Pacific Journal of Mathematics

# THE ANALOGUE OF BÜCHI'S PROBLEM FOR CUBES IN RINGS OF POLYNOMIALS

THANASES PHEIDAS AND XAVIER VIDAUX

Volume 238 No. 2 December 2008

PACIFIC JOURNAL OF MATHEMATICS
Vol. 238, No. 2, 2008

# THE ANALOGUE OF BÜCHI'S PROBLEM FOR CUBES IN RINGS OF POLYNOMIALS

THANASES PHEIDAS AND XAVIER VIDAUX

**Let $F$ be a field of characteristic zero. We give the following answer to a generalization of a problem of Büchi over $F[t]$: A sequence of 92 or more cubes in $F[t]$, not all constant, with constant third difference equal to 6, consists of cubes of successive elements $x$, $x+1$, ..., for some $x \in F[t]$. We use this, in conjunction to the negative answer to Hilbert's tenth problem for $F[t]$, to show that the solvability of systems of degree-one equations, where some of the variables are assumed to be cubes and (or) nonconstant, is an unsolvable problem over $F[t]$.**

## 1. Introduction

Büchi asked the following question, known as the $n$-squares problem:

> *Is there a positive integer $M$ such that any sequence of at least $M$ integer squares, with constant second difference 2, is equal to a sequence of squares of successive integers*?

He intended to apply a possible positive answer to obtain a result in logic (we discuss this below). The question was made public in [Lipshitz 1990]. P. Vojta [2000] proved that a positive answer to the analogous question for rational numbers is implied by a conjecture of S. Lang, or by a positive answer to a weaker question of E. Bombieri; he also answered in the affirmative the analogue of Büchi's question for meromorphic functions defined on $\mathbb{C}$ or for function fields of curves of characteristic zero. (For rings of functions, one naturally demands that the elements of the sequence be nonconstant.) Further discussion can be found in [Mazur 1994]. The original $n$-squares problem is still open.

*MSC2000:* 03C60, 12L05, 11U05, 11C08.
*Keywords:* Buchi's problem, Hilbert's tenth problem, existential undecidability, cubic forms.
Pheidas's work is supported in part by the MODNET European Network. Part of this work has been done while Vidaux was at the University of Oxford, supported by the EC postdoctoral Marie Curie Individual Fellowship MCFI-2002-00722. The work was completed while Pheidas visited Vidaux at the University of Concepción, Chile, supported by the Chilean research project for international cooperation FONDECYT 7070169, under research project FONDECYT 1060947.

D. Hensley [1983] proved that the analogue of Büchi's problem in finite fields $\mathbb{F}_p$, where $p$ is a prime number, has a positive answer with $M = p$. He also gave a nice "heuristic proof" of the conjecture and various lower and upper bounds on the heights of the terms of a Büchi sequence. D. Buell [1987] characterized all the nontrivial integer sequences of length four (we call a sequence of squares of successive numbers *trivial*). R. G. E. Pinch [1993] proved, under a certain condition on the size, that a family of four-term sequences cannot be extended to five-term sequences. J. Browkin and J. Brzeziński [2006] showed that there exist infinitely many nontrivial five- and six-term sequences (originally, Büchi asked the question for five-term sequences), but for certain constants distinct from 2. It is not known to us whether there exist any nontrivial five-term sequences of integers when the constant is 2 as in the original problem.

Vojta's conditional result claims finiteness of the set of eight-term nontrivial sequences of integers. His result actually does not give a value for $M$, but only implies that there exists an $M \geq 8$ such that Büchi's original problem has a positive answer. We must apologize for citing Vojta's result wrongly in our previous works, where we claimed that his conjectural result was for $M = 8$.

In [Pheidas and Vidaux 2005] we generalized Büchi's question as follows:

**Question 1.1.** *Let $k > 1$ be an integer. Is there a positive integer $M$ such that any sequence $y = (y_0, \ldots, y_{M-1})$ of $k$-th powers of integers with constant $k$-th difference equal to $k!$ is necessarily a sequence of $k$-th powers of successive integers*? (*That is, one such that $y_n = (x+n)^k$ for a fixed integer $x$ and $n \in \{0, \ldots, M-1\}$.*)

Except for Vojta's results mentioned above and those of [Pheidas and Vidaux 2006], the question is open for all $k$ and for any global field in place of the integers. (Recall that in the case of function fields we restrict our attention to sequences of *nonconstant* functions.)

In the present paper we prove a positive answer to the analogue of the Question in the case $k = 3$ and for a polynomial ring $F[t]$ in place of the integers, where $F$ is a field of characteristic zero. We prove:

**Theorem 1.2.** *Let $F$ be a field of characteristic 0 and $t$ a transcendental element over $F$. Assume that $x_0, \ldots, x_{M-1} \in F[t]$, that at least one of the $x_n$ is nonconstant and that $M$ is not less than 92. If the third difference of the sequence $(x_0^3, \ldots, x_{M-1}^3)$ is constant and equal to 6, which is to say, if*

$$x_{n+3}^3 - 3x_{n+2}^3 + 3x_{n+1}^3 - x_n^3 = 6 \quad \text{for } n = 0, \ldots, M-4, \tag{1}$$

*then, for some $x \in F[t]$ and for any $n = 0, \ldots, M-1$, we have*

$$x_n^3 = (x+n)^3.$$

Here is a consequence of this theorem to mathematical logic:

**Theorem 1.3.** *Let $F$ be a field of zero characteristic and let $t$ be a variable. Let $L_{3,T}$ be the language $\{0, 1, +, P_3, T\}$. Interpret the unary predicate $P_3$ as '$P_3(y)$ if and only if $y$ is a cube (third power) in $F[t]$', interpret the unary predicate $T$ as '$T(x)$ if and only if $x$ is a nonconstant polynomial' and interpret $0, 1$ and $+$ as usual. Let $L_{3,t}$ be the language $\{0, 1, +, P_3, R\}$ where $R$ is a constant-symbol for the function which sends any $x$ to $tx$ (and the remaining symbols are interpreted as above).*

(a) *Multiplication in $F[t]$ is positive-existentially definable in each of the languages $L_{3,T}$ and $L_{3,t}$.*

(b) *The positive-existential theory of $F[t]$ in the language $L_{3,T}$ is undecidable.*

(c) *The positive-existential theory of $F[t]$ in the language $L_{3,t}$ is undecidable.*

This strengthens a result of J. Denef [1978] — an analogue of Hilbert's tenth problem for rings of polynomials in the variable $t$, in the language $\{+, \cdot, 0, 1, t\}$ (see expositions in [Matiyasevich 1970; Davis 1973; Pheidas and Zahidi 2000; Poonen 2003; Shlapentokh 2000]). It also strengthens the similar result in [Pheidas and Zahidi 1999] referring to the language $\{+, \cdot,$ '$x$ is nonconstant' $, 0, 1\}$.

Here is an immediate consequence of Theorem 1.3:

**Corollary 1.4** (Undecidability of simultaneous representation by cubic forms). *There is no algorithm (Turing machine) that solves the following problem*:

> *Let $A$ and $B$ be two matrices with integer entries and with dimensions $m \times n$ and $m \times 1$, respectively. Assume that $x_1, \ldots, x_n$ are variables and $X$ is the column matrix of the $x_i^3$. Assume that $f_j(Y_1, \ldots Y_n)$ are polynomials of the variables $Y_1, \ldots Y_n$ of degree $1$, for $j = 1, \ldots, n$. Determine whether the system of equations*
>
> $$A \cdot X = B$$
>
> *has a solution with $x_1, \ldots x_n \in F[t]$ with the property that for each $j, f_j(x_1^3, \ldots, x_n^3) \notin F$.*

It would be desirable to be able to prove the similar statement having in place of the conditions $f_j(x_1^3, \ldots, x_n^3) \notin F$ conditions only of the form $x_i \notin F$, or, even, 'some of the $x_i$ are nonconstant'. But for the moment we cannot prove any of these. The proofs of 1.3 and 1.4 (at the end of the paper) show also that the analogous statements (omitting the conditions for nonconstancy) are equivalent over domains such as $\mathbb{Z}$ and $\mathbb{Q}$. It follows that the analogues of Corollary 1.4 over $\mathbb{Z}$ and over $\mathbb{Q}$ are open problems.

**Open problems.** It is natural to ask about the truth of the statements of Theorem 1.2 and 1.3 for domains other than polynomials. Some examples are:

(a) The ring of holomorphic and the field of meromorphic functions (on the complex plane or a $p$-adic plane);

(b) A polynomial ring $F[t]$ in any characteristic other than 3;

(c) The ring of algebraic functions of the variable $t$, integral over $F[t]$ (this would strengthen the result of A. Shlapentokh [Shlapentokh 1992]);

(d) Fields of rational functions in any characteristic other than 3;

(e) Fields of algebraic functions in any characteristic other than 3 (this would strengthen, for example, results of K. Eisentraeger and A. Shlapentokh [2007] (see also [Shlapentokh 2002; 2006]) and of K. Zahidi [2000]);

(f) $\mathbb{Z}$ and $\mathbb{Q}$ (and, in general, global fields).

*Outline of the proof.* We compute an invariant $\nu$ of the sequence which in the end turns out to be an $x$ as in Theorem 1.2. We observe that Equation (1) is equivalent to $x_n^3 = a + nb + (\nu + n)^3$, where $a$ and $b$ are invariants. Differentiating the terms of this equation, combining with the initial one and using an argument involving heights (degrees) we show that a certain invariant of the sequence is equal to 0 (Lemmas 2.7 and 2.9). In this way we obtain a dependence of $a$ on $b$ and $\nu$. Iterating the procedure we obtain $b$ as a function of $\nu$. In consequence the pairs of nontrivial solutions $(x_m, x_n)$ are shown to be on certain curves over $F$, of genus greater than 0, which is impossible for nonconstant $x_n$ and $x_m$. We obtain a number of degenerate cases which we have to rule out before we conclude with Theorem 1.2.

Our method can presumably be applied to the analogous problem for $k > 3$ (with $k$ as in Question 1.1) but the number and nature of degenerate cases seems to increase in a way that we have not been able to systematize to this point. Because of the fact that we use derivatives our proof does not transfer to the analogous problem over the integers or the rationals. □

**Remark.** Very recently, H. Pasten [2008] proved a strong version of Büchi's problem for squares over polynomial rings. His result gives new evidence that the analogous problem for any (fixed) power could have a positive answer.

## 2. Büchi's problem for cubes in polynomial rings

From now on we will fix a solution $(x_0, \ldots, x_{M-1})$ of the system (1) and write $u_n = x_n^3$, so

$$u_{n+3} - 3u_{n+2} + 3u_{n+1} - u_n = 6 \quad \text{for } n = 0, \ldots, M-4. \tag{2}$$

We call the sequence $u = (u_0, \ldots, u_{M-1})$ *trivial* if it is a sequence of cubes of successive elements; that is, if there is $x \in F[t]$ such that $u_n = (x+n)^3$ for all $n$.

Without loss of generality we can suppose that the field $F$ is algebraically closed. From now on we make the following assumption:

*The field $F$ is algebraically closed of characteristic zero, and at least one $x_n$ is not in $F$.*

**Lemma 2.1.** *The system* (2) *is equivalent to*

$$2u_n = n(n-1)u_2 - 2n(n-2)u_1 + (n-2)(n-1)u_0 + 2(n-2)(n-1)n \tag{3}$$

*for $n = 0, \ldots, M-1$, and more generally,*

$$\begin{aligned} 2u_n = {} & (k-n)(k-n-1)u_{k+1} - 2(k-n-1)(k-n+1)u_k \\ & + (k-n)(k-n+1)u_{k-1} - 2(k-n-1)(k-n)(k-n+1) \end{aligned} \tag{4}$$

*for any $k = 1, \ldots, M-2$.*

*Proof.* A brute-force proof by induction on $n$ is possible, but we will present here a shorter one due to the referee. Since the sequence $(w_n)$ defined by

$$w_n = \tfrac{1}{2}n(n-1)u_2 - n(n-2)u_1 + \tfrac{1}{2}(n-2)(n-1)u_0 + (n-2)(n-1)n$$

is a polynomial in $n$ with leading coefficient $n^3$, its third difference is the constant sequence (6). Therefore, $(w_n)$ satisfies Equation (2). Since $w_i = u_i$ for $i = 0, 1, 2$, the sequences $(w_n)$ and $(u_n)$ have the same three first terms, hence are equal. This proves that the system (3) holds. The system (4) holds by a similar argument. □

**Lemma 2.2.** *For any pairwise distinct indices $m, n, q \in \{0, \ldots, M-1\}$, the expression*

$$\nu_{m,n,q} = -\frac{1}{3}\left(\frac{(q-n)u_m + (m-q)u_n + (n-m)u_q}{(q-n)(m-q)(n-m)} + m + n + q\right) \tag{5}$$

*does not depend on $m$, $n$ and $q$.*

*Proof.* Replace $u_m$, $u_n$ and $u_q$ by the expressions given by (3). □

For any $m$, $n$ and $q$, we will be writing $\nu$ instead of $\nu_{m,n,q}$. We will call $\nu$ the *$\nu$-invariant of the sequence $u$*. Since

$$3\nu = \tfrac{1}{2}(u_2 - 2u_1 + u_0 - 6),$$

the $\nu$-invariant of the trivial solution of Büchi's problem (when $x_2 = x_0 + 2$ and $x_1 = x_0 + 1$) is $x_0$. To measure how far a solution $u$ of (2) is from being trivial, we will introduce the new variables

$$a = u_0 - \nu^3 \quad \text{and} \quad b = (u_1 - u_0) - \left((\nu+1)^3 - \nu^3\right).$$

We find

$$u_n = a + nb + (\nu + n)^3 \tag{6}$$

(using the expression for $\nu_{0,n,1}$). Note that $(x_n)$ is the trivial solution if and only if $a = b = 0$.

**Definition 2.3.** For $x \in F[t] \setminus \{0\}$, we denote by $\deg x$ the degree of $x$, while $\deg 0 := -\infty$. We denote by $e$ the maximum of the degrees of the $u_n$ for $n = 0, \ldots, M-1$ (hence $e > 0$). If the degree $e$ is divisible by 3 we write $d = \frac{1}{3}e$. In particular, if $u_n = x_n^3$ for each $n$, then $d$ is the maximum of the degrees of the $x_n$.

**Corollary 2.4.** *One of the following is true*:

(a) *Each $u_n$ has degree $e$.*

(b) *There is an index $l$ such that for each $n \neq l$ we have* $\deg u_n = e$ *and* $\deg u_l < e$.

(c) *There are indices $l_1 \neq l_2$ such that for each $n \neq l_i$, $i = 1, 2$, we have* $\deg u_n = e$ *and* $\deg u_{l_i} < e$, $i = 1, 2$.

*Proof.* Assume we are not in cases (a) or (b). Let $l_1 \neq l_2$ such that $\deg u_{l_i} < e$ and let $k$ be an index such that $\deg u_k = e$. By Lemma 2.2 we have

$$3\nu = \nu_{k,l_1,l_2} = -\frac{(l_2-l_1)u_k + (k-l_2)u_{l_1} + (l_1-k)u_{l_2}}{(l_2-l_1)(k-l_2)(l_1-k)} - k - l_1 - l_2$$

hence $\deg \nu = \deg u_k = e$. So for any index $n \neq l_1, l_2$ we have

$$3\nu = -\frac{(l_2-l_1)u_n + (n-l_2)u_{l_1} + (l_1-n)u_{l_2}}{(l_2-l_1)(n-l_2)(l_1-n)} - n - l_1 - l_2,$$

which implies $\deg u_n = \deg \nu = e$. □

**Corollary 2.5.** *If $m$, $n$, $q$ and $r$ are pairwise distinct indices of the sequence $u$, then $u_m$, $u_n$, $u_q$ and $u_r$ are coprime* (*the four polynomials do not have any common divisor*).

*Proof.* We have

$$\begin{aligned} 3\nu = 3\nu_{m,n,q} &= -\frac{(q-n)u_m + (m-q)u_n + (n-m)u_q}{(q-n)(m-q)(n-m)} - m - n - q \\ &= 3\nu_{m,n,r} = -\frac{(r-n)u_m + (m-r)u_n + (n-m)u_r}{(r-n)(m-r)(n-m)} - m - n - r. \end{aligned}$$

Suppose that there is a nonconstant polynomial $P$ dividing $u_m$, $u_n$, $u_q$ and $u_r$. $P$ has a zero in $F$. Computing the last two quantities of the latter relations at that zero we obtain $m+n+q = m+n+r$, hence $q = r$, which contradicts our hypothesis. □

**Definition 2.6.** Recalling Corollary 2.4, we let $l_1$ and $l_2$ be two indices such that $\deg u_{l_1} \leq e$, $\deg u_{l_2} \leq e$, and

$$\deg u_n = e \quad \text{for all } n \text{ other than } l_1 \text{ and } l_2.$$

**Lemma 2.7.** *Let $\{r_1, \ldots, r_m\} \subseteq \{0, \ldots, M-1\}$ be a set of $m$ distinct indices. If $Q$ is a nonzero polynomial in $F[t]$ divisible by each $x_{r_k}$ for $k = 1, \ldots, m$, then the degree of $Q$ is at least $\frac{1}{3}(m-2)/d$. In particular, if we choose $M \geq 92$ and $m = M$ then the degree of $Q$ is at least $30d$.*

*Proof.* Set $R = \{r_1, \ldots, r_m\}$. For all $n \in R$, let $P_n \in F[t]$ be such that $Q = x_n P_n$. Since $Q$ is not the zero polynomial, for each $n \in R$, neither $x_n$ nor $P_n$ is the zero polynomial. We write $\mu$ for the least common multiple of the elements of the set $\{x_n \mid n \in R\}$. Hence $\mu$ divides $Q$ and it is enough to show that the degree of $\mu$ is at least $\frac{1}{3}(m-2)/d$.

We claim that the product $\prod_{n\in R} x_n$ divides $\mu^3$. Let $P$ be an arbitrary prime of $F[t]$ which divides $\mu$. Write $\mathrm{ord}_P(x)$ for the order of $x \in F[t]$ at $P$. It suffices to show that

$$\mathrm{ord}_P\left(\prod_{n\in R} x_n\right) \leq 3\,\mathrm{ord}_P(\mu).$$

If $P$ does not divide any $x_n$, the result is obvious. So assume that $P$ divides $x_{k_1}$ for some index $k_1$ that we choose so that $\mathrm{ord}_P(x_{k_1})$ is maximum:

$$\mathrm{ord}_P(x_{k_1}) = \mathrm{ord}_P(\mu).$$

By Corollary 2.5, $P$ divides either precisely one $x_n$, or precisely two, or precisely three. Let $x_{k_i}$, $i = 1, \ldots, j$, be the polynomials divisible by $P$ in case j. In order to treat the three cases simultaneously, let $x_{k_2}$ and $x_{k_3}$ be such that $P$ does not divide any $x_n$ with $n \neq k_1, k_2, k_3$. If we choose the indices so that $\mathrm{ord}_P(x_{k_1}) \geq \mathrm{ord}_P(x_{k_2}) \geq \mathrm{ord}_P(x_{k_3})$, we obtain, as required,

$$\mathrm{ord}_P\left(\prod_{n\in R} x_n\right) = \mathrm{ord}_P(x_{k_1}) + \mathrm{ord}_P(x_{k_2}) + \mathrm{ord}_P(x_{k_3}) \leq 3\mathrm{ord}_P(x_{k_1}) = 3\mathrm{ord}_P(\mu),$$

It follows from the claim that

$$\sum_{n\in R} \deg x_n \leq 3 \deg \mu,$$

and by Corollary 2.4 we obtain

$$(m-2)d \leq \sum_{n\in R} \deg x_n,$$

where the $-2$ corresponds to the indices $l_1$ and $l_2$ from Definition 2.6. □

**Notation 2.8.** We write

$$A = -\nu'' a' + \nu' a'' + 6\nu'^3 \nu, \quad B = \nu'' b' - \nu' b'' - 6\nu'^3,$$

and if $B \neq 0$

$$q = \frac{A}{B}.$$

Observe that if $B\nu' \neq 0$ we can write

$$q = \frac{(a'/\nu')' + 6\nu\nu'}{-(b'/\nu')' - 6\nu'}. \tag{7}$$

**Lemma 2.9.** *Only the following mutually exclusive two cases can occur*:

Case 1: $\nu' = 0$.

Case 2: $B \neq 0$, $\nu' \neq 0$ *and we have*

$$a + bq + (\nu + q)^3 = 0, \tag{8}$$

$$a' + b'q + 3\nu'(\nu + q)^2 = 0. \tag{9}$$

*Proof.* By differentiating twice the sides of (6) we get

$$u'_n = a' + nb' + 3\nu'(\nu + n)^2 \tag{10}$$

and

$$u''_n = a'' + nb'' + 6\nu'^2(\nu + n) + 3\nu''(\nu + n)^2. \tag{11}$$

By plugging into (10) the expression for $3(\nu+n)^2$ that results from (11) we obtain

$$\nu'' u'_n = \nu'' a' + n\nu'' b' + \nu'\big(u''_n - a'' - nb'' - 6\nu'^2(\nu + n)\big),$$

which we can rewrite as

$$nB = A + U_n, \tag{12}$$

where

$$U_n = \nu'' u'_n - \nu' u''_n.$$

Multiplying (6) by $B^3$ and (10) by $B^2$ we get

$$B^3 u_n = aB^3 + nbB^3 + (\nu B + nB)^3,$$
$$B^2 u'_n = a'B^2 + nb'B^2 + 3\nu'(\nu B + nB)^2;$$

hence, replacing the expression of $nB$ from (12),

$$B^3 u_n = aB^3 + (A + U_n)bB^2 + (\nu B + A + U_n)^3,$$
$$B^2 u'_n = a'B^2 + (A + U_n)b'B + 3\nu'(\nu B + A + U_n)^2.$$

Separating terms that depend on $n$ from ones that don't, in both equations, we get

$$B^3 u_n - U_n\big(bB^2 + 3(\nu B + A)^2 + 3(\nu B + A)U_n + U_n^2\big) = aB^3 + AbB^2 + (\nu B + A)^3, \tag{13}$$

$$B^2 u'_n - U_n\big(b'B + 6\nu'(\nu B + A) + 3\nu' U_n\big) = a'B^2 + Ab'B + 3\nu'(\nu B + A)^2. \tag{14}$$

We give names to the right-hand sides of these two equations:

$$\Delta = aB^3 + AbB^2 + (\nu B + A)^3, \quad \Gamma = a'B^2 + Ab'B + 3\nu'(\nu B + A)^2.$$

We now use Lemma 2.7 to prove that $\Delta = \Gamma = 0$. Since $u_n = x_n^3$, its first and second derivatives, $u_n'$ and $u_n''$, are each a multiple of $x_n$, hence $U_n = \nu'' u_n' - \nu' u_n''$ is a multiple of $x_n$. Therefore, $\Delta$ and $\Gamma$ are both multiples of $x_n$ for each $n \in \{0, \ldots, M-1\}$. Let us compute an upper bound for the degrees of $\Delta$ and $\Gamma$. Recalling Definition 2.6 we see that the degree of $u_n$ is not more than $e$, hence that of $\nu$ is not more than $e$ and we have $\deg a \le 3e$, $\deg b \le 2e$, and

$$\deg A \le 4e-3, \quad \deg B \le 3e-3, \quad \deg U_n \le 2e-3 \quad \text{and} \quad \deg(\nu B + A) \le 4e-3.$$

Therefore, computing the degrees of the left-hand sides of (13) and (14), we find

$$\deg \Delta \le 10e - 9 = 30d - 9 < 30d,$$
$$\deg \Gamma \le \ 7e - 7 = 21d - 7 < 30d.$$

We deduce from Lemma 2.7 that we have $\Delta = 0$ and $\Gamma = 0$.

If $B$ is not zero then $\nu'$ is not zero and we have

$$\frac{\Delta}{B^3} = a + \frac{A}{B} b + \left(\nu + \frac{A}{B}\right)^3 = 0, \quad \frac{\Gamma}{B^2} = a' + \frac{A}{B} b' + 3\nu' \left(\nu + \frac{A}{B}\right)^2 = 0,$$

which proves (8) and (9).

We next assume that $B = 0$ and prove that $\nu' = 0$. We know from Equation (12) that $A + U_n = 0$ for all $n$. Since $U_n$ is a multiple of $x_n$, and $\deg U_n \le 2e-3 = 6d-3$, we deduce from Lemma 2.7 that $U_n$ is zero. From Corollary 2.4, we know that at most two of the $u_n$ may be constant, namely $u_{l_1}$ and $u_{l_2}$. For all $n \in \{0, \ldots, M-1\}$ distinct from $l_1$ and $l_2$, we may write

$$\frac{U_n}{{u_n'}^2} = \frac{\nu'' u_n' - \nu' u_n''}{{u_n'}^2} = \left(\frac{\nu'}{u_n'}\right)'$$

and deduce that for those $n$, the quotient $\nu'/u_n'$ must be a constant in $F$, say $c_n$. So we have $c_n u_n' = \nu'$ for at least $M-2$ distinct values of $n$, so for at least 90 distinct values of $n$. We conclude by Lemma 2.7: since

$$\deg \nu' \le e - 1 = 3d - 1 < \frac{90-2}{3} d,$$

we have $\nu' = 0$. □

We will need the following proposition, whose proof comes from the theory of elliptic curves (see, for example, [Husemöller 2004, Definition (6.2), page 17] or [Silverman 1986, Hurwitz's Theorem, II.5]). The main observation that concerns us here is that a nonsingular cubic curve is of genus 1.

**Proposition 2.10.** *Let $\mu, \xi \in F$.*

(a) *The curve with affine equation $Y^3 = \mu X^3 + \xi$ has genus 1 provided that $\mu\xi \neq 0$.*

(b) *The curve with affine equation* $Y^2 + \mu Y + \xi = X^3$ *has genus* 1 *provided that* $\mu^2 \neq 4\xi$.

**Remark.** The general strategy from now on will be the following: we will provide relations among $a$, $b$ and $v$ that will produce equations that will define curves as in Proposition 2.10, where the coefficients $\mu$ and $\xi$ will depend on one or various indices $n$. These curves will have rational parametrization by polynomials made up of products of various $x_n$'s; hence they will define curves of genus 0 (for all the indices considered). Proposition 2.10 will then tell us that this can happen for very few values of $n$ (as long as any of $x_n$ or $x_0$ is nonconstant, and in particular, if $n$ is different from $l_1$ and $l_2$). So we will have space to choose the indices such that one of the curves considered is of genus 1, while it admits a rational parametrization, and this will give us a contradiction. The only case that will survive is that in which for all $n$ we have $x_n^3 = (v+n)^3$, which will prove Theorem 1.2.

**Lemma 2.11.** *Case* 1 *is impossible, that is,* $v'$ *can not be zero.*

*Proof.* We will show first that if $v$ is constant then so is $a$, and then that $v$ and $a$ cannot be both constant.

Assume that $v' = 0$ and $a' \neq 0$. So we have $a' = u_0'$ from the definition of $a$, and

$$u_n' = a' + nb', \quad u_n'' = a'' + nb''$$

from (6). This leads to $u_n' b'' = a'b'' + nb''b' = a'b'' + (u_n'' - a'')b'$, that is,

$$u_n' b'' - u_n'' b' = a'b'' - a''b'.$$

Since $x_n$ divides $u_n'$ and $u_n''$ and the degree of $u_n' b'' - u_n'' b'$ is no more than $3e-3$, we deduce from Lemma 2.7 that

$$a'b'' - a''b' = 0.$$

Since $a' \neq 0$, we can write

$$\left(\frac{b'}{a'}\right)' = 0,$$

so $b = ra + s$ for some constants $r, s \in F$. By (6), we have

$$x_n^3 = u_n = a + nb + (v+n)^3 = a + n(ra+s) + (v+n)^3 = (1+nr)a + ns + (v+n)^3$$

for each $n$; hence, recalling the definition of $a$,

$$x_n^3 = (1+nr)x_0^3 + ns + (v+n)^3 - (1+nr)v^3.$$

Thus, for each $n$ such that $x_n$ is nonconstant (hence for at least 90 distinct values of $n$), the curve

$$Y^3 = (1+nr)X^3 + ns + (v+n)^3 - (1+nr)v^3$$

is a curve over $F$ that admits the parametrization $(X, Y) = (x_0, x_n)$ by nonconstant rational functions, hence is a curve of genus 0. According to Proposition 2.10 this implies that $(1+nr)\big(ns + (\nu+n)^3 - (1+nr)\nu^3\big) = 0$, which cannot happen for more than four values of $n$. This gives us a contradiction.

Now we prove that $\nu$ and $a$ cannot be both constant. Recall that

$$x_1^3 = a + b + (\nu+1)^3,$$

hence

$$b = x_1^3 - a - (\nu+1)^3.$$

Therefore, for each $n$, we have

$$x_n^3 = a + n\big(x_1^3 - a - (\nu+1)^3\big) + (\nu+n)^3 = nx_1^3 + (1-n)a - n(\nu+1)^3 + (\nu+n)^3.$$

If both $\nu$ and $a$ are constant, the curve

$$Y^3 = nX^3 + (1-n)a - n(\nu+1)^3 + (\nu+n)^3$$

is a curve over $F$ that admits the parametrization $(X, Y) = (x_1, x_n)$ by nonconstant rational functions, hence is a curve of genus 0. As in the previous paragraph we conclude that this cannot happen for more than four values of $n$. □

**Lemma 2.12.** *In Case* 2 *of Lemma 2.9 there are two mutually exclusive subcases*:

Case 2.1: *For all n we have* $x_n^3 = (\nu+n)^3$ (*that is, the trivial solution*).

Case 2.2: $q' = 0$.

*Proof.* According to Case 2, we assume that $B \neq 0$ and $\nu' \neq 0$. Observe that if $(x_n)$ is the trivial solution then $a = b = 0$ and $q = -\nu$, hence $q' = -\nu' \neq 0$.

Suppose $q'$ is not zero. By differentiating (8) we get

$$a' + b'q + bq' + 3(\nu' + q')(\nu+q)^2 = 0,$$

and subtracting (9), we obtain $bq' + 3q'(\nu+q)^2 = 0$, that is,

$$b = -3(\nu+q)^2. \tag{15}$$

Recall that

$$q = \frac{(a'/\nu')' + 6\nu\nu'}{-(b'/\nu')' - 6\nu'}.$$

We write $\alpha = a'/\nu'$ and $\beta = b'/\nu'$. We obtain

$$q = -\frac{\alpha' + 6\nu\nu'}{\beta' + 6\nu'},$$

hence

$$-\alpha' = q(\beta' + 6\nu') + 6\nu\nu'. \tag{16}$$

On the other hand, dividing by $\nu'$ in Equation (9) we obtain

$$\alpha + \beta q + 3(\nu + q)^2 = 0$$

which, by differentiating, gives

$$-\alpha' = \beta' q + \beta q' + 6(\nu' + q')(\nu + q),$$

hence

$$-\alpha' = \beta' q + \beta q' + 6(\nu'\nu + \nu' q + q'\nu + q' q).$$

Substituting the expression for $\alpha'$ from Equation (16) we obtain

$$q(\beta' + 6\nu') + 6\nu\nu' = \beta' q + \beta q' + 6(\nu'\nu + \nu' q + q'\nu + q' q);$$

hence, simplifying the $q\beta'$, $\nu\nu'$, and $q\nu'$,

$$0 = \beta q' + 6(q'\nu + q' q),$$

hence

$$\beta = -6(\nu + q),$$

or again

$$b' = -6\nu'(\nu + q).$$

From Equation (15) we obtain

$$b' = -6(\nu' + q')(\nu + q),$$

hence $\nu + q = 0$. Therefore, Equation (15) implies $b = 0$, and Equation (8) implies $a = 0$. By Equation (6), we get

$$u_n = (\nu + n)^3.$$

This proves the lemma. □

**Lemma 2.13.** *Case* 2.2 *of the previous lemma is impossible, that is,* $q' \neq 0$.

*Proof.* By Equations (6) and (8) we have

$$u_n = (n - q)\, b + (\nu + n)^3 - (\nu + q)^3,$$

therefore

$$u_n = (n - q)\, b + 3\nu^2(n - q) + 3\nu(n^2 - q^2) + n^3 - q^3,$$

so, for all $n$ distinct from $q$,

$$\frac{u_n}{n - q} = b + 3\nu^2 + 3\nu(n + q) + n^2 + qn + q^2$$

hence

$$\frac{u_n}{n - q} = b + 3\nu^2 + 3q\nu + q^2 + n(3\nu + q) + n^2.$$

If we write

$$w_n = y_n^3 = \frac{u_n}{n-q}, \quad \alpha = b + 3v^2 + 3qv + q^2, \quad \beta = 3v + q,$$

then we have

$$w_n = \alpha + \beta n + n^2, \tag{17}$$

and, differentiating both sides,

$$w_n' = \alpha' + \beta' n. \tag{18}$$

Multipying (17) by $\beta'^2$ and substituting $\beta' n$ from (18) we get

$$\beta'^2 w_n = \beta'^2 \alpha + \beta' \beta (w_n' - \alpha') + (w_n' - \alpha')^2$$

hence

$$\beta'^2 w_n - \beta' \beta w_n' - w_n'^2 + 2\alpha' w_n' = \beta'^2 \alpha - \beta' \beta \alpha' + \alpha'^2. \tag{19}$$

We intend to apply Lemma 2.7.

For the sake of contradiction, in the rest of the proof we assume that $q$ is constant. So, each $y_n$ is a polynomial of the same degree as $x_n$, and by Corollary 2.5, any four distinct $y_n$ are coprime. Also, we have $\deg \alpha \le 2e$, $\deg \beta \le e$ and $\deg w_n \le e$. Hence, the left-hand side of (19) has degree $\le 3e - 2 = 9d - 2$. Observe that $w_n$ is a cube and is divisible by $x_n^3$. Hence the left-hand side of (19) is divisible by $x_n$. So we can apply Lemma 2.7 and conclude that

$$\beta'^2 \alpha - \beta' \beta \alpha' + \alpha'^2 = 0. \tag{20}$$

Recall that $v' \neq 0$, so $\beta' \neq 0$. Hence (20) can be written as

$$\left(\frac{\alpha'}{\beta'}\right)^2 - \beta \frac{\alpha'}{\beta'} + \alpha = 0.$$

Therefore, for some $\gamma \in F(t)$, we have

$$\beta^2 - 4\alpha = \gamma^2 \tag{21}$$

and

$$\frac{\alpha'}{\beta'} = \tfrac{1}{2}(\beta + \varepsilon\gamma) \tag{22}$$

for some $\varepsilon \in \{-1, 1\}$.

Substituting the value of $\alpha$ from (21) into (22) we obtain

$$\gamma(\beta' + \varepsilon\gamma') = 0. \tag{23}$$

Thus we have two cases, according to whether $\beta' = -\varepsilon\gamma'$ or $\gamma = 0$.

*Case* 2.2.1: We assume $\beta' = -\varepsilon\gamma'$. From Equation (22) we obtain

$$\alpha' = c\beta'$$

for some $c \in F$; substituting this expression for $\alpha'$ in (20) we obtain

$$\alpha = c\beta - c^2.$$

Therefore, by (17),

$$y_n^3 = (n+c)\beta + n^2 - c^2.$$

So, for any indices $m$ and $n$, we have

$$y_m^3 y_n^3 = \big((m+c)\beta + m^2 - c^2\big)\big((n+c)\beta + n^2 - c^2\big),$$

hence

$$\lambda_{m,n}^3 y_m^3 y_n^3 = \beta^2 + \mu_{m,n}\beta + \xi_{m,n} \tag{24}$$

where

$$\lambda_{m,n}^3 = \frac{1}{(m+c)(n+c)}, \quad \mu_{m,n} = \frac{(m+c)(n^2-c^2) + (n+c)(m^2-c^2)}{(m+c)(n+c)}$$

and

$$\xi_{m,n} = \frac{(m^2-c^2)(n^2-c^2)}{(m+c)(n+c)}$$

provided that $(m+c)(n+c) \neq 0$. It is obvious that we can choose $m, n \leq M-1$ so that $(m+c)(n+c)(\mu_{m,n}^2 - 4\xi_{m,n}) \neq 0$. So, by Proposition 2.10, the curve

$$Y^3 = X^2 + \mu_{m,n}X + \xi_{m,n} \tag{25}$$

is of genus 1. But by Equation (24) the latter is a curve over $F$ that admits the parametrization $(X, Y) = (\beta, \lambda_{m,n} y_m y_n)$ by nonconstant rational functions (recall that $\beta \notin F$), hence is a curve of genus 0, a contradiction that proves that Case 2.2.1 is impossible.

*Case* 2.2.2: We assume that $\gamma = 0$. From (21) we obtain $4\alpha = \beta^2$, while (17) becomes

$$4y_n^3 = (\beta + 2n)^2.$$

Hence $y_n$ is a square: $y_n = z_n^2$ for some $z_n \in F[t]$. So we have

$$2z_n^3 = \varepsilon_n(\beta + 2n),$$

where $\varepsilon_n = \pm 1$, and we may assume $\varepsilon_n = 1$ for all $n$ by changing $z_n$ by $-z_n$ if necessary. Hence, for each $m$ and $n$ distinct from $q$, $l_1$ and $l_2$, the curve

$$4X^3 = Y^2 + 2(m+n)Y + 4mn$$

admits the parametrization $(X, Y) = (z_m z_n, \beta)$ by nonconstant rational functions, hence is of genus 0. By Proposition 2.10, we have

$$4(m+n)^2 = 16m^2n^2.$$

As long as $m$ has been chosen, this can happen for at most two choices of $n$. So we get a contradiction and conclude that Case 2.2.2 is impossible. □

*Proof of Theorem 1.2.* By Lemmas 2.9, 2.11, 2.12 and 2.13, the only possible case is Case 2.1 of Lemma 2.12, that is, $x_n^3 = (\nu+n)^3$ for each $n$. □

*Proof of Theorem 1.3.* (a) By Theorem 1.2, the formula

$$\phi(x, z, w)\colon \exists y_0 \ldots \exists y_{91}$$
$$x = y_0 \wedge z = y_1 \wedge w = y_2 \wedge \bigwedge_{n=0}^{91} P_3(y_n) \wedge \bigwedge_{n=0}^{88} y_{n+3} - 3y_{n+2} + 3y_{n+1} - y_n = 6$$

is equivalent over $F[t]$ to:

*Either $x, z, w$ are constant polynomials or $x = \nu^3$ and $z = (\nu+1)^3$ and $w = (\nu+2)^3$ for some $\nu \in F[z]$.*

Therefore, the formula

$$\psi(\nu, u)\colon \exists x \exists z \exists w \;\; \phi(x, z, w) \wedge 6\nu + 6 = (w - z) - (z - x) \wedge z - x = 3u + 3\nu + 1$$

is equivalent over $F[t]$ to:

*Either $\nu, u \in F$ or $u = \nu^2$.*

Both $\phi$ and $\psi$ are formulas in the intersection of the languages $L_{3,t}$ and $L_{3,T}$.

Let us prove that the formula

$$\psi_1(\nu, u)\colon \exists g \exists h \;\; \psi(\nu, u) \wedge \psi(\nu + t, g) \wedge \psi(\nu - t, h) \wedge g + h = 2u + 2t^2$$

is satisfied in $F[t]$ if and only if

$$u = \nu^2.$$

One the one hand, if $u = \nu^2$ then we can choose $g = (\nu+t)^2$ and $h = (\nu-t)^2$. On the other hand, if $\psi_1(\nu, u)$ is satisfied in $F[t]$, then either $u = \nu^2$ and we are done, or $u, \nu \in F$, in which case $\nu + t, \nu - t \notin F$, hence $g = (\nu+t)^2$ and $h = (\nu-t)^2$, hence $2u + 2t^2 = g + h = 2\nu^2 + 2t^2$ implies $u = \nu^2$.

Observe that $\psi_1$ is equivalent to a positive-existential $L_{3,t}$-formula. Similarly, the formula

$$\psi_2(\nu, u)\colon \exists f \;\exists g \;\exists h \;\exists z$$
$$T(f) \wedge \psi(f, z) \wedge \psi(\nu, u) \wedge \psi(\nu + f, g) \wedge \psi(\nu - f, h) \wedge g + h = 2u + 2z$$

is equivalent to

$$u = \nu^2.$$

Observe that $\psi_2$ is equivalent to a positive-existential $L_{3,T}$-formula.

Therefore squaring over $F[t]$ is positive-existentially definable in each of the languages $L_{3,t}$ and $L_{3,T}$, hence so is multiplication (for details see L. Lipshitz [Lipshitz 1990]).

Statements (b) and (c) follow from (a) and the fact that the positive-existential theory of $F[t]$ in the language $\{0, 1, +, \cdot, T\}$ (resp. $\{0, 1, +, \cdot, t\}$) is undecidable [Pheidas and Zahidi 1999; Denef 1978]. □

*Proof of Corollary 1.4.* Any positive-existential $L_{3,T}$-sentence is equivalent to a disjunction of sentences each of which claims the solvability of a system of linear equations with integer coefficients, together with conditions stating that certain of the variables are cubes plus conditions which state that certain linear polynomials of the variables are nonconstant ($\notin F$). Now observe that for any $x$ we have

$$6x + 6 = (x + 2)^3 - 2(x + 1)^3 + x^3.$$

Hence we can substitute each variable $x$, which is not assumed to be necessarily a cube, by the expression

$$\tfrac{1}{6}z_1^3 - \tfrac{1}{3}z_2^3 + \tfrac{1}{6}z_3^3 - \tfrac{1}{6},$$

where the $z_j$ are new variables. Hence any positive-existential $L_{3,T}$-sentence is equivalent to a disjunction of sentences of form as in the Corollary. Consequently, if the satisfiability problem for such sentences were decidable, so would be the decidability problem for positive-existential sentences of $L_{3,T}$, which would contradict Theorem 1.3. □

## References

[Browkin and Brzeziński 2006] J. Browkin and J. Brzeziński, "On sequences of squares with constant second differences", *Canad. Math. Bulletin* **49**:4 (2006), 481–491. MR 2007h:11136 Zbl 05177830

[Buell 1987] D. A. Buell, "Integer squares with constant second difference", *Math. Comp.* **49**:180 (1987), 635–644. MR 88j:11090 Zbl 0627.10009

[Davis 1973] M. Davis, "Hilbert's tenth problem is unsolvable", *Amer. Math. Monthly* **80** (1973), 233–269. MR 47 #6465 Zbl 0277.02008

[Denef 1978] J. Denef, "The Diophantine problem for polynomial rings and fields of rational functions", *Trans. Amer. Math. Soc.* **242** (1978), 391–399. MR 58 #10809 Zbl 0399.10048

[Eisentraeger and Shlapentokh 2007] K. Eisentraeger and A. Shlapentokh, "Undecidability in function fields of positive characteristic", preprint, 2007. arXiv 0709.1739v2

[Hensley 1983] D. Hensley, "Sequences of squares with second difference of two and a conjecture of Büchi", unpublished, 1983.

[Husemöller 2004] D. Husemöller, *Elliptic curves*, 2nd ed., Graduate Texts in Mathematics **111**, Springer, New York, 2004. MR 2005a:11078 Zbl 1040.11043

[Lipshitz 1990] L. Lipshitz, "Quadratic forms, the five square problem, and diophantine equations", pp. 677–680 in *The collected works of J. Richard Büchi*, edited by S. MacLane and D. Siefkes, Springer, Berlin, 1990.

[Matiyasevich 1970] Y. V. Matiyasevich, "Enumerable sets are diophantine", *Dokl. Akad. Nauk SSSR* **19** (1970), 279–282. In Russian; translated in Sov. Math. Dokl. **11** (1970), 354-358. Zbl 0212.33401

[Mazur 1994] B. Mazur, "Questions of decidability and undecidability in number theory", *J. Symbolic Logic* **59**:2 (1994), 353–371. MR 96c:03091 Zbl 0814.11059

[Pasten 2008] H. Pasten, "Extension of Büchi's problem for polynomials", preprint, Departamento de Matemática de la Universidad de Concepción, Chile, 2008.

[Pheidas and Vidaux 2005] T. Pheidas and X. Vidaux, "Extensions of Büchi's problem: questions of decidability for addition and $k$th powers", *Fund. Math.* **185**:2 (2005), 171–194. MR 2006f:03064 Zbl 1079.03005

[Pheidas and Vidaux 2006] T. Pheidas and X. Vidaux, "The analogue of Büchi's problem for rational functions", *J. London Math. Soc.* (2) **74**:3 (2006), 545–565. MR 2007k:03097 Zbl 1109.03032

[Pheidas and Zahidi 1999] T. Pheidas and K. Zahidi, "Undecidable existential theories of polynomial rings and function fields", *Comm. Algebra* **27**:10 (1999), 4993–5010. MR 2000f:03125 Zbl 0934.03014

[Pheidas and Zahidi 2000] T. Pheidas and K. Zahidi, "Undecidability of existential theories of rings and fields: a survey", pp. 49–105 in *Hilbert's tenth problem: relations with arithmetic and algebraic geometry* (Ghent, 1999), edited by J. Denef et al., Contemp. Math. **270**, Amer. Math. Soc., Providence, RI, 2000. MR 2002a:03085 Zbl 0981.03013

[Pinch 1993] R. G. E. Pinch, "Squares in quadratic progression", *Math. Comp.* **60**:202 (1993), 841–845. MR 93h:11029 Zbl 0779.11013

[Poonen 2003] B. Poonen, "Hilbert's Tenth Problem over rings of number-theoretic interest", preprint, 2003, Available at http://math.mit.edu/~poonen/papers/aws2003.pdf.

[Shlapentokh 1992] A. Shlapentokh, "Hilbert's tenth problem for rings of algebraic functions of characteristic 0", *J. Number Theory* **40**:2 (1992), 218–236. MR 94d:11018 Zbl 0746.03008

[Shlapentokh 2000] A. Shlapentokh, "Hilbert's tenth problem over number fields, a survey", pp. 107–137 in *Hilbert's tenth problem: relations with arithmetic and algebraic geometry* (Ghent, 1999), edited by J. Denef et al., Contemp. Math. **270**, Amer. Math. Soc., Providence, RI, 2000. MR 2002a:03085 Zbl 0994.03001

[Shlapentokh 2002] A. Shlapentokh, "On Diophantine definability and decidability in some rings of algebraic functions of characteristic 0", *J. Symbolic Logic* **67**:2 (2002), 759–786. MR 2003d:03070 Zbl 1011.03027

[Shlapentokh 2006] A. Shlapentokh, *Hilbert's tenth problem: diophantine classes and other extensions to global fields*, Cambridge U. Press, Cambridge, 2006. Zbl 05129217

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Vojta 2000] P. Vojta, "Diagonal quadratic forms and Hilbert's tenth problem", pp. 261–274 in *Hilbert's tenth problem: relations with arithmetic and algebraic geometry* (Ghent, 1999), edited by J. Denef et al., Contemp. Math. **270**, Amer. Math. Soc., Providence, RI, 2000. MR 2001k:11260 Zbl 0995.11070

[Zahidi 2000] K. Zahidi, "The existential theory of real hyperelliptic function fields", *J. Algebra* **233**:1 (2000), 65–86. MR 2001i:11150 Zbl 0985.11062

Received January 10, 2008.

THANASES PHEIDAS
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CRETE
71409 HERAKLION
CRETE
GREECE

pheidas@math.uoc.gr
http://www.math.uoc.gr/dept/persons/pheidas.html

XAVIER VIDAUX
UNIVERSIDAD DE CONCEPCIÓN
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE MATEMÁTICA
CASILLA 160C
CONCEPCIÓN
CHILE

xvidaux@udec.cl
http://dmat.cfm.cl/faculty/xvidaux.html