Journal of Number Theory 133 (2013) 2964–2998

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Powerful values of polynomials and a conjecture of Vojta ☆

Hector Pasten

Department of Mathematics and Statistics, Queen's University, Jeffery Hall, University ave., Kingston, ON, K7L 3N6, Canada

ARTICLE INFO

Article history:
Received 8 May 2012
Revised 20 December 2012
Accepted 27 March 2013
Available online 10 May 2013
Communicated by Dinesh S. Thakur

MSC:
primary 11D85, 11J97
secondary 11R58, 11U05

Keywords:
Squareful
Powerful numbers
Vojta's conjecture
Büchi's problem
Undecidability

ABSTRACT

We study some problems about powerful values of polynomials over number fields, such as giving uniform bounds for the number of consecutive squareful values of squarefree polynomials, or the higher exponent analogue of the M squares problem. We show that a Diophantine conjecture of Vojta implies complete answers to these problems, and we show unconditional analogues for function fields and complex meromorphic functions. Some of these results have consequences in logic related to Hilbert's tenth problem, and we also explore these.

© 2013 Elsevier Inc. All rights reserved.

Contents

☆ This work was partially supported by an Ontario Graduate Scholarship.
E-mail address: hpasten@gmail.com.

0022-314X/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jnt.2013.03.001

1. Introduction

Let $n \geqslant 2$ be an integer, and recall that an integer N is called *n-powerful* if for each prime p dividing N one has that p^n divides N (N is allowed to be negative or zero). If N is 2-powerful we just say that N is powerful; in the literature such numbers are also known as *squareful* numbers. Extending this concept, let K be a number field and let $n \geqslant 2$ be an integer. We say that $x \in K$ is *n-powerful* if for every non-zero prime $\mathfrak{p}$ in $\mathcal{O}_K$ with $\mathrm{ord}_{\mathfrak{p}}(x) > 0$ we have $\mathrm{ord}_{\mathfrak{p}}(x) \geqslant n$. If x is 2-powerful we just say that x is powerful or squareful. Observe that, if $x \in K$ is an n-th power, then it is n-powerful.

In this work we investigate powerful values of polynomials and we are mainly concerned about *uniform* bounds on the number of consecutive powerful values of a polynomial. For example, let us consider squareful values of squarefree polynomials (polynomials without repeated factors). Let $F \in \mathbb{Z}[s]$ be a squarefree polynomial of degree $n \geqslant 2$. If F is monic and $n = 2$ then F takes infinitely many squareful values at integer arguments, as proved in [34]. On the other hand, results in [34] suggest that squareful values of F should be rare when $n \geqslant 3$ (indeed, finitely many under the ABC conjecture, and even under the assumption that F has at least 3 simple roots as predicted in [28]). In either case, the distribution of squareful values of F seems to strongly depend on the particular F. However, our results provide evidence for the following:

Conjecture 1.1. *Let K be a number field. If $F \in K[s]$ is a monic squarefree polynomial of degree $n \geqslant 2$ then F cannot take squareful values at M consecutive integers, where M is some constant that may depend on n and K, but which is uniform on F.*

Let us consider a similar situation. If $F \in \mathbb{Q}[s]$ is a polynomial of degree $n \geqslant 2$ of the form $F = (s + \nu)^n$ then all the numbers $F(b)$ for $b \in \mathbb{Q}$ are n-th powers, in particular they are n-powerful. Conversely, one may ask if checking that $F(b)$ is an n-th power (or alternatively, n-powerful) for several $b \in \mathbb{Q}$ is enough to conclude that F is of the form $(s + \nu)^n$ for some $\nu \in \mathbb{Q}$. This problem has been addressed by other authors, see for example [8] and [25]. However, due to some reasons coming from logic (more precisely, trying to establish certain improvements of the unsolvability of Hilbert's tenth problem, see below) it is desirable to have a *uniform* converse; the number of such b for which one needs to check if $F(b)$ is an n-th power (or n-powerful) should not depend on F. More generally, if K is a number field one may ask

Question 1.2 (**Pow**(n, K))*. Let $n \geqslant 2$ be an integer. Is it true that there exists an integer constant $M = M(n, K)$ depending only on n and K with the following property?*

If a monic polynomial $F \in K[s]$ of degree n is such that $F(1), \ldots, F(M)$ are n-powerful then $F(s) = (s + \nu)^n$ for some $\nu \in K$.

Similar questions with K replaced by the ring of integers of a number field (in particular $\mathbb{Z}$) can also be asked, but as far as we know the current state of knowledge on such problems is very limited. One can also ask a (apparently) simpler question by replacing the condition 'n-powerful' by 'n-th power'.

A positive answer for **Pow**(n, K) (or even the simpler question for n-th powers) implies a positive answer to the following higher exponents version of *Buchi's problem* for A a number field or the ring of integers of a number field (see [20]).

Question 1.3 (**BP**(n, A))*. Let $n \geqslant 2$ be an integer. Is it true that there exists an integer constant $M = M(n, A)$ with the following property?*

Suppose that $u_1, \ldots, u_M$ is a sequence of n-th powers in A such that the n-th differences of the u_i are constant and equal to $n!$. Then there is an element $\nu \in A$ such that $u_i = (i + \nu)^n$ for $i = 1, \ldots, M$.

In this paper we show that certain conjecture by Vojta on Diophantine approximation for number field extensions of bounded degree implies a general statement on powerful values of polynomials over number fields (Theorem 2.1), which in particular allows us to give positive answers to the above problems (under Vojta's conjecture). We prove unconditional analogues of these results in the function field and meromorphic cases (see Theorem 2.4 below). In this study, the Osgood-Vojta analogy between Nevanlinna theory and Diophantine approximation played a central role, as we were first able to approach the case of functions and then we translated our results to number fields – here, one needs Vojta's conjecture as a substitute for the second main theorem with truncated counting functions for ramified coverings of $\mathbb{C}$ with bounded degree.

Let us state the conjecture of Vojta that we will use. For this we need to introduce some notation. Let $K/\mathbb{Q}$ be a number field. Let h_K be the height on $\bar{K}$ relative to K, and for $x \in \bar{K}^*$ write $N_K^{(1)}(x)$ for the truncated counting function (of zeros). If $x \in \bar{K}$ then we define $d_K(x)$ to be the logarithmic discriminant of x over K (see [31] or Section 4 below for precise definitions of h_K, $N_K^{(1)}$ and d_K).

Conjecture 1.4 *(Vojta). Let $b_1, \dots, b_q$ be distinct elements of K and let $n \geqslant 1$ be an integer. For every $\epsilon > 0$ there exists a constant C_ϵ depending on ϵ (and the previous data) such that the inequality*

$$(q - 2 - \epsilon) h_K(x) \leqslant d_K(x) + \sum_{j=1}^{q} N_K^{(1)}(b_j - x) + C_\epsilon$$

holds for all $x \in \bar{K}$ with $[K(x) : K] \leqslant n$ and $x \neq b_j$ for $1 \leqslant j \leqslant q$.

As we already mentioned, this conjecture is analogous to a result for meromorphic functions, namely, a version of the second main theorem for finite ramified coverings of $\mathbb{C}$. Also, Conjecture 1.4 can be seen as a generalization of the ABC conjecture, see [31] for further details.

Questions **Pow**(n, K) and **BP**(n, A) were the actual motivation for this manuscript. They have a history that goes back to the early seventies, which we now briefly recall.

The starting point is the following question by Büchi (see [14] and [16]), arising as an attempt to improve the negative answer to Hilbert's tenth problem given by Matiyasevic in 1970 after the work of J. Robinson, M. Davis, and H. Putnam (see [15]).

Question 1.5. *Is it true that there exists an integer constant M with the following property?*

Suppose that $u_1, \dots, u_M$ is a sequence of integer squares such that the second differences of the u_i are constant and equal to 2, that is

$$u_{i+2} - 2u_{i+1} + u_i = 2, \quad i = 1, \dots, M - 2.$$

Then there is an integer $\nu \in \mathbb{Z}$ such that $u_i = (i + \nu)^2$ for $i = 1, \dots, M$.

For example, if we take the first differences of the sequence $6^2, 23^2, 32^2, 39^2$ we obtain $493, 495, 497$ and taking differences again we get $2, 2$, but our starting sequence does not consist of squares of consecutive integers (this shows that if such M exists, then $M \geqslant 5$). The problem of answering question 1.5 is known as 'Büchi's problem' or the 'M squares problem'.

Büchi believed that $M = 5$ should work, but to the best of our knowledge this problem is still open (and no counterexample for $M = 5$ has been found). Nevertheless, Vojta [32] showed in 2000 that the Bombieri–Lang conjecture (on the locus of rational points) implies that Büchi's problem has a positive answer (for some $M \geqslant 8$). Furthermore, Vojta's conditional result also applies to the analogue of question 1.5 over number fields.

We refer the reader to [20] for a survey on the literature related to this problem and analogues of it over different structures.

The generalization of Büchi's problem stated above (question **BP**(n, A)) is due to Pheidas and Vidaux, see [21] where consequences in Logic are studied.

Observe that $\mathbf{BP}(2,\mathbb{Z})$ is nothing but Büchi's question 1.5 and one expects this to have a positive answer, as suggested by the work of Vojta mentioned above and by extensive numerical evidence (see [1,4,5,24,30]). However, when $n>2$ there is no evidence towards a positive or negative answer to $\mathbf{BP}(n,\mathbb{Z})$ other than analogies with function fields and meromorphic functions, where some results are known (see [19,2] and the discussion after Corollary 2.11 below). Thus our positive answer to $\mathbf{Pow}(n,K)$ (and hence $\mathbf{BP}(n,A)$) under Vojta's conjecture can be seen as the first arithmetic evidence towards a positive answer to $\mathbf{BP}(n,\mathbb{Z})$ for general n.

Going back to Büchi's original motivation for question 1.5, one may ask if the generalizations and analogues addressed in this work have consequences in Logic. This is indeed the case. Roughly speaking, when one solves an analogue or generalization of Büchi's problem for some 'reasonable' ring A, then one is able to define multiplication in A in a positive existential way over a language $\mathcal{L}$ related to the arithmetic of A but *without multiplication*. If, moreover, some analogue of Hilbert's tenth problem is known to be unsolvable for A (over a suitable language) then this leads to an undecidability result for the positive existential theory of A over $\mathcal{L}$. We explore these consequences for function fields, meromorphic functions and number fields making use of the corresponding analogues to question $\mathbf{Pow}(n,K)$ that we study in each case.

Throughout the paper we only consider powerful values of *monic* polynomials. For applications in logic this is enough, but it would be interesting to consider non-monic polynomials under reasonable hypothesis (such as no common factor among all coefficients). The techniques introduced in this work should have something to say in the general case, but it is not clear to the author if one would still have uniform results.

2. Main results

Let us first state our main result in the case of number fields.

Theorem 2.1. *Assume Conjecture 1.4. Let K be a number field and let $n\geqslant 2$ and $2\leqslant\mu\leqslant n$ be integers. Define*

$$M=\begin{cases}2n^2+9n+1 & \text{if } \mu=n,\\ 2\mu n^2+(2\mu+1)n+1 & \text{in general}\end{cases}$$

in the sense that if we do not assume $\mu=n$ then we use the second value for M. Let $b_1,\dots,b_M\in K$ be distinct. Define E as the set of monic polynomials $F\in K[s]$ of degree n such that all irreducible factors of F have multiplicity strictly less than μ, and such that for each $1\leqslant k\leqslant M$ the number $F(b_k)$ is μ-powerful. Then E is finite.

Theorem 2.1 will be proved in Section 4. We think about E as the set of exceptions to the rule 'if F takes powerful values too many times then F has factors with high exponents'. However, if we restrict our attention to the case $b_k=k$ in Theorem 2.1 then we can get rid of the set E obtaining:

Corollary 2.2. *Assume Conjecture 1.4. Let K be a number field and let $n\geqslant 2$. There is an integer constant M_0 depending only on n and K such that the following holds:*

Let $F\in K[s]$ be a monic polynomial of degree n such that the numbers $F(1),\dots,F(M_0)$ are μ-powerful for some integer $2\leqslant\mu\leqslant n$. Then F has a factor with exponent at least μ.

Proof. It is enough to show that there is such an M_0 depending only on K, n and μ (because $2\leqslant\mu\leqslant n$ so once n is fixed we have only finitely many possible μ). Thus, fix K, n and μ with $2\leqslant\mu\leqslant n$. In the notation of Theorem 2.1 put $b_k=k$ for $1\leqslant k\leqslant M$. Note that if $F\in E$ and $F(1),\dots,F(M+r)$ are μ-powerful then $F_j(s):=F(s+j)\in E$ for each $0\leqslant j\leqslant r$. As E is finite and its cardinality only depends on K, n and μ we conclude that there is some constant $M_0\geqslant M$ depending only on K, n and μ such that if $F\in E$ then some of the numbers $F(1),\dots,F(M_0)$ is not μ-powerful. Thus, if $F\in K[s]$ is a monic polynomial of degree n such that the numbers $F(1),\dots,F(M_0)$ are μ-powerful then F cannot be in E, which implies that some factor of F has exponent at least μ. □

Observe that in Theorem 2.1 one has $M(n) \ll_{K,\mu} n^2$ (under Vojta's conjecture) while in 2.2 we are unable to predict what the value of $M(n)$ should be. If one is willing to assume strong effective versions of Conjecture 1.4, then it would be possible to give a bound for M in Corollary 2.2. On the other hand, one can assume weaker versions of Conjecture 1.4 and still get the existence of M (at the price of losing the explicit bound) in Theorem 2.1, which would be enough to obtain Corollary 2.2. We leave the discussion on these variations to the reader.

In analogy with number fields, if L is the function field of a curve over an algebraically closed field, $n \geqslant 2$ is an integer and $f \in L$, then we say that f is *n-powerful* if all the zeros of f have multiplicity at least n (note that n is not required to be attained and there is no assumption on the poles of f). If f is 2-powerful we just say that f is powerful or squareful. Observe that if f is an n-th power then it is n-powerful. We make similar definitions for meromorphic functions on $\mathbb{C}$.

We introduce some notation that will be used to state our results for function fields and meromorphic functions.

Notation 2.3. *Let K, B, L and g be one of the following*

- *K is an algebraically closed field of characteristic zero, B is a smooth projective curve over K with genus g, and L is the function field of B, or*
- *$K = \mathbb{C}$, $B = \mathbb{C}$ and L is the field of complex meromorphic functions on $\mathbb{C}$. In this case we put $g = 1$ for convenience.*

In either case, we say that an element $a \in L$ is constant if $a \in K$, otherwise it is non-constant.

Our main result for function fields and meromorphic functions is

Theorem 2.4. *Let L/K and g be as in Notation 2.3. Let $F \in L[s]$ be a monic polynomial of degree $n \geqslant 2$ with some non-constant coefficient, that is, $F \notin K[s]$. Let $\lambda \leqslant n$ be an integer such that no irreducible factor of F has multiplicity strictly larger than λ in the factorization of F in $L[s]$. Define*

$$M = \begin{cases} 2n^2 + 4(g+1)n + 1 & \text{if } \lambda = n, \\ 2(\lambda+1)n(n+g) + 1 & \text{in general.} \end{cases}$$

Suppose that we have $b_1, b_2, \ldots, b_M$, distinct elements in K, such that $F(b_j)$ is μ-powerful for each $1 \leqslant j \leqslant M$ and some fixed $\mu \geqslant \lambda$. Then $\mu = \lambda$ and $F = GH$ for some monic polynomials $G \in K[s]$ and $H \in L[s]$ such that the largest exponent in the factorization of H as a product of irreducible polynomials is exactly λ.

This theorem will be proved in Section 3. For applications, the following consequence (analogue to Theorem 2.1) will be enough, but we remark that the somewhat more technical Theorem 2.4 is simpler to prove.

Corollary 2.5. *Let L/K and g be as in Notation 2.3. Let $n \geqslant 2$ and $2 \leqslant \mu \leqslant n$ be integers. Define*

$$M = \begin{cases} 2n^2 + 4(g+1)n + 1 & \text{if } \mu = n, \\ 2\mu n(n+g) + 1 & \text{in general,} \end{cases}$$

in the sense that if we do not assume $\mu = n$ then we use the second value for M. Let $b_1, \ldots, b_M \in K$ be distinct elements of the constant field. Define E as the set of monic polynomials $F \in L[s]$ of degree n such that all irreducible factors of F have multiplicity strictly less than μ, and such that for each $1 \leqslant k \leqslant M$ the function $F(b_k) \in L$ is μ-powerful. Then $E \subseteq K[s]$, that is, all $F \in E$ have constant coefficients.

Proof. If $\mu = n$ then let $F \in E$ and suppose F has some non-constant coefficient. Put $\lambda = \mu$ and use the previous theorem to conclude that F has some factor with exponent exactly λ. This is not possible as $F \in E$. Therefore, F must have constant coefficients.

For the general case $2 \leqslant \mu \leqslant n$, put $\lambda = \mu - 1$ and let $F \in E$. If F has some non-constant coefficient, then the previous theorem leads to a contradiction as $\lambda \neq \mu$. □

An equivalent formulation more amenable for our applications (and analogue to Corollary 2.2) is the following:

Corollary 2.6. *Let L/K and g be as in Notation 2.3. Let $n \geqslant 2$ and $2 \leqslant \mu \leqslant n$ be integers. Define M as in Corollary 2.5. Then the following holds*:

Let $F \in L[s]$ be a monic polynomial of degree n with some non-constant coefficient such that $F(b)$ is μ-powerful for at least M values of $b \in K$. Then F has a factor with exponent at least μ.

We remark that in the case of function fields, the assumption of zero characteristic cannot be dropped as the next example shows (see [23], or [3] for extensions of this example).

Example 2.7. Set $L = \bar{\mathbb{F}}_p(x) = \bar{\mathbb{F}}_p(\mathbb{P}^1_{\bar{\mathbb{F}}_p})$, for $p > 2$. The polynomial

$$F(s) = \left(s + \frac{x^q + x}{2}\right)^2 - \left(\frac{x^q - x}{2}\right)^2 \in L[s]$$

only represents squares as s ranges in $\mathbb{F}_q \subseteq \bar{\mathbb{F}}_p$ for q a power of p, but F has non-constant coefficients and one can show that it is not of the form $(s + \nu)^2$. Thus, a uniform M as in Corollary 2.6 cannot exist for $\mu = n = 2$ in this case.

Choosing suitable values for the parameters in the previous results leads to different statements that can be of interest. Here we focus on the extremal cases $\mu = 2$ and $\mu = n$.

For number fields, from Corollary 2.2 we get

Corollary 2.8. *Assume Conjecture 1.4. Let K be a number field and let $n \geqslant 2$. There are integer constants M_0, M_1 depending only on n and K such that the following holds*:

- *If $F \in K[s]$ is a monic squarefree polynomial of degree n, then not all the numbers $F(1), \ldots, F(M_0)$ are squareful. Hence, F cannot take M_0 consecutive squareful values, where M_0 is uniform on all such F.*
- *If $F \in K[s]$ is a monic polynomial of degree n such that all the numbers $F(1), \ldots, F(M_1)$ are n-powerful, then $F = (s + \nu)^n$ for some $\nu \in K$.*

In particular, Conjecture 1.4 implies Conjecture 1.1 and a positive answer to **Pow**(n, K). The following corollary provides the first evidence towards generalizations of Büchi's problem to higher exponents in the case of $\mathbb{Z}$.

Corollary 2.9. *Let A be an integrally closed subring of a number field K ($A = K$ is allowed). Conjecture 1.4 implies a positive answer to* **BP**(n, A) *for all $n \geqslant 2$.*

Proof. If $A = K$ is a number field, this follows directly from the second item of Corollary 2.8; one can show that there is a monic polynomial $F \in K$ of degree n such that $F(j) = u_j$. For general A one uses the fact that A is integrally closed to conclude that the corresponding ν is in A. Details are left to the reader. □

Next we turn our attention to function fields and meromorphic functions. In this case we can conclude an unconditional analogue of Corollary 2.8, whose formulation is left to the reader (for our purposes, we will focus on a refined analogue of the second item of Corollary 2.8).

The next result would follow immediately from Corollary 2.6 over algebraically closed fields, but we need a slightly more general version for later applications. For this, if L/K is a function field in one variable with constant subfield K (and K is not necessarily algebraically closed), we define the concept 'n-powerful' using valuations as for number fields.

Corollary 2.10. *Let L be the function field of a geometrically irreducible curve of genus g over a field K of characteristic zero which is algebraically closed in L, or let L be the field of meromorphic functions over $K=\mathbb{C}$ and put $g=1$. Let $n\geqslant 2$ and put $M=2n^2+4(g+1)n+1$. Then the following holds*:

If $F\in L[s]$ is a monic polynomial of degree n such that $F(1),\dots,F(M_0)$ are n-powerful then either $F=(s+\nu)^n$ for some $\nu\in L$ or F has constant coefficients (i.e. $F\in K[s]$).

Proof. For meromorphic functions and function fields with algebraically closed base field K, the conclusion follows by letting $\mu=n$ in Corollary 2.6. For the general case (in the function field setting), let L' be the extension of scalars of L/K to $\bar{K}$. Note that if $f\in L$ is n-powerful then it is n-powerful in L', and observe that the genus g is invariant under base change because we are in characteristic zero. Thus, in the situation of the statement, either $F\in\bar{K}[s]$ or there is some $\nu\in L'$ such that $F=(s+\nu)^n$ (by Corollary 2.6). In the first case, $F\in K[s]$ because K is algebraically closed in L and $F\in L[s]$. In the second case, note that $F\in L[s]$ and $F=s^n+n\nu s^{n-1}+\cdots+\nu^n$ hence $\nu\in L$. □

As for number fields, one obtains:

Corollary 2.11. *Let L be the function field of a geometrically irreducible curve over a field K of characteristic zero algebraically closed in L, or let L be the field of meromorphic functions over $K=\mathbb{C}$, and let $n\geqslant 2$ be an integer. The analogue of* **BP**(n,A) *for $A=L$ (for sequences with some u_i non-constant, otherwise it is trivial) has a positive answer with $M(n)\ll_L n^2$.*

We remark that Corollary 2.11 for $n=2$ was proved by Vojta (2000) in [32]. The first result in this direction for $n>3$ was a positive answer to **BP**$(3,\mathbb{C}[x])$, established by Pheidas and Vidaux (2008) in [22]. Then in 2011, in an earlier (unpublished) version of this work[1] we gave a positive answer to **BP**(n,L) with L a function field in characteristic zero and $n\geqslant 2$. Some months later, during the preparation of this paper, Corollary 2.11 was proved independently in [3][2] using a technique completely different from ours – they manage to generalize the approach by Pheidas and Vidaux involving systems of differential equations, from [22]. The approach in [3] is interesting in its own right as it works simultaneously for p-adic meromorphic functions, although it is not clear whether it can be adapted to attack questions on powerful values (the technique seems to be well suited only for studying n-th powers) and it cannot be extended to number fields because it strongly uses derivation. The bound for $M(n)$ obtained in [3] is also polynomial in n but it is slightly weaker than the bound in Corollary 2.11 – they obtain $M(n)\ll_L n^5$.

As we already mentioned, Büchi's motivation to state the M squares problem came from logic. Indeed, he realized that a positive answer to question 1.5 together with the undecidability of the positive existential theory of $\mathbb{Z}$ (which we call $H10$) would imply a very strong undecidability result for diagonal quadratic forms over $\mathbb{Z}$. As we explained in the introduction, our results have consequences related to undecidability through the definability of multiplication over weak languages, extending the program initiated by Büchi. In the discussion below, all the languages have equality.

Theorem 2.12. *Assume Conjecture 1.4. Let K be a number field and let R be an integrally closed subring of K. Let P be a unary predicate symbol and fix one of the following interpretations over R*:

[1] The preprint is available on http://arxiv.org/abs/1107.4019. In that earlier version of this paper, we already considered questions on powerful values, although only in the case of function fields and using a less accurate technique which became the present approach after several refinements.

[2] I would like to express my gratitude to the authors of [3] for kindly sending to me their preprint before publication.

- *$P(x)$ means 'x is an n-th power in R' for some fixed $n \geqslant 2$,*
- *$P(x)$ means 'x is a power in R',*
- *$P(x)$ means 'x is n-powerful' for some fixed $n \geqslant 2$.*

Define the language $\mathcal{L} = \{0, 1, +, P\}$ where $0, 1, +$ are interpreted in the usual way over R. Then multiplication is positive existential $\mathcal{L}$-definable in R. That is, there exists a positive existential $\mathcal{L}$-formula $\mu[x, y, z]$ such that, if $a, b, c \in R$ then $c = ab$ if and only if R satisfies $\mu[a, b, c]$.

We remark that in the above theorem the notion of $x \in R$ being (n-)powerful is relative to K, since it is defined in terms of valuations, but the notion of being an n-th power is relative to R.

The proof of Theorem 2.12 does not involve new ideas and can be deduced from Corollary 2.8 essentially following the original approach by Büchi. We give details in Section 5.

A direct consequence is the following.

Corollary 2.13. *Assume Conjecture 1.4. Let K, R, and P be as in Theorem 2.12. Let $\mathcal{L}_r = \{0, 1, +, \cdot\}$ be the language of rings (with the usual interpretations). Suppose that the positive existential theory of R over $\mathcal{L}_r$ is undecidable. Then the positive existential theory of R over $\mathcal{L} = \{0, 1, +, P\}$ is undecidable.*

Corollary 2.13 may be applied in several situations, as long as some analogue of $H10$ has been established in the corresponding case. See [29] for a very complete exposition on Hilbert's tenth problem for subrings of number fields and related topics.

In order to make clear (for non-specialists) the meaning of Corollary 2.13 for Diophantine problems, let us give two consequences of Corollary 2.13 in terms of systems of Diophantine equations over $\mathbb{Z}$ (similar results hold whenever Corollary 2.13 can be applied, but we state them in this special case for the sake of concreteness).

Corollary 2.14. *Assume Conjecture 1.4. Fix an integer $n \geqslant 2$. There is no algorithm to solve the following decision problem*:

Given $B_1, \ldots, B_s \in \mathbb{Z}[x_1, \ldots, x_r]$, diagonal forms of degree n, and given $c_1, \ldots, c_s \in \mathbb{Z}$, decide whether or not there is some $\mathbf{v} \in \mathbb{Z}^r$ such that $B_i(\mathbf{v}) = c_i$ for each $1 \leqslant i \leqslant s$.

It is easy to see that the decision problem stated in the previous corollary is a particular instance of the decision problem presented in the next corollary (which is immediate from Corollary 2.13 and $H10$).

Corollary 2.15. *Assume Conjecture 1.4. Let $\mathcal{P} \subseteq \mathbb{Z}$ be one of the following sets of integers*

- *the set of n-th powers for some fixed $n \geqslant 2$,*
- *the set of powers,*
- *the set of n-powerful integers for some fixed $n \geqslant 2$.*

There is no algorithm to solve the following decision problem:

Given a system (S) of first degree equations with integer coefficients in the unknowns $x_1, \ldots, x_r$,

$$(S): \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2r}x_r = b_2, \\ \quad \vdots \\ a_{s1}x_1 + a_{s2}x_2 + \cdots + a_{sr}x_r = b_s \end{cases}$$

and given a set of indices $I \subseteq \{1, 2, \ldots, r\}$, decide whether or not there exists $\mathbf{v} = (v_1, \ldots, v_r) \in \mathbb{Z}^r$ such that $\mathbf{v}$ is a solution for (S) and $v_i \in \mathcal{P}$ for each $i \in I$.

That is, Vojta's Conjecture 1.4 implies that the problem of solving systems of linear equations over $\mathbb{Z}$ (or even deciding the existence of solutions) becomes undecidable if we require that some (or all) variables are squareful or powers (or more generally, n-powerful or n-th powers for fixed n).

As in the case of number fields, we can use our arithmetic results for function fields and meromorphic functions in order to obtain consequences in logic.

Theorem 2.16. *Let L be the function field of a geometrically irreducible curve over a field K of characteristic zero which is algebraically closed in L, or let L be the field of meromorphic functions and $K = \mathbb{C}$. Let R be an integrally closed K-subalgebra of L containing some element transcendental over K. Let P be a unary predicate symbol and fix an interpretation for it as in Theorem 2.12. Let α be a unary function symbol interpreted as $x \mapsto u \cdot x$ for some fixed $u \in R$ transcendental over K. Consider the language $\mathcal{L} = \{0, 1, +, P, \alpha\}$ where $0, 1, +$ are interpreted in the usual way over R. Then multiplication is positive existential $\mathcal{L}$-definable on R.*

The proof of Theorem 2.16 goes along the same lines as the proof of Theorem 2.12. We will indicate the main details in the last section. Some results on the direction of Theorem 2.16 are known; we refer the reader to [20] for an exposition of results when $P(x)$ means 'x is a square' over several structures. If $P(x)$ is interpreted as 'x is a power', some cases have been studied, see [10].

As in the number field case a direct consequence is:

Corollary 2.17. *Let K, L, R, P, α and u be as in Theorem 2.16. Define the language $\mathcal{L}_{r,\alpha} = \{0, 1, +, \cdot, \alpha\}$ and consider the obvious interpretations on R (interpret α as in Theorem 2.16). Suppose that for some language $\mathcal{L}^*$ extending $\mathcal{L}_{r,\alpha}$ the positive existential theory of R over $\mathcal{L}^*$ is undecidable. Let $\mathcal{L}_P^*$ be the language obtained from $\mathcal{L}^*$ by replacing the symbol $\cdot$ by P. Then the positive existential theory of R over $\mathcal{L}_P^*$ is undecidable.*

This result is applicable, for example, when $\mathcal{L}^* = \mathcal{L}_{r,\alpha}$ and $R = \mathbb{C}[x]$ or $R = \mathbb{R}(x)$, by results of Denef [9]. The literature on analogues of Hilbert's tenth problem for subrings of function fields is wide – for instance, we refer the reader to [11,18,35] for more cases where Corollary 2.17 can be applied. We remark that although Hilbert's tenth problem is open for $\mathbb{C}(x)$ and for the field of meromorphic functions over $\mathbb{C}$, one can obtain undecidability if we take $\mathcal{L}^*$ a suitable enlargement of $\mathcal{L}_{r,\alpha}$. For example, one obtains undecidability of the positive existential theory of $\mathbb{C}(x)$ if we include a unary predicate symbol 'ord' for elements vanishing at zero, so that in this case we can also apply Corollary 2.17.

The next sections contain the proofs of our main results. We consider first the case of function fields and meromorphic functions (which is simpler), and then the number field situation. We hope that this order of presentation will help to clarify the main ideas. At the end of this paper, we include a short section to explain the proof of the consequences in logic, following Büchi's ideas.

3. Value distribution on extensions of bounded degree

3.1. Function fields

In this section we recall the basic results on function fields that we need for the proof of Theorem 2.4. We focus on value distribution for algebraic extensions of bounded degree.

Let K be an algebraically closed field of characteristic zero. Let B, B' be smooth projective curves over K and let $\pi : B' \to B$ be a non-constant morphism. Write $L = K(B)$ and $L' = K(B')$, so that π corresponds to the algebraic extension L'/L.

In our application, L will be a fixed function field and L' will range among all algebraic extensions of L of bounded degree. Thus, all the definitions below are understood to be relative to B, even if the notation makes no reference to it.

For $f \in L'$ non-constant and $\alpha \in \mathbb{P}^1(K)$ define the *height of f relative to α* by

$$h_{L'/L,\alpha}(f) = h_{L',\alpha}(f) = \frac{1}{[L' : L]} \big(\text{number of pre-images of } \alpha \text{ by } f : B' \to \mathbb{P}^1 \text{ counting multiplicities}\big).$$

We put $h_{L',\alpha}(f) = 0$ for f constant. We always have $h_{L',\alpha}(f) > 0$ for f non-constant.

We define the *truncated counting function* in a similar way but ignoring multiplicities;

$$N^{(1)}_{L'/L,f}(\alpha) = N^{(1)}_{L',f}(\alpha) = \frac{1}{[L' : L]} \big(\text{number of pre-images of } \alpha \text{ by } f : B' \to \mathbb{P}^1 \text{ ignoring multiplicities}\big).$$

Observe that we can take $B' = B$ and $\pi = Id_B$ so that the height and the truncated counting function are defined for $f \in L$.

The following proposition is clear. We call it *first main theorem* by analogy with Nevanlinna theory.

Proposition 3.1 *(First main theorem). For $f \in L'$ non-constant and $\alpha, \beta \in \mathbb{P}^1(K)$ we have*

$$h_{L',\alpha}(f) = h_{L',\beta}(f) = \frac{1}{[L' : L]} \deg(f) > 0$$

where $\deg(f)$ *is the degree of* $f : B' \to \mathbb{P}^1$.

So we can define the *height of $f \in L'$* to be

$$h_{L'}(f) = \frac{\deg(f)}{[L' : L]},$$

where $\deg(f) = 0$ for f constant. Moreover, given finite extensions of function fields $L'' - L' - L$ corresponding to a B-morphism of smooth projective curves $\tau : B'' \to B'$ we have

$$h_{L''/L}\big(\tau^* f\big) = h_{L'/L}(f)$$

for any $f \in L'$ and $\alpha \in \mathbb{P}^1(K)$. Therefore the height is compatible with field extensions (however, the truncated counting function is not). This observation shows that for f algebraic over $L = K(B)$, one has a well defined number

$$h(f) := h_{L'}(f)$$

where L' is any finite extension of L containing f. We call $h(f)$ the *height of f*.

Since the truncated counting function depends on field extensions (due to ramification) we fix the notation

$$N^{(1)}_f(\alpha) = N^{(1)}_{L(f),f}(\alpha).$$

That is, given f algebraic over L, the truncated counting function is considered with respect to the field $L(f)$ unless specified in a different way.

Next two results are elementary.

Lemma 3.2. *Let f, g be algebraic over $L = K(B)$. Then*

$$h(f+g) \leqslant h(f) + h(g) \quad \text{and} \quad h(fg) \leqslant h(f) + h(g).$$

Lemma 3.3. *Let f, g algebraic over $L = K(B)$ and assume that f and g are Galois conjugates. Then $h(f) = h(g)$.*

Lemma 3.4. *Let $G = H_1 \cdots H_c$ with $H_j \in L[s]$ distinct monic irreducible of degree d_j. Let Δ be the discriminant of G. Let f_j be a root of H_j and let $d = \sum_j d_j$. Then*

$$h(\Delta) \leqslant 2(d-1) \sum_{j=1}^{c} d_j h(f_j).$$

Proof. Let $g_1, \ldots, g_d$ be the roots of G in $\bar{L}$, counting multiplicities. Then

$$\Delta = \left(\prod_{1 \leqslant i < j \leqslant d} (g_i - g_j) \right)^2.$$

By Lemma 3.2, first applied to the exponent 2, then to the product and then to each difference $(g_i - g_j)$, we obtain

$$h(\Delta) \leqslant 2(d-1) \sum_{k=1}^{d} h(g_k)$$

and the result follows by Lemma 3.3. □

Lemma 3.5. *Let f be algebraic over $L = K(B)$ and non-constant, let $H \in L[s]$ be its (monic) minimal polynomial and let $\Delta \in L$ be the discriminant of H. Let $L' = L(f)$ and let $\pi : B' \to B$ be a morphism of smooth projective curves associated to the field extension L'/L. Let $p \in B$ and let $q_1, \ldots, q_r \in B'$ be the points above p. If f is regular at all the q_i then the coefficients of H are regular at p. If moreover Δ does not vanish at p then f can vanish at most at one q_{i_0}, in which case $\operatorname{ord}_{q_{i_0}}(f) = \operatorname{ord}_p H(0)$.*

Proof. The claims in this lemma are classical results regarding valuations and field extensions. The proofs can be found, for example, in [27]. Alternatively, see the proof of Lemma 3.17 below. □

The following well-known result can be considered as an analogue of the *second main theorem* with truncated counting functions (from Nevanlinna theory) for algebraic extensions of bounded degree. The proof is easy and we include it for the sake of completeness.

Theorem 3.6. *Let $\pi : B' \to B$ be a non-constant morphism of smooth projective curves over K, write $L = K(B)$ and $L' = K(B')$, and let $f \in L'$ be non-constant. Let $b_1, \ldots, b_q \in \mathbb{P}^1(K)$ be distinct points. Then*

$$(q-2)h(f) \leqslant \frac{\deg R_\pi}{[L':L]} - \chi(B) + \sum_{j=1}^{q} N^{(1)}_{L',f}(b_j)$$

where $\chi(-)$ denotes the Euler characteristic and $R_\pi \in \operatorname{Div}(B')$ is the ramification divisor of π.

Proof. Riemann–Hurwitz formula applied to π gives

$$\chi\big(B'\big) = \big[L' : L\big]\chi(B) - \deg R_\pi .$$

Similarly, applying the (topological version of the) Riemann–Hurwitz formula to the map $f : B' \to \mathbb{P}^1$ we get

$$\begin{aligned}\chi\big(B'\big) &= 2\deg(f) - \sum_{p\in\mathbb{P}^1(K)} \big(\deg(f) - \#f^{-1}(p)\big)\\ &\leqslant 2\deg(f) - \sum_{j=1}^{q}\big(\deg(f) - \#f^{-1}(b_j)\big)\\ &= (2-q)\deg(f) + \big[L' : L\big]\sum_{j=1}^{q} N^{(1)}_{L',f}(b_j)\end{aligned}$$

where # denotes the cardinality of a set. Therefore

$$\big[L' : L\big]\chi(B) - \deg R_\pi \leqslant (2-q)\deg(f) + \big[L' : L\big]\sum_{j=1}^{q} N^{(1)}_{L',f}(b_j)$$

and the result follows. □

The particular case $B' = B$, $\pi = Id$ (or directly from Riemann–Hurwitz) gives

Corollary 3.7. *Let B be a smooth projective curve over K of genus g. Write $L = K(B)$ and let $b_1, \dots, b_q \in \mathbb{P}^1(K)$ be distinct points. Let $f \in L$ be non-constant. Then*

$$(q-2)h(f) \leqslant 2(g-1) + \sum_{j=1}^{q} N^{(1)}_{L',f}(b_j).$$

The term $\deg(R_\pi)/[L' : L]$ in Theorem 3.6 is not convenient for our purposes, so we will bound it in terms of heights. We introduce the notation $e(x|p)$ for the ramification index (the morphism of curves mapping x to p will be clear from the context). We will use the following classical result.

Lemma 3.8. *Let f be algebraic over $L = K(B)$ with (monic) minimal polynomial*

$$H(s) = s^d + c_{d-1}s^{d-1} + \cdots + c_1 s + c_0 \in L[s].$$

Then

$$\sum_{p\in B} \min\{0, \operatorname{ord}_p c_{d-1}, \dots, \operatorname{ord}_p c_0\} = dh(f).$$

Proof. See Proposition 4, p. 49 in [13]. In our situation there are no Archimedean places, so that the constants c_1, c_2 in [13] are equal to 1. □

Lemma 3.9. *Let f be algebraic over $L = K(B)$ and let $L' = L(f)$. Let $\pi : B' \to B$ be a morphism of smooth projective curves such that $L' = K(B')$ and such that π corresponds to L'/L. Let $d = [L' : L] = \deg(\pi)$ and let $R_\pi \in \mathrm{Div}(B')$ be the ramification divisor. Then*

$$\frac{\deg(R_\pi)}{[L' : L]} \leqslant (3d-2)h(f).$$

Proof.[3] Let $\mathcal{D}_\pi \in \mathrm{Div}(B')$ be the different divisor associated to the branched covering π. Let S_f be the set of points in B lying below poles of f. Let $A \subseteq K(B) = L$ be the ring of functions regular away from S_f. Let $H = s^d + a_{d-1}s^{d-1} + \cdots + a_0$ be the minimal polynomial of f over L and observe that $H \in A[s]$ by Lemma 3.5. We use Corollary 2 on p. 56 of [27] to compute

$$\begin{aligned}
\deg R_\pi = \deg \mathcal{D}_\pi &= \sum_{p\in B} \sum_{p'\in\pi^{-1}(p)} \mathrm{ord}_{p'}(\mathcal{D}_{L'/L}) \\
&\leqslant \sum_{p\in S_f} \sum_{p'\in\pi^{-1}(p)} \big(e(p'|p)-1\big) + \sum_{p\in B-S_f} \sum_{p'\in\pi^{-1}(p)} \mathrm{ord}_{p'}\big(H'(f)\big) \\
&\leqslant \sum_{p\in S_f} (d-1) + \sum_{p\in B-S_f} \sum_{p'\in\pi^{-1}(p)} \max\big\{0, \mathrm{ord}_{p'}\big(H'(f)\big)\big\} \\
&\leqslant (d-1)\deg(f)_\infty + \sum_{p'\in B'} \max\big\{0, \mathrm{ord}_{p'}\big(H'(f)\big)\big\} \\
&= d(d-1)h(f) + \deg\big(H'(f)\big)_0 \\
&= d(d-1)h(f) + dh\big(H'(f)\big).
\end{aligned}$$

Note that $H'(f) = df^{d-1} + (d-1)a_{d-1}f^{d-2} + \cdots + a_1$ therefore, looking at poles and using the previous lemma we find

$$\begin{aligned}
dh\big(H'(f)\big) &= \sum_{p'\in B'} -\min\big\{0, \mathrm{ord}_{p'}\big(H'(f)\big)\big\} \\
&\leqslant \sum_{p'\in B'} -\min\big\{0, \mathrm{ord}_{p'}\big(df^{d-1}\big), \mathrm{ord}_{p'}\big((d-1)a_{d-1}f^{d-2}\big), \ldots, \mathrm{ord}_{p'}(a_1)\big\} \\
&\leqslant (d-1)\sum_{p'\in B'} -\min\big\{0, \mathrm{ord}_{p'}(f)\big\} + \sum_{p'\in B'} -\min\big\{0, \mathrm{ord}_{p'}(1), \mathrm{ord}_{p'}(a_{d-1}), \ldots, \mathrm{ord}_{p'}(a_0)\big\} \\
&= (d-1)\sum_{p'\in B'} -\min\big\{0, \mathrm{ord}_{p'}(f)\big\} + d\sum_{p\in B} -\min\big\{0, \mathrm{ord}_{p}(a_{d-1}), \ldots, \mathrm{ord}_{p}(a_0)\big\} \\
&= (d-1)\deg(f)_\infty + d^2h(f) = d(2d-1)h(f).
\end{aligned}$$

Therefore

$$\deg R_\pi \leqslant d(d-1)h(f) + d(2d-1)h(f) = d(3d-2)h(f). \qquad \square$$

[3] The author would like to express his gratitude to Julie Wang for suggesting this proof. Before this suggestion, the bound in Lemma 3.9 had a quadratic dependence on d instead of linear.

Remark 3.10. The above bound is not optimal (for example, take $\pi = Id$) but the proof works without major modifications for meromorphic functions and number fields.

Therefore, we arrive to the following version of the second main theorem:

Theorem 3.11. *Let B be a smooth projective curve over K of genus g, let $d \geqslant 1$ be an integer and let $b_1, \ldots, b_q \in \mathbb{P}^1(K)$ be distinct points. For all non-constant f algebraic over $L = K(B)$ with $[L(f) : L] \leqslant d$, the following inequality holds*

$$(q - 3d)h(f) \leqslant \sum_{j=1}^{q} N_f^{(1)}(b_j) + 2(g-1).$$

3.2. Meromorphic functions on finite ramified coverings of $\mathbb{C}$

We refer the reader to [6,7,26,33] for some standard facts in this section. Let $\pi : B' \to \mathbb{C}$ be a finite ramified covering of Riemann surfaces of degree d. We always assume that such B' is connected. Write $\mathcal{M}(B')$ for the field of meromorphic functions of B'. Define

$$B'(r) = \{z \in B' : \ |\pi(z)| < r\},$$
$$B'\langle r\rangle = \{z \in B' : \ |\pi(z)| = r\},$$

and consider the measure

$$d\sigma = \frac{1}{\deg \pi} \pi^* \frac{d\theta}{2\pi}$$

on $B'\langle r\rangle$. Given a non-constant meromorphic map $f : B' \to \mathbb{C}$ and $\alpha \in \mathbb{C}$ we define

$$m_f(\alpha, r) = \int\limits_{B'\langle r\rangle} \log^+ \frac{1}{|f - \alpha|} d\sigma$$

and for $\alpha = \infty$ we define

$$m_f(\infty, r) = \int\limits_{B'\langle r\rangle} \log^+ |f| \, d\sigma.$$

An analytic divisor on B' is a formal sum of points on B' with integer coefficients and possibly infinite support, such that its support is finite when restricted to $B'(r)$ for any r. Given an analytic divisor $D = \sum_{b \in B'} n_b b$ on B', we define the *counting function*

$$N_D(r) = \frac{1}{\deg \pi} \left(\sum_{b \in B'(r) - \pi^{-1}(0)} n_b \log \frac{r}{|\pi(b)|} + \sum_{b \in \pi^{-1}(0)} n_b \log r \right).$$

If f is a non-constant meromorphic function on B' and D is a divisor on $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C}_\infty$ then one can define the analytic divisor f^*D and the counting function

$$N_\phi(D, r) = N_{f^*D}(r).$$

Moreover, we let $N_{\mathrm{ram}(\pi)}(r)$ be the counting function for the ramification divisor of π (which is an analytic divisor).

If $\alpha \in \mathbb{C}_\infty$ and f is a non-constant meromorphic function on B' then the analytic divisor $f^*\alpha$ is effective (looking at α as a divisor) which means that it has non-negative coefficients. Let $(f^*\alpha)_{\mathrm{red}}$ be the analytic divisor obtained by replacing all the strictly positive coefficients by 1. Then we define the *truncated counting function* by

$$N^{(1)}_{f,B'}(\alpha, r) = N_{(f^*\alpha)_{\mathrm{red}}}(r).$$

Finally, given f a non-constant meromorphic function on B' define its *height* by

$$T_f(r) = m_f(\infty, r) + N_f(\infty, r)$$

which is a function of $r > 0$. In order to include constant functions, we define $T_c(r) = 0$ for any constant function c. If $B'' \to B' \to \mathbb{C}$ are finite ramified coverings and f is a meromorphic function on B', then we can pull-back f to a meromorphic function on B'' which we also denote by f (only when this notation is not confusing). As in the function field case, it is easy to see that $T_f(r)$ is the same when computed on B' or B''. Therefore, given f algebraic over $\mathcal{M}(\mathbb{C})$ the *height* $T_f(r)$ of f is well defined (one realizes f as a meromorphic function on some finite ramified covering of $\mathbb{C}$).

However, given f algebraic over $\mathcal{M}(\mathbb{C})$ the truncated counting function of f may depend on the realization of f as meromorphic function on some Riemann surface. We define $N^{(1)}_f(\alpha, r)$ to be the truncated counting function of f realized as a meromorphic function on some B' such that $\mathcal{M}(B') = \mathcal{M}(\mathbb{C})(f)$ (note that $N^{(1)}_f(\alpha, r)$ is well defined).

The *first main theorem* in this context is

Theorem 3.12. *Let f be a non-constant meromorphic function on B' and let $\alpha \in \mathbb{C}_\infty$. Then*

$$m_f(\alpha, r) + N_f(\alpha, r) = T_f(r) + \mathcal{O}(1)$$

where $\mathcal{O}(1)$ remains bounded as $r \to \infty$.

Unlike the function field case, this is not an obvious fact (see the references indicated at the beginning of this section).

We need the following results about $T_f(r)$.

Lemma 3.13. *(Compare with Lemma 3.2.) Let f, g be algebraic over $\mathcal{M}(\mathbb{C})$. Then we have*

$$T_{f+g}(r) \leqslant T_f(r) + T_g(r) + \mathcal{O}(1)$$

and

$$T_{fg}(r) \leqslant T_f(r) + T_g(r) + \mathcal{O}(1).$$

Proof. This is a straightforward computation. One verifies similar inequalities for $m_f(\infty, r)$ and $N_f(\infty, r)$ separately, and the result follows from the definition of $T_f(r)$. Details are left to the reader. □

Lemma 3.14. *(Compare with Lemma 3.3.) Let $\pi : B' \to \mathbb{C}$ be a finite ramified covering and let $\sigma : B' \to B'$ be a covering automorphism. Then for any non-constant $f \in \mathcal{M}(B')$ we have $T_{\sigma^* f}(r) = T_f(r)$. In particular, $T_\bullet(r)$ is invariant under Galois conjugation.*

Proof. This is clear from the definitions of $m_f(\infty, r)$ and $N_f(\infty, r)$. Indeed, Galois invariance holds for $m_\bullet(\infty, r)$ and $N_\bullet(\infty, r)$ individually. □

Lemma 3.15. *(Compare with Lemma 3.4.) Let $G = H_1 \cdots H_c$ with $H_j \in \mathcal{M}(\mathbb{C})[s]$ distinct monic irreducible of degree d_j. Let f_j be a root of H_j and let $d = \sum_j d_j$. Then*

$$T_\Delta(r) \leqslant 2(d-1) \sum_{j=1}^{c} d_j T_{f_j}(r) + \mathcal{O}(1)$$

where $\Delta \in \mathcal{M}(\mathbb{C})$ is the discriminant of G.

Proof. The proof is the same as in the function field setting (Lemma 3.4), except for the bounded error term coming from Lemma 3.13. □

The next lemma is used to prove an analogue of Lemma 3.5.

Lemma 3.16. *Let f be algebraic over $\mathcal{M}(\mathbb{C})$, non-constant with monic minimal polynomial H, and let $\pi : B' \to \mathbb{C}$ be a ramified covering such that $\mathcal{M}(B') = \mathcal{M}(\mathbb{C})(f)$. For $z_0 \in \mathbb{C}$ not a zero of the discriminant of H and not a pole of any coefficient of H, let $H_{z_0} \in \mathbb{C}[s]$ be the polynomial obtained by evaluating the coefficients of H at z_0. Let S_{z_0} be the set of roots of H_{z_0}. Then f restricts to a bijective map $\pi^{-1}(z_0) \to S_{z_0}$.*

Proof. Since the discriminant of H does not vanish at z_0 we have that $\#S_{z_0} = \deg \pi$, so it is enough to show surjectivity. Let $x \in S_{z_0}$, then one can construct a finite ramified covering $\pi' : B'' \to \mathbb{C}$ and $g \in \mathcal{M}(B'')$ such that $H(g) = 0$, $\mathcal{M}(B'') = \mathcal{M}(\mathbb{C})(g)$ and $g(w) = x$ for some $w \in \pi'^{-1}(z_0)$. Since we have an $\mathcal{M}(\mathbb{C})$-isomorphism $u : \mathcal{M}(B'') \to \mathcal{M}(B')$ defined by $u(g) = f$, we get a bi-holomorphic map $h : B' \to B''$ commuting with π and π' such that $f = g \circ h$ (see Theorem 3.1 in [12]). Then x is in the image of $\pi^{-1}(z_0) \to S_{z_0}$. □

We have:

Lemma 3.17. *Let f be algebraic over $\mathcal{M}(\mathbb{C})$ and non-constant, let $H \in \mathcal{M}(\mathbb{C})[s]$ be its monic minimal polynomial and let $\Delta \in \mathcal{M}(\mathbb{C})$ be the discriminant of H. Let $\pi : B' \to \mathbb{C}$ be a finite branched covering such that $\mathcal{M}(B') = \mathcal{M}(\mathbb{C})(f)$. Let $p \in \mathbb{C}$ and let $q_1, \ldots, q_r \in B'$ be the points above p. If f is regular at all the q_i then the coefficients of H are regular at p. Moreover, if Δ does not vanish at p then f can vanish at most at one q_{i_0}, in which case $\operatorname{ord}_{q_{i_0}}(f) = \operatorname{ord}_p H(0)$.*

Proof. This is similar to Lemma 3.5, and we include it for the sake of completeness.

That the coefficients of H are regular at p is clear after we express the coefficients of H in terms of the Galois conjugates of f.

By the previous lemma, the map π is unramified above p and moreover f takes distinct values at the q_i. Thus, at most one of the $\operatorname{ord}_{q_i}(f)$ can be non-zero (and hence positive because f is regular above p).

If all the $\operatorname{ord}_{q_i}(f)$ are zero, then 0 is not in the image of f restricted to $\{q_i\}_i = \pi^{-1}(p)$. Thus, by the previous lemma, 0 is not one of the d zeros of H_p (the complex polynomial obtained by evaluating the coefficients of H at p), and we get that $\operatorname{ord}_p H(0) = 0$. Taking any i_0 proves the result in this case.

Now suppose that there is some (and hence, a unique) index such that $\operatorname{ord}_{q_{i_0}}(f) > 0$. Write $H(s) = s^d + c_{d-1}s^{d-1} + \cdots + c_0$. Then we have $H(0) = c_0$, and since 0 is in the image of f restricted to $\{q_i\} = \pi^{-1}(p)$ we conclude that 0 is one of the d distinct roots of H_p. Therefore $c_0(p) = 0$ and $c_1(p) \neq 0$ (since H_p has no repeated zeros). Finally, consider

$$\left(f^{d-1}+\pi^*c_{d-1}f^{d-2}+\cdots+\pi^*c_1\right)f=-\pi^*c_0,$$

and recall that all the c_i are regular at p. We get

$$\operatorname{ord}_{q_{i_0}}(f)=\operatorname{ord}_{q_{i_0}}\pi^*c_0=\operatorname{ord}_p c_0=\operatorname{ord}_p H(0),$$

where the second equality holds because π is unramified above p. □

Let us introduce the following notation; if $X(r), Y(r)$ are functions on $r>0$ we write $X(r).\leqslant .Y(r)$ if one has $X(r)\leqslant Y(r)$ for r outside a set of finite measure.

The following version of the second main theorem is a corollary of McQuillan's tautological inequality (see Corollary 29.7 in [33] and use Theorem 3.6 in the case $T_f(r)\ll\log r$).

Theorem 3.18. *Let B' be a finite branched covering of $\mathbb{C}$, let f be a meromorphic function on B' and let $b_1,\ldots,b_q$ be distinct points in $\mathbb{C}_\infty$. Let $\epsilon>0$. Then*

$$(q-2-\epsilon)T_f(r).\leqslant .\sum_{j=1}^{q}N^{(1)}_{f,B'}(b_j,r)+N_{\mathrm{ram}(\pi)}(r).$$

In the classical case $B=\mathbb{C}$, $\pi=Id$ one gets

Theorem 3.19. *Let f be a meromorphic function on B and let $b_1,\ldots,b_q$ be distinct points in $\mathbb{C}_\infty$. Let $\epsilon>0$. Then*

$$(q-2-\epsilon)T_f(r).\leqslant .\sum_{j=1}^{q}N^{(1)}_{f}(b_j,r).$$

For our application, we want to replace the ramification term in the second main theorem by some expression depending on the height of f. First we need an analogue of Lemma 3.8.

Lemma 3.20. *Let f be algebraic over $\mathcal{M}(\mathbb{C})$ with monic minimal polynomial*

$$H(s)=s^d+c_{d-1}s^{d-1}+\cdots+c_1s+c_0\in\mathcal{M}(\mathbb{C})[s].$$

Then

$$N_c(\infty,r)+m_c(\infty,r)=dT_f(r)+\mathcal{O}(1)$$

where $N_c(\infty,r)$ is the counting function of the analytic divisor

$$D=\sum_{p\in\mathbb{C}}\min\{0,\operatorname{ord}_p c_{d-1},\ldots,\operatorname{ord}_p c_0\}p$$

and

$$m_c(\infty,r)=\int_{\mathbb{C}\langle r\rangle}\log\max\left\{1,|c_{d-1}|,\ldots,|c_0|\right\}\frac{d\theta}{2\pi}.$$

Proof. Let $\gamma : B'' \to \mathbb{C}$ be a branched covering such that $\mathcal{M}(B'')$ is the splitting field of H, and let $\phi_1, \ldots, \phi_d \in \mathcal{M}(B'')$ be the Galois conjugates of f. The same argument as in the (quoted) proof of Lemma 3.8 gives

$$N_c(\infty, r) = \sum_{j=1}^{d} N_{\phi_j}(\infty, r).$$

On the other hand, using Lemma 1 on p. 47 of [13], pointwise on $B''\langle r\rangle$ we get

$$\begin{aligned} m_c(\infty, r) &= \frac{1}{\deg \gamma} \int\limits_{B''\langle r\rangle} \log \max\{1, |\gamma^* c_{d-1}|, \ldots, |\gamma^* c_0|\} \gamma^* \frac{d\theta}{2\pi} \\ &= \frac{1}{\deg \gamma} \int\limits_{B''\langle r\rangle} \log \prod_{j=1}^{d} \max\{1, |\phi_j|\} \gamma^* \frac{d\theta}{2\pi} + \mathcal{O}(1) \\ &= \sum_{j=1}^{d} \frac{1}{\deg \gamma} \int\limits_{B''\langle r\rangle} \log \max\{1, |\phi_j|\} \gamma^* \frac{d\theta}{2\pi} + \mathcal{O}(1) \\ &= \sum_{j=1}^{d} m_{\phi_j}(\infty, r) + \mathcal{O}(1) \end{aligned}$$

where the error term is bounded in absolute value by $(\log 2)d$. Therefore we get

$$\begin{aligned} N_c(\infty, r) + m_c(\infty, r) &= \sum_{j=1}^{d} N_{\phi_j}(\infty, r) + \sum_{j=1}^{d} m_{\phi_j}(\infty, r) + \mathcal{O}(1) \\ &= \sum_{j=1}^{d} T_{\phi_j}(r) + \mathcal{O}(1) = dT_f(r) + \mathcal{O}(1). \end{aligned}$$

□

Lemma 3.21. *Let f be algebraic over $\mathcal{M}(\mathbb{C})$ and let $\pi : B' \to \mathbb{C}$ be a finite ramified covering such that $\mathcal{M}(B') = \mathcal{M}(\mathbb{C})(f)$. Let $n = \deg(\pi)$. Then for all $\epsilon > 0$ we get*

$$N_{\mathrm{ram}(\pi)} \leqslant (3n - 2)T_f(r) + \mathcal{O}(1).$$

Proof. The proof of this result goes along the same lines as the proof of Lemma 3.9, but using Lemma 3.17 instead of Lemma 3.5, and Lemma 3.20 instead of Lemma 3.8. The error term also has a contribution coming from an application of the first main theorem when we compute the height of $H'(f)$ using poles instead of zeros. Details are left to the reader. □

Thus we conclude

Theorem 3.22. *Let $d \geqslant 1$ be an integer and let $b_1, \ldots, b_q \in \mathbb{C}_\infty$ be distinct points. Let f be algebraic over $\mathcal{M}(\mathbb{C})$, non-constant and with $[\mathcal{M}(\mathbb{C})(f) : \mathcal{M}(\mathbb{C})] \leqslant d$. For all $\epsilon > 0$ the following inequality holds*

$$(q - 3d - \epsilon)T_f(r). \leqslant . \sum_{j=1}^{q} N_f^{(1)}(b_j, r).$$

3.3. Proof of Theorem 2.4

Let us recall the notation introduced before Theorem 2.4. Let K, B, g and L be one of the following

- K is an algebraically closed field of characteristic zero, B is a smooth projective curve over K with genus g, and L is the function field of B, or
- $K=\mathbb{C}$, $B=\mathbb{C}$ and L is the field of complex meromorphic functions on $\mathbb{C}$. In this case we can set $g=1$ for notational convenience (actually, the second main theorem of Nevanlinna theory suggests that for any $\epsilon>0$ we can think about g as $g=1+\epsilon$).

In either case, if $B'\to B$ is a branched covering then we denote by $K(B')$ the field of meromorphic functions on B', which is a field extension of L via the pull-back induced by $B'\to B$.

The purpose of this section is proving Theorem 2.4. We begin with

Lemma 3.23. *Let $H(s)=s+a\in L[s]$ with $a\in L$ non-constant. There are at most*

$$W:=\begin{cases}\max\{3,4g\} & \text{in the function field case},\\ 4 & \text{in the meromorphic case}\end{cases}$$

values of $b\in K$ such that $H(b)$ has only multiple zeros.

Proof. Let $b_1,\dots,b_q\in K$ be distinct elements such that $H(b_j)$ only has multiple zeros for each j. In the function field case, Corollary 3.7 gives

$$\begin{aligned}(q-2)h(a)&\leqslant 2(g-1)+\sum_{j=1}^{q}N_a^{(1)}(-b_j)\\ &\leqslant 2(g-1)+\frac{1}{2}\sum_{j=1}^{q}h_{-b_j}(a)=2(g-1)+\frac{q}{2}h(a)\end{aligned}$$

where we used the fact that $a+b_j$ only has multiple zeros for each j. So we conclude

$$q\leqslant 4+\frac{4(g-1)}{h(a)}.$$

Since $a\in L$ is non-constant we have $h(a)\geqslant 1$ by Lemma 3.1. Thus, when $g=0$ we get $q\leqslant 3$, and when $g\geqslant 1$ we get $q\leqslant 4g$. The meromorphic case goes along the same lines using Theorem 3.19 instead of Corollary 3.7. □

The next lemma reduces the proof of Theorem 2.4 to the proof of a simpler statement.

Lemma 3.24. *It suffices to prove Theorem 2.4 under the additional hypothesis that F cannot be factored as $F=GH$ for some $H\in L[s]$ and some $G\in K[s]$ of degree at least 1 in s.*

Proof. First we note that if F satisfies the hypothesis in Theorem 2.4 then F cannot be factored as $F=G(s)H(s)$ with $G\in K[s]$ and $H\in L[s]$ linear on s with a non-constant coefficient. Indeed, $F(b_i)$ is powerful if and only if $H(b_i)$ is powerful or $G(b_i)=0$, and therefore such an F can be powerful for at most

$$W+\deg G\leqslant W+(n-1)<M$$

values of $s \in K$ (with W as in the previous lemma), contrary to the value of M in the statement of Theorem 2.4.

Suppose now that Theorem 2.4 is proved under the additional requirement; we will deduce the general case from this. For our argument below, it will be useful to write $M(n)$ for the value of M in the statement of Theorem 2.4 because we will consider different degrees n (although the field L is fixed).

Given F satisfying the hypotheses of Theorem 2.4 suppose that we can factor it as $F = GH$ for some $G \in K[s]$ and some $H \in L[s]$, and moreover assume that G is the largest (in degree) such factor. We can further assume that G, H are monic as polynomials on s and that H is not linear on s (by the first paragraph of this proof). Write

$$H = s^{n'} + \cdots + b_1 s^{n'-1} + b_0, \quad b_j \in L$$

and note that $G \in K[s]$ has degree $n - n'$. Since G can vanish at most for $n - n'$ values of $s \in K$, we know that $H(s)$ is μ-powerful in L for at least

$$M(n) - (n - n') \geqslant M(n')$$

values of s in K, with $\mu \geqslant \lambda \geqslant \lambda'$ where $\lambda' = \min\{n', \lambda\} \leqslant n'$. Observe that no irreducible factor of H can have multiplicity larger than λ' in the factorization of H.

Therefore, by maximality of G, we can apply to H the version of the theorem that we are assuming as proved. Therefore we must have $\mu = \lambda'$ and hence $\lambda = \mu = \lambda'$ (because $\mu \geqslant \lambda \geqslant \lambda'$), and moreover we also conclude that some irreducible factor of H has multiplicity exactly $\lambda' = \lambda$.

Finally we conclude that the theorem holds for F, namely, $\mu = \lambda$ and $F = GH$ with monic polynomials $H \in L[s]$ and $G \in K[s]$ such that the largest exponent in the factorization of H in $L[s]$ is exactly λ. □

Now we fix some F satisfying the hypotheses in Theorem 2.4. We factor

$$F = H_1^{m_1} \dots H_c^{m_c}$$

where $H_j \in L[s]$ are distinct, monic, irreducible and non-constant on s of degree d_j. By the above lemma, we can further assume that $H_j \notin K[s]$, that is, each H_j has at least one non-constant coefficient.

We define $d = \sum_{j=1}^{c} d_j$ and $m^+ = \max_j m_j \leqslant \lambda$. With this notation, we want to show

$$m^+ = \lambda = \mu \tag{1}$$

(observe that we already know $m^+ \leqslant \lambda \leqslant \mu$). Let $\Delta \in L$ be the discriminant of $G = \prod_j H_j$ and write

$$H_j(s) = s^{d_j} + c_{d_j-1,j} s^{d_j-1} + \cdots + c_{1j} s + c_{0j}$$

with $c_{ij} \in L$ the coefficients of H_j (hence, for fixed j not all the c_{ij} are constant).

For each $1 \leqslant j \leqslant c$, let ϕ_j be a zero of H_j and let $\pi_j : B_j \to B$ be a branched covering such that $L_j := K(B_j) = L(\phi_j)$. Note that each ϕ_j is non-constant since H_j has some non-constant coefficient and observe also that $d_j = [L_j : L]$ because H_j are irreducible.

If $z_0 \in B$ is not a zero of Δ and all the ϕ_j are regular above p then we say that z_0 is *good*, otherwise it is *bad*. Finally, define Θ to be the (analytic) divisor of bad points on B, without counting multiplicities. Observe that all the non-zero coefficients of Θ are 1 by definition. Recall that in the meromorphic case $N_\Theta(r)$ stands for the counting function of Θ; in the function field case we let $N_\Theta = \deg \Theta$.

In the function field case, Theorem 3.11 gives

$$(M-3d)h(\phi_j) \leqslant (M-3d_j)h(\phi_j) \leqslant \sum_{k=1}^{M} N_{\phi_j}^{(1)}(b_k) + 2(g-1) \tag{2}$$

and in the meromorphic case, Theorem 3.22 yields for every $\epsilon > 0$,

$$(M-3d-\epsilon)T_{\phi_j}(r) \leqslant (M-3d_j-\epsilon)T_{\phi_j}(r). \leqslant . \sum_{k=1}^{M} N_{\phi_j}^{(1)}(b_k, r). \tag{3}$$

We want an upper estimate for truncated counting functions in terms of heights.

Lemma 3.25. *In the function field case we have*

$$\sum_{k=1}^{M}\sum_{j=1}^{c} d_j N_{\phi_j}^{(1)}(b_k) \leqslant \frac{M}{\mu}\sum_{j=1}^{c} m_j d_j h(\phi_j) + dN_{\Theta}$$

and in the meromorphic case we have

$$\sum_{k=1}^{M}\sum_{j=1}^{c} d_j N_{\phi_j}^{(1)}(b_k, r) \leqslant \frac{M}{\mu}\sum_{j=1}^{c} m_j d_j T_{\phi_j}(r) + dN_{\Theta}(r) + \mathcal{O}(1).$$

Proof. Let $[b_k]$ be the divisor of the point b_k in $\mathbb{P}^1(K)$, and write

$$\phi_j^*[b_k] = \sum_{w\in B_j} n_{j,w,b_k} w$$

that is, $n_{j,w,b_k} = \operatorname{ord}_w^+(\phi_j - b_k)$. Observe that for fixed j and w, at most one of the n_{j,w,b_k} is non-zero (b_k are distinct), hence, for each $z \in B$ we have

$$\begin{aligned}\sum_{k=1}^{M}\sum_{j=1}^{c}\sum_{w\in\pi_j^{-1}(z)} \min\{1, n_{j,w,b_k}\} &= \sum_{j=1}^{c}\sum_{w\in\pi_j^{-1}(z)}\sum_{k=1}^{M}\min\{1, n_{j,w,b_k}\} \\ &\leqslant \sum_{j=1}^{c}\sum_{w\in\pi_j^{-1}(z)} 1 \leqslant \sum_{j=1}^{c} d_j = d\end{aligned}$$

therefore for all $z \in B$,

$$\sum_{k=1}^{M}\sum_{j=1}^{c}\sum_{w\in\pi_j^{-1}(z)} \min\{1, n_{j,w,b_k}\} \leqslant d. \tag{4}$$

Let z_0 be good, in particular all c_{ij} are regular at z_0 (by Lemmas 3.5 and 3.17). Let H_{jz_0} be the complex polynomial obtained by evaluating the coefficients of H_j at z_0 and observe that H_{jz_0} does not have repeated roots and for $i \neq j$ the polynomials H_{iz_0} and H_{jz_0} do not share roots (since Δ does

not vanish at z_0). It follows that for given k only one of the $H_{j_0}(b_k) \in L$ can have a zero at z_0, which happens if and only if $F(b_k)$ has a zero at z_0 (all the c_{ij} are regular at z_0). By Lemmas 3.5 and 3.17 we have some index j_0 such that

$$m_{j_0} n_{j_0,w_0,b_k} = m_{j_0} \operatorname{ord}_{z_0} H_{j_0}(b_k) = \sum_{j=1}^{c} m_j \operatorname{ord}_{z_0} H_j(b_k) = \operatorname{ord}_{z_0} F(b_k).$$

Therefore

$$\begin{aligned} \mu \min\{1, n_{j_0,w_0,b_k}\} &= \mu \min\{1, m_{j_0} n_{j_0,w_0,b_k}\} \\ &= \mu \min\{1, \operatorname{ord}_{z_0} F(b_k)\} \\ &\leqslant \operatorname{ord}_{z_0} F(b_k) = m_{j_0} n_{j_0,w_0,b_k} \end{aligned}$$

because $\operatorname{ord}_{z_0} F(b_k) = 0$ or $\operatorname{ord}_{z_0} F(b_k) \geqslant \mu$ by hypothesis. For fixed k we can have $n_{j,w,b_k} > 0$ for at most one pair (j, w) with $w \in \pi_j^{-1}(z_0)$, so we obtain

$$\sum_{j=1}^{c} \sum_{w \in \pi_j^{-1}(z_0)} \min\{1, n_{j,w,b_k}\} \leqslant \frac{1}{\mu} \sum_{j=1}^{c} \sum_{w \in \pi_j^{-1}(z_0)} m_j n_{j,w,b_k}.$$

Thus, adding over k we conclude that for $z_0 \in B$ good

$$\sum_{k=1}^{M} \sum_{j=1}^{c} \sum_{w \in \pi_j^{-1}(z_0)} \min\{1, n_{j,w,b_k}\} \leqslant \frac{1}{\mu} \sum_{k=1}^{M} \sum_{j=1}^{c} m_j \sum_{w \in \pi_j^{-1}(z_0)} n_{j,w,b_k}. \tag{5}$$

If we use (5) when $z_0 \in B$ is good and (4) when $z_0 \in B$ is bad, then the lemma follows just by adding over all $z_0 \in B$. We include the computation in the function field case; the steps in the case of meromorphic functions are exactly the same.

Let $\delta_z = 0$ if z is good and $\delta_z = 1$ if z is bad. In the function field case we have

$$\begin{aligned} \sum_{k=1}^{M} \sum_{j=1}^{c} d_j N_{\phi_j}^{(1)}(b_k) &= \sum_{k=1}^{M} \sum_{j=1}^{c} \sum_{z \in B} \sum_{w \in \pi_j^{-1}(z)} \min\{1, n_{j,w,b_k}\} \\ &\leqslant \frac{1}{\mu} \sum_{k=1}^{M} \sum_{j=1}^{c} m_j \sum_{z \in B} \sum_{w \in \pi_j^{-1}(z)} n_{j,w,b_k} + \sum_{k=1}^{M} \sum_{j=1}^{c} \sum_{z \in B} \delta_z \sum_{w \in \pi_j^{-1}(z)} \min\{1, n_{j,w,b_k}\} \\ &\leqslant \frac{1}{\mu} \sum_{k=1}^{M} \sum_{j=1}^{c} m_j \sum_{z \in B} \sum_{w \in \pi_j^{-1}(z)} n_{j,w,b_k} + \sum_{z \in B} \delta_z d \\ &= \frac{1}{\mu} \sum_{k=1}^{M} \sum_{j=1}^{c} m_j d_j h_{b_k}(\phi_j) + d N_{\Theta} \end{aligned}$$

and we conclude using the first main theorem. □

Using Lemma 3.4 one finds

$$N_\Theta \leqslant 2(d-1)\sum_{j=1}^{c} d_j h(\phi_j) + \sum_{j=1}^{c} \deg \phi_j^* \infty = (2d-1)\sum_{j=1}^{c} d_j h(\phi_j)$$

in the function field case, and similarly in the meromorphic case we use Lemma 3.15 to get

$$N_\Theta(r) \leqslant 2(d-1)\sum_{j=1}^{c} d_j T_{\phi_j}(r) + \sum_{j=1}^{c} d_j N_{\phi_j}(\infty, r) + \mathcal{O}(1) \leqslant (2d-1)\sum_{j=1}^{c} d_j T_{\phi_j}(r) + \mathcal{O}(1).$$

Now we use the previous two inequalities together with inequalities (2), (3) (added over j with weight d_j) and Lemma 3.25 to conclude

$$\left(M - \frac{m^+}{\mu}M - 3d - d(2d-1)\right)\sum_{j=1}^{c} d_j h(\phi_j) \leqslant 2d(g-1), \quad \text{and}$$

$$\left(M - \frac{m^+}{\mu}M - 3d - \epsilon - d(2d-1)\right)\sum_{j=1}^{c} d_j T_{\phi_j}(r). \leqslant .0$$

in the function field an meromorphic cases respectively. For function fields observe that

$$\sum_{j=1}^{c} d_j h(\phi_j) \geqslant c \geqslant 1,$$

and for meromorphic functions note that $\sum_{j=1}^{c} d_j T_{\phi_j}(r) \gg \log r$ as $r \to \infty$, so that we get

$$\left(1 - \frac{m^+}{\mu}\right)M \leqslant \begin{cases} 3d + d(2d-1) + 2d(g-1) & \text{for function fields,} \\ 3d + d(2d-1) + \epsilon & \text{for meromorphic functions.} \end{cases}$$

Using the convention $g = 1 + \epsilon$ for meromorphic functions (and perhaps using a different ϵ), we get

$$\left(1 - \frac{m^+}{\mu}\right)M \leqslant 2d(d+g) = 2(d-1)d + 2(g+1)d \tag{6}$$

in both cases. We have the following simple claim

Claim 3.26. *One has $n + 1 \geqslant m^+ + d$.*

Proof. Let j_0 be an index such that $m_{j_0} = m^+$, then

$$n = \sum m_j d_j \geqslant m^+ d_{j_0} + \sum_{j \neq j_0} d_j \geqslant m^+ + d_{j_0} - 1 + \sum_{j \neq j_0} d_j = m^+ - 1 + d. \qquad \square$$

Assuming that Eq. (1) fails for our F, one has $\lambda < \mu$ or $m^+ < \lambda$. Suppose first that $\mu \geqslant \lambda + 1$, then

$$1 - \frac{m^+}{\mu} \geqslant 1 - \frac{m^+}{\lambda + 1} \geqslant \begin{cases} \frac{d}{n+1} & \text{if } \lambda = n, \\ \frac{1}{\lambda+1} & \text{in general,} \end{cases}$$

where we used the previous claim for the first case. Secondly, if $\lambda \geqslant m^+ + 1$ and we use the bound $\mu \geqslant \lambda$ to obtain

$$1 - \frac{m^+}{\mu} \geqslant 1 - \frac{m^+}{\lambda} \geqslant \begin{cases} \frac{d-1}{n} & \text{if } \lambda = n, \\ \frac{1}{\lambda} & \text{in general,} \end{cases}$$

where one notes that $d \geqslant 2$ (otherwise F would be an n-th power but in this case $m^+ < \lambda \leqslant n$). So, in either case ($\lambda < \mu$ or $m^+ < \lambda$) we use inequality (6) to conclude

$$M \leqslant \left(1 - \frac{m^+}{\mu}\right)^{-1} 2d(d+g) \leqslant \begin{cases} 2(n+1)(d+g) \leqslant 2n^2 + 2(g+1)n + 2g & \text{if } \mu > \lambda = n, \\ 2nd + 2(g+1)n\frac{d}{d-1} \leqslant 2n^2 + 4(g+1)n & \text{if } m^+ < \lambda = n, \\ 2(\lambda+1)n(n+g) & \text{in general,} \end{cases}$$

which gives

$$M \leqslant \begin{cases} 2n^2 + 4(g+1)n & \text{if } \lambda = n, \\ 2(\lambda+1)n(n+g) & \text{in general.} \end{cases}$$

This is a contradiction with the actual value of M (for meromorphic functions let $\epsilon \to 0^+$ so that $g \to 1^+$). Therefore $m^+ = \lambda = \mu$ which proves Eq. (1), finishing the proof of Theorem 2.4.

4. Diophantine approximation on extensions of bounded degree

4.1. Algebraic points of the line

In this section we present some results and conjectures on Diophantine approximation along the same lines as our presentation of preliminary results on value distribution and Nevanlinna theory for function fields and meromorphic functions.

Given a number field L we write M_L for the set of (normalized) places of L, which can be written as the disjoint union of the set of non-Archimedean valuations M_L^0 and the set of Archimedean valuation M_L^∞. Elements of M_L^0 can be identified with maximal ideals $\mathfrak{P} \subseteq \mathcal{O}_L$ while the elements of M_L^∞ can be identified with embeddings $\sigma : L \to \mathbb{C}$ (here, the pairs of complex conjugate non-real embeddings are identified as just one embedding). For $x \in L$, if $\mathfrak{P} \in M_L^0$ we write $v_{\mathfrak{P}}(x) = \mathrm{ord}_{\mathfrak{P}}(x)$ for the normalized $\mathfrak{P}$-adic valuation, while for $\sigma \in M_L^\infty$ we write $v_\sigma(x) = -\log|\sigma(x)|$ (here, $|\cdot|$ is the usual absolute value on $\mathbb{C}$). In any case $v_p(0) = +\infty$, but we will always avoid this case for simplicity. Given L/K finite and $\mathfrak{P} \in M_L^0$, we write

$$\deg \mathfrak{P} = \log \# \frac{\mathcal{O}_L}{\mathfrak{P}}$$

and given $\sigma \in M_L^\infty$ we write

$$\deg \sigma = \begin{cases} 1 & \text{if } \sigma \text{ is real,} \\ 2 & \text{otherwise.} \end{cases}$$

We can extend deg additively to formal sums of places (divisors). This notion of degree is borrowed from Arakelov geometry and it is convenient for our discussion.

In general, if F is a real valued function, we write $F^+ = \max\{0, F\}$.

From now on we fix a base number field K and consider finite extensions of it. Let $x \in \bar{K}^*$ ($x \neq 0$) and choose L/K a finite extension such that $x \in L$. Define the *counting function*

$$N_K(x) = \frac{1}{[L:K]} \sum_{\mathfrak{P} \in M_L^0} v_{\mathfrak{P}}^+(x) \deg \mathfrak{P}$$

and the *proximity function*

$$m_K(x) = \frac{1}{[L:K]} \sum_{\sigma \in M_L^\infty} v_\sigma^+(x) \deg \sigma .$$

They are non-negative quantities that do not depend on the choice of L, and should be seen as 'proximity/counting functions of zeros'. For $x \in \bar{K}^*$ define the normalized *height* by

$$h_K(x) = m_K(x) + N_K(x).$$

Given $x \in \bar{K}^*$ we define the *truncated counting function* by

$$N_K^{(1)}(x) = \frac{1}{[K(x):K]} \sum_{\mathfrak{P} \in M_L^0} \min\{1, v_{\mathfrak{P}}^+(x)\} \deg \mathfrak{P}.$$

Note that this definition uses the field $K(x)$ and not just any finite extension L/K containing x.

We record here some facts that will be used in the proof of Theorem 2.1.

Lemma 4.1. *(See Lemmas 3.2, 3.13.) For $x, y, \in \bar{K}$ we have*

$$h_K(xy) \leqslant h_K(x) + h_K(y) + \mathcal{O}(1) \quad \text{and} \quad h_K(x+y) \leqslant h_K(x) + h_K(y) + \mathcal{O}(1)$$

where the implicit constants do not depend on x or y.

Lemma 4.2. *(See Lemmas 3.3, 3.14.) The height h_K on $\bar{K}^*$ is invariant under the action of* $\mathrm{Gal}(\bar{K}/K)$.

Lemma 4.3. *(See Lemmas 3.4, 3.15.) Let $G = H_1 \cdots H_c$ with $H_j \in K[s]$ distinct monic irreducible of degree d_j and let Δ be the discriminant of G. Let $x_j \in \bar{K}$ be a root of H_j and let $d = \sum_j d_j$. Then*

$$h_K(\Delta) \leqslant 2(d-1) \sum_{j=1}^{c} d_j h_K(x_j) + \mathcal{O}(1)$$

where the implied constant depends on the numbers d_j but does not depend on the particular H_j or x_j.

Proof. The proof is the same as in the case of function fields and meromorphic functions. We leave the details to the reader. □

Lemma 4.4. *Let $b \in K$ and $x \in \bar{K}$. Let $H \in K[s]$ be the monic minimal polynomial of x over K. Let $\mathfrak{p}$ be a non-zero prime in $\mathcal{O}_K$ and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the primes in $\mathcal{O}_{K(x)}$ above $\mathfrak{p}$. Then*

$$\sum_{i=1}^{r} \mathrm{ord}_{\mathfrak{P}}(x-b) \deg \mathfrak{P} = \mathrm{ord}_{\mathfrak{p}} H(b) \deg \mathfrak{p}.$$

Proof. This follows from Proposition 8.7 in [17] and the fact that $N_{K(x)/K}(b-x) = H(b)$ (where $N_{L/K}$ stands for the norm of the extension L/K). □

Lemma 4.5. *(See Lemmas 3.5, 3.17.) Let $L = K(x)$ for x algebraic over K with monic minimal polynomial $H \in K[s]$ and write Δ for the discriminant of H. Let $\mathfrak{p}$ be a non-zero prime in K and let $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ be the primes in $\mathcal{O}_L$ lying above $\mathfrak{p}$. If x is regular at the $\mathfrak{P}_i$ then the coefficients of H are regular at $\mathfrak{p}$. Moreover, if Δ does not vanish at $\mathfrak{p}$ then x can vanish at most at one $\mathfrak{P}_{i_0}$, and we have*:

- *if x does not vanish above $\mathfrak{p}$ then $\operatorname{ord}_{\mathfrak{P}} x = \operatorname{ord}_{\mathfrak{p}} H(0) = 0$ for each $\mathfrak{P}|\mathfrak{p}$;*
- *if x indeed vanishes at some (hence unique) $\mathfrak{P}_{i_0}$ then one has $\deg \mathfrak{P}_{i_0} = \deg \mathfrak{p}$ and $\operatorname{ord}_{\mathfrak{P}_{i_0}} x = \operatorname{ord}_{\mathfrak{p}} H(0)$.*

We remark that the second item is not only a statement about ramification; we can have $\deg \mathfrak{P} > \deg \mathfrak{p}$ for each $\mathfrak{P}|\mathfrak{p}$ even if $\mathfrak{p}$ does not ramify in L.

Proof. Most of the proof follows from classical facts that can be found, for instance, in [27]. We include a proof just to clarify the last point of the statement. Note that the computations are essentially the same as in the meromorphic counterpart of this lemma.

That the coefficients of H are regular (i.e. integral) at $\mathfrak{p}$ is clear after we express them in terms of the Galois conjugates of x.

For the second part, assume that Δ does not vanish at $\mathfrak{p}$. By the previous lemma with $b = 0$ we get

$$\sum_{i=1}^{r} \operatorname{ord}_{\mathfrak{P}_i}(x) \deg \mathfrak{P}_i = \operatorname{ord}_{\mathfrak{p}}\big(H(0)\big) \deg \mathfrak{p} \tag{7}$$

and since all the terms are non-negative we conclude that $H(0)$ vanishes at $\mathfrak{p}$ if and only if x vanishes at some $\mathfrak{P}_i$ (observe that $H(0) \neq 0$ in $\mathcal{O}_K$ since H is irreducible). If x does not vanish at any $\mathfrak{P}_i$ then the result is clear, so, without loss of generality we assume that x vanishes at $\mathfrak{P}_1$. Since Δ does not vanish at $\mathfrak{p}$ we obtain that H mod $\mathfrak{p}$ is separable. But $c_0 = H(0) = 0 \bmod \mathfrak{p}$ (because x vanishes at $\mathfrak{P}_1$) so we get that c_1 does not vanish at $\mathfrak{p}$. In particular c_1 does not vanish at $\mathfrak{P}_1$. Then the equation

$$x\big(x^{d-1} + c_{d-1}x^{d-2} + \cdots + c_1\big) = -c_0 = -H(0),$$

the fact that all the c_i are regular at $\mathfrak{p}$ and the assumption $x = 0 \bmod \mathfrak{P}_1$ show that

$$\operatorname{ord}_{\mathfrak{P}_1} x = \operatorname{ord}_{\mathfrak{P}_1} H(0) = e(\mathfrak{P}_1|\mathfrak{p}) \operatorname{ord}_{\mathfrak{p}} H(0) \geqslant \operatorname{ord}_{\mathfrak{p}} H(0)$$

where $e(\mathfrak{P}_1|\mathfrak{p})$ is the ramification index of $\mathfrak{P}_1$ above $\mathfrak{p}$. Also, note that the embedding $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{P}_1$ implies $\deg \mathfrak{P}_1 \geqslant \deg \mathfrak{p}$. So, we conclude from Eq. (7) (and the fact that all the terms in (7) are non-negative) that $\operatorname{ord}_{\mathfrak{P}_1} x = \operatorname{ord}_{\mathfrak{p}} H(0)$, $\deg \mathfrak{P}_1 = \deg \mathfrak{p}$ and moreover $\operatorname{ord}_{\mathfrak{P}_i} x = 0$ for $i > 1$. □

For L/K finite let $\mathcal{D}_{L/K}$ be the different of $\mathcal{O}_L/\mathcal{O}_K$. Define

$$d_K(L) = \frac{1}{[L:K]} \sum_{\mathfrak{P} \in M_L^0} \operatorname{ord}_{\mathfrak{P}}(\mathcal{D}_{L/K}) \deg \mathfrak{P}$$

and for $x \in \bar{K}$ define the *logarithmic discriminant*

$$d_K(x) = d_K\big(K(x)\big).$$

For the convenience of the reader, let us recall the conjecture of Vojta that we will need (see Conjecture 2.3 in [31], or Conjecture 25.3.b in [33]). This conjecture is analogue to Theorems 3.6 and 3.18.

Conjecture 4.6 *(Vojta). Let $b_1, \dots, b_q$ be distinct elements of K and let $n \geqslant 1$ be an integer. For every $\epsilon > 0$ there exists a constant C_ϵ depending on ϵ (and the previous data) such that the inequality*

$$(q - 2 - \epsilon)h_K(x) \leqslant d_K(x) + \sum_{j=1}^{q} N_K^{(1)}(x - b_j) + C_\epsilon$$

holds for all $x \in \bar{K}$ with $[K(x) : K] \leqslant n$ and $x \neq b_j$ for $1 \leqslant j \leqslant q$.

We remark that this formulation is slightly different to the statement in [31]. Our simpler definition of the truncated counting function does not take poles into account. However, since the b_j have a bounded number of poles, this contribution is absorbed by the error term leading to our formulation.

For our purposes, the logarithmic discriminant appearing in Conjecture 4.6 is not convenient and we need a bound for it in terms of heights.

Lemma 4.7. *(See Lemmas 3.9, 3.21.) Let K be a number field. Let $x \in \bar{K}$ and write $d = [K(x) : K]$. Then*

$$d_K(x) \leqslant (3d - 2)h_K(x) + \mathcal{O}(1)$$

where the implicit constant depends on K and the number $[K(x) : \mathbb{Q}]$ but not on the particular x.

Proof. Write $L = K(x)$ and let $H = s^d + a_{d-1}s^{d-1} + \cdots + a_0 \in K[s]$ be the minimal polynomial of x over K. Let S_x be the set of places in K above which x has poles, let T_x be the set of places in L lying above S and let $A = S_x^{-1}\mathcal{O}_K$. Note that $H \in A[s]$ by Lemma 4.5. We have

$$[L : K]d_K(x) = \sum_{\mathfrak{P} \in M_L^0} \operatorname{ord}_{\mathfrak{P}}(\mathcal{D}_{L/K}) \deg \mathfrak{P}.$$

We claim that

$$\sum_{\mathfrak{P} \in T_x} \operatorname{ord}_{\mathfrak{P}}(\mathcal{D}_{L/K}) \deg \mathfrak{P} = \sum_{\mathfrak{P} \in T_x} \big(e(\mathfrak{P}|\mathfrak{p}) - 1\big) \deg \mathfrak{P} + \mathcal{O}(1)$$

where $\mathfrak{p}$ is a prime of K below $\mathfrak{P}$ and the error term depends only on the numbers d and $[K : \mathbb{Q}]$. Indeed, if p is a rational prime with $p > d$ and $\mathfrak{P} - \mathfrak{p} - p$ is a tower of primes corresponding to $L - K - \mathbb{Q}$, then the residue characteristic at $\mathfrak{P}$ is coprime to $e(\mathfrak{P}|\mathfrak{p}) \leqslant d$ and thus $\operatorname{ord}_{\mathfrak{P}}(\mathcal{D}_{L/K}) = e(\mathfrak{P}|\mathfrak{p}) - 1$. For the remaining cases, note that we have at most $[L : \mathbb{Q}]d$ primes $\mathfrak{P}$ of L lying above a rational prime $p \leqslant d$, each of them satisfying $N\mathfrak{P} \leqslant p^{[L:\mathbb{Q}]} \leqslant d^{[L:\mathbb{Q}]}$, and for each such $\mathfrak{P}$ we use the bounds (cf. p. 58 in [27])

$$e(\mathfrak{P}|\mathfrak{p}) - 1 \leqslant \operatorname{ord}_{\mathfrak{P}}(\mathcal{D}_{L/K}) \leqslant e(\mathfrak{P}|\mathfrak{p}) - 1 + \operatorname{ord}_{\mathfrak{P}}\big(e(\mathfrak{P}|\mathfrak{p})\big)$$

together with

$$\operatorname{ord}_{\mathfrak{P}}\big(e(\mathfrak{P}|\mathfrak{p})\big) \leqslant e(\mathfrak{P}|p) \operatorname{ord}_p\big(e(\mathfrak{P}|\mathfrak{p})\big) \leqslant [L : \mathbb{Q}] \frac{\log d}{\log p}$$

to conclude the claimed equality with an error term at most

$$[L : \mathbb{Q}]d \cdot \log d^{[L:\mathbb{Q}]} \cdot [L : \mathbb{Q}] \frac{\log d}{\log 2}, \quad \text{where } [L : \mathbb{Q}] = [K : \mathbb{Q}]d.$$

From here, the proof continues along the same lines as in Lemma 3.9, as we just need to bound

$$\sum_{\mathfrak{P}\in T_x}\big(e(\mathfrak{P}|\mathfrak{p})-1\big)\deg\mathfrak{P}+\sum_{\mathfrak{P}\in M_L-T_x}\operatorname{ord}_{\mathfrak{P}}(\mathcal{D}_{L/K})\deg\mathfrak{P}.$$

Instead of Lemma 3.8 one has to use Proposition 4 on p. 49 of [13]. The only difference with the case of function fields is that the coefficients of the derivative of H are ja_j and not a_j, so there is a contribution to the height coming from the j's, but it is easily absorbed by the error term. □

4.2. Proof of Theorem 2.1

This section is devoted to prove Theorem 2.1. We begin with a reduction

Lemma 4.8. *With the notation as in Theorem 2.1 let $M'=M-n$ and E' the set of monic polynomials $F\in K[s]$ of degree n such that all irreducible factors of F have multiplicity strictly less than μ, and such that for each $1\leqslant k\leqslant M'$ the number $F(b_k)$ is* non-zero *and μ-powerful. Then it is enough to show that E' is finite.*

Proof. If one proves this restricted form of Theorem 2.1 then we can apply it to all subsets of size M' in $\{b_1,\dots,b_M\}$. As a polynomial of degree n has at most n zeros, each $F\in E$ belongs to some of the several E' that we obtain (there are at most $\binom{M}{M'}$ such sets E'). Since each E' is finite, so is E. □

Thus we work under the assumptions and notation from the previous lemma. We must show that E' is finite.

Let $F\in E'$ and factor F as $F=H_1^{m_1}\cdots H_c^{m_c}$ where $H_j\in K[s]$ are monic, irreducible, non-constant and distinct. Write $d_j=\deg H_j$, $d=\sum_j d_j$ and let Δ be the discriminant of $\prod_j H_j$. By hypothesis we have $m^+\leqslant\mu-1$ where $m^+:=\max_j m_j$. For each j let $\phi_j\in\bar{K}$ be a root of H_j and define $K_j=K(\phi_j)$.

Let S be the (finite) set of places on K consisting of

- the places at infinity,
- the poles of all the b_k, and
- the places above which two or more b_k meet.

Note that $\phi_j\neq b_k$ for all j,k because $F(b_k)\neq 0$ for each k, thus, assuming Conjecture 4.6 and using Lemma 4.7 we have that for every $\epsilon>0$ there is a constant C_ϵ not depending on F (and hence not depending on ϕ_j) such that for each j,

$$\big(M'-3d-\epsilon\big)h_K(\phi_j)\leqslant\big(M'-3d_j-\epsilon\big)h_K(\phi_j)\leqslant\sum_{k=1}^{M'}N^{(1)}_{K,S}(b_k-\phi_j)+C_\epsilon \tag{8}$$

where $N^{(1)}_{K,S}$ is defined as $N^{(1)}_K$ but omitting the contribution of the places above S (this contribution can be absorbed by C_ϵ because S is fixed, and is independent of ϕ_j). It is important to keep in mind that C_ϵ is a constant depending on ϵ, K, all the b_k, S and the number n (which is a bound for $[K(\phi_j):K]$), but the point is that C_ϵ does not depend on the particular F or ϕ_j as long as $F\in E'$.

We need an upper bound for the truncated counting functions. For this, let Θ be the reduced effective divisor on $B=\operatorname{Spec}\mathcal{O}_K$ supported on the points $\mathfrak{p}\in B$ such that $\mathfrak{p}\in S$, or Δ vanishes at $\mathfrak{p}$, or some ϕ_j has a pole above $\mathfrak{p}$ (we call such $\mathfrak{p}$ *bad* points, otherwise $\mathfrak{p}$ is *good*).

Lemma 4.9. *We have*

$$\sum_{k=1}^{M'}\sum_{j=1}^{c} d_j N_{K,S}^{(1)}(b_k-\phi_j) \leqslant \frac{M'}{\mu}\sum_{j=1}^{c} m_j d_j h_K(\phi_j) + d\deg\Theta + \mathcal{O}(1)$$

where the error depends just on K and n, but not on the particular $F \in E'$, and hence not on the ϕ_j's.

Remark 4.10. Since this lemma might be useful for some other applications, it worths noticing that it is unconditional; it does not depend on Conjecture 4.6.

Proof. Write $M_j^0 = M_{K_j}^0$ and let $T_j \subseteq M_j^0$ be the set of places above S. By definition of S and $N_{K,S}^{(1)}$ we have

$$N_{K,S}^{(1)}(b_k-\phi_j) = \frac{1}{d_j}\sum_{\mathfrak{p}\in M_K^0-S}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j} \min\{1, n_{j,k,\mathfrak{P}}\}\deg\mathfrak{P}$$

where $\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}$ denotes a sum extended over all primes in $\mathcal{O}_{K_j}$ dividing $\mathfrak{p}$, and

$$n_{j,k,\mathfrak{P}} = \operatorname{ord}_{\mathfrak{P}}^{+}(b_k-\phi_j) \quad \text{for } \mathfrak{P}\in M_j^0 - T_j.$$

If $\mathfrak{p}\in M_j^0 - S$ then no pair of the b_k agree at $\mathfrak{p}$ by definition of S; more precisely, they are regular at $\mathfrak{p}$ and have distinct reductions modulo $\mathfrak{p}$. Thus, for given ϕ_j and $\mathfrak{P}\in M_j^0 - T_j$ we see that at most one $n_{j,k,\mathfrak{P}}$ is non-zero (and hence positive) as k varies. Therefore, for $\mathfrak{p}\in M_K^0 - S$ we get

$$\begin{aligned}\sum_{k=1}^{M'}\sum_{j=1}^{c}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}\min\{1,n_{j,k,\mathfrak{P}}\}\deg\mathfrak{P} &= \sum_{j=1}^{c}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}\sum_{k=1}^{M'}\min\{1,n_{j,k,\mathfrak{P}}\}\deg\mathfrak{P}\\ &\leqslant \sum_{j=1}^{c}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}\deg\mathfrak{P} = \sum_{j=1}^{c}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j} f(\mathfrak{P}|\mathfrak{p})\deg\mathfrak{p}\\ &\leqslant \sum_{j=1}^{c} d_j\deg\mathfrak{p} = d\deg\mathfrak{p}\end{aligned}$$

where $f(\mathfrak{P}|\mathfrak{p})$ is the degree of the extension of residue fields $\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}}$. Thus for $\mathfrak{p}\in M_K^0 - S$ we have

$$\sum_{k=1}^{M'}\sum_{j=1}^{c}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}\min\{1,n_{j,k,\mathfrak{P}}\}\deg\mathfrak{P} \leqslant d\deg\mathfrak{p}. \tag{9}$$

Observe that for $\mathfrak{p}$ good one has that the discriminant of each H_j is non-zero at $\mathfrak{p}$; indeed, $H_1\cdots H_c$ has no repeated roots in the algebraic closure of the residue field $\kappa_{\mathfrak{p}}$, so the same holds for each H_j.

For $\mathfrak{p}$ good and given $1\leqslant k\leqslant M'$, $1\leqslant j\leqslant c$ we use Lemma 4.5 (with $H(s)=H_j(s+b_k)$, $x=\phi_j-b_k$ which is allowed since $\mathfrak{p}$ is good) to conclude that there exists $\mathfrak{P}_0|\mathfrak{p}$ in M_j^0 such that

$$\operatorname{ord}_{\mathfrak{p}} H_j(b_k)\deg\mathfrak{p} = \sum_{\mathfrak{P}|\mathfrak{p}}^{K_j} \operatorname{ord}_{\mathfrak{P}}(\phi_j - b_k)\deg\mathfrak{P} = \operatorname{ord}_{\mathfrak{P}_0}(\phi_j - b_k)\deg\mathfrak{P}_0 \tag{10}$$

where

$$\operatorname{ord}_{\mathfrak{P}}(\phi_j - b_k) = \begin{cases} \operatorname{ord}_{\mathfrak{p}} H_j(b_k) & \text{for } \mathfrak{P} = \mathfrak{P}_0, \\ 0 & \text{for } \mathfrak{P} \in M_j^0, \mathfrak{P}|\mathfrak{p}, \mathfrak{P} \neq \mathfrak{P}_0 \end{cases}$$

and moreover $\deg\mathfrak{P}_0 = \deg\mathfrak{p}$ if $\operatorname{ord}_{\mathfrak{P}}(\phi_j - b_k) > 0$.

Since $\mathfrak{p}$ is good, by Lemma 4.5 one knows that the coefficients of each H_j are regular at $\mathfrak{p}$. Moreover, since Δ does not vanish at $\mathfrak{p}$ the H_j do not share zeros at $\mathfrak{p}$. This implies that given $1 \leqslant k \leqslant M'$ we have some $1 \leqslant j_0 \leqslant c$ such that

$$m_{j_0} \operatorname{ord}_{\mathfrak{p}} H_{j_0}(b_k) = \begin{cases} \operatorname{ord}_{\mathfrak{p}} F(b_k) & \text{if } j = j_0, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, given $\mathfrak{p}$ good and $1 \leqslant k \leqslant M'$ we have some $1 \leqslant j_0 \leqslant c$ and for this index j_0 we have a prime $\mathfrak{P}_0 \in K_{j_0}$ dividing $\mathfrak{p}$ with the above properties, which allows us to perform the following computation (some of the steps are explained below):

$$\begin{aligned}
&\sum_{j=1}^{c} m_j \sum_{\mathfrak{P}|\mathfrak{p}}^{K_j} \operatorname{ord}_{\mathfrak{P}}(\phi_j - b_k)\deg\mathfrak{P} \\
&\quad = \sum_{j=1}^{c} m_j \operatorname{ord}_{\mathfrak{p}} H_j(b_k)\deg\mathfrak{p} \quad \text{by (10)} \\
&\quad = m_{j_0} \operatorname{ord}_{\mathfrak{p}} H_{j_0}(b_k)\deg\mathfrak{p} = \operatorname{ord}_{\mathfrak{p}} F(b_k)\deg\mathfrak{p} \\
&\quad \geqslant \mu \min\{1, \operatorname{ord}_{\mathfrak{p}} F(b_k)\}\deg\mathfrak{p} = \mu \min\{1, m_{j_0} \operatorname{ord}_{\mathfrak{p}} H_{j_0}(b_k)\}\deg\mathfrak{p} \\
&\quad = \mu \min\{1, \operatorname{ord}_{\mathfrak{p}} H_{j_0}(b_k)\}\deg\mathfrak{p} \\
&\quad = \mu \min\{1, \operatorname{ord}_{\mathfrak{p}} H_{j_0}(b_k)\}\deg\mathfrak{P}_0 \qquad (*) \\
&\quad = \mu \min\{1, \operatorname{ord}_{\mathfrak{P}_0}(\phi_{j_0} - b_k)\}\deg\mathfrak{P}_0 \\
&\quad = \mu \sum_{j=1}^{c} \sum_{\mathfrak{P}|\mathfrak{p}}^{K_j} \min\{1, \operatorname{ord}_{\mathfrak{P}}(\phi_j - b_k)\}\deg\mathfrak{P}.
\end{aligned}$$

Observe that the inequality from the second line to the third line of the above computation is exactly the point where we use the hypothesis that for every b_k the number $F(b_k)$ is n-powerful (and we also used the assumption that $\mathfrak{p}$ is good, hence $\operatorname{ord}_{\mathfrak{p}} F(b_k) \geqslant 0$ because all the b_k and coefficients of H_j's are regular at $\mathfrak{p}$). Let us justify $(*)$; as explained before, if $\operatorname{ord}_{\mathfrak{p}} H_{j_0}(b_k) > 0$ then $\phi_{j_0} - b_k$ vanishes above $\mathfrak{p}$ and hence $\deg\mathfrak{P}_0 = \deg\mathfrak{p}$. On the other hand, if $\operatorname{ord}_{\mathfrak{p}} H_{j_0}(b_k) = 0$ then the equality in $(*)$ just states $0 = 0$ and is trivially true.

If $\mathfrak{p}$ is good then both ϕ_j and b_k are regular at the primes $\mathfrak{P} \in M_j^0$ lying above $\mathfrak{p}$ so that $n_{j,k,\mathfrak{P}} = \operatorname{ord}_{\mathfrak{P}}(\phi_j - b_k)$, and we conclude

$$\mu \sum_{j=1}^{c} \sum_{\mathfrak{P}|\mathfrak{p}}^{K_j} \min\{1, n_{j,k,\mathfrak{P}}\}\deg\mathfrak{P} \leqslant \sum_{j=1}^{c} m_j \sum_{\mathfrak{P}|\mathfrak{p}}^{K_j} n_{j,k,\mathfrak{P}}\deg\mathfrak{P}$$

which implies that for $\mathfrak{p}$ good we have

$$\sum_{k=1}^{M'}\sum_{j=1}^{c}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}\min\{1,n_{j,k,\mathfrak{P}}\}\deg\mathfrak{P}\leqslant\frac{1}{\mu}\sum_{k=1}^{M'}\sum_{j=1}^{c}m_j\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}n_{j,k,\mathfrak{P}}\deg\mathfrak{P}. \tag{11}$$

Finally we can conclude in the same way as for function fields and meromorphic functions. We include the computation for the sake of completeness. For $\mathfrak{p}\in M_K^0-S$ put $\delta_{\mathfrak{p}}=0$ if $\mathfrak{p}$ is good and $\delta_{\mathfrak{p}}=1$ otherwise. With this notation, using the inequalities (9) and (11) we get

$$\begin{aligned}
&\sum_{k=1}^{M'}\sum_{j=1}^{c}d_jN_{K,S}^{(1)}(b_k-\phi_j)\\
&\quad=\sum_{k=1}^{M'}\sum_{j=1}^{c}\sum_{\mathfrak{p}\in M_K^0-S}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}\min\{1,n_{j,k,\mathfrak{P}}\}\deg\mathfrak{P}\\
&\quad\leqslant\frac{1}{\mu}\sum_{k=1}^{M'}\sum_{j=1}^{c}m_j\sum_{\mathfrak{p}\in M_K^0-S}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}n_{j,k,\mathfrak{P}}\deg\mathfrak{P}+\sum_{k=1}^{M'}\sum_{j=1}^{c}\sum_{\mathfrak{p}\in M_K^0-S}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}\delta_{\mathfrak{p}}\min\{1,n_{j,k,\mathfrak{P}}\}\deg\mathfrak{P}\\
&\quad\leqslant\frac{1}{\mu}\sum_{k=1}^{M'}\sum_{j=1}^{c}m_jd_jN_K(b_k-\phi_j)+\sum_{\mathfrak{p}\in M_K^0-S}\delta_{\mathfrak{p}}\sum_{k=1}^{M'}\sum_{j=1}^{c}\sum_{\mathfrak{P}|\mathfrak{p}}^{K_j}\min\{1,n_{j,k,\mathfrak{P}}\}\deg\mathfrak{P}\\
&\quad\leqslant\frac{1}{\mu}\sum_{k=1}^{M'}\sum_{j=1}^{c}m_jd_jN_K(b_k-\phi_j)+\sum_{\mathfrak{p}\in M_K^0-S}\delta_{\mathfrak{p}}d\deg\mathfrak{p}\\
&\quad\leqslant\frac{1}{\mu}\sum_{k=1}^{M'}\sum_{j=1}^{c}m_jd_jh_K(b_k-\phi_j)+\sum_{\mathfrak{p}\in M_K^0-S}\delta_{\mathfrak{p}}d\deg\mathfrak{p}\\
&\quad\leqslant\frac{M'}{\mu}\sum_{j=1}^{c}m_jd_jh_K(\phi_j)+d\deg\Theta+\mathcal{O}(1)
\end{aligned}$$

where the error term comes form an application of Lemma 4.1. This finishes the proof. □

From now on it is implicit that the error terms may depend on K, $b_1,\dots,b_{M'}$, the integer n and the real number $\epsilon>0$, but they do not depend on the particular $F\in E'$ (and in particular, the error terms do not depend on ϕ_j, H_j, d_j or Δ). We leave to the reader the task of verifying that this is indeed the case – dependences of error terms are explicitly stated in each of our previous lemmas and inequalities. Since K, $b_1,\dots,b_{M'}$ and n are fixed but $\epsilon>0$ still has to be chosen, we will only indicate explicitly the dependence of the error terms on ϵ.

Next we give an upper bound for $\deg\Theta$.

Lemma 4.11. *We have*

$$\deg\Theta\leqslant(2d-1)\sum_{j=1}^{c}d_jh_K(\phi_j)+\mathcal{O}(1).$$

Proof. As S is fixed, the contribution to $\deg \Theta$ coming from places in S can be absorbed in a bounded error term. Let $S_j \subseteq M_K^0$ be the set of places lying below poles of ϕ_j, we have

$$\deg \Theta \leqslant \sum_{j=1}^{c} \sum_{\mathfrak{p} \in S_j} \deg \mathfrak{p} + N_K(\Delta) + \mathcal{O}(1) \leqslant \sum_{j=1}^{c} \sum_{\mathfrak{p} \in S_j} \deg \mathfrak{p} + h_K(\Delta) + \mathcal{O}(1)$$

where the sum counts for poles of the ϕ_j and $N_K(\Delta)$ counts for zeros of Δ. Note that

$$\sum_{j=1}^{c} \sum_{\mathfrak{p} \in S_j} \deg \mathfrak{p} \leqslant \sum_{j=1}^{c} d_j h_K\big(\phi_j^{-1}\big) = \sum_{j=1}^{c} d_j h_K(\phi_j)$$

because $h_K(x^{-1}) = h_K(x)$ for $x \in \bar{K}^*$, and finally we conclude by Lemma 4.3. □

By inequality (8), Lemma 4.9 and Lemma 4.11 we have

$$\left(\left(1 - \frac{m^+}{\mu}\right) M' - \big(2d^2 + 2d + \epsilon\big)\right) \sum_{j=1}^{c} d_j h_K(\phi_j) \leqslant \mathcal{O}_\epsilon(1).$$

Similar to the case of functions, one has

$$1 - \frac{m^+}{\mu} \geqslant \begin{cases} \frac{d-1}{n} & \text{if } \mu = n, \\ \frac{1}{\mu} & \text{in general.} \end{cases}$$

Observe that in the first case $d - 1 \geqslant 1$, for otherwise $d = 1$ and this forces $\mu > m^+ = n \geqslant \mu$, which is not possible. Now recall that

$$M' = M - n = \begin{cases} 2n^2 + 8n + 1 & \text{if } \mu = n, \\ 2\mu n(n+1) + 1 & \text{in general} \end{cases}$$

(in the sense that if we are not assuming $\mu = n$ then we use the second value for M') so that if we assume $\mu = n$ then

$$\begin{aligned} M'\left(1 - \frac{m^+}{\mu}\right) - \big(2d^2 + 2d + \epsilon\big) &\geqslant \big(2n^2 + 8n + 1\big)\frac{d-1}{n} - \big(2d^2 + 2d + \epsilon\big) \\ &= \frac{d-1}{n} + (d-1)\left(2n + 8 - \left(2d + 4 + \frac{4}{d-1}\right)\right) - \epsilon \\ &\geqslant \frac{1}{n} - \epsilon \end{aligned}$$

and in general (i.e. $2 \leqslant \mu \leqslant n$)

$$M'\left(1 - \frac{m^+}{\mu}\right) - \big(2d^2 + 2d + \epsilon\big) \geqslant \big(2\mu n(n+1) + 1\big)\frac{1}{\mu} - \big(2d^2 + 2d + \epsilon\big) \geqslant \frac{1}{\mu} - \epsilon \geqslant \frac{1}{n} - \epsilon.$$

Thus, in either case we conclude

$$\left(\frac{1}{n}-\epsilon\right)\sum_{j=1}^{c} d_j h_K(\phi_j) \leqslant \mathcal{O}_\epsilon(1)$$

and fixing any $\epsilon < 1/n$ (say $\epsilon = 1/(n+1)$) we see that the quantity

$$\sum_{j=1}^{c} d_j h_K(\phi_j)$$

is bounded from above uniformly for $F \in E'$. As the degrees d_j of the ϕ_j are also uniformly bounded by n we use Northcot's theorem to conclude that E' is finite, finishing the proof of Theorem 2.1.

Remark 4.12. In several applications one uses Northcot's theorem only for points of a fixed number field having bounded height, but for this application it is crucial that Northcot's theorem works for points of bounded degree and bounded height, without fixing the field.

5. Logic

First we give a proof of Theorem 2.12.

Proof. Write $\Delta^{(n)}$ for the n-th iterate of the operator $\Delta\{u_i\}_{i=1}^{M} = \{u_{i+1} - u_i\}_{i=1}^{M-1}$. Assuming Conjecture 1.4, the second item of Theorem 2.8 implies that the positive-existential $\mathcal{L}$-formula $\Psi[u_1, \ldots, u_{M_0}]$

$$\left(\bigwedge_{1\leqslant i\leqslant M_0} P(u_i)\right) \wedge \left(\Delta^{(n)}\{u_i\}_i = \{n!\}_i\right)$$

is satisfied for $\{u_i\}_i \subseteq R$ if and only if there is some $\nu \in K$ such that $u_j = (j+\nu)^n$ for each j. As R is integrally closed in K, one actually has $\nu \in R$. Observe that

$$\Delta^{(n-1)}\left\{(j+\nu)^n\right\}_j = \Delta^{(n-1)}\left\{j^n + nj^{n-1}\nu\right\}_j = \left\{n!j + \frac{n!(n-1)}{2} + n!\nu\right\}_j$$

in particular

$$\Delta^{(n-1)}\left\{(j+\nu)^n\right\}_{j=1}^{n} = n! + \frac{n!(n-1)}{2} + n!\nu.$$

Therefore, the formula

$$\Phi[x, y] : \exists\{u_i\}_{i=1}^{M_0}\Psi[u_1, \ldots, u_{M_0}] \wedge \left(n!x + \frac{n!(n-1)}{2} = \Delta^{(n-1)}\{u_j\}_{j=1}^{n}\right) \wedge y = u_1$$

defines the function $x \mapsto y = x^n$ in a positive-existential way over the language $\mathcal{L}$. At this point, defining multiplication in a positive existential way is standard, see for example [21]. We indicate here the main steps:

Let $\mathcal{P}_n \subseteq \mathbb{Z}[x]$ be the set of polynomials with integer coefficients of degree at most n. $\mathcal{P}_n$ is a free $\mathbb{Z}$ module of rank $n+1$ and the polynomials $x^n, (x+1)^n, \ldots, (x+n)^n$ are linearly independent. So, there are integers $a_0, \ldots, a_n, b$ with $b \neq 0$ depending only on n such that

$$bx^2 = a_0 x^n + a_1 (x+1)^n + \cdots + a_n (x+n)^n.$$

This relation allows one to define $x \mapsto y = x^2$ with a positive existential $\mathcal{L}$-formula over R. Then one can define multiplication $xy = z$ by observing that $xy = z \Leftrightarrow x^2 + 2z + y^2 = (x+y)^2$. □

One last remark on this argument; the desired conclusion follows from the fact that one can express the function $x \mapsto x^n$. Note that the language $\mathcal{L}$ might allow one to say *a priori* that some element $u \in R$ is an n-th power (in the case that P is interpreted in this way), however, this is very different to being able to express the function $x \mapsto x^n$.

Finally, the proof of Theorem 2.16 is very similar to the above proof but one has to be careful with the case of constant coefficients. The straightforward adaptation of the previous argument (using Corollary 2.10 instead of 2.8) would give a positive existential $\mathcal{L}$-definition $\varpi[x, y]$ of the relation

$$y = x^n \quad \text{or} \quad x, y \in K.$$

Then the formula

$$\varpi[x, y] \wedge \varpi\left[\alpha x, \alpha^n y\right]$$

(here n is fixed and $\alpha^n = \alpha\alpha \cdots \alpha n$ times) gives a positive existential definition for $y = x^n$, and the rest of the argument is the same.

Acknowledgments

The author thanks Paulo Ribenboim for driving his attention to some useful references. He is also in debt to Tzu-Yueh Julie Wang for several suggestions that improved some of the results in this paper. The author wants to express his gratitude to Ram Murty and Xavier Vidaux for reading this manuscript and suggesting several changes that improved the presentation. Finally, the careful revision and suggestions made by the anonymous referee are gratefully acknowledged.

References

[1] D. Allison, On square values of quadratics, Math. Proc. Cambridge Philos. Soc. 99 (3) (1986) 381–383.
[2] T. An, J. Wang, Hensley's problem for complex and non-Archimedean meromorphic functions, J. Math. Anal. Appl. 381 (2) (2011) 661–677.
[3] T. An, H. Huang, J. Wang, Generalized Büchi's problem for algebraic functions and meromorphic functions, Math. Z. 273 (1–2) (2013) 95–122, http://dx.doi.org/10.1007/s00209-012-0997-9.
[4] A. Bremner, On square values of quadratics, Acta Arith. 108 (2) (2003) 95–111.
[5] J. Browkin, J. Brzeziński, On sequences of squares with constant second differences, Canad. Math. Bull. 49 (4) (2006) 481–491.
[6] W. Cherry, S. Lang, Topics in Nevanlinna Theory, Lecture Notes in Math., vol. 1433, Springer, Berlin, ISBN 3-540-52785-0, 1990.
[7] W. Cherry, Z. Ye, Nevanlinna's Theory of Value Distribution; The Second Main Theorem and Its Error Terms, Springer, Berlin, 2001.
[8] H. Davenport, D.J. Lewis, A. Schinzel, Polynomials of certain special types, Acta Arith. 9 (1964) 107–116.
[9] J. Denef, The Diophantine problem for polynomial rings and fields of rational functions, Trans. Amer. Math. Soc. 242 (1978) 391–399.
[10] N. Garcia-Fritz, Representation of powers by polynomials and the language of powers, J. Lond. Math. Soc. 87 (2) (2013) 347–364, http://dx.doi.org/10.1112/jlms/jds052.
[11] K.H. Kim, F. Roush, Diophantine unsolvability over p-adic function fields, J. Algebra 176 (1) (1995) 83–110.
[12] I. Kra, On the ring of holomorphic functions on an open Riemann surface, Trans. Amer. Math. Soc. 132 (1) (1968) 231–244.

[13] S. Lang, Diophantine Geometry, Intersci. Tracts in Pure Appl. Math., vol. 11, Interscience Publishers (a division of John Wiley & Sons), New York, London, 1962, x+170 pp.
[14] L. Lipshitz, Quadratic forms, the five square problem, and Diophantine equations, in: S. MacLane, Dirk Siefkes (Eds.), The Collected Works of J. Richard Büchi, Springer, 1990, pp. 677–680.
[15] Y. Matiyasevic, Enumerable sets are diophantine, Dokl. Akad. Nauk SSSR 191 (1970) 279–282; English translation: Sov. Math. Dokl. 11 (1970) 354–358.
[16] B. Mazur, Questions of decidability and undecidability in number theory, J. Symbolic Logic 59 (2) (1994) 353–371.
[17] J.S. Milne, Algebraic number theory, Lecture notes for a course given at the University of Michigan, available on-line at http://www.jmilne.org/math/CourseNotes/ant.html.
[18] L. Moret-Bailly, A. Shlapentokh, Diophantine undecidability of holomorphy rings of function fields of characteristic 0, Ann. Inst. Fourier (Grenoble) 59 (5) (2009) 2103–2118.
[19] H. Pasten, An extension of Büchi's Problem for polynomial rings in zero characteristic, Proc. Amer. Math. Soc. 138 (2010) 1549–1557.
[20] H. Pasten, T. Pheidas, X. Vidaux, A survey on Buchi's problem: new presentation and open problems, in: Proceedings of the Hausdorff Institute of Mathematics, Zap. POMI Tom 377 (2010) 111–140.
[21] T. Pheidas, X. Vidaux, Extensions of Büchi's problem: Questions of decidability for addition and n-th powers, Fund. Math. 185 (2005) 171–194.
[22] T. Pheidas, X. Vidaux, The analogue of Büchi's problem for cubes in rings of polynomials, Pacific J. Math. 238 (2) (2008) 349–366.
[23] T. Pheidas, X. Vidaux, Corrigendum: The analogue of Büchi's problem for rational functions, J. Lond. Math. Soc. (2) 82 (1) (2010) 273–278, http://dx.doi.org/10.1112/jlms/jdq002.
[24] R.G.E. Pinch, Squares in quadratic progression, Math. Comp. 60 (202) (1993) 841–845.
[25] P. Ribenboim, Polynomials whose values are powers, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II, J. Reine Angew. Math. 268/269 (1974) 34–40.
[26] M. Ru, Nevanlinna Theory and Its Relation to Diophantine Approximation, World Scientific, River Edge, NJ, 2001.
[27] J.-P. Serre, Local Fields, Grad. Texts in Math., vol. 67, Springer, New York, Heidelberg, Berlin, 1979, translation of Corps Locaux by M. Greenberg.
[28] A. Shinzel, R. Tijdeman, On the equation $y^m = P(x)$, Acta Arith. 31 (2) (1976) 199–204.
[29] A. Shlapentokh, Hilbert's Tenth Problem. Diophantine Classes and Extensions to Global Fields, New Math. Monogr., vol. 7, Cambridge University Press, Cambridge, 2007, ISBN 978-0-521-83360-8, 0-521-83360-0-521-4, xiv+320 pp.
[30] X. Vidaux, Polynomial parametrizations of length 4 Büchi sequences, Acta Arith. 150 (3) (2011) 209–226.
[31] P. Vojta, A more general abc conjecture, Int. Math. Res. Not. IMRN 1998 (1998) 1103–1116.
[32] P. Vojta, Diagonal quadratic forms and Hilbert's tenth problem, Contemp. Math. 270 (2000) 261–274.
[33] P. Vojta, Diophantine approximation and Nevanlinna theory, in: Arithmetic Geometry, in: Lecture Notes in Math., vol. 2009, Springer, Berlin, 2011, pp. 111–224.
[34] P.G. Walsh, On a conjecture of Schinzel and Tijdeman, in: Number Theory in Progress, vol. 1, Zakopane-Kos'cielisko, 1997, de Gruyter, Berlin, 1999, pp. 577–582.
[35] K. Zahidi, Hilbert's tenth problem for rings of rational functions, Notre Dame J. Form. Log. 43 (3) (2002) 181–192, 2003.