REPRESENTATION OF SQUARES BY MONIC SECOND DEGREE POLYNOMIALS IN THE FIELD OF p-ADIC MEROMORPHIC FUNCTIONS

HECTOR PASTEN

Abstract. We prove a result on the representation of squares by monic second degree polynomials in the field of p-adic meromorphic functions in order to solve positively Büchi's n squares problem in this field. Using this result, we prove the non-existence of an algorithm to decide whether a system of diagonal quadratic forms over $\mathbb{Z}[z]$ represents or not in the ring of p-adic entire functions (in the variable z) a given vector of polynomials in $\mathbb{Z}[z]$, and a similar result for p-adic meromorphic functions when the systems allow vanishing conditions on the unknowns. This improves the known negative answers for the analogue of Hilbert's Tenth Problem for these structures. We also improve some results by Vojta concerning the case of complex meromorphic functions, the case of function fields and finally the case of number fields, and show an intimate relation of the latter with Bombieri's conjecture for surfaces over number fields.

Contents

1. Introduction

In 1970, after the work developed by M. Davis, H. Putnam and J. Robinson, Hilbert's Tenth Problem was answered negatively by Y. Matiyasevic (see [11] or [5]). In logical terms, it was shown that the positive existential theory of $\mathbb{Z}$ in the language of rings $\mathcal{L}_R = \{0, 1, +, \cdot\}$ is undecidable, which means that there exists no algorithm to decide whether a system of diophantine equations (or equivalently, a single diophantine equation) has integer solutions or not. For a general survey on Hilbert's Tenth Problem and extensions of it, see for example [17] or [19] (see [22] for results about number fields and function fields).

Soon after the problem was solved, J. R. Büchi proved in an unpublished work (see [9] or [12]) that a positive answer to a certain problem in Number Theory (which we write here $\mathbf{BP}(\mathbb{Z})$) would allow

2010 *Mathematics Subject Classification.* Primary 11U05, 30D35; Secondary 30D30.

Key words and phrases. p-adic meromorphic, Büchi's problem, Hilbert's tenth problem.

to show that there exists no algorithm to decide whether a system of diagonal quadratic forms over $\mathbb{Z}$ represents or not a given vector of integers.

The number-theoretical problem $\mathbf{BP}(\mathbb{Z})$ is based on the following observation. If we consider the first difference of a sequence of consecutive integer squares (for example $1, 4, 9, 16$), we obtain a sequence of consecutive odd integers (in our example $3, 5, 7$). Hence, the second difference is the constant sequence (2). One may ask whether a sequence of squares having second difference equal to the constant sequence (2) must be a sequence of consecutive squares. The sequence $6^2, 23^2, 32^2, 39^2$ shows that it is not true in general.

Problem 1.1 ($\mathbf{BP}(\mathbb{Z})$)**.** *Does there exist an integer M such that the following happens: If the second difference of a sequence $(x_i^2)_{i=1}^M$ of integer squares is constant and equal to 2, then there exists an integer ν such that $x_i^2 = (\nu + i)^2$ for $i = 1, \ldots, M$ (that is, the squares must be consecutive).*

This problem became known as the *n Squares Problem* or *Büchi's Problem.* Numerical evidence suggests that $M = 5$ should work (see for example [18]), but $\mathbf{BP}(\mathbb{Z})$ still is an open problem.

Assuming a positive answer to $\mathbf{BP}(\mathbb{Z})$, Büchi was able to prove, using the negative answer given to Hilbert's tenth problem and assuming a positive answer to $\mathbf{BP}(\mathbb{Z})$, the non-existence of an algorithm for the problem of representation of a vector of integers by diagonal quadratic forms. The problem of the existence of such an algorithm can be shown to be equivalent to the problem of decidability of the positive existential theory of $\mathbb{Z}$ over the language $\mathcal{L}_2 = \{0, 1, +, P_2\}$, where $P_2(x)$ is interpreted as 'x is a square'.

In order to get similar consequences in Logic for other rings of interest, and motivated by the arithmetical interest of the problem, several authors have studied variants of $\mathbf{BP}(\mathbb{Z})$. A natural thing to do is to replace the ring $\mathbb{Z}$ by another commutative ring A with unit. Depending on the ring, we sometimes need to make additional hypothesis in the statement of $\mathbf{BP}(A)$:

- If A is a ring of functions of characteristic zero in the variable z, then we ask for at least one x_i to be non-constant.
- If A is a ring of positive characteristic, then we ask M to be at most the characteristic of A.

For variants on Büchi's problem (for example, considering sequences whose second difference is a constant sequence (m) for some m not necessarily $= 2$), see [1] and [3]. For the problem $\mathbf{BP}(A)$ with A a ring, we know that the following cases (among various others) have a positive answer: $\mathbf{BP}^2(\mathbb{F}_p)$ with $p > 2$ (see [7]), $\mathbf{BP}^2(\mathcal{M})$ where $\mathcal{M}$ is the field of complex meromorphic functions (see [26]), $\mathbf{BP}^2(F(z))$ where $F(z)$ is the field of rational functions over a field of characteristic 0 or $p \geq 19$ (see [15, 16]). Moreover, Büchi's problem has a positive answer even in the case of function fields of curves (see [26] for the characteristic zero case and see [23] for 'large enough' positive characteristic). Under a conjecture in Diophantine Geometry, Vojta showed in [26] that $\mathbf{BP}^2(\mathbb{Q})$ would have a positive answer (hence $\mathbf{BP}^2(\mathbb{Z})$ would have a positive answer). See [14] for a survey on Büchi's problem and its variants.

The positive existential $\mathcal{L}_2$-theory of a ring is usually much weaker than its positive existential $\mathcal{L}_R$-theory. But when Büchi's problem has a positive answer for a ring A then those theories for A are (in general) equivalent. This is what happens for example for p-adic analytic functions and for p-adic meromorphic functions (see Section 3.2).

We will solve $\mathbf{BP}(A)$ for some rings of functions, namely, the field of p-adic meromorphic functions, the field of complex meromorphic functions and function fields of curves in characteristic zero by showing in each case a somewhat stronger result on representation of squares by polynomials, in the spirit of the following:

Given a ring B and a subset A of B, there exists a constant M satisfying the following condition: For any set $\{a_1, \ldots, a_M\}$ of M elements in A, there exists a 'small' set $E \subseteq B[X]$ such that, if a monic polynomial of degree two $P \in B[X]$ has the property that each $P(a_i)$ is a square in B, then $P \in E$ or P is a square in $B[X]$.

We will prove such a result for number fields, but assuming that the following conjecture by Bombieri holds for surfaces.

Conjecture 1.2 (Bombieri)**.** *If X is a smooth projective variety of general type defined over a number field $K/\mathbb{Q}$, then $X(K)$ is contained in a proper Zariski closed set of X.*

The results for function fields, complex meromorphic functions and number fields are based in Vojta's work on Büchi's problem (see [26]), where he solved Büchi's problem for complex meromorphic functions, function fields and (assuming the above conjecture) for number fields. The results related to the p-adic setting are proved in a completely different way from Vojta's proof for the complex meromorphic case, and indeed, our proof is closer to the ideas in [15].

On the one hand, from an arithmetic point of view, our interest is not only in solving Büchi's problem in some structures, but also understand *how many times a second degree polynomial which is not a square, can represent a square.*

On the other hand, from the point of view of Logic, our main interest in solving Büchi's problem for p-adic meromorphic functions is that some analogues of Hilbert's Tenth Problem for the ring of p-adic analytic functions (see [10]) and the field of p-adic meromorphic functions (see [24]) have been proved to be undecidable (those problems are open in the complex case). Those results allow us, in the p-adic case, to derive consequences in Logic from Büchi's problem. This will be explained below in Section 3.2.

We also refer the reader to [6] where is developed a general method used to solve negatively analogues of Hilbert's Tenth Problem for rings of functions.

2. Acknowledgements

I would like to express my gratitude to Alain Escassut and Jacqueline Ojeda for carefully reading the results and proofs related to p-adic complex analysis and for all their useful suggestions, to Ricardo Baeza for his reading of some results in p-adic analysis and connections with Logic, and to Antonio Laface for his reading of the geometric results and all the useful comments he made. It is also a pleasure for me to thank Thanases Pheidas and Xavier Vidaux for suggesting me the problem and for the clarifying explanations in Logic they provided me, particularly in the context of Hilbert's Tenth Problem and Büchi's problem, and for the several suggestions they gave me during the writing of this paper.

3. Main results

In this section, we present the statements of the results proven in this work.

3.1. Representation of squares in the field of p-adic meromorphic functions.

Let p be a prime number and let $\mathbb{C}_p$ be the field of p-adic complex numbers (the completion of the algebraic closure of the field $\mathbb{Q}_p$ of p-adic numbers). Throughout the paper, one can replace $\mathbb{C}_p$ by any algebraically closed field of characteristic zero, complete with respect to a non-trivial non-Archimedean valuation.

Let $\mathcal{A}_p$ be the ring of entire functions over $\mathbb{C}_p$ and let $\mathcal{M}_p$ be the field of meromorphic functions over $\mathbb{C}_p$. We prove the following theorem on representation of squares by polynomials.

Theorem 3.1. *Let $P \in \mathcal{M}_p[X]$ be a monic polynomial of degree two. If $P(a)$ is a square in $\mathcal{M}_p$ for at least 35 values of $a \in \mathbb{C}_p$, then either P has constant coefficients or P is a square in $\mathcal{M}_p[X]$.*

By solving the second order recurrence implied in the statement of Büchi's problem, we can use the above theorem to show the following.

Corollary 3.2. *The problems $\mathbf{BP}(\mathcal{A}_p)$ and $\mathbf{BP}(\mathcal{M}_p)$ have a positive answer.*

Theorem 3.1 can be improved for the ring $\mathcal{A}_p$ of p-adic entire functions in the following way.

Theorem 3.3. *Let $P \in \mathcal{A}_p[X]$ be a monic polynomial of degree two. If $P(a)$ is a square in $\mathcal{A}_p$ for at least 13 values of $a \in \mathbb{C}_p$, then either P has constant coefficients or P is a square in $\mathcal{A}_p[X]$.*

The proof of Theorem 3.3 is shorter and simpler than the proof of Theorem 3.1. Indeed, the method used in the proof of Theorem 3.3 essentially is a p-adic simplified version of the method in [15]. Unfortunately, several technical difficulties arise when we consider the problem for $\mathcal{M}_p$, and this requires the use of Nevanlinna theory and some combinatoric arguments.

We will prove these results in Section 5 and Section 6. In Section 4, the reader will find some results from p-adic Complex Analysis that we will need later in the proofs.

3.2. **Undecidability for p-adic entire and meromorphic functions in Büchi's language.** Corollary 3.2 allows us to obtain very strong undecidability results for p-adic analytic and meromorphic functions, improving results by Lipshitz, Pheidas and Vidaux. In order to state the theorems, we need to introduce some notation.

Recall that $\mathcal{A}_p$ stands for the ring of entire functions over $\mathbb{C}_p$, and $\mathcal{M}_p$ stands for the field of meromorphic functions over $\mathbb{C}_p$, with variable z.

By a *diagonal quadratic equation over a ring A* we will mean an equation of the form:

$$a_1x_1^2 + \cdots + a_nx_n^2 = b$$

where the a_i and b are elements of A and the x_i are the unkowns.

Define the following languages:

$$\begin{aligned}\mathcal{L}_R^z =&\{0, 1, +, \cdot, z\},\\ \mathcal{L}_R^* =&\{0, 1, +, \cdot, z, \mathrm{ord}\},\\ \mathcal{L}_2^z =&\{0, 1, +, P_2, f_z\}, \text{ and}\\ \mathcal{L}_2^* =&\{0, 1, +, P_2, f_z, \mathrm{ord}\},\end{aligned}$$

where P_2 and ord are unary predicate symbols, and f_z is a unary function symbol. In $\mathcal{A}_p$ and $\mathcal{M}_p$, $P_2(x)$ is interpreted as 'x is a square', $f_z(x)$ is interpreted as '$x \mapsto zx$', and we interpret $\mathrm{ord}(x)$ as '$x(0) = 0$' (all other symbols are interpreted in the obvious way).

Theorem 3.4. *Multiplication is positive existentially definable in $\mathcal{M}_p$ and in $\mathcal{A}_p$ over the language $\mathcal{L}_2^z$.*

See Section 7 for a proof.

We recall that the following two theories are undecidable: the positive existential theory of $\mathcal{A}_p$ in the language $\mathcal{L}_R^z$ (see [10]) and the positive existential theory of $\mathcal{M}_p$ in the language $\mathcal{L}_R^*$ (see [24]). From this and Theorem 3.4 we conclude

Theorem 3.5. *The positive existential theory of $\mathcal{A}_p$ in the language $\mathcal{L}_2^z$ and the positive existential theory of $\mathcal{M}_p$ in the language $\mathcal{L}_2^*$ are undecidable.*

This result allows us to prove the following (see Section 7).

Theorem 3.6. *There is no algorithm to solve any of the following problems:*

(1) *Given a system of diagonal quadratic equations*

$$\sum_{i=1}^{r} a_{ij}x_i^2 = b_j \quad j = 1, \dots, s$$

with all the a_{ij} and b_j in $\mathbb{Z}[z]$, to decide whether or not the system has a solution in $\mathcal{A}_p$.

(2) *Given a system of diagonal quadratic equations*

$$\sum_{i=1}^{r} a_{ij}x_i^2 = b_j \quad j = 1, \dots, s$$

with all the a_{ij} and b_j in $\mathbb{Z}[z]$, and given a set $I \subseteq \{1, \dots, r\}$, to decide whether or not the system has a solution in $\mathcal{M}_p$ satisfying $x_i(0) = 0$ for each $i \in I$.

3.3. **Representation of squares in number fields.** The statements given below will be proved in Section 10.

Theorem 3.7. *Assume Bombieri's Conjecture 1.2 holds for surfaces. Let K be a number field and $\{a_1, \dots, a_8\}$ a set of eight elements in K. There exists a finite (possibly empty) set $E = E(K, (a_i)_i)$ of polynomials in $K[x]$ such that the following holds: for each polynomial f of the form $x^2+ax+b \in K[x]$, if $f(a_i)$ are squares in K for each i then either $f \in E$, or $f = (x + c)^2$ for some $c \in K$.*

This theorem is an extension of Theorem 0.5 in [26]. The method used to obtain this result is essentially an adaptation of the method by Vojta in [26].

It is an obvious but remarkable fact that, if one could find a number field K and a sequence $a = (a_1, \dots, a_8)$ of distinct elements of K such that the set $E(K, (a_i))$ is infinite, then one would automatically obtain a counterexample to Bombieri's Conjecture. On the other hand, showing finiteness for $E(K, (a_i))$ for some K and some sequence (a_i) would give a new example of a surface (over K) where Bombieri's question has a positive answer. We are not able to prove nor disprove the finiteness of the set $E(K, (a_i))$ in any case.

From the finiteness of the sets $E(K, (a_i))$ one can easily derive the following (see Section 10).

Corollary 3.8. *Assume that Bombieri's conjecture holds for surfaces defined over $\mathbb{Q}$. Let $a_1, a_2, \dots$ be a sequence of integers without repeated terms. There exists a constant M (depending on the sequence $(a_i)_i$) such that: if a polynomial $f = x^2 + ax + b \in \mathbb{Q}[x]$ satisfies the property '$f(a_i)$ is a square in $\mathbb{Z}$ for $i = 1, \dots, M$', then f is of the form $f = (x + c)^2$, for some $c \in \mathbb{Z}$.*

Observe that the dependence of M on the sequence cannot be dropped. Consider for example the polynomial $f_N = x^2 - 4(2N)!$, where N is a positive integer, and define

$$a_i = i! + \frac{(2N)!}{i!}.$$

Then it is obvious that $(a_i)_{i=1}^N$ is a strictly decreasing sequence in $\mathbb{Z}$ and each $f_N(a_i)$ is a square in $\mathbb{Z}$.

Note that, if in Corollary 3.8 we set $a_n = n$ for each n, then we obtain a positive answer to Büchi's Problem for $\mathbb{Z}$ (under Bombieri's Conjecture).

3.4. Representation of squares for function fields and for complex meromorphic functions.

The geometric results in Section 8 will be used in Section 10 to prove the following theorems, analogues to Theorem 3.1.

Theorem 3.9. *Let F be a field of characteristic zero and C a non-singular projective curve defined over F. Define the integer $M = \max\{8, 4(g + 1)\}$ where g is the genus of C. Write $K(C)$ for the function field of C and let X be transcendental over $K(C)$. Let $P \in K(C)[X]$ be a monic polynomial of degree two. If $P(a)$ is a square in $K(C)$ for at least M values of $a \in F$, then either P has constant coefficients or P is a square in $K(C)[X]$.*

Theorem 3.10. *Write $\mathcal{M}$ for the field of meromorphic functions on $\mathbb{C}$. Let $P \in \mathcal{M}[X]$ be a monic polynomial of degree two. If $P(a)$ is a square in $\mathcal{M}$ for at least 8 values of $a \in \mathbb{C}$, then either P has constant coefficients or P is a square in $\mathcal{M}[X]$.*

These theorems give as a direct consequence a positive answer to Büchi's problem in the respective cases, but such a positive answer is not new since it was proved in [26] for both cases. Moreover, Büchi's problem was solved recently by a new method in characteristic zero and (large enough) positive characteristic in [23].

4. Some results in p-adic Nevanlinna Theory

First we present the notation we use for the usual functions in p-adic Nevanlinna Theory.

We will work over the field $\mathbb{C}_p$ with absolute value $|\cdot|_p$. Write $\mathcal{A}_p$ for the ring of entire functions over $\mathbb{C}_p$ and $\mathcal{M}_p$ for the field of meromorphic functions over $\mathbb{C}_p$. We denote by F^+ the positive part of a function F in to $\mathbb{R}$, that is $F^+ = \max\{F, 0\}$. We adopt the following notation for the standard functions in p-adic Nevanlinna theory, where $f = \frac{h}{g} \in \mathcal{M}_p$ is non-zero, and where $g, h \in \mathcal{A}_p$ are coprime:

$$\begin{aligned}
B[r] &= \{z \in \mathbb{C}_p \colon |z|_p \leq r\}\\
n(r,h,0) &= \text{number of zeros of } h \text{ in } B[r] \text{ counting multiplicity}\\
n(r,f,0) &= n(r,h,0)\\
n(r,f,\infty) &= n(r,g,0)\\
N(r,h,0) &= \int_0^r \frac{n(t,h,0)-n(0,h,0)}{t}dt + n(0,h,0)\log r\\
N(r,f,0) &= N(r,h,0)\\
N(r,f,a) &= N(r,f-a,0)\\
N(r,f,\infty) &= N(r,g,0)\\
|h|_r &= \max_{n\geq 0} |a_n|_p r^n, \text{ where } h(z) = a_0 + \sum_{n\geq 1} a_n z^n\\
|f|_r &= \frac{|h|_r}{|g|_r}\\
m(r,f,a) &= \log^+ \frac{1}{|f-a|_r}\\
m(r,f) = m(r,f,\infty) &= \log^+ |f|_r
\end{aligned}$$

We recall to the reader that for each $r > 0$, the function $|\cdot|_r : \mathcal{M} \to \mathbb{R}$ is a non-archimedean absolute value satisfying $|a|_r = |a|_p$ when a is constant.

We will need the following standard results from p-adic Nevanlinna Theory. For a general presentation of p-adic complex analysis, see for example [20]. For references on p-adic Nevanlinna Theory (in particular, for a proof of the following results) see for example [4], [21] or the Chapter II of [8].

First we have the *Logarithmic Derivative Lemma*:

Lemma 4.1. *If $n > 0$ is a positive integer and $f \in \mathcal{M}_p$ then*

$$\left|\frac{f^{(n)}}{f}\right|_r \leq \frac{1}{r^n}$$

where $f^{(n)}$ stands for the n-th derivative.

We will also need the *Poisson-Jensen Formula*:

Theorem 4.2. *Given $f \in \mathcal{M}_p$, there exists a constant C depending only on f such that*

$$\log|f|_r = N(r,f,0) - N(r,f,\infty) + C.$$

As a consequence of the Poisson-Jensen Formula, we get the *First Main Theorem*:

Theorem 4.3. *Let $f \in \mathcal{M}_p$ be a non-constant meromorphic function and $a \in \mathbb{C}_p$. As $r \to \infty$ we have*

$$m(r,f,a) + N(r,f,a) = m(r,f,\infty) + N(r,f,\infty) + O(1).$$

Finally, we state the *Second Main Theorem*:

Theorem 4.4. *Let $f \in \mathcal{M}_p$ be a non-constant meromorphic function and let $a_1, \ldots, a_q \in \mathbb{C}_p$ be distinct. Then, as $r \to \infty$ we have*

$$\sum_{i=1}^q m(r,f,a_i) \leq N(r,f,\infty) + O(1).$$

5. Proof of Theorem 3.1 (p-adic Meromorphic Functions)

The following equality will be used many times without mention within this section:

$$N(r,f,x) = K + \int_1^r \frac{n(t,f,x)}{t}dt, \quad \text{for large } r. \tag{1}$$

It will be used systematically in order to deduce inequalities (for large r) about N when we know inequalities about n (the point is that the integral is a linear and monotone operator).

In order to simplify the proof of Theorem 3.1, we actually will prove the following equivalent result.

Theorem 5.1. *Let $h_1,\dots,h_M$ be elements of $\mathcal{M}_p$ such that at least one h_i is non-constant. Let $a_1,\dots,a_M$ be M distinct elements of $\mathbb{C}_p$. If there exist $f,g\in\mathcal{M}_p$, with g non-zero, such that*

$$h_j^2=(a_j+f)^2-g \qquad j=1,\dots,M \tag{2}$$

then $M\le 34$.

For the rest of this section, we will assume that we are under the hypothesis of Theorem 5.1. Assuming $M\ge 35$ we will obtain a contradiction.

First, we observe that

$$h_i^2-h_j^2=(a_i-a_j)(2f+a_i+a_j). \tag{3}$$

Lemma 5.2. *The function f is not constant.*

Proof. If f is constant then so is $c_i=(a_i+f)^2$. Note that since some h_i is non-constant, g is non-constant. Taking i, j and k such that c_i, c_j, and c_k are pairwise distinct constants, the following equality

$$(h_ih_jh_k)^2=(c_i-g)(c_j-g)(c_k-g)$$

gives a non-constant meromorphic parametrization of an elliptic curve over $\mathbb{C}_p$, which is impossible by a theorem of Berkovich (see [2]). □

Lemma 5.3. *Let $x\in\mathbb{C}_p$ be a pole of some h_i. There exists an index k depending on x such that for each $i\neq k$ we have (simultaneously)*

1. $\mathrm{ord}_x h_k\ge \mathrm{ord}_x h_i$;
2. $\mathrm{ord}_x f\ge 2\mathrm{ord}_x h_i$;
3. $\mathrm{ord}_x g\ge 4\mathrm{ord}_x h_i$;
4. $\mathrm{ord}_x h_i=\mathrm{ord}_x h_j$ *for all $j\neq k$; and*
5. $\mathrm{ord}_x h_i\le -1$.

Moreover, for each i we have

$$\min\{\mathrm{ord}_x h_i,0\}\ge \frac{1}{M-1}\sum_l \min\{\mathrm{ord}_x h_l,0\} \tag{4}$$

and, there exists a positive constant K such that for large enough r and for each i we have

$$N(r,h_i,\infty)\le \frac{1}{M-1}\sum_l N(r,h_l,\infty). \tag{5}$$

Proof. Let i_0 be an index such that h_{i_0} has a pole at x.

First suppose that *all* h_i have the same order at x (hence negative). In this case, Items (1), (4) and (5) hold trivially, Item (2) comes from Equation (3), and Item (3) comes from Equation (2). Indeed for Item (3) we have

$$\begin{aligned}\mathrm{ord}_x(g)&\ge 2\min\{\mathrm{ord}_x(h_i),\mathrm{ord}_x(f+a_i)\}\\&=2\min\{\mathrm{ord}_x(h_i),\mathrm{ord}_x(f)\}\\&=2\min\{\mathrm{ord}_x(h_i),2\mathrm{ord}_x(h_i)\}\\&\ge 4\mathrm{ord}_x h_i,\end{aligned}$$

where the last inequality comes from Item (2).

The other case is when not all h_i have the same order at x. Choose k such that item (1) holds true. By Equation (3) for indices k and any $i\neq k$, Item (4) holds true. If $i_0=k$ then all h_i have a pole at x (by maximality of k), and if $i_0\neq k$ then by Item (4), for all $i\neq k$, h_i has a pole at x. Hence Item (5) holds true. Items (2) and (3) for $i\neq k$ follow as in the previous case.

Finally, by Items (1), (4) and (5), and observing that $\mathrm{ord}_x h_k$ could be positive, we have for each i

$$(M-1)\min\{\mathrm{ord}_x h_i,0\}=\sum_{l\neq k}\min\{\mathrm{ord}_x h_l,0\}\ge\sum_l \min\{\mathrm{ord}_x h_l,0\}.$$

Summing for $x \in B[r]$ we obtain

$$(M-1)n(r,h_i,\infty) \leq \sum_l n(r,h_l,\infty).$$

which gives the inequality (5) by Equation (1). □

Lemma 5.4. *The following inequality holds*

$$\sum_{n=1}^{M} \log|h_n|_r + \frac{1}{M-1}\sum_{n=1}^{M} N(r,h_n,\infty) \geq -\frac{1}{2}N(r,f,\infty) + O(1).$$

Proof. By the Second Main Theorem 4.4, we have for each $i \in \{1,\dots,M\}$

$$-N(r,f,\infty)+O(1) \leq -\sum_{j\neq i}\log^+\left|\frac{1}{f+\frac{a_i+a_j}{2}}\right|_r \leq \sum_{j\neq i}\log\left|f+\frac{a_i+a_j}{2}\right|_r.$$

Since by Equation (3) we have

$$h_i^2 - h_j^2 = 2(a_i-a_j)\left(f+\frac{a_i+a_j}{2}\right),$$

we deduce

$$-N(r,f,\infty)+O(1) \leq \sum_{j\neq i}\log\left|h_i^2-h_j^2\right|_r.$$

If for a given r, i_r is an index such that $|h_i|_r$ is minimal, then

$$\begin{aligned}
\frac{1}{2}\sum_{j\neq i_r}\log\left|h_{i_r}^2-h_j^2\right|_r &\leq \sum_{j\neq i_r}\log|h_j|_r \\
&= C + \sum_{j\neq i_r}\left(N(r,h_j,0)-N(r,h_j,\infty)\right) \\
&\leq C + N(r,h_{i_r},\infty) + \sum_n \left(N(r,h_n,0)-N(r,h_n,\infty)\right) \\
&= C' + N(r,h_{i_r},\infty) + \sum_n \log|h_n|_r \\
&\leq C'' + \frac{1}{M-1}\sum_n N(r,h_n,\infty) + \sum_n \log|h_n|_r
\end{aligned}$$

where the first and second equalities are given by the Poisson-Jensen Formula 4.2, the third inequality is given by Lemma 5.3 (see Equation (5)), and C, C', C'' are fixed constants (not depending on r nor on i_r).

Finally we have

$$-\frac{1}{2}N(r,f,\infty)+O(1) \leq \frac{1}{2}\sum_{j\neq i_r}\log\left|h_{i_r}^2-h_j^2\right|_r \leq \sum\log|h_n|_r + \frac{1}{M-1}\sum N(r,h_n,\infty) + C''$$

for each r large enough, and the lemma is proven. □

Lemma 5.5. *The following inequalities hold:*

$$n(r,f,\infty) \leq \frac{2}{M-1}\sum_n n(r,h_n,\infty)$$

and

$$\sum_n N(r,h_n,0) \geq \frac{M-3}{M-1}\sum_n N(r,h_n,\infty) + O(1).$$

Proof. Observe that by Lemma 5.3 (Item (2) and Equation (4)) we have

$$(M-1)n(r,f,\infty) \le 2\sum n(r,h_j,\infty),$$

hence

$$(M-1)N(r,f,\infty) \le 2\sum N(r,h_n,\infty)+O(1).$$

The second formula comes immediately by Lemma 5.4 and the Poisson-Jensen Formula 4.2. □

The equations

$$\begin{aligned} h_n^2+g &= (a_n+f)^2 \\ 2h_n'h_n+g' &= 2f'(a_n+f) \end{aligned}$$

are directly deduced by reordering and differentiating the one given in the hypothesis. From this we deduce

$$(2h_n'h_n+g')^2 = 4f'^2(h_n^2+g)$$

hence

$$g'^2-4f'^2g = 4h_n(h_nf'^2-h_n'^2h_n-h_n'g').$$

Writing

$$\begin{aligned} \Delta &= g'^2-4f'^2g \\ \Delta_n &= h_nf'^2-h_n'^2h_n-h_n'g' \end{aligned}$$

we have

$$\Delta = 4h_n\Delta_n. \tag{6}$$

Lemma 5.6. *If Δ is not identically zero, then*

$$N(r,\Delta,0) \ge \frac{1}{2}\sum N(r,h_n,0) - \frac{8}{M-1}\sum N(r,h_n,\infty)+O(1).$$

Proof. On the one hand, for a given $x\in\mathbb{C}_p$ suppose f has a pole at x and $h_j(x)=0$ for some index j. Set $l=\mathrm{ord}_x(h_j)$ and $m=\mathrm{ord}_x(f)$. Note that $\mathrm{ord}_x(g)=2m$ because $h_j(x)=0$ (see Equation (2)). Write

$$h_j = u_l(z-x)^l+u_{l+1}(z-x)^{l+1}+\cdots,$$
$$f = v_m(z-x)^m+v_{m+1}(z-x)^{m+1}+\cdots$$

and

$$g = w_{2m}(z-x)^{2m}+w_{2m+1}(z-x)^{2m+1}+\cdots$$

for the Laurent series of h_j, f and g at x. Observe that $w_{2m}=v_m^2$. The first term of the Laurent series at x for respectively $h_jf'^2$, $h_j'^2h_j$ and $h_j'g'$ is, respectively,

$$\begin{aligned} &m^2u_lv_m^2(z-x)^{l+2m-2} \\ &l^2u_l^3(z-x)^{3l-2} \\ &2lmu_lv_m^2(z-x)^{l+2m-2} \end{aligned}$$

hence $\mathrm{ord}_x\Delta_j = l+2m-2$ since $2l\ne m$. Therefore, we have

$$\mathrm{ord}_x\Delta = 2(l+m-1).$$

On the other hand, if $x\in\mathbb{C}_p$ is not a pole of f and is a zero of some h_j, then we have

$$\mathrm{ord}_x\Delta \ge \mathrm{ord}_x(h_j)$$

because by Equation (2), g does not have a pole, hence Δ_j does not have a pole and we conclude by Equation (6).

Let A_r be the set of $x\in B[r]$ such that f has not a pole at x and $h_j(x)=0$ for some index j, and let B_r be the set of $x\in B[r]$ such that f has a pole at x and $h_j(x)=0$ for some index j. Observe that, by Equation (3), no three of the h_n can share a zero (we use it for the fifth inequality below). We have then

$$\begin{aligned}
n(r,\Delta,0) &\geq \sum_{x\in A_r}\mathrm{ord}_x\Delta + \sum_{x\in B_r}\mathrm{ord}_x\Delta\\
&\geq \sum_{x\in A_r}\max_{h_i(x)=0}\mathrm{ord}_x(h_i) + \sum_{x\in B_r}\max_{h_i(x)=0} 2(\mathrm{ord}_x(h_i)+\mathrm{ord}_x(f)-1)\\
&\geq \sum_{x\in A_r\cup B_r}\max_{h_i(x)=0}\mathrm{ord}_x(h_i) + 2\sum_{x\in B_r}\max_{h_i(x)=0}(\mathrm{ord}_x(f)-1)\\
&= \sum_{x\in A_r\cup B_r}\max_{h_i(x)=0}\mathrm{ord}_x(h_i) + 2\sum_{x\in B_r}(\mathrm{ord}_x(f)-1)\\
&\geq \sum_{x\in A_r\cup B_r}\max_{h_i(x)=0}\mathrm{ord}_x(h_i) + 4\sum_{x\in B_r}\mathrm{ord}_x(f)\\
&\geq \frac{1}{2}\sum_i n(r,h_i,0) - 4n(r,f,\infty)\\
&\geq \frac{1}{2}\sum_i n(r,h_i,0) - \frac{8}{M-1}\sum n(r,h_i,\infty)
\end{aligned}$$

where the last inequality comes from Lemma 5.5. The result follows. □

Lemma 5.7. *If Δ is not identically zero, then*

$$N(r,\Delta,\infty) \leq \frac{8}{M-1}\sum N(r,h_n,\infty) + O(1).$$

Proof. Suppose that some $x\in\mathbb{C}_p$ is a pole of Δ. Then, by definition of Δ, it is a pole of f or of g. If none of the h_i has a pole at x then by Equation (3) f does not have a pole, and by Equation (2), g does not have a pole, which contradicts our hypothesis. Therefore, some h_i has a pole at x. Take k as in Lemma 5.3. For each index $i\neq k$ we have (observing that $\mathrm{ord}_x(h_i)\leq -1$ and that if $g'=0$ then $\mathrm{ord}_x h_i' g'$ is infinite)

$$\begin{aligned}
\mathrm{ord}_x\Delta &\geq \mathrm{ord}_x h_i + \min\{\mathrm{ord}_x h_i f'^2, \mathrm{ord}_x h_i'^2 h_i, \mathrm{ord}_x h_i' g'\}\\
&\geq \mathrm{ord}_x h_i + \min\{7\mathrm{ord}_x h_i, 5\mathrm{ord}_x h_i, 7\mathrm{ord}_x h_i\}\\
&= 8\mathrm{ord}_x h_i.
\end{aligned}$$

Hence, using the Lemma 5.3 (Equation (4)) we have

$$\mathrm{ord}_x\Delta \geq \frac{8}{M-1}\sum_l \min\{\mathrm{ord}_x h_l, 0\}.$$

Write D_r for the set of poles of Δ in $B[r]$. We have

$$\begin{aligned}
n(r,\Delta,\infty) &= \sum_{x\in D_r} -\mathrm{ord}_x\Delta\\
&\leq \frac{8}{M-1}\sum_{x\in D_r}\sum_l \max\{-\mathrm{ord}_x h_l, 0\}\\
&\leq \frac{8}{M-1}\sum_l\sum_{x\in B[r]} \max\{-\mathrm{ord}_x h_l, 0\}\\
&= \frac{8}{M-1}\sum_l n(r,h_l,\infty).
\end{aligned}$$

and the result follows. □

Lemma 5.8. (1) *For each $r>0$, there exists an index k_r such that $|h_{k_r}|_r$ is minimal.*

(2) *There exists a positive constant K_f such that, for any $r>0$ and for all $i\neq k_r$, we have*

$$\log|f|_r \leq \max\{0, 2\log|h_i|_r\} + K_f.$$

(3) *There exists a positive constant K_g such that, for any $r > 0$ and for all $i \neq k_r$, we have*

$$\log |f|_r \leq \max\{0, 4\log |h_i|_r\} + K_g.$$

Proof. Item (1) is immediate since for each r, the set $\{|h_i|_r : i = 1, \ldots, M\}$ is finite. Let us prove Item (2). There exists a positive constant $K' > 1$ such that for each $r > 0$, i and j, we have

$$|2f|_r \leq |2f + a_i + a_j|_r + |a_i + a_j|_r \leq K' + |2f + a_i + a_j|_r. \tag{7}$$

On the other hand, by Equation (3) there exists a constant $K'' > 1$ such that, for any $r > 0$, $i \neq k_r$ and j, we have

$$\begin{aligned} |2f + a_i + a_j|_r &= \left| \frac{h_i^2 - h_{k_r}^2}{a_i - a_{k_r}} \right|_r \\ &\leq \left| \frac{h_i^2}{a_i - a_{k_r}} \right|_r \qquad \text{(by Item (1))} \\ &\leq K''|h_i^2|_r \end{aligned}$$

hence by Equation (7)

$$|2f|_r \leq K''|h_i^2|_r + K' \leq K'' \max\{|h_i^2|_r, 1\} + K'.$$

Therefore, we have

$$\begin{aligned} \log |f|_r &\leq \log(K'' \max\{|h_i^2|_r, 1\} + K') - \log |2|_r \\ &\leq \log(K'' \max\{|h_i^2|_r, 1\}) + \log K' + \log 2 - \log |2|_r \\ &\leq \max\{2\log |h_i|_r, 0\} + K_f \end{aligned}$$

with K_f is a positive constant greater than $\log K'' + \log K' + \log 2 - \log |2|_r$, and where the second inequality comes from the fact that for all real numbers $x, y \geq 1$, we have $\log(x+y) \leq \log x + \log y + \log 2$ (just write $(1-x)(y-1) \leq 0$).

Finally, we prove Item (3). By Equation (2) and Item (2), for each $i \neq k_r$ we have

$$\begin{aligned} \log |g|_r &= \log |(f + a_i)^2 - h_i^2|_r \\ &\leq \log\left(\max\{|h_i^2|_r, |f^2|_r, |2a_i f|_r, |a_i^2|_r\}\right) \\ &\leq \log\left(\max\{|h_i^2|_r, |f^2|_r, |a_i^2|_r\}\right) \\ &\leq \max\{2\log |h_i|_r, 0, 2\log |f|_r\} + \max\{|a_i^2|_r\} \\ &\leq \max\{2\log |h_i|_r, 0, 2\max\{0, 2\log |h_i|_r\} + 2K_f\} + \max\{|a_i^2|_r\} \\ &\leq \max\{2\log |h_i|_r + 2K_f, 2K_f, 4\log |h_i|_r + 2K_f\} + \max\{|a_i^2|_r\} \\ &\leq \max\{0, 4\log |h_i|_r\} + K_g \end{aligned}$$

where K_g is a fixed positive constant bigger than $2K_f + \max\{|a_i^2|_r\}$, and where the second inequality comes from the following:

$$|2a_i f|_r \leq |a_i|_r |f|_r \leq \frac{|a_i^2|_r + |f^2|_r}{2} \leq \max\{|a_i^2|_r, |f^2|_r\}.$$

□

Lemma 5.9. *If Δ is not identically zero, then*

$$\log |\Delta|_r \leq \frac{6M - 2}{M(M-1)} \sum \log |h_n|_r + \frac{8}{(M-1)^2} \sum N(r, h_n, \infty) - 2\log r + O(1).$$

Proof. By the Poisson-Jensen Formula 4.2 and Lemma 5.3 (Equation (5)) we have for r large enough and for each i

$$\begin{aligned} \log |h_i|_r &= N(r, h_i, 0) - N(r, h_i, \infty) + C \\ &\geq -N(r, h_i, \infty) + C \\ &\geq -\frac{1}{M-1} \sum_n N(r, h_n, \infty) + C' \end{aligned}$$

for some constants C, C'.

Given $r > 0$ take k_r as in Lemma 5.8. Choose i_r such that $|h_{i_r}|_r$ is minimal in $\{|h_i|_r : i \neq k_r\}$, and note that

$$\log |h_{i_r}|_r \leq \frac{1}{M-1} \sum_{i \neq k_r} \log |h_i|_r.$$

By Item (2) in Lemma 5.8, we have for each r large enough

$$\begin{aligned}
\log |f|_r &\leq \max\{0, 2\log|h_{i_r}|_r\} + K_f \\
&\leq \max\left\{0, \frac{2}{M-1}\sum_{i\neq k_r} \log|h_i|_r\right\} + K_f \\
&\leq \max\left\{0, \frac{2}{M-1}\sum \log|h_n|_r + \frac{2}{(M-1)^2}\sum N(r,h_n,\infty)\right\} - \frac{2C'}{M-1} + K_f
\end{aligned}$$

and by Item (3) in Lemma 5.8 we have for each r large enough

$$\begin{aligned}
\log |g|_r &\leq \max\{0, 4\log|h_{i_r}|_r\} + K_g \\
&\leq \max\left\{0, \frac{4}{M-1}\sum_n \log|h_n|_r + \frac{4}{(M-1)^2}\sum_n N(r,h_n,\infty)\right\} - \frac{4C'}{M-1} + K_g.
\end{aligned}$$

Hence, for large r we get

$$\log |f|_r \leq \max\left\{0, \frac{2}{M-1}\sum_n \log|h_n|_r + \frac{2}{(M-1)^2}\sum_n N(r,h_n,\infty)\right\} + O(1) \tag{8}$$

$$\log |g|_r \leq \max\left\{0, \frac{4}{M-1}\sum_n \log|h_n|_r + \frac{4}{(M-1)^2}\sum_n N(r,h_n,\infty)\right\} + O(1). \tag{9}$$

Since Δ is not the zero function, from Lemma 4.1 (Logarithmic Derivative Lemma) we have for each index n

$$|\Delta|_r \leq |h_n|_r \max\{|h_n f'^2|_r, |h_n'^2 h_n|_r, |h_n' g'|_r\} \leq \frac{1}{r^2}|h_n|_r^2 \max\{|f|_r^2, |h_n|_r^2, |g|_r\}$$

and by Equation (2) for each n holds

$$2\log|h_n|_r \leq \max\{2\log|f|_r, 0, \log|g|_r\} + O(1)$$

therefore we have for each n

$$\log|\Delta|_r \leq \log\left(\frac{1}{r^2}|h_n|_r^2\right) + \max\{2\log|f|_r, 0, \log|g|_r\} + O(1).$$

Since this last expression is true *for each* n, we have

$$\log|\Delta|_r \leq \frac{2}{M}\sum \log|h_n|_r - 2\log r + \max\{2\log|f|_r, 0, \log|g|_r\} + O(1).$$

Note that by equations (8) and (9)

$$\max\{2\log|f|_r, 0, \log|g|_r\} \leq \max\left\{0, \frac{4}{M-1}\sum \log|h_n|_r + \frac{4}{(M-1)^2}\sum N(r,h_n,\infty)\right\} + O(1)$$

and by Lemma 5.4 we have that this last expression is less than or equal to

$$\frac{4}{M-1}\sum \log|h_n|_r + \frac{4}{(M-1)^2}\sum N(r,h_n,\infty) + \frac{2}{M-1}N(r,f,\infty) + O(1).$$

Therefore

$$\begin{aligned}
\log|\Delta|_r \leq \left(\frac{2}{M} + \frac{4}{M-1}\right)\sum \log|h_n|_r - 2\log r + \frac{4}{(M-1)^2}\sum N(r,h_n,\infty) \\
+\frac{2}{M-1}N(r,f,\infty) + O(1)
\end{aligned}$$

Finally, we bound $N(r,f,\infty)$ using Lemma 5.5 and the result follows. □

Lemma 5.10. $\Delta = 0$ *for* $M \geq 35$.

Proof. The proof goes by contradiction, so we assume Δ is not identically zero. Consider the equation

$$\log|\Delta|_r = N(r,\Delta,0) - N(r,\Delta,\infty) + O(1).$$

Lemmas 5.6, 5.7 and 5.9 allow us to bound $\log|\Delta|_r$ above and below, obtaining

$$\frac{6M-2}{M(M-1)}\sum \log|h_n|_r + \frac{8}{(M-1)^2}I - 2\log r \geq \frac{1}{2}Z - \frac{8}{M-1}I - \frac{8}{M-1}I + O(1)$$

where we write $Z = \sum N(r,h_n,0)$ and $I = \sum N(r,h_n,\infty)$. Observe that

$$\sum \log|h_n|_r = Z - I + O(1)$$

by Poisson-Jensen Formula 4.2. This and Lemma 5.5 give

$$\begin{aligned}
-2\log r &\geq \left(\frac{1}{2} - \frac{6M-2}{M(M-1)}\right)Z + \left(\frac{6M-2}{M(M-1)} - \frac{16}{M-1} - \frac{8}{(M-1)^2}\right)I + O(1)\\
&\geq \left(\left(\frac{1}{2} - \frac{6M-2}{M(M-1)}\right)\frac{M-3}{M-1} - \frac{10M^2-2}{M(M-1)^2}\right)I + O(1)\\
&= \frac{M^2-35M+8}{2M(M-1)}I + O(1).
\end{aligned}$$

A contradiction for $M \geq 35$. □

Finally, we have that Δ is the zero function, f is not a constant and g is non-zero. We get the equation $g'^2 = 4f'^2 g$, which implies that exists a meromorphic function u such that $g = u^2$ and $u'^2 = f'^2$. Hence $u = \alpha f + b$ for certain $\alpha \in \{-1,1\}$ and $b \in \mathbb{C}_p$, and we obtain

$$\begin{aligned}
h_n^2 &= (a_n+f)^2 - (\alpha f + b)^2\\
&= (a_n+f)^2 - (f+\alpha b)^2\\
&= (a_n - \alpha b)(a_n + \alpha b + 2f).
\end{aligned}$$

From this we get

$$\left(\frac{h_i h_j h_k}{\sqrt{(a_i-\alpha b)(a_j-\alpha b)(a_k-\alpha b)}}\right)^2 = (a_i+\alpha b+2f)(a_j+\alpha b+2f)(a_k+\alpha b+2f).$$

This is a contradiction because f is not a constant. Therefore the Theorem 5.1 is proven.

6. Proof of Theorem 3.3 (p-adic Entire Functions)

The purpose of this section is to prove Theorem 3.3. Up to some adaptations for the p-adic setting, the proof goes along essentially the same lines as the solution of Büchi's problem for $\mathbb{C}[z]$ using the method of Pheidas and Vidaux (see for example [15] for the paper where this method was used by first time, or [14] for a quite simplified exposition in the particular case $\mathbb{C}[x]$, which is closer to the case of p-adic entire functions) and we include it here just for the sake of completeness.

We prefer to avoid the use of Berkovich's theorem and replace it by an elementary argument on factorization.

In order to simplify the proof, we will prove the Theorem in the following equivalent form:

Theorem 6.1. *Let $h_j \in \mathcal{A}_p, j = 1,\dots,M$ with at least one of them non-constant, and let $a_j \in \mathbb{C}_p$ be distinct for $j = 1,\dots,M$. Assume we have $f,g \in \mathcal{A}_p$ with f,g non-zero, such that $h_j^2 = (a_j+f)^2 - g$ for $j = 1,\dots,M$. Then $M \leq 12$.*

We will assume $M > 12$ to obtain a contradiction.

Lemma 6.2. *The function f is non-constant.*

Proof. Suppose that f is constant. Then $(h_i - h_j)(h_i + h_j) = (a_i - a_j)(a_i + a_j + 2f)$ also is constant for $i \neq j$, hence each $h_i = \frac{1}{2}((h_i - h_j) + (h_i + h_j))$ is constant, which contradicts the hypothesis. □

For $i \neq j$ we have

$$h_i^2 - h_j^2 = \big((a_i + f)^2 - g\big) - \big((a_j + f)^2 - g\big) = 2(a_i - a_j)f + (a_i^2 - a_j^2)$$

hence, for each r we have

$$2 \max_n m(r, h_n) \geq m(r, h_i^2 - h_j^2) = m(r, f) + \mathcal{O}(1) \tag{10}$$

and the equality $g = (a_j + f)^2 - h_j^2$ implies

$$m(r, g) \leq 2 \max\{m(r, a_j + f), m(r, h_j)\} + \mathcal{O}(1) \leq 4 \max_n m(r, h_n) + \mathcal{O}(1). \tag{11}$$

As in the previous section, we define

$$\begin{aligned} \Delta &= g'^2 - 4f'^2 g \\ \Delta_n &= h_n f'^2 - {h'_n}^2 h_n - h'_n g' \end{aligned}$$

and these functions satisfy the same equation as in the previous section (see Equation (6))

$$\Delta = 4h_n\Delta_n.$$

Lemma 6.3. *The function Δ is the zero function.*

The point is that, if Δ is not the zero function then we can apply to it the function $m(r, \cdot)$, and we will obtain a contradiction by bounding above and below $m(r, \Delta)$. We we will need the following three claims.

Claim 6.4. *For each r large enough, we have*

$$m(r, \Delta) \leq 6 \max_n m(r, h_n) - 2 \log r + \mathcal{O}(1).$$

Proof of Claim 6.4. By definition of Δ we have

$$\begin{aligned} m(r, \Delta) &= m(r, h_n) + m(r, \Delta_n) + \mathcal{O}(1) \\ &\leq m(r, h_n) + \max\{m(r, h_n f'^2), m(r, {h'_n}^2 h_n), m(r, h'_n g')\} + \mathcal{O}(1) \end{aligned}$$

In order to estimate an upper bound for this last expression, by the inequalities (10) and (11) and Lemma 4.1 we obtain for each r large enough

$$\begin{aligned} m(r, h_n f'^2) &\leq m(r, h_n) + 2m(r, f) - 2 \log r + \mathcal{O}(1) \\ &\leq 5 \max_n m(r, h_n) - 2 \log r + \mathcal{O}(1) \\ m(r, {h'_n}^2 h_n) &\leq m(r, h_n) + 2m(r, h_n) - 2 \log r + \mathcal{O}(1) \\ &\leq 3 \max_n m(r, h_n) - 2 \log r + \mathcal{O}(1) \\ m(r, h'_n g') &\leq m(r, h_n) + m(r, g) - 2 \log r + \mathcal{O}(1) \\ &\leq 5 \max_n m(r, h_n) - 2 \log r + \mathcal{O}(1) \end{aligned}$$

Therefore, for each r large enough we have

$$m(r, \Delta) \leq 6 \max_n m(r, h_n) - 2 \log r + \mathcal{O}(1).$$

□

Claim 6.5. *For each r large enough, we have*

$$\max m(r, h_n) \leq \frac{1}{M - 1} \sum_n m(r, h_n) + O(1)$$

Proof of Claim 6.5. Given an r, if all the $m(r, h_n)$ are equal the result is obvious, so let us assume that we have two indices s, t such that $m(r, h_s)$ is minimal, $m(r, h_t)$ is maximal and $m(r, h_s) \neq m(r, h_t)$. For r large enough and for all $i \neq j$ we have $|2f|_r = |a_i + a_j + 2f|_r$ because of Lemma 6.2 and the definition of $|\cdot|_r$, moreover, $|2f|_r > 1$ for large r. Write $C = \log^+ \max_{i \neq j} |a_i - a_j|_p$ and note that this constant does not depend on r. Since $h_i^2 - h_j^2 = (a_i - a_j)(a_i + a_j + 2f)$ we have for r large enough

$$m(r, f) \leq m(r, h_i^2 - h_j^2) \leq m(r, f) + C.$$

On the one hand, by the strong triangle inequality of $|\cdot|_r$ we have for each n

$$m(r,f)+C\geq m(r,h_t^2-h_s^2)=2m(r,h_t)=2\max_n m(r,h_n).$$

On the other hand, for each $n\neq s$ we have

$$2m(r,h_n)\geq m(r,h_n^2-h_s^2)\geq m(r,f).$$

adding these inequalities as long as $n\neq s$ we get

$$2\sum_n m(r,h_n)\geq 2\sum_{n\neq s} m(r,h_n)\geq (M-1)m(r,f).$$

Therefore

$$2\sum_n m(r,h_n)\geq (M-1)m(r,f)\geq (M-1)(2\max_n m(r,h_n)-C).$$

□

Claim 6.6. *For each r large enough, we have*

$$\frac{1}{2}\sum_n m(r,h_n)\leq m(r,\Delta)+\mathcal{O}(1)$$

Proof of Claim 6.6. Define

$$n(r)=\sum_{|\rho|\leq r}\max_n \mathrm{ord}_\rho h_n$$

and note that this sum is always finite because the h_n are entire. Since $4h_n\Delta_n=\Delta$ holds for each n and Δ is not identically zero, we have $\mathrm{ord}_\rho h_n\leq \mathrm{ord}_\rho\Delta$ for each n and each ρ, therefore $n(r)\leq n(r,\Delta,0)$.

Observe that no three of the h_i can share a zero (if ρ is a common zero of h_i,h_j,h_k for distinct indices, then the polynomial $(f(\rho)+X)^2-g(\rho)$ has three roots, namely a_i,a_j,a_k), hence

$$\sum_n n(r,h_n,0)\leq 2n(r)$$

and we arrive to

$$\sum_n n(r,h_n,0)\leq 2n(r,\Delta,0)$$

hence

$$\sum_n N(r,h_n,0)\leq 2N(r,\Delta,0)+\mathcal{O}(1).$$

This inequality and Theorem 4.2 applied to Δ (which is an entire function) lead to

$$\sum_n m(r,h_n)\leq 2m(r,\Delta)+\mathcal{O}(1).$$

□

Proof of Lemma 6.3. We suppose Δ is not identically zero. We apply to it $m(r,\cdot)$ and use the bounds given in the above Claims to get:

$$2\log r+\frac{1}{2}\sum_n m(r,h_n)\leq \frac{6}{M-1}\sum_n m(r,h_n)+\mathcal{O}(1)$$

which is a contradiction for $M>12$. This proves that $\Delta=0$. □

From the equation $\Delta=0$ we have

$$g'^2=4f'^2g. \tag{12}$$

By Lemma 6.2 we have that f is non-constant, hence the equation $g'^2=4f'^2g$ implies that g is a square in $\mathcal{M}_p$, but $g\in\mathcal{A}_p$ implies that g is a square in $\mathcal{A}_p$. Thus $g=u^2$ for some $u\in\mathcal{A}_p$ and replacing in

Equation (12) we get $u'^2 = f'^2$. Therefore there exists $b \in \mathbb{C}_p$ and $\alpha \in \{-1, 1\}$ such that $g = (\alpha f + b)^2$, hence

$$\begin{aligned} h_n^2 &= (a_n + f)^2 - (\alpha f + b)^2 \\ &= (a_n + f)^2 - (f + \alpha b)^2 \\ &= (a_n - \alpha b)(a_n + \alpha b + 2f). \end{aligned}$$

Observe that this and Lemma 6.2 imply h_n non-constant for all n such that $a_n \neq \alpha b$, and this is the case for al but at most one index m since the a_n are pairwise distinct. Define

$$v_n = \frac{f_n}{a_n - \alpha b}$$

for each $n \neq m$, and note that each v_i is non-constant. Take any two indices $i \neq j$ such that $i, j \neq m$. We have

$$(v_i - v_j)(v_i + v_j) = v_i^2 - v_j^2 = (a_i + \alpha b + 2f) - (a_j + \alpha b + 2f) = a_i - a_j$$

and this implies that $v_i - v_j$ and $v_i + v_j$ are constant, therefore each $v_i = \frac{1}{2}((v_i + v_j) + (v_i - v_j))$ is constant. This is the desired contradiction, and the proof of Theorem 6.1 is complete.

7. Proof of Theorem 3.4 (Undecidability Results)

We will use the positive answer to Problems $\mathbf{BP}(\mathcal{M}_p)$ and $\mathbf{BP}(\mathcal{A}_p)$. First we define the following $\mathcal{L}_2^z$-formulas:

$$\begin{aligned} \mathrm{Bu}[x,y] &: \exists u_1 \cdots \exists u_{35} \left(\wedge_{i=1}^{35} P_2(u_i)\right) \wedge \left(\wedge_{i=2}^{34} u_{i-1} + u_{i+1} = 2u_i + 2\right) \wedge x = u_1 \wedge 2y + 1 = u_2 - u_1 \\ \mathrm{Sq}[x,y] &: \mathrm{Bu}[x,y] \wedge \mathrm{Bu}[f_z x, f_z f_z y] \\ \mathrm{Prod}[x,y,w] &: \exists u \exists v P_2(u) \wedge P_2(v) \wedge (\mathrm{Sq}[x+y,u] \wedge \mathrm{Sq}[x-y,v] \wedge u = v + 4w)\,. \end{aligned}$$

Note that all the above formulas are positive existential.

Next we define the following systems of equations:

$$\mathrm{Bu}_{\mathrm{sys}}(a,b) : \begin{cases} q_3^2 - 2q_2^2 + q_1^2 = 2 \\ \vdots \\ q_{35}^2 - 2q_{34}^2 + q_{33}^2 = 2 \\ q_1^2 = b \\ q_2^2 - q_1^2 = 2a + 1 \end{cases}$$

$$\mathrm{Sq}_{\mathrm{sys}}(a,b) : \begin{cases} \mathrm{Bu}_{\mathrm{sys}}(a,b) \\ \mathrm{Bu}_{\mathrm{sys}}(za, z^2 b) \end{cases}$$

and

$$\mathrm{Prod}_{\mathrm{sys}}(a,b,c) : \begin{cases} \mathrm{Sq}(a, x^2) \\ \mathrm{Sq}(b, y^2) \\ \mathrm{Sq}(a+b, w^2) \\ w^2 = x^2 + 2c + y^2 \end{cases}$$

where it is understood that, if we consider a system of equations built up by several of these systems, then the unknowns in each of them are distinct. For example, in the definition of $\mathrm{Sq}_{\mathrm{sys}}$, since we use twice $\mathrm{Bu}_{\mathrm{sys}}$, it is understood that the variables q_i in the first $\mathrm{Bu}_{\mathrm{sys}}$ are distinct from the variables q_i appearing in the second $\mathrm{Bu}_{\mathrm{sys}}$.

Note that the system $\mathrm{Prod}_{\mathrm{sys}}(x^2, y^2, z^2)$ (where x, y, z also are considered as unknowns) is a system of diagonal quadratic equations with coefficients in $\mathbb{Z}[z]$.

From the definition of the above formulas and systems of equations, it is clear that given $a, b, c \in R$, where $R = \mathcal{A}_p$ or $\mathcal{M}_p$, we have the following:

- $R \models \mathrm{Bu}[a,b]$ if and only if the system $\mathrm{Bu}_{\mathrm{sys}}(a,b)$ has a solution in R
- $R \models \mathrm{Sq}[a,b]$ if and only if the system $\mathrm{Sq}_{\mathrm{sys}}(a,b)$ has a solution in R
- $R \models \mathrm{Prod}[a,b,c]$ if and only if the system $\mathrm{Prod}_{\mathrm{sys}}(a,b,c)$ has a solution in R.

Lemma 7.1. *If $a, b, c \in R$, where $R = \mathcal{A}_p$ or $R = \mathcal{M}_p$, then the following statements are equivalent:*

i. $ab = c$
ii. $R \models \mathrm{Prod}[a, b, c]$
iii. $\mathrm{Prod}_{\mathrm{sys}}(a, b, c)$ *has a solution in R.*

Proof. Because of the above discussion, it is enough to prove that item i is equivalent to item ii. By Corollary 3.2 we have: R satisfies $\mathrm{Bu}[a, b]$ if and only if $b = a^2$ or a and b are constants. Thus, R satisfies $\mathrm{Sq}[a, b]$ if and only if $b = a^2$. Therefore, R satisfies $\mathrm{Prod}[a, b, c]$ if and only if $c = ab$. □

Proof of Theorem 3.4. This is a consequence of the equivalence of items i and ii in Lemma 7.1, and the fact that $\mathrm{Prod}[x, y, z]$ is a positive existential $\mathcal{L}_2^z$-formula. □

Proof of Theorem 3.6. From Theorem 3.4 we obtain the non-existence of an algorithm to solve any of the following problems:

(1) Given a system

$$\sum_{i=1}^{r} a_{ik}x_i^2 + \sum_{j=1}^{s} b_{jk}y_j = c_k, \quad k = 1, \dots, t \tag{13}$$

with all the a_{ik}, b_{jk}, c_k in $\mathbb{Z}[z]$, to decide whether or not the system has a solution in $\mathcal{A}_p$.

(2) Given a system

$$\sum_{i=1}^{r} a_{ik}x_i^2 + \sum_{j=1}^{s} b_{jk}y_j = c_k, \quad k = 1, \dots, t \tag{14}$$

with all the a_{ik}, b_{jk}, c_k in $\mathbb{Z}[z]$, and given two sets $I \subseteq \{1, \dots, r\}$ and $J \subseteq \{1, \dots, s\}$, to decide whether or not the system has a solution in $\mathcal{M}_p$ satisfying $x_i(0) = 0$ for each $i \in I$ and $y_j(0) = 0$ for each $k \in J$.

To prove item (1) of the theorem, consider the diagonal quadratic system

$$\sum_{i=1}^{r} a_{ik}x_i^2 + \sum_{k=1}^{s} b_{jk}(u_j^2 - v_j^2) = c_k, \quad k = 1, \dots, t. \tag{15}$$

System (15) has a solution in $\mathcal{A}_p$ if and only if System (13) has, because of the identity

$$x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2.$$

In order to prove item (2) of the theorem, we cannot perform the same substitution as before in order to eliminate the degree-one part, because a technical problem arises with the vanishing conditions. Namely, if we replace an unknown y_j with condition $y_j(0) = 0$ by $(u_j^2 - v_j^2)$ as in the previous case, then the vanishing condition becomes $(u_j^2 - v_j^2)(0) = 0$, which is useless because we want vanishing conditions on the *unknowns*, not on *polynomial expressions* of the unknowns. To fix this problem, we will use again the positive answer to Büchi's problem in order to perform a substitution in such a way that vanishing conditions on unknowns become vanishing conditions on the new unknowns. We will obtain not one but several diagonal quadratic systems, but this will be enough to prove the Theorem.

Consider the following $2^{|J|}$ diagonal quadratic systems S_α indexed by $\alpha \subseteq J$:

$$(S_\alpha)\begin{cases} \displaystyle\sum_{i=1}^{r} a_{ik}x_i^2 + \sum_{j\in\alpha} b_{jk}(u_{j2}^2 - u_{j1}^2 - 1) + \sum_{\substack{1\le j\le s\\ j\notin J}} b_{jk}(w_{j2}^2 - w_{j1}^2) = c_k, & k = 1, \dots, t\\ u_{j3}^2 - 2u_{j2}^2 + u_{j1}^2 = 2, & j \in \alpha\\ \vdots & \\ u_{j35}^2 - 2u_{j34}^2 + u_{j33}^2 = 2, & j \in \alpha\\ \mathrm{Prod}(u_{j1}^2, v_j^2, 1), & j \in \alpha \end{cases}$$

with conditions $x_i(0) = 0$ for each $i \in I$ and $u_{j1}(0) = 0$ for each $j \in \alpha$.

We make the following two obvious observations about functions in $\mathcal{M}_p$:

(A) $f(0) = 0$ and f is constant if and only if $f = 0$.

(B) $f(0) = 0$ and f is non-constant if and only if $f(0) = 0$ and f is invertible

We will prove now that System (14) has a solution in $\mathcal{M}_p$ satisfying its corresponding vanishing conditions if and only at least one of the Systems S_α has a solution in $\mathcal{M}_p$ satisfying its vanishing conditions.

First, assume that System (14) has a solution $x_i = f_i$, $y_j = g_j$ satisfying the vanishing conditions and define

$$\alpha = \{j \in J : g_j \text{ is non-constant}\}.$$

Then S_α has the following solution satisfying its vanishing conditions (by Lemma 7.1):

$$\begin{array}{rcll} x_i & = & f_i & \\ u_{jl} & = & \frac{g_j}{2} + l - 1 & \text{for } j \in \alpha \\ v_j & = & \frac{1}{u_{jl}} & \text{for } j \in \alpha \\ w_{j1} & = & \frac{g_j - 1}{2} & \text{for } 1 \leq j \leq s \text{ and } j \notin J \\ w_{j2} & = & \frac{g_j + 1}{2} & \text{for } 1 \leq j \leq s \text{ and } j \notin J. \end{array}$$

Observe that the y_j with $j \in J - \alpha$ have been replaced by 0 (observation (A)).

Assume now that System S_α has the following solution satisfying its vanishing conditions:

$$\begin{array}{rcll} x_i & = & \chi_i & \\ u_{jl} & = & \mu_{jl} & \text{for } j \in \alpha \\ v_j & = & \nu_j & \text{for } j \in \alpha \\ w_{j1} & = & \omega_{j1} & \text{for } 1 \leq j \leq s \text{ and } j \notin J \\ w_{j2} & = & \omega_{j2} & \text{for } 1 \leq j \leq s \text{ and } j \notin J. \end{array}$$

Then the following is a solution of System (14):

$$\begin{array}{rcll} x_i & = & \chi_i & \\ y_j & = & 0 \text{ for } j \in J - \alpha & \\ y_j & = & \mu_{j2}^2 - \mu_{j1}^2 - 1 & \text{for } j \in \alpha \\ y_j & = & \omega_{j2}^2 - \omega_{j1}^2 & \text{for } 1 \leq j \leq s \text{ and } j \notin J. \end{array}$$

It only remains to show that this solution satisfies the vanishing conditions of System (14). Indeed, the condition $x_i(0) = 0$ for $i \in I$ holds because it is the same vanishing condition on the x_i as in S_α. For $j \in J$ we have $y_j(0) = 0$, which is trivially true for $j \in J - \alpha$. For $j \in \alpha$ we have $\mu_{j1}(0) = 0$ (this is a condition on S_α) and μ_{j1} is invertible (its inverse is $\pm\nu_j$). Therefore, by observation (B) the function μ_{j1} is non-constant. Observe that $(\mu_{jl})_{l=1}^{35}$ is a Büchi sequence with a non-constant term, hence, by Corollary 3.2 there exists a non-cosntant γ_j such that $\mu_{jl}^2 = (\gamma_j + l)^2$. This implies that

$$y_j = \mu_{j2}^2 - \mu_{j1}^2 - 1 = 2(\gamma_j + 1) = 2\mu_{j1}$$

hence, using the condition $\mu_{j1}(0) = 0$ for $j \in \alpha$ on S_α, we obtain $y_j(0) = 2\mu_{j1}(0) = 0$. □

8. Some geometric results

This section contains most of the geometric results that we will use in the next two sections. The arguments given here essentially are adaptations of the arguments given by Vojta in [26]. For the sake of completeness, we will perform most of the computations.

During the whole section, we assume that the base field is $\mathbb{C}$, and we write $g(X)$ for the genus of the curve X.

Let $S = (\delta_2, \delta_3, \ldots)$ be a sequence in $\mathbb{C}^*$ with pairwise distinct terms. Set $X_2 = \mathbb{P}^2(\mathbb{C})$ and for $n > 2$ let $X_n \subset \mathbb{P}^n(\mathbb{C})$ be the algebraic set defined by the equations

$$\delta_2 x_i^2 = \delta_i \delta_2 (\delta_i - \delta_2) x_0^2 - (\delta_i - \delta_2) x_1^2 + \delta_i x_2^2 \qquad (16)$$

as the index i ranges from 3 to n. If $[x_0 : \cdots : x_n] \in X_n$, it is easy to see that at most 2 of the x_i can be zero, hence $X_n \subset U_0 \cup U_1 \cup U_2$ where U_i is the open set $\{x_i \neq 0\}$.

Lemma 8.1. *The variety X_n is a smooth surface in $\mathbb{P}^n$, contains the lines*

$$\pm x_1 = \pm x_2 - \delta_2 x_0 = \cdots = \pm x_n - \delta_n x_0 \tag{17}$$

and has canonical sheaf $\mathcal{O}_{X_n}(n-5)$. In particular, X_n is of general type for $n \geq 6$.

Proof. Observe that, for $[x_0 : \cdots , x_n] \in X_n \cap U_0$ the matrix

$$\begin{bmatrix} (\delta_3 - \delta_2)x_1 & -\delta_3 x_2 & \delta_2 x_3 & 0 & \cdots & 0 \\ (\delta_4 - \delta_2)x_1 & -\delta_4 x_2 & 0 & \delta_2 x_4 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ (\delta_n - \delta_2)x_1 & -\delta_n x_2 & 0 & 0 & \cdots & \delta_2 x_n \end{bmatrix} \tag{18}$$

has rank $n-2$. Indeed, there are 3 cases depending on the number of zeroes among $x_3, \ldots, x_n$:

1. (1) No zero: trivial.
2. (2) One zero: at least one of the first two columns has no zero.
3. (3) Two zeroes: suppose that $x_i = x_j = 0$ where $3 \leq i < j \leq n$, then no entry in the first two columns is zero. Therefore
$$\begin{vmatrix} (\delta_i - \delta_2)x_1 & -\delta_i x_2 \\ (\delta_j - \delta_2)x_1 & -\delta_j x_2 \end{vmatrix} = \delta_2 x_1 x_2 (\delta_j - \delta_i) \neq 0.$$

hence, X_n is nonsingular at each point in $X_n \cap U_0$. The verification that X_n is nonsingular at each point in $X_n \cap U_1$ and $X_n \cap U_2$ is quite similar, but the determinants in case (3) are

$$\begin{vmatrix} -\delta_i \delta_2 (\delta_i - \delta_2)x_0 & -\delta_i x_2 \\ -\delta_j \delta_2 (\delta_j - \delta_2)x_0 & -\delta_j x_2 \end{vmatrix} = \delta_2 \delta_i \delta_j x_0 x_2 (\delta_j - \delta_i) \neq 0$$

and

$$\begin{vmatrix} -\delta_i \delta_2 (\delta_i - \delta_2)x_0 & (\delta_i - \delta_2)x_1 \\ -\delta_j \delta_2 (\delta_j - \delta_2)x_0 & (\delta_j - \delta_2)x_1 \end{vmatrix} = \delta_2 x_0 x_1 (\delta_j - \delta_i)(\delta_j - \delta_2)(\delta_i - \delta_2) \neq 0$$

respectively. Therefore X_n is a smooth surface in $\mathbb{P}^n$.

The claim about the lines (17) is an easy computation (looking at $U_0 \cap X_n$).

Finally, since X_n is a complete intersection surface in $\mathbb{P}^n$ defined as the intersection of $n-2$ smooth hypersurfaces of degree 2, its canonical sheaf is $\mathcal{O}(2(n-2)-n-1) = \mathcal{O}(n-5)$. □

Definition 8.2. *Define the trivial lines of X_n as the lines* (17)*.*

Observe that for $n \geq 3$ the rational map $[x_0 : \cdots : x_n] \mapsto [x_0 : \cdots : x_{n-1}]$ induces a finite morphism $\pi_n : X_n \to X_{n-1}$ of degree 2 ramified along the curve $C_n \subset X_n$ defined by $x_n = 0$. This curve is nonsingular. Indeed, if

$$[x_0 : \cdots : x_n] \in C_n = X_n \cap \{x_n = 0\}$$

then at most one of the $x_0, \ldots, x_{n-1}$ can be zero and the remaining verification can be performed as in the proof of Lemma 8.1 for cases (2) and (3) since $x_n = 0$, but adding the extra row $(0, \ldots, 0, 1)$ to each matrix.

Define $\phi_n = \pi_3 \circ \cdots \circ \pi_n$. We note that the image of C_n in X_2 via ϕ_n is

$$\delta_n \delta_2 (\delta_n - \delta_2) x_0^2 - (\delta_n - \delta_2) x_1^2 + \delta_n x_2^2 = 0. \tag{19}$$

Definition 8.3. *Let X be a smooth surface over $\mathbb{C}$ and let $\mathcal{L}$ be an invertible sheaf on X. Take a section $\omega \in H^0(X, \mathcal{L} \otimes S^2(\Omega^1_X))$. Let $Y \subset X$ be a curve with normalization $i : \tilde{Y} \to Y$. We say that Y is $\omega-$*integral *if $i^*\omega \in H^0(\tilde{Y}, i^*(\mathcal{L}) \otimes S^2(\Omega^1_{\tilde{Y}}))$ vanishes identically on $\tilde{Y}$.*

On $U_0 \subset \mathbb{P}^2 = X_2$ define

$$\omega = x_1 x_2 dx_1 \otimes dx_1 + (\delta_2^2 - x_1^2 - x_2^2) dx_1 \otimes dx_2 + x_1 x_2 dx_2 \otimes dx_2.$$

Note that, after the change of variables $y_0 = x_0/x_1$ and $y_2 = x_2/x_1$, on $U_0 \cap U_1$, we have

$$\omega = \frac{1}{y_0^5}\left(\delta_2^2 y_0 y_2 dy_0 \otimes dy_0 + (1 - \delta_2^2 y_0^2 - y_2^2) dy_0 \otimes dy_2 + y_0 y_2 dy_2 \otimes dy_2\right)$$

hence ω extends to a section

$$\omega_2 \in H^0(X_2, \mathcal{O}_{X_2}(5) \otimes S^2(\Omega^1_{X_2})).$$

Lemma 8.4. *Write $[x_0 : x_1 : x_2]$ for homogeneous coordinates on $\mathbb{P}^2 = X_2$. The only ω_2-integral curves on X_2 are*

1. *$x_0 = 0$, $x_1 = 0$, and $x_2 = 0$*
2. *the four trivial lines*
3. *the conics $\delta_2 c(c - \delta_2)x_0^2 - (c - \delta_2)x_1^2 + cx_2^2 = 0$ for $c \neq 0, \delta_2$.*

Moreover, if $f \colon \mathbb{C} \to X_2(\mathbb{C})$ is a non-constant holomorphic map satisfying $f^*\omega_2 = 0$ then its image is contained in one of these curves.

Proof. It is easy to see that curves of type (1) and (2) are ω_2-integral. Let's show that curves of type (3) are ω_2-integral. If we look at the affine chart U_0, on a curve of type (3) we have

$$(c - \delta_2)x_1 dx_1 = cx_2 dx_2$$

hence

$$\begin{aligned}
\omega_2 &= \left(\frac{c^2 x_2^3}{(c - \delta_2)^2 x_1} + \frac{cx_2}{(c - \delta_2)x_1}(\delta_2^2 - x_1^2 - x_2^2) + x_1 x_2\right) dx_2 \otimes dx_2 \\
&= \left(c^2 x_2^2 + c(c - \delta_2)(\delta_2^2 - x_1^2 - x_2^2) + (c - \delta_2)^2 x_1^2\right) \frac{x_2 dx_2 \otimes dx_2}{(c - \delta_2)^2 x_1} \\
&= \left(\delta_2^2 c(c - \delta_2) - \delta_2(c - \delta_2)x_1^2 + \delta_2 c x_2^2\right) \frac{x_2 dx_2 \otimes dx_2}{(c - \delta_2)^2 x_1} \\
&= \delta_2\left(\delta_2 c(c - \delta_2) - (c - \delta_2)x_1^2 + cx_2^2\right) \frac{x_2 dx_2 \otimes dx_2}{(c - \delta_2)^2 x_1} = 0.
\end{aligned}$$

Conversely, let Y be an ω_2-integral curve on X_2 not of type (1) or (2). We will show that Y is of type (3). Let $P \in Y$ be a regular point of Y not in a line of type (1) nor (2). As Y is regular at P, in some neighborhood of P one can assume that one affine coordinate is function of the other, say $x_1 = x_1(x_2)$. Since Y is ω_2-integral, we get a quadratic ordinary differential equation for x_1. Hence there are 2 local solutions at P. But exactly 2 curves of type (3) pass through P. Therefore, Y is locally of type (3) on a dense set of points, and so Y is of type (3).

A similar computation proves the assertion about holomorphic maps. □

Observe that the image of C_n in X_2 is ω_2-integral (see Equation (19)).

Write $\omega'_n = \phi_n^*\omega_2$ and note that

$$\omega'_n \in H^0(X_n, \mathcal{O}_{X_n}(5) \otimes S^2(\Omega^1_{X_n}))$$

because $\pi_n^*\mathcal{O}_{X_{n-1}}(1) = \mathcal{O}_{X_n}(1)$ for each $n \geq 3$.

Lemma 8.5. *Let $n \geq 6$ be an integer. The only ω'_n-integral curves on X_n are*

1. *the pull-backs via ϕ_n of the coordinate axes on X_2 to X_n*
2. *the trivial lines*
3. *the pull-backs via ϕ_n of the conics $\delta_2 c(c - \delta_2)x_0^2 - (c - \delta_2)x_1^2 + cx_2^2 = 0$ for $c \neq 0, \delta_2$.*

These curves are nonsingular and the only one with genus $\leq 2^{n-3}$ are the trivial lines, with genus 0. Moreover, if $h : \mathbb{C} \to X_n(\mathbb{C})$ is a non-constant holomorphic map satisfying $h^*\omega'_n = 0$ then the image of h is contained in one of these curves.

Proof. Let $Y \subset X_n$ be a ω'_n-integral curve. Write $Z = \phi_n(Y)$ and $Y' = \phi_n^*(Z)$. Note that Z is ω_2-integral. Hence we have 3 cases by Lemma 8.4.

Suppose that $Z = \{x_j = 0\} \subset X_2$ is a coordinate axe. Then $Y' = X_n \cap \{x_j = 0\}$ is nonsingular by a verification similar to the one done for C_n. Since Z meets all the curves $\phi(C_i)$ for $i = 3, \ldots, n$ and they form the branch divisor, Y' is connected. Hence $Y' = Y$ and Y is nonsingular. Note that

$\phi_n|_Y : Y \to Z$ has degree 2^{n-2} and is ramified at $2^{n-2}(n-2)$ points, hence $g(Y) = 2^{n-3}(n-4)+1$ by the Hurwitz formula.

Now suppose that Z is a trivial line in X_2. Replacing the value of x_2 in terms of x_1 in the defining equations of X_n we obtain that Y is a trivial line, with genus 0.

Finally suppose that Z is a curve of type (3) in Lemma 8.4. By the same argument as in the first case, Y' is connected. One can show that Y' is nonsingular by a direct computation (on the affine chart U_0 we add the row $((c-\delta_2)x_1, -cx_2, 0, \dots, 0)$ in 18, and for U_1, U_2 the computation is similar) therefore $Y = Y'$. Consider the map $\phi_n|_Y : Y \to Z$. This map induces a morphism $\psi_n : Y \to Z$. If Y lies above one of the curves C_i then $\deg(\psi_n) = 2^{n-3}$ and if Y does not lie above any C_i then $\deg(\psi_n) = 2^{n-2}$. Anyway, ϕ_n is ramified at least in $(n-3)\cdot 4 \cdot 2^{n-4} = 2^{n-2}(n-3)$ points and $g(Z) = 0$, thus for $n \geq 6$ by the Hurwitz formula we have

$$g(Y) > -2^{n-2} + 2^{n-3}(n-3) = 2^{n-3}(n-5) \geq 2^{n-3}.$$

The assertion about holomorphic maps follows from taking $f = \phi_n \circ h$ in Lemma 8.4 and noting that f is not constant since ϕ_n is finite, and $f^*\omega_2 = h^*\psi_n^*\omega_2 = h^*\omega_n' = 0$. □

Lemma 8.6. *Let $\pi : X' \to X$ be a finite morphism of smooth projective surfaces over $\mathbb{C}$, ramified along a curve $Y \subset X'$. Let $\mathcal{L}$ be a invertible sheaf on X, and take a section $\omega \in H^0(X, \mathcal{L} \otimes S^2(\Omega^1_X))$. If $\pi(Y)$ is $\omega-$integral, then $\pi^*\omega \in H^0(X', \pi^*\mathcal{L} \otimes S^2(\Omega^1_{X'}))$ vanishes identically on Y.*

Proof. This is a particular case of [26] Lemma 2.10. □

We recall to the reader that $\omega_n' = \phi_n^*\omega_2$.

Lemma 8.7. *Define $\omega_2' = \omega_2$. The sections ω_n' determine sections*

$$\omega_n \in H^0(X_n, \mathcal{O}_{X_n}(7-n) \otimes S^2(\Omega^1_{X_n}))$$

such that each ω_n-integral curve is a $\omega_n'-$integral curve. Moreover, the ω_n-integral curves are the same as the $\omega_n'-$integral curves, with the only possible exception of $\omega'-$integral curves lying over $C_3, \dots, C_n$.

Proof. By induction. The case $n = 2$ is clear. Assume it for $n = m-1$ with $m > 2$. Note that $\pi_m(C_m)$ does not lie over any of the curves $C_3, \dots, C_{m-1}$ because they have different images in X_2, hence $\pi_m(C_m)$ is $\omega_{m-1}-$integral by Lemma 8.5 and induction hypothesis. Consider the section

$$\pi_m^*\omega_{m-1} \in H^0(X_m, \pi_m^*\mathcal{O}_{X_{m-1}}(7-(m-1)) \otimes S^2(\Omega^1_{X_m})) = H^0(X_m, \mathcal{O}_{X_m}(7-(m-1)) \otimes S^2(\Omega^1_{X_m}))$$

(recall that $\pi_n^*\mathcal{O}_{X_{n-1}}(1) = \mathcal{O}_{X_n}(1)$). By Lemma 8.6 we have that $\pi_m^*\omega_{m-1}$ vanishes identically on C_m, thus $\pi_m^*\omega_{m-1}$ determines a global section ω_m in $\mathcal{O}_{X_m}(7-m) \otimes S^2(\Omega^1_{X_m})$ by taking

$$\omega_m = \frac{1}{x_m}\pi_m^*\omega_{m-1}.$$

Call U_m the open set of X_m obtained by deleting the curves lying over any of the $C_3, \dots, C_m$. The sections ω_m' and ω_m agree on U_m up to a non-vanishing factor, therefore the $\omega_m'-$integral curves and the ω_m-integral curves are the same on U_m. A curve lying over some C_i is of type (3) in Lemma 8.5 (see Equation 19), hence it is ω_m'-integral, and we are done. □

Corollary 8.8. *For $n \geq 6$, the only ω_n-integral curves with genus $\leq 2^{n-3}$ on X_n are the trivial lines, with genus 0. Moreover, if $h : \mathbb{C} \to X_n(\mathbb{C})$ is a non-constant holomorphic map such that $h^*\omega_n = 0$ then the image of h lies in a trivial line.*

Proof. From Lemma 8.5 and Lemma 8.7 we deduce the first part of the Lemma, and the fact that the image of h lies in a curve with genus $> 2^{n-3}$ or in a trivial line. Use Picard's Theorem to conclude. □

Theorem 8.9. *For $n \geq 8$, the only curves of genus 0 or 1 on X_n are the trivial lines.*

Proof. Let $Y \subset X_n$ be a curve of genus 0 or 1 and write $i : \tilde{Y} \to Y$ for its normalization. On the one hand, the curve $\tilde{Y}$ has genus 0 or 1, hence $\mathcal{K}_{\tilde{Y}}$ has non-positive degree. On the other hand, the sheaf $i^*\mathcal{O}_{X_n}(7-n)$ has negative degree because $n \geq 8$. Therefore, $i^*\mathcal{O}_{X_n}(7-n) \otimes \mathcal{K}_{\tilde{Y}}^{\otimes 2}$ has no nonzero global section on $\tilde{Y}$, hence $i^*\omega_n$ vanishes identically on $\tilde{Y}$. From this we deduce that Y is a ω_n-integral curve with genus ≤ 1 on X_n, and we are done by Corollary 8.8. □

9. Correspondence between polynomials and points

We understand that, given a sequence $\delta_2, \delta_3, \dots$ of distinct non-zero elements in $K/\mathbb{Q}$, the surfaces X_n are defined by Equation (16).

Lemma 9.1. *Fix a sequence $(a_1, a_2, \dots a_n)$ in $K/\mathbb{Q}$, with $n \geq 3$ and pairwise distinct a_i. Set $\delta_i = a_i - a_1$ for $i \geq 2$. There is an injective map from the set of monic polynomials $f \in K[x]$ of degree two satisfying that $f(a_i)$ is a square for $i = 1, \dots, n$, to the set $X_n(K) \cap \{x_0 \neq 0\}$. The map is $j(f) = [1 : \sqrt{f(a_1)} : \dots : \sqrt{f(a_n)}]$ (for a fixed choice of square roots) and has the property that f is a square in $K[x]$ if and only if $j(f)$ lies in a trivial line of X_n.*

Proof. Take a polynomial $f = x^2 + ax + b \in K[x]$ with the property that $f(a_1) = b_1^2, \dots, f(a_n) = b_n^2$ are squares in K, then

$$\begin{aligned}\delta_2 b_i^2 &= (a_2 - a_1)f(a_i) = (a_2 - a_1)(a_i^2 + ua_i + v)\\ &= (a_i - a_1)(a_2 - a_1)(a_i - a_2)\cdot 1 - (a_i - a_2)(a_1^2 + ua_1 + v) + (a_i - a_1)(a_2^2 + ua_2 + v)\\ &= \delta_i\delta_2(\delta_i - \delta_2)1^2 - (\delta_i - \delta_2)b_1^2 + \delta_i b_2^2\end{aligned}$$

Therefore, for each polynomial $f = x^2 + ux + v \in K[x]$ with the property that $f(a_1), \dots, f(a_n)$ are squares in K, we have that $j(f) \in X_n(K) \cap \{x_0 \neq 0\}$.
Now we check injectivity. Given a point $p = [1 : b_1 : \dots : b_n] \in X_n(K) \cap \{x_0 \neq 0\}$, define

$$f_p = x^2 + \frac{b_2^2 - b_1^2 - a_2^2 + a_1^2}{a_2 - a_1}x + \frac{a_1a_2(a_2 - a_1) - a_1b_2^2 + a_2b_1^2}{a_2 - a_1} \in K[x]$$

The polynomial f_p is the *only* monic polynomial of degree two satisfying $f_p(a_1) = b_1^2$ and $f_p(a_2) = b_2^2$. Moreover, after a standard computation we get

$$\delta_2 f_p(a_1 + \delta_i) = \delta_i\delta_2(\delta_i - \delta_2) - (\delta_i - \delta_2)b_1^2 + \delta_i b_2^2$$

and, since $p \in X_n(K) \cap \{x_0 \neq 0\}$, we obtain $\delta_2 f_p(a_1 + \delta_i) = \delta_2 b_i^2$. Therefore $f_p(a_i) = b_i^2$ for each i. The uniqueness of f_p proves that j is injective.

Assume that $j(g) = [1 : b_1 : \dots : b_n]$ lies in a trivial line for some $g = x^2 + ux + v \in K[x]$. Thus we have an equation of the kind $\pm b_2 - \delta_2 = \pm b_1$, say $\epsilon' b_2 = \epsilon b_1 + a_2 - a_1$ for $\epsilon, \epsilon' \in \{1, -1\}$. Therefore $b_2^2 = b_1^2 + 2\epsilon(a_2 - a_1)b_1 + (a_2 - a_1)^2$ and we get

$$\left(\frac{b_2^2 - b_1^2 - a_2^2 + a_1^2}{a_2 - a_1}\right)^2 - 4\left(\frac{a_1a_2(a_2 - a_1) - a_1b_2^2 + a_2b_1^2}{a_2 - a_1}\right) = 4b_1^2(\epsilon^2 - 1) = 0$$

So, using the above definition of f_p, we have $g = f_{j(g)} = \left(x + \frac{u}{2}\right)^2$. □

10. Case of number fields, function fields and complex meromorphic functions

We use the same notation as in Section 8. First we prove Theorem 3.7.

Proof. We follow the notation of Section 8. For $i = 2, \dots, 8$ set $\delta_i = a_i - a_1$ and note that $X_2, \dots, X_8$ are defined over K. If Conjecture 1.2 holds then there exists a proper Zariski closed subset $Z \subset X_8$ such that all the K-rational points of X_8 belong to Z. Given an irreducible curve $Y \subset X_n$, if $Y(K)$ is dense in $Y(\mathbb{C})$ then Y is defined over K and, by Faltings' Theorem, Y has genus at most 1. Therefore we can take Z as the union of a finite number of curves on X_8 with genus 0 or 1, up to a finite number of K-rational points. We conclude by Theorem 8.9 and Lemma 9.1. □

Let us prove Corollary 3.8.

Proof. Since the set $E(\mathbb{Q}, (a_i)_i)$ is finite, it is enough to show that a monic polynomial $f \in \mathbb{Z}[z]$ which is not a square, is such that $f(n)$ is a square at most for a finite number of $n \in \mathbb{Z}$. Indeed, the graph of $y = \sqrt{f(x)}$ is asymptotic to the graph of $y = |x|$, and hence has no integer point for large enough $|x|$. □

The next proposition will be useful to prove Theorem 3.9.

Proposition 10.1. *Let $n \geq 8$. If $Y \subseteq X_n$ is a curve, its normalization is $i : \tilde{Y} \to Y$ and $g(\tilde{Y}) < \frac{n-3}{4}$, then Y is an ω_n-integral curve.*

Proof. Let $i : \tilde{Y} \to Y$ be the normalization map. We have

$$i^*\omega_n \in H^0(X_n, i^*\mathcal{O}(7-n) \otimes \mathcal{K}_{\tilde{Y}}^{\otimes 2}).$$

As $\deg i^*\mathcal{O}_{X_n}(1) \geq 1$, for $n \geq 8$ we get

$$\begin{aligned}\deg\left(i^*\mathcal{O}_{X_n}(7-n) \otimes \mathcal{K}_{\tilde{Y}}^{\otimes 2}\right) &= (7-n)\deg i^*\mathcal{O}_{X_n}(1) + 4g(\tilde{y}) - 4\\ &\leq 7 - n + 4g(\tilde{Y}) - 4\\ &= 4g(\tilde{Y}) + 3 - n < 0.\end{aligned}$$

Therefore, $i^*\omega_n$ is zero in $\tilde{Y}$. □

Now we present the proof of Theorem 3.9.

Proof. We can assume $F = \mathbb{C}$. Suppose P has some non-constant coefficient and $P(a_i) = h_i^2, i = 1, \ldots, M$ for some $a_i \in \mathbb{C}$ and $h_i \in K(C)$. Using Lemma 9.1 with $K = K(C)$, one can verify that $h = [1 : h_1 : \ldots : h_M]$ defines a non-constant morphism $h : C \to X_M$, where we consider $\delta_i = a_i - a_1$ in the definition of X_M. Since C is a complete variety we obtain that $\mathrm{im}(h)$ is algebraic. Let Y be an irreducible curve containing $\mathrm{im}(h)$, since h is dominant on Y, we conclude that h factors through $\tilde{Y}$. By Riemann-Hurwitz Formula, we have

$$g(\tilde{Y}) \leq g(C) \leq \frac{M}{4} - 1 < \frac{M-3}{4}$$

hence Y is a ω_M integral curve by the previous Lemma. Finally, Lemma 8.8 implies that $\mathrm{im}(h)$ is contained in a trivial line, and the conclusion follows from Lemma 9.1. □

Before proving Theorem 3.10 we need to fix some notation in complex Nevanlinna theory. We refer the reader to the notes [27] on Diophantine Approximation and Complex Nevanlinna Theory, where Vojta gives a concise and self-contained introduction to this topic. We follow the notation used there.

Let X be a smooth projective variety over $\mathbb{C}$. For each divisor $D \in \mathrm{Div}(X)$ and for each holomorphic map $f : \mathbb{C} \to X$ whose image is not contained in the support of D, we denote by $T_{D,f} : \mathbb{R}^+ \to \mathbb{R}$ the *Nevanlinna height function* associated to D and f. Moreover, one can define (up to a bounded term as r varies) a *Nevanlinna height function* for line sheaves by letting $T_{\mathcal{L},f} = T_{D,f}$, where $D \in \mathrm{Div}(X)$ can be any divisor such that $\mathcal{L} = \mathcal{O}(D)$ and the image of f is not contained in D. There is a formal analogy between these height functions and the ones produced by the Weil Height Machine in the context of heights for algebraic points on varieties. Indeed, this is part of a deep formal analogy between Nevanlina Theory for holomorphic maps and Diophantine Approximation; see for example [13] or [25].

We need the following result:

Theorem 10.2 (See [26] Prop. 6.1). *Let X be a complex non-singular projective variety, $f : \mathbb{C} \to X$ an holomorphic curve, $d > 0$ an integer, $\mathcal{L}$ a line sheaf on X, ω a global section of $\mathcal{L}^\vee \otimes S^d\Omega_X^1$, and $\mathcal{A}$ an ample line sheaf on X. If $f^*\omega$ is not identically zero, then there exists a set $U \subseteq \mathbb{R}^+$ of finite Lebesgue measure such that for any $r \notin U$ we have*

$$T_{\mathcal{L},f}(r) \leq O(\log T_{\mathcal{A},f}(r)) + o(\log r).$$

Proof of Theorem 3.10. Let $P \in \mathcal{M}[X]$ be a monic second degree polynomial, with some non-constant coefficient, which is not a square in $\mathcal{M}[X]$, and assume that there exists $a_1, a_2, \ldots, a_8 \in \mathbb{C}$ such that $P(a_i)$ is a square in $\mathcal{M}$ for each i, say

$$\sqrt{P(a_i)} = h_i \in \mathcal{M}.$$

Since P has some non-constant coefficient, some of the h_i is non-constant. By Lemma 9.1 we have that $h := [1 : h_1 : \cdots : h_8]$ does not belong to a trivial line of $X_8(\mathcal{M})$, that is, the image of the non-constant holomorphic map $h : \mathbb{C} \to X_8(\mathbb{C})$ is not contained in the trivial lines.

Now take $\mathcal{L} = \mathcal{O}(1)$. Since $\mathcal{L}$ is the line sheaf associated to a hyperplane divisor on X_8, it is very ample. Note that $\mathcal{O}(1)^\vee \simeq \mathcal{O}(-1)$ and consider the section ω_8 of

$$\mathcal{O}(-1) \otimes S^2\Omega^1_{X_8}.$$

Taking $\mathcal{L} = \mathcal{A} = \mathcal{O}(1)$, $f = h$, $d = 2$ and $\omega = \omega_8$ in Theorem 10.2 we conclude that $h^*\omega_8 = 0$ because h is non-constant. By Corollary 8.8, the image of h must be contained in the trivial lines, a contradiction. □

References

[1] D. Allison, *On square values of quadratics*, Math. Proc. Camb. Philos. Soc. **99**, no. 3, 381-383 (1986).

[2] W. Berkovich, *Spectral theory and analytic geometry over non-Archimedean fields*, Math. Surveys and Monographs, Coll. Amer. Math Soc. (1990).

[3] J. Browkin and J. Brzeziński, *On sequences of squares with constant second differences*, Canad. Math. Bull. **49-4**, 481-491 (2006).

[4] W. Cherry and Z. Ye, *Non-Archimedean Nevanlinna theory in several variables and non-Archimedean Nevanlinna inverse problem*, Transactions of the American Mathematical Society **349**, 5047-5071, (1997).

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

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

[7] D. Hensley, *Sequences of squares with second difference of two and a problem of logic*, unpublished (1980-1983).

[8] P. C. Hu and C. C. Yang, *Meromorphic functions over non-Archimedean fields*, Mathematics and Its Applications 522, Kluwer Academic Publishers, 2000. MR 1794326 — Zbl 0984.30027

[9] L. Lipshitz, *Quadratic forms, the five square problem, and diophantine equations*, The collected works of J. Richard Büchi (S. MacLane and Dirk Siefkes, eds.) Springer, 677-680, (1990).

[10] L. Lipshitz and T. Pheidas, *An analogue of Hilbert's tenth problem for p-adic entire functions*, Jour. Symb. Logic **60**, no. 4 (1995).

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

[12] B. Mazur, *Questions of decidability and undecidability in number theory*, The Journal of Symbolic Logic **59-2**, 353-371 (1994).

[13] C. Osgood, *A number theoretic-differential equations approach to generalizing Nevanlinna theory*, Indian J. of Math. 23 (1981), 1-15.

[14] H. Pasten, T. Pheidas and X. Vidaux, *A survey on Büchis problem: new presentations and open problems*, to appear in the Proceedings of the Workshop New methods in the Hilbert tenth problem, Hausdorff Institute of Mathematics, Bonn, Germany (2010).

[15] T. Pheidas and X. Vidaux, *The analogue of Büchi's problem for rational functions*, Journal of The London Mathematical Society **74-3**, 545-565 (2006).

[16] —— *Corrigendum: The analogue of Büchi's problem for rational functions*, to appear in the Journal of the London Mathematical Society (2010).

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

[18] R. G. E. Pinch, *Squares in Quadratic Progression*, Mathematics of Computation, **60-202**, pp. 841-845 (1993).

[19] B. Poonen, *Hilbert's Tenth Problem over rings of number-theoretic interest*, downloadable from http://math.mit.edu/∼poonen/papers/aws2003.pdf

[20] A. M. Robert, *A course in p-adic analysis*, Springer, Graduate Texts in Mathematics **198**.

[21] M. Ru, *A note on p-adic Nevanlinna Theory*, Proceedings of the American Mathematical Society, **129(5)**, 1263-1269 (2000).

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

[23] A. Shlapentokh and X. Vidaux *The analogue of Büchi's problem for function fields*, preprint.

[24] X. Vidaux, *An analogue of Hilbert's tenth problem for fields of meromorphic functions over non-Archimedean valued fields*, Journal of Number Theory **101**, Issue 1, 48-73 (2003).

[25] P. Vojta, *Diophantine Approximations and Value Distribution Theory, Lecture Notes in Mathematics 1239*, Springer-Verlag, 1987.

[26] —— *Diagonal quadratic forms and Hilbert's Tenth Problem*, Contemporary Mathematics **270**, 261-274 (2000).

[27] —— *Diophantine Approximation and Nevanlinna Theory*, available on line http://math.berkeley.edu/∼vojta/cime/cime.pdf

Department of Mathematics, Universidad de Concepción, Chile
E-mail address: hpasten@gmail.com