The analogue of Büchi's problem for rational functions

Thanases Pheidas
University of Crete
and
Xavier Vidaux
Universidad de Concepción

revised version in Journal of LMS, vol. 74-3, pp. 545-565 (2006)

Abstract Büchi's problem asked whether a surface of a specific type, defined over the rationals, has integer points other than some known ones. A consequence of a positive answer would be the following strengthening of the negative answer to Hilbert's Tenth Problem: the positive existential theory of the rational integers in the language of addition and a predicate for the property 'x is a square' would be undecidable. Despite some progress, including a conditional positive answer (pending on conjectures of Lang), Büchi's problem remains open.

In this article we prove

(A) An analogue of Büchi's problem in rings of polynomials of characteristic either 0 or $p \geq 17$ and for fields of rational functions of characteristic 0 and

(B) An analogue of Büchi 's problem in fields of rational functions of characteristic $p \geq 19$, but only for sequences that satisfy a certain additional hypothesis.

As a consequence we prove the following result in Logic :

Let F be a field of characteristic either 0 or ≥ 17 and let t be a variable. Let L_t be the first order language which contains symbols for 0 and 1, a symbol for addition, a symbol for the property 'x is a square' and symbols for multiplication by each element of the image of $\mathbb{Z}[t]$ in $F[t]$. Let R be a subring of $F(t)$, containing the natural image of $\mathbb{Z}[t]$ in $F(t)$. Assume that one of the following is true :

- $R \subset F[t]$.
- The characteristic of F is either 0 or $p \geq 19$.

Then multiplication is positive-existentially definable over the ring R, in the language L_t. Hence the positive-existential theory of R in L_t is decidable if and only if the

positive-existential ring-theory of R in the language of rings, augmented by a constant-symbol for t, is decidable.

AMS Subject Classification: 03C60; 12L05

1 Introduction

In unpublished work J. Richard Büchi asked the following problem:

Büchi's problem ('the M squares problem') 1.1 *Is it true that, for large enough M, the only integer solutions of the system of equations*

$$x_n^2 + x_{n-2}^2 = 2x_{n-1}^2 + 2 \qquad\qquad n = 2, \ldots, M-1 \tag{1}$$

satisfy $\pm x_n = \pm x_{n-1} + 1$?

Büchi's problem remains unsolved. In this paper:

1. We prove a positive answer to the analogous problem for a sequence of non-constant rational functions x_n, if the characteristic of F is 0, for $M \geq 18$, or if each x_n is in $F[t]$ and the characteristic of F is either 0 or $p \geq 17$, for $M \geq 14$. We prove the similar result in the case of fields $F(t)$ where the characteristic of F is $p \geq 19$ but only for sequences satisfying an additional assumption, for $M \geq 19$. This is Theorem 1.4. All these results for $p > 0$ are new while that for characteristic 0 follows (for $M \geq 8$) from results of Vojta. In contrast to the methods of Vojta, which use results of modern Algebraic Geometry and Nevanlinna Theory, our proofs are of an elementary nature.

2. As a consequence of (1) we prove a theorem in Logic (Theorem 1.7).

Büchi's problem and its implications were publicized by Leonard Lipshitz in [14]. It was discussed publicly by Joseph Lipman and Barry Mazur (cf. [16]). In [30] Paul Vojta gave two pieces of evidence that Büchi's problem may have a positive answer:

(A) He proved that a conjecture of Serge Lang implies a positive answer to it for $M \geq 8$. In fact Vojta's result gives the same kind of (conditional) answer over the field $\mathbb{Q}$ of rational numbers.

(B) He showed (using Nevanlinna theory) that the analogous problem for holomorphic functions has a positive answer. This may be regarded as evidence in favor of a positive answer to Büchi's problem in the light of the observation that algebraic varieties which posses infinitely many points in some number field are often of a special geometric type (Kobayashi hyperbolic) - conjectures have been made that this correspondence is an equivalence (cf. [12] and [29]).

In what follows X_M is the projective subvariety of the projective M-space $\mathbf{P}^M$, over $\mathbb{C}$, cut out by the equations (in projective coordinates $(x, x_0, \dots, x_{M-1})$)

$$x_n^2 + x_{n-2}^2 = 2x_{n-1}^2 + 2x^2 \qquad n = 2, \dots M-1 \ .$$

Vojta observed :

Fact 1.2 *For $M \geq 6$ the variety X_M is a surface of general type.*

Then he showed :

Theorem 1.3 *(i) ([30], Theorem 3.1) For $M \geq 8$, the only curves on X_M of geometric genus 0 or 1 are the 'trivial' lines $\pm x_n = \pm x_0 - nx$, $n = 0, \dots, M-1$.*

(ii) ([30], Theorem 6.1) Let $M \geq 8$ be an integer and let $f : \mathbb{C} \to X_M$ be a non-constant meromorphic curve. Then the image of f lies in one of the 'trivial' lines.

Statement (i) of the theorem has as a consequence that if a conjecture of Lang (or a weaker 'question' of Bombieri) is true then Büchi's problem has a positive answer. Statement (ii) shows that the analogue of Büchi's problem for holomorphic functions has a positive answer.

Our main result in this article is a solution of an analogue of Büchi's problem for fields of rational functions.

Theorem 1.4 *Let F be a field and t a variable. Assume that $(x_n)_{n=0}^{M-1}$ is a sequence of rational functions $x_n \in F(t)$, not all constant, which satisfy the recurrence relation (1). Assume that one of the following holds:*

1. *The terms x_n of the sequence are polynomials (i.e. in $F[t]$), the characteristic of F is either 0 or $p \geq 17$ and $M \geq 14$.*

2. *The characteristic of F is 0 and $M \geq 18$.*

3. *The characteristic of F is $p \geq 19$ and $M \geq 18$ and the following statement is not true:*

   'For some sequence $(\zeta_n)_{n=0}^{M-1}$ with $\zeta_n \in F(t)$ we have $\zeta_0 \notin F(t^p)$, there is an $s \in \{0, 1, \dots\}$ such that $x_n = \zeta_n^{p^s}$ (for $n = 0, \dots, M-1$) and there is a $\gamma \in F(t^p) \setminus F$ such that

$$\frac{\zeta_2^2}{\gamma + 2} - 2 = \frac{\zeta_1^2}{\gamma + 1} - 1 = \frac{\zeta_0^2}{\gamma} \ . \ ,$$

Then there are $\varepsilon_0, \dots, \varepsilon_{M-1}$ with $\varepsilon_n \in \{-1, 1\}$ such that for each n, $\varepsilon_n x_n = \varepsilon_0 x_0 + n$.

We prove it in Section 2. The case of zero characteristic follows also from any of the two statements of Theorem 1.3, for $M \geq 8$ (for a proof see [18]).

Theorem 1.4, and especially the case of positive characteristic, may be regarded as evidence in favor of a positive answer to Büchi's problem, independent of that provided by Vojta.

Büchi's problem, besides being a testing ground for number theoretical techniques and conjectures, has some interesting applications in Logic. Büchi had in mind to apply the answer, if positive, in order to prove a negative answer to the following question.

Let L be the language (set of symbols) which contains a symbol for addition, a symbol for the property 'x is a square', a symbol for equality and symbols for the elements 0 and 1 (all symbols, operations and relations are interpreted in $\mathbb{Z}$ in the usual manner).

Question 1.5 *Is the positive-existential theory of L over $\mathbb{Z}$ decidable?*

If answered negatively, Question 1.5 will be one of the strongest forms of negative answer to Hilbert's tenth problem (cf. [15] and [2]) known today - and optimal in many ways (for example cf. the decidability results in [13] and [23] and the surveys in [24] and [20]). A negative answer to Question 1.5 would imply that there is no algorithm to answer the solvability of systems $A \cdot X = B$ over $\mathbb{Z}$, where A is an $n \times m$ matrix and B an $m \times 1$ matrix with entries in $\mathbb{Z}$ and X is an $m \times 1$ matrix whose i-th entry is x_i^2 - each x_i is an unknown. (But the solvability of one - only - quadratic equation is decidable, cf. [6] and the more general result in [7]).

We define the languages (sets of symbols) L_t and L_T, in which we will write statements (formulas) which we will interpret in the field $F(t)$ of rational functions.

The language L_t extends L by the following symbols

- Constant-symbols for the elements of the natural image of $\mathbb{Z}[t]$ in $F[t]$;
- For each element c of the natural image of $\mathbb{Z}[t]$ in $F[t]$, a unary function-symbol for the function $f_c : x \mapsto cx$.

The language L_T extends L by the following symbol

- A one-place predicate symbol T which will be interpreted as '$T(x)$ if and only if $x \notin F$'.

A sentence of L_t (resp. L_T) is *positive-existential* if it is of the form $\exists x \psi(x)$ where $x = (x_1, \ldots, x_n)$ is a tuple of variables and $\psi(x)$ is a disjunction of conjunctions of formulas of the form $g(x) = 0$ and 'x_i is a square' (resp. and $T(x_i)$), where

$$g(x) = a_1 x_1 + \cdots + a_n x_n - b$$

with the $a_i, b \in \mathbb{Z}[t]$ (resp. $\in \mathbb{Z}$). The *positive-existential theory* of a subring R of $F(t)$ in the language L_t (resp. L_T) is the set of positive-existential sentences of L_t (resp. L_T) which are true in R. We ask:

Question 1.6 *Let R be a ring of functions of the independent variable t.*
(a) Is the positive-existential theory of R in L_t decidable?
(b) Is the positive-existential theory of R in L_T decidable?

Büchi's problem is crucial in answering Question 1.6(a) in the following way: Let L_t^{ring} (resp. L_T^{ring}) be the extension of L_t (resp. L_T) by a symbol for multiplication in $F(t)$. Consider a ring R satisfying the hypothesis of Theorem 1.4. The conclusion of Theorem 1.4 implies that multiplication in R is positive-existentially definable in L_t (we will show this in the last section). Hence, if the analogue of Hilbert's tenth problem over R, in the language L_t^{ring} has a negative answer, then the positive-existential theory of R in L_t is undecidable. We prove a similar result in the language L_T, but only for polynomials (in characteristic 0 or $p \geq 17$) and function fields of characteristic 0.

Theorem 1.7 *Let F be a field of characteristic either 0 or $p \geq 17$. Let t be transcendental over F (a variable) and let R be a subring of $F(t)$, containing the natural image of $\mathbb{Z}[t]$ in $F[t]$. Then:*

(i) If $R \subset F[t]$ then multiplication over R is positive-existential in the language L_t. Consequently the positive-existential theory of R in L_t is undecidable.

(ii) Assume that the characteristic of F is either 0 or $p \geq 19$. Then multiplication over R is positive-existential in the language L_t. Consequently the positive-existential theory of R in L_t is decidable if and only if the positive-existential theory of R in the language L_t^{ring} is decidable.

(iii) Assume that $R \subset F[t]$. Then multiplication over R is positive-existential in the language L_T. Consequently the positive-existential theory of R in L_T is undecidable.

(iv) Assume that the characteristic of F is 0. Then multiplication over R is positive-existential in the language L_T. Consequently the positive-existential theory of R in L_T is decidable if and only if the positive-existential theory of R in the language L_T^{ring} is decidable.

Statement (i) of the Theorem follows from the results of [3] and [4], where it is proved that the positive-existential L_t^{ring}-theory of a ring of polynomials $F[t]$, and any subring R as in (i) of the Theorem, is undecidable. Statement (iii) follows from the similar result (for polynomial rings) in L_T^{ring} of [19]. The general problem of whether the positive-existential L_t^{ring}-theory of an arbitrary field of rational functions $F(t)$ is decidable or undecidable is open (for example, for $\mathbb{C}(t)$). The existing results are all of a negative nature (undecidable). The similar problems for the language L_T are open. We list as a corollary some of the known cases. Some more cases can be found in the results of the bibliography. For the status of problems regarding decidability of Diophantine problems over rings of functions, see [20].

Corollary 1.8 *Let F be a field of characteristic either 0 or $p \geq 19$. Let t be a variable and let R be a subring of $F(t)$ containing the natural image of $\mathbb{Z}[t]$. Then the following hold:*

(i) The positive-existential L_t-theory of R is undecidable if F is any of the following fields:

(a) A real field (cf. [3]).

(b) A finite field $\mathbf{F}_q(t)$ (cf. [17] and [28]) or an extension of a finite field, satisfying the assumptions of [24].

(c) A p-adic field [10].

(ii) Assume $F = K(s)$ where K is a field and s is a variable (algebraically independent of t over K). Assume that $s \in R$. Let $L_{t,s}$ be the extension of the language L_t by symbols of constants for the elements of the natural image of $\mathbb{Z}[s,t]$ in $K(s,t)$) and by unary symbols of function, one for each of the functions $f_c : x \mapsto cx$, where $c \in R$. Then the positive-existential $L_{t,s}$-theory of R is undecidable (cf.[9]).

The proof that Theorem 1.4 implies Theorem 1.7 is given in Section 3 and is an easy adaptation of the analogous argument for $\mathbb{Z}$, which is due to Büchi (made public by Lipshitz). The same, essentially, proof shows the similar result for the field of meromorphic functions on the complex plane, using Vojta's Theorem 1.3(ii). We state it :

Theorem 1.9 *(Vojta) Let R be a subring of the field of meromorphic functions of the variable t, on the complex plane, containing the ring $\mathbb{Z}[t]$. Then multiplication in R is positive-existentially definable in the languages L_t. Consequently, if the positive-existential theory of R in the language L_t^{ring} is undecidable, then the positive-existential theory of R in L_t is undecidable as well.*

Further problems : Four directions of possible generalizations of the present results are obvious :

- Prove the similar result for sequences of non-constant elements of $F(t)$, in the case of positive characteristic, without the additional hypothesis of Theorem 1.4.
- Treat the cases of characteristic $p = 3, \ldots, 17$. Also study the sequences which satisfy Relation (1) but have a smaller number of terms than that assumed in the hypothesis of Theorem 1.4.
- Generalize to algebraic function fields (perhaps, as a first step, to integral extensions of the polynomial rings). Besides the independent interest of the problem in those domains, the results would provide evidence for the analogous problem in number fields (or rings of integers in number fields). Note that there exist undecidability results for rings of algebraic functions : [5], [24], [26], [31] but the general problem (for algebraic functions of a fixed degree) remains open.
- Replace the property 'x is a square' by 'x is a k-th power', where k is an arbitrary integer with $k \geq 3$. In [18] a problem for k-th powers is presented, similar to that of Büchi's (that paper contains also a positive-existential definition of the rational integers or a quadratic extension in an arbitrary field of rational functions of characteristic zero for $k = 3$, and various conditional undecidability results).

2 Büchi's problem for rational functions

In this section we prove Theorem 1.4.

We suppose that the characteristic of the field F is either 0 or $p \geq M$. We can suppose without loss of generality that the base field F is algebraically closed. Also observe that if the characteristic of F is $p > 0$ and all the x_n are p-th powers, that is, $x_n \in F(t^p)$, then if the sequence $(x_n)_n$ satisfies (1), so does the sequence

$$(x_n^{\frac{1}{p}})_n$$

hence it suffices to consider only the case in which not all the x_n are p-th powers. So from now on we assume:

Assumption 2.1 *(a) The field F is algebraically closed.*
(b) One of the following holds:

1. *The characteristic of F is 0 and at least one of the x_n is not in F.*

2. *The characteristic of F is $p \geq 3$, $p \geq M \geq 3$ and not all x_n are elements of $F(t^p)$.*

Definition 2.2 *A* prime *is either a prime ideal of the ring $F[t]$, which we will* affine prime *or the* 'prime at infinity. *We will identify an affine prime P with the monic monomial $t - \rho$ that generates it. For any $x \in F(t) \setminus \{0\}$ we will write* $\mathrm{ord}_P(x)$ *for the order of x at the affine prime P and* $\mathrm{ord}_\infty(x)$ *for the order of x at the prime at infinity (*$\mathrm{ord}_\infty(x) =$ *(the degree of the denominator of x minus the degree of the numerator of x).*

Lemma 2.3 *There is an automorphism σ of $F(t)$ over F such that some $\sigma(x_n)$ has negative order at infinity.*

Proof: If some x_n has negative order at infinity then we are done. So assume that all x_n have non-negative order at infinity. By Assumption 2.1, some x_n is non-constant, hence has a pole P which is not the prime at infinity and is therefore of the form $t - \rho$ for some $\rho \in F$. Let σ be the automorphism of $F(t)$ over F which sends t to $\frac{1}{t} + \rho$. It is obvious that $\sigma(x_n)$ has negative order at infinity. $\diamond$

We apply a suitable automorphism σ to the sequence $(x_n)_n$ to obtain the sequence $(\sigma(x_n))_{n=0}^{M-1}$ with the property that some $\sigma(x_n)$ has negative order at infinity. Observe that the sequence $(\sigma(x_n))_{n=0}^{M-1}$ satisfies relation (1). Hence we consider the latter sequence instead of the given one, that is, we may assume, without loss of generality, the following:

Assumption 2.4 *Some x_n has negative order at infinity.*

Lemma 2.5 *(i) The system of equations (1) is equivalent to the following system:*

$$x_n^2 = (1-n)x_0^2 + nx_1^2 + n(n-1), \qquad n = 0, \ldots, M-1. \tag{2}$$

(ii) For any two indices n and m we have

$$mx_n^2 = (m-n)x_0^2 + nx_m^2 - mn(m-n) \tag{3}$$

Proof: (i) The proof, done by induction on n, is easy and left to the reader.

(ii) From Equation (2)

$$x_m^2 = (1-m)x_0^2 + mx_1^2 + m(m-1)$$

we can express x_1^2 in terms of x_0 and x_m

$$mx_1^2 = x_m^2 - (1-m)x_0^2 - m(m-1)$$

and plug it in

$$x_n^2 = (1-n)x_0^2 + nx_1^2 + n(n-1)$$

where $n \neq 0, m$. Observe that m may take the value 1. We obtain

$$mx_n^2 = m(1-n)x_0^2 + n[x_m^2 - (1-m)x_0^2 - m(m-1)] + mn(n-1)$$

after multiplication by m, hence

$$mx_n^2 = [m(1-n) - n(1-m)]x_0^2 + nx_m^2 - mn(m-1) + mn(n-1)$$

hence

$$mx_n^2 = (m-n)x_0^2 + nx_m^2 - mn(m-n)$$

after obvious simplifications. ◇

From Equation (3) we observe:

Corollary 2.6 *(i) Assume that the characteristic of F is 0. Then all but possibly one of the x_n are non-constant rational functions.*

(ii) Assume that the characteristic of F is $p > 0$. Then all but possibly one of the x_n are in $F(t) \setminus F(t^p)$.

The next lemma gives us an invariant of the sequence (x_n) which will be used often from now on.

Lemma 2.7 *For any two integers $n \neq m$ the expression*

$$\frac{x_m^2 - x_n^2}{m-n} - m - n$$

does not depend on n and m.

Proof: The proof follows from Equation (3) and is left to the reader. ◇

Definition 2.8 *(i) For any $n, m = 0, \ldots, M-1$ with $n \neq m$ we will be writing*

$$\nu = \frac{x_m^2 - x_n^2}{m-n} - m - n \tag{4}$$

(and we will be recalling that it does not depend on n and m).

(ii) For any $k = 0, \ldots, M-1$ we will be writing

$$\nu_k = \nu + 2k$$

that is,

$$\nu_k = \frac{x_m^2 - x_n^2}{m-n} - m - n + 2k \ .$$

Definition 2.9 *We will be writing*

$$\nu = \frac{f}{g}$$

where f and g are co-prime polynomials, and for each index n,

$$x_n = \frac{f_n}{g_n}$$

where f_n and g_n are co-prime polynomials. We will write

$$V_P = \min\{\mathrm{ord}_P(x_n) \mid n = 0, \ldots, M-1\}$$

for each prime P of $F(t)$ (including the prime at infinity).

Definition 2.10 *Denote by y the least common multiple of the g_n and write $x_n = \frac{y_n}{y}$, for some polynomials $y_n \in F[t]$. We denote by d_n the degree of y_n, by d^+ the maximum of the d_n (for $n = 0, \ldots, M-1$) and by d the degree of y.*

Lemma 2.11 *Let m, n, k be pairwise different integers. Then the greatest common divisor of $\{f_m, f_n, f_k\}$ is (1) (the unit ideal).*

Proof: ¿From Lemma 2.7, we have:

$$\frac{x_n^2 - x_m^2}{n-m} - n - m = \frac{x_m^2 - x_k^2}{m-k} - m - k = \frac{x_k^2 - x_n^2}{k-n} - k - n$$

for all m, n and k. Suppose there is a non-constant polynomial P dividing f_m, f_n and f_k. This polynomial has a zero in F, since F is by assumption algebraically closed. Therefore, computing the expressions of the last equation at this zero, we would have

$$n + m = m + k = k + n$$

hence $m = n = k$ which contradicts our hypothesis. ◇

Lemma 2.12 *Let P be a prime pole of some x_r. Then one of the following holds:*

(a) For each index n, $\mathrm{ord}_P(x_n) = V_P$ and $\mathrm{ord}_P(\nu) \geq 2V_P$.

(b) There is an index $\ell = \ell(P)$ such that: (1) $\mathrm{ord}_P(x_\ell) > V_P$, (2) For all $n \neq \ell$ we have $\mathrm{ord}_P(x_n) = V_P$ and (3) $\mathrm{ord}_P(\nu) = 2V_P$.

Proof: In case that for each index n, $\mathrm{ord}_P(x_n) = V_P$, from Equation (4) we obtain $\mathrm{ord}_P(\nu) \geq 2V_P$. So assume that there is an index ℓ such that $\mathrm{ord}_P(x_\ell) > V_P$. Let m be an index for which $\mathrm{ord}_P(x_m) = V_P$. From Lemma 2.7 we can write

$$\nu = \frac{x_m^2 - x_\ell^2}{m - \ell} - m - \ell$$

hence $\mathrm{ord}_P(\nu) = 2V_P$. And since for any index $n \neq \ell$ we have also

$$\nu = \frac{x_n^2 - x_\ell^2}{n - \ell} - n - \ell$$

we obtain

$$2\mathrm{ord}_P(x_n) = \mathrm{ord}_P(\nu) = 2V_P$$

hence $\mathrm{ord}_P(x_n) = V_P$. ◇

By Assumption 2.4 the prime at infinity is a pole of some x_n. Hence we obtain:

Corollary 2.13 *There is an index $\ell(\infty)$ such that for each $n \neq \ell(\infty)$ we have*

$$\mathrm{ord}_\infty(x_n) = V_\infty \ .$$

Hence, for any $m, n \neq \ell(\infty)$, we have

$$\deg(y_m) = \deg(y_n) \ .$$

Moreover $\mathrm{ord}_\infty(\nu) \geq 2V_\infty$.

Definition 2.14 *We fix the notation of Corollary 2.13, so we let $\ell(\infty)$ be an index such that for each index n we have $\mathrm{ord}_\infty(x_{\ell(\infty)}) \geq \mathrm{ord}_\infty(x_n)$.*

Definition 2.15 *We define*

$$\Delta_n = 2\nu_n \nu' x_n' - \nu'^2 x_n - 4 x_n x_n'^2$$

for each index n.

Lemma 2.16 *Assume that one of the following is true:*

- *The characteristic of F is either 0 or $p \geq 17$, for each index $n = 0, \ldots, M-1$ we have $x_n \in F[t]$, and $M \geq 14$ or*

- *The characteristic of F is either 0 or $p \geq 19$ and $M \geq 19$.*

Then we have

$$\Delta_n = 0 \tag{5}$$

for each index n.

Proof: We will split the proof into a sequence of claims.

Claim 1 : We have

$$x_m \Delta_m = x_n \Delta_n$$

for each two indices m and n.

Proof: Substitute

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

(resulting from Equation (4)) and

$$2x_m x'_m = 2x_n x'_n + (m-n)\nu'$$

(obtained by differentiating the two sides of Equation (4)) in $x_m \Delta_m$ and recall that $\nu_m = \nu + 2m$ and $\nu_n = \nu + 2n$. $\diamond$

Recall that $x_n = \frac{y_n}{y}$ where y_n and y are polynomials with $\deg(y_n) \leq d^+$ and $\deg(y) = d$.

Claim 2 : We may write

$$\nu = \frac{u}{y^2}$$

where $u \in F[t]$ and $\deg(u) \leq 2d^+$.

Proof: By Equation (4) we obtain that for $m \neq n$ we have $u = \frac{1}{m-n}(y_m^2 - y_n^2) - (m+n)y^2$. $\diamond$

For each index n we write $G_n = y^7 \Delta_n$.

Claim 3 : (i) The function G_n is a polynomial in $F[t]$ of degree at most $7d^+ - 4$.

(ii) If all the x_n are polynomials in $F[t]$ then Δ_n is a polynomial of degree less than or equal to $5d^+ - 2$.

Proof: (i) By the definition of Δ_n we obtain

$$G_n = y^7[2\nu_n \nu' x'_n - \nu'^2 x_n - 4x_n x'^2_n] =$$

$$y^7 \left[2\frac{u+2ny^2}{y^2} \frac{u'y - 2uy'}{y^3} \frac{y'_n y - y_n y'}{y^2} - \left(\frac{u'y - 2uy'}{y^3} \right)^2 \frac{y_n}{y} - 4\frac{y_n}{y} \left(\frac{y'_n y - y_n y'}{y^2} \right)^2 \right] =$$

$$2(u+2ny^2)(u'y - 2uy')(y'_n y - y_n y') - (u'y - 2uy')^2 y_n - 4y^2 y_n (y'_n y - y_n y')^2 \ .$$

It follows that $G_n \in F[t]$. To find an upper bound for $\deg(G_n)$ recall that we have

$$\deg(u) \leq 2d^+ \qquad \deg(y_n) \leq d^+ \qquad \deg(y) = d \qquad d+1 \leq d^+$$

and observe that if $z \in F[t]$ then $\deg(z') \leq \deg(z) - 1$. It follows that

$$\deg(u+2ny^2) \leq 2d^+ \qquad \deg(u'y-2uy') \leq 2d^+ + d - 1 \qquad \deg(y_n'y - y_n y') \leq d^+ + d - 1 \ .$$

Therefore we have

$$\begin{aligned} \deg(G_n) &\leq \max\{5d^+ + 2d - 2,\ 5d^+ + 2d - 2,\ 3d^+ + 4d - 2\} = \\ &\max\{5d^+ + 2d - 2,\ 3d^+ + 4d - 2\} \leq \max\{7d^+ - 4,\ 7d^+ - 6\} = 7d^+ - 4 \ . \end{aligned}$$

(ii) In the case that each x_n is in $F[t]$ we may take $y = 1$. Going through the proof of (i) with this adjustment we obtain the result. $\diamond$

We want to prove that for each index n, $\Delta_n = 0$. For the sake of contradiction we assume that for some index r, $\Delta_r \neq 0$. Throughout the rest of the proof we fix an arbitrary index r for which $\Delta_r \neq 0$. By the definition of Δ_r it follows that $x_r \neq 0$, so $x_r \Delta_r \neq 0$

Claim 4 : For each index n, $y_n G_n = y_r G_r$.

Proof: Substitute $x_n = \frac{y_n}{y}$, $x_r = \frac{y_r}{y}$ and $\nu = \frac{u}{y^2}$ in the terms of the relation $x_n \Delta_n = x_r \Delta_r$ of Claim 1. $\diamond$

We write β for the least common multiple of the elements of the set $\{y_n \mid n \neq r\}$.

Claim 5 : (i) $\deg(\beta) \leq 8d^+ - 4$.

(ii) If all x_n are polynomials in $F[t]$ then $\deg(\beta) \leq 6d^+ - 2$.

Proof: (i) By Claim 4 we obtain that each y_n divides $y_r G_r$ in $F[t]$. It follows that β divides $y_r G_r$ in $F[t]$. Hence, since $y_r G_r \neq 0$, $\deg(\beta) \leq \deg(y_r) + \deg(G_r)$. By Claim 3 we have $\deg(y_r) + \deg(G_r) \leq 8d^+ - 4$ and the result follows.

(ii) In the last sentence of the proof of (i) substitute the relation by $\deg(y_r) + \deg(G_r) \leq 6d^+ - 2$ (coming from Claim 3(ii)). $\diamond$

Claim 6 : We have

$$\prod_{n \neq r} y_n | \beta^2 \qquad \text{and} \qquad \deg(\beta) \geq \frac{M-2}{2} d^+$$

where the symbol $|$ means 'divides in $F[t]$'.

Proof: We prove that we have

$$\prod_{n \neq r} y_n | \beta^2 \ .$$

Let P be an arbitrary affine prime of $F(t)$. Assume that P divides some y_n (otherwise our assertion is trivially true). It suffices to show that

$$\mathrm{ord}_P\left(\prod_{n\neq r} y_n\right) \leq 2\ \mathrm{ord}_P(\beta)\ .$$

We distinguish two cases, according to whether P divides y or not.

Assume that P divides y. Then, by Lemma 2.12, P divides precisely one y_n, say y_k, so

$$\mathrm{ord}_P\left(\prod_{n\neq r} y_n\right) = \mathrm{ord}_P(y_k) = \mathrm{ord}_P(\beta)\ .$$

Now assume that P does not divide y. Then, by Lemma 2.11, P divides either precisely one y_n, say y_k, or precisely two, say y_k and y_m. In the first of these subcases we have

$$\mathrm{ord}_P\left(\prod_{n\neq r} y_n\right) = \mathrm{ord}_P(y_k) = \mathrm{ord}_P(\beta)\ .$$

In the second subcase assume that $\mathrm{ord}_P(y_k) = e$ and $\mathrm{ord}_P(y_m) = h$ with $e \geq h$. Then

$$\mathrm{ord}_P\left(\prod_{n\neq r} y_n\right) = \mathrm{ord}_P(y_k) + \mathrm{ord}_P(y_m) = e + h$$

while $\mathrm{ord}_P(\beta) = e$. Then $e + h \leq 2e$ so

$$\mathrm{ord}_P\left(\prod_{n\neq r} y_n\right) \leq 2\ \mathrm{ord}_P(\beta)\ .$$

To prove the second statement of the Claim observe that we have

$$\sum_{n\neq r,\ell(\infty)} \deg(y_n) \leq 2\ \deg(\beta)$$

from the first statement. By Corollary 2.13 we know that for $n \neq \ell(\infty)$ we have $\deg(y_n) = d^+$. Hence we have

$$\sum_{n\neq r,\ell(\infty)} \deg(y_n) = (M-2)d^+\ .$$

$\diamond$

The proof of the Lemma follows: by Claims 5 and 6 we obtain

$$\frac{M-2}{2}d^+ \leq \deg(\beta) \leq 8d^+ - 4$$

hence

$$\frac{M-2}{2}d^+ \leq 8d^+ - 4$$

which can not hold if $M \geq 19$.

By the same argument, if each x_n is a polynomial, we obtain

$$\frac{M-2}{2}d^+ \leq \deg(\beta) \leq 6d^+ - 2$$

which can not hold if $M \geq 14$.

The contradiction that we obtained proves the lemma. ◇

Lemma 2.17 *With the assumptions of Lemma 2.16 we have*

$$\nu' \neq 0 \ .$$

Proof: The conclusion of Lemma 2.16 gives $\Delta_n = 0$ for each index n. So if $\nu' = 0$ then $\nu'_n = 0$ and

$$x_n x_n'^2 = 0$$

for each n. Hence all x_n are either in F (in the case of characteristic 0) or in $F(t^p)$ (in the case of positive characteristic), which contradicts Assumption 2.1. ◇

Lemma 2.18 *With the assumptions of Lemma 2.16, for each index n, one of the following two statements is true:*
(a) There is a rational function $\gamma_n \in F(t) \setminus \{0\}$ such that $\gamma'_n = 0$ and

$$\nu_n = \frac{x_n^2}{\gamma_n} + \gamma_n \tag{6}$$

(b) There is a rational function δ_n such that $\delta'_n = 0$ and

$$\nu_n = 2\epsilon_n x_n + \delta_n \tag{7}$$

where $\epsilon_n = \pm 1$.

Proof: Let us rewrite the equations $\Delta_n = 0$ as

$$2\nu_n \nu'_n x'_n = x_n(\nu_n'^2 + 4x_n'^2)$$

by reordering and factorizing by x_n. Let us divide both sides of this equation by $x_n x_n'^2$ and write

$$\frac{\nu_n}{x_n} = \frac{\zeta_n}{\rho_n}$$

and

$$\frac{\nu'_n}{x'_n} = \frac{a_n}{b_n}$$

where a_n, b_n, ζ_n and ρ_n are polynomials such that a_n and b_n, respectively ζ_n and ρ_n, are co-prime. We obtain

$$2\zeta_n a_n b_n = \rho_n(a_n^2 + 4b_n^2)$$

after multiplication by $\rho_n b_n^2$. Since a_n and b_n are co-prime as well as ζ_n and ρ_n, we obtain that $\zeta_n = \beta_n(a_n^2 + 4b_n^2)$ and $\rho_n = 2\beta_n a_n b_n$ for some non-zero β_n in the base field F. Defining

$$\mu_n = \beta_n \frac{\nu_n}{\zeta_n}$$

we can express ν_n and x_n as

$$\nu_n = \frac{1}{\beta_n}\zeta_n\mu_n = (a_n^2 + 4b_n^2)\mu_n \tag{8}$$

$$x_n = \frac{\rho_n}{\zeta_n}\nu_n = \frac{2\beta_n a_n b_n}{\beta_n(a_n^2 + 4b_n^2)}(a_n^2 + 4b_n^2)\mu_n = 2a_n b_n \mu_n \tag{9}$$

in terms of these new variables. Next we compute the derivatives

$$\nu_n' = (2a_n a_n' + 8b_n b_n')\mu_n + (a_n^2 + 4b_n^2)\mu_n'$$

$$x_n' = 2a_n' b_n \mu_n + 2a_n b_n' \mu_i + 2a_n b_n \mu_n'$$

of ν_n and x_n. By the definition of a_n and b_n we have $b_n\nu_n' = a_n x_n'$, which gives

$$b_n[(2a_n a_n' + 8b_n b_n')\mu_n + (a_n^2 + 4b_n^2)\mu_n'] = a_n[2a_n' b_n\mu_n + 2a_n b_n'\mu_n + 2a_n b_n \mu_n'] \ .$$

after plugging our new expressions for ν_n' and x_n'. Hence we obtain

$$[b_n(2a_n a_n' + 8b_n b_n') - 2a_n a_n' b_n - 2a_n^2 b_n']\mu_n = [-b_n(a_n^2 + 4b_n^2) + 2a_n^2 b_n]\mu_n'$$

which gives

$$2[4b_n^2 - a_n^2]b_n'\mu_n = [-4b_n^2 + a_n^2]b_n\mu_n'$$

after obvious cancelation.

Suppose first that we have $a_n^2 = 4b_n^2$. By definition of a_n and b_n, it implies $\nu_n'^2 = 4x_n'^2$, hence $\nu_n' = \pm 2x_n'$. In this case we obtain :

$$\nu_n = \pm 2x_n + \delta_n$$

for some δ_n which is in F if the characteristic of F is 0 and in $F(t^p)$ if the characteristic of F is $p > 0$.

Suppose now that we have $a_n^2 \neq 4b_n^2$. In this case we obtain (recall that by Lemma 2.17 we have $\nu' \neq 0$, hence $\nu_n \neq 0$ and $\mu_n \neq 0$)

$$\frac{\mu_n'}{\mu_n} = -2\frac{b_n'}{b_n}$$

hence

$$\mu_n = \frac{\alpha_n}{b_n^2}$$

for some non-zero α_n which is in F if the characteristic of F is 0 and in $F(t^p)$ if the characteristic of F is $p > 0$. The latter relation and Equations (8) and (9) give the following new expressions

$$x_n = 2\alpha_n \frac{a_n}{b_n}$$

and

$$\nu_n = \alpha_n \frac{a_n^2 + 4b_n^2}{b_n^2} = \frac{x_n^2}{4\alpha_n} + 4\alpha_n$$

which gives Equation 6 by writing $\gamma_n = 4\alpha_n$. ◇

Lemma 2.19 *With assumptions and notation as in Lemma 2.18 the following holds: if Equation (7) holds for some index r then we have $\delta_r = 0$.*

Proof: Assume that for some index r Equation (7) holds and that x_r does not have zero derivative (cf. Corollary 2.6). Substituting $\nu_r = 2\epsilon_r x_r + \delta_r$ in the equation

$$\Delta_r = 2\nu_r \nu_r' x_r' - \nu_r'^2 x_r - 4x_r x_r'^2 = 0$$

we get

$$2(2\epsilon_r x_r + \delta_r)(2\epsilon_r x_r + \delta_r)' x_r' - (2\epsilon_r x_r + \delta_r)'^2 x_r - 4x_r x_r'^2 = 0$$

hence

$$4\epsilon_r(2\epsilon_r x_r + \delta_r)x_r'^2 - 4x_r'^2 x_r - 4x_r x_r'^2 = 0$$

since δ_r has zero derivative. The equation simplifies into

$$\delta_r x_r'^2 = 0$$

and the lemma is proven since we supposed $x_r' \neq 0$. ◇

Corollary 2.20 *With assumptions and notation as in Lemma 2.18 if for some r Equation (7) holds then it holds for all indices and the conclusion of Theorem 1.4 holds.*

Proof: By Lemmas 2.16 and 2.18 we obtain that for each index n one of Equations (6) and (7) holds. Assume that for some index r, Equation (7) holds. It then follows from Lemma 2.19 that $\nu_r = 2\epsilon_r x_r$ for some $\epsilon_r \in \{-1, 1\}$. Let us choose an index n distinct to r. Then by Equation (4) we obtain

$$x_n^2 = (n-r)(\nu + n + r) + x_r^2 = (n-r)(\nu_r + n - r) + x_r^2 = \\ (n-r)^2 + 2(n-r)\epsilon_r x_r + x_r^2 = (\epsilon_r x_r + (n-r))^2$$

which proves the corollary. ◇

Lemma 2.21 *With assumptions and notation as in Lemma 2.18 we have:*

(i) If Equation (6) holds for one index then it holds for each index and there is a $\gamma \in F(t)$ such that for each index n we have $\gamma_n = \gamma + n$.

(ii) With the additional assumption that either the characteristic of F is 0 or each x_n is a polynomial, the following holds: Equation (6) can not hold for any index.

Proof: By Corollary 2.20, it is clear that if Equation (6) holds for one index then it holds for each index. Consider two distinct indices, m and h, for each of which Equation (6) holds. So, for $i = m, h$ we have $\nu_i = \frac{x_i^2}{\gamma_i} + \gamma_i$. Substituting $\nu_i = \nu + 2i$ we obtain

$$\nu = \frac{x_i^2}{\gamma_i} + \gamma_i - 2i \ .$$

Differentiating both sides of Equation (4) and of the latter equation, for each of the indices m and h, we obtain

$$\frac{2x_m x'_m - 2x_h x'_h}{m-h} = \nu' = \frac{2x_m x'_m}{\gamma_m} = \frac{2x_h x'_h}{\gamma_h}$$

so

$$\nu' = \frac{\frac{2x_m x'_m}{2x_h x'_h} - 1}{m-h} 2x_h x'_h = \frac{\frac{\gamma_m}{\gamma_h} - 1}{m-h} 2x_h x'_h = \frac{\gamma_m - \gamma_h}{m-h} \frac{2x_h x'_h}{\gamma_h} = \frac{\gamma_m - \gamma_h}{m-h} \nu'$$

and (recall that by Lemma 2.17 $\nu' \neq 0$) consequently $\frac{\gamma_m - \gamma_h}{m-h} = 1$ so

$$\gamma_m - \gamma_h = m - h \ .$$

It then follows that there is a $\gamma \in F$ (and, in the case of characteristic $p > 0$, $\gamma \in F(t^p)$) such that for each index n for which Equation (6) holds, we have

$$\gamma_n = \gamma + n \ .$$

This proves (i).

Suppose that Equation (6) holds for some index, hence for every indices. Observe that from Equation (6) it follows that

$$\nu - \gamma = \frac{x_m^2}{\gamma + m} - m$$

and

$$\frac{x_m^2}{\gamma + m} - m = \frac{x_h^2}{\gamma + h} - h \ . \tag{10}$$

First we consider the case that F has characteristic 0. Let k be an index other than m, h. Then we obtain from Equation (6) that the elliptic curve

$$Y^2 = (X + m)(X + h)(X + k)$$

has as solutions

$$(X,Y) = \left(\nu - \gamma, \frac{x_m}{\sqrt{\gamma+m}}\frac{x_h}{\sqrt{\gamma+h}}\frac{x_k}{\sqrt{\gamma+k}}\right)$$

which is impossible since an elliptic curve is of genus 1 and does not admit a non-constant rational parametrization (by Hurwitz's formula, see [8]).

Now we consider the case in which the characteristic of F is $p \geq 17$ and each x_n is in $F[t]$.

Observe that if for some index k Equation(6) holds and $x_k \in F(t^p)$ then $\nu \in F(t^p)$ and then, from Equation (4), all x_n are in $F(t^p)$, which contradicts Assumption 2.1. Therefore we have $x_n \notin F(t^p)$ for each index n.

Now observe that by Equation (4) we have $\nu \in F[t]$ and since from Equation (10)

$$x_m^2 = (\nu - \gamma + m)(\gamma + m) = (\nu + 2m - (\gamma + m))(\gamma + m)$$

we have

$$\left(\gamma + m - \frac{\nu + 2m}{2}\right)^2 = \frac{(\nu+2m)^2}{4} - x_m^2$$

therefore $\gamma \in F[t^p]$. Observe that $\gamma + m$ and $\gamma + h$ can not have any common zero; It then follows by Equation (10) that $\gamma + m$ divides x_m^2 in $F[t]$ and $\gamma + h$ divides x_h^2 in $F[t]$.

Write $x_m = u_m^p z_m$ and $x_h = u_h^p z_h$ where $u_m, u_h \in F[t]$ and each of z_m and z_h has only zeros of multiplicities $\leq p-1$ and positive degree. Then

$$\frac{u_m^{2p}}{\gamma+m},\ \frac{u_h^{2p}}{\gamma+h} \in F[t]\ .$$

Differentiating both sides of Equation (10) we obtain

$$\frac{u_m^{2p}}{\gamma+m} z_m z_{m'} = \frac{u_h^{2p}}{\gamma+h} z_h z_h'\ .$$

Observe that

$$\frac{x_m^2}{\gamma+m} \qquad \text{and} \qquad \frac{x_h^2}{\gamma+h}$$

can not have a common zero, because from Equation (10) it would follow that $m = h$ (and we have assumed that $m, h < p$). Therefore z_m has no common zeros with $\frac{u_h^{2p}}{\gamma+h} z_h$, hence z_m divides z_h' in $F[t]$, therefore we obtain

$$\deg(z_m) \leq \deg(z_h') \leq \deg(z_h) - 1\ .$$

Similarly, z_h divides z_m' in $F[t]$ hence $\deg(z_h) \leq \deg(z_m) - 1$. The last two relations can not hold simultaneously. This contradiction proves the Lemma. $\diamond$

Proof of Theorem 1.4. By Lemmas 2.18, 2.19 and 2.21 and Corollary 2.20 we only have to consider the case in which the characteristic of F is $p \geq 19$ and Equation (6) holds for each index. Then, from Equation (6) and Lemma 2.21(i) applied for the indices 0, 1 and 2 gives

$$\frac{x_2^2}{\gamma+2} - 2 = \frac{x_1^2}{\gamma+1} - 1 = \frac{x_0^2}{\gamma} \ ,$$

which contradicts the hypothesis of the Theorem.

3 Consequences for Logic

Proof of Theorem 1.7 Our proof is an adjustment of the proof of Theorem 1.4 of [18].

We write $P_2(x)$ to mean 'x is a square in $F(t)$'. We consider a ring R as in the hypothesis of the Theorem. Let $N = 14$ if $R \subset F[t]$ and let $N = 18$ otherwise. Let $\psi(z, w, w_0, \ldots, w_{N-1})$ denote the formula

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

and $\phi(z, w)$ denote the formula

$$\exists w_0, \ldots, w_{N-1} \in R \ \psi(z, w, w_0, \ldots, w_{N-1}) \ .$$

We claim:

Proposition 3.1 *Assume that F and R satisfy the hypothesis of some of the cases of Theorem 1.7. Then the following hold:*

(I) Assume that $z, w \in R$ and $w = z^2$. Then $\phi(z, w)$ holds true.

(II) Assume that $z, w, w_0, \ldots, w_{N-1} \in R$ and that $\psi(z, w, w_0, \ldots, w_{N-1})$ holds true. Assume that $x_0, \ldots, x_{N-1} \in R$ are such that the sequence

$$(w_n)_{n=0}^{N-1} = (x_n^2)_{n=0}^{N-1}$$

satisfies $\psi(z, w, w_0, \ldots, w_{N-1})$. Then either $w = z^2$ or one of the following Conditions holds:

(A) The hypothesis of Case (i) of Theorem 1.7 holds, so each x_i is in $F[t]$, and $z, w \in F$.

(B) The hypothesis of Case (ii) of Theorem 1.7 holds and the characteristic of F is 0, and $z, w \in F$.

(C) The hypothesis of Case (ii) of Theorem 1.7 holds and the characteristic of F is $p \geq 19$, and $z, w \in F(t^p)$.

(D) The hypothesis of Case (ii) of the Theorem holds and the characteristic of F is $p \geq 19$, and, in addition, not both of z and w are in $F(t^p)$, and there is a $\gamma \in F(t^p)$ such that

$$\frac{x_2^2}{\gamma+2} - 2 = \frac{x_1^2}{\gamma+1} - 1 = \frac{x_0^2}{\gamma} \ .$$

Proof:

(I) Take $w_i = (z+i)^2$.

(II) Assume that Conditions (A), (B), (C) and (D) do not hold. Then $(w_n)_{n=0}^{N-1}$ satisfies the hypothesis of Theorem 1.4 and consequently

$$w_1 = x_1^2 = (\pm x_0 + 1)^2$$

hence, since $2z = w_1 - w_0 - 1$, we have

$$2z = x_1^2 - x_0^2 - 1 = (\pm x_0 + 1)^2 - x_0^2 - 1 = \pm 2x_0$$

and $w = z^2$. $\diamond$

We continue with the proof of Theorem 1.7, proving separately each case:

(i) This is the case in which $R \subset F[t]$.

Consider the formula

$$\eta(z,w)\colon \phi(z,w) \wedge \phi(tz, t^2w) \wedge \phi(z+t, w+2tz+t^2)\ .$$

We claim that it is equivalent to $w = z^2$. By the above Proposition and Theorem 1.4, if $w \neq z^2$, we have that condition (A) holds, hence $z, tz, z+t, w, t^2w, w+2tz+t^2 \in F$, which is impossible.

Thus squaring and, consequently, multiplication over R is positive-existentially definable in the language L_t. By [3] and [4] the positive-existential theory of R in L_t^{ring} is undecidable. Hence the positive-existential theory of R in L_t is undecidable.

[Note that in [3] (for polynomial rings) and [4] the undecidability results are stated only for $R = F[t]$; one has to go through the statements of the Lemmas to see that actually it holds for any subring R which contains the natural image of $\mathbb{Z}[t]$.]

(ii) This is the case in which $R \subset F(t)$.

Subcase 1: Assume that the characteristic of F is 0. Then the proof is exactly the same as in Case (i): The formula η (for $N = 18$) defines squaring. So one obtains: Decidabilty of the existential theory of R in L_t is equivalent to decidability of R in L_t^{ring} but it is unknown whether the latter is decidable or undecidable for arbitrary F (cf. the discussion in [20]).

Subcase 2: Assume that the characteristic of F is $p \geq 19$.

Consider the formula

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

Obviously, if $w = z^2$, then $\theta(z,w)$ holds. We claim:

Claim: If $\theta(z,w)$ holds and $w \neq z^2$ then one of the following three conditions holds:

(a) both z and w are in $F(t^p)$,

(b) both $z+t$ and $w+2tz+t^2$ are in $F(t^p)$,
(c) both $z-t$ and $w-2tz+t^2$ are in $F(t^p)$. $\diamond$

We assume for the moment that the Claim is true and show that a consequence of the Claim and Proposition 3.1 is that the formula

$$\eta_1(z,w)\colon \theta(z,w)\wedge\theta(z+t^2, w+2t^2z+t^4)$$

is equivalent to $w=z^2$. By Proposition 3.1 (I), if $w=z^2$ then clearly $\eta_1(z,w)$ holds true. Conversely, suppose that $\eta_1(z,w)$ holds true and $w\neq z^2$. Then for each couple

$$X=(z,w) \qquad \text{and} \qquad Y=(z+t^2, w+2t^2z+t^4)$$

one of (a), (b) or (c) of the Claim is true. Suppose (a) is true for both X and Y. Then in particular $z, z+t^2\in F(T^p)$ which is absurd. Suppose (a) is right for X and (b) is right for Y. Then $z, w, z+t^2+t, w+2t^2z+t^4+2t(z+t^2)+t^2\in F(T^p)$ hence $t^2+t\in F(t^p)$ and $w+2(t^2+t)z+t^2+2t^3+t^4\in F(t^p)$ which is absurd. All the other cases are done similarly (the proof is left to the reader).

Then the proof of Theorem 1.7 follows as in the previous Case (i).

We continue with a proof of the Claim. Assume that $\theta(z,w)$ holds. For the sake of contradiction assume that $w\neq z^2$ and that none of the conditions (a), (b) and (c) holds. Then, by Proposition 3.1, Condition (D) holds relative to each of the formulas

$$\phi(z,w), \qquad \phi(z+t, w+2tz+t^2) \qquad \text{and} \qquad \phi(z-t, w-2tz+t^2)\ .$$

Hence we obtain:

- By the hypothesis that $\phi(z,w)$ is true, there is a $\gamma\in F(t^p)$ such that

$$\frac{x_2^2}{\gamma+2}-2=\frac{x_1^2}{\gamma+1}-1=\frac{x_0^2}{\gamma}\ .$$

  Then, computing, we have $x_1^2=(\gamma+1)(\frac{x_0^2}{\gamma}+1)$ and

$$2z=x_1^2-x_0^2-1=(\gamma+1)(\frac{x_0^2}{\gamma}+1)-x_0^2-1=\frac{1}{\gamma}w+\gamma\ . \tag{11}$$

- By the similar argument for $\phi(z+t, w+2tz+t^2)$ instead of $\phi(z,w)$ we conclude that there is a $\gamma_2\in F(t^p)$ such that

$$2(z+t)=\frac{1}{\gamma_2}(w+2tz+t^2)+\gamma_2 \tag{12}$$

  and

- By the similar argument for $\phi(z-t, w-2tz+t^2)$ we conclude that there is a $\gamma_3 \in F(t^p)$ such that

$$2(z-t) = \frac{1}{\gamma_3}(w-2tz+t^2)+\gamma_3 \ . \tag{13}$$

By Equation (11) we solve for w:

$$w = 2\gamma z - \gamma^2$$

and substitute in Equations (12) and (13):

$$2\gamma_2(z+t) = (\gamma z - \gamma^2) + 2tz + t^2 + \gamma_2^2 \tag{14}$$

and

$$2\gamma_3(z-t) = (\gamma z - \gamma^2) - 2tz + t^2 + \gamma_3^2 \ . \tag{15}$$

Adding the corresponding sides of Equations (14) and (15) we obtain

$$2(\gamma_2+\gamma_3-\gamma)z = 2t^2 - 2(\gamma_2-\gamma_3)t + (\gamma_2^2+\gamma_3^2-2\gamma^2) \ . \tag{16}$$

Considering Equation (16) as a linear equation over the field $F(t^p)$ observe that the coefficient of z, $2(\gamma_2+\gamma_3-\gamma)$, cannot be equal to 0, since the set $\{1, t, t^2\}$ is linearly independent over $F(t^p)$. We conclude that z has the form

$$z = \alpha_0 + \alpha_1 t + \alpha_2 t^2 \tag{17}$$

where α_0, α_1 and α_2 are in $F(t^p)$ (and can be computed easily as functions of γ, γ_2 and γ_3). Substituting this expression for z in Equation (14) we find (recalling that the set $\{1, t, t^2, t^3\}$ is linearly independent over $F(t^p)$) that $\alpha_2 = 0$; Substituting $z = \alpha_0 + \alpha_1 t$ in Equation (16) we find a contradiction (since the set $\{1, t, t^2\}$ is linearly independent over $F(t^p)$).

(iii) and (iv) Work like in (i) but with η substituted by

$$\eta_2(z,w)\colon \phi(z,w) \wedge T(w) \ .$$

The result follows by [19] where it is proved that the positive-existential theory of a ring R, satisfying our hypothesis, in L_T^{ring} is undecidable.

References

[1] F. Campana, *Special varieties and classification theory: an overview. Monodromy and differential equations* (Moscow, 2001). Acta Appl. Math. 75 (2003), no. 1-3, 29–49. 14Jxx (32J18 32Q57)

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

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

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

[5] K. Eisenträger *Hilbert's tenth problem for algebraic function fields of characteristic 2*, Pacific J. Math. **210**, no. 2, 261-281 (2003).

[6] F. Grunewald and D. Segal, *How to solve a quadratic equation in integers*, Mathematical Proceedings of the Cambridge Philosophical Society **89**, 1-5 (1981).

[7] F. Grunewald and D. Segal, *Some general algorithms I and II*, Ann. Math., 112 (1980), 531-617

[8] R. Hartshorne, *Algebraic geometry*, Springer Verlag, Grad. texts in math. (1977).

[9] K.H. Kim and F.W. Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, Journal of Algebra **150**, 35-44 (1992).

[10] ——*Diophantine unsolvability over p-adic function fields*, Journal of Algebra **176**, no. 1, 83-110. (1995).

[11] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics, Springer-Verlag, New York (1987).

[12] —— *Hyperbolic diophantine analysis*, Bulletin of the American Mathematical Society **14**, 159-205 (1986).

[13] L. Lipshitz, *The diophantine problem for addition and divisibility*, Trans. Amer. Math. Soc. **235** (1978), 271-283.

[14] 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).

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

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

[17] T. Pheidas, *Hilbert's Tenth Problem for fields of rational functions over finite fields*, Inventiones Matematicae **103**, 1-8, (1991).

[18] T. Pheidas and X. Vidaux, *Extensions of Büchi's problem: Questions of decidability for addition and k-th powers*, to appear in Fundamenta Mathmaticae.

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

[20] —— *Undecidability of existential theories of rings and fields: A survey*, Contemporary Mathematics **270**, 49-106 (1999).

[21] Y. Pourchet, *Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques*, Acta Arith. **XIX**, 89-104 (1971).

[22] E. S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85**, 203-362 (1951); **92**, 191-197 (1954).

[23] A. Semenov, *Logical theories of one-place functions on the set of natural numbers*, Mathematics of the USSR-Izvestija **22**, 587-618 (1984).

[24] A. Shlapentokh, *Diophantine Undecidability over Algebraic Function Fields over Finite Fields of constants*, Journal of Number Theory **58**, no.2, 317-342 (1996).

[25] —— *Hilbert's tenth problem over number fields, a survey*, Contemporary Mathematics **270**, 107-137 (2000).

[26] —— *Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic*, Pacific Journal of Mathematics **193**, no. 2, 463-500 (2000).

[27] J. H. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, Grad. texts in math. (1986).

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

[29] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, Springer-Verlag, **1239** (1987)

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

[31] K. Zahidi, *The existential theory of real hyperelliptic function fields*, Journal of Algebra **233**, 65-86 (2000)