DEFINABILITY OF FROBENIUS ORBITS AND A RESULT ON RATIONAL DISTANCE SETS

HECTOR PASTEN

Abstract. We prove that the first order theory of (possibly transcendental) meromorphic functions of positive characteristic $p > 2$ is undecidable. We also establish a negative solution to an analogue of Hilbert's tenth problem for such fields of meromorphic functions, for Diophantine equations including vanishing conditions. These undecidability results are proved by showing that the binary relation $\exists s \geq 0, f = g^{p^s}$ is positive existentially definable in such fields. We also prove that the *abc* conjecture implies a solution to the Erdös-Ulam problem on rational distance sets. These two seemingly distant topics are addressed by a study of power values of bivariate polynomials of the form $F(X)G(Y)$.

1. Introduction and results

In this paper we investigate the definability of the binary relation $f \geq_p g$ given by $\exists s \geq 0, f = g^{p^s}$ in rings of functions of positive characteristic p (this is the "Frobenius orbit" mentioned in the title), and we explore consequences in undecidability. We also present some arithmetic results that naturally follow from our techniques, and in particular we prove that the *abc* conjecture for number fields implies a solution to the Erdös-Ulam problem on rational distance sets of the plane.

These two apparently distant themes (definability in positive characteristic and rational distance sets) are linked by a common approach: the study of power values of bivariate polynomials of the form $F(X)G(Y)$ (even the case $F(X)F(Y)$ will be useful in some of our applications). The method that we will use to study power values of $F(X)G(Y)$ is inspired by the method developed by the author in [13] and adapted to positive characteristic by J. Wang and the author in [15]. The results on power values of polynomials of the form $F(X)G(Y)$ can be of interest beyond the applications discussed in the previous paragraph, so we present the results with some additional generality.

Given a field k endowed with an absolute value, we write $\mathcal{A}_k$ for the ring of entire analytic functions defined over k on the variable z, that is, power series over k with infinite radius of convergence (although the notation does not reflect the absolute value). We denote by $\mathcal{M}_k$ the field of meromorphic functions defined over k on the

Date: July 23, 2016.

2010 *Mathematics Subject Classification.* Primary 11U05; Secondary 11J97, 52C10.

Key words and phrases. undecidability; positive characteristic; abc conjecture; Erdös-Ulam problem; rational distance sets.

Supported by a Benjamin Peirce Fellowship at Harvard and by a Schmidt Fellowship and by the NSF at the Institute for Advanced Study. This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

variable z, which is the fraction field of $\mathcal{A}_k$. In general $\mathcal{M}_k$ contains transcendental functions: one has $\mathcal{M}_k = k(z)$ if and only if the absolute value on k is trivial.

Consider the language $L_t = \{0, 1, t, +, \cdot, =\}$ and let k be a field endowed with an absolute value. Then $\mathcal{M}_k$ is an L_t-structure by interpreting t as z (and the other symbols in the obvious way).

Theorem 1.1. *There is a positive existential L_t formula $\psi(x, y)$ with the following property:*

Given any field k of positive characteristic $p > 2$ endowed with an absolute value, we have that for every pair of elements $f, g \in \mathcal{M}_k$

$$\mathcal{M}_k \models \psi(f, g) \Leftrightarrow \exists s \geq 0, f = g^{p^s}.$$

That is, the relation $\geq_p$ is uniformly positive existentially L_t-definable across the class of structures $\mathcal{M}_k$ as k varies over valued fields of odd positive characteristic.

Using this theorem we establish two undecidability results for fields of meromorphic functions in positive characteristic.

Theorem 1.2. *Let k be a field of positive characteristic $p > 2$ endowed with an absolute value, and let $\mathcal{M}_k$ be the field of meromorphic functions with variable z defined over k. The semi-ring $(\mathbb{N}; 0, 1, +, \times, =)$ is interpretable in the structure*

$$(\mathcal{M}_k; 0, 1, z, +, \times, =).$$

Moreover, the first order theory of

$$(\mathcal{M}_k; 0, 1, +, \times, =)$$

is undecidable.

Theorem 1.3. *Let k be a field of positive characteristic $p > 2$ endowed with an absolute value. Let v_z denote the z-adic valuation in $\mathcal{M}_k$. Let V be the 1-ary relation on $\mathcal{M}_k$ given by*

$$V(f) : \quad v_z(f) \geq 0$$

The semi-ring $(\mathbb{N}; 0, 1, +, \times, =)$ is positive existentially interpretable in the structure

$$(\mathcal{M}_k; 0, 1, z, +, \times, V, =).$$

Hence, the structure $(\mathcal{M}_k; 0, 1, z, +, \times, V, =)$ has undecidable positive existential theory.

Theorem 1.2 establishes undecidability of the first order theory of the field of (possibly transcendental) meromorphic functions over a valued field of *positive characteristic*. The situation is different for meromorphic functions in characteristic zero: at present, it is not known if the first order theory of the field of complex meromorphic functions is decidable or not, and similarly for p-adic meromorphic functions. On the other hand, when k has the trivial absolute value, i.e. $\mathcal{M}_k = k(z)$, and more generally for algebraic function fields of positive characteristic, the undecidability of the first order theory is known, see [4] and the references therein.

Theorem 1.3 establishes a version of Hilbert's tenth problem for $\mathcal{M}_k$ over the language L_t augmented by the valuation ring of v_z. Namely, an equivalent formulation of the result is the following: *there is no algorithm to decide existence of solutions in $\mathcal{M}_k$ to Diophantine equations with coefficients in $\mathbb{F}_p(z)$ together with vanishing conditions for some prescribed variables.* Theorem 1.3 is the positive characteristic counterpart of the version of Hilbert's tenth problem established by

Vidaux in [28], also over the language $L_t \cup \{V\}$ (thus, also for Diophantine equations with vanishing conditions). In fact, Vidaux addresses the non-archimedean case of characteristic zero, and we remark that the complex meromorphic case over the language $L_t \cup \{V\}$ remains open.

In the case of entire analytic (possibly transcendental) functions instead, one knows that the positive existential theory is undecidable in the non-archimedean case (see [9] for characteristic zero and [7] for positive characteristic), while it remains as an open problem whether the positive existential theory of complex holomorphic functions $\mathcal{A}_{\mathbb{C}}$ is undecidable, although it is known that the full first order theory of $\mathcal{A}_{\mathbb{C}}$ is in fact undecidable (see for instance Section 6 in [18]).

The interpretation of $(\mathbb{N}; 0, 1, +, \times, =)$ in $(\mathcal{M}_k; 0, 1, z, +, \times, =)$ in Theorem 1.2 follows the standard method of showing that the binary relation $\geq_p$ is definable –in fact, Theorem 1.1 shows that it is positive existentially definable– and then interpreting $(\mathbb{N}; 0, S, |, =)$ (S is the successor function and $|$ is the divisibility relation) which is enough thanks to a result of Julia Robinson [19]. Then one deduces undecidability over the language of rings *without parameters* (namely, for the structure $(\mathcal{M}_k; 0, 1, +, \times, =)$) using a method of Eisentraeger and Shlapentokh [4], getting rid of the parameters by interpreting the Q-theory of Raphael Robinson. This approach to undecidability is the same as in the function field case treated by Eisentraeger and Shlapentokh in [4], and our contribution is the definability of $\geq_p$ in $\mathcal{M}_k$ given by Theorem 1.1.

Similarly, the positive existential interpretation of $(\mathbb{N}; 0, 1, +, \times, =)$ in the structure $(\mathcal{M}_k; 0, 1, z, +, \times, =)$ in Theorem 1.3 follows the method of Pheidas developed in [16] for rational functions (unlike the proof of Vidaux result in characteristic zero [28]) and our contribution is the definability of $\geq_p$ in $\mathcal{M}_k$ given by Theorem 1.1.

The proof of Theorem 1.1 follows the ideas from [14] with the main difference that here we replace the arithmetic input of Büchi's problem by the following result, which can be of independent interest[1]:

Theorem 1.4. *Let $d \geq 1$ be an integer and let $p > 2$ be a prime. Let*

$$M = M(d,p) = 1 + \left\lceil \frac{1}{d} \left(12 + 8 \sum_{j=1}^{\lceil (d-1)/2 \rceil} p^j \right) \right\rceil .$$

Then we have the following:

Let k be a field of positive characteristic p endowed with an absolute value. Let $F_1, ..., F_M \in \mathbb{F}_p[X]$ be pairwise coprime irreducible polynomials of degree d. Let $f, g \in \mathcal{M}_k$ not both constant. If each $F_j(f)F_j(g)$ is a square in $\mathcal{M}_k$ for $j = 1, 2, ..., M$, then there is $s \geq 0$ such that $f = g^{p^s}$ or $g = f^{p^s}$.

We also prove the following algebraic version of Theorem 1.1, for which we see function fields of curves as L_t-structures by interpreting t as any fixed element which is a uniformizer at some point. For instance, in $K = k(z)$ we can interpret t as z.

Theorem 1.5. *Let $\mathfrak{g} \geq 0$ be an integer. There is a positive existential L_t formula $\varphi_{\mathfrak{g}}(x, y)$ with the following property:*

[1]We remark that a similar result is obtained for characteristic 2 replacing "square" by "cube", provided that we require s odd. For applications in definability, such a version is enough. We leave this straightforward modification to the interested reader.

Given any prime $p > 2$, any field k of positive characteristic p, and any function field K/k of a curve of genus $\leq \mathfrak{g}$, we have that for every pair of elements $f, g \in K$

$$K \models \varphi_{\mathfrak{g}}(f,g) \Leftrightarrow \exists s \geq 0, f = g^{p^s}.$$

As in the transcendental case, the theorem follows from the following arithmetic result:

Theorem 1.6. *Let $\mathfrak{g} \geq 0$ and $d \geq 1$ be integers and let $p > 2$ be a prime. Let*

$$M = M(\mathfrak{g}, d, p) = \left\lceil \frac{1}{d} \left(4\mathfrak{g} + 12 + 8 \sum_{j=1}^{\lceil (d-1)/2 \rceil} p^j \right) \right\rceil .$$

Then we have the following:

Let k be a field of characteristic p and let K be a one variable function field of genus $\mathfrak{g}$ defined over k. Let $F_1, ..., F_M \in \mathbb{F}_p[X]$ be pairwise coprime irreducible polynomials of degree d. Let $f, g \in K$ not both constant (i.e, not both in the algebraic closure of k in K). If each $F_j(f)F_j(g)$ is a square in K for $j = 1, 2, ..., M$, then there is $s \geq 0$ such that $f = g^{p^s}$ or $g = f^{p^s}$.

Although our main contribution in the aspect of definability of $\geq_p$ is Theorem 1.1 for meromorphic functions, we remark that in the function field case our Theorem 1.5 gives an improvement (with a simpler proof) of some existing results regarding the definability of $\geq_p$ in characteristic p. In fact, a version of Theorem 1.5 is proved in [14] using Büchi's problem (solved for positive characteristic function fields in [17] and [23]) *provided that the characteristic is sufficiently large* with respect to the genus. The general case has been recently established in [5] by a different method extending an argument by Pheidas in [16] –this adaptation is not straightforward and it involves several intricate computations– although the result in [5] requires a larger number of parameters in the definition (our definition only uses the parameter t). We also refer the reader to [22] for the case of S-integers in function fields.

Perhaps more relevant than the number of parameters being used, is the fact that our method for defining $\geq_p$ is much simpler than previous approaches. While it seems difficult to adapt Pheidas method from [16] and [5] to the transcendental case of $\mathcal{M}_k$ (among other reasons, because is uses induction on the degree of the functions), and while the analogue of Büchi's problem for $\mathcal{M}_k$ remains open in the positive characteristic case (which is an obstruction to a direct adaptation of the proof in [14]), our Theorem 1.6 admits a simple proof which works with no additional difficulty in $\mathcal{M}_k$ after the appropriate translation from function field arithmetic to Nevanlinna theory, yielding Theorem 1.4. Because of this reason, we will first prove the results for function fields (Section 2) and then for meromorphic functions (Section 4).

It is natural to ask for analogues of Theorems 1.4 and 1.6 in characteristic zero. We present below such an analogue for meromorphic functions in characteristic zero, which includes the complex and the p-adic case. Compared to our results in positive characteristic, the result below gives a more general formulation (power values of polynomials of the form $F(X)G(Y)$ instead of square values of $F(X)F(Y)$) at the cost of permitting a more general exceptional Zariski closed set.

Theorem 1.7. *Suppose that k is an algebraically closed field of characteristic 0, complete with respect to a given absolute value. Let d be a positive integer and let*

M be an integer satisfying

$$M > 8\left(1+\sqrt{1+\frac{1}{d}}\right)^2$$

(in particular, $M = 47$ is acceptable for all d). Let $F_1, \dots, F_M$ and $G_1, \dots, G_M$ be elements of $k[X]$ of degree d, without repeated factors and with the property that the F_j are pairwise coprime, and similarly the G_j are pairwise coprime. There is a non-zero polynomial $P(X,Y) \in k[X,Y]$ of degree $\leq d\sqrt{2M}$ such that for all $f, g \in \mathcal{M}_k$ not both constant, if $F_j(f)G_j(g)$ is a power in $\mathcal{M}_k$ for all $1 \leq j \leq M$ then $P(f,g) = 0$.

(There is a similar theorem for function fields in characteristic 0; the details are left to the interested reader.) The proof is given in Section 6 and it will follow the same ideas as for Theorems 1.4 and 1.6 in the setting of Nevanlinna theory, with the only relevant difference that in characteristic zero we construct certain auxiliary divisor using an elementary result from algebraic combinatorics, while in positive characteristic we use graphs of iterates of the Frobenius map –this difference will be explained in the proof.

From a geometric point of view, in the particular case of squares (say), we get from Theorem 1.7 that every analytic map to the projective closure in $\mathbb{P}^{M+2}$ of the surface defined by

$$F_j(X)G_j(Y) = Z_j^2, \quad (1 \leq j \leq M)$$

is algebraically degenerate, with a special set independent of the particular map. This special set is necessary as one could have $F_j = G_j$, requiring (at least) the diagonal in the special set.

Using Vojta's analogy between Nevanlinna Theory and Diophantine approximation, we can translate the proof of Theorem 1.7 from meromorphic functions to number fields. Since Theorem 1.7 will require the Second Main Theorem with truncation, the number field analogue will require a version of the *abc* conjecture. In particular, we will obtain:

Theorem 1.8. *Let K be a number field, let d be a positive integer, and let M be an integer satisfying*

$$M > 8\left(1+\sqrt{1+\frac{1}{d}}\right)^2$$

(in particular, $M = 47$ is acceptable for all d). Let $F_j, G_j \in K[X]$ for $1 \leq j \leq M$ be polynomials of degree d, without repeated factors and with the property that the F_j are pairwise coprime, and similarly for the G_j. Let L be a number field containing all the roots of the polynomials F_j and G_j, and assume that the abc conjecture holds for L. There is a proper Zariski closed set $Z \subseteq \mathbb{A}^2_K$ such that the following holds:

Given $(\alpha, \beta) \in K^2$, if for each $1 \leq j \leq M$ we have that $F_j(\alpha)G_j(\beta)$ is a power in K, then $(\alpha, \beta) \in Z$.

A more general result (Theorem 7.1) is presented in Section 7, where we also recall the statement of the *abc* conjecture for number fields (Conjecture 1).

Finally, in Section 8 we deduce the following consequence from our results in the number field case: we prove that the *abc* conjecture implies a solution to the Erdös-Ulam problem. Namely, we prove that the *abc* conjecture implies that there is no

dense subset U of $\mathbb{R}^2$ satisfying that the distances between each pair of elements of U are rational; see Section 8 for more details on this classical problem.

2. Function fields

In this section we consider function fields of positive characteristic and we prove Theorems 1.5 and 1.6.

For later reference, let us record here a particularly useful tool that will also be applied in our study of positive characteristic meromorphic functions. Despite being an elementary remark, it was systematically used in [15] where it played a key role. We will refer to it as the "Frobenius trick":

Remark 1. *Let $F \in \mathbb{F}_p(X)$ and f in a field K of characteristic p. Let $s \geq 0$. Suppose that an integer n divides $p^s - 1$. Then there is $h \in K$ such that*

$$F(f^{p^s}) = h^n F(f).$$

In fact,

$$F(f^{p^s}) = F(f)^{p^s} = \left(F(f)^{(p^s-1)/n}\right)^n F(f).$$

We will also need the next two lemmas:

Lemma 2.1. *Let $d, M \geq 1$ be positive integers. Let $S_1, ..., S_M \subseteq \overline{\mathbb{F}_p}$ be finite subsets consisting of algebraic elements of degree $\leq d$ over $\mathbb{F}_p$, such that each S_j is an orbit for the Frobenius map $\sigma_p : x \mapsto x^p$. Let $f, g \in k(C)$ be distinct non p-th power elements of the function field of a curve C defined over an algebraically closed field k of characteristic p (in particular, f, g are non-constant). Let $D = \max\{\deg f, \deg g\}$. The set*

$$A = \{q \in C : (f(q), g(q)) \in S_j \times S_j \text{ for some } 1 \leq j \leq M\}$$

satisfies

$$\#A \leq \left(2 + 4 \sum_{j=1}^{\lceil (d-1)/2 \rceil} p^j\right) D.$$

Proof. Consider $\mathbb{P}^2_k$ with coordinates $[x_0 : x_1 : x_2]$ and identify the affine chart $\{x_0 \neq 0\}$ with k^2. Let

$$\Omega = \bigcup_{j=1}^{M} S_j \times S_j \subseteq k^2 \subseteq \mathbb{P}^2.$$

By our hypotheses on the sets S_j, we see that Ω is contained in the union of the curves

$$\Gamma_j = \{x_1^{p^j} = x_0^{p^j - 1} x_2\} \text{ for } 1 \leq j \leq \lceil (d-1)/2 \rceil$$
$$\Delta = \{x_1 = x_2\}$$
$$\Gamma'_j = \{x_0^{p^j - 1} x_1 = x_2^{p^j}\} \text{ for } 1 \leq j \leq \lceil (d-1)/2 \rceil.$$

In fact, for all i we have that if $(\alpha, \beta) \in S_i \times S_i$ then α, β are Galois conjugate over $\mathbb{F}_p$ and both have degree d. Thus, there is $0 \leq j \leq \lceil (d-1)/2 \rceil$ such that $\alpha^{p^j} = \beta$ or $\alpha = \beta^{p^j}$, proving our claim that the union of the previous curves contains Ω.

The conditions on f, g imply that the image of $F = [1 : f : g] : C \to \mathbb{P}^2$ is an irreducible curve C' not contained in the support of the divisor

$$E = \Delta + \sum_{j=1}^{\lceil (d-1)/2 \rceil} (\Gamma_j + \Gamma'_j).$$

Thus, C' and E meet properly. Finally, we deduce from the definition of A and Ω, and from intersection theory (here, H is the line at infinity $\{x_0 = 0\}$)

$$\begin{aligned} \#A &\leq \deg F^* E = (\deg F)(C'.E) \\ &= (\deg F)(\deg C')(\deg E) = (\deg F^* H) \deg E. \end{aligned}$$

The result now follows from

$$\deg E = 1 + 2 \sum_{j=1}^{\lceil (d-1)/2 \rceil} p^j.$$

and from

$$\begin{aligned} \deg F^* H &= \sum_{\mathfrak{p} \in C} \max\{0, -v_{\mathfrak{p}}(f), -v_{\mathfrak{p}}(g)\} \\ &\leq \sum_{\mathfrak{p} \in C} \max\{0, -v_{\mathfrak{p}}(f)\} + \sum_{\mathfrak{p} \in C} \max\{0, -v_{\mathfrak{p}}(g)\} \qquad (2.1) \\ &= \deg(f^* \infty) + \deg(g^* \infty) = \deg(f) + \deg(g). \end{aligned}$$

□

Lemma 2.2. *Suppose that k is an algebraically closed field of characteristic $p > 2$ or 0. Let $f \in k(C)$ be non-constant, where C/k is a smooth projective curve of genus $\mathfrak{g}$. Let $F_1, \ldots, F_r \in k[X]$ be pairwise coprime polynomials of degree d without repeated factors. If $F_j(f)$ is a square for each $1 \leq j \leq r$, then*

$$r \leq \frac{1}{d} (4 + 4\mathfrak{g}).$$

Proof. If we are in positive characteristic we can assume that f is not a p-th power by the Frobenius trick. Let $q_1, \ldots q_n$ $(n = rd)$ be the roots of the polynomials F_j. In all cases, we can use the Riemann-Hurwitz formula to get

$$\sum_{i=1}^{n} \#f^{-1}(q_i) \geq (n-2) \deg(f) + 2 - 2\mathfrak{g}.$$

On the other hand,

$$\sum_{i=1}^{n} \#f^{-1}(q_i) = \sum_{j=1}^{r} \#(F_j(f))^{-1}(0) \leq \frac{1}{2} \sum_{j=1}^{r} \deg(F_j(f)) = \frac{rd}{2} \deg(f)$$

so we have

$$rd \leq 4 + \frac{4\mathfrak{g} - 4}{\deg(f)}.$$

□

Proof of Theorem 1.6. With no loss of generality we may assume that k is algebraically closed, and by the previous lemma we can assume that *both* f, g are non-constant. Using the Frobenius trick (cf. Remark 1) we can moreover assume

that f, g are not p-th powers, then (after this last reduction) our goal is showing that $f = g$.

It will be convenient to see f, g as morphisms from an algebraic curve C of genus $\mathfrak{g}$ (whose function field is K) to $\mathbb{P}^1$. Let $D = \deg(f) \geq D' = \deg g$. Let S_j be the set of roots of the polynomial F_j, let $N = dM$ and let $q_1, ..., q_N \in k$ be the roots of all the polynomials F_j (so that $\cup_i S_i = \{q_j\}_j$). The Riemann-Hurwitz formula gives

$$\sum_{j=1}^{N} \# f^{-1}(q_j) \geq (N-2)D + 2 - 2\mathfrak{g}. \tag{2.2}$$

Suppose that $f \neq g$. Let A be the set of points in C where f and g simultaneously take a value in some S_j (not necessarily the same value for both), and let P be the set of points of C where f or g have a pole. Put $B = A \cup P$. Then we have

$$\begin{aligned}
\sum_{j=1}^{N} \# f^{-1}(q_j) &= \sum_{j=1}^{N} \sum_{\mathfrak{p} \in C} \min\{1, v_{\mathfrak{p}}^{+}(f - q_j)\} \\
&= \sum_{\mathfrak{p} \in C} \sum_{j=1}^{N} \min\{1, v_{\mathfrak{p}}^{+}(f - q_j)\} \\
&\leq \sum_{\mathfrak{p} \in C \smallsetminus B} \sum_{j=1}^{N} \min\{1, v_{\mathfrak{p}}^{+}(f - q_j)\} + \# A + \# P
\end{aligned}$$

where the last inequality is due to the following observation: the q_j are pairwise distinct, so for each p at most one of the

$$\min\{1, v_{\mathfrak{p}}^{+}(f - q_j)\}$$

can be non-zero, in which case it takes the value 1.

Note that that $\# P \leq 2D$. To bound $\# A$ we apply Lemma 2.1 (which is possible, as f and g are not p-th powers and we are assuming $f \neq g$) with S_j the zero set of the polynomial $F_j \in \mathbb{F}_p[X]$, to get

$$\# A \leq \left(2 + 4 \sum_{j=1}^{\lceil (d-1)/2 \rceil} p^j \right) D.$$

Therefore we obtain

$$(N-2)D + 2 - 2\mathfrak{g} \leq \sum_{\mathfrak{p} \in C \smallsetminus B} \sum_{j=1}^{N} \min\{1, v_{\mathfrak{p}}^{+}(f - q_j)\} + \left(4 + 4 \sum_{j=1}^{\lceil (d-1)/2 \rceil} p^j \right) D.$$

Since $F_i(f)F_i(g)$ is a square for each i, we see that for each $\mathfrak{p} \in C \smallsetminus B$ and for each j, the function $f - q_j$ either vanishes with multiplicity ≥ 2 at $\mathfrak{p}$, or it takes a finite non-zero value at $\mathfrak{p}$. (Let us remark that it is at this point where we use our careful choice of the set A; it controls the common zeros of each pair $F_j(f)$, $F_j(g)$.)

Thus

$$\sum_{\mathfrak{p}\in C\smallsetminus B}\sum_{j=1}^{N}\min\{1,v_{\mathfrak{p}}^{+}(f-q_j)\}\le\frac{1}{2}\sum_{\mathfrak{p}\in C\smallsetminus B}\sum_{j=1}^{N}v_{\mathfrak{p}}^{+}(f-q_j)$$
$$\le\frac{1}{2}\sum_{j=1}^{N}\sum_{\mathfrak{p}\in C}v_{\mathfrak{p}}^{+}(f-q_j)=\frac{ND}{2}.$$

Putting these bounds together, it follows that

$$(N-2)D+2-2\mathfrak{g}\le\frac{ND}{2}+\left(4+4\sum_{j=1}^{\lceil(d-1)/2\rceil}p^j\right)D.$$

Recalling that $N=dM$, this gives

$$M<\frac{1}{d}\left(4\mathfrak{g}+12+8\sum_{j=1}^{\lceil(d-1)/2\rceil}p^j\right)$$

which contradicts the actual value of M. Hence, $f=g$ (after all the initial reductions), proving the result. □

Proof of Theorem 1.5. Fix $\mathfrak{g}\ge 0$. We will first prove the result for a formula depending on p and $\mathfrak{g}$ (not on the particular k and K), and at the end of the proof we will explain why one can actually take the same formula for all large p, thus proving the theorem.

Recall that we are only concerned with the case of characteristic $p>2$, so that Theorem 1.6 is available[2].

For $d\ge 1$ let M_d be the number of monic irreducible polynomials of degree d in $\mathbb{F}_p[X]$, then

$$M_d=\frac{1}{d}\sum_{t\mid d}\mu(t)p^{d/t}$$

where μ is the Möbius function. In particular, if $d\ge 3$ is prime (which we assume from now on), then

$$M_d=\frac{p^d-p}{d}\ge\frac{2p^d}{3d}\ge\frac{p^d}{2d}+\frac{3^d}{6d}\ge\frac{p^d}{2d}+1.$$

Note that since $p\ge 3$, the value of M in Theorem 1.6 is

$$M(\mathfrak{g},d,p)<1+\frac{1}{d}\left(4\mathfrak{g}+12+8p\cdot\frac{p^{d/2}-1}{p-1}\right)<1+\frac{1}{d}\left(4\mathfrak{g}+12+12p^{d/2}\right).$$

Therefore, we have $M_d>M(\mathfrak{g},d,p)$ as soon as $d\ge 3$ is a prime satisfying

$$p^d\ge 8\mathfrak{g}+24+24p^{d/2},$$

for which it suffices to take

$$d\ge 2\log\left(12+\sqrt{8\mathfrak{g}+168}\right)\ge\frac{2\log\left(12+\sqrt{8\mathfrak{g}+168}\right)}{\log p}.$$

[2]The reader wishing to extend the proof to the case $p=2$ might find it convenient to first establish a slightly modified version of Theorem 1.6 concerning cube values rather than square values.

Take d any prime satisfying the previous condition. Then $M_d > M = M(\mathfrak{g}, d, p)$ so that we can take distinct monic irreducible polynomials $F_j \in \mathbb{F}_p[X]$ for $j = 1, 2, ..., M$ as required in Theorem 1.6. Let k' be the algebraic closure of k in K, and consider the equivalence relation $f \sim_p g$ on K defined by: $f \geq_p g$ or $g \geq_p f$. It follows that there is a positive existential L_t-formula $\phi_{\mathfrak{g},p}(x, y)$ depending only on the two integers $\mathfrak{g}, p$, with the property that for every $f, g \in K$

- $K \models \phi_{\mathfrak{g},p}(f, g) \Rightarrow f \sim_p g$ or $f, g \in k'$ (by Theorem 1.6)
- $f \sim_p g \Rightarrow K \models \phi_{\mathfrak{g},p}(f, g)$ (by the Frobenius trick).

In fact, we can take $\phi_{\mathfrak{g},p}(x, y)$ as

$$\bigwedge_{j=1}^{M} \exists h_j, \tilde{F}_j(x)\tilde{F}_j(y) = h_j^2$$

where $\tilde{F}_j$ is a lift of F_j to $\mathbb{Z}[X]$. We remark that the only way in which the formula $\phi_{\mathfrak{g},p}(x, y)$ depends on p is in the choice of polynomials F_j and their lifts (this observation will be relevant later).

Thus, the positive existential L_t-formula

$$\exists u, \phi_{\mathfrak{g},p}(u, t) \wedge \phi_{\mathfrak{g},p}(f, g) \wedge \phi_{\mathfrak{g},p}(uf, tg)$$

defines the relation $\exists s \geq 0, f = g^{p^s}$ and we have not introduced new dependency of the formula on p. Note that the variable u in the previous formula not only distinguishes $\leq_p$ from $\geq_p$, but it also makes the formula work even in the case when f, g are constant.

Finally, note that if

$$p > 4\mathfrak{g} + 12$$

we can actually take $d = 1$ choosing $F_j = X - j$ for $j = 1, ..., M$ with $M = 4\mathfrak{g} + 12$. These polynomials can be written in the language L_t uniformly on p (i.e. they can be lifted to characteristic 0 uniformly on p), thus proving that for $p > 4\mathfrak{g} + 12$ one can choose the previous formulas $\phi_{\mathfrak{g},p}(x, y)$ uniformly on p; call this uniform formula $\phi_{\mathfrak{g}}(x, y)$. Then the positive existential L_t-formula $\varphi_{\mathfrak{g}}(x, y)$ (from the statement) can be taken as (note that $a \neq b$ is defined by $\exists c, (a - b)c = 1$)

$$\left(\phi_{\mathfrak{g}}(x, y) \wedge \bigwedge_{p \leq 4\mathfrak{g}+12} p \neq 0 \right) \vee \bigvee_{p \leq 4\mathfrak{g}+12} (p = 0 \wedge \phi_{\mathfrak{g},p}(x, y)) .$$

□

Remark 2. *Alternatively, the last part of the argument concerning the uniform formula $\phi_{\mathfrak{g}}(x, y)$ can be avoided (in the function field case) by recalling the uniform definitions from* [14]*; in fact the proof is the same, using Büchi's problem instead of our Theorem 1.6. However, the arguments in Section 4 regarding $\mathcal{M}_k$ cannot invoke Büchi's problem for large characteristic, since this problem remains open for meromorphic functions in positive characteristic (the case of meromorphic functions in characteristic zero is established in* [30] *and* [12]*).*

3. Basic facts of Nevanlinna theory

In later sections of the paper we will extend our results to the case of meromorphic functions; in particular, Section 4 contains the results relevant for our undecidability applications in positive characteristic. The proofs proceed in the same

way as in the function field case of the previous section, with the only difference that we have to replace:

- the use of degrees of rational functions for the Nevanlinna height,
- cardinalities of sets for Nevanlinna counting functions,
- intersection theory for the First Main Theorem (FMT) of Nevanlinna theory, and
- the application of the Riemann-Hurwitz formula (2.2) for the Second Main Theorem (SMT) of Nevanlinna theory.

The purpose of this section is to briefly recall the basic notation, definitions and key facts of Nevanlinna theory that we will be using. Further details on Nevanlinna theory for complex meromorphic functions can be found in [29], and the case of non-archimedean meromorphic functions (including positive characteristic) is discussed in detail in [2] and [8].

Let k be an algebraically field of characteristic $p \geq 0$, complete with respect to an absolute value. We write $\mathcal{M}_k$ for the field of meromorphic functions on $\mathbb{A}^1_k$, which is the fraction field of the ring of globally convergent power series over k.

Given an analytic divisor $D = \sum_i n_i \mathfrak{p}_i$ on $\mathbb{A}^1_k$ (where $n_i \in \mathbb{Z}$ and $\mathfrak{p}_i \in \mathbb{A}^1_k(k)$ satisfy that for all $B > 0$ the set $\{\mathfrak{p}_i : |\mathfrak{p}_i| < B\}$ is finite) one defines the Nevanlinna counting function for $r > 0$

$$N(D, r) = \int_0^r \frac{n(D, r) - n(D, 0)}{t} dt + n(D, 0) \log r$$

where $n(D, r) = \sum_{|\mathfrak{p}_i| \leq r} n_i$.

An (analytic) divisor is effective if all its coefficients n_i are non-negative. If D is effective we write D^{red} for the reduced divisor obtained by setting all strictly positive coefficients of D equal to 1 (i.e. we ignore multiplicities).

Let $F : \mathbb{A}^1_k \to \mathbb{P}^n_k$ be an analytic map, then for every divisor D on $\mathbb{P}^n_k$ whose support does not contain the image of F one defines the *proximity function* $m_F(D, r)$ for $r > 0$. When D is effective, the proximity function $m_F(D, r)$ is non-negative. The precise definition of the proximity function depends on whether the absolute value is archimedean or not, and we omit it here –see [29, 8] for details. In the particular case when D is the hyperplane at infinity defined by $x_0 = 0$, the proximity function takes the simple form

$$m_F(D, r) = \begin{cases} \displaystyle\int_0^{2\pi} \log\left(1 + |f_1|^2 + \ldots + |f_n|^2\right) \frac{d\theta}{4\pi} & \text{if } k = \mathbb{C} \\ \log \max\{1, |f_1|_r, \ldots, |f_n|_r\} & \text{if } k \text{ is non-archimedean} \end{cases}$$

provided that we write F in the form $[1 : f_1 : \ldots : f_n]$, which is possible as long as the image of F is not contained in the support of D. Here, for any given real number $r > 0$, we write θ for the angular parameter on the arc $\{z \in \mathbb{C} : |z| = r\}$, and in the non-archimedean case $|\cdot|_r$ is the unique extension to $\mathcal{M}_k$ of the absolute value

$$\left| \sum_{j \geq 0} a_j z^j \right|_r = \max_{j \geq 0} |a_j| \cdot r^j$$

on the ring $\mathcal{A}_k$.

The pull-back of D by F is denoted by F^*D, and it is an analytic divisor provided that the support of D does not contain the image of F. The *counting function of*

F with respect to D is

$$N_F(D,r) = N(F^*D, r)$$

and if D is effective one defines the *truncated counting function* as

$$N_F^{(1)}(D,r) = N((F^*D)^{red}, r).$$

The *Nevanlinna height* (or "characteristic") of F with respect to a divisor D on $\mathbb{P}^n_k$ not containing the image of F is defined as

$$T_F(D,r) = m_F(D,r) + N_F(D,r).$$

The following basic property of T_F is the *First Main Theorem*:

Theorem 3.1 (FMT)**.** *If D and E are linearly equivalent divisors in $\mathbb{P}^n_k$ and $F : \mathbb{A}^1_k \to \mathbb{P}^n_k$ is a non-constant analytic map with image not contained in the support of D or E, then*

$$T_F(D,r) = T_F(E,r) + O(1).$$

A deeper result, although standard in Nevanlinna theory, is the *Second Main Theorem*. There are many versions of it, but we will restrict our attention to the truncated version for $\mathbb{P}^1$, see [31] for details in the positive characteristic case. To simplify the exposition in the case of maps to $\mathbb{P}^1$, to each $f \in \mathcal{M}_k$ we associate the holomorphic map $F = [1 : f] : \mathbb{A}^1_k \to \mathbb{P}^1_k$ adapting the previous notation accordingly, and moreover we write $T_f(r) := T_F(\infty, r)$.

Theorem 3.2 (SMT)**.** *Let $f \in \mathcal{M}_k$ be non-constant and assume that it is not a p-th power (where $p \geq 0$ is the characteristic). Let $a_1, \ldots, a_M$ be distinct points in $\mathbb{P}^1_k$. Then for every $\epsilon > 0$ we have*

$$(M - 2 - \epsilon) T_f(r). < . \sum_{j=1}^{M} N_f^{(1)}(a_j, r)$$

where $. < .$ means that the inequality occurs for r outside a set of finite Lebesgue measure in $\mathbb{R}_{\geq 0}$.

It will be useful to point out that in the case of a holomorphic map F to $\mathbb{P}^1_k$ induced by $f \in \mathcal{M}_k$ and for $a \in k$, we have a simple expression for the function $n_f^{(1)}(a,r) := n((F^*a)^{red}, r)$ occurring in the definition of $N_f^{(1)}(a,r)$, namely

$$n_f^{(1)}(a,r) = \sum_{|z| \leq r} \min\{1, v_z^+(f-a)\}$$

where v_z is the order at z, and $v_z^+(-) = \max\{0, v_z(-)\}$.

Also, we will need the following substitute for the bound (2.1).

Lemma 3.3. *Let $F : \mathbb{A}^1_k \to \mathbb{P}^n_k$ be an analytic map of the form $F = [1 : f_1 : \ldots : f_n]$ with $f_j \in \mathcal{M}_k$. Let H be the hyperplane at infinity in $\mathbb{P}^n_k$, given by $x_0 = 0$. Then*

$$T_F(H,r) \leq \sum_{j=1}^{n} T_{f_j}(r).$$

Proof. The analogous inequality for the counting function is proved as in the function field case (cf. the bound (2.1)). The corresponding bound for the proximity function in the complex case is obtained by integrating the logarithm of

$$1 + |f_1(z)|^2 + \ldots + |f_n(z)|^2 \leq (1 + |f_1(z)|^2) \ldots (1 + |f_n(z)|^2)$$

which is valid for $z \in \mathbb{C}$ away from the poles of the f_j. Finally, the corresponding estimate for the proximity function in the non-archimedean case follows from

$$\max\{1, |f_1|_r, \dots, |f_n|_r\} \leq \prod_{j=1}^{n} \max\{1, |f_1|_r\}.$$

□

4. Meromorphic functions in positive characteristic

In this section we develop the analogues for $\mathcal{M}_k$ of the results proved in Section 2.

The following lemma will be used in place of Lemma 2.1

Lemma 4.1. *Suppose that k is an algebraically closed field of positive characteristic p, complete with respect to an absolute value. Let $d, M \geq 1$ be positive integers. Let $S_1, ..., S_M \subseteq \overline{\mathbb{F}_p}$ be finite subsets consisting of algebraic elements of degree $\leq d$ over $\mathbb{F}_p$, such that each S_j is an orbit for the Frobenius map $\sigma_p : x \mapsto x^p$. Let $f, g \in \mathcal{M}_k$ be distinct non p-th power elements (in particular, f, g are non-constant). Consider the set*

$$A = \{q \in k : (f(q), g(q)) \in S_j \times S_j \text{ for some } 1 \leq j \leq M\}.$$

Then the formal sum of the elements of A is an analytic divisor (which we also denote by A) and it satisfies

$$N(A, r) \leq \left(2 + 4 \sum_{j=1}^{\lceil (d-1)/2 \rceil} p^j\right) \max\{T_f(r), T_g(r)\} + O(1).$$

Proof. A defines an analytic divisor on $\mathbb{A}^1_k$ because $f \neq g$. To prove the bound we proceed as in Lemma 2.1. Define the map $F = [1 : f : g] : \mathbb{A}^1_k \to \mathbb{P}^2$ and define the set Ω and the divisor E on $\mathbb{P}^2$ exactly as in Lemma 2.1. Then

$$A = \{q \in k : F(q) \in \Omega\}$$

so that

$$N(A, r) \leq N_F(E, r) \leq T_F(E, r) = \deg(E) T_F(H, r) + O(1)$$

where H is the line at infinity. Here we used the positivity of $m_F(E, r)$ (as E is effective) and the FMT, which is possible since the image of F is not contained in the support of E and of H. The result follows, using Lemma 3.3. □

The next lemma will substitute Lemma 2.2

Lemma 4.2. *Suppose that k is an algebraically closed field of characteristic $p > 2$, complete with respect to an absolute value. Let $f \in \mathcal{M}_k$ be non-constant. Let $F_1, \dots, F_\ell \in k[X]$ be coprime polynomials of degree d without repeated factors. If $F_j(f)$ is a square for each $1 \leq j \leq \ell$, then $\ell \leq 4/d$.*

Proof. We can assume that f is not a p-th power by the Frobenius trick. Let $q_1, \dots q_n$ ($n = \ell d$) be the roots of the polynomials F_j. The SMT gives for any $\epsilon > 0$

$$\sum_{i=1}^{n} N_f^{(1)}(q_i, r). \geq .(n - 2 - \epsilon) T_f(r).$$

On the other hand, looking at the vanishing orders at points, we find

$$\sum_{i=1}^{n} N_f^{(1)}(q_i, r) = \sum_{j=1}^{\ell} N_{F_j(f)}^{(1)}(0, r) \leq \frac{1}{2} \sum_{j=1}^{\ell} N_{F_j(f)}(0, r) \leq \frac{1}{2} \sum_{j=1}^{\ell} T_{F_j(f)}(r) + O(1)$$

where we used the fact that $F_j(f)$ is a power, hence, all its zeros have multiplicity ≥ 2. Since all F_j have degree d we have $T_{F_j(f)}(r) = dT_f(r) + O(1)$, therefore

$$(d\ell - 2 - \epsilon) T_f(r). \leq . \frac{d\ell}{2} T_f(r) + O(1)$$

and the result follows, because $T_f(r) \gg \log r$ as f is non-constant. □

Now we can prove the transcendental counterpart of Theorem 1.6.

Proof of Theorem 1.4. It suffices to prove the result after k is replaced by a larger valued field whose absolute value extends that of k, so we can assume that k is algebraically closed and complete. After the same initial reductions as in the proof of Theorem 1.6, we can assume that f, g are not p-th powers, and it suffices to prove that $f = g$.

Now we cannot simply choose f or g having the "largest degree"; nevertheless, there is a set $X \subseteq \mathbb{R}_{\geq 0}$ of infinite Lebesgue measure such that $T_f(r) \geq T_g(r)$ (say) for every $r \in X$.

We define S_j as the set of roots of F_j, and we let $q_1, \ldots, q_N$ be the elements of $\cup_{i=1}^{M} S_i$ (so that $N = dM$). Let P be the analytic divisor of poles of f and g, and let

$$A = \{x \in k : (f(x), g(x)) \in S_j \times S_j \text{ for some } 1 \leq j \leq N\}$$

which defines an analytic divisor (also denoted by A). Let $B = (A + P)^{red}$, which plays the role of the union of the underlying sets of A and P. Instead of the bound (2.2), the SMT gives for any fixed $\epsilon > 0$

$$\sum_{j=1}^{N} N_f^{(1)}(q_j, r). \geq .(N - 2 - \epsilon) T_f(r).$$

A computation as in the proof of Theorem 1.6 shows the following inequalitiy of analytic divisors (with $\mathbb{Q}$-coefficients) on $\mathbb{A}_k^1$ (meaning pointwise inequalities of coefficients):

$$\sum_{j=1}^{N} (f^* q_j)^{red} \leq A + P + \frac{1}{2} \sum_{j=1}^{N} f^* q_j$$

Taking counting functions and using Lemma 4.1 this yields

$$\begin{aligned}\sum_{j=1}^{N} N_f^{(1)}(q_j,r) &\leq N(A,r)+N(P,r)+\frac{1}{2}\sum_{j=1}^{N} N_f(q_j,r)\\ &\leq \left(2+4\sum_{j=1}^{\lceil (d-1)/2\rceil} p^j\right)\max\{T_f(r),T_g(r)\}+O(1)+N(P,r)\\ &\quad+\frac{1}{2}\sum_{j=1}^{N} T_f(q_j,r)\\ &= \left(2+4\sum_{j=1}^{\lceil (d-1)/2\rceil} p^j\right)\max\{T_f(r),T_g(r)\}+N(P,r)\\ &\quad+\frac{N}{2}T_f(r)+O(1)\end{aligned}$$

where we used the FMT. Moreover, note that $N(P,r)\leq T_f(r)+T_g(r)\leq_X 2T_f(r)$ where $\leq_X$ means that the inequality occurs for every $r\in X$. Therefore, after possibly deleting a finite measure set from X, we get

$$(N-2-\epsilon)T_f(r)\leq_X \left(\frac{N}{2}+4+4\sum_{j=1}^{\lceil (d-1)/2\rceil} p^j\right)T_f(r)+O(1).$$

As f is non-constant $T_f(r)$ grows to infinity on X (in fact, $T_f(r)\gg \log r$) so, taking ϵ very small we deduce

$$dM=N\leq 12+8\sum_{j=1}^{\lceil (d-1)/2\rceil} p^j.$$

□

Proof of Theorem 1.1. Using Theorem 1.4 instead of Theorem 1.6, the proof is the same as the proof of Theorem 1.5 given in Section 2.

(Note that this claim strongly uses the fact that the uniformity argument given at the end of the proof of Theorem 1.5 was independent of the existing results on Büchi's problem, see Remark 2 for details.) □

5. Undecidability consequences

Now that we have proved our results concerning definability of the relation $\geq_p$, we use them in this section to derive undecidability results.

First we prove Theorem 1.2. For this, we recall the following result of J. Robinson [19]:

Theorem 5.1. *Let S be the successor function on $\mathbb{N}$ and let $|$ be the divisibility relation. Multiplication is first order definable in $(\mathbb{N};0,S,|,=)$.*

Therefore, to prove the first part of Theorem 1.2 it suffices to interpret the structure $(\mathbb{N};0,S,|,=)$ in the L_t-structure $(\mathcal{M}_k;0,1,z,+,\times,=)$. For interpretations, we

will follow the same conventions as used in [7] to simplify the exposition. The interpretation will occur through the function

$$\theta : T := \{t^{p^n} : n \geq 0\} \to \mathbb{N}; \quad \theta(f) = v_p(\deg(f))$$

which is bijective. The set T is L_t-definable because $T = \{f : f \geq_p t\}$ and thanks to Theorem 1.1. Note also that $\theta^* 0 = \{t\}$ is L_t-definable and the pull-back of the equality relation is L_t-definable too.

The set $\theta^* S$ is L_t-definable because

$$S\theta(f) = \theta(g) \text{ if and only if } f, g \in T \wedge g = f^p$$

(using multiplication p times). For the set $\theta^*|$ we need

Lemma 5.2. *The ternary relation $R = \{(z^{p^n}, x, x^{p^n}) : x \in \mathcal{M}_k^*, n \geq 0\}$ is L_t-definable.*

Proof. In fact, $(f, x, y) \in R$ if and only if

$$x \neq 0 \wedge (f \geq_p z) \wedge (y \geq_p x) \wedge (yf \geq_p xz) \wedge ((f+1)y \geq_p (z+1)x).$$

Verifying the equivalence is easy in the case that x (hence, y) has a zero or pole away from 0 (after possibly extending k). In $\mathcal{M}_k$ the only functions without zeros or poles over a complete, algebraically closed extension of k are the non-zero constants (because k is non-archimedean) and for x constant the result is also clear. So we can assume that $x = az^m$ with $m \neq 0$. At this point, the equivalence follows from examining the clause $(f+1)y \geq_p (z+1)x$. □

Recall the simple arithmetic fact that $m|n$ if and only if $p^m - 1 | p^n - 1$. Using this and the previous lemma, we see that $\theta^*|$ is L_t-definable because

$$\theta(f)|\theta(g) \text{ if and only if } f, g \in T \wedge \exists x, y \in \mathcal{M}_k,\ (f, x, y) \in R \wedge y/x = g/z.$$

Therefore we conclude that $(\mathbb{N}; 0, S, |, =)$ is interpretable in $(\mathcal{M}_k; 0, 1, z, +, \times, =)$, proving the first part of Theorem 1.2.

The second part of Theorem 1.2 is proved in exactly the same way as in Section 5 of [4], by interpreting a suitable consistent extension of Raphael Robinson's Q-theory. For the convenience of the reader, let us recall the argument here.

Recall that Raphael Robinson [20] constructed a finitely axiomatizable and essentially undecidable theory in the language $L_Q = \{0, S, +, \times, =\}$, of which $\mathbb{N} = \{0, 1, 2, \ldots\}$ is a model. This theory is traditionally denoted by Q. Let us observe that by the previous work in this section, for all fields k as in this section we have a syntactic algorithm A_k that takes L_Q-formulas into L_t formulas, with the property that for an L_Q-sentence F one has $\mathbb{N} \models F$ if and only if $\mathcal{M}_k \models A_k(F)$ (this is a standard fact; the algorithm basically consists of replacing the symbols of L_Q by the definitions of their interpretations in $\mathcal{M}_k$).

Let T be a new variable, and given an L_Q-sentence F we define an $\{0, 1, +, \times, =\}$-formula $F'[T]$ with free variable T by replacing in $A_k(F)$ al the occurrences of the constant t by the variable T.

Let C be the conjunction of all the (finitely many) axioms of Q. Let us define the L_Q-theory $\mathcal{T}_k$ as the collection of all L_Q-formulas F satisfying that

$$\mathcal{M}_k \models \forall T(C'[T] \to F'[T]).$$

We observe that all axioms of Q are in $\mathcal{T}_k$ and that $\mathcal{T}_k$ is closed under proofs. Moreover, $\mathcal{T}_k$ is consistent: for otherwise, there is an L_Q-statement F such that

both F and $\neg F$ are in $\mathcal{T}_k$. In particular (specializing to $T = t$) we have both $\mathcal{M}_k \models A_k(C) \to A_k(F) \equiv A_k(C \to F)$ and $\mathcal{M}_k \models A_k(C \to \neg F)$. This means that $\mathbb{N} \models C \to F$ and $\mathbb{N} \models C \to \neg F$, and since $\mathbb{N}$ is a model for the Q-theory, we deduce that $\mathbb{N} \models F \wedge \neg F$; a contradiction.

Hence, we have that $\mathcal{T}_k$ is a consistent extension of the Q-theory, and therefore it is undecidable. It follows that the first order theory of $\mathcal{M}_k$ in the language of rings $\{0, 1, +, \times, =\}$ is undecidable, for otherwise we could decide satisfaction sentences of the form $\forall T(C'[T] \to F'[T])$ on $\mathcal{M}_k$, and thus we could decide membership of L_Q-sentences to $\mathcal{T}_k$. This proves Theorem 1.2.

Finally, we prove Theorem 1.3. We begin by observing that the same argument from p.7 of Pheidas' paper [16] gives a positive existential interpretation of the structure $(\mathbb{N}; 0, 1, +, \times, =)$ in

$$(\mathcal{M}_k; 0, 1, z, +, \times, V, \leq_p, =).$$

By Theorem 1.1, the relation $\leq_p$ can be dropped from the language because it is positive existentially definable in terms of the other symbols (in fact, V is not used here), so we obtain that $(\mathbb{N}; 0, 1, +, \times, =)$ is positive existentially interpretable in $(\mathcal{M}_k; 0, 1, z, +, \times, V, =)$.

It only remains to recall that, by the solution to the original Hilbert's tenth problem given by Matiyasevich after the work of Davis, Putnam and Robinson (see [11]), we know that the positive existential theory of the semi-ring $(\mathbb{N}; 0, 1, +, \times, =)$ is undecidable. Thus, the positive existential theory of $(\mathcal{M}_k; 0, 1, z, +, \times, V, =)$ is also undecidable. This concludes the proof of Theorem 1.3.

6. Meromorphic functions in characteristic zero

In this section we prove Theorem 1.7. The proof is a straightforward modification of the arguments in previous sections, but there is one point that needs to be addressed in a different way, so we will give details.

The only relevant difference with the arguments in Section 2 and 4 consists of the choice of the divisor E passing through all the points in Ω. Instead of using graphs of iterates of the Frobenius map, here we use a standard (and elementary) construction from algebraic combinatorics to obtain a polynomial of low degree vanishing at every point in a prescribed finite set. Despite the fact that the result is very elementary, it has found striking applications such as the proof of the finite field Kakeya conjecture [3], see also Lemma 1.4 and its applications in [25]. We state it in dimension 2 just for simplicity.

Lemma 6.1 (Auxiliary polynomial)**.** *Let L be a field and let $\Omega \subseteq L \times L$ be a finite set. There is a non-zero polynomial $P(X, Y) \in k[X, Y]$ of degree $\leq \sqrt{2 \cdot \#\Omega}$ which vanishes at each point of Ω.*

Proof. Let V_D be the space of bivariate polynomials of degree $\leq D$; it has dimension $\binom{D+2}{2}$. Consider the linear map $e_{\Omega,D} : V_D \to L^{\#\Omega}$ taking a polynomial Q to the tuple of its values at the points in Ω. The result follows by comparing dimensions, forcing $e_{\Omega,D}$ to have non-trivial kernel. □

Lemma 6.2. *Let $\Omega \subseteq k^2$ be a finite subset. There is a non-zero polynomial $P(X, Y) \in k[X, Y]$ of degree $\leq \sqrt{2 \cdot \#\Omega}$ with the following property:*

Let $f, g \in \mathcal{M}_k$ be distinct elements, at least one of them non-constant. Consider the set

$$A = \{x \in k : (f(x), g(x)) \in \Omega\}.$$

If $P(f, g)$ is not identically zero, then the formal sum of the elements of A is an analytic divisor (which we also denote by A) and it satisfies

$$N(A, r) \leq 2\sqrt{2 \cdot \#\Omega} \max\{T_f(r), T_g(r)\} + O(1).$$

Proof. The proof is similar to the proof of Lemmas 2.1 and 4.1. The polynomial P is obtained from Lemma 6.1, and in this context the divisor E on $\mathbb{P}^2_k$ is not constructed using graphs of Frobenius maps, but instead we define it as the zero divisor of (the homogenization of) P. As long as the image of $F = [1 : f : g]$ is not contained on E, we can use the FMT and Lemma 3.3 as in the proof of Lemma 4.1, giving the result. □

Lemma 6.3. *Suppose that k is an algebraically closed field of characteristic 0, complete with respect to an absolute value. Let $f \in \mathcal{M}_k$ be non-constant. Let $F_1, \dots, F_\ell \in k[X]$ be coprime polynomials of degree d without repeated factors. If $F_j(f)$ is a power for each $1 \leq j \leq \ell$, then $\ell \leq 4/d$.*

Proof. The proof is the same as for Lemma 4.2, except for the fact that here we use power values instead of squares (we don't need to use the Frobenius trick, so there is no need to work with square values). □

Proof of Theorem 1.7. By Lemma 6.3 we can assume that both f and g are non-constant (in particular, none of $F_j(f)$ and $G_j(g)$ is identically zero). Let S_j and T_j be the zero sets of F_j and G_j respectively, so that all the S_j are disjoint and all the T_j are disjoint. Define

$$\Omega = \bigcup_{j=1}^{M} S_j \times T_j.$$

This set has d^2M elements, and the polynomial P afforded by Lemma 6.2 has degree $\leq \sqrt{2 \cdot \#\Omega} = d\sqrt{2M}$. Define

$$A = \{x \in k : (f(x), g(x)) \in \Omega\}$$

and observe that Lemma 6.2 gives that

$$N(A, r) \leq 2d\sqrt{2M} \max\{T_f(r), T_g(r)\} + O(1)$$

provided that $P(f, g)$ is not identically zero, which we assume from now on. Let $\mathcal{P}$ be the analytic divisor of the poles of f and g, then $N(\mathcal{P}, r) \leq 2 \max\{T_f(r), T_g(r)\}$.

Without loss of generality we can assume that there is a set $X \subseteq \mathbb{R}_{\geq 0}$ of infinite measure with $T_f(r) \geq T_f(g)$ for all $r \in X$, and let us label by q_j $(1 \leq j \leq N := dM)$ the elements of $\cup_{j=1}^{M} S_j$. The same computations as in the proof of Theorem 1.4 now give

$$\sum_{j=1}^{N} N_f^{(1)}(q_j, r) \leq_X \left(2d\sqrt{2M} + 2 + \frac{N}{2}\right) T_f(r) + O(1).$$

(Here we used the hypothesis of $F_j(f)G_j(g)$ being a power, so that it only has multiple zeros.) Putting this together with the SMT (and possibly deleting a finite

measure set from X) shows for any given $\epsilon > 0$

$$(N - 2 - \epsilon)T_f(r) \leq_X \left(2d\sqrt{2M} + 2 + \frac{N}{2}\right) T_f(r).$$

Letting $r \to \infty$ on X and recalling that $N = dM$, we deduce

$$M \leq \frac{8}{d} + 4\sqrt{2M}.$$

The result follows. □

7. A number field analogue

As an application of Vojta's analogy between Nevanlinna theory and diophantine approximation, in this section we give a number theoretical analogue of Theorem 1.7. Since we used the SMT with *truncated* counting functions for analytic maps $\mathbb{A}^1 \to \mathbb{P}^1$, this analogue will be conditional on the *abc* conjecture for number fields, which we recall below.

First, let us introduce the relevant notation. Let L be a number field with set of places $M_L = M_L^0 \cup M_L^\infty$ where the exponent 0 (resp. ∞) denotes the non-archimedean (resp. archimedean) places. For $v \in M_L^\infty$ let ϵ_v be 1 or 2 according to whether v is real or not, and $|-|_v$ will denote the absolute value associated to v. For $\mathfrak{p}$ a non-zero prime ideal in $\mathcal{O}_L$ we write $N\mathfrak{p}$ for the norm of $\mathfrak{p}$, and $v_\mathfrak{p}$ for the valuation at $\mathfrak{p}$. Let S be a finite set of places containing M_L^∞. For $\alpha \in L^*$ we define the counting function

$$N_S(\alpha) = \frac{1}{[L:\mathbb{Q}]} \sum_{\mathfrak{p} \in M_L^0 \smallsetminus S} v_\mathfrak{p}^+(\alpha) \log N\mathfrak{p}.$$

It is also convenient to define the truncated counting function

$$N_S^{(1)}(\alpha) = \frac{1}{[L:\mathbb{Q}]} \sum_{\mathfrak{p} \in M_L^0 \smallsetminus S} \min\{1, v_\mathfrak{p}^+(\alpha)\} \log N\mathfrak{p}.$$

The proximity function is

$$m_S(\alpha) = \frac{1}{[L:\mathbb{Q}]} \left(\sum_{\mathfrak{p} \in S \cap M_L^0} v_\mathfrak{p}^+(\alpha) \log N\mathfrak{p} + \sum_{v \in M_L^\infty} \epsilon_v \log |\alpha|_v \right)$$

The (logarithmic, normalized) *height* of $\alpha \in L^*$ is defined as

$$h(\alpha) = N_S(\alpha) + m_S(\alpha)$$

and it is independent of S and independent of L (as long as L contains α) thanks to the normalization $1/[L:\mathbb{Q}]$. We will be using basic properties of heights without explicit reference.

The *abc* conjecture for the number field L can be formulated as follows.

Conjecture 1. *Let $\epsilon > 0$ and let $b_1, \ldots, b_M \in L$ be distinct. For all but finitely many $\alpha \in L$ we have*

$$(M - 2 - \epsilon)h(\alpha) < \sum_{j=1}^{M} N_S^{(1)}(\alpha - b_j).$$

We remark that the particular case $M = 3$ is equivalent to the general case, thanks to an argument of Elkies [6] using Belyi maps. When $L = \mathbb{Q}$ and $M = 3$ we recover the traditional *abc* conjecture of Masser and Oesterle, after possibly applying a Möbius transformation to move b_1, b_2, b_3 to $0, 1, \infty$.

Also, note that this conjecture is about diophantine approximation in dimension 1 over one fixed number field, as opposed to other more general conjectures of Vojta involving diophantine approximation over higher dimensional varieties, and for algebraic points of bounded degree.

Translating the proof of Theorem 1.7 to the number field setting, one gets:

Theorem 7.1. *Let K be a number field. Let d be a positive integer and let M be an integer satisfying*

$$M > 8\left(1+\sqrt{1+\frac{1}{d}}\right)^2$$

(in particular, $M = 47$ is admissible for all d). Let $F_1, \dots, F_M$ and $G_1, \dots, G_M$ be elements of $K[X]$ of degree d, without repeated factors and with the property that the F_j are pairwise coprime, and similarly the G_j are pairwise coprime. Let L be a number field containing the roots of all the polynomials F_j and G_j and assume that the abc conjecture holds for L. There is a non-zero polynomial $P(X, Y) \in K[X, Y]$ of degree $\leq [L : K]d\sqrt{2M}$ such that for all but finitely many $\alpha, \beta \in K$, if $F_j(\alpha)G_j(\beta)$ is a non-zero power in K for all $1 \leq j \leq M$ then $P(\alpha, \beta) = 0$.

Remark 3. *The condition "$F_j(\alpha)G_j(\beta)$ is a non-zero power in K" can be relaxed to "$F_j(\alpha)G_j(\beta)$ is a power in K" in two ways: either by allowing P to have larger degree and replacing it by $P\prod_j(F_j(X)G_j(Y))$ (this is the trivial fix), or by proving an analogue of Lemmas 2.2, 4.2 and 6.3 under the abc conjecture (non-trivial fix, but still straightforward). In the application given in the next section the trivial fix suffices.*

We keep the notation from the theorem for the rest of this section.

Lemma 7.2. *Let $\Omega \subseteq L^2$ be a finite subset. For $(a, b) \in L^2$ and $\mathfrak{p} \in M_L^0$ define $\delta_{\mathfrak{p},\Omega}(a, b)$ as 1 if a, b and every element of Ω has non-negative valuation at $\mathfrak{p}$, and moreover (a, b) reduces to an element in Ω modulo $\mathfrak{p}$, and define $\delta_{\mathfrak{p},\Omega}(a, b) = 0$ otherwise.*

There is a non-zero polynomial $Q(X, Y) \in L[X, Y]$ of degree $\leq \sqrt{2 \cdot \#\Omega}$ with the following property:

For $(a, b) \in L^2$ with $Q(a, b) \neq 0$, we have

$$\sum_{\mathfrak{p}\in M_L^0} \delta_{\mathfrak{p},\Omega}(a, b) \log N\mathfrak{p} \leq 2\sqrt{2 \cdot \#\Omega}\max\{h(a), h(b)\} + O_\Omega(1)$$

as (a, b) varies.

Proof. The polynomial Q is obtained from Lemma 6.1, which is valid for any field. The rest of the proof proceeds in exactly the same way as in Lemmas 2.1, 4.1 and 6.2 using heights in $\mathbb{P}^2_L(L)$ applied to the points $[1 : a : b]$, and invoking the linear equivalence property of heights. One needs an analogue of the bound (2.1) and Lemma 3.3, which is straightforward from the definition of height in projective spaces in terms of valuations.

The error term is affected by the choice of polynomial Q and by the places where elements of Ω have poles or reduce to the same residue class, hence, the error term depends only on Ω. □

Proof of Theorem 7.1. We will replace K by L and do diophantine approximation on L. This is possible since the powers in K remain as powers in L; the polynomial $P \in K[X,Y]$ in the statement will be the product of the Galois conjugates of the polynomial $Q \in L[X,Y]$ that the previous lemma will produce for us.

Let $S_j, T_j \subseteq L$ be the sets of roots of F_j, G_j respectively. Define

$$\Omega = \bigcup_{j=1}^{M} S_j \times T_j \subseteq L^2.$$

The proof of the theorem follows the same idea and computations as in the proof of Theorem 1.7, except for the minor inconvenience that now the elements of Ω can have poles, and can take the same value at some primes $\mathfrak{p} \in M_L^0$. This is controlled by letting S be the set of these bad places, together with the places at infinity, and considering counting functions N_S and $N_S^{(1)}$ relative to primes in the complement of S, as defined above. We give below the relevant details specific to the number field case.

The computations are performed for (a,b) *varying*[3] in L^2 under the condition $Q(a,b) \neq 0$.

If the conclusion of the theorem fails, then we can take an infinite sequence of counterexamples (a_n, b_n) with $Q(a_n, b_n) \neq 0$, and satisfying that $F_j(a_n)G_j(b_n)$ is a power for each $1 \leq j \leq M$. Without loss of generality we can also assume that $h(a_n) \geq h(b_n)$ in this sequence (passing to a sub-sequence if necessary – this is the analogue of our previous use of $\leq_X$). Let q_i $(1 \leq i \leq N := dM)$ be the elements of $\cup_{j=1}^{M} S_j$. By the same valuation-theoretical computations that we have done before and using the hypothesis that $F_j(a_n)G_j(b_n)$ are non-zero powers, we obtain

$$\sum_{i=1}^{N} N_S^{(1)}(a_n - q_i) \leq \left(2d\sqrt{2M} + 2 + \frac{N}{2}\right) h(a_n) + O_\Omega(1)$$

where the error term is independent of n.

Take $\epsilon > 0$. After possibly discarding finitely many a_n (depending on ϵ), the *abc* conjecture for L gives

$$(N - 2 - \epsilon)h(a_n) \leq \sum_{i=1}^{N} N_S^{(1)}(a_n - q_j)$$

hence

$$(N - 2 - \epsilon)h(a_n) \leq \left(2d\sqrt{2M} + 2 + \frac{N}{2}\right) h(a_n) + O_\Omega(1).$$

This means

$$\left(dM - 8 - 4d\sqrt{2M} - 2\epsilon\right) h(a_n) \leq O_\Omega(1)$$

and by our condition on M, this means that if ϵ is sufficiently small (depending only on d and M, not on n) one has

$$h(a_n) \leq O_{d,M,\Omega}(1).$$

[3]Let us recall that in Vojta's analogy, what corresponds to a single analytic map to a variety X is an infinite set of rational points of X (as opposed to a single rational point).

Thus the heights of the elements of the sequence a_n are bounded. This sequence is in the number field L, so the Northcott theorem (finiteness property of heights) gives that the sequence is finite, a contradiction. □

8. Application: The Erdös-Ulam problem

In 1945, Anning and Erdös [1] proved that any infinite set of points in the real plane satisfying that all pairwise (euclidean) distances between them are integers, must be contained in a line. The same year, Stanislaw Ulam considered sets with *rational* distances, and asked the following:

Problem 8.1 (Erdös-Ulam Problem)**.** *Is there a topologically dense subset of points U in the plane satisfying that all pairwise distances between points in U are rational?*

See the first paragraph of section III.5 in [27], and see [24] for further historical remarks and some relevant partial progress on this problem.

As stated, the Erdös-Ulam problem remains open. Very recently, it has been observed by Tao [26] and by Shaffaf [21] that the Bombieri-Lang conjecture for surfaces implies a negative solution to the problem, and no such set U can exist (see also [10]). Here is the basic idea: after some initial (standard) reduction regarding the field in which the elements of U have their coordinates, the condition that a point $P \in U$ has rational euclidean distances to a fixed finite set of points $F \subseteq U$, gives rise to a system of quadratic equations defining a surface X_F (depending only on F, over a number field L_F depending only on F), and each such P produces an L_F-rational point in X_F. Then one verifies that X_F is of general type so that the Bombieri-Lang conjecture implies that, up to finitely many cases, P is restricted to belong to some (possibly reducible) algebraic curve, and the result follows. Let us point out that Shaffaf and Tao consider slightly different surfaces X_F, but in both cases the idea is the same.

Our Theorem 7.1, which naturally followed from our method to define the relation $\geq_p$ in meromorphic functions of positive characteristic, has the following (arguably) unexpected consequence:

Theorem 8.1. *The abc conjecture for number fields implies a negative solution to the Erdös-Ulam problem. Moreover, under the abc conjecture for number fields, any infinite set $U \subseteq \mathbb{R}^2$ with rational distances between each pair of elements must be algebraically degenerate: it is contained in a (possibly reducible) plane algebraic curve.*

In fact, one "only" needs the *abc* conjecture for number fields of the form $K(i)$ with $i = \sqrt{-1}$ and K real quadratic. Another relevant aspect of our proof is that the *abc* conjecture that we are using is about rational approximation in *dimension* 1, while the Erdös-Ulam problem seems to be a problem in dimension 2 (for instance, the Shaffaf-Tao result relates the problem to the Bombieri-Lang conjecture for *surfaces*).

Proof of Theorem 8.1. Let $U \subseteq \mathbb{R}^2$ be an infinite set such that every pair of points in U has euclidean distance in $\mathbb{Q}$. Suppose that U is not algebraically degenerate, then we will reach a contradiction under the *abc* conjecture.

It is well-known (see for instance Lemma 3.4 in [24], apparently due to Kemnitz) that one can assume with no loss of generality (namely, after rotation, dilation and translation in $\mathbb{R}^2$ preserving rationality of distances, and preserving algebraic

(non-)degeneracy of sets) that there is a real quadratic number field K such that all the points in U have coordinates in K.

As U is not algebraically degenerate, we can take points $P_j = (x_j, y_j) \in U \subseteq K^2$ for $j = 1, \ldots, 47$ such that all the x_j are distinct, and all the y_j are distinct. Consider the number field $L = K(i)$ (with $i^2 = -1$) and in L we take the elements $a_j = x_j + iy_j$, $b_j = x_j - iy_j$ for $1 \leq j \leq 47$. Then all the a_j are distinct and all the b_j are distinct. More generally, for each $P = (x_P, y_P) \in U$ we define $a_P = x_P + iy_P$, $b_P = x_P - iy_P$ and note that they are in L.

For $1 \leq j \leq 47$ we consider the polynomials $F_j(X) = X - a_j$ and $G_j(Y) = Y - b_j$; (trivially) these have all their roots in L. We claim that for all $P \in U$ we have that $F_j(a_P)G_j(b_P)$ is a square in L for each $1 \leq j \leq 47$. In fact,

$$\begin{aligned} F_j(a_P)G_j(b_P) &= (x_P - x_j + i(y_P - y_j))(x_P - x_j - i(y_P - y_j)) \\ &= (x_P - x_j)^2 + (y_P - y_j)^2 = \|P - P_j\|^2 \end{aligned}$$

which is a square in $\mathbb{Q}$, hence in L. Therefore, under the *abc* conjecture for the number field L, Theorem 7.1 (with $K = L$, $d = 1$, $M = 47$ and recalling Remark 3) gives that there is a non-zero polynomial $P(X, Y) \in L[X, Y]$ with $P(a_P, b_P) = 0$ for all but finitely many $P \in U$. This means that all but finitely many points in U are contained in the zero set of

$$Q(X, Y) = P(X + iY, X - iY) \in L[X, Y]$$

which is not the zero polynomial. This is a contradiction, thus proving the theorem. □

Finally, let us observe that the previous result together with the theorems of [24] yield the following more precise description of infinite rational distance sets.

Corollary 8.2. *Under the abc conjecture for number fields, any infinite set $U \subseteq \mathbb{R}^2$ with rational distances between each pair of elements must be of one of the following forms:*

- *all but at most 4 points of U are on a line, or*
- *all but at most 3 points of U are on a circle.*

(Both cases can occur.)

9. Acknowledgments

I thank Alexandra Shlapentokh for some useful references and Julie T.-Y. Wang for comments and corrections on an earlier version of this manuscript. I am indebted to Xavier Vidaux for several suggestions that improved the presentation of this paper, and to Pierre Deligne for asking some questions that led me to include Theorem 1.3 and other improvements. Also, I heartily thank the referee for providing valuable feedback and corrections.

This work originated as an attempt to present a simplified proof of Pheidas theorem form [16] in the graduate course *Diophantine Definability* (Math 259) taught at Harvard during the Spring term of 2015. I thank the Mathematics Department at Harvard for giving me the opportunity to teach this course.

References

[1] N. Anning, P. Erdös, *Integral distances*. Bull. Amer. Math. Soc. 51, (1945). 598-600.

[2] W. Cherry, *Lecture notes on non-Archimedean function theory*, Advanced school on p-adic analysis and applications, The Abdus Salam International Centre for Theoretical Physics, Trieste, Italy (2009). Preprint, available at http://arxiv.org/pdf/0909.4509.pdf

[3] Z. Dvir, *On the size of Kakeya sets in finite fields*. J. Amer. Math. Soc. 22 (2009), 1093-1097.

[4] K. Eisenträger, A. Shlapentokh, *Undecidability in function fields of positive characteristic*. Int. Math. Res. Not. IMRN 2009, no. 21, 4051-4086.

[5] K. Eisenträger, A. Shlapentokh, *Hilbert's tenth problem over function fields of positive characteristic not containing the algebraic closure of a finite field*. To appear in Journal of the European Math. Soc. (2015)

[6] N. Elkies, *ABC implies Mordell*. Internat. Math. Res. Notices 1991, no. 7, 99-109.

[7] N. Garcia-Fritz, H. Pasten, *Uniform positive existential interpretation of the integers in rings of entire functions of positive characteristic*. J. Number Theory 156 (2015), 368-393.

[8] P. C. Hu, C.-C. Yang, *Value distribution theory related to number theory*. Birkhauser Verlag, Basel, 2006. xii+543 pp. ISBN: 978-3-7643-7568-3; 3-7643-7568-X

[9] L. Lipshitz, T. Pheidas, *An analogue of Hilbert's tenth problem for p-adic entire functions*. J. Symbolic Logic 60 (1995), no. 4, 1301-1309.

[10] M. Makhul, J. Shaffaf, *On uniform boundedness of a rational distance set in the plane*. (English, French summary) C. R. Math. Acad. Sci. Paris 350 (2012), no. 3-4, 121-124.

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

[12] H. Pasten, *Representation of squares by monic second degree polynomials in the field of p-adic meromorphic functions*. Trans. Amer. Math. Soc. 364 (2012), no. 1, 417-446.

[13] H. Pasten, *Powerful values of polynomials and a conjecture of Vojta*. J. Number Theory 133 (2013), no. 9, 2964-2998.

[14] H. Pasten, T. Pheidas, X. Vidaux, *Uniform existential interpretation of arithmetic in rings of functions of positive characteristic*. Inventiones Mathematicae 196 (2014), no. 2, 453-484.

[15] H. Pasten, J. Wang, *Extensions of Büchi's higher powers problem to positive characteristic*, to appear in IMRN (2014).

[16] T. Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*. Invent. Math. 103 (1991), no. 1, 1-8.

[17] T. Pheidas, X. Vidaux, *Corrigendum: The analogue of Büchi's problem for rational functions*. J. Lond. Math. Soc. (2) 82 (2010), no. 1, 273-278.

[18] T. Pheidas, K. Zahidi, *Undecidability of existential theories of rings and fields: a survey*. Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 49-105, Contemp. Math., 270, Amer. Math. Soc., Providence, RI, 2000.

[19] J. Robinson, *Definability and decision problems in arithmetic*. J. Symbolic Logic 14, (1949). 98-114.

[20] R. Robison, *An essentially undecidable axiom system*. Proceedins of the ICM (1950) 729-730.

[21] J. Shaffaf, *A proof of the Erd'os-Ulam problem assuming Bombieri-Lang conjecture*. Preprint available at http://arxiv.org/pdf/1501.00159.pdf

[22] A. Shlapentokh, *Diophantine relations between rings of S-integers of fields of algebraic functions in one variable over constant fields of positive characteristic*. J. Symbolic Logic 58 (1993), no. 1, 158-192.

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

[24] J. Solymosi, F. de Zeeuw, *On a question of Erdös and Ulam*. Discrete Comput. Geom. 43 (2010), no. 2, 393-401.

[25] T. Tao, *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*. EMS Surveys in Mathematical Sciences (2014) 1(1), 1-46.

[26] T. Tao, *The Erdös-Ulam problem, varieties of general type, and the Bombieri-Lang conjecture*. Post (2014/12/20) in terrytao.wordpress.com

[27] S. Ulam, *A Collection of Mathematical Problems*. Interscience Tracts in Pure and Applied Mathematics, vol. 8. Interscience, New York (1960). XIII, 150 p.

[28] X. Vidaux, *An analogue of Hilbert's 10th problem for fields of meromorphic functions over non-Archimedean valued fields*. J. Number Theory 101 (2003), no. 1, 48-73.
[29] P. Vojta, *Diophantine approximation and Nevanlinna theory*, in: Arithmetic Geometry, in: Lecture Notes in Math., vol. 2009, Springer, Berlin, 2011, pp. 111-224.
[30] P. Vojta, *Diagonal quadratic forms and Hilbert's Tenth Problem*. Contemporary Mathematics 270, 261-274 (2000).
[31] J. Wang, *The truncated second main theorem of function fields*. J. Number Theory 58 (1996), no. 1, 139-157.

Department of Mathematics, Harvard University
1 Oxford Street,
Cambridge, MA 02138 USA
and
School of Mathematics, Institute for Advanced Study
1 Einstein Drive,
Princeton, NJ 08540 USA
E-mail address, H. Pasten: hpasten@math.harvard.edu