The Analogue of Büchi's Problem for Cubes in Rings of Polynomials

Thanases Pheidas - Xavier Vidaux

Abstract : Let F be a field of zero characteristic. 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 third difference constant and equal to* 6*, is of the form* $(x+n)^3$*,* $n = 0, \ldots, 91$*, for some* $x \in F[t]$ *(cubes of successive elements).* We use this, in conjunction to the negative answer to the analogue of Hilbert's Tenth Problem for $F[t]$ in order to show that the solvability of systems of degree-one equations, where some of the variables are assumed to be cubes and (or) non-constant, is an unsolvable problem over $F[t]$.
MSC: 03C60, 12L05, 11U05, 11C08

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 second difference constant and equal to* 2*, is equal to a sequence of squares of successive integers?*

He had the intention to apply a possible positive answer in order to obtain a result in Mathematical Logic (we discuss this below). The question was made public by L. Lipshitz in [7]. In [19] P. Vojta proved that a positive answer - 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 proved that the similar question for non-constant meromorphic functions (defined on $\mathbb{C}$), rather than integers, has a positive answer. A relevant discussion can be found in a work of B. Mazur [9]. The n squares problem is still open.

In 1987 D. Buell [2] characterized all the non-trivial integer sequences of length four (we call a sequence of squares of successive numbers *trivial*). In 1993, R. G. E. Pinch [14] proved, under a certain condition on the size, that a family of four-term sequences cannot be extended to five-term sequences. In 2006, J. Browkin and J. Brzeziński [1] proved that there exist infinitely many non-trivial five- and six-term sequences (originally, Büchi asked the question for five-term sequences). It is not known whether or not there exist any non-trivial seven-term sequence of integers. Note that

Vojta's conditional result claims non-existence of eight-term non-trivial sequences of integers.

In [10] we generalized Büchi's question as follows:

Question 1.1 *Let k be an integer, greater than 1. Is there a positive integer M so that the following holds?*

Assume that $y = (y_0, \ldots, y_{M-1})$ is a sequence of k-th powers of integers. If the k-th difference of y is constant and equal to $k!$, then y is the sequence of k-th powers of successive integers, that is, there is an integer x so that, for each $n \in \{0, \ldots, M-1\}$, we have $y_n = (x+n)^k$.

Except for the above results of Vojta and those of [11] the question is open for any k and for any global field (in place of the integers) - we note that in fields of functions the Question should be interpreted so that by 'solutions' one means solutions which are non-constant 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 $x_0, \ldots, x_{M-1} \in F[t]$, at least one of the x_n is non-constant 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, or equivalently, if the following system of equations is satisfied*

$$x_{n+3}^3 - 3x_{n+2}^3 + 3x_{n+1}^3 - x_n^3 = 6, \qquad n = 0, \ldots, M-4 \qquad (1)$$

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

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

A consequence in Logic is the following:

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 non-constant 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).*

1. *Multiplication in $F[t]$ is positive-existentially definable in each of the languages $L_{3,T}$ and $L_{3,t}$.*
2. *The positive-existential theory of $F[t]$ in the language $L_{3,T}$ is undecidable.*
3. *The positive-existential theory of $F[t]$ in the language $L_{3,t}$ is undecidable.*

This strengthens the result of J. Denef in [4] which is an analogue of Hilbert's Tenth Problem for rings of polynomials of the variable t, in the language $\{+, \cdot, 0, 1, t\}$ (cf. Y. Matiyasevic [8], the presentation of M. Davis in [3] and the surveys by the first author and K. Zahidi in [13], by B. Poonen in [15] and by A. Shlapentokh in [17]). It also strengthens the similar result of the first author and K. Zahidi in [12], but in the language $\{+, \cdot,$ 'x is non-constant' $, 0, 1\}$.

An immediate consequence of Theorem 1.3 is the following:

Corollary 1.4 (Undecidability of simultaneous representation by cubic forms) *There is no algorithm (i.e. Turing Machine) which 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 $f_j(Y_1, \ldots Y_r)$ are polynomials of the variables $Y_1, \ldots Y_n$ of degree 1, for $j = 1, \ldots, r$. 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 is non-constant'. But for the moment we can not 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 'non-constancy') 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: We consider it natural to ask about the truth of the statements of Theorem 1.2 and 1.3 for domains other than polynomials. Some examples are:

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

2. A polynomial ring $F[t]$ in any characteristic other than 3;

3. The ring of algebraic functions of the variable t, integral over $F[t]$ (this would strengthen the result of A. Shlapentokh [16]);

4. Fields of rational functions in any characteristic other than 3;

5. Fields of algebraic functions in any characteristic other than 3 (this would strengthen, for example, the result of K. Zahidi [20]);

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

Outline of the proof: We compute an invariant ν 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 2.8 and 2.10). In this way we obtain a dependence of a on b and ν. Iterating the procedure we obtain b as a function of ν. In consequence the pairs of non-trivial solutions (x_m, x_n) are shown to be on certain curves over F, of genus greater than 0, which is impossible for non-constant 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 $k > 3$ (k is 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.

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 of Equations (1) and write $u_n = x_n^3$, so that we have

$$u_{n+3} - 3u_{n+2} + 3u_{n+1} - u_n = 6 \tag{2}$$

for $n = 0, \ldots, M-4$.

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

Without loss of generality we can suppose that the field F is algebraically closed. Hence we suppose from now on:

Assumption 2.1
(a) The field F is algebraically closed.
(b) The characteristic of F is 0.
(c) At least one x_n is not in F.

Lemma 2.2 *The system of Equations (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: By induction on n. It is clearly true for $n = 3$. Suppose it is true up to n. By Equation (1) we have

$$u_{n+1} = 3u_n - 3u_{n-1} + u_{n-2} + 6$$

where we may replace u_n, u_{n-1} and u_{n-2} using the hypothesis of induction. We obtain

$$\begin{aligned}
2u_{n+1} &= 6u_n - 6u_{n-1} + 2u_{n-2} + 12 \\
&= 3\,[n(n-1)u_2 - 2n(n-2)u_1 + (n-2)(n-1)u_0 + 2(n-2)(n-1)n] \\
&-3\,[(n-1)(n-2)u_2 - 2(n-1)(n-3)u_1 + (n-3)(n-2)u_0 + 2(n-3)(n-2)(n-1)] \\
&+[(n-2)(n-3)u_2 - 2(n-2)(n-4)u_1 + (n-4)(n-3)u_0 + 2(n-4)(n-3)(n-2)] + 12
\end{aligned}$$

hence the coefficient of u_2 is

$$3n(n-1) - 3(n-1)(n-2) + (n-2)(n-3) = n^2 + n = n(n+1)$$

the coefficient of $2u_1$ is

$$-3n(n-2) + 3(n-1)(n-3) - (n-2)(n-4) = -n^2 + 1 = -(n+1)(n-1)$$

the coefficient of u_0 is

$$3(n-2)(n-1) - 3(n-3)(n-2) + (n-4)(n-3) = n^2 - n = (n-1)n$$

and the constant term is

$$\begin{aligned}
&6(n-2)(n-1)n - 6(n-3)(n-2)(n-1) + 2(n-4)(n-3)(n-2) + 12 \\
&= 2(n-2)[3(n-1)n - 3(n-3)(n-1) + (n-4)(n-3)] + 12 \\
&= 2(n-2)[n^2 + 2n + 3] + 12 = 2[n^3 - n - 6] + 12 = 2[n^3 - n] = 2n(n-1)(n+1)\ .
\end{aligned}$$

Hence Equation (3) is true up to $n + 1$. The more general relation can be obtained by brute computation, and is left to the reader. ◇

Lemma 2.3 *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 ν instead of $\nu_{m,n,q}$. We will call ν the *ν-invariant of the sequence u*. Observe that since we have

$$3\nu = \frac{1}{2}[u_2 - 2u_1 + u_0 - 6]$$

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

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

We find

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

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

Definition 2.4 *For any $x \in F[t] \setminus \{0\}$, $\deg(x)$ will denote the degree of x. We adopt the convention that $\deg(0) = -\infty$. 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 then we write $d = \frac{e}{3}$. In the case we consider $u_n = x_n^3$, hence $d = \frac{e}{3}$ is the maximum of the degrees of the x_n.*

Corollary 2.5 *One of the following is true:*

1. *Each u_n has degree e.*
2. *There is an index ℓ such that for each $n \neq \ell$ we have $\deg(u_n) = e$ and $\deg(u_\ell) < e$.*
3. *There are indices $\ell_1 \neq \ell_2$ such that for each $n \neq \ell_i$, $i = 1, 2$, we have $\deg(u_n) = e$ and $\deg(u_{\ell_i}) < e$, $i = 1, 2$.*

Proof: Assume we are not in cases 1 or 2. Let $\ell_1 \neq \ell_2$ such that $\deg(u_{\ell_i}) < e$ and let k be an index such that $\deg(u_k) = e$. By Lemma 2.3 we have

$$3\nu = \nu_{k,\ell_1,\ell_2} = -\frac{(\ell_2 - \ell_1)u_k + (k - \ell_2)u_{\ell_1} + (\ell_1 - k)u_{\ell_2}}{(\ell_2 - \ell_1)(k - \ell_2)(\ell_1 - k)} - k - \ell_1 - \ell_2$$

hence $\deg(\nu) = \deg(u_k) = e$. So for any index $n \neq \ell_1, \ell_2$ we have

$$3\nu = -\frac{(\ell_2 - \ell_1)u_n + (n - \ell_2)u_{\ell_1} + (\ell_1 - n)u_{\ell_2}}{(\ell_2 - \ell_1)(n - \ell_2)(\ell_1 - n)} - n - \ell_1 - \ell_2 \ ,$$

which implies $\deg(u_n) = \deg(\nu) = e$. ◇

Corollary 2.6 *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

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

Suppose that there is a non-constant 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. $\diamond$

Definition 2.7 Recalling Corollary 2.5, we let ℓ_i, $i = 1, 2$, be two indices such that for each index n, other than ℓ_1 and ℓ_2, we have

$$\deg(u_{\ell_i}) \leq \deg(u_n) = e$$

for $i = 1, 2$.

Lemma 2.8 *Let $\{r_1, \ldots, r_m\} \subseteq \{0, \ldots, M-1\}$. If Q is a non-zero polynomial in $F[t]$ divisible by $\prod_{k=1}^{m} x_{r_k}$, then the degree of Q is at least $\frac{m-2}{3}d$. In particular, if we choose $M \geq 92$ and $m = M$ then the degree of Q is at least $30d$.*

Proof: Denote $R = \{r_1, \ldots, r_m\}$. 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 μ for the least common multiple of the elements of the set $\{x_n \mid n \in R\}$. Hence μ divides Q and it is enough to show that the degree of μ is at least $\frac{m-2}{3}d$.

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

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

If P does not divide any x_n, then 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, namely, so that

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

By Corollary 2.5, P divides either precisely one x_n (Case 1), or precisely two (Case 2), or precisely three (Case 3). Let x_{k_i}, $i = 1, \ldots, j$, be the polynomials divisible by P in case j. In order to treat the three cases simultanously, 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

$$\mathrm{ord}_P(x_{k_1}) \geq \mathrm{ord}_P(x_{k_2}) \geq \mathrm{ord}_P(x_{k_3})$$

then we have

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

This proves the claim.

Hence we have

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

and by Corollary 2.5 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 2.7. $\diamond$

Notation 2.9 *We write*

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

and if $B \neq 0$

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

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

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

Lemma 2.10 *Only the following mutually exclusive two cases can occur:*
Case 1: $\nu' = 0$
Case 2: $B \neq 0$, $\nu' \neq 0$ *and we have*

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

and

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

Proof: By differentiating twice the sides of Equation (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 the expresion for $3(\nu + n)^2$ that results from Equation (11) into Equation (10) we obtain

$$\nu'' u_n' = \nu'' a' + n\nu'' b' + \nu'(u_n'' - a'' - nb'' - 6\nu'^2(\nu + n))$$

that we can write in the form

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

where

$$U_n = \nu'' u_n' - \nu' u_n''.$$

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

$$B^3 u_n = aB^3 + nbB^3 + (\nu B + nB)^3$$

and

$$B^2 u_n' = a'B^2 + nb'B^2 + 3\nu'(\nu B + nB)^2$$

hence, replacing the expresion of nB from Equation (12),

$$B^3 u_n = aB^3 + (A + U_n)bB^2 + (\nu B + A + U_n)^3$$

and

$$B^2 u_n' = a'B^2 + (A + U_n)b'B + 3\nu'(\nu B + A + U_n)^2.$$

Separating the terms that depend on n from those that do not, in both equations, we get

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

and

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

Write

$$\Delta = aB^3 + AbB^2 + (\nu B + A)^3$$

and

$$\Gamma = a'B^2 + Ab'B + 3\nu'(\nu B + A)^2$$

(the right hand sides of the above equations).

We will now use Lemma 2.8 in order to prove that we have $\Delta = \Gamma = 0$. Note that 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, Δ and Γ are both multiples of x_n for each $n \in \{0, \ldots, M-1\}$. Let us compute an upper bound for the degrees of Δ and Γ. Recalling Definition 2.7 we see that the degree of u_n is not more than e, hence that of ν is not more than e and we have $\deg(a) \leq 3e$, $\deg(b) \leq 2e$, and

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

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

$$\deg(\Delta) \leq 10e - 9 = 30d - 9 < 30d$$

and

$$\deg(\Gamma) \leq 7e - 7 = 21d - 7 < 30d \ .$$

We deduce from Lemma 2.8 that we have $\Delta = 0$ and $\Gamma = 0$.

If B is not zero then ν' is not zero and we have

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

and

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

namely Equations (8) and (9).

Let us prove that if $B = 0$ then $\nu' = 0$. If $B = 0$ then from Equation (12) we have $A + U_n = 0$ for all n. Since U_n is a multiple of x_n, and $\deg U_n \leq 2e - 3 = 6d - 3$, we deduce from Lemma 2.8 that U_n is zero. From Corollary 2.5, 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 $\frac{\nu'}{u_n'}$ 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 2.8 : since

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

we have $\nu' = 0$. $\diamond$

We will need the following Proposition, whose proof comes from the theory of elliptic curves (see, for example, Husemöller [5], Definition (6.2), page 17, or Silverman [18], Hurwitz's Theorem, Ch. II, par. 5) - the main observation that concerns us here is that a non-singular cubic curve is of genus 1.

Proposition 2.11 *Let $\mu, \xi \in F$.*

1. *The curve with affine equation*

$$Y^3 = \mu X^3 + \xi$$

is of genus 1 provided that $\mu\xi \neq 0$.

2. The curve with affine equation

$$Y^2 + \mu Y + \xi = X^3$$

is of 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 ν that will produce equations that will define curves as in Proposition 2.11, where the coeficients μ and ξ 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 (and some other fixed polynomial, independent of n), hence they will define curves of genus 0 (for all the indices considered). Proposition 2.11 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 non-constant, 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 $x_n^3 = (\nu + n)^3$, which will prove Theorem 1.2. $\diamond$

Lemma 2.12 *Case 1 is impossible, that is,* ν' *can not be zero.*

Proof : We will show first that if ν is constant then so is a, and then that ν and a can not be both constant.

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

$$u_n' = a' + nb' \qquad \text{and} \qquad u_n'' = a'' + nb''$$

(from Equation 6). Hence we have

$$u_n' b'' = a'b'' + nb''b' = a'b'' + (u_n'' - a'')b' \ ,$$

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 $3e - 3$, then by Lemma 2.8, we deduce

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

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

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

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

$$\begin{aligned} x_n^3 &= u_n \\ &= a + nb + (\nu + n)^3 \\ &= a + n(ra + s) + (\nu + n)^3 \\ &= (1 + nr)a + ns + (\nu + n)^3 \end{aligned}$$

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

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

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

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

is a curve over F that admits the parametrization $(X,Y) = (x_0, x_n)$ by non-constant rational functions, hence is a curve of genus 0. According to Proposition 2.11 this implies that $(1+nr)[ns + (\nu+n)^3 - (1+nr)\nu^3] = 0$, which can not happen for more than four values of n. This gives us a contradiction.

Now we prove that ν and a can not 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

$$\begin{aligned} x_n^3 &= a + n[x_1^3 - a - (\nu+1)^3] + (\nu+n)^3 \\ &= nx_1^3 + (1-n)a - n(\nu+1)^3 + (\nu+n)^3 \ . \end{aligned}$$

If both ν and a are constant then 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 non-constant rational functions, hence is a curve of genus 0. Similarly to the previous paragraph we conclude that this can not happen for more than four values of n. $\diamond$

Lemma 2.13 *In Case 2 of Lemma 2.10 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); or*
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 Equation (8), we get

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

and subtracting (9), we obtain

$$bq' + 3q'(\nu+q)^2 = 0.$$

We have

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

Recall that

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

We write $\alpha = \frac{a'}{\nu'}$ and $\beta = \frac{b'}{\nu'}$. 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 ν' 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 α' 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

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

hence

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

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 2.14 *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

$$w_n = y_n^3 = \frac{u_n}{n-q}, \qquad \alpha = b + 3\nu^2 + 3q\nu + q^2 \qquad \text{and} \qquad \beta = 3\nu + q \ ,$$

then we have

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

and, taking derivatives of both sides:

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

Multipying the sides of Equation (17) by β'^2 and then substituting $\beta' n$ by the value resulting from Equation (18) we get

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

hence

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

We intend to apply Lemma 2.8.

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 2.6, any four distinct y_n are coprime. Also, we have $\deg(\alpha) \leq 2e$, $\deg(\beta) \leq e$ and $\deg(w_n) \leq e$. Hence, the degree of the left-hand side of Equation (19) has degree $\leq 3e - 2 = 9d - 2$. 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 2.8 and conclude that

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

Recall that we have $\nu' \neq 0$, so $\beta' \neq 0$. So Equation (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

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

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

Substituting the value of α from Equation (21) into Equation (22) we obtain

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

So 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 $\frac{\alpha'}{\beta'}$ by c 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

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

hence

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

where

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

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

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 2.11, 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 non-constant 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 Equation (21) we obtain

$$4\alpha = \beta^2$$

and Equation (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

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

where $\varepsilon = \pm 1$. 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 non-constant rational functions, hence is of genus 0. By Proposition 2.11, 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. $\diamond$

Proof of Theorem 1.2: By Lemmas 2.10, 2.12, 2.13 and 2.14, the only possible case is Case 2.1 (Lemma 2.13), that is, $x_n^3 = (\nu + n)^3$ for each n. $\diamond$

Proof of Theorem 1.3: Statement (1). By Theorem 1.2, the formula

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

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

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

is equivalent over $F[t]$ to :

$$\text{`Either } \nu, u \in F \text{ or } u = \nu^2.$$

Note that both ϕ and ψ are formulas in the intersection of the languages $L_{3,t}$ and $L_{3,T}$.

Let us prove that the formula

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

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 ψ_1 is equivalent to a positive-existential $L_{3,t}$-formula. Similarly, the formula

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

is equivalent to

$$u = \nu^2 \ .$$

Observe that ψ_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 [7]).

Statements (2) and (3) follow from (1) 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 (see the first author and K. Zahidi [12], and J. Denef [4]). $\diamond$

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 non-constant ($\notin F$). 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 $\frac{1}{6}z_1^3 - \frac{1}{3}z_2^3 + \frac{1}{6}z_3^3 - \frac{1}{6}$, 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. $\diamond$

References

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

[2] D. A. Buell, *Integer Squares with Constant Second Difference*, Mathematics of Computation, **49**, no. 180, 635-644 (1987).

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

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

[5] D. Husemöller, *Elliptic curves, second edition*, Springer, Graduate Texts in Mathematics **111** (2004).

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

[7] 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).

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

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

[10] 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).

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

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

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

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

[15] B. Poonen, *Hilbert's Tenth Problem over rings of number-theoretic interest*, survey downloadable from: **http://math.berkeley.edu/∼poonen/**

[16] A. Shlapentokh, *Hilbert's Tenth Problem of algebraic functions of characteristic 0*, Journal of Number Theory, **40-2**, 218-236 (1992).

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

[18] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, Graduate Texts in Mathematics **106** (1986).

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

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