

Indeed, if $\mathrm{Den}_p(x,y)$ holds, then there exists an integer s such that $y = x^{p^s}$. If either xy or $x+y$ is transcendental, then A satisfies

$$(T(xy) \vee T(x+y)) \wedge \beta_{M(\mathcal{B})}(x,y),$$

by Proposition 4.1. If none of xy and $x+y$ is transcendental, then choose u transcendental and $v = u^{p^s}$ if $s \geq 0$, or choose v transcendental and $u = v^{p^{-s}}$ if $s < 0$. For these choices of u and v, A satisfies

$$(T(uv) \vee T(u+v)) \wedge \beta_{M(\mathcal{B})}(ux, vy) \wedge \beta_{M(\mathcal{B})}(u,v).$$

Suppose now that A satisfies $\varphi_{\mathcal{B}}^T(x,y)$. If A satisfies

$$(T(xy) \vee T(x+y)) \wedge \beta_{M(\mathcal{B})}(x,y),$$

then $\mathrm{Den}_p(x,y)$ holds by Proposition 4.1. If not, then in particular both of xy and $x+y$ are algebraic, hence both of x and y are algebraic. Also there exist $u, v \in A$ such that

- uv or $u+v$ is transcendental (hence u or v is transcendental);
- there exists $r \in \mathbb{Z}$ such that $v = u^{p^r}$ (by Proposition 4.1 and the previous item); and

- A satisfies $\beta_{M(\mathcal{B})}(ux, vy)$.

Note that the first and second items imply that both u and v are transcendental.

Suppose that x or y is not 0 (otherwise $\mathrm{Den}_p(x, y)$ holds trivially).
Case 1: If $uxvy$ or $ux + vy$ is transcendental, then, by the third item and Proposition 4.1, there exists $s \in \mathbb{Z}$ such that $vy = (ux)^{p^s}$. Hence, neither x nor y is 0 and

$$u^{p^r} y = (ux)^{p^s},$$

which implies

$$yu^{p^r - p^s} = x^{p^s}.$$

Therefore, we have $r = s$ (since u is transcendental, but x and y are nonzero and not transcendental). Hence, $\mathrm{Den}_p(x, y)$ holds.

Case 2: If both $uxvy$ and $ux + vy$ are algebraic, then both ux and vy are algebraic, hence they are 0 (since u and v are transcendental but x and y are algebraic), which contradicts the fact that x or y is nonzero. This finishes the proof of Item 1 of Theorem 4.2.

Let us prove Item 2, namely, let us prove that the positive existential formula

$$\varphi^z_{\mathcal{B}}(x, y) \colon \beta_{M(\mathcal{B})}(x, y) \vee \exists u(\beta_{M(\mathcal{B})}(z, u) \wedge (\beta_{M(\mathcal{B})}(zx, uy) \vee \beta_{M(\mathcal{B})}(ux, zy))),$$

uniformly defines Den_p in $\mathcal{B}$ over $\mathcal{L}_z = \{0, 1, +, \cdot, z\}$.

Suppose first that $\mathrm{Den}_p(x, y)$ holds. There exists an integer s such that $y = x^{p^s}$. If $s \geq 0$, then by taking $u = z^{p^s}$ the formula $\beta_{M(\mathcal{B})}(zx, uy)$ holds in A by Proposition 4.1. If $s \leq 0$, then by taking $u = z^{p^{-s}}$ the formula $\beta_{M(\mathcal{B})}(ux, zy)$ holds in A by Proposition 4.1.

Suppose now that A satisfies $\varphi^z_{\mathcal{B}}(x, y)$. If xy or $x + y$ is transcendental then as A satisfies $\beta_{M(\mathcal{B})}(x, y)$ we are done by Proposition 4.1. So suppose that both xy and $x + y$ are algebraic (hence both x and y are algebraic).

Suppose that A satisfies

$$\exists u(\beta_{M(\mathcal{B})}(z, u) \wedge \beta_{M(\mathcal{B})}(zx, uy))$$

(the other case is done similarly). Since A satisfies $\beta_{M(\mathcal{B})}(z, u)$ and z is transcendental (hence zu or $z + u$ is transcendental), by Proposition 4.1, there exists an integer r such that

$$u = z^{p^r} \tag{3}$$

and in particular u is transcendental. Note that if both x and y are 0 then we are done. So we may assume that one of the two is nonzero.

Case 1: If $uy + zx$ or $uyzx$ is transcendental, as A satisfies $\beta_{M(\mathcal{B})}(zx, uy)$, there exists an integer k such that $uy = (zx)^{p^k}$ by Proposition 4.1. In particular, neither x nor y is 0. By Equation (3) we have $z^{p^r} y = (zx)^{p^k}$, hence

$$z^{p^r - p^k} y = x^{p^k},$$

which implies $k = r$ (since x and y are algebraic and nonzero and z is transcendental) and the result follows.

Case 2: If both $uy + zx$ and $uyzx$ are algebraic, then both uy and zx are algebraic, which is impossible since u and z are transcendental, x and y are algebraic, and at least one of x or y is nonzero. □

7 Functions over $\mathcal{L}_z$

7.1 Proof of Theorem 4.5

By Theorem 4.3, the semi-ring $(\mathbb{N}; 0, 1, +, \cdot)$ is uniformly $\exists^+$-interpretable in $\mathcal{N}$. By the transitivity property of uniform interpretability, in order to prove that $(\mathbb{N}; 0, 1, +, \cdot)$ is uniformly $\exists^+$-interpretable in any $\mathcal{L}_{z,\mathrm{ord},\neq,S}$-Büchi class, it is enough to prove the following:

Proposition 7.1. *Let $\mathcal{B}$ be an $\mathcal{L}_{z,\mathrm{ord},\neq,S}$-Büchi class. There exists a set of $\mathcal{L}_{z,\mathrm{ord},\neq,S}$-formulas Φ so that for every prime p with $\mathcal{B}_p$ non-empty (where $\mathcal{B}_p$ is the sub-class of structures of $\mathcal{B}$ with characteristic p), the $\mathcal{L}_R^*$-structure $\mathfrak{N}_p$ is uniformly $\exists^+$-interpretable in the class $\mathcal{B}_p$ by Φ.*

Proof. The proof is based on techniques from [Ph91]. Recall that by the definition of a Büchi class, for each structure $\mathfrak{B}$ in some $\mathcal{B}_p$, we have

- $\mathfrak{B}$ is a sub-ring of a function field of characteristic p, transcendental over the field of constants,
- $\mathrm{ord}^{\mathfrak{B}} = \mathfrak{B} \cap \mathcal{O}_{\mathfrak{P}}$ where $\mathcal{O}_{\mathfrak{P}}$ is the valuation ring at some prime $\mathfrak{P}$,
- $z^{\mathfrak{B}}$ is a uniformizer at $\mathfrak{P}$ which belongs to $\mathfrak{B}$, and
- $S(x, y)$ is satisfied in $\mathfrak{B}$ if and only if x and y have the same order at $\mathfrak{P}$.

Following the notation of the definition of uniform interpretability, we choose

- $\varphi_{\mathcal{L}_R^*}(x)$ to be $\mathrm{ord}(x) \wedge x \neq 0$;
- $\varphi_0 := 1$, $\varphi_1 := z$;
- $\varphi_=(x_1, x_2)$ to be the formula $S(x_1, x_2) \wedge x_1 \neq 0 \wedge x_2 \neq 0$;
- $\varphi_+(x_1, x_2, x_3)$ to be the formula

$$\exists u \left(\bigwedge_{i=1}^{3} \varphi_{\mathcal{L}_R^*}(x_i) \wedge x_1 \cdot x_2 = u \wedge S(x_3, u) \right);$$

- $\varphi_{|_p}(x_1, x_2)$ to be the formula

$$\exists u \left(\bigwedge_{i=1}^{2} \varphi_{\mathcal{L}_R^*}(x_i) \wedge \beta_M^z(x_1, u) \wedge S(u, x_2) \right);$$

- for every $\mathfrak{B} \in \mathcal{B}_p$, the map $\theta_{\mathfrak{B}} \colon \mathrm{ord}^{\mathfrak{B}} \smallsetminus \{0\} \to \mathbb{N}$ to be the (normalized) valuation map associated to the valuation ring $\mathcal{O}_{\mathfrak{P}}$.

Recall that by Theorem 4.2, β_M^z defines Den_p uniformly in any $\mathcal{L}_z$-Büchi class. The verification that this set of formulas fulfills the conditions for having a uniform interpretation is easy and left to the reader. □

7.2 Proof of Corollary 4.6

Let us first prove Item 1. The positive existential formula

$$\exists u, v (z \nmid u \wedge z \nmid v \wedge ux = vy),$$

where $z \nmid u$ stands for

$$\exists \lambda, \mu \, (\lambda\mu = 1 \wedge z \mid u - \lambda),$$

uniformly $\exists^+$-$\mathcal{L}_z$-defines S in the class of all polynomial rings over fields. Also, the relation $\neq$ is uniformly $\exists^+$-$\mathcal{L}_z$-definable in the class of all polynomial rings over fields by the formula (which we learned from a talk by A. Shlapentokh)

$$\varphi_{\neq}(t) \colon \exists x, u, v ((zu - 1)((z + 1)v - 1) = tx).$$

The verification is easy and left to the reader (for a general discussion on the relation $\neq$, see [MB07]). Finally, ord is uniformly $\exists^+$-$\mathcal{L}_z$-definable by any tautology.

We prove Items 2 and 3. In any class of fields, to be distinct from 0 is the same as being invertible, hence $\neq$ is uniformly $\exists^+$-$\mathcal{L}_{\mathrm{rings}}$-definable. Also S is uniformly $\exists^+$-$\mathcal{L}_{z,\mathrm{ord}}$-definable by the formula

$$\exists u, v \, (uv = 1 \wedge \mathrm{ord}(u) \wedge \mathrm{ord}(v) \wedge x = uy)$$

in the classes considered in these items.

We prove Item 4. To say that x and y have the same order in a valuation ring, we can use the $\mathcal{L}_{\mathrm{rings}}$-formula $\exists u, v \, (uv = 1 \wedge ux = y)$. The predicate ord can be defined using any tautology. Finally for the relation $\neq$, it is remarkable that, once more, one can use the solution to Büchi's problem to obtain a uniform definition in a simple way. Indeed, the $\mathcal{L}_z$-formula

$$\exists t \, (x \mid t \wedge \beta_M^z(t, z))$$

uniformly $\exists^+$-defines '$x \neq 0$' in the class considered in this item. Here one can take $M = 312g_0 + 169$.

8 Polynomials over $\mathcal{L}_T$

8.1 Pell Equations Uniformly

In this subsection, all the fields F have characteristic distinct from 2, and z stands for a transcendental element over F. If x and a are polynomials in z, we will denote by $x(a)$ the composition $x \circ a$.

Let $a \in F[z] \setminus F$ and $\Sigma_a(F)$ the set of solutions of

$$X^2 - (a^2 - 1)Y^2 = 1 \tag{4}$$

in $F[z]$. Recall that the operation

$$(x, y) \oplus (x', y') = (xx' + (a^2 - 1)yy', xy' + x'y)$$

defines a group law on $\Sigma_a(F)$, whose neutral element is $(1, 0)$. Note that $(-1, 0)$ is the only point of order 2 and that we have $\ominus(x, y) = (x, -y)$ and $(x, y) \oplus (-1, 0) = (-x, -y)$. Much more is known:

Theorem 8.1. *Every $(x, y) \in \Sigma_a(F)$ is of the form $(\pm x_n(a), y_n(a))$, where the pairs $(x_n(z), y_n(z))$ are defined by*

$$x_n(z) + \sqrt{z^2 - 1}y_n(z) = \left(z + \sqrt{z^2 - 1}\right)^n. \tag{5}$$

Moreover, for any $m, n \in \mathbb{Z}$ we have $n(a, 1) = (x_n(a), y_n(a))$ and

1. *$x_{m+n}(a) = x_m(a)x_n(a) + (a^2 - 1)y_m(a)y_n(a)$;*
2. *$y_{m+n}(a) = x_m(a)y_n(a) + x_n(a)y_m(a)$;*
3. *m divides n in $\mathbb{Z}$ if and only if $y_m(a)$ divides $y_n(a)$ in $F[z]$;*
4. *$y_n(a)$ is non constant if and only if $n \notin \{-1, 0, 1\}$;*
5. *if moreover $p \neq 0$ then for any s we have: $n = \pm mp^s$ if and only if $x_n(a) = x_m^{p^s}(a)$.*

Proof. See [PZ99a, Section 2]. □

Let $\Sigma_a^+(F)$ be the subset of $\Sigma_a(F)$ consisting of the pairs $(x_n(a), y_n(a))$. Consider the $\mathcal{L}^*_{|,R,T}$-structure

$$\mathfrak{S}_a^+(F) = \left(\Sigma_a^+(F); (1, 0), (a, 1), \oplus, |, \tilde{R}, \tilde{T}\right)$$

where

- $(f, g) \mid (h, k)$ means "g divides k";

- $\tilde{R}((f,g),(h,k))$ means "there exists $s \in \mathbb{Z}$ such that $f^{p^s} = h$";
- $\tilde{T}(f,g)$ means "g is not a constant".

It is then an immediate consequence of Theorem 8.1 that $\mathfrak{S}_a^+(F)$ is isomorphic to $\mathfrak{D}_p$ as $\mathcal{L}_{|,R,T}^*$-structures through the map

$$\begin{array}{rccc} \theta_{F[z]}\colon & \mathfrak{S}_a^+(F) & \to & \mathbb{Z} \\ & (x_n(a), y_n(a)) & \mapsto & n. \end{array}$$

8.2 Proof of Theorem 4.7

Consider the $\mathcal{L}_{\text{rings}}$-formula

$$\delta(\alpha; v, w)\colon v^2 - (\alpha^2 - 1)w^2 = 1.$$

Lemma 8.2. *If α is interpreted as a non-constant element $a \in F[z]$, then the positive existential $\mathcal{L}_{\text{rings}}$-formula*

$$\begin{aligned} \eta(\alpha; v, w)\colon \delta(\alpha; v, w) \wedge (\exists x, y(\delta(\alpha; x, y) \wedge (v = x^2 + (\alpha^2 - 1)y^2 \wedge w = 2xy) \vee \\ (v = (x^2 + (\alpha^2 - 1)y^2)\alpha + (\alpha^2 - 1)2xy \wedge w = x^2 + (\alpha^2 - 1)y^2 + 2\alpha xy))) \end{aligned}$$

is satisfied in $F[z]$ if and only if $(v, w) \in \Sigma_a^+(F)$.

Proof. The first part of the formula, namely $\delta(\alpha; v, w)$, says that (v, w) belongs to $\Sigma_a(F)$. The rest of the formula says that (v, w) is either of the form $2(x, y)$ or $2(x, y) \oplus (a, 1)$ for some $(x, y) \in \Sigma_a(F)$, which is equivalent to saying that $(v, w) \in \Sigma_a^+(F)$. □

Lemma 8.3. *Assume that F has characteristic $p > 2$. If α is interpreted as a non-constant element $a \in F[z]$, then the positive existential $\mathcal{L}_{\text{rings}}$-formula*

$$\Delta(\alpha; x, y, u, v) : \eta(\alpha; x, y) \wedge \eta(\alpha; u, v) \wedge \exists y_1 y_2 \, (\eta(x; u, y_1) \wedge \eta(x + 1; u + 1, y_2))$$

is satisfied in $F[z]$ if and only if $\mathrm{Den}_p(x, u)$ and both (x, y) and (u, v) lie in $\Sigma_a^+(F)$.

Proof. The proof is similar to the proof of Lemma 2.4 in [PZ99a]. Our formula is slightly different because we are working with $\Sigma_a^+(F)$ rather than $\Sigma_a(F)$, but this does not affect the proof. □

Theorem 8.4. *There exists a set Φ_α of positive existential $\mathcal{L}_T$-formulas with parameter α such that for each prime $p > 2$, the structure $\mathfrak{D}_p$ is uniformly interpretable in the class of polynomial rings of characteristic p by Φ_α.*

Proof. We list the formulas of Φ_α (following the notation in Subsection 3.3):

- $\varphi_{\mathcal{L}_{|,R,T}^*}(\alpha; x, y) : \eta(\alpha; x, y)$;

- $\varphi_0(x,y) : x = 1 \wedge y = 0$;
- $\varphi_1(\alpha; x, y) : x = \alpha \wedge y = 1$;
- $\varphi_=(\alpha; x, y, u, v) : \eta(\alpha; x, y) \wedge \eta(\alpha; u, v) \wedge x = u \wedge y = v$;
- $\varphi_+(\alpha; x, y, u, v, z, w) : xu + (\alpha^2 - 1)yv = z \wedge xv + yu = w \wedge \eta(\alpha; x, y) \wedge \eta(\alpha; u, v)$;
- $\varphi_|(\alpha; x, y, u, v) : \eta(\alpha; x, y) \wedge \eta(\alpha; u, v) \wedge \exists z(yz = v)$;
- $\varphi_R(\alpha; x, y, u, v) : \Delta(\alpha; x, y, u, v)$;
- $\varphi_T(\alpha; x, y) : \eta(\alpha; x, y) \wedge T(y)$.

Let us fix a prime $p > 2$. Note that by Lemma 8.2 the set $\varphi_{\mathcal{L}^*_{|,R,T}}(a; x, y)^{F[z]}$ is $\Sigma^+_a(F)$. The conclusion that $\mathfrak{D}_p$ is uniformly interpretable in the class of polynomial rings of characteristic p by Φ_α through the maps

$$\theta_{F[z],a} \colon \Sigma^+_a(F) \to \mathbb{Z}$$

follows from the discussion in this section. □

By Theorem 4.3, the semi-ring $(\mathbb{N}; 0, 1, +, \cdot)$ is uniformly $\exists^+$-interpretable in $\mathcal{D}$. By the transitivity property, the latter together with Theorem 8.4 implies that $(\mathbb{N}; 0, 1, +, \cdot)$ is uniformly $\exists^+$-interpretable with one parameter restricted by T in the class of polynomial rings of characteristic > 2 over $\mathcal{L}_T$.

The results at the end of the last section in [PZ99a] can be used to prove a result analogous to Theorem 8.4 in the case $p = 2$, so that $\mathfrak{D}_2$ is uniformly $\exists^+$-interpretable with one parameter restricted by T in the class of polynomial rings of characteristic 2 over $\mathcal{L}_T$. Therefore, $(\mathbb{N}; 0, 1, +, \cdot)$ is uniformly $\exists^+$-interpretable with one parameter restricted by T in the class of polynomial rings of characteristic 2 over $\mathcal{L}_T$. We can then deduce Theorem 4.7 from Fact 3.5 applied to the classes of $\mathcal{L}_T$-structures $\{F[z] \colon \mathrm{char}(F) = 2\}$ and $\{F[z] \colon \mathrm{char}(F) > 2\}$, since these classes can be distinguished by the formulas $1 + 1 = 0$ and $\exists x\, x + x = 1$.

References

[A67] J. Ax, *Solving Diophantine problems modulo every prime*, Annals of Mathematics **85-2**, 161-183 (1967).

[AK65a] J. Ax and S. Kochen, *Diophantine problems over local fields I*, American Journal of Mathematics **87-3**, 605-630 (1965).

[AK65b] J. Ax and S. Kochen, *Diophantine problems over local fields II*, American Journal of Mathematics **87-3**, 631-648 (1965).

[AK66] J. Ax and S. Kochen, *Diophantine problems over local fields III*, Annals of Mathematics **83-3**, 437-456 (1966).

[CDM92] Z. Chatzidakis, L. van den Dries and A. Macintyre, *Definable sets over finite fields*, J. reine u. ang. Math. **427**, 107-135 (1992).

[CH03] Z. Chatzidakis and E. Hrushovski, *Asymptotic theories of differential fields*, Illinois Journal of Mathematics **47-3**, 593-618 (2003).

[CL93] R. Cori and D. Lascar, *Logique mathématique 1 - Calcul propositionnel; algèbre de Boole; calcul des prédicats*, Masson - Collection Axiomes (1993). ISBN : 2-225-84079-2.

[D73] M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly **80**, 233-269 (1973).

[DMR74] M. Davis, Y. Matijasevich and J. Robinson, *Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution, Mathematical developments arising from Hilbert problems*, Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 323-378 (1974) (loose erratum) Amer. Math. Soc., Providence, R. I., 1976.

[Dem07] J. Demeyer, *Recursively enumerable sets of polynomials over a finite field are Diophantine*, Inventiones Mathematicae **170-3**, 655-670 (2007).

[Den78] J. Denef, *The Diophantine Problem for polynomial rings and fields of rational functions*, Transactions of the American Mathematical Society **242**, 391-399 (1978).

[Den79] —— *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium 78, M. Boffa, D. van Dalen, K. McAloon (eds.), North Holland, 131-145 (1979).

[E03] K. Eisenträger, *Hilbert's tenth problem for algebraic function fields of characteristic 2*, Pacific Journal of Mathematics **210-2**, 261-281 (2003).

[ES09] K. Eisenträger and A. Shlapentokh, *Undecidability in Function Fields of Positive Characteristic*, International Mathematics Research Notices, 4051-4086 (2009).

[Ho08] W. Hodges, *Model Theory*, Cambridge University Press, Encyclopedia of Mathematics and Its Applications **42**, (2008).

[Hr06] E. Hrushovski, *The elementary theory of the Frobenius automorphisms*, arXiv:math/0406514v1 (2006).

[KR92] K.H. Kim and F.W. Roush, *Diophantine unsolvability for function fields over certain infinite fields of positive characterisitic p*, Journal of Algebra **152-1**, 230-239 (1992).

[Mac] A. Macintyre, *Nonstandard Frobenius*, In preparation.

[Mat70] Y. Matijasevich, *Enumerable sets are Diophantine*, Doklady Akademii Nauk SSSR **191**, 279-282 (1970); English translation. Soviet Mathematics Doklady **11**, 354-358 (1970).

[MB07] L. Moret-Bailly, *Sur la définissabilité existentielle de la non-nullité dans les anneaux*, Algebra and Number Theory **1-3**, 331-346 (2007).

[Nat00] M. B. Nathanson, *Elementary Methods in Number Theory*, Springer, Graduate Texts in Mathematics **195**, (2000).

[Nav10] J. A. Navarro, *Álgebra conmutativa básica* (2010). Downloadable from http://matematicas.unex.es/∼navarro/ACB.pdf

[PPV10] H. Pasten, T. Pheidas and X. Vidaux, *A survey on Büchi's problem: new presentations and open problems*, Zapiski Nauchn. Sem. POMI **377**, 111-140 (2010).

[Ph87] T. Pheidas, *An undecidability result for power series rings of positive characteristic II*, Proceedings of the American Mathematical Society **100-3**, 526-530 (1987).

[Ph91] ——, *Hilbert's Tenth Problem for fields of rational functions over finite fields*, Inventiones Mathematicae **103**, 1-8 (1991).

[PV06] T. Pheidas and X. Vidaux, *The analogue of Büchi's problem for rational functions*, Journal of The London Mathematical Society **74-3**, 545-565 (2006). *Corrigendum: The analogue of Büchi's problem for rational functions*, Journal of The London Mathematical Society **82-1**, 273-278 (2010).

[PZ99a] T. Pheidas and K. Zahidi, *Undecidable existential theories of polynomial rings and function fields*, Communications in Algebra **27-10**, 4993-5010 (1999).

[PZ99b] T. Pheidas and K. Zahidi, *Undecidability of existential theories of rings and fields: A survey*, Contemporary Mathematics **270**, 49-106 (1999).

[Po07] B. Poonen, *Uniform first-order definitions in finitely generated fields*, Duke Mathematical Journal **138-1**, (2007).

[Po03] ——, *Hilbert's Tenth Problem over rings of number-theoretic interest*, downloadable from
www-math.mit.edu/∼poonen/papers/aws2003.pdf

[Rub95] L. Rubel, *An essay on Diophantine equations for analytic functions*, Expositiones Mathematicae, **13** 81-92 (1995).

[Rum80] R. Rumely, *Undecidability and definability for the theory of global fields*, Transactions of the American Mathematical Society **262-1**, 195-217 (1980).

[Sc08] T. Scanlon, *Infinite finitely generated fields are biinterpretable with* $\mathbb{N}$, Journal of the American Mathematical Society **21-3**, 893-908 (2008). *Erratum*, Journal of the American Mathematical Society **24-3**, 917 (2011).

[Sh96] A. Shlapentokh, *Diophantine Undecidability over Algebraic Function Fields over Finite Fields of Constants*, Journal of Number Theory **58**, 317-342 (1996).

[Sh00] —— *Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic*, Pacific Journal of Mathematics **193-2** (2000).

[Sh07] —— *Hilbert's tenth problem - Diophantine classes and extensions to global fields*, New Mathematical Monographs **7**, Cambridge University Press (2007).

[ShV11] A. Shlapentokh and X. Vidaux, *The analogue of Büchi's problem for function fields*, Journal of Algebra **330-1**, 482-506 (2011).

[V94] C. Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proceedings of the American Mathematical Society **120-1**, 249-253 (1994).