Записки научных
семинаров ПОМИ
Том 377, 2010 г.

H. Pasten, T. Pheidas, X. Vidaux

A SURVEY ON BÜCHI'S PROBLEM: NEW PRESENTATIONS AND OPEN PROBLEMS

Abstract. In a commutative ring with a unit, *Büchi sequences* are those sequences whose second difference of squares is the constant sequence (2). Sequences of elements x_n, satisfying $x_n^2 = (x+n)^2$ for some fixed x are Büchi sequences that we call *trivial*. Since we want to study sequences whose elements do not belong to certain subrings (e.g. for fields of rational functions $F(z)$ over a field F, we are interested in sequences that are not over F), the concept of *trivial sequences* may vary. Büchi's Problem for a ring asks, whether there exists a positive integer M such that any Büchi sequence of length M or more is trivial.

We survey the current status of knowledge for Büchi's problem and its analogues for higher-order differences and higher powers. We propose several new and old open problems. We present a few new results and various sketches of proofs of old results (in particular Vojta's conditional proof for the case of integers and a rather detailed proof for the case of polynomial rings in characteristic zero), and present a new and short proof of the positive answer to Büchi's problem over finite fields with p elements (originally proved by Hensley). We discuss applications to logic, which were the initial aim for solving these problems.

1. Preamble

We survey the current status of knowledge for Büchi sequences, and:

- recall several old and propose new open problems;
- present a number of new results (in particular Lemmas 5.2 and 11.1, most of Section 12, and various 'small' results all along the text);
- present various sketches of proofs of old results (in particular: Vojta's conditional proof for the case of integers and a quite detailed proof for the case of polynomial rings in characteristic zero); and

Key words and phrases. Büchi, "n squares problem", Diophantine equations, Hilbert's tenth problem, undecidability.

This work has been realized under the third author's Fondecyt Research Project 1090233 (Conicyt - Chile) and is part of the Master Thesis of the first author. Part of this work was done while the second and third authors were in Bonn (Germany) for the Trimester on Diophantine Equations in 2010, organized and partially financed by the Hausdorff Institute of Mathematics.

- present a new (very short) proof of the positive answer to Büchi's problem over finite fields with p elements (originally proved by Hensley in [9]).

As it is a survey on Büchi's problem and not on Hilbert's tenth problem, we chose to refer only to surveys or books for the latter, except for a few results that do not appear in those or are of a special importance for our presentation. We have tried (certainly unsuccessfully) to make a bibliography as complete as possible relative to Büchi's problem.

Some of the facts that we present are yet unpublished.

Section 4 explains how a problem of Logic (the (un)decidability of simultaneous representation of integers by diagonal quadratic forms) leads naturally to Büchi's 'n squares problem'.

In Section 5, we propose an analogue of Büchi's problem for a general commutative ring with unit. Then we discuss the 'conservation' of positive and negative answers to Büchi's problem under various operations (like intersection and cartesian product) and separate the rings of characterisitc zero, for which Büchi's problem has a negative answer, into two types.

In Section 6 we present a formulation of Büchi's problem that usually makes positive answers easier to obtain.

In Section 9 we present conditional positive answers to (strong forms of) Büchi's problem for number fields and a sketch of proof of a result by Vojta: if a certain question of Bombieri has a positive answer then Büchi's problem for integers has a positive answer.

In Section 10 we present an analogue of Büchi's problem for rings of functions and the connection with Logic in this context. We also present the general method to obtain a positive answer for rings of functions.

In Section 11 we generalize most of the concepts that were developed in the previous sections to higher powers. We discuss intermediate problems and explain the connection with Logic.

In Section 12 we explain in details two phenomena that occur in the case of positive characteristic. In particular we explain how the notion of a *trivial sequence* has to be adapted.

Section 13 is a list of open problems. We feel that some of them may be not too hard to solve, while others may be rather difficult, given the current status of knowledge in Number Theory.

The authors would like to thank A. Laface, J. Lipman, L. Lipshitz, L. Moret-Bailly, B. Poonen, A. Shlapentokh and P. Vojta, for useful discussions and suggestions at various stages of preparation of this article. We are very grateful to the referee for all his useful and clarifying comments

and examples.

2. Introduction

A sequence of rational numbers (or integers, or elements of a commutative ring A with unit) is a *Büchi sequence* if the sequence of its squares has second difference constant and equal to the constant sequence (2). Equivalently, a sequence (x_n) is a Büchi sequence if any three consecutive terms x_n, x_{n+1}, x_{n+2} satisfy the relation

$$x_{n+2}^2 - 2x_{n+1}^2 + x_n^2 = 2.$$

Obviously any sequence of successive elements, $x_n = x + n$, is a Büchi sequence. We call such sequences 'trivial' and we investigate the existence of non-trivial Büchi sequences of length M, for 'large' M. It has been conjectured that no such sequences of rational numbers exist, for M large enough. Experimentally no non-trivial integer Büchi sequences of length 5 have been found, but the problem is still open – note that

$$\left(\frac{11}{9}, \frac{50}{9}, \frac{71}{9}, \frac{88}{9}, \frac{103}{9}\right)$$

is a Büchi sequence, cf [4].

On the other hand it has been established that in several commonly used rings there are no 'proper' non-trivial Büchi sequences of sufficiently large length. This is true for fields of rational functions in characteristic 0 and fields of global meromorphic functions (for rings of functions, the word 'proper' is interpreted as 'non-constant'). In positive characteristic $p > 2$, the sequences of the form

$$\left((f+n)^{\frac{p^s+1}{2}}\right)_{n=0,1,\ldots} \tag{1}$$

where s is a positive integer and $f^{p^s} \neq f$, are non-trivial Büchi sequences of infinite length. It has been proved that these are the only examples of proper non-trivial Büchi sequences of large length in fields of rational functions (actually even in function fields of curves in large enough positive characteristic).

We discuss in some detail the above and relevant results in Sections 5 to 12. We also discuss 'Büchi sequences for higher powers' which are characterized by the property that the kth difference of their sequence of kth powers is constant and equal to $k!$.

Büchi sequences (for any power k) give rise to varieties of arbitrarily large dimension and those provide a good testing ground for some conjectures in Number Theory and Arithmetic Algebraic Geometry (cf. B. Mazur [14] and P. Vojta [29]). Moreover, some of the mentioned properties permit applications in Logic (this was the initial intention of Büchi, cf. L. Lipshitz [11]). The main relevant results so far are strong versions of negative answers to "analogues" of Hilbert's tenth problem. Hilbert's tenth problem, the tenth in the famous list of problems that Hilbert gave at the International Conference of Mathematicians in Sorbonne (Paris), in 1900, was:

Hilbert's tenth problem: *To find a process according to which one can determine, in a finite number of steps, whether a polynomial equation with integer coefficients has or does not have integer solutions.*

The problem was answered in 1970 when Yu. Matiyasevich, based on work of J. Robinson, M. Davis and H. Putnam, proved that no such 'process' (in modern terminology: algorithm) exists - and all this was built on the work of (among others) K. Gödel and A. Turing who laid the necessary foundations in Logic (see [13] and [5]).

Later, various authors asked similar questions for rings other than the integers (first J. Denef and L. Lipshitz). An outstanding problem, the similar question for the field of rational numbers, remains open. So does the similar question for any field of rational functions, such as $\mathbb{C}(z)$, over an algebraically closed field. For surveys of such results see for example [7], [24] or [25].

All the negative existing results (non-existence of an algorithm, or, in the terminology of Logic, *undecidability*) have been obtained via *definability* results: working in a ring A, one shows that certain, sufficiently complicated sets, are *positive-existentially definable*, which in this context usually means projections of algebraic sets along some of the directions of the variables. The sets that are thus defined are then used to encode effectively the set of rational integers together with the graphs of integer addition and multiplication, which results in an argument of the type: 'If there were an algorithm to solve polynomial equations over A, then one would be able to convert it to an algorithm to solve positively Hilbert's tenth problem', a contradiction that shows that the analogue of Hilbert's tenth problem for A is undecidable.

An analogue of Hilbert's tenth problem for a polynomial ring $F[z]$ or a field of rational functions $F(z)$ (where F is a field, z is a variable) is the question:

Is there an algorithm which, given any polynomial equation (in several variables), with coefficients in $F_0[z]$ (F_0 is the prime subfield of F) decides whether the equation has or does not have solutions in $F[z]$ (or in $F(z)$)?

The answer for $F[z]$ in the characteristic zero case is negative (see Denef [6], where a negative answer is obtained also for $F(z)$, for F a formally real field). A similar result is true if one asks about the solvability in $F[z]$ of polynomial equations with coefficients in F, but together with conditions which mean that some of the variables represent non-constant polynomials (cf. [22]). In logical terminology this amounts to asking the (un)decidability of the positive-existential theory of a structure (such as a polynomial ring) in the language $\mathcal{L}_T = \{0, 1, +, \cdot, T\}$ where T is a symbol of unary relation for 'x is non constant'. There are very few results for decidability questions in that language, but Büchi's problem, whenever it has a positive answer, is particularly useful in that direction (since Büchi sequences, viewed as varieties, are defined over the prime subfield) – see for example any of [18, 19] or [21]. All existing results for questions of decidability of existential theories over 'global domains' (number fields, fields of rational or algebraic functions, etc.) are of a negative nature but many problems remain open, e.g. a similar question for $F(z)$, for an algebraically closed field F.

We consider that the main contribution of this paper is a large number of questions for future research that arise naturally from our discussion.

3. Definitions and notation

- All rings will be commutative with unit.
- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ stand respectively for the set of non-negative natural numbers, the ring of integers, and the fields of rational, real and complex numbers respectively.
- The *prime subring* of a ring A is the natural image of $\mathbb{Z}$ in A.
- If A_z is a ring of functions in the variable z, we will say that $x \in A_z$ is *non-constant* if it depends on z.
- $\bar{\mathbb{Z}}$ is the ring of algebraic integers.
- $\bar{\mathbb{Q}}$ is the field of algebraic numbers.
- $\mathbb{F}_q$ is the field with $q = p^r$ elements, where p is a prime number.
- $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{C}_p$ stand respectively for the ring of p-adic integers, the field of p-adic numbers and the field of p-adic complex numbers (complete and algebraically closed).

- $\mathbb{Z}/n\mathbb{Z}$ is the ring of integers modulo n.
- $\mathcal{L}_R = \{0, 1, +, \cdot\}$ is the *ring language*. We adopt the convention that in any ring the symbols $+$ and $\cdot$ are interpreted by the ring operations in the usual way and the symbols 0, 1 are interpreted by the corresponding neutrals.
- For any positive integer $k \geq 2$, P^k is a unary predicate which, in any given ring, is interpreted by

$$P^k(x) \quad \text{if and only if} \quad \text{`x is a kth power'}.$$

- $\mathcal{L}^k = \{0, 1, +, P^k\}$ is *Büchi's language for kth powers.*
- $\mathcal{L}_z = \{0, 1, +, \cdot, z\}$ is the augmentation of the ring language by the constant-symbol z, which, in any ring of functions of one independent variable, is interpreted as the independent variable.
- $\mathcal{L}_z^k = \{0, 1, +, P^k, f_z\}$, where f_z is a symbol of unary function interpreted as $f(x) = zx$, is *Büchi's language for kth powers and rings of functions.*
- The symbol $\mathbf{T}_{\mathcal{L}}^{\mathsf{pe}}(\mathfrak{M})$ stands for the positive-existential theory of the $\mathcal{L}$-structure $\mathfrak{M}$.
- A *Büchi System for kth powers* is a *formal* system (S_M^k) of $M - k$ equations

$$(S_M^k) \quad \begin{cases} \sum\limits_{i=1}^{k+1} (-1)^{i-1} \mathsf{C}_k^{i-1} x_i^k = k! \\ \vdots \\ \sum\limits_{i=n-k}^{n} (-1)^{i-n+k} \mathsf{C}_k^{i-n+k} x_i^k = k! \\ \vdots \\ \sum\limits_{i=M-k}^{M} (-1)^{i-M+k} \mathsf{C}_k^{i-M+k} x_i^k = k! \end{cases}$$

in the variables x_i, where $\mathsf{C}_k^m = \frac{k!}{m!(k-m)!}$ (we use the word 'formal' because we do not want to specify in the notation the ring in which we consider the system). Equivalently, if $\sigma = (x_n^k)_{1 \leq n \leq M}$ is a sequence of kth powers of variables, the system (S_M^k) can be written as

$$\Delta^k(\sigma) = (k!)_{1 \leq n \leq M-k},$$

where $\Delta^k(\sigma)$ stands for the kth difference sequence of the sequence σ. For example, for $k = 2$:

$$(S_M^2) \quad \begin{cases} x_3^2 - 2x_2^2 + x_1^2 = 2 \\ \vdots \\ x_{n+2}^2 - 2x_{n+1}^2 + x_n^2 = 2 \\ \vdots \\ x_M^2 - 2x_{M-1}^2 + x_{M-2}^2 = 2 \end{cases}$$

is equivalent to

$$\begin{cases} (x_3^2 - x_2^2) - (x_2^2 - x_1^2) = 2 \\ \vdots \\ (x_{n+2}^2 - x_{n+1}^2) - (x_{n+1}^2 - x_n^2) = 2 \\ \vdots \\ (x_M^2 - x_{M-1}^2) - (x_{M-1}^2 - x_{M-2}^2) = 2. \end{cases}$$

- *An M-term Büchi sequence* is a finite sequence $(x_n)_{1\leq n\leq M}$ satisfying (S_M^k).
- A *Büchi sequence* is a finite or infinite Büchi sequence.
- A *trivial Büchi sequence* is a sequence (x_n) for which there exists an x such that $x_n^k = (x+n)^k$ for all n. In any commutative ring with identity these sequences are trivially solutions of (S_M^k), for any M (depending on the ring in which we consider the system, some other sequences may be considered as *trivial*).
- $\mathbf{DF}^k(A)$ is the *problem of simultaneous representation of elements of a subset B of the ring A by diagonal forms of degree k over B*. The subset B will depend on the context (for example, if A is a number field, then B will be the natural image of $\mathbb{Z}$ in A). See Sections 4 and 11.
- $\mathbf{B}^k(A)$ is *Büchi's Problem for kth powers over the ring A*. See Sections 4, 5 and 11.
- $\mathbf{HP}_\ell^k(A)$ is *Hensley's Problem for ℓ and k over the ring A*. See Sections 6 and 11.

4. The origin of Büchi's problem

Already in 1938, it was known that any system of diophantine equations could be reduced *in an effective way* to a system of equations of degree at most 2 (see for example Skolem [27], Britton [3] or Davis [5]). Hence, by the negative answer to Hilbert's tenth problem, it follows that there is no algorithm to decide whether or not a system of quadratic equations has an integer solution. So it is natural to wonder about the existence of an algorithm which solves systems of *diagonal* quadratic equations. Hence Büchi asked:

Simultaneous Representation of Integers by Diagonal Quadratic Forms$\mathbf{DF^2}(\mathbb{Z})$ *Is there an algorithm to decide whether any given system of a finite number of diophantine equations, each of the form*

$$\sum_i \alpha_i x_i^2 = \gamma$$

has an integer solution?

Following the work of Siegel, it is proved in [8] that there exists an algorithm to decide whether a *single* polynomial equation over $\mathbb{Z}$ (or over $\mathbb{Q}$), of degree at most 2, has an integral solution.

On the other hand, the $\mathcal{L}^2$-positive-existential theory of $\mathbb{Z}$ is undecidable if and only if the following problem is undecidable:

$\mathbf{T}^{\mathbf{pe}}_{\mathcal{L}^2}(\mathbb{Z})$ *Given a system S of a finite number of diophantine equations, each of the form*

$$\sum_i \alpha_i x_i^2 + \sum_j \beta_j y_j = \gamma, \tag{2}$$

does S have an integer solution (the coefficients α_i, β_j and γ are integers and each variable y_j is distinct from each variable x_i)?

Since any integer can be written as $u^2 + v^2 - w^2$ for some integers u, v, and w, the existence of solutions for Equation (2) is equivalent to the existence of solutions for the equation

$$\sum_i \alpha_i x_i^2 + \sum_j \beta_j (u_j^2 + v_j^2 - w_j^2) = \gamma,$$

where the u_j, v_j and w_j are new variables. So we have:

$$\mathbf{T}^{\mathbf{pe}}_{\mathcal{L}^2}(\mathbb{Z}) \text{ undecidable } \iff \mathbf{DF^2}(\mathbb{Z}) \text{ undecidable.}$$

Since $\mathbf{T}^{\mathbf{pe}}_{\mathcal{L}_{\mathbf{R}}}(\mathbb{Z})$ is undecidable, in order to obtain the undecidability of $\mathbf{T}^{\mathbf{pe}}_{\mathcal{L}^2}(\mathbb{Z})$ it suffices to find an $\mathcal{L}^2$-positive-existential formula that defines multiplication, that is, a positive-existential formula of $\mathcal{L}^2$ with free variables x, y and t which is satisfied in $\mathbb{Z}$ if and only if $xy = t$.

One might think that the following observation solves the problem: since

$$4xy = (x+y)^2 - (x-y)^2$$

the formula $\Psi(x, y, t)$

$$\exists u \exists v \left((x+y)^2 = u \wedge (x-y)^2 = v \wedge 4t = u - v\right)$$

is true in $\mathbb{Z}$ if and only if $xy = t$. But this formula is not an $\mathcal{L}^2$-formula because in the language $\mathcal{L}^2$ we cannot in an obvious way express that a variable is the square of another variable. In the language $\mathcal{L}^2$, we can only, *a priori*, express that a variable is the square of *some* other element.

We observe that, over any ring of characteristic other than 2, our problem is now reduced to finding a positive-existential formula $\varphi(r, s)$ in the language $\mathcal{L}^2$ which is satisfied in $\mathbb{Z}$ if and only if $s = r^2$: if such a φ exists, then the formula

$$\exists u \exists v \left(\varphi(x+y, u) \wedge \varphi(x-y, v) \wedge 4t = u - v\right)$$

is an $\mathcal{L}^2$-formula that is satisified in $\mathbb{Z}$ if and only if $t = xy$. This is what we wanted. So

How can we find such a formula $\varphi(r, s)$?

Let us try to explain how this logical problem gives rise naturally to Büchi's n squares problem. We want to find some kind of characterization of the function $f(z) = z^2$, but we only have the right to sum and say that something is a square. If we wanted to characterize f among polynomials in $\mathbb{Z}[z]$ and if we could use derivatives with respect to z in our language, then by saying that the second derivative of f is constant and equal to 2, we would characterize f up to a degree one term:

$$\{g \in \mathbb{Z}[z] \colon g'' = 2\} = \{z^2 + az + b \colon a, b \in \mathbb{Z}\}.$$

Since we do not have derivatives, we look at the discrete analogue, taking the second difference of the sequence $(g(n))_{n \in \mathbb{Z}}$ (this is the usual way to proceed in discretization processes). It is easy to see that we have:

$$\{g \in \mathbb{Z}[z] \colon \forall n \, g(n+2) - 2g(n+1) + g(n) = 2\} = \{z^2 + az + b \colon a, b \in \mathbb{Z}\}.$$

Since we want a statement about integers and not about polynomials, we may consider sequences of values of the polynomials g. We obtain the following equalities of sets

$$\begin{aligned}&\{(u_n)_{n\in\mathbb{Z}}\colon \forall n\, u_n \in \mathbb{Z} \text{ and } u_{n+2}-2u_{n+1}+u_n=2\} =\\ &\quad\{(g(n))_{n\in\mathbb{Z}}\colon g\in\mathbb{Z}[z] \text{ and } \forall n\, g(n+2)-2g(n+1)+g(n)=2\} =\\ &\qquad\qquad\qquad\qquad\{(n^2+an+b)_{n\in\mathbb{Z}}\colon a,b\in\mathbb{Z}\}\end{aligned}$$

where the first equality can be proved by solving the recurrence $u_{n+2}-2u_{n+1}+u_n=2$ (it is actually well known that the first set is included in the second one). In order to eliminate the degree one part in the sequence $(n^2+an+b)_{n\in\mathbb{Z}}$, we consider only sequences of squares in the left hand side set. After a standard computation, we obtain:

$$\big\{(x_n^2)_{n\in\mathbb{Z}}\colon \forall n\, x_{n+2}^2-2x_{n+1}^2+x_n^2=2\big\} = \big\{((x+n)^2)_{n\in\mathbb{Z}}\colon x\in\mathbb{Z}\big\}$$

(of course one could prove this equality of sets directly, but our purpose was to show how Büchi's problem comes from the problem of Logic). We are almost ready except that we are using a universal quantifier. So the question is:

Büchi's Problem, or the n squares problem.
$\mathbf{B}^2(\mathbb{Z})$ *Does there exist a positive integer M such that any sequence of M integer squares, whose second difference is constant and equal to 2, is of the form $(x+n)^2$, $n=1,\dots,M$, for some integer x?*

If Büchi's problem has a positive answer, then it is easy to see that the $\mathcal{L}^2$-formula $\varphi(r,s)$

$$\exists u_1\cdots\exists u_M \left(\bigwedge_{i=1}^{M} P_2(u_i)\right) \wedge \left(\bigwedge_{i=1}^{M-2} u_{i+2}-2u_{i+1}+u_i=2\right) \wedge s=u_1 \wedge 2r+1=u_2-u_1$$

is satisfied in $\mathbb{Z}$ if and only if $s=r^2$. Unfortunately, Büchi's problem is still open.

5. Other rings

Observe that Büchi's problem as stated makes sense in any commutative ring A with a multiplicative unit (instead of $\mathbb{Z}$).

$\mathbf{B}^2(A)$ *Does there exist a positive integer M such that any sequence of M squares of A, whose second difference is constant and equal to 2, is of the form $(x+n)^2$, $n = 1, \dots, M$, for some $x \in A$?*

It is easy to find rings for which the answer is trivially negative. Note the following:

General Rule *If $\mathbf{B}^2(A)$ has a positive answer, then for any subring B of A, $\mathbf{B}^2(B)$ has a positive answer.*

So in particular a positive answer for $\mathbf{B}^2(A)$ for any ring A containing $\mathbb{Z}$ would imply a positive answer for $\mathbb{Z}$.

Observe first that if the ring A has characteristic 2, then $\mathbf{B}^2(A)$ has trivially a negative answer. Indeed, the system (S_M^2) gives: $x_n^2 = x_m^2$ if and only if $n - m$ is even. Hence, any constant sequence of length M will satisfy (S_M^2), and such a sequence is non-trivial.

Also, if $A = \bar{\mathbb{Q}}$ is the field of algebraic numbers, then for any M, any sequence of the form

$$\left(x_1, x_2, \sqrt{2 + 2x_2^2 - x_1^2}, \dots, x_M = \sqrt{2 + 2x_{M-1}^2 - x_{M-2}^2}\right)$$

is a solution of the system (S_M^2). Actually, $\mathbf{B}^2(\bar{\mathbb{Z}} \cap \mathbb{R})$ has a negative answer: take for example the sequence $(\sqrt{n^2+1})_{n \geq 1}$. We 'suspect' that $\mathbf{B}^2(\mathbb{Z}_p)$ (where $\mathbb{Z}_p$ is the ring of p-adic integers) has a negative answer as well.

We may distinguish two kinds of rings in which Büchi's problem has a negative answer:

- **Type 1**: Rings for which there exists an infinite non-trivial Büchi sequence.
- **Type 2**: Rings for which there exist non-trivial Büchi sequences of any length, but there is no infinite one.

All the examples we gave here are of type 1, but we believe that it is possible to cook up a ring of type 2.

Philosophy of the Problem*:*

1. *If there are too many squares in the ring, then Büchi's problem for this ring should have a negative answer.*
2. *If there are* really *too many squares in the ring, then Büchi's problem for this ring should have a negative answer of type* 1.

We suspect that, in any characteristic, the intersection of two rings for which Büchi's problem has a negative answer does not necessarily have a negative answer (the opposite would be *too nice* to be true).

Open Problem 5.1

1. *Let C be a ring of characteristic 0 and A and B be subrings of C. If $\mathbf{B}^2(A)$ and $\mathbf{B}^2(B)$ have a negative answer then does $\mathbf{B}^2(A \cap B)$ necessarily have a negative answer?*
2. *Do there exist rings A and B of type 1 whose intersection is of type 2?*

To find a counter-example to Open Problem 5.1 (1) above is harder than proving $\mathbf{B}^2(\mathbb{Z})$, because of the General Rule given above (see Section 12 for a counter-example in positive characteristic). Observe also that Open Problem 5.1 (2) makes sense only for rings of characteristic zero.

Can we find rings for which $\mathbf{B}^2(A)$ has trivially a positive answer? Let us show that $\mathbf{B}^2\,(\mathbb{Z}/4\mathbb{Z})$ has a positive answer with $M = 3$. The squares are 0 and 1. Suppose first that $x_{n+1}^2 = 0$ for some n. Then from $x_{n+2}^2 - 2x_{n+1}^2 + x_n^2 = 2$, we see that $x_{n+2}^2 = x_n^2 = 1$. Next, if for some n we have $x_{n+1}^2 = 1$ then we get $x_{n+2}^2 = x_n^2 = 0$. Hence, the only solutions of the system (S_M^2) satisfy $x_n^2 = (x+n)^2$.

In [9], Hensley proves that $\mathbf{B}^2(\mathbb{F}_p)$ has a positive answer with $M = p$. By direct computation (checking all possible cases), we see that actually $M = 4$ is enough in order to get a positive answer to $\mathbf{B}^2(\mathbb{F}_5)$ (and this M is optimal). We do not know what the optimal M is for $\mathbb{F}_p$ in general.

Lemma 5.2. *Let A and B be rings. Then $\mathbf{B}^2(A \times B)$ has a positive answer if and only if both $\mathbf{B}^2(A)$ and $\mathbf{B}^2(B)$ have a positive answer. Moreover, if $\mathbf{B}^2(A)$ has a positive answer with $M = M_A$ and $\mathbf{B}^2(B)$ has a positive answer with $M = M_B$, then $\mathbf{B}^2(A \times B)$ has a positive answer with $M = \max\{M_A, M_B\}$.*

Proof. Let M_A be such that $(S_{M_A}^2)$ has only trivial solutions in A and M_B such that $(S_{M_B}^2)$ has only trivial solutions in B. Let M be the maximum of M_A and M_B and suppose that some $\sigma = ((x_1, y_1), \dots, (x_M, y_M))$ is a solution to the system (S_M^2) in $A \times B$. Through the canonical projections $\pi_1 \colon A \times B \to A$ and $\pi_2 \colon A \times B \to B$, we get solutions $\pi_1(\sigma)$ of (S_M) in A and $\pi_2(\sigma)$ of (S_M) in B, which must be trivial by hypothesis, hence satisfying $x_n^2 = (x+n)^2$ and $y_n^2 = (y+n)^2$ for some $x \in A$ and $y \in B$. Hence σ satisfies

$$(x_n^2, y_n^2) = ((x+n)^2, (y+n)^2) = [(x, y) + n(1, 1)]^2$$

for each n.

Conversely, if for any N we can find a non-trivial sequence $(x_i)_{i=1}^N$ in A, then $((x_i, i))_{i=1}^N$ is a non-trivial sequence of length N in $A \times B$. □

From Lemma 5.2 we see that $\mathbf{B}^2(\mathbb{Z}/60\mathbb{Z})$ has a positive answer for $M = 5$ (actually $M = 4$ works and is optimal since $\mathbb{Z}/60\mathbb{Z} = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and it is optimal for all $\mathbf{B}^2(\mathbb{Z}/5\mathbb{Z})$, $\mathbf{B}^2(\mathbb{Z}/4\mathbb{Z})$ and $\mathbf{B}^2(\mathbb{Z}/3\mathbb{Z})$).

6. Hensley's problem

D. Hensley in [9] noticed that Büchi's Problem for integers could be formulated in a quite simpler way (known by people working in Difference Equations).

Much of what we will present here works for any characteristic other than 2, but for simplicity we work in zero characteristic (see Section 12 for the case of positive characteristic). Consider a solution (x_n) of the system (S_M^2) over any ring of characteristic 0. It is easy to see that the quantity

$$\mu_n = \frac{x_n^2 - x_1^2}{n-1} - (n+1) \tag{3}$$

(for $n \geq 2$) does not actually depend on n. Oberve that μ_2 belongs to the ring. Hence μ_n belongs to the ring for each n.

Assumption 6.1*Suppose that there exists $\nu \in A$ such that $\mu_n = 2\nu$.*

We get

$$x_n^2 - x_1^2 = 2(n-1)\nu + (n-1)(n+1),$$

hence

$$x_n^2 - 2\nu n - n^2 = x_1^2 - 2\nu - 1.$$

Therefore, we have

$$x_n^2 - (\nu + n)^2 = x_1^2 - (\nu + 1)^2$$

and $x_n^2 - (\nu + n)^2$ does not depend on n. Write this quantity a. If we can prove that $a = 0$ then we will have showed that all the solutions of (S_M^2) are trivial, and obtain a positive answer to $\mathbf{B}^2(A)$.

On the other hand, suppose that $\mathbf{B}^2(A)$ has a positive answer for some integer M. Any sequence of the form

$$(\nu + n)^2 + a, \quad 1 \leq n \leq M,$$

has second difference constant equal to 2. Hence, if it is a sequence of squares, then there exists $x \in A$ such that for each n

$$(\nu + n)^2 + a = (x + n)^2$$

(since $\mathbf{B}^2(A)$ has a positive answer). In particular, for $n = 1$, we have

$$\nu^2 + 2\nu + a = x^2 + 2x,$$

and for $n = 2$, we have

$$\nu^2 + 4\nu + a = x^2 + 4x.$$

Taking the difference, we obtain $\nu = x$ and conclude that $a = 0$.

This analysis leads us to the following:

Hensley's Problem:

$\mathbf{HP}_\mathbf{2}^\mathbf{2}(A)$. *Does there exist a positive integer M such that, if for some fixed elements ν and a of A the quantities*

$$(\nu + n)^2 + a$$

are squares for $n = 1, \dots, M$, then $a = 0$?

We proved in the above discussion that $\mathbf{B}^2(A)$ implies $\mathbf{HP}_\mathbf{2}^\mathbf{2}(A)$ for any ring A of characteristic 0, and that $\mathbf{B}^2(A)$ is equivalent to $\mathbf{HP}_\mathbf{2}^\mathbf{2}(A)$ for any ring A of characteristic 0 if Assumption 6.1 holds. In [16], the first author shows that this assumption holds in any ring A such that, either 2 is invertible in A, or $A/4A$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ (it comes from an easy study of cases of the system (S_M^2) modulo four).

It turns out that it is usually much easier to work with Hensley's formulation of Büchi's problem than with the original formulation by Büchi. Nevertheless, it is Büchi's formulation that is needed in order to obtain logical consequences.

7. Optimal bounds for the length of sequences

We may reformulate $\mathbf{B}^2(\mathbb{Z})$ in the following way:

$\mathbf{B}^2(\mathbb{Z})$ *Does there exist an integer M such that no M-term non-trivial Büchi sequences exist?*

D. Hensley in [10, Theorem 2.1] characterizes all the non-trivial (non-negative increasing) 3-term Büchi sequences of integers up to any fixed integer x.

Theorem 7.1 (Hensley). *Let x be a positive integer. Let σ_x be the set of all non-trivial 3-term Büchi sequences (x_1, x_2, x_3) with $0 \leqslant x_1 < x_2 < x_3 \leq x$. Let τ_x be the set of pairs (u, v) of positive integers such that*

- *u is even;*
- *u divides $v^2 - 1$;*
- *$u^2 < 2(v^2 - 1)$; and*
- *$u^2 + 4uv + 2(v^2 - 1) < 2ux$.*

The following maps

$$\begin{aligned} \sigma_x &\longrightarrow \tau_x \\ (x_1, x_2, x_3) &\mapsto (2x_2 - x_1 - x_3, x_3 - x_2) \end{aligned}$$

and

$$\begin{aligned} &\tau_x \longrightarrow \sigma_x \\ &(u, v) \mapsto \left(-\frac{u}{2} + \frac{v^2 - 1}{u}, \frac{u}{2} + v + \frac{v^2 - 1}{u}, \frac{u}{2} + 2v + \frac{v^2 - 1}{u}\right) \end{aligned}$$

are reciprocal bijections. Moreover, there exist positive constants α and β such that, for large enough x,

$$\alpha < \frac{|\sigma_x|}{x \log x} < \beta$$

where $|\sigma_x|$ stands for the cardinal of σ_x.

It seems that Büchi knew the existence of infinitely many non-trivial 4-term Büchi sequences. For example, taking the square of the sequence $\sigma = (6, 23, 32, 39)$, we get the sequence $(36, 529, 1024, 1521)$, whose first difference is the sequence $(493, 495, 497)$ and second difference is $(2, 2)$. Hence σ is a non-trivial 4-term sequence which satisfies (S_4^2).

Hensley in [10] (in a note just after the end of the proof of Theorem 2.1) indicates a way to generate infinitely many non-trivial 4-term Büchi sequences. Indeed, taking w an arbitrary positive integer, $u = w + 3$ and $v = 2w^2 + 6w + 1$, the sequence

$$\begin{aligned} x_1 &= \frac{v^2 - 1}{2u} - u \\ x_2 &= x_1 + 2u + v \\ x_3 &= x_2 + v \\ x_4 &= x_3 + v - 2w \end{aligned}$$

is a non-trivial 4-term Büchi sequence. Hensley then observes that since x_4 is a degree 3 polynomial in w, there exists a constant α such that, for any x large enough, at least $\alpha x^{\frac{1}{3}}$ non-trivial 4-term Büchi sequences exist.

We do not know whether or not there exists *any* non-trivial 5-term Büchi sequence of integers. In this direction, R. G. E. Pinch in [Pinch] proved that 'many' non-trivial 4-term Büchi sequences cannot be extended to 5-term Büchi sequences. Actually the original problem posed by Büchi was:

Open Problem 7.2*Does there exist a non-trivial* 5*-term Büchi sequence?*

8. Büchi's problem with constant $\neq 2$

Various researchers (Allison [1] in 1986, Pinch [23] in 1993, Bremner [2] in 2003, and Browkin and Brzezinski [4] in 2006) have been studying the following problem:

A Generalized Büchi's Problem for Squares:
$\mathbf{B}^2(\mathbb{Z}, \ell)$ *Does there exist an integer M such that the system of equations*

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

where $\ell \in \mathbb{Z}$, has only solutions whose squares are the squares of an arithmetic progression (other types of solutions are called non-trivial)?

We refer to Browkin and Brzezinski [4] for a general survey of results in this direction.

Changing the constant 2 of the original problem seems to be related to $\mathbf{B}^2(K)$ where $K/\mathbb{Q}$ is a finite extension. For example, solving the system of equations

$$x_{n+2}^2 - 2x_{n+1}^2 + x_n^2 = 3, \quad n = 1, \ldots, M-2$$

over $\mathbb{Z}$ is equivalent to solving the system

$$\left(\sqrt{\frac{2}{3}}x_{n+2}\right)^2 - 2\left(\sqrt{\frac{2}{3}}x_{n+1}\right)^2 + \left(\sqrt{\frac{2}{3}}x_n\right)^2 = 2, \quad n = 1, \ldots, M-2$$

over $\mathbb{Z}$.

9. Number fields

In 2001, P. Vojta gave a new piece of evidence for $\mathbf{B}^2(\mathbb{Z})$ (actually even for $\mathbf{B}^2(\mathbb{Q})$) to have a positive answer, under the assumption that the following (open) question by Bombieri would have a positive answer:

Bombieri's Question
Let X be a smooth projective algebraic variety of general type, defined over a number field k. Does there exist a proper Zariski-closed subset Z of X such that $X(k) \subseteq Z$?

Using Bogomolov theory, Vojta is then able to show:

Theorem 9.1 (Vojta [29]). *If Bombieri's Question has a positive answer, then there are only finitely many non-trivial 8-term Büchi sequences of rational numbers.*

So if Bombieri's question had a positive answer, then Vojta's theorem would imply in particular that $\mathbf{B}^2(\mathbb{Z})$ would have a positive answer for *some* $M \geq 8$.

We present here a sketch of the proof of Vojta. Note that the proof works for any number field K just by replacing $\mathbb{Q}$ by K in the proof (this was first noted by Yamagishi [30]).

Sketch of the proof of Vojta's result. Let $X_2 = \mathbb{P}^2_{\mathbb{C}}$ and for $n > 2$ define $X_n \subset \mathbb{P}^n_{\mathbb{C}}$ to be the complete intersection surface

$$\begin{cases} x_3^2 - 2x_2^2 + x_1^2 = 2x_0^2 \\ x_4^2 - 2x_3^2 + x_2^2 = 2x_0^2 \\ \vdots \\ x_n^2 - 2x_{n-1}^2 + x_{n-2}^2 = 2x_0^2. \end{cases}$$

The variety X_n is smooth with canonical sheaf $\mathcal{O}_{X_n}(n-5)$. This says that X_n is of general type for $n \geqslant 6$. Since $[0 : \cdots : 0 : 1] \notin X_n$ for $n > 2$, the rational map

$$[x_0 : x_1 : \cdots : x_n] \mapsto [x_0 : x_1 : \cdots : x_{n-1}]$$

defines a morphism $\pi_n : X_n \to X_{n-1}$ of degree 2, ramified along the smooth curve

$$C_n = X_n \cap \{x_n = 0\}.$$

Given an algebraic complex surface X, an invertible sheaf L on X and a section

$$\omega \in H^0(X_2, L \otimes S^2(\Omega^1_{X_2}))$$

we say that a curve $Y \subseteq X$ with normalization $i : \tilde{Y} \to Y$ is *ω-integral* if the pull-back $i^*\omega$ vanishes identically on $\tilde{Y}$. Note that the condition of being an ω-integral curve, locally requires Y to be a solution of a certain differential equation on each affine chart of X. A standard computation shows that the form

$$\omega = x_1x_2dx_1 \otimes dx_1 + (1 - x_1^2 - x_2^2)dx_1 \otimes dx_2 + x_1x_2dx_2 \otimes dx_2 \qquad (4)$$

extends to a section

$$\omega_2 \in H^0(X_2, \mathcal{O}_{X_2}(5) \otimes S^2(\Omega^1_{X_2})).$$

The condition of being an ω_2-integral curve becomes locally equivalent to the condition of being the solution of the differential equation that comes from expressing one affine coordinate in terms of the other in Equation (4). So, the only ω_2-integral curves on X_2 are:

- the 4 *trivial lines* $\pm x_1 = \pm x_2 - x_0$;
- the 3 lines at infinity $x_0 = 0$, $x_1 = 0$ and $x_2 = 0$; and
- some smooth conics.

For $n > 2$, call $R_n \subseteq X_n$ the union of C_n and the pull-back of each C_k via

$$\pi_{k+1} \circ \pi_{k+2} \circ \cdots \circ \pi_n,$$

for $3 \leqslant k < n$. Let ω_n be the pull-back of ω_2 to X_n via the π_k. A crucial part of the proof is that one can find a section

$$\omega'_n \in H^0(X_2, \mathcal{O}(7 - n) \otimes S^2(\Omega^1_{X_2}))$$

such that the ω_n-integral curves and the ω'_n-integral curves are the same out of the set R_n. One can show that each ω_n-integral curve on X_n is the pull-back via the π_k of some ω_2-integral curve on X_n. Hence if $Y \subseteq X_n$ is a ω'_n-integral curve, then Y lies

(a) above a trivial line of X_2: in this case Y is one of the 2^n *trivial lines*

$$\pm x_1 = \pm x_2 - x_0 = \cdots = \pm x_n - nx_0; \text{ or}$$

(b) above a line at infinity of X_2; or

(c) above a smooth conic in X_2; or

(d) in R_n.

If $n \geqslant 8$ then the only case when the ω'_n-integral curve Y has genus at most 1 is case (a) (this is done by applying the Riemann–Hurwitz formula to the composition of the maps π_k). Moreover, one can show that for $n \geqslant 8$, *the* 2^n *trivial lines are the only curves on* X_n *with genus at most* 1. Indeed, it is enough to show that a curve $Y \subseteq X_n$ with genus at most 1 must be ω'_n-integral. If we write $i : \tilde{Y} \to Y$ for the normalization of Y, then

$$i^*\omega'_n \in H^0(X_n, i^*\mathcal{O}_{X_n}(7-n) \otimes \mathcal{K}_{\tilde{Y}}^{\otimes 2})$$

must vanish identically because the degree of $i^*\mathcal{O}_{X_n}(7-n)$ is negative for $n \geqslant 8$ and the degree of $\mathcal{K}_{\tilde{Y}}^{\otimes 2}$ is at most 0 (note that the genus of $\tilde{Y}$ is at most 1).

Let us now prove the theorem. Assuming a positive answer to Bombieri's Question for X_8, there exists a proper Zariski-closed set $Z \subseteq X_8$ which contains all the $\mathbb{Q}$-rational points of X_8. Such a set Z is a finite collection of curves and points. Hence, by Falting's theorem, the set of $\mathbb{Q}$-rational points lies (up to a finite number of them) in the union of all the curves with genus at most 1, that is, the 2^8 trivial lines. The points on trivial lines correspond to the trivial solutions of the Büchi system of equations, and the other ones to non-trivial solutions. Thus we get only a finite number of trivial solutions for $n = 8$. Each of them can be extended only to a solution of finite length because all their subsequences of lenght 8 are already counted. So we can conclude by taking M large enough. □

In 2009, the first author [17] adapted Vojta's method in order to obtain the following result (for number fields) on representation of squares by quadratic polynomials:

Theorem 9.2. *If Bombieri's Question has a positive answer, then there exists an absolute constant N (that can be chosen to be 9 if Bombieri's question is true for any surface) such that, for each number field $K/\mathbb{Q}$ and each set $\{a_1, \dots, a_N\}$ of N elements in K, there is only a finite number of polynomials $f = x^2 + ax + b \in K[x]$ not of the form $f = (x+c)^2$, satisfiying that $f(a_i)$ are squares in K for each i.*

Corollary 9.3. *Let K be a number field. If Bombieri's Question has a positive answer, then the positive existential theory of K in $\mathcal{L}^2$ is undecidable if and only if the positive existential theory of K in the language of rings is undecidable.*

For a survey of results about Hilbert's Tenth Problem for number fields, see for example [25].

10. Rings of functions in characteristic 0

Consider a ring of polynomials $A[z]$ over the ring A. Since the recurrence relation (S_M^2) defining Büchi sequences has coeficients in the prime subring of A, from any Büchi sequence (x_n) of $A[z]$ we may obtain a Büchi sequence in A, by evaluating the independent variable z at any point of A. Thus we cannot hope to solve Büchi's problem for the ring $A[z]$ if we do not know how to solve it for A. But it still makes sense to ask whether there are non-trivial Büchi sequences in $A[z]$, other than those that may possibly be in A. Therefore, we ask whether there exist non-trivial Büchi sequences (x_n) in $A[z]$ such that at least one of the x_n is non-constant.

Büchi's Problem for rings of functions:
$\mathbf{B}^2(A_z)$ *Does there exist an integer M such that any sequence of M squares in A_z, not all constant, whose second difference is constant and equal to 2, is of the form $(x+n)^2$, $n = 1, \dots, M$, for some $x \in A_z$?*

In this context, *Büchi sequences* will refer to Büchi sequences having at least one non-constant term.

In the case of rings of functions of characteristic 0, Hensley's problem becomes:

Hensley's Problem for a ring of functions in the variable z:
$\mathbf{HP_2^2}(A_z)$ *Does there exist an integer M such that, if for some fixed element ν of A_z, the quantities*

$$(\nu + n)^2 + a$$

are all squares for $n = 0, \dots, M-1$ (and not all constant), then $a = 0$?

It is easy to see that the proof given at the beginning of Section 6 is still valid and shows that if Assumption 6.1 holds in A_z then $\mathbf{B}^2(A_z)$ is equivalent to $\mathbf{HP}_2^2(A_z)$.

The first positive answer to this question was given by P. Vojta in 2001 [29]. He used Nevanlinna theory and Algebraic Geometry in order to prove that Büchi's problem for the field of complex meromorphic functions has a positive answer for $M = 8$. In the same article, he obtained a positive answer for function fields of curves of characteristic 0 (in this case the bound M depends on the genus) – see [7, 15] and [25] for results on

Hilbert's tenth problem for function fields. In particular this solves positively $\mathbf{B}^2(F(z))$ for any rational function field over a field of characteristic zero.

In 2006, the second and third authors [19] developed an elementary method to solve $\mathbf{B}^2(F(z))$ that has the advantage to be adaptable to various other structures (as well as to Büchi's problem for higher powers and to the case of positive characteristic – see Sections 11 and 12), but does not give usually bounds as good as Vojta's ($M = 14$ for polynomial rings and $M = 18$ for rational function fields).

In 2009, the third author together with A. Shlapentokh proved that this method is adaptable to any algebraic function field of characteristic 0 (see [26]).

The first author showed that the same method (using Nevanlinna theory) can be adapted to prove that Büchi's problem for the field $\mathcal{M}_z(\mathbb{C}_p)$ of p-adic complex meromorphic functions has a positive answer for $M = 42$ (see [17], 2009). This improves the undecidability results in [12] by Lipshitz and the second author, and in [28] by the third author.

In all known cases, whenever $\mathbf{B}^2(A)$ has a positive answer for an integral domain A, we can adapt the proof to the field of fractions of A. So we wonder:

Open Problem 10.1. *Let A be an integral domain and K be its field of fractions. Assume that $\mathbf{B}^2(A)$ has a positive answer. Does it follow that $\mathbf{B}^2(K)$ has a positive answer as well?*

Let us now give a sketch of the method in the simplest case, the case of the polynomial ring $\mathbb{C}[z]$ (see [19]).

$\mathbf{B}^2(\mathbb{C}[z])$ has a positive answer.
Suppose that we have a system of $M = 14$ equations

$$u_n = (\nu + n)^2 + a, \quad n = 1, \ldots, 14 \tag{5}$$

where $u_n = x_n^2$. Taking derivatives we obtain:

$$u_n' = 2\nu'\nu + 2n\nu' + a'. \tag{6}$$

Plugging the expression for n obtained from (6) into (5), we obtain

$$4\nu'^2 u_n = (2\nu'\nu + u_n' - a' - 2\nu'\nu)^2 + 4\nu'^2 a$$

which simplifies into

$$4{\nu'}^2 u_n = (u_n' - a')^2 + 4{\nu'}^2 a.$$

Hence the quantity

$$\begin{aligned} 4{\nu'}^2 a + {a'}^2 &= 4{\nu'}^2 u_n - {u_n'}^2 + 2u_n' a' \\ &= x_n \left(4{\nu'}^2 x_n - 4{x_n'}^2 x_n + 4x_n' a'\right) = x_n \Delta_n \qquad (7) \end{aligned}$$

does not depend on n (recalling that $u_n = x_n^2$). Therefore, x_n divides $4{\nu'}^2 a + {a'}^2$ for all n.

We will now show that any three distinct x_n have to be coprime. Consider three distinct equations from System (5):

$$u_n = (\nu + n)^2 + a, \quad u_m = (\nu + m)^2 + a, \quad u_r = (\nu + r)^2 + a$$

and suppose that for some $z_0 \in \mathbb{C}$ we have $u_n(z_0) = u_m(z_0) = u_r(z_0) = 0$. Hence the degree 2 polynomial equation

$$(\nu(z_0) + X)^2 + a(z_0) = 0$$

has three distinct roots, which is impossible.

Since the x_n are coprime in triples, the degree of their least common multiple increases as M increases. One can show that if $M \geq 14$ then the degree of the least common multiple of the x_n will be higher than the degree of $4{\nu'}^2 a + {a'}^2$, getting a contradiction unless $\Delta_n = 0$ by Equation (7).

At this stage, we still have to solve the differential equation given by (7)

$$4{\nu'}^2 a + {a'}^2 = 0. \qquad (8)$$

First observe that ν cannot be a constant (we could have proven this from the beginning, but it would not easily generalize to other rings). Indeed, if it were constant then a would be constant, hence every x_n would be constant, which would contradict the hypothesis.

From Equation (8) we see that a has to be a square, say $a = \alpha^2$, so the equation can be written as:

$$4{\nu'}^2 \alpha^2 + 4{\alpha'}^2 \alpha^2 = 0,$$

and we deduce that $\alpha = 0$ or ${\nu'}^2 + {\alpha'}^2 = 0$.
Case 1: $\alpha \neq 0$. We have then

$$\nu = \varepsilon i \alpha + K$$

for some constant $K \in \mathbb{C}$ and $\varepsilon = \pm 1$. Note that we have

$$a = \alpha^2 = \left(\frac{\nu - K}{\varepsilon i}\right)^2 = -(\nu - K)^2,$$

hence from Equations (5), we get

$$x_n^2 = (\nu + n)^2 - (\nu - K)^2 = (n + K)(2\nu + n - K).$$

If $n \neq -K$, write

$$y_n^2 = \left(\frac{x_n}{\sqrt{n + K}}\right)^2 = 2\nu + n - K. \tag{9}$$

Choose three distinct indices n, m and r, all distinct from $-K$.
First way (generalizes to various fields): Writing

$$(y_n y_m y_r)^2 = (2\nu - K + n)(2\nu - K + m)(2\nu - K + r),$$

we obtain a (non-constant) rational parametrization of the elliptic curve

$$Y^2 = (X + n)(X + m)(X + r),$$

which is impossible.
Second way (generalizes to higher powers): Considering

$$(y_n - y_m)(y_n + y_m) = y_n^2 - y_m^2 = n - m \neq 0$$

we see that both $y_n - y_m$ and $y_n + y_m$ are constant polynomials. Therefore, y_n is a constant polynomial, which contradicts the fact that ν is non-constant (by Equation (9)).

Case 2: $\alpha = 0$. In this case we also have $a = \alpha^2 = 0$. Hence $x_n^2 = (\nu + n)^2$ for all n, which means that the sequence (x_n) is a trivial Büchi sequence. □

Note: The first author in [16] shows how to get a contradiction in Case 1, without the use of elliptic curves. Instead, he shows that the greatest common divisor of the $x_n' x_n$ cannot have too high degree (here we showed that the least common multiple of the x_n cannot have a degree that is too small). This combinatorial argument that avoids the use of elliptic curves turned out to be essential in order to make the method work for other rings of functions.

11. Higher powers

Since Büchi's problem is about the second difference of sequences of squares, it is quite natural to study the kth difference of a sequence of kth powers for any $k \geq 2$, or to study the positive existential theory of a ring over the language $\mathcal{L}_k = \{0, 1, +, P_k\}$, where P_k is a unary predicate that stands for 'x is a kth power'. Let A be a ring.

Büchi's Problem for kth Powers:
$\mathbf{B}^k(A)$ *Does there exist an integer M such that any sequence of length M consisting of kth powers of A, whose kth difference is constant and equal to $k!$, is of the form $(x+n)^k$, $n = 1, \dots, M$, for some $x \in A$?*

The only result we know so far was obtained in 2008 by the second and the third authors in [21]: $\mathbf{B}^3(\mathbb{C}[z])$ has a positive answer with $M = 92$ (as in the case of squares, the sequences considered have at least one non-constant term). The method used is a quite tricky adaptation of the method presented in Section 10 (using a 'cubic version' of Hensley's problem – see below). We do not know whether the proof can be adapted to one that would work *uniformly* for any power, as it seems that the number of cases to study increases with k. But it probably can be adapted to $k = 4$, $k = 5$ etc.

It is not hard to show that Hensley's problem for squares has a 'kth power version'.

Hensley's Problem for Higher Powers:
$\mathbf{HP}_k^k(A)$ *Does there exist a positive integer M such that, for any fixed elements ν and $a_0, \dots, a_{k-2}$ of A, if the quantities*

$$(\nu + n)^k + a_{k-2}n^{k-2} + \cdots + a_1 n + a_0$$

are kth powers in A for $n = 1, \dots, M$, then $a_0 = \cdots = a_{k-2} = 0$?

For any ring, if $\mathbf{B}^k(A)$ has a positive answer then $\mathbf{HP}_k^k(A)$ has a positive answer. We do not know under which conditions the reciprocal is true (we know only that it is true in the case $k = 3$ for polynomial rings in characteristic zero – see [21]).

The following Lemma is proved in the same way as Lemma 5.2.

Lemma 11.1. *Let A and B be rings. Then $\mathbf{B}^k(A \times B)$ has a positive answer if and only if $\mathbf{B}^k(A)$ and $\mathbf{B}^k(B)$ have a positive answer. Moreover, if $\mathbf{B}^k(A)$ has a positive answer with $M = M_A$ and $\mathbf{B}^k(B)$ has a positive* *answer with $M = M_B$, then $\mathbf{B}^k(A \times B)$ has a positive answer with $M = \max\{M_A, M_B\}$.*

For the moment it seems too hard to solve Büchi's problem for kth powers in general, but still, there is another indication that it should have a positive answer in fields of functions or at least in polynomial rings. Let A be a ring.

Hensley's Problem for ℓ and k:
$\mathbf{HP}^k_\ell(A)$. *Let ℓ be an integer such that $2 \leq \ell \leq k$. Does there exist a positive integer M such that, if for some fixed elements ν and $a_0, \dots, a_{\ell-2}$ of A the quantities*

$$(\nu + n)^k + a_{\ell-2}n^{\ell-2} + \ldots + a_1 n + a_0$$

are kth powers for $n = 1, \dots, M$, then $a_0 = \cdots = a_{\ell-2} = 0$?

In [16], the first author proved that $\mathbf{HP}^k_2(\mathbb{C}[z])$ has a positive answer. He essentially used the method presented in Section 10 to solve $\mathbf{B}^2(\mathbb{C}[z])$ (but the part of the method using elliptic curves had to be modified). So it is rather likely that combining the method used in [21] for $\mathbf{B}^3(\mathbb{C}[z])$ with the method used in [21] for $\mathbf{HP}^k_2(\mathbb{C}[z])$ should allow one to prove that $\mathbf{HP}^k_3(\mathbb{C}[z])$ has a positive answer.

From the point of view of Logic, one may consider the following generalization of the problem $\mathbf{DF}^2(\mathbb{Z})$ to any ring A of characteristic 0 and to higher powers:

Simultaneous Representation of Elements of the Prime Subring by Diagonal Forms of Degree k
$\mathbf{DF}^k(A)$ *Is there an algorithm to decide whether a system of a finite number of equations, each of the form*

$$\sum_i \alpha_i x_i^k = \gamma,$$

where α_i and γ are elements of the prime subring of A, has a solution in A?

In [21], the second and third authors observe that if $\mathbf{B}^3(\mathbb{Z})$ has a positive answer then $\mathbf{DF}^3(\mathbb{Z})$ has a positive answer (the same statement would be true with $\mathbb{Q}$ instead of $\mathbb{Z}$ if Hilbert's Tenth Problem for $\mathbb{Q}$ were solved negatively). This is actually true for any power $k \geq 3$ because the $(k-1)$th difference of a sequence of the form $((x+1)^k, \dots, (x+k-1)^k)$ is of the form $a(x+1)+b$ for some $a, b \in \mathbb{Z}$, so that we can apply the same trick as for squares. So suppose that $\mathbf{B}^k(\mathbb{Z})$ has a positive answer for some M. The following formula $\varphi^k(r, s)$

$$\exists u_1 \cdots \exists u_M \left(\bigwedge_{i=1}^{M} P_k(u_i) \right) \wedge \Delta^{(k)}((u_1, \dots, u_M)) = (k!) \wedge s = u_1$$
$$\wedge\, ar + b = \Delta^{(k-1)}((u_1, \dots, u_k))$$

is true in $\mathbb{Z}$ if and only if $s = r^k$.

In relation to $\mathbf{B}^k(A)$, Problem $\mathbf{DF}^k(A)$ has a different statement in the case of a ring of functions. Let A_z be a ring of functions in the variable z.

Simultaneous Representation Problem for Rings of Functions $\mathbf{DF}^k(A_z)$ *Let B be the prime subring of A_z. Is there an algorithm to decide whether a system of a finite number of diophantine equations, each of the form*

$$\sum_i \alpha_i x_i^k = \gamma,$$

where $\alpha_i, \gamma \in B[z]$, and with conditions of the form "x_i is non-constant", has a solution in A_z?

Open Problem 11.2. *Is it always true that if $\mathbf{B}^k(A)$ has a positive answer and $\mathbf{T}^{\mathbf{pe}}_{\mathcal{L}_{\mathbf{R}}}(A)$ is undecidable then $\mathbf{DF}^k(A)$ is undecidable?*

12. Positive characteristic

All rings in this section have characteristic $c > 2$ not necessarily prime.

We carefully avoided up to this point the case of rings of positive characteristic. This is because there are at least two *special* phenomena that occur in this case.

The first phenomenon is the following: if $M > c$, then the system (S_M^2) is equivalent to the system (S_c^2). The reason is that by solving the recurrence formally we get:

$$x_n^2 = (2-n)x_1^2 + (n-1)x_2^2 + (n-1)(n-2)$$

for all $n = 1, \dots, M$, and so we have $x_n^2 = x_{n+c}^2$ for all n. So we should change the formulation of Büchi's problem in this context. Let A be a ring.

Büchi's Problem for Squares in Positive Characteristic:
$\mathbf{B}^2(A)$ *Does there exist an integer $M \leq c$ such that any sequence of M squares of A, whose second difference is constant and equal to 2, is of the form $(x+n)^2$, $n = 1, \dots, M$, for some $x \in A$?*

Also Hensley's formulation becomes:

Hensley's Problem in Positive Characteristic:
$\mathbf{HP}_2^2(A)$ *Does there exist an integer $M \leq c$ such that, if for some fixed elements ν and a of A the quantities*

$$(\nu + n)^2 + a$$

are squares for $n = 1, \dots, M$, then $a = 0$?

It is easy to see that if c is prime then: if $\mathbf{HP}_2^2(A)$ has a positive answer then $\mathbf{B}^2(A)$ has a positive answer (the proof is as in Section 6).

Let us use Hensley's formulation in order to get a simple proof of the fact that $\mathbf{B}^2(\mathbb{F}_p)$ has a positive answer (this result was first obtained by Hensley in [9] using the original formulation by Büchi).

Proposition 12.1. *If $p > 2$ then $\mathbf{B}^2(\mathbb{F}_p)$ has a positive answer with $M = p$.*

Proof. Let $p > 2$ be a prime and assume that we have some $\nu, a \in \mathbb{F}_p$ such that $(\nu+n)^2 + a$ is a square for $n = 1, 2, \dots, p$. Call R the set of the $\frac{p+1}{2}$ squares in $\mathbb{F}_p$. Therefore we have $R + a = R$. Then for any $m \in \mathbb{F}_p$, we have $R + ma = R + a + \cdots + a = R$. Hence if $a \neq 0$, then R covers the whole of $\mathbb{F}_p$, which is impossible. Therefore we have $a = 0$. □

The second special phenomenon comes from the following observation which was made by the first author in January 2009: Let A be a ring of characteristic $p > 2$ and let $x \in A$. Consider the sequence (x_n) given by

$$x_n = (x+n)^{\frac{p^s+1}{2}}.$$

Then we have

$$\begin{aligned} x_n^2 &= (x+n)^{p^s+1} \\ &= (x+n)^{p^s}(x+n) \\ &= (x^{p^s}+n)(x+n) \\ &= \left(\frac{x^{p^s}+x}{2} + n\right)^2 - \left(\frac{x^{p^s}-x}{2}\right)^2. \end{aligned}$$

Hence if

Condition (C) *there exists* $x \in A$ *and a positive integer* s *such that* $x^{p^s} \neq x$

is satisfied in A then the sequence (x_n^2) is of the form $(x+n)^2 - a$ for some non-zero a, which implies that $\mathbf{HP}_2^2(A)$ (hence also $\mathbf{B}^2(A)$) has a negative answer.

In particular this remark allows us to give a negative answer to the analogue of Open Problem 5.1 (1) in the case of positive characteristic:

- Condition (C) holds in $\mathbb{F}_{p^r}$ if $r > 1$ (taking $s = 1$ and $x \notin \mathbb{F}_p$) hence $\mathbf{B}^2(\mathbb{F}_{p^r})$ has a negative answer for $r > 1$.
- If r and t are coprime then $\mathbb{F}_{p^r} \cap \mathbb{F}_{p^t} = \mathbb{F}_p$ (we may see these fields in the algebraically closure of $\mathbb{F}_p$).
- By Proposition 12.1, $\mathbf{B}^2(\mathbb{F}_p)$ has a positive answer.

In the case of a ring of functions A_z in the variable z, one can always choose $x = z$ and $s = 1$ for Condition (C) to hold. Hence, in this situation Büchi's problem, in order not to be trivial, should be:

Büchi's Problem for Rings of Functions of Characteristic $p > 0$**:** $\mathbf{B}^2(A_z)$ *Does there exist an integer* $M \leq p$ *such that any* M*-term Büchi sequence* (x_n) *of elements of* A_z *(with at least one* x_n *non-constant), satisfies* $x_n^2 = (x+n)^{p^s+1}$, $n = 1, \dots, M$, *for some* $x \in A_z$ *and some* $s \in \mathbb{N}$*?*

In [20], the second and third authors prove that $\mathbf{B}^2(F(z))$ has a positive answer (here F is any field of characteristic ≥ 19). Fortunately, this is enough in order to prove that the positive existential theory of such fields $F(z)$ over $\mathcal{L}_z^2$ is undecidable whenever it is undecidable over $\mathcal{L}_z$.

In [26], A. Shlapentokh and the third author prove that $\mathbf{HP}_2^k(K)$ has a positive answer for any function field K (of a curve) of characteristic $\geq \alpha g + \beta$, where g is the genus of K, α and β are computable constants, and with $M \geq \alpha g + \beta$.

13. To be done

In this section we list a number of open problems:

1. Solve $\mathbf{B}^2(\mathcal{O}_K)$ for any number field K (where $\mathcal{O}_K$ denotes the ring of integers of K).
2. Let K be the field of fractions of a domain A. Solve $\mathbf{B}^2(K)$ whenever $\mathbf{B}^2(A)$ has a positive answer.
3. Let K be the field of fractions of a domain A. Is it always true that if $\mathbf{B}^2(A)$ has a positive answer then $\mathbf{B}^2(K)$ has a positive answer?

4. Solve $\mathbf{B}^k(A)$ for any k, whenever $\mathbf{B}^2(A)$ has a positive answer. So at the moment and in order of difficulty: polynomial rings, rational function fields, function fields and meromorphic functions (over $\mathbb{C}$ and $\mathbb{C}_p$).
5. Solve $\mathbf{HP}^k_\ell(A)$ for all k whenever $\mathbf{B}^\ell(A)$ has a positive answer.
6. Find a ring A for which $\mathbf{B}^2(A)$ has a negative answer, but where no infinite non-trivial Büchi sequence exists.
7. Solve $\mathbf{DF}^k(A)$ for all rings for which the corresponding Büchi's Problem has a positive answer.
8. Show that if $\mathbf{B}^k(A)$ has a positive answer and Hilbert's Tenth Problem for A has a negative answer then $\mathbf{DF}^k(A)$ is undecidable.
9. Find the optimal M whenever $\mathbf{B}^k(A)$ has a positive answer.

References

1. D. Allison, *On square values of quadratics.* — Math. Proc. Camb. Philos. Soc. **99-3**, (1986), 381–383.
2. A. Bremner, *On square values of quadratics.* — Acta Arith. **108-2** (2003), 95–111.
3. J. L. Britton, *Integers solutions of systems of quadratic equations.* — Math. Proc. of the Cambridge Phil. Soc. **86** (1979), 385–389.
4. J. Browkin and J. Brzeziński, *On sequences of squares with constant second differences.* — Canad. Math. Bull. **49-4** (2006), 481–491.
5. M. Davis, *Hilbert's tenth problem is unsolvable.* — Amer. Math. Monthly **80** (1973), 233–269.
6. J. Denef, *The Diophantine Problem for polynomial rings and fields of rational functions.* — Trans. Amer. Math. Soc. **242** (1978), 391–399.
7. J. Denef, L. Lipshitz, T. Pheidas, J. Van Geel (Eds.), *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry, Ghent 1999*, Contemporary Mathematics **270** (2000).
8. F. Grunewald and D. Segal, *How to solve a quadratic equation in integers.* — Math. Proc. Cambridge Philosophical Soc. **89** (1981), 1–5.
9. D. Hensley, *Sequences of squares with second difference of two and a problem of logic*, unpublished (1980-1983).
10. D. Hensley, *Sequences of squares with second difference of two and a conjecture of Büchi*, unpublished (1980-1983).
11. L. Lipshitz, *Quadratic forms, the five square problem, and diophantine equations.* — In: The collected works of J. Richard Büchi (S. MacLane and Dirk Siefkes, eds.) Springer, (1990), 677–680.
12. L. Lipshitz and T. Pheidas, *An analogue of Hilbert's tenth problem for p-adic entire functions.* — J. Symb. Logic **60-4** (1995), 1301–1309.
13. Ю. В. Матиясевич (Yu. Matiyasevic), *Диофантовость перечислимых множеств.* — Доклады АН СССР **191** (1970), 279–282; English translation: Enumerable sets are diophantine. — Soviet Mathematics Doklady **11** (1970), 354–358.
14. B. Mazur, *Questions of decidability and undecidability in number theory.* — J. Symbolic Logic **59-2** (1994), 353–371.

15. L. Moret-Bailly and A. Shlapentokh, *Diophantine Undecidability of Holomorphy Rings of Function Fields of Characteristic Zero.* — Annales de l'Institut Fourier **59-5** (2009), 2103–2118.
16. H. Pasten, *An extension of Büchi's Problem for polynomial rings in zero characteristic.* — Proc. Amer. Math. Soc. **138** (2010), 1549–1557.
17. H. Pasten, *Representation of squares by monic second degree polynomials in the field of p-adic meromorphic functions*, `arXiv:1003.1969`.
18. T. Pheidas and X. Vidaux, *Extensions of Büchi's problem : Questions of decidability for addition and nth powers.* — Fundamenta Mathmaticae **185** (2005), 171–194.
19. T. Pheidas and X. Vidaux, *The analogue of Büchi's problem for rational functions.* — J. London Math. Soc. **74-3** (2006), 545–565.
20. T. Pheidas and X. Vidaux, *Corrigendum: The analogue of Büchi's problem for rational functions*, to appear in t he Journal of the London Mathematical Society (2010).
21. T. Pheidas and X. Vidaux, *The analogue of Büchi's problem for cubes in rings of polynomials.* — Pacific J. Math. **238-2** (2008), 349–366.
22. T. Pheidas and K. Zahidi, *Undecidable existential theories of polynomial rings and function fields.* — Commun. Algebra **27-10** (1999), 4993–5010.
23. R. G. E. Pinch, *Squares in Quadratic Progression.* — Math. Comput. **60-202** (1993), 841–845.
24. B. Poonen, *Hilbert's Tenth Problem over rings of number-theoretic interest*, downloadable from `http://math.mit.edu/~poonen/papers/aws2003.pdf`.
25. A. Shlapentokh, *Hilbert's tenth problem – Diophantine classes and extensions to global fields.* — Cambridge Univ. Press, New Mathematical Monographs **7** (2007).
26. A. Shlapentokh and X. Vidaux *The analogue of Büchi's problem for function fields*, `arXiv:1004.0731v1`.
27. Th. Skolem, *Diophantische Gleichungen*, Ergebnisse d. Math. u. Ihrer Grenzgebiete, Bd. 5, Julius Springer (1938).
28. X. Vidaux, *An analogue of Hilbert's tenth problem for fields of meromorphic functions over non-Archimedean valued fields.* — J. Number Theory **101-1** (2003), 48–73.
29. P. Vojta, *Diagonal quadratic forms and Hilbert's Tenth Problem.* — Contemporary Math. **270** (2000), 261–274.
30. H. Yamagishi, *On the solutions of certain diagonal quadratic equations and Lang's conjecture.* — Acta Arithmetica **109-2** (2003), 159–168.

Universidad de Concepción
E-mail: hpasten@udec.cl

University of Crete
E-mail: pheidas@math.uoc.gr

Universidad de Concepción
E-mail: hpasten@udec.cl

Поступило 2 июня 2010 г.