Extensions of Büchi's problem : Questions of decidability for addition and k-th powers

Thanases PHEIDAS
Xavier VIDAUX

Fundamenta Mathematicae, vol. 185, pp. 171-194 (2005)

The authors thank the referee for his comments.

The second author aknowledges the hospitality of the University of Crete-Heraklion, where the main part of this work was done.

Abstract. We generalize a question of Büchi : Let R be an integral domain, C a subring and $k \geq 2$ an integer. Is there an algorithm to decide the solvability in R of any given system of polynomial equations, each of which is linear in the $k-$th powers of the unknowns, with coefficients in C?

We state a number-theoretical problem, depending on k, a positive answer to which would imply a negative answer to the question for $R = C = \mathbb{Z}$.

We reduce a negative answer for $k = 2$ and for $R = F(t)$, a field of rational functions of zero characteristic, to the undecidability of the ring theory of $F(t)$.

We address the similar question, where we allow, along with the equations, also conditions of the form 'x is a constant' and 'x takes the value 0 at $t = 0$', for $k = 3$ and for function fields $R = F(t)$ of zero characteristic, with $C = \mathbb{Z}[t]$. We prove that a negative answer to this question would follow from a negative answer for a ring between $\mathbb{Z}$ and the extension of $\mathbb{Z}$ by a primitive cube root of 1.

AMS Subject Classification: 03C60; 12L05

1 Introduction

Given any $k = 2, 3, \ldots$, we will call *Büchi's question for k* (for short $\mathbf{Bq}(k)$) the following

Question 1.1 *($\mathbf{Bq}(k)$) Does there exist an algorithm to determine, given $m, n \in \mathbb{N}$, $A = (a_{i,j})_{i,j} \in \mathcal{M}_{m,n}(\mathbb{Z})$ and $B = (b_i) \in \mathcal{M}_{m,1}(\mathbb{Z})$, whether there exist $x_1, ..., x_n \in \mathbb{Z}$ satisfying the equations*

$$\sum_{j=1}^{n} a_{i,j} x_j^k = b_i, \qquad i = 1, \ldots, m?$$

(where $\mathcal{M}_{m,r}(\mathbb{Z})$ is the set of $n \times r$ matrices with entries in $\mathbb{Z}$)

J. Richard Büchi asked the question for $k = 2$ and this was made public by L. Lipshitz in [9]. The problem was investigated by Joseph Lipman and Barry Mazur (cf. [11]). Paul Vojta in [19] proved that a conjecture of Serge Lang implies a negative answer to it (we discuss this in Section 2).

It is obvious that, for any k, a negative answer to $\mathbf{Bq}(k)$ would be a strong form of a negative answer to Hilbert's Tenth Problem (cf. [10] and [1]). In this paper,:

- We show that for each odd $k \geq 3$ a negative answer to $\mathbf{Bq}(k)$ would follow from a positive answer to a number theoretical problem (Problem 2.2) - the similar problem for $k = 2$ was asked by Büchi. This is Theorem 2.4.

- We generalize Question $\mathbf{Bq}(k)$ to any commutative ring R and for any subring C of allowed coefficients of equations (in this Section, below).

- We show, using results of Vojta, that for $k = 2$ the generalized problem for $R = F(t)$, a field of rational functions in the variable t with coefficients in a field F of zero characteristic, and for $C = \mathbb{Z}[t]$ has a negative answer if the existential ring-theory of $F(t)$ in the language of rings augmented by t is undecidable. These results are stated in Theorem 1.4 and Corollary 1.5 and their proofs are given in Section 3.

- We show that a question similar to 1.1 for $k = 3$, for fields of rational functions of zero characteristic, will have a negative answer if $\mathbf{Bq}(3)$

has a negative answer. The results are stated in Theorem 1.6. and Corollary 1.7 and proved in Sections 4 and 5.

We generalize $\mathbf{Bq}(k)$ to arbitrary integral domains as follows: Assume that R is a commutative ring with a multiplicative identity, C is a finitely generated subring of R, $k \in \mathbb{Z}$ and $k \geq 2$.

Question 1.2 *($\mathbf{Bq}(k, R, C)$) Does there exist an algorithm to determine, given $m, n \in \mathbb{N}$, $A = (a_{i,j})_{i,j} \in \mathcal{M}_{m,n}(C)$, $B = (b_i) \in \mathcal{M}_{m,1}(C)$ and a subset $J \subset \{1, \ldots, n\}$, whether there exist $x_1, \ldots, x_n \in R$ satisfying the equations*

$$\sum_{j=1}^{n} a_{i,j} x_j = b_i, \qquad i = 1, \ldots, m$$

and subject to the conditions*: for $j \in J$, $x_j \in \{y^k : y \in R\}$? ($\mathcal{M}_{m,r}(C)$ is the set of $n \times r$ matrices with entries in C)*

If $R = \mathbb{Z}$, it is trivial to see, using linear elimination, that $\mathbf{Bq}(k, \mathbb{Z}, \mathbb{Z})$ is equivalent to $\mathbf{Bq}(k)$.

We state Question 1.2 in the terminology of Logic. For each $k \in \mathbb{N}$ we let $L_{k,C}$ denote the *language* which consists of the following symbols: (a) symbols for the elements of the ring C, (b) the symbol $+$ for addition, (c) the predicate-symbol P_k for the relation 'x is a k-th power', so $P_k(x) \leftrightarrow \exists y \in R[x = y^k]$, (d) for each $c \in C$, a symbol for the function of multiplication by c: $x \to cx$. We adopt the convention that we will interpret always these symbols in the stated way. Obviously, a *positive-quantifier-free* formula of $L_{k,C}$ is a disjunction of systems of linear equations of the type occurring in Question 1.2, together with conditions of the form $P_k(x_i)$. A *positive-existential formula* of $L_{k,C}$ is a formula of the form $\exists y \phi(x, y)$ where ϕ is a positive-quantifier-free formula of $L_{k,C}$ (x and y are tuples of variables ranging in R). A subset of a power of R that can be defined by a positive-existential formula is said to be *positive-existentially definable*. Since the quantifier $\exists$ distributes over $\vee$ (the conjunction *or*) it is easy to see that finite unions and finite intersections of positive-existential sets are positive-existential. The *positive-existential theory* of R in the language $L_{k,R}$ is the set of all positive-existential formulas of $L_{k,C}$ which are true over R. It is trivial to see that Question 1.2 is equivalent to the following

Question 1.2(b): *Is the positive-existential theory of R in the language $L_{k,C}$ decidable?*

We will deal with the case in which $R = F(t)$ is a field of rational functions in the variable t, with coefficients in the field F. We will assume throughout that F has characteristic zero, so that $\mathbb{Z}$ can be thought to be a subring of F. Then Question 1.2 for $R = F(t)$ and for $C = \mathbb{Z}[t]$ becomes

Question 1.3 *Is the positive existential theory of $F(t)$ in the language $L_{k,\mathbb{Z}[t]}$ decidable?*

In Section 3 we will show that for $k = 2$ a negative answer to Question 1.3 follows from [19] for all fields F such that the positive-existential ring-theory of $F(t)$, in the language of rings augmented by a symbol for t, is undecidable. Such is the case, for example for $F = \mathbb{R}$, the field of reals (see [3]), so $\mathbf{Bq}(2, \mathbb{R}(t), \mathbb{Z}[t])$ has a negative answer. We remark that it is unknown whether the ring-theory of $\mathbb{C}(t)$ is undecidable ($\mathbb{C}$ is the field of complex numbers). More accurately, we prove:

Theorem 1.4 *Let F be a field of zero characteristic and let t be a variable. Then multiplication in $F(t)$ is positive-existentially definable in $L_{2,\mathbb{Z}[t]}$. Consequently, if the existential ring theory of $F(t)$ in the language of rings augmented by a symbol for t is undecidable, then the positive-existential $L_{2,\mathbb{Z}[t]}$-theory of $F(t)$ is undecidable.*

By [3] we obtain:

Corollary 1.5 *(a) Assume that F is a real-closed field. Then the subset $\mathbb{Z}$ of $F(t)$ is positive-existentially definable in the language $L_{2,\mathbb{Z}[t]}$ and the positive-existential theory of $F(t)$ in the language $L_{2,\mathbb{Z}[t]}$ is undecidable.*

(b) Assume that F is a real field. Then the positive-existential theory of $F(t)$ in the language $L_{2,\mathbb{Z}[t]}$ is undecidable.

We think it likely that our proof of Theorem 1.4 can be adjusted to any function field of an elliptic curve over F in the place of $F(t)$.

For $k \geq 3$ essentially nothing is known on $\mathbf{Bq}(k, R, C)$. Our guess is that in some cases, at least, if the positive-existential ring-theory of R with constants from C is undecidable then the positive-existential $L_{k,C}$-theory of R is undecidable. Our next result is in this direction. In Section 5 we will answer a question similar to Question 1.3, for $k = 3$, allowing additional conditions such as '$x \in F$' and '$x(0) = 0$', in the case that R is a field of rational functions $F(t)$ in the variable t, with coefficients in the field F, and for $C = \mathbb{Z}[t]$.

We introduce the necessary terminology. Let $L_{k,\mathbb{Z}[t],\mathrm{Con,ord}}$ be the augmentation of $L_{k,\mathbb{Z}[t]}$ by the predicate 'Con' which is interpreted as

$$\mathrm{Con}(x) \leftrightarrow x \in F$$

and by the predicate 'ord' which is interpreted as

$$\mathrm{ord}(x) \leftrightarrow x(0) = 0$$

(the value of the rational function x at $t = 0$ is 0). The languages $L_{k,\mathbb{Z}[t],\mathrm{Con}}$ and $L_{k,\mathbb{Z}[t],\mathrm{ord}}$ are the restrictions of $L_{k,\mathbb{Z}[t],\mathrm{Con,ord}}$ by deleting the obvious predicate symbols.

We prove:

Theorem 1.6 *Let F be a field of zero characteristic, let t be a variable and let ξ be a primitive cube root of 1 in an extension of F. Then*

(a) The subset $\mathbb{Z}[\xi] \cap F$ of $F(t)$ is positive-existentially definable in the language $L_{3,\mathbb{Z}[t],\mathrm{Con,ord}}$. Consequently if $\mathbf{Bq}(3,\mathbb{Z}[\xi] \cap F, \mathbb{Z})$ has a negative answer (for example, if $\mathbb{Z}[\xi] \cap F = \mathbb{Z}$ and $\mathbf{Bq}(3)$ has a negative answer) then the positive-existential theory of $F(t)$ in the language $L_{3,\mathbb{Z}[t],\mathrm{Con,ord}}$ is undecidable.

(b) Assume that for some $a, b \in \mathbb{Z}$, with $ab \neq 0$, F has a subset D such that for all $n \in \mathbb{Z}[\xi] \cap F$ there is a $d \in D$ such that $an^3 + bd^3 = 1$. Then the subset $\mathbb{Z}[\xi] \cap F$ of $F(t)$ is positive-existentially definable in the language $L_{3,\mathbb{Z}[t],\mathrm{ord}}$. Hence if $\mathbf{Bq}(3, \mathbb{Z}[\xi] \cap F, \mathbb{Z})$ has a negative answer then the positive-existential theory of $F(t)$ in the language $L_{3,\mathbb{Z}[t],\mathrm{ord}}$ is undecidable.

The next Corollary provides some examples where the hypothesis of (b) of the Theorem holds.

Corollary 1.7 *(a) Assume that F is a field containing the set of algebraic numbers (over $\mathbb{Q}$). Then the subset $\mathbb{Z}[\xi]$ of $F(t)$ is positive-existentially definable in the language $L_{3,\mathbb{Z}[t],\mathrm{ord}}$. Hence if $\mathbf{Bq}(3, \mathbb{Z}[\xi], \mathbb{Z})$ has a negative answer then the positive-existential theory of $F(t)$ in the language $L_{3,\mathbb{Z}[t],\mathrm{ord}}$ is undecidable.*

(b) Assume that F is a real-closed field. Then the subset $\mathbb{Z}$ of $F(t)$ is positive-existentially definable in the language $L_{3,\mathbb{Z}[t],\mathrm{ord}}$. Hence if $\mathbf{Bq}(3)$ has a negative answer then the positive-existential theory of $F(t)$ in the language $L_{3,\mathbb{Z}[t],\mathrm{ord}}$ is undecidable.

In particular, if $\mathbf{Bq}(3)$ has a negative answer then the positive-existential theories of $\mathbb{Q}(t)$ and $\mathbb{R}(t)$ in the language $L_{3,\mathbb{Z}[t],\mathrm{ord}}$ are undecidable.

Both statements are easy consequences of Theorem 1.6: The proof of (a) is obvious; The proof of (b) follows from Theorem 1.6(b) by taking $a = 1 = -b$.

We present an outline of the proof of Theorem 1.6 in Section 4 and the complete proof in Section 5.

It is obvious that $\mathbf{Bq}(k, R, C)$ is a sub-problem of the decidability problem for the positive-existential theory of R with constant symbols for the elements of C (sometimes called "diophantine problem for (R, C)"). Let L_t be the language of rings, augmented by the constant-symbol t. Undecidability is known for the positive-existential theories in L_t of fields of rational functions $F(t)$ in the cases that F is a real field or a finite field (see [3], [12] and [18]). Open is the problem of the existence of an algebraically closed field F for which the diophantine problem for $(F(t), \mathbb{Z}[t])$ is undecidable. But it is known that the positive-existential theory of any field $F(t)$ in the extension of L_t by a predicate for the elements of F and a predicate for 'ord(x)' is undecidable (cf. [22]). The question whether these predicates are positive-existentially definable in L_t is open, but in special cases such as for F equal to the field of real numbers and for F equal to a finite field. This is the motivation behind our choice to extend the languages $L_{k,\mathbb{Z}[t]}$ by the predicates Con and ord.

For more undecidability results and questions in this direction the reader may consult [6], [15], [21] and the surveys in [13] and [16].

We remark that the method of proof of Theorem 1.6 does not give a positive-existential definition of multiplication in $L_{3,\mathbb{Z}[t],\mathrm{Con,ord}}$. Also the method does not generalize to values of k greater than 3.

In Section 2 we present a number theoretical problem, Problem 2.2 which, if answered positively, will imply a negative answer to $\mathbf{Bq}(k)$. It is a generalization of the "n squares problem" (or *Büchi's problem*) of [9], [11] and [19]. Our motivation for presenting it is that if one thinks that it is plausible, then one will consider the undecidability statement of Theorem 1.6 at least as likely.

Throughout $\mathbb{N}$ is the set of natural numbers $\{1, 2, \dots\}$ and $\mathbb{Z}$ the set of rational integers.

2 The "n $k-$th powers problem"

Definition 2.1 *Let $y = (y_i)_{i=0,\dots,n-1}$ be a sequence of complex numbers. We call the* difference sequence of y *the sequence $\Delta(y) = (\Delta(y)(i))_{i=0,\dots,n-2}$*

defined by $\Delta(y)(i) = y_{i+1} - y_i$. *The* ℓ*-th difference of* y*, denoted*

$$\Delta^{(\ell)}(y) = (\Delta^{(\ell)}(y)(i))_{i=0,\ldots,n-\ell-1}$$

is defined recursively by $\Delta^{(1)}(y) = \Delta(y)$ *and* $\Delta^{(\ell+1)}(y) = \Delta(\Delta^{(\ell)}(y))$.

Let $k \in \mathbb{Z}$, $k \geq 2$. Let R be any integral domain of characteristic zero. It is easy to see that for any $x \in R$, the ℓ-th difference

$$\Delta^{(\ell)}((x+i)^k_{i=0,\ldots,n-1})$$

for $\ell \leq k$, is a sequence of the form

$$(p_{\ell,k}(x), p_{\ell,k}(x+1), \ldots, p_{\ell,k}(x+n-\ell-1)$$

where $p_{\ell,k}(x)$ is a polynomial in x, of degree $k-\ell$, with integer coefficients which depend on k and ℓ. Observe that $p_{k,k}(x) = k!$.

We formulate the 'n $k-$**th powers problem**' (or '**Büchi's problem for** k').

Problem 2.2 *Let* k *be a rational integer with* $k \geq 2$.

(i) Is there a natural number $n \geq k$ *such that any sequence of natural numbers* $(x_i)_{i=0,\ldots,n-1}$ *which satisfies*

(2.2.1) $$\Delta^{(k)}((x_i^k)_{i=0,\ldots,n-1}) = (k!)$$

(the sequence with $n-k$ *terms, each equal to* $k!$*) is necessarily a sequence of successive numbers (that is, either for each* i*,* $x_i = x_0 + i$ *or, for each* i*,* $x_i = x_0 - i$*)?*

(ii) Is there a natural number $n \geq k$ *such that any sequence of rational numbers* $(x_i)_{i=0,\ldots,n-1}$ *which satisfies (2.2.1) is such that for each* $i = 0, \ldots, n-1$*,* $\pm x_{i+1} = \pm x_i + 1$*? (the* $\pm$ *do not have to correspond). Moreover, if* k *is odd, is it true that, additionally,* $x_{i+1} = x_i + 1$*?*

It is obvious that a positive answer to (ii) of Problem 2.2 implies a positive answer to (i).

For $k = 2$, (2.2.1) gives a system of $n-2$ equations of the form

$$x_{i+2}^2 - 2x_{i+1}^2 + x_i^2 = 2$$

and for $k = 3$ it gives $n - 3$ equations of the form

$$x_{i+3}^3 - 3x_{i+2}^3 + 3x_{i+1}^3 - x_i^3 = 6 \ .$$

It is obvious from the above observations that if $x_{i+1} = x_i + 1$ then relation (2.2.1) holds. In fact for $k = 2$ more is known.

Lang's Conjecture [8, Conjecture 5.8] *Let X be a smooth projective algebraic variety of general type, defined over a number field M. Then there exists a proper Zariski-closed subset Z of X such that for all number fields K containing M, $X(K) - Z(K)$ is finite.*

Define X_n to be the projective subvariety of $\mathbb{P}^n$ cut out by the homogenizations of equations (2.2.1) for $k = 2$ (see the first set of equations in Section 3). Vojta proved:

Theorem 2.3 [19, Theorem 0.5] *If Lang's Conjecture holds for some $X_n(\mathbb{Q})$ then the n 2−nd powers problem has a positive answer.*

In fact the proof of Vojta shows that, assuming Lang's Conjecture, equation (2.2.1) for $k = 2$ has only the solutions $\pm x_{i+1} + 1 = \pm x_i$ over $\mathbb{Q}$. At this point we have no further evidence in favor of a positive answer to Problem 2.2. In [9] it is shown that a positive answer to the n 2−nd powers problem implies a negative answer to $\mathbf{Bq}(2)$. We present a similar argument for k−th powers, for k odd.

Theorem 2.4 *Let $k \geq 3$ be an odd rational integer. If Problem 2.2(ii) has a positive answer then the positive existential theory of $\mathbb{Z}$ in the language $L_{k,\mathbb{Z}}$ is undecidable, thus $\boldsymbol{Bq}(k)$ has a negative answer.*

Proof: Linear elimination proves the equivalence of the decidability of the positive-existential theory of $\mathbb{Z}$ in the language $L_{k,\mathbb{Z}}$ and $\mathbf{Bq}(k)$ (the details are left to the reader).

Assume that n is such that Problem 2.2(ii) (both statements) has a positive answer for n. We will represent arbitrary integers as certain linear combinations of k-th powers and we will interpret multiplication among two integers in terms of the corresponding representations in a way that is positive-existential in the language $L_{k,\mathbb{Z}}$. Thus, if the positive-existential theory of $\mathbb{Z}$ in $L_{k,\mathbb{Z}}$ were decidable, then the ring-theory of $\mathbb{Z}$ would be

decidable, which would contradict the negative answer to Hilbert's tenth problem given in [10].

The formula

$$\phi(y_0,\dots,y_{n-1}) \equiv [\Delta^{(k)}((y_i)_{i=0,\dots,n-1}) = (k!)] \bigwedge_{i=0,\dots,n} \text{`}y_i \text{ is a } k\text{-th power'}$$

is a formula of the language $L_{k,\mathbb{Z}}$. Having assumed a positive answer to Problem 2.2(ii) we obtain that $\phi(y_0,\dots,y_{n-1})$ implies that, setting $y_i = x_i^k$, we have

$$x_{i+1} = x_i + 1 \ .$$

Then, obviously, writing $x = x_0$, we have

$$y_{i+1} - y_i = p_{1,k}(x+i) \ .$$

It is easy to see that

$$\{X^k, (X+1)^k, \dots, (X+k)^k\}$$

is a basis of the vector space of polynomials in the variable X of degree at most k over $\mathbb{Q}$. Hence both X and X^2 can be written as $\mathbb{Q}$-linear combinations of elements of this basis, say

$$X = \sum_i c_i (X+i)^k \qquad \text{and} \qquad X^2 = \sum_i d_i (X+i)^k$$

for some fixed rational numbers (depending on k) c_i and d_i. Write

$$h_1(Y_0,\dots,Y_k) = \sum_i c_i Y_i \qquad \text{and} \qquad h_2(Y_0,\dots,Y_k) = \sum_i d_i Y_i \ .$$

We interpret arbitrary elements x of $\mathbb{Z}$ as the quantities $x = h_1(y_0,\dots,y_k)$ for which

$$\exists y_{k+1},\dots,y_{n-1}\phi(y_0,\dots,y_k,\dots,y_n)$$

is true. Then we have

$$x^2 = h_2(y_0,\dots,y_k)$$

hence we obtain a representation of the graph of the squaring function in $L_{k,\mathbb{Z}}$ (in the end we will need to clear denominators of terms of the equations so that only integers appear as coefficients). Finally we interpret multiplication using the equivalence

$$c = ab \leftrightarrow (a+b)^2 = a^2 + b^2 + 2c \ .$$

$\diamond$

Remark 2.5 If the n $k-$th powers problem has a positive answer over $\mathbb{Q}$ then one obtains a result similar to that of Theorem 2.4 for $\mathbb{Q}$. But undecidability does not follow from current knowledge: the analogue of Hilbert's tenth problem for $\mathbb{Q}$ is an open problem (cf. [13]).

Remark 2.6 It seems plausible that the 'n $k-$th powers problem' may have a positive answer over any ring of integers of a number field, or in any number field. Certainly it has a negative answer in any extension of the ring of real algebraic integers. We can not predict a characterization of the extensions of $\mathbb{Z}$ where it holds.

3 Systems of Squares

We consider Question 1.3 for $k = 2$ (that is, $\mathbf{Bq}(2, F(t), \mathbb{Z}[t])$ of the Introduction) where F is a field of characteristic zero. In what follows X_n is the projective subvariety of the projective n-space $\mathbb{P}^n$, over $\mathbb{C}$, cut out by the equations (in projective coordinates $(x, x_1, \ldots, x_n)$)

$$x_i^2 + x_{i-2}^2 = 2x_{i-1}^2 + 2x^2, \qquad i = 3, \ldots n$$

In [19] P. Vojta observed that

Theorem 3.1 *For $n \geq 6$ the variety X_n is a surface of general type.*

Then he showed

Theorem 3.2 *([19], Theorem 3.1) For $n \geq 8$, the only curves on X_n of geometric genus 0 or 1 are the 'trivial' lines*

$$\pm x_i = \pm x_1 - (i-1)x, i = 2, \ldots, n \ .$$

This has as an immediate consequence the following:

Corollary 3.3 *Let $n \geq 8$. Assume that F is a field of zero characteristic and that $y_1, \ldots, y_n \in F(t)$ are not all constant (i.e. in F) and satisfy*

$$y_i^2 + y_{i-2}^2 = 2y_{i-1}^2 + 2$$

for $i = 3, \ldots, n$. Then for some $\epsilon = \pm 1$ and for all $i = 2, \ldots, n$ we have

$$\pm y_i = \epsilon y_1 - (i-1) \ .$$

Proof: Assume that y_i are as in the hypothesis. The y_i involve finitely many coefficients. Embed the subring of F generated by those coefficients into the field of complex numbers and observe that the hypothesis of the Corollary remains true with F replaced by $\mathbb{C}$. So, without loss of generality, we assume that $F = \mathbb{C}$. Write $y_i = \frac{a_i}{b}$ with $a_i, b \in F[t]$ such that the greatest common divisor of the elements of the set $(b, a_1, \ldots, a_n)$ is the unit ideal. Homogenize simultaneously all the a_i and b, that is, substitute t by $\frac{t_1}{t_0}$, and find homogeneous polynomials $B(t_0, t_1), A_1(t_0, t_1), \ldots, A_n(t_0, t_1)$ of the form

$$B(t_0, t_1) = t_0^r b\left(\frac{t_1}{t_0}\right) \qquad \text{and} \qquad A_i(t_0, t_1) = t_0^{r_i} a_i\left(\frac{t_1}{t_0}\right)$$

so that the only common zero of all B and A_i is $(t_0, t_1) = (0, 0)$. Then the correspondence

$$(t_0, t_1) \to (B(t_0, t_1), A_1(t_0, t_1), \ldots, A_n(t_0, t_1))$$

is a map from the projective line $\mathbb{P}(\mathbb{C})$ into X_n. By Hurwitz's formula (cf. [5]) the image of that map is a projective curve of geometric genus 0, or, in different words,

$$(x, x_1, \ldots, x_n) = (B(t_0, t_1), A_1(t_0, t_1), \ldots, A_n(t_0, t_1))$$

is a parametrization of a curve on X_n of geometric genus 0. Hence, by Theorem 3.2, we have

$$\pm x_i = \pm x_1 - (i-1)x \ .$$

The latter relation implies that for each $i = 2, \ldots, n$ we have

$$\pm y_i = \pm y_1 - (i-1) \ .$$

Finally, we show that the $\pm$ correspond in the way stated in the conclusion: Set $\pm y_2 = \epsilon y_1 - 1$ for some $\epsilon = \pm 1$ and assume that for some $k \geq 2$ we have $\pm y_i = \epsilon y_1 - (i-1)$ for $i = 2, \ldots, k$ but $\pm y_{k+1} = -\epsilon y_1 - k$. Then

$$y_{k+1}^2 + y_{k-1}^2 - 2y_k^2 = 2\epsilon(k+1)y_1 + 2 \ .$$

On the other hand, by hypothesis, (y_{k-1}, y_k, y_{k+1}) satisfies

$$y_{k+1}^2 + y_{k-1}^2 - 2y_k^2 = 2 \ .$$

Equating the right hand sides of the last two equalities we obtain

$$\epsilon(k+1)y_1 = 0 \ .$$

Then all y_i are in F, which contradicts the hypothesis. The conclusion follows. $\diamond$

Note: Corollary 3.3 follows also from Theorem 0.6 of [19] which states:

Let $n \geq 8$ be an integer, and let $f : \mathbb{C} \to X_n$ be a non-constant holomorphic map. Then the image of f lies in one of the 'trivial lines'.

The proof of this Theorem is by results of Vojta in Nevanlinna Theory while the proof of Theorem 3.2 is based on algebro-geometric tools.

The proof of Corollary 3.3 is the following (the authors thank Paul Vojta for pointing this out): As in the above proof, assume without loss of generality that $F = \mathbb{C}$. Then the array $(y_1, \ldots, y_n)$ of rational functions induces a meromorphic map from $\mathbb{C}$ to X_n, which extends to a holomorphic map from $\mathbb{C}$ to X_n, by the valuative criterion of properness (for the terminology and the necessary facts see [20]). Then the latter Theorem implies the conclusion.

Proof of Theorem 1.4. Let $\phi(z, w)$ denote the formula

$$\exists w_1, \ldots, w_8 \in F(t) \ [w = w_1 \wedge 2z = w_2 - w_1 - 1 \bigwedge_{i=3,\ldots,8} w_i + w_{i-2} = 2w_{i-1} + 2 \bigwedge_{i=1,\ldots,8} P_2(w_i)] \ .$$

Assume that $w = z^2$. Then it is trivial to see that $\phi(z, w)$ holds true by taking $w_{i+1} = (z + i)^2$ for $i = 2, \ldots, 7$. Now assume that $\phi(z, w)$ is true. We claim that then either $w = z^2$ or $w \in F$. Assume that $w \notin F$. Let w_i satisfy the quantifier-free part of ϕ. Set $w_i = y_i^2$ for some $y_i \in F(t)$ (since ϕ is true such y_i exist). Then $y_1 \notin F$ and by Corollary 3.3, for some $\epsilon = \pm 1$ and for all $i = 2, \ldots, n$ we have

$$\pm y_i = \epsilon y_1 - (i - 1) \ .$$

Then $w = y_1^2$ and

$$2z = (\epsilon y_1 - 1)^2 - y_1^2 - 1$$

hence $z = -\epsilon y_1$ and $w = z^2$.

It is then trivial to see that $w = z^2$ is equivalent to

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

Thus squaring and, consequently, multiplication is definable in $L_{2,\mathbb{Z}[t]}$. $\diamond$

It follows that for any field F of characteristic zero the positive-existential $L_{2,\mathbb{Z}[t]}$-theory of $F(t)$ is decidable if and only if the existential ring-theory (in the language L_t of the Introduction) of $F(t)$ is decidable.

4 The case $k = 3$ for fields of rational functions: Outline of method

We consider the case $k = 3$. Let ξ be a primitive cube root of unity. Consider the following equation

$$(1 - t^3)y^3 = 1 - x^3 \qquad \text{(MD1)}$$

over $F(t)$. The crucial fact for the proof of Theorem 1.6 is:

For any solution (x, y) of (MD1), the value of y at $t = 1$ is in $\mathbb{Z}[\xi]$.
This results from the following analysis. Consider the elliptic curve $\mathcal{E}$ defined by the affine equation

$$X^3 + Y^3 = 1$$

(for the theory of elliptic curves the reader may consult [7] and [17]). It is well known that $\mathcal{E}$ together with any point $\mathcal{O}$ on the line at infinity is an elliptic curve over F. Fix an s such that $t^3 + s^3 = 1$. For each $x, y \in F(t)$ which satisfy (MD1) the rational function

$$(t, s) \to (x(t), sy(t))$$

defines a function from $\mathcal{E}$ into itself. By a theorem of Weil, any such function is the translation (by some point of $\mathcal{E}$, rational over F) of an endomorphism of $\mathcal{E}$. We will show that in our situation the set of possible translations is finite. So, modulo (in the group sense) a finite set, one can associate to each solution of (MD1) an endomorphism of $\mathcal{E}$. The ring of endomorphisms of $\mathcal{E}$

is isomorphic to $\mathbb{Z}[\xi]$. It turns out that, depending on the endomorphism $[n]$, three cases can occur. The function $[n](t,s)$ can be of any the forms (x_n, sy_n), (sx_n, y_n) and $(\frac{1}{s}x_n, \frac{1}{s}y_n)$. Each of these cases gives an equation which is either (MD1) or one of two similar equations (they are equations (MD2) and (MD0) of the next Section). Conversely, the rational maps which are defined by any of those equations form a subset of the group $\mathrm{Rat}_F(\mathcal{E})$ of rational maps from $\mathcal{E}$ to $\mathcal{E}$ over F. We will prove that this subset is actually a subgroup which is isomorphic to the group $\mathrm{End}_F(\mathcal{E}) \oplus \mathcal{E}_3(F)$, where $\mathrm{End}_F(\mathcal{E})$ denotes the ring of endomorphisms on $\mathcal{E}$ and $\mathcal{E}_3(F)$ the group of rational points of order 3 on $\mathcal{E}$. Finally we will show that any $n \in \mathbb{Z}[\xi]$ is the value of a rational function (such as y) associated to some solution of one of the equations (MDi), at $t = 1$. Thus we will obtain a definition of $F \cap \mathbb{Z}[\xi]$ over $F(t)$ which is positive-existential in $L_{3,\mathbb{Z}[t],\mathrm{Con,ord}}$ and Theorem 1.6 will follow.

We note that elliptic curves of the form of equations (MDi) have been studied first by Y. Manin and J. Denef.

5 Systems of Cubes

Throughout this section F is a field of characteristic zero. We consider the elliptic curve $\mathcal{E}$ defined by the projective equation

$$X^3 + Y^3 = Z^3,$$

with the distinguished point being $\mathcal{O} = [1, -1, 0]$ on the 'line at infinity' $Z = 0$. Note that there are two other points on the line at infinity, that is $[1, -\xi, 0]$ and $[-\xi, 1, 0]$, where $\xi \neq 1$ denotes a cube root of unity. The curve $\mathcal{E}$ has complex multiplication, and its j-invariant is 0 (see [17, chapter III, exercise 3.3, p. 104]). Therefore it has 6 automorphisms (see [17, Chapter III, Theorem 10.1, p. 103]). Writing

$$x = \frac{X}{Z} \qquad \text{and} \qquad y = \frac{Y}{Z}$$

we obtain the equation

$$x^3 + y^3 = 1$$

which defines the affine part $\mathcal{E}_a$ of the elliptic curve $\mathcal{E}$. The six automorphisms are given by [1], $[\xi]$, $[\xi^2]$ and their negatives, where $[\xi]$ and $[\xi^2]$ are

defined by

$$[\xi](x,y) = (\xi x, \xi y) \qquad \text{and} \qquad [\xi^2](x,y) = (\xi^2 x, \xi^2 y)\ .$$

We will now describe the addition law on $\mathcal{E}$. If $P = (x_0, y_0)$ its negative is given by

$$\ominus P = (y_0, x_0)\ .$$

Let $P_i = (x_i, y_i)$, $i = 1, 2$, be two points on $\mathcal{E}$. If

$$(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$$

then we find, by applying the method described in [17, Chapter III, §2, pp. 55-59] :

$$y_3 = \frac{-3\lambda^2\nu}{1+\lambda^3} - x_1 - x_2$$

which, if $x_1 x_2 \neq 0$, can be written

$$y_3 = \frac{1-\nu^3}{(1+\lambda^3)x_1 x_2}$$

where λ and ν are given by, if $x_1 \neq x_2$,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \text{and} \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

and, if $x_1 = x_2 = x$,

$$\lambda = -\frac{x^2}{y^2} \qquad \text{and} \qquad \nu = \frac{1}{y^2}.$$

The first coordinate x_3 is then given by $x_3 = \lambda y_3 + \nu$. But by symmetry, x_3 can also be obtained by exchanging x_1 with y_1, and x_2 with y_2, in y_3. In particular, we obtain the 'duplication formula' for the curve $\mathcal{E}$:

$$2(x,y) = \left(y\frac{x^3+1}{y^3-x^3}, x\frac{y^3+1}{x^3-y^3} \right) = \left(y\frac{x^3+1}{1-2x^3}, x\frac{x^3-2}{1-2x^3} \right).$$

In order to compute the order of the points at infinity, it is convenient to write it also in projective coordinates :

$$2[T,S,R] = [S(T^3+R^3), T(T^3-2R^3), R(R^3-2T^3)].$$

We find

$$2[1,-\xi,0] = [-\xi,1,0] = \ominus[1,-\xi,0]$$

which implies that the points $[1,-\xi,0]$, as well as $[-\xi,1,0]$, are of order 3. We observe that the point $[1,0,1]$ is also of order 3, since

$$2[1,0,1] = [0,1,1] = \ominus[1,0,1]\ .$$

The image of this point through each of the 6 automorphisms give 6 new points of order 3. So we found all the 9 points of order 3 on $\mathcal{E}$, remembering that 3 of them (counting the neutral) are on the line at infinity (see [17, chapter 3, Corollary 6.4, p. 89]).

More generally, the addition formula is given in projective coordinates by the following. If

$$[X_1,Y_1,Z_1] \oplus [X_2,Y_2,Z_2] = [X_3,Y_3,Z_3]$$

then we can choose :

$$\begin{aligned} X_3 &= Z_1Z_2(Z_2Y_1 - Z_1Y_2) + X_1X_2(X_1Y_2 - X_2Y_1) \\ Y_3 &= Z_1Z_2(Z_2X_1 - Z_1X_2) + Y_1Y_2(X_2Y_1 - X_1Y_2) \\ Z_3 &= X_1X_2(X_1Z_2 - X_2Z_1) + Y_1Y_2(Y_1Z_2 - Y_2Z_1) \end{aligned}$$

We deduce from this the 'triplication formula' (note that by applying the addition formula to $2(T,S,R) \oplus (T,S,R)$, all the coordinates X_3, Y_3 and Z_3 have $(T+S)$ as a common factor, and this simplifies much the computation) :

$$\begin{aligned} 3[T,S,R] = [&-T^9 - 3R^3T^6 + 6R^6T^3 - R^9, \\ &T^9 - 6R^3T^6 + 3R^6T^3 + R^9, TSR(3T^6 - 3R^3T^3 + 3R^6)]. \end{aligned}$$

If $n = n_1 + n_2\xi \in \mathbb{Z}[\xi]$ and $i \in \{0,1,2\}$ we will write $n \sim i$, if $n_1 + n_2$ is congruent to i mod 3 (this corresponds to congruence modulo $1-\xi$).

Lemma 5.1 *(i) Let S, T, R be such that $S^3 + T^3 = R^3$. For any $n \in \mathbb{Z}[\xi]$, there exist homogeneous polynomials F_n, G_n, H_n in $F[T^3, R^3]$ such that :*

$$\begin{aligned} n[T,S,R] &= [F_n, G_n, TSRH_n] && \text{if } n \sim 0 \\ n[T,S,R] &= [TF_n, SG_n, RH_n] && \text{if } n \sim 1 \\ n[T,S,R] &= [SF_n, TG_n, RH_n] && \text{if } n \sim 2. \end{aligned}$$

(ii) For any $n \in \mathbb{Z}[\xi]$, the three coordinates of $n[T,S,R]$ have the same global degree d_n in the variables T, S, R (not uniquely determined).

(iii) Let X, Y and Z be elements of $F(T,R)$. Then $(X,Y,SZ)\oplus(T,S,R)$ is of the form (X_0,SY_0,Z_0), $(X,SY,Z)\oplus(T,S,R)$ is of the form (SX_1,Y_1,Z_1) and $(SX,Y,Z)\oplus(T,S,R)$ is of the form (X_2,Y_2,SZ_2), for some functions X_i, Y_i and Z_i in $F(T,R)$.
(iv) Write $s=\frac{S}{R}$ and $t=\frac{T}{R}$ so that $s^3+t^3=1$. For any $n\in\mathbb{Z}[\xi]$, there exist homogeneous polynomials X_n, Y_n, Z_n in $F[T,R]$, and, if $n\neq 0$, rational functions x_n, y_n in $F(t)$ such that:

$$\begin{aligned} n[T,S,R] &= [X_n,Y_n,SZ_n] && \text{if } n\sim 0\\ n[T,S,R] &= [X_n,SY_n,Z_n] && \text{if } n\sim 1\\ n[T,S,R] &= [SX_n,Y_n,Z_n] && \text{if } n\sim 2 \end{aligned}$$

and, on the affine part of $\mathcal{E}$,

$$\begin{aligned} n(t,s) &= (\tfrac{1}{s}x_n,\tfrac{1}{s}y_n) && \text{if } n\sim 0\\ n(t,s) &= (x_n,sy_n) && \text{if } n\sim 1\\ n(t,s) &= (sx_n,y_n) && \text{if } n\sim 2. \end{aligned}$$

(v) We have

$$x_{n+a}(1)=\frac{y_n(1)}{a}\frac{1}{y_n^2(1)-ax_n(1)}$$

for all $n\sim 2$.

Proof: We prove (i) by induction in 3 steps. Observe that the assertion is true for $n=0,1,2,3$. Let $a=1$ or ξ.

1. First suppose that $n\sim 1$. We apply the addition formula to

$$[TF_n,SG_n,RH_n]\oplus[aT,aS,R]$$

and find polynomials U,V,W such that

$$\begin{aligned} U &= S[R^3H_n(G_n-aH_n)+a^2T^3F_n(F_n-G_n)]\\ V &= T[R^3H_n(F_n-aH_n)+a^2S^3G_n(G_n-F_n)]\\ W &= R[T^3F_n(aF_n-a^2H_n)+S^3G_n(aG_n-a^2H_n)]. \end{aligned}$$

Choose $F_{n+a}=\frac{U}{S}$, $G_{n+a}=\frac{V}{T}$ and $H_{n+a}=\frac{W}{R}$.

2. Now suppose that $n \sim 2$. We apply the addition formula to

$$[SF_n, TG_n, RH_n] \oplus [aT, aS, R]$$

and find polynomials

$$\begin{aligned} U &= T(R^3 G_n H_n + a^2 S^3 F_n^2) - S(aR^3 H_n^2 + a^2 T^3 F_n G_n) \\ V &= S(R^3 F_n H_n + a^2 T^3 G_n^2) - T(aR^3 H_n^2 + a^2 S^3 F_n G_n) \\ W &= aTSR[S(F_n^2 - aG_n H_n) + T(G_n^2 - aF_n H_n)]. \end{aligned}$$

In the formula for W, write $A = (F_n^2 - aG_n H_n)$ and $B = (G_n^2 - aF_n H_n)$. So we have $W = aTSR[SA + TB]$. Note that

$$(SA + TB)(S^2 A^2 - STAB + T^2 B^2) = S^3 A^3 + T^3 B^3.$$

By multiplying U, V and W by $S^2 A^2 - STAB + T^2 B^2$, and writing the new quantities X_{n+1}, Y_{n+1} and Z_{n+1} respectively, we obtain new polynomials U_1, V_1 and W_1. The polynomials U_1 and V_1 can be written in the form

$$S^3\alpha + S^2 T\beta + ST^2\gamma + T^3\delta \ .$$

It happens that in both cases the polynomials β and γ are 0. The computation finally gives:

$$\begin{aligned} U_1 = T^3(R^3 G_n H_n + a^2 S^3 F_n^2)(G_n^2 - aF_n H_n)^2 \\ - S^3(aR^3 H_n^2 + a^2 T^3 F_n G_n)(F_n^2 - aG_n H_n)^2 \end{aligned}$$

$$\begin{aligned} V_1 = S^3(R^3 F_n H_n + a^2 T^3 G_n^2)(F_n^2 - aG_n H_n)^2 \\ - T^3(aR^3 H_n^2 + a^2 S^3 F_n G_n)(G_n^2 - aF_n H_n)^2 \end{aligned}$$

$$W_1 = aTSR[S^3(F_n^2 - aG_n H_n)^3 + T^3(G_n^2 - aF_n H_n)^3].$$

Choose $F_{n+a} = U_1$, $G_{n+a} = V_1$ and $H_{n+a} = \frac{W_1}{TSR}$.

3. Suppose finally that $n \sim 0$ and apply the addition formula to

$$[F_n, G_n, TSRH_n] \oplus [aT, aS, R].$$

We find polynomials

$$U = T[S(R^3G_nH_n + a^2F_n^2) - T(aR^3S^3H_n^2 + a^2F_nG_n)]$$
$$V = S[T(R^3F_nH_n + a^2G_n^2) - S(aR^3T^3H_n^2 + a^2F_nG_n)]$$
$$W = aR[T(F_n^2 - aS^3G_nH_n) + S(G_n^2 - aT^3F_nH_n)].$$

We use the same technique as in the second step to obtain :

$$U_1 = T[S^3(R^3G_nH_n + a^2F_n^2)(G_n^2 - aT^3F_nH_n)^2 \\ - T^3(aR^3S^3H_n^2 + a^2F_nG_n)(F_n^2 - aS^3G_nH_n)^2]$$

$$V_1 = S[T^3(R^3F_nH_n + a^2G_n^2)(F_n^2 - aS^3G_nH_n)^2 \\ - S^3(aR^3T^3H_n^2 + a^2F_nG_n)(G_n^2 - aT^3F_nH_n)^2]$$

$$W_1 = aR[T^3(F_n^2 - aS^3G_nH_n)^3 + S^3(G_n^2 - aT^3F_nH_n)^3].$$

Choose $F_{n+a} = \frac{U_1}{T}$, $G_{n+a} = \frac{V_1}{S}$ and $H_{n+a} = \frac{W_1}{R}$.

Note that we proved the first part of the lemma for all integers $n_1+n_2\xi \in \mathbb{Z}[\xi]$ such that n_1 and n_2 are non-negative. It follows obviously for all the other integers in $\mathbb{Z}[\xi]$. The details are left to the reader.

(ii) and (iii) are immediate consequences of the computations above.

(iv) The first part is a direct consequence of (i). The second part is a consequence of (ii). The fact that d_n is not uniquely determined by n (since we are in projective coordinates) does not matter : we divide each coordinate of $n[T, S, R]$ by R^{d_n} in order to obtain new coordinates in the variables t and s. The lemma follows.

(v) Consider the second step of the proof of (i). In U_1 and $\frac{1}{S}W_1$, replace T and R by 1, F_n by $x_n(1)$, G_n by $y_n(1)$ and H_n by 1. Observe that $S^3 = R^3 - T^3$ must be replaced by 0. We get

$$x_{n+a}(1) = \frac{y_n(1)}{a}\frac{(y_n^2(1) - ax_n(1))^2}{(y_n^2(1) - ax_n(1))^3} = \frac{y_n(1)}{a}\frac{1}{y_n^2(1) - ax_n(1)}.$$

$\diamond$

Lemma 5.2 *For any* $[n] \in \mathrm{End}_F(\mathcal{E})$, $n \neq 0$, *we have*

$$x_n = y_{-n}$$

Proof: First consider $n \sim 1$. Therefore $-n \sim 2$. We have

$$(sx_{-n}, y_{-n}) = [-n](t,s) = \ominus[n](t,s) = \ominus(x_n, sy_n) = (sy_n, x_n)$$

using Lemma 5.1(iv). And we have

$$\left(\frac{1}{s}x_{-n}, \frac{1}{s}y_{-n}\right) = [-n](t,s) = \ominus[n](t,s) = \ominus\left(\frac{1}{s}x_n, \frac{1}{s}y_n\right) = \left(\frac{1}{s}y_n, \frac{1}{s}x_n\right)$$

for $n \sim 0$. ◇

Let us denote by $\mathrm{Rat}_F(\mathcal{E})$ the group of F-rational maps $\mathcal{E} \to \mathcal{E}$, by $\mathrm{End}_F(\mathcal{E})$ the ring of endomorphisms of $\mathcal{E}$ and by $\mathcal{E}(F)$ the group of F-rational points of $\mathcal{E}$. Let us write

$$\begin{aligned} R_0 = &\ \{f \in \mathrm{Rat}_F(\mathcal{E}) \mid \exists X, Y, Z \in F[T,R], f([T,S,R]) = [X, Y, SZ])\} \\ R_1 = &\ \{f \in \mathrm{Rat}_F(\mathcal{E}) \mid \exists X, Y, Z \in F[T,R], f([T,S,R]) = [X, SY, Z])\} \\ R_2 = &\ \{f \in \mathrm{Rat}_F(\mathcal{E}) \mid \exists X, Y, Z \in F[T,R], f([T,S,R]) = [SX, Y, Z])\}. \end{aligned}$$

We will identify $[T,S,R]$ with the identity map in $\mathrm{Rat}_F(\mathcal{E})$. Also we will use the symbol $\oplus$ for the addition in $\mathrm{Rat}_F(\mathcal{E})$.

Lemma 5.3 *Let* $i \in \{0,1,2\}$. *Denote by* $\bar{i}$ *the congruent class of* i *mod* 3. *We have*

$$R_i \oplus [T,S,R] = R_{\overline{i+1}}$$

and the union $\bigcup_{i=0}^{2} R_i$ *is a subgroup of* $\mathrm{Rat}_F(\mathcal{E})$.

Proof: From Lemma 5.1(iii), we know that $R_i \oplus [T,S,R] \subset R_{\overline{i+1}}$. Actually this inclusion is an equality of sets:

$$R_0 \subset R_1 \ominus [T,S,R] \subset R_2 \ominus 2[T,S,R] \subset R_0 \ominus 3[T,S,R] = R_0.$$

The last equality comes from the fact that $3[T,S,R] \in R_0$. So we have

$$\bigcup_{i=0}^{2} R_i = R_0 \cup (R_0 \oplus [T,S,R]) \cup (R_0 \oplus 2[T,S,R]).$$

Therefore it suffices to prove that R_0 is a subgroup of $\mathrm{Rat}_F(\mathcal{E})$. But this is obvious from the addition formula. $\diamond$

We consider the natural morphism of groups, which is an isomorphism (see [17, Chapter III, §4, p. 75]) :

$$\Psi \colon \mathrm{End}_F(\mathcal{E}) \oplus \mathcal{E}(F) \longrightarrow \mathrm{Rat}_F(\mathcal{E}).$$

There are actually two natural ways to define $\Psi(P)$ if $P \in \mathcal{E}(F)$. We can define it as the translation map by P or as the constant map. We will choose the second way. Write $\mathcal{E}_3(F)$ for the set of points of order 3 of the curve $\mathcal{E}$ (including the neutral). Write

$$P_1^a = [a, 0, 1] \qquad P_2^a = [0, a, 1] \qquad \text{and} \qquad P_0^a = [1, -a, 0]$$

where a denotes any of the three cube roots of unity. Write

$$P_i = \{P_i^a \mid a = 1, \xi, \xi^2\} \ .$$

With the following lemma one can see how a point on $\mathcal{E}$ behaves after adding a point of order 3.

Lemma 5.4 *Let $[U, V, W]$ be a point on $\mathcal{E}$, and $a = 1$, ξ or ξ^2. We have*

$$\begin{array}{ll} [U,V,W] \oplus [1,-a,0] & = [aU, a^2V, W] \\ [U,V,W] \oplus [0,a,1] & = [-aW, U, -a^2V] \\ [U,V,W] \oplus [a,0,1] & = [V, -aW, -a^2U] \end{array}$$

Proof: To get the first and the second equations we apply the addition formula and multiply the 3 coordinates of the results respectively by

$$\frac{U^2 - a^2UV + aV^2}{W^3},$$

and

$$\frac{W^2 + a^2VW + aV^2}{U^3}.$$

In order to find the third equation, observe that $[a, 0, 1]$ is the negative of $[0, a, 1]$ and use the second equation.

If one does not like using the addition formula, one could observe that the right hand sides of the equations define morphisms without fixed points,

therefore translations; the image of the origin by these translations give the constants on the left hand sides. $\diamond$

Write

$$U_i = \{[n] \oplus P_j^a \mid [n] \in \mathrm{End}_F(\mathcal{E}),\ n + j \sim i \text{ and } a = 1, \xi \text{ or } \xi^2\}.$$

Lemma 5.5 *We have*

$$\Psi^{-1}(\bigcup_{i=0}^{2} R_i) = \mathrm{End}_F(\mathcal{E}) \oplus \mathcal{E}_3(F).$$

More precisely, we have $\Psi^{-1}(R_i) = U_i$.

Proof: It is clear from Lemma 5.1(i) that we have

$$\Psi^{-1}(\bigcup_{i=0}^{2} R_i) \supseteq \mathrm{End}_F(\mathcal{E})$$

and we have

$$\Psi^{-1}(\bigcup_{i=0}^{2} R_i) \supseteq \mathcal{E}_3(F)$$

observing that the points of order 3 have one of their coordinates which is 0. We prove the other inclusion. Since $\bigcup_{i=0}^{2} R_i$ is a group, it suffices to prove that the only constant points in the image by Ψ^{-1} of $\bigcup_{i=0}^{2} R_i$ are points of order 3. If $P = [X, Y, Z]$ is a point in

$$\mathcal{E}(F) \cap \Psi^{-1}(\bigcup_{i=0}^{2} R_i),$$

$\Psi(P)$ is just the constant map, and we know it belongs to some R_i. Either $i = 1$ which implies that the coordinate Y must be 0 and then $P \in P_1$, or $i = 2$ which implies that $X = 0$ and then $P \in P_2$, or $i = 0$ which implies that $Z = 0$ and then $P \in P_0$. Therefore the point P is one of the nine points of order 3. The first part of the lemma is proven.

We now prove the second part. From Lemma 5.1(i) we have $\Psi(\{[n] \in \mathrm{End}_F(\mathcal{E}) \mid n \sim i\}) \subseteq R_i$. It is clear from Lemma 5.4 that $\Psi(U_i) \subseteq R_i$. This inclusion is actually an equality because the sets U_i form a partition

of $\mathrm{End}_F(\mathcal{E}) \oplus \mathcal{E}_3(F)$. $\diamond$

Let us consider the following equations :

$$\begin{array}{ll} \text{(MD0)} & x^3 + y^3 = 1 - t^3 \\ \text{(MD1)} & x^3 + (1-t^3)y^3 = 1 \\ \text{(MD2)} & (1-t^3)x^3 + y^3 = 1 \end{array}$$

and their analogues in projective coordinates

$$\begin{array}{ll} \text{(pMD0)} & X^3 + Y^3 = (1-t^3)Z^3 \\ \text{(pMD1)} & X^3 + (1-t^3)Y^3 = Z^3 \\ \text{(pMD2)} & (1-t^3)X^3 + Y^3 = Z^3. \end{array}$$

Each equation (pMDi) defines an elliptic curve $\mathcal{E}_i$ over $F(t)$. The point $[t, 1, 1]$ is obviously a solution of Equation (pMD1). Observe that each set P_i is the set of constant points of the curve $\mathcal{E}_i$ and that the points P_i^a are of order 3 on $\mathcal{E}$, therefore also on the curves $\mathcal{E}_i$. Denote by $\mathcal{E}_i(F(t))$ the group of points of $\mathcal{E}_i$ which are rational over $F(t)$.

Theorem 5.6 *The disjoint union of sets $\bigcup_{i=0}^{2} \mathcal{E}_i(F(t))$ has a natural structure of group and we have*

$$\mathcal{E}_i(F(t)) = \{[X_n, Y_n, Z_n] \oplus P_j^a \mid n + j \sim i \text{ and } a = 1, \xi \text{ or } \xi^2\}$$

for $i = 0, 1, 2$.

Proof : Consider the map

$$\Phi \colon \bigcup_{i=0}^{2} \mathcal{E}_i(F(t)) \longrightarrow \bigcup_{i=0}^{2} R_i$$

defined by

$$[X, Y, Z] \mapsto \begin{cases} f \colon [T, S, R] \to [X, Y, sZ] & \text{if } [X, Y, Z] \in \mathcal{E}_0(F(t)) \\ f \colon [T, S, R] \to [X, sY, Z] & \text{if } [X, Y, Z] \in \mathcal{E}_1(F(t)) \\ f \colon [T, S, R] \to [sX, Y, Z] & \text{if } [X, Y, Z] \in \mathcal{E}_2(F(t)) \end{cases}$$

where $t = \frac{T}{R}$ and $s = \frac{S}{R}$. This map is obviously a bijection of sets, and therefore Φ^{-1} brings the structure of group of $\bigcup_{i=0}^{2} R_i$ on $\bigcup_{i=0}^{2} \mathcal{E}_i(F(t))$. The

second assertion of the theorem is an immediate consequence of Lemma 5.5, we have

$$\mathcal{E}_i(F(t)) = \Phi^{-1}(R_i) = \Phi^{-1} \circ \Psi(U_i)$$

for $i = 0, 1, 2$. $\diamond$

Consider the elliptic curve $\mathcal{E}^0$ defined by its affine equation

$$y^2 = 4x^3 - 1.$$

The curve $\mathcal{E}^0$ is isomorphic to $\mathcal{E}$ through the following isomorphism

$$\begin{array}{rccl} \tau: & \mathcal{E}^0 & \longrightarrow & \mathcal{E} \\ & [X, Y, Z] & \longmapsto & [Y - \sqrt{3}Z, -Y - \sqrt{3}Z, -2\sqrt{3}X]. \end{array}$$

Denote by $\mathcal{Q}$ the Weierstrass function on $\mathcal{E}^0$ (the reader who is not familiar with basic properties of the Weierstrass functions may look into [17]). Let $(\mathcal{P}, \mathcal{R})$ denote the affine part of $\tau([\mathcal{Q}, \mathcal{Q}', 1])$. We write shortly

$$(\mathcal{P}, \mathcal{R}) = \tau(\mathcal{Q}, \mathcal{Q}') \ .$$

If

$$n = a + b\xi \in \mathrm{End}_F(\mathcal{E})$$

we will write

$$\overline{n} = a + b\xi^2$$

for the conjugate of n. We have

$$n\overline{n} = a^2 + b^2 - ab \in \mathbb{Z}$$

and for $m, n \in \mathrm{End}_F(\mathcal{E})$, the obvious relations

$$\overline{m+n} = \overline{m} + \overline{n} \qquad \text{and} \qquad \overline{mn} = \overline{m}\,\overline{n} \ .$$

Denote by Id the identity map.

Lemma 5.7 *We have*

$$\mathcal{P}' = -\sqrt{3}\mathcal{R}^2$$

and for any $[n] \in \mathrm{End}_F(\mathcal{E})$

$$[n](\mathcal{P}, \mathcal{R}) = (\mathcal{P}, \mathcal{R}) \circ (\overline{n}\mathrm{Id}\,).$$

Proof: First we compute the derivative of $\mathcal{P}$. We get

$$\mathcal{P} = \frac{\mathcal{Q}' - \sqrt{3}}{-2\sqrt{3}\mathcal{Q}} \qquad \text{and} \qquad \mathcal{R} = \frac{\mathcal{Q}' + \sqrt{3}}{2\sqrt{3}\mathcal{Q}}$$

from $(\mathcal{P}, \mathcal{R}) = \tau(\mathcal{Q}, \mathcal{Q}')$. Hence we have

$$\mathcal{P}' = \frac{-2\sqrt{3}\mathcal{Q}''\mathcal{Q} + 2\sqrt{3}(\mathcal{Q}' - \sqrt{3})\mathcal{Q}'}{12\mathcal{Q}^2} = -\sqrt{3}\left(\frac{\mathcal{Q}''\mathcal{Q} - \mathcal{Q}'^2 + \sqrt{3}\mathcal{Q}')}{6\mathcal{Q}^2}\right)$$

for the derivative of $\mathcal{P}$. From $\mathcal{Q}'^2 = 4\mathcal{Q}^3 - 1$ we get $2\mathcal{Q}''\mathcal{Q}' = 12\mathcal{Q}'\mathcal{Q}^2$ hence $\mathcal{Q}'' = 6\mathcal{Q}^2$. On the one hand we replace $\mathcal{Q}''$ and $\mathcal{Q}'^2$ in the expression of $\mathcal{P}'$

$$\mathcal{P}' = -\sqrt{3}\left(\frac{6\mathcal{Q}^3 - (4\mathcal{Q}^3 - 1) + \sqrt{3}\mathcal{Q}')}{6\mathcal{Q}^2}\right) = -\sqrt{3}\left(\frac{2\mathcal{Q}^3 + 1 + \sqrt{3}\mathcal{Q}')}{6\mathcal{Q}^2}\right)$$

and on the other hand we have

$$-\sqrt{3}\mathcal{R}^2 = -\sqrt{3}\left(\frac{\mathcal{Q}' + \sqrt{3}}{2\sqrt{3}\mathcal{Q}}\right)^2 = -\sqrt{3}\left(\frac{\mathcal{Q}'^2 + 2\sqrt{3}\mathcal{Q}' + 3}{12\mathcal{Q}^2}\right)$$

hence

$$-\sqrt{3}\mathcal{R}^2 = -\sqrt{3}\left(\frac{4\mathcal{Q}^3 - 1 + 2\sqrt{3}\mathcal{Q}' + 3}{12\mathcal{Q}^2}\right) = -\sqrt{3}\left(\frac{2\mathcal{Q}^3 + \sqrt{3}\mathcal{Q}' + 1}{6\mathcal{Q}^2}\right)$$

which proves the first assertion of the lemma.

Concerning the second assertion, it is known that for any $[n]^0 \in \mathrm{End}_F(\mathcal{E}^0)$, we have

$$[n]^0(\mathcal{Q}, \mathcal{Q}') = (\mathcal{Q}, \mathcal{Q}') \circ (n\mathrm{Id}\,)$$

(by construction of the Weierstrass function, see for example [17]). For $a = 1$, ξ, or ξ', write $[a]^0$ the automorphism on $\mathcal{E}^0$ defined by

$$[a]^0[X, Y, Z] = [aX, Y, Z]$$

(note the difference with the case of $\mathcal{E}$). It is easy to see that

$$[\xi] \circ \tau = \tau \circ [\xi^2]^0 \ .$$

Therefore, if $n = p + q\xi$, we have

$$[n] \circ \tau = [p + q\xi] \circ \tau := ([p] \oplus [q] \circ [\xi]) \circ \tau = \\ [p] \circ \tau \oplus [q] \circ (\tau \circ [\xi^2]^0) = \\ \tau \circ [p]^0 \oplus \tau \circ [q]^0 \circ [\xi^2]^0 = \tau \circ [\overline{n}]^0.$$

Combining the two equalities above, we find

$$[n](\mathcal{P}, \mathcal{R}) = [n] \circ \tau(\mathcal{Q}, \mathcal{Q}') = \tau \circ [\overline{n}]^0(\mathcal{Q}, \mathcal{Q}') = \\ \tau \circ (\mathcal{Q}, \mathcal{Q}') \circ (\overline{n}\mathrm{Id}\,) = (\mathcal{P}, \mathcal{R}) \circ (\overline{n}\mathrm{Id}\,).$$

$\diamond$

Lemma 5.8 *If $n \sim 1$, then we have*

$$\frac{x_n'}{y_n^2} = \overline{n}$$

Proof: Since $n \sim 1$, we know from Lemma 5.1(iv) and Lemma 5.7 that

$$(\mathcal{P}, \mathcal{R}) \circ (\overline{n}\mathrm{Id}\,) = [n](\mathcal{P}, \mathcal{R}) = (x_n \circ \mathcal{P}, \mathcal{R}y_n \circ \mathcal{P})$$

Therefore we have

$$x_n' \circ \mathcal{P} = \frac{1}{\mathcal{P}'}(x_n \circ \mathcal{P})' = \frac{1}{-\sqrt{3}\mathcal{R}^2}(\mathcal{P} \circ \overline{n}\mathrm{Id}\,)' = \frac{1}{-\sqrt{3}\mathcal{R}^2}\overline{n}\mathcal{P}' \circ \overline{n}\mathrm{Id} = \overline{n}\frac{\mathcal{R}^2 \circ \overline{n}\mathrm{Id}}{\mathcal{R}^2}.$$

Since we have

$$\mathcal{R}^2 \circ \overline{n}\mathrm{Id} = \mathcal{R}^2 y_n^2 \circ \mathcal{P}$$

we have

$$x_n' \circ \mathcal{P} = \overline{n} y_n^2 \circ \mathcal{P}.$$

The lemma follows because $(\mathcal{P}, \mathcal{R})$, seen as a map $\mathbb{C} \to \mathcal{E}$, is a global parametrization of the curve $\mathcal{E}$ (by construction of the Weierstrass function, see [17]). $\diamond$

Theorem 5.9 *Let $n \in \mathbb{Z}[\xi]$. We have*

$$x_n^3(1) = \begin{cases} \frac{1}{\overline{n}^3} & \text{if } n \sim 0 \\ 1 & \text{if } n \sim 1 \\ -\overline{n}^3 & \text{if } n \sim 2 \end{cases} \qquad y_n^3(1) = \begin{cases} -\frac{1}{\overline{n}^3} & \text{if } n \sim 0 \\ \overline{n}^3 & \text{if } n \sim 1 \\ 1 & \text{if } n \sim 2 \end{cases}$$

Proof: Because of Lemma 5.2, it suffices to prove it for the y_n's. The proof is done in two steps. Observe that if $x, y \in F(t)$ satisfy the equation $x^3+(1-t^3)y^3 = 1$, then y cannot have a pole at 1: suppose it had a pole of order n at 1; then $(1-t^3)y^3$ would have a pole at 1 of order $3n-1$, which would be also the order of x^3 at 1, but this is impossible since it is not a multiple of 3.

Suppose that $n \sim 1$. From Lemma 5.1(iv), we know that

$$x_n^3 + (1-t^3)y_n^3 = 1 \ .$$

This implies that $x_n^3(1) = 1 = y_{-n}^3(1)$. We get

$$3x_n' x_n^2 - 3t^2 y_n^3 + 3(1-t^3)y_n' y_n^2 = 0$$

by differentiating both sides of Equation (MD1). By Lemma 5.8 we know that $x_n' = \overline{n} y_n^2$. The equation becomes

$$\overline{n} x_n^2 - t^2 y_n + (1-t^3)y_n' = 0$$

after canceling the term $3y_n^2$. Evaluating at $t = 1$, we find

$$y_n(1) = \overline{n} x_n^2(1)$$

and therefore

$$y_n^3(1) = \overline{n}^3 x_n^6(1) = \overline{n}^3 \ .$$

Observe that for $n \sim 2$ we have $x_n(1) = -\overline{n} y_n^2(1)$.

Suppose now that $n \sim 0$ and write $n = m + a$, where a is equal to 1 or ξ. Since $m \sim 2$ we get

$$x_{m+a}(1) = \frac{y_m(1)}{a} \frac{1}{y_m^2(1) - a x_m(1)}$$

from Lemma 5.1(v). Also we know from the previous step that

$$x_m(1) = -\overline{m} y_m^2(1) \ .$$

Therefore the equation above becomes

$$\begin{aligned} x_{m+a}(1) = \frac{y_m(1)}{a} \frac{1}{y_m^2(1) + a\overline{m} y_m^2(1)} &= \frac{1}{a y_m(1)} \frac{1}{1 + a\overline{m}} \\ &= \frac{a}{y_m(1)} \frac{1}{a^2 + \overline{m}} = \frac{a}{y_m(1)} \frac{1}{\overline{a+m}} \ . \end{aligned}$$

We know from the previous step that $y_m(1)^3 = 1$, therefore we have

$$x_n^3(1) = x_{m+a}^3(1) = \frac{1}{(\overline{a+m})^3} = \frac{1}{\overline{n}^3} \ .$$

We obtain $y_n^3(1)$ from Lemma 5.2. $\diamond$

For $n + i \sim 1$, write (see the definition of P_i^a before Lemma 5.4)

$$(x_{n\oplus P_i^a}, sy_{n\oplus P_i^a}) = [n](t, s) \oplus P_i^a.$$

Corollary 5.10 *For any* $[n] \in \mathrm{End}_F(\mathcal{E})$ *and* $i = 0, 1, 2$ *such that* $n + i \sim 1$ *we have*

$$y_{n\oplus P_i^a}^3(1) = \overline{n}^3.$$

Proof: From Lemma 5.4, we find

$$y_{n\oplus P_0^a} = a^2 y_n \qquad y_{n\oplus P_1^a} = a^2 \frac{1}{x_n} \qquad y_{n\oplus P_2^a} = -a\frac{x_n}{y_n} \ .$$

We conclude with Theorem 5.9. $\diamond$

Proof of Theorem 1.6. a) Consider the following formula $\Psi_0(z)$, in the language $L_{3,\mathbb{Z}[t],\mathrm{Con,ord}}$:

$$\exists x, y(P_3(x) \wedge P_3(y) \wedge [1 - (t+1)^3]y = 1 - x \wedge \mathrm{Con}(z) \wedge \mathrm{ord}(y - z)).$$

Apply Corollary 5.10 with t replaced by $t+1$ to see that $\Psi_0(z)$ is equivalent to '$z \in \mathbb{Z}[\xi] \cap F$ and z is a cube'. The second difference of the three successive cubes $q-1$, q and $q+1$ is

$$[(q+1)^3 - q^3] - [q^3 - (q-1)^3] = 6q.$$

Then the formula $\Psi_1(z)$, given by

$$\exists z_1, z_2, z_3[\Psi_0(z_1) \wedge \Psi_0(z_2) \wedge \Psi_0(z_3) \wedge z = (z_3 - z_2) - (z_2 - z_1)]$$

defines a set

$$U = \{z \in F(t) \mid \Psi_1(z)\}$$

which satisfies

$$6\mathbb{Z}[\xi] \cap F \subset U \subset \mathbb{Z}[\xi] \cap F \ .$$

Finally we get a positive-existential definition of $\mathbb{Z}[\xi] \cap F$ by:

$$z \in \mathbb{Z}[\xi] \cap F \Longleftrightarrow \bigvee_{i=0}^{5} \exists w \Psi_1(w) \wedge z = w + i.$$

b) Assume that for some $a, b \in \mathbb{Z}$ with $ab \neq 0$, F has a subset D such that for all $n \in \mathbb{Z}[\xi] \cap F$, there is a $d \in D$ such that

$$an^3 + bd^3 = 1 \ .$$

Replace each occurrence of $\mathrm{Con}(z)$ in the proof of (a) by the formula:

$$\theta(z)\colon \exists w[P_3(z) \wedge P_3(w) \wedge az + bw = 1].$$

Then the proof of (a) still works. This is, first, because the curve

$$aX^3 + bY^3 = 1$$

is of genus 1 and does not admit a rational parametrization (by Hurwitz's formula, see [5]), hence any z satisfying $\theta(z)$ must be in F and secondly because, by assumption, for any $n \in \mathbb{Z}[\xi] \cap F$, $\theta(n^3)$ holds. $\diamond$

References

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

[2] J. Denef, *Hilbert's tenth problem for quadratic rings*, Proceedings of the American Mathematical Society **48**, 214-220 (1975).

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

[4] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, Journal of the London Mathematical Society (2) **18**, 385-391 (1978).

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

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

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

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

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

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

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

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

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

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

[15] A. Shlapentokh, *Diophantine Undecidability over Algebraic Function Fields over Finite Fields of constants*, Journal of Number Theory **58**, 317-342 (1996).

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

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

[18] 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).

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

[20] ——, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, Springer-Verlag, (1987)

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

[22] ——, *Hilbert's Tenth Problem for rings of rational functions Notre Dame Journal of Formal Logic*, **43-3**, 181-192 (2002)