arXiv:1004.0731v1 [math.NT] 5 Apr 2010

THE ANALOGUE OF BÜCHI'S PROBLEM FOR FUNCTION FIELDS

ALEXANDRA SHLAPENTOKH
AND
XAVIER VIDAUX

Abstract. Büchi's n Squares Problem asks for an integer M such that any sequence $(x_0, \ldots, x_{M-1})$, whose second difference of squares is the constant sequence (2) (i.e. $x_n^2 - 2x_{n-1}^2 + x_{n-2}^2 = 2$ for all n), satisfies $x_n^2 = (x+n)^2$ for some integer x. Hensley's problem for r-th powers (where r is an integer ≥ 2) is a generalization of Büchi's problem asking for an integer M such that, given integers ν and a, the quantity $(\nu + n)^r - a$ cannot be an r-th power for M or more values of the integer n, unless $a = 0$. The analogues of these problems for rings of functions consider only sequences with at least one non-constant term.

Let K be a function field of a curve of genus g. We prove that Hensley's problem for r-th powers has a positive answer for any r if K has characteristic zero, improving results by Pasten and Vojta. In positive characteristic p we obtain a weaker result, but which is enough to prove that Büchi's problem has a positive answer if $p \geq 312g+169$ (improving results by Pheidas and the second author).

AMS Subject Classification: 03B25, 11D41, 11U05

1. Introduction

A 1990 paper by L. Lipshitz [11] containing a description of a question posed in the 70's by J. R. Büchi inspired a new interest in what is known today as "Büchi's Problem" or "the n Squares Problem" (denoted by $\mathbf{B^2}(\mathbb{Z})$ in the future):

Does there exist a positive integer M such that any sequence of M integer squares, whose second difference is constant and equal to 2, is of the form $(x+n)^2$, $n = 1, \ldots, M$, for some integer x?

Büchi asked this question because a positive answer to it would imply a stronger form of the negative answer to Hilbert's Tenth Problem solved in 1970 by Yuri Matiyasevich using results of Martin Davis, Hilary Putnam and Julia Robinson. In logical terms, Matiyasevich's result (see [13] and [5]) implies that the positive existential theory of $\mathbb{Z}$ in the language $\mathscr{L} = \{0, 1, +, \cdot\}$ of rings is undecidable. Büchi observed that a positive answer to his problem would allow him to define existentially the multiplication over $\mathbb{Z}$ in the language $\mathscr{L}^2 = \{0, 1, +, P_2\}$, where P_2 is a unary predicate for "x is a square", hence proving that the positive existential theory of $\mathbb{Z}$ in the language $\mathscr{L}^2$ is undecidable.

It makes sense to ask Büchi's question over other rings. If R is a commutative ring with identity, the problem $\mathbf{B^2}(R)$ becomes:

Date: April 7, 2010.

Does there exist a positive integer M such that any sequence of M squares in R, whose second difference is constant and equal to 2, is of the form $(x+n)^2$, $n = 0, \ldots, M-1$, for some $x \in R$?

A positive (or "almost positive") answer to $\mathbf{B^2}(R)$ *in general* has similar logical consequences to a positive answer to $\mathbf{B^2}(\mathbb{Z})$ if the existential ring theory of R is undecidable.

Büchi's Problem is still open. However, in 2001, Vojta proved in [25] that $\mathbf{B^2}(\mathbb{Q})$, and hence also $\mathbf{B^2}(\mathbb{Z})$, have a positive answer for some $M \geq 8$ if the following (open) question of Bombieri has a positive answer for surfaces:

Let X be a smooth projective algebraic variety of general type, defined over a number field k. Does there exist a proper Zariski-closed subset Z of X such that $X(k) \subseteq Z$?

Vojta's proof actually is valid for any number field as was first noted by Yamagishi in [26]. Continuing this line of investigation, in 2009, Pasten in [16] produced the following generalization of Vojta's result:

If Bombieri's Question has a positive answer, then there exists an absolute constant N (that can be chosen to be 8 if Bombieri's question is true for any surface) such that, for each number field $K/\mathbb{Q}$ and each set $\{a_1, \ldots, a_N\}$ of N elements in K, there is only a finite number of polynomials $f = x^2 + ax + b \in K[x]$ not of the form $f = (x+c)^2$, satisfiying that $f(a_i)$ are squares in K for each i.

At the same time, R. G. E. Pinch in [22] proved that 'many' non-trivial Büchi sequences of length 4 could not be extended to Büchi sequences of length 5 (originally Büchi asked his question for $M = 5$).

Before turning our attention to rings of functions, we should note that a number of people (Allison [1] in 1986, Bremner [2] in 2003, and Browkin and Brzezinski [4] in 2006) have been studying the following analogue of Büchi's problem:

Does there exist an integer M such that the system of equations

$$x_{n+2}^2 - 2x_{n+1}^2 + x_n^2 = \ell, \quad n = 0, \ldots, M-3,$$

where $\ell \in \mathbb{Z}$, has only solutions whose squares are the squares of an arithmetic progression?

Observe that this problem is related to the original Büchi's problem over an integral extension of $\mathbb{Z}$: multiply the equations by $2\ell^{-1}$ and consider the change of variables

$$y_n = \frac{\sqrt{2}}{\sqrt{\ell}} x_n.$$

In [25] Vojta also considered analogues of Büchi's Problem over rings of functions. If R_t is a ring of functions in the variable t, the problem $\mathbf{B^2}(R_t)$ becomes:

Does there exist a positive integer M such that any sequence of M squares in R_t, not all constant, whose second difference is constant and equal to 2, is of the form $(x+n)^2$,

$n = 0, \ldots, M-1$, for some $x \in R_t$?

Vojta proved that $\mathbf{B^2}(R_t)$ had a positive answer when R_t was the field of meromorphic functions over $\mathbb{C}$, or a function field of characteristic zero. In [19] and [20], T. Pheidas and the second author used a different method to show that $\mathbf{B^2}(F(t))$ had a negative answer when F had characteristic zero. The new method was also extendible to the case of F of positive characteristic. It turned out that if F had positive characteristic, $\mathbf{B^2}(F(t))$ had a *negative answer* but one could still derive all the desired logical consequences.

In 1981, D. Hensley (in [8] and [9]) proved that $\mathbf{B^2}(\mathbb{F}_p)$ had a positive answer, with $M = p$. This was the first (though as explained above not the last) positive answer to an analogue of Büchi's Problem. In the same work, he noticed that a positive answer to $\mathbf{B^2}(\mathbb{Z})$ is implied by a positive answer to what we now call Hensley's Problem denoted in the future by $\mathbf{HP^2}(\mathbb{Z})$:

Does there exist a positive integer M such that, given any integers ν and a, if the quantity $(\nu+n)^2 - a$ is a square for more than M values of n then $a = 0$?

Remark 1.1. *This implication is not hard to see. Indeed, suppose that a sequence (x_n) of integers satisfies*

$$x_n^2 - 2x_{n-1}^2 + x_{n-2}^2 = 2 \tag{1.1}$$

for $n = 2, \ldots, M-1$, namely, the sequence (x_n^2) has constant second difference equal to 2. In [21] it was noted that the quantity $\frac{x_n^2 - x_0^2}{n} - n$ does not depend on n. Denoting this quantity by 2ν, we can now rewrite (1.1) as $x_n^2 - x_0^2 = 2n\nu + n^2$. Therefore we now have

$$x_n^2 - (\nu+n)^2 = x_n^2 - \nu^2 - 2n\nu - n^2 = x_n^2 - \nu^2 - (x_n^2 - x_0^2) = -\nu^2 + x_0^2$$

which does not depend on n. Writing $a = \nu^2 - x_0^2$, we obtain $x_n^2 = (\nu+n)^2 - a$. Hence if $\mathbf{HP^2}(\mathbb{Z})$ has a positive answer for some M, then a must be zero and $\mathbf{B^2}(\mathbb{Z})$ has a positive answer with the same M.

We might consider the obvious analogues of Hensley's Problem over other rings (over a ring of functions we will ask some x_n to be non-constant). For a general discussion on the equivalence between $\mathbf{B^2}(R)$ and $\mathbf{HP^2}(R)$ (for some rings R the two problems *may not* be equivalent) see the survey [17], or [15].

In [18], T. Pheidas together with the second author proposed a generalization of Büchi's Problem to higher powers for a ring R, denoted in the future by $\mathbf{B^r}(R)$:

Does there exist a positive integer M such that any sequence of M r-th powers in R (not all constant if $R = R_t$ is a ring of functions), whose second difference is constant and equal to $r!$, is of the form $(x+n)^r$, $n = 0, \ldots, M-1$, for some $x \in R$?

It is easy to see that there is a *Hensley Formulation* of this problem which we denote by $\mathbf{HF^r}(R)$. More precisely, $\mathbf{B^r}(R)$ is equivalent (over *many* rings) to the following question:

Does there exist a positive integer M such that, for all ν, a_0, ..., a_{r-2} in R, if the quantity

$$(\nu+n)^r + a_{r-2}n^{r-2} + \cdots + a_1 n + a_0$$

is an r-th power x_n^r for more than M values of n then $a_0 = \cdots = a_{r-2} = 0$?

Again, if R is a ring of functions, we ask for some x_n to be non-constant. In [21], Pheidas and the second author proved that $\mathbf{HF^3}(F[t])$, hence also $\mathbf{B^3}(F[t])$, had a positive answer with $M = 92$, if the field F has characteristic zero.

In [15], Pasten considered the following problem, called now Hensley's Problem for r-th powers and denoted by $\mathbf{HP^r}(R)$:

Does there exist a positive integer M such that, for all ν and a in R, if the quantity

$$(\nu+n)^r - a$$

is an r-th power x_n^r for more than M values of n then $a = 0$?

As usual, if R is a ring of functions, we ask for some x_n not to be constant. Pasten proved that $\mathbf{HP^r}(F[t])$ had a positive answer if F had characteristic zero, for any $r \geq 2$. This result was a new evidence that $\mathbf{B^r}(F[t])$ had a positive answer for any power r.

Let K be a function field. In this paper we prove that $\mathbf{HP^r}(K)$ has a positive answer for any r if K has characteristic zero (see Theorem 1.3 below). This implies in particular that $\mathbf{B^2}(K)$ has a positive answer. We also prove that an analogue of $\mathbf{B^2}(K)$ has a positive answer if K has (large enough) positive characteristic (see Theorem 1.4 below) while obtaining all the desired logical consequences as in the case of the rational function fields of positive characteristic. More specifically we show that while there are non-trivial solutions to Büchi's equations for large enough M, they are of a specific form (these non-trivial solutions were discovered by Pasten, see [20]).

For both results, the number M depends only on r and the genus of K. Note that the dependence on the genus is to be expected: if M did not depend on the genus then we could add to K "enough" r-th powers (while increasing the genus) in order for $(\nu+n)^r - a$ to be an r-th power for a few more values of n.

In order to state the main theorems we introduce the following notation.

Notation 1.2. (1) *Let K be a function field of genus g over a field of constants F and let F_0 be the prime field of K.*

(2) *Let $r \geq 2$ and $M \geq 1$ be natural numbers.*

(3) *If $\bar{c} = (c_0, \ldots, c_{M-1})$ is a sequence of distinct elements of F and ξ is a primitive r-th root of unity, we write*

$$c_{i,j,n} = \frac{c_i - \xi^n c_j}{1 - \xi^n}$$

for any indices i and j and for any $n \in \{1, \ldots, r-1\}$.

(4) *Given $\bar{c}$ as above, let $\ell(\bar{c})$ be equal to 3 if either $\mathrm{char}(F)$ does not divide r and for all indices i, j, k, m, n we have $c_{i,j,n} \neq c_{i,k,m}$, or for all indices i, j, k we have*

$$[F_0(c_i, c_j, c_k, \xi) \colon F_0(c_i, c_j, c_k)] = r - 1$$

(in particular, the latter happens if $\mathrm{char}(F) = 0$ and c_i are rational numbers). Otherwise set $\ell(\bar{c}) = r + 1$.

(5) *Let*

$$B(r,\ell) = \beta_0(r,\ell)g + \beta_1(r,\ell)$$

and

$$\beta_0 = \left(8r + 4 + \frac{3r}{r-1}\right) r^2\ell, \qquad \text{and} \qquad \beta_1 = \left(4r + 2 + \frac{2r}{r-1}\right) r^2\ell + 1.$$

Theorem 1.3. *Let K be a function field of genus g over a field of constants F of characteristic 0. Let $a, \nu \in K$ and $(x_0, \ldots, x_{M-1})$ be a sequence of elements of K such that at least one x_i is not in F. Let $\bar{c} = (c_0, \ldots, c_{M-1})$ be a sequence of distinct elements of F. If $M \geq B(r,\ell)$ and the sequence satisfies*

$$x_n^r = (\nu + c_n)^r - a, \quad n = 0, \ldots, M-1 \tag{1.2}$$

then $a = 0$.

Theorem 1.4. *Let K be a function field of genus g over a field of constants F of characteristic $p \geq B(2,3)$. Let $a, \nu \in K$ and $(x_0, \ldots, x_{M-1})$ be a sequence of elements of K such that at least one x_i is not in F. If $M \geq B$, then the sequence satisfies*

$$x_n^2 = (\nu + n)^2 - a,\ n = 0, \ldots, M-1 \tag{1.3}$$

if and only if, either $a = 0$, or there exists a non-negative integer s and $f \in K$ such that for all n we have

$$x_n = (f+n)^{\frac{p^s+1}{2}}. \tag{1.4}$$

Let $\mathscr{L}_\tau^2 = \mathscr{L}^2 \cup \{\tau\}$ be the language obtained by adding to $\mathscr{L}^2$ a symbol of unary function τ for multiplication by a transcendental element t of K. Similarly, let $\mathscr{L}_\tau = \mathscr{L} \cup \{\tau\}$ be the language obtained by adding to $\mathscr{L}$ the symbol τ.

In this notation we obtain the following corollaries in Logic:

Corollary 1.5. *If K is a function field of genus g over a field of constants F of characteristic 0 or $p \geq B(2,3)$, then multiplication over K is positive-existential in the languages $\mathscr{L}_\tau^2$.*

Corollary 1.6. *If K is a function field of genus g over a field of constants F of characteristic 0 or $p \geq B(2,3)$, then the positive existential theory of K in $\mathscr{L}_\tau^2$ is undecidable if and only if the positive existential theory of K in $\mathscr{L}_\tau$ is undecidable.*

There are many function fields for which the positive existential theory is known to be undecidable. For more information, we refer the interested reader to [6], [23] and [24].

2. Technical preliminaries

Notation and Assumptions 2.1. *Below we will use the following notation and assumptions.*

(1) *Let K be a function field of genus g over a field of constants F and let F_0 be the prime field of K.*
(2) *A* prime *of K is a valuation of K.*
(3) *Let ξ be a primitive r-th root of unity.*
(4) *If $\mathfrak{I}$ is an effective (i.e. integral) divisor, we will denote by* $\deg \mathfrak{I}$ *the degree of $\mathfrak{I}$.*

(5) *If $\mathfrak{I}_1$ and $\mathfrak{I}_2$ are integral divisors, we write $\mathfrak{I}_1|\mathfrak{I}_2$ ($\mathfrak{I}_1$ divides $\mathfrak{I}_2$) to mean that for all primes $\mathfrak{p}$ of K we have that $\mathrm{ord}_{\mathfrak{p}}\mathfrak{I}_1 \leq \mathrm{ord}_{\mathfrak{p}}\mathfrak{I}_2$. Similarly for any prime $\mathfrak{p}$ of K we write that $\mathfrak{p}|\mathfrak{I}_1$ ($\mathfrak{p}$ divides $\mathfrak{I}_1$) to mean $\mathrm{ord}_{\mathfrak{p}}\mathfrak{I}_1 > 0$.*

(6) *For $x \in K$, let $\mathfrak{n}(x)$ denote the zero divisor of x and $\mathfrak{d}(x)$ the pole divisor of x. Let $\mathfrak{D}(x) = \frac{\mathfrak{n}(x)}{\mathfrak{d}(x)}$ be the divisor of x. Let $\mathrm{H}(x)$ denote the height of x, i.e. $\deg \mathfrak{d}(x) = \deg \mathfrak{n}(x)$.*

(7) *Let $\mathfrak{p}_\infty$ be a valuation of K.*

(8) *Let $t \in K \setminus F$ having a pole at $\mathfrak{p}_\infty$ only (such a t exists by* [7, Fried and Jarden, Lemma 3.2.3, p. 55]*). We can also assume that t is not a p-th power in the case K has characteristic $p > 0$ (by taking successive p-th roots if necessary).*

(9) *For a prime $\mathfrak{p}$ of K, let $e(\mathfrak{p})$ be the ramification degree of $\mathfrak{p}$ over $F(t)$.*

(10) *We can define a global derivation with respect to t as in Mason* [12, p. 9]*. Given an element x of K, the derivative with respect to t will be denoted in the usual fashion as x' or $\frac{dx}{dt}$. Observe that usual differentiation rules apply to the global derivation with respect to t. Thus, the only functions with the global derivative with respect to t equal to zero are constants in the case the characteristic is equal to zero and p-th powers in the case the characteristic is equal to $p > 0$.*

(11) *If the field F is algebraically closed and $\mathfrak{p}$ is a prime of K we can also define a local derivation with respect to the prime $\mathfrak{p}$ as in Mason* [12, p. 9]*. The derivative of $x \in K$ with respect to $\mathfrak{p}$ will be denoted as $\frac{\partial x}{\partial \mathfrak{p}}$.*

(12) *For all primes $\mathfrak{p}$, let*

$$d(\mathfrak{p}) = \mathrm{ord}_{\mathfrak{p}}\left(\frac{\partial t}{\partial \mathfrak{p}}\right)$$

and let

$$\mathfrak{E} = \prod_{d(\mathfrak{p})>0} \mathfrak{p}^{d(\mathfrak{p})}.$$

(13) *If $\mathfrak{A}$ is a divisor of K, we will write*

$$L(\mathfrak{A}) = \{f \in K \mid \mathrm{ord}_{\mathfrak{p}} f \geq -\mathrm{ord}_{\mathfrak{p}}\mathfrak{A} \text{ for all primes } \mathfrak{p} \text{ of } K\}$$

and $\ell(\mathfrak{A})$ for the dimension of $L(\mathfrak{A})$ over F.

(14) *Throughout the paper the following constants will be used:*

$$C_1 = g + 1, \qquad C_2 = 3g$$

$$C_3 = C_2 + 2 = 3g + 2 \qquad \text{and} \qquad C_4 = C_2 + C_1 + 1 = 4g + 2.$$

Assumption 2.2. *Without loss of generality, we may assume that F is algebraically closed (therefore, all primes of K, in particular $\mathfrak{p}_\infty$, have degree 1).*

The following lemma gathers some general formulae we need in this section.

Lemma 2.3. (1) *Let E be a finite degree subfield of K. Let $\mathfrak{P}$ be a prime of E and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the primes in K above $\mathfrak{P}$. Let $e(\mathfrak{p}_i/\mathfrak{P})$ be the ramification index of $\mathfrak{p}_i$ over $\mathfrak{P}$. Let $f(\mathfrak{p}_i/\mathfrak{P})$ be the relative degree of $\mathfrak{p}_i$ over $\mathfrak{P}$ (the degree of the extension of the residue field). We have*

$$[K : E] = \sum_{i=1}^{n} e(\mathfrak{p}_i/\mathfrak{P}) f(\mathfrak{p}_i/\mathfrak{P}).$$

(2) *(Riemann-Roch) Let* $\mathfrak{A}$ *be a divisor of* K *of degree* d*.*
   (a) *If* $g = 0$ *then* $\ell(\mathfrak{A}) = d + 1$*;*
   (b) *If* $g > 0$ *and* $0 < d < 2g - 2$ *then* $\ell(\mathfrak{A}) \geq d - g + 1$*;*
   (c) *If* $g > 0$ *and* $d = 2g - 2$ *then* $\ell(\mathfrak{A}) \geq g - 1$*;*
   (d) *If* $g > 0$ *and* $d > 2g - 2$ *then* $\ell(\mathfrak{A}) = d - g + 1$*;*

Proof. For (1) see Fried and Jarden [7, Proposition 2.3.2, Theorem 3.6.1]. For (2) see Koch [10, Theorem 5.6.2]. □

Lemma 2.4. *If* $\mathfrak{A}$ *is a divisor of* K *of degree* $g + 1$ *then* $\ell(\mathfrak{A}) \geq 2$*.*

Proof. Since $\mathfrak{A}$ has degree $d = g + 1$, we have

- if $g = 0$ then $d = 1$ and $\ell(\mathfrak{A}) = d + 1 = 2$ by Lemma 2.3 (2a);
- if $g = 1$ or 2 then $d > 2g - 2$ and $\ell(\mathfrak{A}) = d - g + 1 = 2$ by Lemma 2.3 (2d);
- if $g = 3$ then $d = 4 = 2g - 2$ and $\ell(\mathfrak{A}) \geq g - 1 = 2$ by Lemma 2.3 (2c);
- if $g \geq 4$ then $d = g + 1 < 2g - 2$ and $\ell(\mathfrak{A}) \geq d - g + 1 = 2$ by Lemma 2.3 (2b).

Hence in all cases, $\ell(\mathfrak{A}) \geq 2$. □

Lemma 2.5. *Let* $x \in K$ *and* $\mathfrak{p}$ *be a prime of* K*. We have*

(1) $\operatorname{ord}_{\mathfrak{p}}(\frac{\partial x}{\partial \mathfrak{p}}) \geq \operatorname{ord}_{\mathfrak{p}}(x) - 1$*; and*
(2) *if* $\operatorname{ord}_{\mathfrak{p}}(x) \geq 0$*, then* $\operatorname{ord}_{\mathfrak{p}}(\frac{\partial x}{\partial \mathfrak{p}}) \geq 0$*.*

Proof. See Mason [12, p. 9]. □

Lemma 2.6. *The function* t *can be chosen so that*

(1) $[K : F(t)] \leq C_1$*,*
(2) $d(\mathfrak{p}) \geq 0$ *for all* $\mathfrak{p} \neq \mathfrak{p}_\infty$*,*
(3) $d(\mathfrak{p}_\infty) \geq -g - 2$*, and*
(4) $\deg \mathfrak{E} \leq C_2$*.*

Proof. Since the integral divisor $\mathfrak{p}_\infty^{g+1}$ of K has degree $g + 1$, we have

$$\ell\left(\mathfrak{p}_\infty^{g+1}\right) = 2 > 1$$

by Lemma 2.4. Therefore, $L(\mathfrak{p}_\infty^{g+1})$ contains a non-constant element w such that

$$\mathfrak{d}(w) = \mathfrak{p}_\infty^{\alpha},$$

where $\alpha \leq g + 1$. Let us show that w satisfies the conclusions of the lemma.

(1) Let $\mathfrak{P}_\infty$ be the prime of $F(w)$ below $\mathfrak{p}_\infty$. Observe that the ramification degree of $\mathfrak{p}_\infty$ over $\mathfrak{P}_\infty$ is α and each prime has degree 1 in its respective field. Since there is no constant field extension we also conclude that the relative degree of $\mathfrak{p}_\infty$ over $\mathfrak{P}_\infty$ is 1. Thus by Lemma 2.3 (1) we have $[K : F(w)] = \alpha \leq g + 1$ and we can choose w as our new t. If $p = \operatorname{char}(K) > 0$ and w happens to be a p-th power, we will replace w by its p-th root sufficiently many times until the result is no longer a p-th power in K. Observe that taking a p-th root will only reduce α, and therefore the conclusion of the lemma remains unchanged. Observe also that we can assume that $dw/dt \neq 0$. For the rest of the proof, let $d_w(\mathfrak{p})$ stands for $\operatorname{ord}_{\mathfrak{p}}\left(\frac{\partial w}{\partial \mathfrak{p}}\right)$.
(2) By Lemma 2.5 (2) we have that $d_w(\mathfrak{p}) \geq 0$ for all $\mathfrak{p} \neq \mathfrak{p}_\infty$,
(3) By Lemma 2.5 (1), we have $d_w(\mathfrak{p}_\infty) \geq -\alpha - 1 \geq -g - 2$.

(4) By Mason [12, Equation (5) p. 10], we have

$$\sum_{\mathfrak{p}} d_w(\mathfrak{p}) = \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}\left(\frac{\partial w}{\partial \mathfrak{p}}\right) = 2g-2$$

since w has non-zero global derivative. Therefore, by Items (2) and (3), we have

$$\sum_{d_w(\mathfrak{p})>0} d_w(\mathfrak{p}) \leq 2g-2 < 3g,$$

if $\mathrm{ord}_{\mathfrak{p}_\infty}\left(\frac{\partial w}{\partial \mathfrak{p}_\infty}\right) \geq 0$, and

$$\sum_{d_w(\mathfrak{p})>0} d_w(\mathfrak{p}) = 2g-2-\mathrm{ord}_{\mathfrak{p}_\infty}\left(\frac{\partial w}{\partial \mathfrak{p}_\infty}\right) \leq 2g-2+g+2 = 3g,$$

if $\mathrm{ord}_{\mathfrak{p}_\infty}\left(\frac{\partial w}{\partial \mathfrak{p}_\infty}\right) < 0$.

□

Lemma 2.7. *For all $x \in K$ and $\mathfrak{p}$ prime of K, we have*

(1) *if* $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$ *then*

$$\mathrm{ord}_{\mathfrak{p}}(x') \geq \max(0, \mathrm{ord}_{\mathfrak{p}}(x)-1) - d(\mathfrak{p})$$

and

(2) *if* $\mathrm{ord}_{\mathfrak{p}}(x) < 0$ *then*

$$\mathrm{ord}_{\mathfrak{p}}(x') \geq \mathrm{ord}_{\mathfrak{p}}(x) - 1 - d(\mathfrak{p}).$$

Proof. From Mason [12, p. 96] we have for any prime $\mathfrak{p}$ (including $\mathfrak{p}_\infty$)

$$\frac{\partial x}{\partial \mathfrak{p}} = \frac{dx}{dt}\frac{\partial t}{\partial \mathfrak{p}} \tag{2.1}$$

hence, if $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$ then

$$\mathrm{ord}_{\mathfrak{p}}(x') = \mathrm{ord}_{\mathfrak{p}}\left(\frac{dx}{dt}\right) = \mathrm{ord}_{\mathfrak{p}}\left(\frac{\partial x}{\partial \mathfrak{p}}\right) - \mathrm{ord}_{\mathfrak{p}}\left(\frac{\partial t}{\partial \mathfrak{p}}\right) \geq \max(0, \mathrm{ord}_{\mathfrak{p}}(x)-1) - d(\mathfrak{p})$$

and if $\mathrm{ord}_{\mathfrak{p}}(x) < 0$ then

$$\mathrm{ord}_{\mathfrak{p}}(x') = \mathrm{ord}_{\mathfrak{p}}\left(\frac{dx}{dt}\right) = \mathrm{ord}_{\mathfrak{p}}\left(\frac{\partial x}{\partial \mathfrak{p}}\right) - \mathrm{ord}_{\mathfrak{p}}\left(\frac{\partial t}{\partial \mathfrak{p}}\right) \geq \mathrm{ord}_{\mathfrak{p}}(x) - 1 - d(\mathfrak{p})$$

by Lemma 2.5. □

Corollary 2.8. (1) *Let x be a non constant element of K. If $\mathfrak{p}$ is a prime of K such that $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$ and $\mathrm{ord}_{\mathfrak{p}}(x') < 0$, then $d(\mathfrak{p}) > 0$ (so that $\mathfrak{p}|\mathfrak{E}$), and we have*

$$\mathrm{ord}_{\mathfrak{p}}(x') \geq -d(\mathfrak{p}).$$

(2) *If x is a non constant element of K then $\mathfrak{d}(x')$ divides $\mathfrak{d}(x^2)\mathfrak{E}$.*

Proof. (1) By Lemma 2.7 Item (1), for x without a pole at $\mathfrak{p}$ we have

$$0 > \mathrm{ord}_{\mathfrak{p}}(x') \geq \max(0, \mathrm{ord}_{\mathfrak{p}}(x)-1) - d(\mathfrak{p}) \geq -d(\mathfrak{p}).$$

(2) If $\mathfrak{p}$ is a pole of x' then

- either it does not divide $\mathfrak{E}$ (hence $d(\mathfrak{p}) \leq 0$), in which case it is a pole of x (by Item (1)), and we have $\mathrm{ord}_{\mathfrak{p}}(x') \geq \mathrm{ord}_{\mathfrak{p}}(x) - 1 - d(\mathfrak{p}) \geq \mathrm{ord}_{\mathfrak{p}}(x) - 1$ by Lemma 2.7 (2), hence
$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x')) \leq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x)) + 1;$$
- or it divides $\mathfrak{E}$ (hence $d(\mathfrak{p}) > 0$), in which case
  - either $\mathrm{ord}_{\mathfrak{p}}(x) < 0$, hence $\mathrm{ord}_{\mathfrak{p}}(x') \geq \mathrm{ord}_{\mathfrak{p}}(x) - 1 - d(\mathfrak{p})$ by Lemma 2.7 (2), and we conclude
  $$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x')) \leq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x)) + 1 + d(\mathfrak{p});$$
  - or $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$, hence $\mathrm{ord}_{\mathfrak{p}}(x') \geq -d(\mathfrak{p})$ (by Item (1)), hence
  $$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x')) \leq d(\mathfrak{p}).$$

We deduce that $\mathfrak{d}(x')$ divides
$$\prod_{\mathfrak{p}\nmid\mathfrak{E}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x))+1} \prod_{\substack{\mathfrak{p}|\mathfrak{E}\\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x))>0}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x))+1+d(\mathfrak{p})} \prod_{\substack{\mathfrak{p}|\mathfrak{E}\\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x))=0}} \mathfrak{p}^{d(\mathfrak{p})}$$
where in the first product we have $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x)) > 0$. Multiplying the rightmost product by
$$\prod_{\substack{\mathfrak{p}|\mathfrak{E}\\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x))>0}} \mathfrak{p}^{d(\mathfrak{p})}$$
and dividing the 'middle product' by the same quantity, we see that $\mathfrak{d}(x')$ divides
$$\prod_{\substack{\mathfrak{p}\nmid\mathfrak{E}\\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x))>0}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x))+1} \prod_{\substack{\mathfrak{p}|\mathfrak{E}\\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x))>0}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x))+1} \prod_{\mathfrak{p}|\mathfrak{E}} \mathfrak{p}^{d(\mathfrak{p})}$$
which in turn divides
$$\prod_{\mathfrak{p}} \mathfrak{p}^{2\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x))} \prod_{\mathfrak{p}|\mathfrak{E}} \mathfrak{p}^{d(\mathfrak{p})} = \mathfrak{d}(x^2)\mathfrak{E}$$
which was to be proved.

□

Corollary 2.9. *For any $x \in K$ which is not a constant, we have*
$$\deg \mathfrak{d}(x') \leq C_3 \deg \mathfrak{d}(x).$$

Proof. From Corollary 2.8 (2) we have that $\mathfrak{d}(x')$ divides $\mathfrak{d}(x^2)\mathfrak{E}$ and therefore
$$\deg(\mathfrak{d}(x')) \leq \deg(\mathfrak{d}(x^2)\mathfrak{E}) \leq 2\deg \mathfrak{d}(x) + C_2 \leq (C_2+2)\deg \mathfrak{d}(x) = C_3 \deg \mathfrak{d}(x)$$
by Lemma 2.6 (4) and definition of C_3. □

Lemma 2.10. *For any non-trivial effective divisor $\mathfrak{A}$ there exists $y \in K$ such that*
(1) *the divisor $\mathfrak{A}\mathfrak{E}$ divides $\mathfrak{n}(y)$;*
(2) *the function y has only one pole at $\mathfrak{p}_\infty$; and*
(3) *we have*
$$\deg \mathfrak{d}(y) \leq C_4 \deg(\mathfrak{A}).$$

Proof. Let

$$\mathfrak{B} = \frac{\mathfrak{A}\mathfrak{E}}{\mathfrak{p}_\infty^d}$$

where $d = \deg(\mathfrak{A}\mathfrak{E}) + g + 1$. Since $\mathfrak{B}^{-1}$ has degree $g+1$, we have

$$\ell(\mathfrak{B}^{-1}) \geq 2 > 1$$

by Lemma 2.4. Therefore, the vector space $L(\mathfrak{B}^{-1})$ contains a non-constant element y such that $\mathfrak{d}(y) = \mathfrak{p}_\infty^\alpha$ where $1 \leq \alpha \leq d$, and $\mathfrak{n}(y)$ is divisible by $\mathfrak{A}\mathfrak{E}$, so that Items (1) and (2) are satisfied. Finally observe that

$$\deg(\mathfrak{d}(y)) = \alpha \leq d = \deg(\mathfrak{A}\mathfrak{E}) + g + 1 = \deg(\mathfrak{A}) + \deg(\mathfrak{E}) + g + 1 \leq \deg(\mathfrak{A}) + C_2 + C_1,$$

where the last inequality holds by Lemma 2.6. We finally get

$$\deg(\mathfrak{d}(y)) \leq \deg(\mathfrak{A}) + C_2 + C_1 \leq (C_2 + C_1 + 1)\deg(\mathfrak{A}) = C_4 \deg(\mathfrak{A}),$$

where the last inequality comes from the fact that $\deg \mathfrak{A} \geq 1$. □

3. Intermediate Theorem

This section is devoted to the proof of Theorem 3.2 below. In order to state the theorem we introduce the following notation.

Notation 3.1. (1) *Let $r \geq 2$ and M be positive natural numbers.*

(2) *If $\bar{c} = (c_0, \ldots, c_{M-1})$ is a sequence of distinct elements of F, we will write*

$$c_{i,j,n} = \frac{c_i - \xi^n c_j}{1 - \xi^n}$$

for any indices i and j and for any $n \in \{1, \ldots, r-1\}$.

(3) *Given $\bar{c}$ as above, let $\ell(\bar{c})$ be equal to 3 if for all indices i, j, k, m, n we have either $c_{i,j,n} \neq c_{i,k,m}$, or for all indices i, j, k we have*

$$[F_0(c_i, c_j, c_k, \xi) \colon F_0(c_i, c_j, c_k)] = r - 1$$

(in particular, the latter happens if $\mathrm{char}(F) = 0$ and c_i are rational numbers). Otherwise set $\ell(\bar{c}) = r + 1$.

Theorem 3.2. *Let $a, \nu \in K$ and $(x_0, \ldots, x_{M-1})$ be a sequence of elements of K such that at least one x_i has non-zero derivative. Let $\bar{c} = (c_0, \ldots, c_{M-1})$ be a sequence of distinct elements of F. If*

$$M \geq r^2 \ell(\bar{c}) \left(1 + C_3 \left(5r + \frac{r+1}{r-1}\right)\right) + 1$$

and

$$x_n^r = (\nu + c_n)^r - a,\ n = 0, \ldots, M-1$$

then either $a = 0$ or there exist $\gamma \in K$ such that $\gamma' = 0$, and ξ_0 an r-th root of unity, such that

$$a = (\xi_0 \nu + \gamma)^r.$$

Throughout this section we will suppose that $a, \nu, x_0, \ldots, x_{M-1}$ and $\bar{c}$ satisfy the hypothesis of Theorem 3.2.

The following notation will also be used throughout the section.

Notation 3.3. (1) *Write* $u_n = x_n^r$ *and*

$$\mathfrak{D} = \prod_{i=0}^{M-1} \mathfrak{d}(x_i) \qquad \text{and} \qquad \mathfrak{N} = \prod_{i=0}^{M-1} \mathfrak{n}(x_i).$$

(2) *Let* $d = \deg \mathfrak{D}$.

(3) *Let* $\mathfrak{L}_\mathfrak{d} = \operatorname{lcm}(\mathfrak{d}(x_0), \ldots, \mathfrak{d}(x_{n-1}))$ *(where* lcm *stands for "the least common multiple"). Let* $\mathfrak{L}_\mathfrak{n} = \operatorname{lcm}(\mathfrak{n}(x_0), \ldots, \mathfrak{n}(x_{n-1}))$.

(4) *Let* $y \in K$ *be such that*

- *the divisor* $\mathfrak{L}_\mathfrak{d}\mathfrak{E}$ *divides* $\mathfrak{n}(y)$*;*
- *the function* y *has only one pole at* $\mathfrak{p}_\infty$*; and*
- $\deg \mathfrak{d}(y) \leq C_4 \deg \mathfrak{L}_\mathfrak{d}$

(such a y *exists by Lemma 2.10 and because* $\deg \mathfrak{L}_\mathfrak{d} \neq 0$ *since by hypothesis at least one* x_i *is non-constant).*

Remark 3.4. In the previous section there was no assumption whatsoever on $\mathfrak{p}_\infty$. We will now set it to be a valuation of K *not occurring as a pole or zero of any element of the (finite) set* $\{x_0, \ldots, x_{M-1}, \nu, a\}$.

Lemma 3.5. *The following equality holds:*

$$u_i - u_j = r(c_i - c_j) \prod_{n=1}^{r-1} [\nu + c_{i,j,n}] \tag{3.1}$$

where $c_{i,j,n}$ *have been defined in Notation 3.3* (3).

Proof. From Equation (1.2), we have

$$\begin{aligned} u_i - u_j &= (\nu + c_i)^r - (\nu + c_j)^r \\ &= (c_i - c_j) \prod_{n=1}^{r-1} [(\nu + c_i) - \xi^n(\nu + c_j)] \\ &= (c_i - c_j) \prod_{n=1}^{r-1} [(1 - \xi^n)\nu + (c_i - \xi^n c_j)] \\ &= (c_i - c_j) \prod_{n=1}^{r-1} (1 - \xi^n) \prod_{n=1}^{r-1} \left[\nu + \frac{c_i - \xi^n c_j}{1 - \xi^n}\right] \end{aligned}$$

hence

$$u_i - u_j = r(c_i - c_j) \prod_{n=1}^{r-1} [\nu + c_{i,j,n}].$$

□

Lemma 3.6. (1) *At most one* x_i *is an element of* F.

(2) *For any prime* $\mathfrak{p}$ *of* K*, either*

$$\operatorname{ord}_\mathfrak{p} \mathfrak{d}(u_n) = \operatorname{ord}_\mathfrak{p} \mathfrak{d}(u_m) \geq (r-1) \operatorname{ord}_\mathfrak{p} \mathfrak{d}(\nu) \tag{3.2}$$

for all m *and* n*, or there exists* $n_0 = n_0(\mathfrak{p})$ *such that*

$$(r-1) \operatorname{ord}_\mathfrak{p} \mathfrak{d}(\nu) = \operatorname{ord}_\mathfrak{p} \mathfrak{d}(u_n) > \operatorname{ord}_\mathfrak{p} \mathfrak{d}(u_{n_0}) \tag{3.3}$$

for all n *distinct from* n_0.

Proof. (1) Fix an index k and suppose that x_k is not constant (we know by hypothesis of Theorem 3.2 that there exists at least one such k). Suppose that there exists an index $i \neq k$ such that x_i is constant. From Equation (3.1), substituting k for j, it follows that ν is not a constant. Hence for any $j \neq i$, Equation (3.1) for i and j implies that x_j is not a constant.

(2) Fix a prime $\mathfrak{p}$ of K. If for all indices n and m we have $\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(u_n) = \mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(u_m)$, then by Equation (3.1) for n and m, we have also

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(u_m) \geq (r-1)\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(\nu).$$

Hence (3.2) holds. Otherwise there exist indices $n_0 \neq n_1$ such that for

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(u_{n_0}) < \mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(u_{n_1}).$$

From Equation (3.1) with indices n_0 and n_1, we have

$$(r-1)\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(\nu) = \mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(u_{n_1}).$$

From the same equation for any index $j \neq n_0$ and n_0 we conclude that

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(u_j) = (r-1)\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(\nu).$$

Hence (3.3) holds.

□

Proposition 3.7. *The following inequalities hold (see Notation 2.1):*

(1) *for any index n and prime $\mathfrak{p}$ of K*

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n) \leq \frac{\mathrm{ord}_{\mathfrak{p}}\mathfrak{D}}{M-1};$$

(2) $\deg \mathfrak{L}_{\mathfrak{d}} \leq \dfrac{d}{M-1}$;

(3) $\deg \mathfrak{d}(x_n) \leq \dfrac{d}{M-1}$ *for any index n.*

Proof. (1) By Lemma 3.6, we have

$$\mathrm{ord}_{\mathfrak{p}}[\mathfrak{d}(x_0)\dots\mathfrak{d}(x_n)\dots\mathfrak{d}(x_{M-1})] \geq (M-1)\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n)$$

for any prime $\mathfrak{p}$ in K and any index n (note that we consider the product of M factors on the left-hand side).

(2) For any prime $\mathfrak{p}$ such that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{L}_{\mathfrak{d}}) > 0$, by definition of $\mathfrak{L}_{\mathfrak{d}}$ there exists an index n such that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{L}_{\mathfrak{d}}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x_n))$ and therefore by Item (1) we have

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{L}_{\mathfrak{d}}) \leq \frac{\mathrm{ord}_{\mathfrak{p}}\mathfrak{D}}{M-1}.$$

(3) This part follows directly from either (1) or (2).

□

Lemma 3.8. *The following inequalities hold:*

(1) *For any prime $\mathfrak{p}$ of K and for all but at most one index n we have*

$$(r-1)\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(\nu) \leq r\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n).$$

(2) *We have*

$$(r-1)(M-1)\deg \mathfrak{d}(\nu) \leq rd.$$

(3) *For any prime* $\mathfrak{p}$ *of* K *and for all but at most one index* n *we have*

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(a) \leq r\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n).$$

(4) *We have*

$$(M-1)\deg \mathfrak{d}(a) \leq rd.$$

Proof. (1) This comes from Lemma 3.6 and by definition of $u_n = x_n^r$.

(2) By Proposition 3.7 we have

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n) \leq \frac{\mathrm{ord}_{\mathfrak{p}}\mathfrak{D}}{M-1}$$

for all n. From Item (1) we deduce

$$(r-1)\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(\nu) \leq \frac{r}{M-1}\mathrm{ord}_{\mathfrak{p}}\mathfrak{D}$$

and the claim follows.

(3) From Equation (1.2) we have for any index n and any prime $\mathfrak{p}$ in K

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(a) \leq \max\{r\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n), r\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(\nu)\}.$$

Hence by Item (1), for all but at most one index n, we have

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(a) &\leq \max\{r\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n), \frac{r}{r-1}\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n)\}\\ &\leq r\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n)\end{aligned}$$

which was to be proved.

(4) From Item (3) and Proposition 3.7 we have

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(a) \leq r\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n) \leq \frac{r\mathrm{ord}_{\mathfrak{p}}\mathfrak{D}}{M-1},$$

hence

$$\deg(\mathfrak{d}(a)) \leq \frac{rd}{M-1}$$

by definition of d.

□

Corollary 3.9. *The divisors* $\mathfrak{d}(x_n)$, $\mathfrak{d}(a)$, $\mathfrak{d}(\nu)$, $\mathfrak{d}(x_n')$, $\mathfrak{d}(a')$ *and* $\mathfrak{d}(\nu')$ *divide* $\mathfrak{n}(y^{2r+1})$. *Moreover we have*

$$\deg \mathfrak{d}(y) \leq C_4\frac{d}{M-1}.$$

Proof. Recall that $y \in K$ is such that the divisor $\mathfrak{L}_{\mathfrak{d}}\mathfrak{E}$ divides $\mathfrak{n}(y)$ (see Notation 3.3), hence for all primes $\mathfrak{p} \in K$ and for all index n, we have

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(x_n)) \leq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{L}_{\mathfrak{d}}) \leq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}(y)). \tag{3.4}$$

(reacall that $\mathfrak{L}_{\mathfrak{d}}$ is the least common multiple of the $\mathfrak{d}(x_n)$).

Also, since $\deg \mathfrak{d}(y) \leq C_4 \deg \mathfrak{L}_{\mathfrak{d}}$ (see Notation 3.3), by Proposition 3.7 (2) we get

$$\deg \mathfrak{d}(y) \leq C_4\frac{d}{M-1}.$$

(1) Equation (3.4) implies that $\mathfrak{d}(x_n)$ divides $\mathfrak{n}(y)$.

(2) From Lemma 3.8 (3), for all prime p of K we have $\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(a) \leq r\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n)$, hence $\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(a) \leq r\mathrm{ord}_{\mathfrak{p}}\mathfrak{n}(y)$ by Equation (3.4). So $\mathfrak{d}(a)$ divides $\mathfrak{n}(y^r)$.

(3) From Lemma 3.8 (1), we have

$$(r-1)\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(\nu) \leq r\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n),$$

hence

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(\nu) \leq \frac{r}{r-1}\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(x_n) \leq \frac{r}{r-1}\mathrm{ord}_{\mathfrak{p}}y \leq (2r+1)\mathrm{ord}_{\mathfrak{p}}y$$

by Equation (3.4). Therefore, $\mathfrak{d}(\nu)$ divides $\mathfrak{n}(y^{2r+1})$.

(4) By Corollary 2.8 (2), the pole divisor of x_n' divides $\mathfrak{d}(x_n^2)\mathfrak{E}$, which in turn divides $\mathfrak{n}(y^{2+1})$. Observe that 3 is less than $2r+1$.

(5) By Corollary 2.8 (2) again, the pole divisor of a' divides $\mathfrak{d}(a^2)\mathfrak{E}$, which in turn divides $\mathfrak{n}(y^{2r})\mathfrak{n}(y)$ by (2) and because $\mathfrak{E}$ divides $\mathfrak{n}(y)$. Hence $\mathfrak{d}(a')$ divides $\mathfrak{n}(y^{2r+1})$.

(6) Similarly, by Corollary 2.8 (2), the pole divisor of ν' divides $\mathfrak{d}(\nu^2)\mathfrak{E}$, hence by Item (3)

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(\nu') \leq \mathrm{ord}_{\mathfrak{p}}\mathfrak{d}(\nu^2\mathfrak{E}) \leq \left(2\frac{r}{r-1}+1\right)\mathrm{ord}_{\mathfrak{p}}y \leq (2r+1)\mathrm{ord}_{\mathfrak{p}}y$$

and we conclude that $\mathfrak{d}(\nu')$ divides $\mathfrak{n}(y^{2r+1})$.

□

Lemma 3.10. (1) *For any set of distinct indices $n_1, \ldots, n_{r+1}$, the functions x_{n_i} do not have a common zero.*

(2) *If the characteristic p of K does not divide r and for all indices i, j, k, m, n we have that $c_{i,j,n} \neq c_{i,k,m}$, then for any three distinct indices i, j and k, the functions x_i, x_j and x_k do not have a common zero.*

(3) *Suppose $r \neq 2$. If for all indices i, j, k we have that*

$$[F_0(c_i, c_j, c_k, \xi) \colon F_0(c_i, c_j, c_k)] = r-1$$

then for all distinct indices i, j, k we have that x_i, x_j and x_k do not have a common zero. In particular, this is true if c_i are rational numbers.

Proof. (1) Since we have assumed that the field of constants is algebraically closed, the proof in Pasten [15, Lemma 3.3] goes through for the general case essentially unchanged.

(2) From (3.1), we have for any indices i and j

$$x_i^r - x_j^r = u_i - u_j = r(c_i - c_j)\prod_{n=1}^{r-1}\left[\nu + c_{i,j,n}\right].$$

Suppose now that $\mathfrak{p}$ is a prime of K which is a common zero of x_i, x_j and x_k for some distinct indices i, j and k. Consequently, for some n and m, $\mathfrak{p}$ is a zero of $\nu + c_{i,j,n}$ and $\nu + c_{i,k,m}$, hence of $c_{i,j,n} - c_{i,k,m} \in F$, implying

$$c_{i,j,n} = c_{i,k,m}. \tag{3.5}$$

(3) Suppose that Equation (3.5) holds for some i, j, k, m and n. Without loss of generality, assume $n \geq m$. By definition of $c_{i,j,n}$, from Equation (3.5) we get

$$\begin{aligned} 0 &= (1-\xi^m)(c_i - \xi^n c_j) - (1-\xi^n)(c_i - \xi^m c_k) \\ &= \xi^m(c_k - c_i) + \xi^n(c_i - c_j) + \xi^{n+m}(c_j - c_k) \\ &= \xi^m[(c_k - c_i) + \xi^{n-m}(c_i - c_j) + \xi^n(c_j - c_k)]. \end{aligned}$$

If $n = m$, since $c_j \neq c_k$ (by hypothesis of Theorem 3.2), then $\xi^n = 1$, which is impossible since

$$1 \leq n \leq r - 1.$$

Otherwise, 1, ξ^{n-m} and ξ^n are linearly dependent over $F_0(c_i, c_j, c_k)$. This contradicts our assumption on the degree of the extension if $r > 3$. If $r = 3$, since $n > m$, we must have that $n = 2$ and $m = 1$, yielding

$$\begin{aligned} 0 &= (c_k - c_i) + \xi(c_i - c_j) + \xi^2(c_j - c_k) \\ &= (c_k - c_i) + \xi(c_i - c_j) - (1 + \xi)(c_j - c_k) \\ &= (2c_k - c_i - c_j) + \xi(c_i - 2c_j + c_k). \end{aligned}$$

The last equation under our assumptions is equivalent to the system

$$\begin{cases} 2c_k - c_i - c_j = 0 \\ c_i - 2c_j + c_k = 0 \end{cases}$$

Replacing c_i in the first equation by $2c_j - c_k$ we obtain $2c_k - 2c_j + c_k - c_j = 0$, i.e. $c_k = c_j$ contradicting our assumptions on $\bar{c}$ in the hypothesis of Theorem 3.2. Therefore the assumption of Item (2) holds.

□

Notation 3.11. *Let $\ell \geq 2$ be a natural number such that any ℓ of the x_i are coprime (such an ℓ exists by Lemma 3.10).*

Recall that $\mathfrak{L}_{\mathfrak{n}}$ stands for the least common multiple of the $\mathfrak{n}(x_n)$ (see Notation 3.3).

Corollary 3.12. *The following inequality holds:*

$$\deg \mathfrak{L}_{\mathfrak{n}} \geq \frac{d}{\ell} .$$

Proof. Let $\mathfrak{p}$ be a prime such that $\operatorname{ord}_{\mathfrak{p}}\mathfrak{N} > 0$ (where $\mathfrak{N}$ is the product of the numerator divisors of the x_n). Further, let $x_{i_1}, \ldots, x_{i_s}$, with $s < \ell$, be all the functions in the sequence (x_i) with a zero at $\mathfrak{p}$. Without loss of generality, assume

$$\operatorname{ord}_{\mathfrak{p}} x_{i_1} \geq \cdots \geq \operatorname{ord}_{\mathfrak{p}} x_{i_s}.$$

We have $\operatorname{ord}_{\mathfrak{p}}\mathfrak{L}_{\mathfrak{n}} = \operatorname{ord}_{\mathfrak{p}} x_{i_1}$. Also, we have

$$\operatorname{ord}_{\mathfrak{p}}\mathfrak{N} \leq s \cdot \operatorname{ord}_{\mathfrak{p}} x_{i_1} < \ell \cdot \operatorname{ord}_{\mathfrak{p}} x_{i_1} = \ell \cdot \operatorname{ord}_{\mathfrak{p}}\mathfrak{L}_{\mathfrak{n}},$$

hence

$$d = \deg(\mathfrak{D}) = \deg(\mathfrak{N}) \leq \ell \deg(\mathfrak{L}_{\mathfrak{n}}).$$

□

Lemma 3.13. *We have*

$$(rx_n' x_n^{r-1} + a')^r = r^r \nu'^r (x_n^r + a)^{r-1}. \tag{3.6}$$

Proof. This can easily be derived from Pasten [15, Equation (3.2)] through the obvious change of variables. □

Notation 3.14. *Set $\Delta = a'^r - r^r \nu'^r a^{r-1}$ (this is just the "part" of Equation (3.6) that does not depend on n).*

Lemma 3.15. *If $\Delta \neq 0$ then the following inequality holds:*

$$\deg \mathfrak{d}(\Delta) \leq \frac{C_3 r^2 d}{M-1}\left(1+\frac{1}{r-1}\right).$$

Proof. From Proposition 3.7, Lemma 3.8, and Corollary 2.9 it follows that

$$\begin{aligned}\deg \mathfrak{d}(\Delta) &\leq \max(rC_3 \deg \mathfrak{d}(a), rC_3 \deg \mathfrak{d}(\nu) + (r-1)\deg \mathfrak{d}(a)) \\ &\leq rC_3(\deg \mathfrak{d}(a) + \deg \mathfrak{d}(\nu)) \\ &\leq rC_3\left(\frac{rd}{M-1} + \frac{rd}{(r-1)(M-1)}\right) \\ &= \frac{C_3 r^2 d}{M-1}\left(1+\frac{1}{r-1}\right).\end{aligned}$$

□

Notation 3.16. (1) *Let us write $z = y^{2r+1}$ and $z_n = x_n z$.*

(2) *Write*

$$C_5 = (2r+1)C_4 + \left(1+\frac{1}{r-1}\right)C_3 = (2r+1)(4g+2) + \left(1+\frac{1}{r-1}\right)(3g+2) = \left(8r+4+\frac{3r}{r-1}\right)g + \left(4r+2+\frac{2r}{r-1}\right)$$

and

$$B = C_5 r^2 \ell + 1 = \beta_0(r,\ell)g + \beta_1(r,\ell),$$

where

$$\beta_0(r,\ell) = \left(8r+4+\frac{3r}{r-1}\right)r^2\ell,$$

$$\beta_1(r,\ell) = \left(4r+2+\frac{2r}{r-1}\right)r^2\ell + 1.$$

Observe that $\mathfrak{n}(z_n)$ is divisible by $\mathfrak{n}(x_n)$ because z has a pole at $\mathfrak{p}_\infty$ only, and by assumption $\mathfrak{p}_\infty$ is not a zero of any x_n.

Lemma 3.17. *If $M > B(r,\ell)$ then $\Delta = 0$, namely,*

$$a'^r = r^r \nu'^r a^{r-1}. \tag{3.7}$$

Proof. Multiplying both sides of Equation (3.6)

$$(rx'_n x_n^{r-1} + a')^r = r^r \nu'^r (x_n^r + a)^{r-1}$$

by z^{r^2} and replacing x_n by $z_n = x_n z$ we get

$$(rx'_n z_n^{r-1} z + a' z^r)^r = r^r (\nu' z)^r (z_n^r + a z^r)^{r-1}. \tag{3.8}$$

Let $\mathfrak{p}$ be a prime of K dividing $\mathfrak{n}(x_n)$. Let us remind the reader that by Corollary 3.9 and definition of $z = y^{2r+1}$, the divisors $\mathfrak{d}(x_n)$, $\mathfrak{d}(a)$, $\mathfrak{d}(\nu)$, $\mathfrak{d}(x'_n)$, $\mathfrak{d}(a')$ and $\mathfrak{d}(\nu')$ divide $\mathfrak{n}(z)$. Therefore, none of the terms $x'_n z$, $a'z^r$, $\nu' z$ and az^r appearing in Equation (3.8) have a pole at $\mathfrak{p}$.

We claim that $z^{r^2}\Delta$, that is, the part of Equation (3.8) that does not depend on n, is divisible by $\mathfrak{n}(x_n)$. To see that, recall that $\mathfrak{n}(z_n)$ is divisible by $\mathfrak{n}(x_n)$, and hence $\mathfrak{n}(rx'_n z_n^{r-1} z)$ is divisible by $\mathfrak{n}(x_n)$ (see the left hand side of Equation (3.8)). Also, there

is no problem with the right hand side since the only part depending on n is z_n^r. Thus modulo $\mathfrak{n}(x_n)$, Equation (3.8) becomes

$$(a'z^r)^r \equiv r^r(\nu' z)^r(az^r)^{r-1} \qquad \mod \mathfrak{n}(x_n).$$

Hence we have

$$z^{r^2}\Delta = z^{r^2}(a'^r - r^r\nu'^r(az)^{r-1}) \equiv 0 \qquad \mod \mathfrak{n}(x_n)$$

Thus, if $\Delta \neq 0$ then from Corollary 3.12 we have

$$\begin{aligned}
\frac{d}{\ell} &\leq \deg \mathfrak{L}_{\mathfrak{n}} \\
&\leq \deg \mathfrak{d}(z^{r^2}\Delta) \\
&\leq r^2 \deg \mathfrak{d}(y^{2r+1}) + \deg \mathfrak{d}(\Delta) \\
&\leq r^2(2r+1)C_4\frac{d}{M-1} + \frac{C_3 r^2 d}{M-1}\left(1+\frac{1}{r-1}\right) \\
&= \frac{r^2 d}{M-1}\left((2r+1)C_4 + \left(1+\frac{1}{r-1}\right)C_3\right) \\
&= C_5\frac{r^2 d}{M-1}.
\end{aligned}$$

See Notation 3.3 (4), Proposition 3.7 (2) and Lemma 3.15). Solving for M we obtain

$$M \leq C_5 r^2 \ell + 1 = B(r,\ell).$$

So, for $M > B(r,\ell)$, the quantity Δ must be zero. □

Remark 3.18. *Note that from* $\Delta = a'^r - r^r\nu'^r a^{r-1} = 0$ *we deduce that*

$$\nu' \neq 0.$$

Otherwise, both ν *and* a *would have zero derivative, which would imply by Equation* (1.2) *that all* x_n *have zero derivative and contradict the hypothesis of Theorem 3.2.*

Proof of Theorem 3.2. Suppose a is not zero. From Equation (3.7), the quantity

$$a^{r-1} = \frac{a^r}{a}$$

is an r-th power. Hence a is an r-th power, say $a = b^r$.

On the one hand, from Equation (3.7), we have

$$a'^r = r^r\nu'^r b^{r(r-1)}.$$

Hence, taking an r-th root, we obtain

$$a' = r\xi_0\nu' b^{r-1},$$

where ξ_0 is an r-th root of unity.

On the other hand, from $a = b^r$, we have $a' = rb'b^{r-1}$, hence $\xi_0\nu' = b'$. Thus we get $b = \xi_0\nu + \gamma$ for some $\gamma \in K$ whose derivative is zero.

Finally from the Equation (1.2), we obtain

$$x_n^r = (\nu + c_n)^r - a = (\nu + c_n)^r - b^r = (\nu + c_n)^r - (\xi_0\nu + \gamma)^r.$$

□

4. Proof of Theorem 1.3

From Theorem 3.2, we have

$$x_n^r = (\nu + c_n)^r - a = (\nu + c_n)^r - (\xi_0\nu + \gamma)^r$$

which is polynomial in ν (and ν is non-constant by Remark 3.18), with coefficients in $F(\xi_0)$ (since γ has zero derivative, it belongs to F). Therefore,

$$a = (\nu + c_n)^r - x_n^r$$

also is a polynomial in ν with coefficients in $F(\xi_0)$ and the problem is reduced to to Hensley's Problem for polynomials in characteristic zero over $F(\xi_0)$. But we know that this problem has only trivial solutions for our M (see Pasten [15]), implying that $a = 0$. Contradiction.

5. Proof of Theorem 1.4

What remains to do in order to prove Theorem 1.4 is taken from [20], with essentially no changes. We include it here for the convenience of the reader.

In this section we let $r = 2$ and $c_n = n$ for all n. Note that in this case $\ell(\bar{c}) = 3$. For convenience of the reader, we rewrite Theorem 3.2 under these assumptions:

Theorem 5.1. *Let $a, \nu \in K$, where K is a function field of characteristic $p \geq B(2,3)$. Let M be a positive integer, and let $(x_0, \ldots, x_{M-1})$ be a sequence of elements of K such that at least one x_i is not a p-th power. If $M \geq B(2,3)$ and*

$$x_n^2 = (\nu + n)^2 - a,\ n = 0, \ldots, M-1, \tag{5.9}$$

then either $a = 0$ or $a = (\nu - \gamma)^2$ for some $\gamma \in K^p$.

The rest of the section contains a proof of Theorem 1.4. First we will dispose of the case where not all the x_n are p-th powers. In this case Theorem 5.1 applies, namely there exists a p-th power $\gamma \in K$ such that

$$x_n^2 = (\nu + n)^2 - (\nu - \gamma)^2.$$

Write $\gamma = f^{p^s}$ so that $f \in K \setminus K^p$. For all n we have

$$\begin{aligned} x_n^2 &= (\nu + n)^2 - (\nu - f^{p^s})^2 \\ &= (2\nu - f^{p^s} + n)(f^{p^s} + n) \\ &= (2\nu - f^{p^s} + n)(f + n)^{p^s} \\ &= (2\nu - f^{p^s} + n)(f + n)(f + n)^{p^s - 1} \\ &= \left[\left(\nu + \frac{f - f^{p^s}}{2} + n\right)^2 - \left(\nu + \frac{f - f^{p^s}}{2} - f\right)^2\right](f + n)^{p^s - 1} \end{aligned} \tag{5.10}$$

(note that for the third equality to hold, we need c_n to be n). Considering the sequence defined by

$$y_n = \frac{x_n}{(f + n)^{\frac{p^s - 1}{2}}}$$

we obtain

$$y_n^2 = (\bar{\nu} + n)^2 - (\bar{\nu} - f)^2 \tag{5.11}$$

where

$$\bar{\nu} = \nu + \frac{f - f^{p^s}}{2}. \tag{5.12}$$

We want to apply Theorem 5.1 to the sequence y_n. In order to do so, we show that y_n cannot be a p-th power for more than one index n. Suppose that y_n and y_m are p-th powers for some distinct indices n and m. Since

$$y_n^2 - y_m^2 = (\bar{\nu} + n)^2 - (\bar{\nu} - m)^2 = 2(n+m)\bar{\nu} + n^2 - m^2,$$

$\bar{\nu}$ is a p-th power. From Equation (5.11) we deduce that $(\bar{\nu} - f)^2$ is a p-th power, hence $\bar{\nu} - f$ is a p-th power, hence f is a p-th power, and we have a contradiction of our assumption on f.

Since not all y_n are p-th powers we may apply Theorem 5.1 to the sequence (y_n). We assume that $\bar{\nu} - f \neq 0$ and obtain a contradiction. Since $\bar{\nu} - f \neq 0$, there exists a p-th power $\tilde{\gamma}$ such that $(\bar{\nu} - f)^2 = (\bar{\nu} - \tilde{\gamma})^2$. Since f is not a p-th power, we have $f \neq \tilde{\gamma}$, hence

$$\bar{\nu} - f = -\bar{\nu} + \tilde{\gamma}$$

therefore,

$$2\bar{\nu} = f + \tilde{\gamma}.$$

From Equation (5.12) we deduce

$$f + \tilde{\gamma} = 2\nu + f - f^{p^s}$$

hence

$$\tilde{\gamma} = 2\nu - f^{p^s}.$$

It follows that ν is a p-th power. Therefore, by Equations (5.10) we have

$$\begin{aligned} x_n^2 &= (2\nu - f^{p^s} + n)(f^{p^s} + n) \\ &= (\tilde{\gamma} + n)(f^{p^s} + n) \end{aligned}$$

is a p-th power, hence also each x_n is a p-th power. Thus we have a contradiction, implying $\bar{\nu} - f = 0$.

From Equation (5.12) we get

$$f = \nu + \frac{f - f^{p^s}}{2}$$

hence

$$\nu = \frac{f + f^{p^s}}{2}$$

and

$$\begin{aligned} x_n^2 &= (2\nu - f^{p^s} + n)(f^{p^s} + n) \\ &= (f + n)(f^{p^s} + n) \\ &= (f + n)^{p^s + 1}. \end{aligned}$$

Now we will address the case where all the x_n are p-th powers. Under this assumption we consider the sequence (w_n) such that for each n we have $x_n = w_n^{p^h}$ and not all w_n are p-th powers. So we may apply the above argument to the sequence (w_n) (and the new corresponding values of ν and γ - see [20] for the details) and deduce that either (w_n)

is such that $w_n^2 = (w+n)^2$ for some $w \in K$, or there exists $f \in K$ and a non-negative integer s such that $w_n^2 = (f+n)^{p^s+1}$. Therefore, either $x_n^2 = (w^{p^h}+n)^2$, or

$$x_n = \left[(f+n)^{\frac{p^s+1}{2}}\right]^{p^h} = (f^{p^h}+n)^{\frac{p^s+1}{2}}.$$

It remains to verify that if the sequence (x_n) satisfies Equations (1.4) then it indeed satisfies Equations (1.3). Suppose that for each n we have

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

for some $f \in K$ and s a non-negative integer. Then we have

$$\begin{aligned} x_n^2 &= (f+n)^{p^s+1} \\ &= (f+n)^{p^s}(f+n) \\ &= (f^{p^s}+n)(f+n) \\ &= \left(\frac{f^{p^s}+f}{2}+n\right)^2 - \left(\frac{f^{p^s}-f}{2}\right)^2. \end{aligned}$$

which has the form $(x+n)^2 + a$ for some polynomials x and a not depending on n.

6. Proof of Corollary 1.5

The proof is similar to the proof of Theorem 1.8 in [19] (this part of the proof was not affected by the mistake fixed in [20]). We reproduce it here for the convenience of the reader.

Observe that in order to define multiplication, it is enough to define squaring. The following Lemmas 6.2 and 6.4 prove Corollary 1.5.

Let $M \geq B(2,3)$ be an integer. Let $\phi(z,w)$ denote the formula

$$\exists w_0, \ldots, w_{M-1}$$

$$\left[\bigwedge_{i=2,\ldots,M-1} w_i - 2w_{i-1} + w_{i-2} = 2 \bigwedge_{i=0,\ldots,M-1} P_2(w_i) \wedge w = w_0 \wedge 2z = w_1 - w_0 - 1\right]$$

in the language $\mathscr{L}_2$ (and thus also in the language $\mathscr{L}_\tau^2$). (We remind the reader that $P_2(w)$ denotes the predicate "w is a square".)

It is clear that if $z, w \in K$ satisfy $z^2 = w$, then $\phi(z,w)$ is true over K, since we can set $w_i = (z+i)^2$ for each $i = 0, \ldots, M-1$. Observe that

$$w_1 - w_0 - 1 = (z+1)^2 - z^2 - 1 = 2z,$$

and under our assumptions $(w_0, \ldots, w_{M-1})$ is a trivial Büchi sequence.

Lemma 6.1. *If $\phi(z,w)$ is satisfied over K for some z and w such that $z^2 \neq w$ and K has characteristic 0, then z and w are in F. If $\phi(z,w)$ is satisfied over K for some z and w such that $z^2 \neq w$ and K has characteristic $p \geq B(2,3)$, then either z and w are constant, or there exist $f \in K$ and a non-negative integer s such that $w = f^{p^s+1}$ and $2z = f^{p^s} + f$.*

Proof. Suppose that $\phi(z,w)$ is true in K. Write $x_i^2 = w_i$, so that we have $x_i^2 - 2x_{i-1}^2 + x_{i-2}^2 = 2$ for each $i = 2, \ldots, M-1$. Writing $2\nu = \frac{x_n^2 - x_0^2}{n} - n$ and $a = \nu^2 - x_0^2$ we have $x_n^2 = (\nu + n)^2 - a$ for each n (see Remark 1.1).

If K has characteristic 0, then by Theorem 1.3 either $a = 0$, and $\nu = \pm x_0$, so that

$$2z = w_1 - w_0 - 1 = x_1^2 - x_0^2 - 1 = 2\nu = \pm 2x_0$$

and $z^2 = x_0^2 = w_0 = w$ contradicting our assumption, or for all indices n we have that $w_n = x_n^2 = (\nu + n)^2 - a$ is in F, in which case $w = w_0 \in F$ and $2z = w_1 - w_0 - 1 \in F$. Hence the first assertion of the Lemma is proved.

If K has characteristic $p \geq B(2,3)$, then, as above, by Theorem 1.4, either $a = 0$ and $z^2 = w$ again contradicting our assumption, or for each index n it is the case that $(\nu + n)^2 - a$ is in F and thus $w, z \in F$, or there exist $f \in K$ and a non-negative integer s such that for each n, we have $w_n = x_n^2 = (f + n)^{p^s+1}$, $w = w_0 = f^{p^s+1}$ and

$$2z = w_1 - w_0 - 1 = (f+1)^{p^s+1} - f^{p^s+1} - 1 = (f^{p^s} + 1)(f+1) - f^{p^s+1} - 1 = f^{p^s} + f.$$

□

Lemma 6.2. *If K has characteristic 0, then it satisfies the formula of the language $\mathscr{L}_\tau^2$*

$$\psi(z,w) \colon \phi(z,w) \wedge \phi(tz, t^2 w)$$

if and only if $z^2 = w$ (where tz stands for $\tau(z)$ and $t^2 w$ stands for $\tau\tau w$).

Proof. First we note that if $z, w \in K$ satisfy $z^2 = w$, then the formula $\psi(z,w)$ is true in K as was shown above. Suppose now that the formula $\psi(z,w)$ is satisfied in K and that $z^2 \neq w$ (hence $z, w \in F$). Since $\phi(tz, t^2 w)$ is true in K, by Lemma 6.1 we have that either $(tz)^2 = t^2 w$ (which would contradict the hypothesis $z \neq w^2$), or both tz and $t^2 w$ are in F. Since t stands for a transcendental element, this implies $z = w = 0$, and in particular $z^2 = w$. Contradiction. □

Lemma 6.3. *Suppose that K has characteristic $p \geq B(2,3)$. If it satisfies the formula of the language $\mathscr{L}_\tau^2$*

$$\theta(z,w) \colon \phi(z,w) \wedge \phi(z+t, w + 2tz + z^2) \wedge \phi(z-t, w - 2tz + z^2)$$

and $z^2 \neq w$ then either both z and w are p-th powers, or both $z + t$ and $w + 2tz + z^2$ are p-th powers, or both $z - t$ and $w - 2tz - z^2$ are p-th powers.

Proof. See [19, Section 3, Claim p. 563]. Note that the proof is exactly the same since the expressions we have for w and z in Lemma 6.1 (2) are just special cases of the one used in [19]. □

Lemma 6.4. *If K has characteristic $p \geq B(2,3)$ then it satisfies the formula of the language $\mathscr{L}_2^t$*

$$\eta(z,w) \colon \theta(z,w) \wedge \theta(z + t^2, w + 2t^2 z + t^4)$$

if and only if $z^2 = w$.

Proof. It is a direct consequence of Lemma 6.3 (or see [19, Section 3, p. 563]). □

References

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

[2] A. Bremner, *On square values of quadratics*, Acta Arith. **108**, no. 2, 95-111 (2003).

[3] J. L. Britton, *Integers solutions of systems of quadratic equations*, Math. Proc. of the Cambridge Phil. Soc. **86**, 385-389 (1979).

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

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

[6] J. Denef, L. Lipshitz, T. Pheidas, J. v. Geel Eds. *Hilbert's tenth problem : relations with arithmetic and algebraic geometry, Ghent 1999*, Contemporary Mathematics **270** (2000).

[7] Fried, Michael D. and Jarden, Moshe, *Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], **11**, Second edition, Springer-Verlag, Berlin, (2005).

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

[9] —— *Sequences of squares with second difference of two and a conjecture of Büchi*, unpublished (1980-1983).

[10] H. Koch *Number Theory, Algebraic Numbers and Functions*, American Mathematical Society, Graduate Studies in Mathematics **176** (2000).

[11] 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).

[12] Mason, R. C., *Diophantine Equations over Function Fields*, London Mathematical Society Lecture Notes **96**, Cambridge University Press, Cambridge, UK (1996).

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

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

[15] H. Pasten, *An extension of Büchi's Problem for polynomial rings in zero characteristic*, Proceedings of the American Mathematical Society **138**, 1549-1557 (2010).

[16] —— *Representation of squares by monic second degree polynomials in the field of p-adic meromorphic functions*, arXiv:1003.1969.

[17] H. Pasten, T. Pheidas and X. Vidaux, *A survey on Büchi's problem : new presentations and open problems*, to appear in the Proceedings of the Hausdorff Institute of Mathematics (2010).

[18] T. Pheidas and X. Vidaux, *Extensions of Büchi's problem : Questions of decidability for addition and n-th powers*, Fundamenta Mathmaticae **185**, 171-194 (2005).

[19] —— *The analogue of Büchi's problem for rational functions*, Journal of The London Mathematical Society **74-3**, 545-565 (2006).

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

[21] —— *The analogue of Büchi's problem for cubes in rings of polynomials*, Pacific Journal of Mathematics **238** (2), 349-366 (2008).

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

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

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

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

[26] H. Yamagishi, *On the solutions of certain diagonal quadratic equations and Lang's conjecture*, Acta Arithmetica **109-2** (2003).