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

Thanasis PHEIDAS
University of Crete
Department of mathematics
71 409 Heraklion
Crete, GREECE
pheidas@math.uoc.gr

Xavier VIDAUX
University of Oxford
Mathematical Institute
24-29 St Giles'
OX1 3LB, Oxford, UK
vidaux@maths.ox.ac.uk

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

We examine variances of this problem for $k = 2, 3$ and for R a field of rational functions of characteristic zero. We obtain negative answers, provided that the analogous problem over $\mathbf{Z}$ has a negative answer. In particular we prove that the generalization of Büchi's question for fields of rational functions over a real-closed field F, for $k = 2$, has a negative answer if the analogous question over $\mathbf{Z}$ has a negative answer.

1 Introduction

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

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

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

J. Richard Büchi asked the question for $k = 2$ and this was publicized by L. Lipshitz in [11]. The problem was investigated by Joseph Lipman and Barry Mazur (cf. [13]) and Paul Vojta proved that a conjecture of Serge Lang implies a negative answer to it (we discuss this below). In fact Vojta's result gives a negative (conditional) answer to the analogous question in which we require solvability in the field $\mathbf{Q}$ of rational numbers.

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

Question 1.2 *(*$\mathbf{Bq}(k, R, C)$*) Does there exist an algorithm to determine, given* $m, n \in \mathbf{N}$*,* $A = (a_{i,j})_{i,j} \in M_{m,n}(C)$*,* $B = (b_i) \in M_{m,1}(C)$ *and a subset* $I \subset \{1, ..., n\}$*, whether there exist* $x_1, ..., x_n \in R$ *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* $i \in I$*,* $x_i \in \{y^k : y \in R\}$?

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

Fix a field F of characteristic zero and let $F(t)$ be the field of rational functions in the variable t, with coefficients in F. In this paper we deal with questions of type $\mathbf{Bq}(k, F(t), \mathbf{Z}[t])$ for $k = 2$ and 3. One of our results, is that if F is a real-closed field then, if $\mathbf{Bq}(2)$ has a negative answer then $\mathbf{Bq}(2, F(t), \mathbf{Z}[t])$ has a negative answer as well.

Some of the questions that we answer are similar to Question 1.2 but allowing additional conditions, of the forms $x \in F$ and $x(0) = 0$ (the value of x at $t = 0$ is 0).

It is convenient to use the terminology of Logic. Let $k \geq 2$ be an integer. Let $L_{k,\mathbf{Z}[t]}$ be the set of symbols (called a *language*) $\{+, P_k\} \cup \mathbf{Z}[t]$ with symbols for addition in $F(t)$ $(+)$, the predicate P_k which is interpreted in $F(t)$ as $P_k(x) \leftrightarrow \exists y \in F(t)(x = y^k)$ and symbols for each element of $\mathbf{Z}[t]$. A *quantifier-free* formula of $L_{k,\mathbf{Z}[t]}$ 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 $L_{k,\mathbf{Z}[t]}$ is a formula of the form $\exists y \phi(x, y)$ where ϕ is a quantifier-free formula of $L_{k,\mathbf{Z}[t]}$. A subset of a power of $F(t)$ 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 the unions and intersections of positive-existential sets are positive-existential. The *positive-existential theory* of $F(t)$ in the language $L_{k,\mathbf{Z}[t]}$ is the set of all positive-existential formulas of $L_{k,\mathbf{Z}[t]}$ which are true over $F(t)$. In this terminology, Question 1.2 is equivalent to

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

Let $L_{k,\mathbf{Z}[t],\mathrm{Con,ord}}$ be the augmentation of $L_{k,C}$ 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 languages $L_{k,\mathbf{Z}[t],\mathrm{Con}}$ and $L_{k,\mathbf{Z}[t],\mathrm{ord}}$ are the restrictions of $L_{k,\mathbf{Z}[t],\mathrm{Con,ord}}$ by deleting the obvious predicate symbols. Our main results are:

Theorem 1.4 *Let F be a field of zero characteristic and let t be a variable. Then*

(a) The ring of integers $\mathbf{Z}$ is positive-existentially definable over $F(t)$ in the language $L_{2,\mathbf{Z}[t],\mathrm{Con,ord}}$; consequently if $\mathbf{Bq}(2)$ has a negative answer then the positive-existential theory of $F(t)$ in the language $L_{2,\mathbf{Z}[t],\mathrm{Con,ord}}$ is undecidable.

(b) Assume that F is a real field. The ring of integers $\mathbf{Z}$ is positive-existentially definable over $F(t)$ in the language $L_{2,\mathbf{Z}[t],\mathrm{Con}}$; consequently if $\mathbf{Bq}(2)$ has a negative answer then the positive-existential theory of $F(t)$ in the language $L_{2,\mathbf{Z}[t],\mathrm{Con}}$ is undecidable.

(c) Assume that F is a real-closed field. Then $\mathbf{Z}$ is positive-existentially definable over $F(t)$ in the language $L_{2,\mathbf{Z}[t]}$; consequently if $\mathbf{Bq}(2)$ has a negative answer then $\mathbf{Bq}(2, F(t), \mathbf{Z}[t])$ is undecidable.

Theorem 1.5 *Let F be a field of zero characteristic, let t be a variable and let ξ be a primitive cube root of 1. Then*

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

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

It is obvious that $\mathbf{Bq}(k, R, C)$ is a sub-problem of the "diophantine problem" for R with constants in C, that is the question whether there exists an algorithm which decides, given a system of polynomial equations in several variables and with coefficients in C, the solvability of this system over R. So far $\mathbf{Bq}(k, R, C)$ is open for all k and for any (R, C) whose diophantine problem is known to be undecidable; such is the case for fields of rational functions $F(t)$ with F being either a real field or a finite field (see [3], [14], [20], [23] and [25]). Open is the problem whether the diophantine problem for $\mathbf{C}(t)$ is decidable (and similarly for any $F(t)$ with F algebraically closed). For more results and questions in this direction the reader may consult [8], and the surveys in [16] and [21]. For two examples of decidability results see [6] and [19].

Our methods of proof apparently do not generalize to values of k other than $k = 2, 3$.

In Section 2 we present a number theoretical problem 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 [11] and [24].

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

Definition 2.1 *Let $y = (y_i)_{i=0}^n$ be a sequence of complex numbers. We call the* difference sequence of *y the sequence $\Delta(y) = (\Delta(y)(i))_{i=0,\ldots,n-1}$ defined by $\Delta(y)(i) = y_{i+1} - y_i$. The $k-$th difference of y, denoted $\Delta^{(k)}(y) = (\Delta^{(k)}(y)(i))_{i=0,\ldots,n-k}$, is defined recursively by $\Delta^{(1)}(y) = \Delta(y)$ and $\Delta^{(k+1)}(y) = \Delta(\Delta^{(k)}(y))$.*

Let $k \in \mathbf{Z}$, $k \geq 2$. Let R be any integral domain of characteristic zero. It is easy to see that for any $x \in R$, the $l-$th difference $\Delta^{(l)}(p(x, k))$ of the sequence $p(x, k) = ((x + i)^k)_{i=0,\ldots,k}$, for $l \leq k$, is a sequence of polynomials in x, of degree $k - l$, with integer coefficients which depend only on k and l. Observe that $\Delta^{(k)}(p(x, k))$ is a 1-term sequence. We define the constant λ_k by

$$\Delta^{(k)}(p(x, k)) = (\lambda_k).$$

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

Problem 2.2 *Let k be a rational integer with $k \geq 2$. Is there a natural number n such that for any sequence of natural numbers $(x_i)_{i=0}^n$ which satisfies*

$$\Delta^{(k)}(x_i^k)_{i=0}^k = \lambda_k \tag{2.2.1}$$

is such that, for each $i = 0, \ldots, n-1$, $\pm x_{i+1} = x_i + 1$?

For $k = 2$, (2.2.1) gives $x_{i+2}^2 - 2x_{i+1}^2 + x_i^2 = 2$ and for $k = 3$ it gives $x_{i+3}^3 - 3x_{i+2}^3 + 3x_{i+1}^3 - x_i^3 = 6$. 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 [10, 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 $\mathbf{P}^n$ cut out by the homogenizations of equations (2.2.1) for $k = 2$.

Theorem 2.3 [24, Theorem 0.5] *If Lang's Conjecture holds for some $X_n(\mathbf{Q})$ 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 $\mathbf{Q}$. At this point we have no further evidence in favor of a positive answer to Problem 2.2. In [11] it is shown that a positive answer to the n $2-$nd powers problem implies a negative answer to $\mathbf{Bq}(2)$. A similar argument holds for $k-$th powers. We present it for the sake of completeness.

Lemma 2.4 *Let $k \geq 2$ be a rational integer. If the n $k-th$ powers problem has a positive answer then multiplication is positive existentially definable in $L_{k,\mathbf{Z}}$ over $\mathbf{Z}$ and the positive existential theory of $\mathbf{Z}$ in the language $L_{k,\mathbf{Z}}$ is undecidable, thus $\mathbf{Bq}(k)$ has a negative answer.*

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

Remark 2.6 It seems plausible that the n $k-$th powers problems may have a positive answer even over rings such as a ring of integers of a number field, $\mathbf{Z}[t]$ or $\mathbf{Q}(t)$. But it is obvious that it has a negative answer over any ring containing the field $\mathbf{R}$ of real numbers. Therefore, the undecidability results of Theorems 1.4 and 1.5 for fields such as $\mathbf{R}(t)$ requires other techniques.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[20] A. Shlapentokh, *Diophantine undecidability of function fields of characteristic greater than 2, finitely generated over fields algebraic over a finite field*, Compositio Mathematica **132-1**, 99-120 (2002).

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

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

[23] 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).

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

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