UNIVERSIDAD DE CONCEPCIÓN
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
PROGRAMA DE MAGISTER EN MATEMATICA - ACADÉMICO

Extensiones del problema de Büchi a distintas estructuras y potencias más altas

Profesor Guía: Xavier Vidaux Negre
Codirector: Antonio Laface
Dpto. de Matemáticas
Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Tesis para ser presentada a la Dirección de Postgrado de la Universidad de Concepción

HÉCTOR HARDY PASTÉN VÁSQUEZ
CONCEPCIÓN-CHILE
2010

Agradezco a mi familia, amigos, y profesores del
Departamento de Matemática quienes hicieron
posible la elaboración de esta Tesis.

Tesis de Magister

Título: *Extensiones del problema de Büchi a distintas estructuras y potencias más altas*

Héctor Pastén Vásquez

Índice general

Capítulo 1

Presentación

1.1. Introducción

En 1900 Hilbert propuso el problema de encontrar un algoritmo para decidir si dada una ecuación polinomial con coeficientes enteros, ella posee o no soluciones enteras. Este problema, conocido como el Décimo Problema de Hilbert (el cual denotamos H10), fue resuelto por Matiyasevich 70 años más tarde [16] concluyendo un trabajo desarrollado principalmente por M. Davis, H. Putnam y J. Robinson. El resultado obtenido fue que en realidad no existe tal algoritmo. En realidad se demostró algo mucho más fuerte: "los conjuntos recursivamente enumerables (i.e. listables por una máquina de Turing) de $\mathbb{Z}$ son diofantinos". En consecuencia, la teoría positiva existencial de $\mathbb{Z}$ es indecidible en el lenguaje de anillos $\{0, 1, +, \cdot\}$.

Notación 1.1.1 *En adelante, si $\mathcal{L}$ es un lenguaje y M es una $\mathcal{L}$-estructura, entonces* $\mathrm{TPE}(M, \mathcal{L})$ *es la teoría positiva existencial de M sobre $\mathcal{L}$ (i.e.: el conjunto de todos los enunciados que se pueden expresar en el lenguaje $\mathcal{L}$ sin cuantificador universal ni negación).*

A partir de H10 aparecen dos problemas naturales:

P1: Estudiar análogos de H10 en otras estructuras.

P2: Si H10 para una $\mathcal{L}$-estructura M es indecidible, debilitar el lenguaje $\mathcal{L}$ manteniendo la indecidibilidad.

Para el problema P1, una técnica que surge es tratar de definir existencialmente $\mathbb{Z}$ en la estructura M que nos interesa. De esta forma por un argumento clásico de Lógica se puede demostrar la indecidibilidad del análogo de H10 en M utilizando el resultado para $\mathbb{Z}$.

Por otra parte, relativo al problema P2, J. R. Büchi (entre otros) estudió la posibilidad de debilitar el lenguaje $\mathcal{L} = \{0, 1, +, \cdot\}$ y mantener el resultado de indecidibilidad de $\mathrm{TPE}(\mathbb{Z}, \mathcal{L})$. Concretamente, Büchi formuló una conjetura

en teoría de números y probó (en un trabajo no publicado y comunicado póstumamente por Lipshitz [14]) que suponiendo que dicha conjetura era correcta, $\mathrm{TPE}(\mathbb{Z}, \mathcal{L}')$ es indecidible con el lenguaje $\mathcal{L}' = \{0, 1, +, S\}$, donde S es un símbolo de relación unaria que se interpreta de la siguiente forma: $S(k)$ si y sólo si "*k es un cuadrado*". El problema aritmético que condiciona este resultado actualmente es conocido como el Problema de Büchi para enteros ($\mathrm{BP}_2(\mathbb{Z})$) y es el siguiente:

Problema 1.1.1 *¿Existe algún N tal que toda solución en $\mathbb{Z}$ del sistema de ecuaciones*

$$x_{i-1}^2 - 2x_i^2 + x_{i+1}^2 = 2, \quad i = 2, \ldots, N-1$$

satisface $x_i^2 = (\nu + i)^2, i = 1, \ldots, N$ para algún $\nu \in \mathbb{Z}$?

Análisis numéricos del problema y argumentos heurísticos (ver [5, 6, 12]) sugieren que $N = 5$ serviría, pero no se ha logrado probar siquiera que tal N exista. La conjetura es que $\mathrm{BP}_2(\mathbb{Z})$ tiene respuesta positiva, y en esta dirección Vojta [32] demostró, usando técnicas de Bogomolov, que $\mathrm{BP}_2(\mathbb{Z})$ tiene respuesta positiva si asumimos una conjetura de Lang sobre puntos racionales en superficies de tipo general.

En muchos casos, dado un anillo M y un lenguaje $\mathcal{L}$, si $\mathrm{TPE}(M, \mathcal{L})$ es indecidible y si el análogo del problema de Büchi es cierto en M, entonces es posible utilizar el argumento de Büchi para debilitar $\mathcal{L}$ y mantener la indecidibilidad. De aquí nació el interés de resolver un análogo de $\mathrm{BP}_2(\mathbb{Z})$ para otros anillos.

En este trabajo presentamos evidencia a favor de un análogo del problema de Büchi para potencias mas altas. También resolvemos un análogo del problema de Büchi para $\mathcal{A}_p$ (funciones analíticas p-ádicas) con el objetivo de mejorar los resultados existentes de indecidibilidad para esta estructura.

1.2. Problemática y Objetivos

En adelante $\mathcal{L}_R = \{0, 1, +, \cdot\}$ es el lenguaje de anillos. Si $\mathcal{L}$ es un lenguaje que contiene a $\mathcal{L}_R$ entonces $\overline{\mathcal{L}}$ es el lenguaje obtenido a partir de $\mathcal{L}$ reemplazando $\cdot$ por un nuevo símbolo de relación unaria S que se interpreta por '*x es un cuadrado*'.

Büchi consiguió probar, usando la indecidibilidad de $\mathrm{TPE}(\mathbb{Z}, \mathcal{L}_R)$, que si tenemos una respuesta afirmativa para $\mathrm{BP}_2(\mathbb{Z})$ entonces $\mathrm{TPE}(\mathbb{Z}, \overline{\mathcal{L}_R})$ es indecidible. En muchos casos, si uno es capaz de encontrar un 'buen análogo' de $\mathrm{BP}_2(M)$ y si además $\mathrm{TPE}(M, \mathcal{L})$ es indecidible entonces es posible adaptar el argumento de Büchi para probar que $\mathrm{TPE}(M, \overline{\mathcal{L}})$ es indecidible.

Explicitemos por ejemplo lo que sería un "buen análogo" del problema de Büchi en el caso de anillos de funciones en característica cero. Si A_z es un anillo de funciones de variable z y de característica cero, entonces se plantea el siguiente problema $\mathrm{BP}_2(A_z)$:

Problema 1.2.1 *¿Existe algún N tal que toda solución en A_z del sistema de ecuaciones*

$$x_{i-1}^2 - 2x_i^2 + x_{i+1}^2 = 2, \quad i = 2, \ldots, N-1,$$

con algún x_i no constante, satisface $x_i^2 = (\nu + i)^2, i = 1, \ldots, N$, para algún $\nu \in A_z$?

En esta dirección, se sabe que tienen respuesta positiva $\mathrm{BP}_2(\mathcal{M})$ para funciones meromorfas complejas y $\mathrm{BP}_2(K)$ donde K es el campo de funciones de una curva algebraica en característica cero (ver [32]), $\mathrm{BP}_2(F(z))$ donde F es un campo de característica cero o mayor que 18 (ver [21, 22]), y recientemente $\mathrm{BP}_2(K)$ donde K es el campo de funciones de una curva algebraica en característica positiva y suficientemente grande (ver [29]). Siguiendo con el objetivo de Lógica, claramente la aplicación más directa del Problema de Büchi en otras estructuras es mejorar resultados de indecibilidad. En este sentido, el problema natural es:

Problema 1.2.2 *Resolver el Problema de Büchi en estructuras donde ya fue probada la indecidibilidad de la teoría positiva existencial sobre un lenguaje adecuado (que contenga el lenguaje de anillos), y mejorar los resultados de indecidibilidad.*

Para ir a ejemplos concretos donde sería útil resolver el problema anterior, consideremos de nuevo el lenguaje de los anillos $\mathcal{L}_R = \{0, 1, +, \cdot\}$, y definamos los enriquecimientos $\mathcal{L}_R^z = \mathcal{L}_R \cup \{z\}$ y $\mathcal{L}_R^* = \mathcal{L}_R^z \cup \{P\}$, donde z es un símbolo de constante y P es un símbolo de relación unaria. Para campos de funciones en una variable, z se interpreta como la variable y $P(x)$ se interpreta como "$x(0) = 0$". Definimos $\mathcal{A}_p$ como el anillo de funciones analíticas (enteras) p-ádicas y $\mathcal{M}_p$ como el campo de funciones meromorfas (globales) p-ádicas. El siguiente resultado fue probado en [15].

Teorema 1.2.1 *(Lipshitz-Pheidas) La teoría positiva existencial de $\mathcal{A}_p$ en el lenguaje $\mathcal{L}_R^z$ es indecidible.*

Y el siguiente resultado fue probado en [31].

Teorema 1.2.2 *(Vidaux) La teoría positiva existencial de $\mathcal{M}_p$ en el lenguaje $\mathcal{L}_R^*$ es indecidible.*

Usando estos teoremas, al resolver el Problema de Büchi en $\mathcal{A}_p$ o $\mathcal{M}_p$ se obtendría un mejoramiento fuerte de la indecidibilidad.

Por otro lado, debido al interés aritmético del problema, aparece de forma natural el siguiente análogo del problema de Büchi para potencias más altas, $\mathrm{BP}_r(\mathbb{Z})$ (ver [20]).

Problema 1.2.3 *¿Existe N tal que toda secuencia de enteros de largo N, cuyos términos sean r-potencias enteras y con r-ésimas diferencias constantes iguales a $r!$, sea necesariamente una secuencia de r-potencias consecutivas?*

Este problema no está resuelto en $\mathbb{Z}$ para ningún r. Luego, cabe preguntarse si es posible encontrar alguna estructura donde BP_r tenga una respuesta positiva para todo r. Hasta el momento, el *único* ejemplo de un anillo A donde $\mathrm{BP}_r(A)$ tiene respuesta positiva con $r > 2$ es $\mathrm{BP}_3(F[z])$ donde F es cualquier campo de característica cero (ver [23]). Así, un problema interesante es el siguiente:

Problema 1.2.4 *Para cualquier $r > 2$, dar ejemplos de anillos A donde* $\mathrm{BP}_r(A)$ *tenga respuesta positiva.*

Hensley [12] observó que resolviendo el sistema de recurrencias de $\mathrm{BP}_2(\mathbb{Z})$ llegamos al siguiente problema $\mathrm{HP}_2(\mathbb{Z})$:

Problema 1.2.5 *¿Existe N tal que ocurre lo siguiente: si $\nu, a \in \mathbb{Z}$ cumplen con "$(i+\nu)^2 - a$ es un cuadrado en $\mathbb{Z}$ para $i = 1, \ldots, N$", entonces $a = 0$?*

Análogamente cabe preguntarse el siguiente problema $\mathrm{HP}_r(\mathbb{Z})$ de representación de r-potencias:

Problema 1.2.6 *¿Existe N tal que ocurre lo siguiente: si $\nu, a \in \mathbb{Z}$ cumplen con "$(i+\nu)^r - a$ es una r-potencia en $\mathbb{Z}$ para $i = 1, \ldots, N$", entonces $a = 0$?*

Si en un anillo A se logra resolver un análogo de $\mathrm{BP}_2(A)$, el paso siguiente es intentar formular y resolver análogos de los problemas de Hensley y Büchi para potencias más altas. Es importante señalar que muchas veces $\mathrm{BP}_2(A)$ y $\mathrm{HP}_2(A)$ resultan ser equivalentes, pero en general $\mathrm{HP}_r(A)$ es más débil que $\mathrm{BP}_r(A)$.

El objetivo principal de esta investigación es responder a las interrogantes planteadas en esta sección y utilizarlas como punto de partida para continuar con el desarrollo de la teoría en torno al Problema de Büchi.

1.3. Resultados principales

Presentamos a continuación un breve resumen con los principales resultados obtenidos. Se indican oportunamente los capítulos donde el lector puede encontrar de manera específica cada resultado, demostraciones y consecuencias.

Respecto a los análogos del problema de Hensley en potencias más altas (el problema $\mathrm{HP}_r(A)$) obtenemos el siguiente resultado (ver [19] o Capítulo 3):

Teorema 1.3.1 *Sea F un campo de característica cero, t una variable y $r \geq 2$ un entero. El problema* $\mathrm{HP}_r(F[t])$ *tiene respuesta positiva.*

También en el Capítulo 3, proporcionamos una caracterización de una familia de anillos en los cuales los problemas HP_2 y BP_2 son equivalentes (ver Proposition 29).

En el Capítulo 4 presentamos los primeros ejemplos de anillos donde el análogo del problema de Büchi en potencias mas altas es cierto para cualquier exponente. Básicamente, ahí probamos el siguiente resultado.

Teorema 1.3.2 *Para cualquier entero $k \geq 2$ y cualquier primo p de la forma $kl + 1$, existe una constante M tal que, si un polinomio mónico $f \in \mathbb{F}_p[x]$ de grado k tiene la propiedad que $f(n) \in \mathbb{F}_p$ es una potencia k-ésima para al menos M valores de $n \in \mathbb{F}_p$, entonces f es una potencia k-ésima en $\mathbb{F}_p[x]$.*

Este resultado permite obtener el análogo que buscamos al Problema de Büchi en potencias más altas.

Los resultados contenidos en los Capítulos 3 y 4 nos entregan evidencia que apoya la idea de una respuesta positiva para el problema 1.2.3.

Con relación al anillo de funciones enteras p-ádicas $\mathcal{A}_p$, en el capítulo 5 obtenemos el resultado siguiente.

Teorema 1.3.3 *Sea $F = x^2 + ux + v \in \mathcal{A}_p[x]$ un polinomio con alguno de sus coeficientes no constante. Si $F(a)$ es un cuadrado en $\mathcal{A}_p$ para al menos 13 valores de $a \in \mathbb{C}_p$ entonces F es un cuadrado en $\mathcal{A}_p[x]$.*

Este resultado nos permite resolver positivamente el Problema de Büchi en $\mathcal{A}_p$, y más aún, nos permite probar (en el Capítulo 5) el siguiente mejoramiento a la respuesta negativa dada por Lipshitz y Pheidas al Décimo Problema de Hilbert en $\mathcal{A}_p$ (Teorema 1.2.1).

Teorema 1.3.4 *No existe un algoritmo para hacer lo siguiente: Dado un sistema de ecuaciones diagonales cuadráticas con coeficientes en $\mathbb{Z}[z]$ (donde z es la variable de $\mathcal{A}_p$), decidir si el sistema tiene o no solución en $\mathcal{A}_p$.*

Capítulo 2

A survey on Büchi's problem : new presentations and open problems

Hector Pasten
Universidad de Concepción
and
Thanases Pheidas
University of Crete
and
Xavier Vidaux
Universidad de Concepción

Abstract: In any commutative ring A with 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 A 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 quite 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).

2.1. 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 2 and 8, most of Section 2.12, 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
- 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 [12]).

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 2.4 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 2.5, 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 2.6 we present a formulation of Büchi's problem that usually makes positive answers easier to obtain.

In Section 2.9 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 2.10 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 2.11 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 2.12 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 2.13 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.

2.2. 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 Büchi sequences of length 5 have been found) but the problem is still open.

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

$$\left((f+n)^{\frac{p^s+1}{2}}\right)_{n=0,1,\ldots} \tag{2.1}$$

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 2.5 to 2.12. We also discuss 'Büchi sequences for higher powers' which are characterized by the property that the k-th difference of their sequence of k-th 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 [17] and P. Vojta [32]). Moreover, some of the mentioned properties permit applications in Logic (this was the initial intention of Büchi, cf. L. Lipshitz [14]). 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 Y. 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 [16] and [8]).

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 [10], [26] or [28].

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 [9], 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. [24]). 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 [20], [21] or [23]. 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.

2.3. 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

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

- $\mathcal{L}^k = \{0, 1, +, P^k\}$ is *Büchi's language for k-th 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 k-th powers and rings of functions.*

- The symbol $\mathbf{T}^{\mathbf{pe}}_{\mathcal{L}}(\mathfrak{M})$ stands for the positive-existential theory of the $\mathcal{L}$-structure $\mathfrak{M}$.

- A *Büchi System for k-th powers* is a *formal* system (S^k_M) of $M-k$ equations

$$(S^k_M) \qquad \begin{cases} \sum_{i=1}^{k+1}(-1)^{i-1}\complement_k^{i-1}x_i^k = k! \\ \vdots \\ \sum_{i=n-k}^{n}(-1)^{i-n+k}\complement_k^{i-n+k}x_i^k = k! \\ \vdots \\ \sum_{i=M-k}^{M}(-1)^{i-M+k}\complement_k^{i-M+k}x_i^k = k! \end{cases}$$

  in the variables x_i, where $\complement_k^m = \frac{k!}{m!(k-m)!}$ (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 k-th powers of variables, the system (S^k_M) can be written as

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

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

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

  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^k_M).

- 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^k_M), 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 2.4 and 2.11.
- $\mathbf{B}^k(A)$ is *Büchi's Problem for k-th powers over the ring A*. See Sections 2.4, 2.5 and 2.11.
- $\mathbf{HP}^k_\ell(A)$ is *Hensley's Problem for ℓ and k over the ring A*. See Sections 2.6 and 2.11.

2.4. 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 [30], Britton [4] or Davis [8]). 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?

Note that, implicitely by Siegel's work, we know 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 (for an explicit exposition, see [11]).

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:

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

$$\sum_i \alpha_i x_i^2 + \sum_j \beta_j y_j = \gamma, \tag{2.2}$$

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 (2.2) 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:

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

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

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

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:

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

(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 $(x+n)^2$, $n = 1, \ldots, M$, 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.

2.5. 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 $(x+n)^2$, $n = 1, \ldots, M$, 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

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

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 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 1 (1) above is harder than proving $\mathbf{B}^2(\mathbb{Z})$, because of the General Rule given above (see Section 2.12 for a counter-example in positive characteristic). Observe also that Open Problem 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 [12], 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 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 $\sigma = ((x_1, y_1), \ldots, (x_M, y_M))$ 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 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 $\mathbf{B}^2(\mathbb{Z}/3\mathbb{Z})$).

2.6. Hensley's problem

D. Hensley in [12] 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 2.12 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

$$\mu_n = \frac{x_n^2 - x_1^2}{n-1} - (n+1) \tag{2.3}$$

(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 3 *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

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

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:
$\mathbf{HP_2^2}(A)$ 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 $n = 1, \ldots, M$, then $a = 0$?

We proved in the above discussion that $\mathbf{B}^2(A)$ implies $\mathbf{HP_2^2}(A)$ for any ring A of characteristic 0, and that $\mathbf{B}^2(A)$ is equivalent to $\mathbf{HP_2^2}(A)$ for any ring A of characteristic 0 if Assumption 3 holds. In [19] (see Chapter 3), 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.

2.7. 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 [13, Theorem 2.1] characterizes all the non-trivial (non-negative increasing) 3-term Büchi sequences of integers up to any fixed integer x.

Theorem 4 (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 $0 \leq x_1 < x_2 < x_3 \leq x$. 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

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

and

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

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 [13] (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 exist *any* non-trivial 5-term Büchi sequence of integers. In this direction, R. G. E. Pinch in [25] 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 5 *Does there exist a non-trivial* 5*-term Büchi sequence?*

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

Various researchers (Allison [1] in 1986, Pinch [25] in 1993, Bremner [3] in 2003, and Browkin and Brzezinski [5] 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 [5] 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 $\mathbb{Z}$.

2.9. 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 6 *(Vojta, 2001) 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 [33]).

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 $n \geq 6$. 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

$$\omega = x_1x_2dx_1 \otimes dx_1 + (1 - x_1^2 - x_2^2)dx_1 \otimes dx_2 + x_1x_2dx_2 \otimes dx_2 \tag{2.4}$$

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 (2.4). 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 $3 \leq k < n$. 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*

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

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

(c) above a smooth conic in X_2; or

(d) in R_n.

If $n \geq 8$ 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 $n \geq 8$, *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 $n \geq 8$ 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.$\Diamond$

For a survey of results about Hilbert's Tenth Problem for number fields, see for example [28].

2.10. 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* $(x+n)^2$*,* $n = 1, \ldots, M$*, 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 2.6 is still valid and shows that if Assumption 3 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 [32]. 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 [10], [18] and [28] 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 [21] 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 2.11 and 2.12), 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 [29]).

The first author showed that the same method (using Nevanlinna theory) can be adapted to prove that Büchi's problem for the ring $\mathcal{A}_z(\mathbb{C}_p)$ of p-adic complex analytic functions has a positive answer for $M=13$ (see Chapter 5). This improves the undecidability results in [15] by Lipshitz and the second 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 7 *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 [21]).

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

$$u_n=(\nu+n)^2+a,\quad n=1,\dots,14 \tag{2.5}$$

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

$$u_n' = 2\nu'\nu + 2n\nu' + a'. \tag{2.6}$$

Plugging the expression for n obtained from (2.6) into (2.5), 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

$$\begin{aligned} 4\nu'^2 a + a'^2 &= 4\nu'^2 u_n - u_n'^2 + 2u_n' a' \\ &= x_n \left(4\nu'^2 x_n - 4x_n'^2 x_n + 4x_n' a'\right) = x_n \Delta_n \end{aligned} \tag{2.7}$$

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 (2.5):

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

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 (2.7).

At this stage, we still have to solve the differential equation given by (2.7)

$$4\nu'^2 a + a'^2 = 0. \tag{2.8}$$

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 (2.8) 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 (2.5), we get

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

If $n \neq -K$, write

$$y_n^2 = \left(\frac{x_n}{\sqrt{n+K}}\right)^2 = 2\nu + n - K. \tag{2.9}$$

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 (2.9)).

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. $\Diamond$

Note : The first author in [19] (see Chapter 3) 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.

2.11. Higher powers

Since Büchi's problem is about the second difference of sequences of squares, it is quite natural to study the k-th difference of a sequence of k-th 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 k-th

power'. Let A be a ring.

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

The only result we know so far was obtained in 2008 by the second and the third authors in [23]: $\mathbf{B}^3(\mathbb{C}[z])$ 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 2.10 (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 'k-th 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 $a_0,\ldots,a_{k-2}$ of A, if the quantities

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

are k-th powers in A for $n = 1,\ldots,M$, 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 [23]).

The following Lemma is proved in the same way as Lemma 2.

Lemma 8 *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 $M = \text{máx}\{M_A, M_B\}$.*

For the moment it seems too hard to solve Büchi's problem for k-th 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:
$\mathbf{HP}_\ell^k(A)$ *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 $a_0,\ldots,a_{\ell-2}$ of A the quantities*

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

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

In [19] (see Chapter 3), the first author proved that $\mathbf{HP}_2^k(\mathbb{C}[z])$ has a positive answer. He essentially used the method presented in Section 2.10 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 [23] for $\mathbf{B}^3(\mathbb{C}[z])$ with the method used in [19] for $\mathbf{HP}_2^k(\mathbb{C}[z])$ should allow one to prove that $\mathbf{HP}_3^k(\mathbb{C}[z])$ 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 [23], 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 $((x+1)^k, \ldots, (x+k-1)^k)$ 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 $\varphi^k(r,s)$

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

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 9 *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?*

2.12. 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^2_M) is equivalent to the system (S^2_c). 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 $n = 1, \ldots, M$, 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* $(x+n)^2$*,* $n = 1, \ldots, M$*, 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 $n = 1, \ldots, M$*, 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 [12] using the original formulation by Büchi).

Proposition 10 *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 $n = 1, 2, \ldots, p$. 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 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 10, $\mathbf{B}^2(\mathbb{F}_p)$ 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 $x_n^2 = (x+n)^{p^s+1}$, $n = 1, \ldots, M$, for some $x \in A_z$ and some $s \in \mathbb{N}$?*

In [22], 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 [29], 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 $M \geq \alpha g + \beta$.

2.13. 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.

Capítulo 3

An Extension of Büchi's Problem for Polynomial Rings in Zero Characteristic

El contenido de este capitulo corresponde al articulo *An Extension of Büchi's Problem for Polynomial Rings in Zero Characteristic* (ver [19]), publicado en la entrega Mayo 2010 de la revista *Proceedings of the American Mathematical Society*. Para mayor informacion, ver el sitio web
`http://www.ams.org/proc/2010-138-05/S0002-9939-09-10259-9/home.html`

The content of this chapter corresponds to the article *An Extension of Büchi's Problem for Polynomial Rings in Zero Characteristic* (see [19]), published in the May 2010 issue of the *Proceedings of the American Mathematical Society*. For further references, see the website
`http://www.ams.org/proc/2010-138-05/S0002-9939-09-10259-9/home.html`

Abstract: We prove a strong form of the 'n Squares Problem' over polynomial rings with characteristic zero constant field. In particular we prove: for all $r \geq 2$ there exists an integer $M = M(r)$ depending only on r such that, if $z_1, z_2, ..., z_M$ are M distinct elements of F and we have polynomials $f, g, x_1, x_2, \ldots, x_M \in F[t]$, with some x_i non-constant, satisfiying the equations $x_i^r = (z_i + f)^r + g$ for each i, then g is the zero polynomial.

3.1. Introduction

Büchi's Problem, also known as the "n squares' Problem", asks whether there exists some positive integer M such that any sequence of M integer squares, whose second difference is constant and equal to 2, is of the form $(x + n)^2$, $n = 0, 1, \ldots, M$, for some integer x. This Problem, still open, was proposed

by J. R. Büchi in the 1970s (and publicized by L. Lipshitz in 1990 in [14]) as he realized that a positive answer to it would imply a strong improvement to the negative answer to Hilbert's Tenth Problem, recently obtained by Y. Matiyasevich, after the works of M. Davis, H. Putnam and J. Robinson. See [8] and [16].

Vojta proved in [32] that a positive answer to Büchi's Problem follows from a conjecture of Lang on rational points on projective varieties of general type. In [20], Pheidas and Vidaux proposed a problem $\mathrm{BP}_r(A)$ extending Büchi's Problem by considering r-th differences of r-th powers constant and equal to $r!$, and where the variables range over any integral domain A, the point being that in most cases, a positive answer to $\mathrm{BP}_r(A)$ will have logical consequences similar to the "integer and square case". If A is a ring of functions, then it is required also that not all the r powers are constant. Vojta [32] proved that the problem $\mathrm{BP}_2(\mathcal{M})$, where $\mathcal{M}$ is the field of functions that are meromorphic over $\mathbb{C}$, has a positive answer (using Nevanlinna Theory). Pheidas and Vidaux proved [21] that $\mathrm{BP}_2(A)$ has a positive answer whenever A is a ring of polynomials or is a field of rational functions of zero characteristic - but if the characteristic is positive and large, there are more "trivial solutions" than those named in the original statement (see [22]). In [23], they proved that $\mathrm{BP}_3(F[t])$ has a positive answer when F is any field of zero characteristic.

As D. Hensley noticed in [12], $\mathrm{BP}_2(\mathbb{Z})$ is equivalent to the following problem:

$\mathrm{HP}_2(\mathbb{Z})$: Does there exist a positive integer M such that, for any integers μ and ν, the following system of equations

$$x_n^2 = (n+\nu)^2 + \mu \ , \quad n = 0, \ldots, M$$

has an integer solution if and only if $\mu = 0$?

It is not so difficult to see that this equivalence holds for many commutative rings (see Section 3.5).

So we may write $\mathrm{HP}_2(A)$ for the analogue of Hensley's formulation over the ring A. Then we may consider the problem $\mathrm{HP}_r(A)$ where the squares are simply replaced by r-th powers. Observe that a positive answer to $\mathrm{BP}_r(A)$ would imply a positive answer to $\mathrm{HP}_r(A)$, but the converse is true only if $r = 2$.

We sharpen techniques developed in [21] and [23] in order to prove that $\mathrm{HP}_r(F[t])$, where F is a field of zero characteristic, has a positive answer (see Theorem 11 in Section 3.2). Other forms of analogous of Büchi's Problem over the integers have been studied by Buell [6], then by Pinch [25] and eventually by Browkin and Brzezinski [5]. Our main result, Theorem 11, actually implies a quite stronger form of $\mathrm{HP}_r(F[t])$ for any power r, so we may consider it as a new evidence for $\mathrm{BP}_r(F[t])$ to have a positive answer.

We observe that in contrast to the method developed in [21] and [23], we do not make use of the fact that elliptic curves do not admit rational parametrizations. Our proof is essentially combinatorial and therefore should be more easily adaptable, for example, to algebraic extensions of polynomial rings and rational function fields, both in positive and in zero characteristic.

3.2. Main Result and Corollaries

Let F be a field of characteristic zero. If S is a non-empty finite subset of F and $r \geq 2$ is an integer, we will write

$$\xi(S,r) = \max_{c,d \in \bar{F}} |S \cap \{x \in F : (x+c)^r = d\}|$$

were $\bar{F}$ denotes an algebraic closure of F. Observe that $1 \leq \xi(S,r)$ because $(s+0)^r = s^r$ for each s in S, and $\xi(S,r) \leq r$ since the polynomial $(X+c_1)^r - c_2$ has degree r.

For $x \in \mathbb{R}$ we denote by $\lceil x \rceil$ the least integer greater than or equal to x ($\lceil . \rceil$ is the ceiling function).

Theorem 11 (Main Result) *Let F be a field of characteristic zero and $r \geq 2$ an integer. Suppose we have a sequence $(x_n)_{n=1}^M \subseteq F[t]$ of M polynomials such that:*

1. *Not all the x_n are constant.*
2. *There exist a set $S = \{z_n : n = 1, \ldots, M\} \subseteq F$ with M elements and two polynomials f, g in $F[t]$ such that $\left\lceil \frac{r^3}{(r-1)^2} \xi(S,r) \right\rceil \leq M - 1$ and $x_n^r = (z_n + f)^r + g$ for each n.*

Then g is the zero polynomial.

If we know some information about r, F or S in the Main Result, then a constant M can be computed explicitly. To illustrate that, we may set $F = \mathbb{R}$ and $S \subseteq \mathbb{Z}$. At most 2 of the elements in S at the same time can be solutions of an equation of the form $(z + c_1)^r = c_2$ with c_1, c_2 in $\mathbb{C} = \bar{\mathbb{R}}$ (since the integers are colinear in $\mathbb{C}$), hence $\xi(S,r) = 2$. Another example is given by considering $F = \mathbb{C}$ and S a set of complex numbers such that no cyclic k-gon ($k \geq 3$) has vertices in S. Then $\xi(S,r) \leq \min\{r, k-1\}$ and we can compute an explicit value for M.

From Theorem 11, we can derive the following strong form of $\mathrm{HP}_r(F[t])$.

Corollary 12 *For all $r \geq 2$ there exists an integer $M = M(r)$ depending only on r such that, if $z_1, z_2, ..., z_M$ are M distinct elements of F and we have polynomials $f, g, x_1, x_2, \ldots, x_M \in F[t]$, with some x_i non-constant, satisfying the equations $x_i^r = (z_i + f)^r + g$ for each i, then g is the zero polynomial.*

Proof. Take $M = \lceil \frac{r^4}{(r-1)^2} \rceil + 1$ and $S = \{z_1, \ldots, z_M\}$. We have then

$$|S| = M = \left\lceil \frac{r^4}{(r-1)^2} \right\rceil + 1 \geq \left\lceil \frac{r^3}{(r-1)^2} \xi(S,r) \right\rceil + 1 \ .$$

■

In particular we have $\mathrm{HP}_r(F[t])$:

Corollary 13 *Let $r \geq 2$ be an integer. There exists an integer $M = M(r)$ depending only on r such that, if the polynomials $f, g, x_1, x_2, ..., x_M \in F[t]$ (with some x_i non-constant) satisfy the equations $x_n^r = (n+f)^r + g$ for $n = 1, 2, \ldots, M$, then g is the zero polynomial.*

and the n Squares Problem in $F[t]$ follows:

Corollary 14 *There exists an integer M such that any sequence $(x_n)_{n=1}^M$ of (not all constant) polynomials in $F[t]$ satisfying the system of equations*

$$\begin{aligned} x_1^2 - 2x_2^2 + x_3^2 &= 2 \\ x_2^2 - 2x_3^2 + x_4^2 &= 2 \\ &\cdots \\ x_{M-2}^2 - 2x_{M-1}^2 + x_M^2 &= 2 \end{aligned}$$

satisfies also the system of equations $x_n^2 = (n+f)^2$, $n = 1, \ldots, M$, for some $f \in F[t]$.

Proof. This follows immediately from Corollary 13 (with $r = 2$) by solving the recurrence, see Section 3.5 ∎

3.3. Intermediate Results

In this section we shall prove some Lemmas before proving Theorem 11.

Assumption 15 *Without loss of generality, assume that F is algebraically closed.*

Notation 16 *Write $h = -g$ and $\xi = \xi(S, r)$. Set $I = \{1, 2, \ldots, M\}$ where $M = \left\lceil \frac{r^3}{(r-1)^2}\xi \right\rceil + 1$. Note that $M > 1$, since $\frac{r^3}{(r-1)^2}\xi > 0$. Label the elements of S as $z_n, n \in I$. So by hypothesis we have*

$$x_n^r = (z_n + f)^r - h \ . \tag{3.1}$$

Set

$$d_f = \deg f \quad \text{and} \quad d_h = \deg h$$

and choose $\alpha \neq \omega \in I$ such that $d = \deg x_\alpha$ is maximum and $d_0 = \deg x_\omega$ is minimum (possibly $d = d_0$), among the degrees of the x_n's. Write

$$I' = I - \{\omega\} \ .$$

On the one hand, differentiating both sides of Equation (3.1) we obtain

$$r x_n' x_n^{r-1} = r f'(z_n + f)^{r-1} - h'$$

hence

$$(r x_n' x_n^{r-1} + h')^r = r^r f'^r (z_n + f)^{r(r-1)}.$$

On the other hand, from the same Equation (3.1) we have

$$(x_n^r + h)^{r-1} = (z_n + f)^{r(r-1)} \ .$$

Substituting $(z_n + f)^{r(r-1)}$ into the previous equation, we obtain

$$(rx_n' x_n^{r-1} + h')^r = r^r f'^r (x_n^r + h)^{r-1} \ . \tag{3.2}$$

Let us denote

$$\Delta = h'^r - r^r f'^r h^{r-1} \ ,$$

namely, the part of Equation (3.2) that does not depend on n.

Lemma 17 *We have*

1. $0 < d = \deg x_n$, *for all* $n \in I'$;
2. $\deg(\Delta) \leq \dfrac{r(dr^2 - (r-1))}{r-1}$.

Proof. For $j \neq k \in I$ we note that

$$\begin{aligned} x_j^r - x_k^r &= (z_j + f)^r - (z_k + f)^r \\ &= r(z_j - z_k) f^{r-1} + (\text{terms in lower powers of } f) \ . \end{aligned}$$

Therefore we have

$$\deg(x_j^r - x_k^r) = (r-1)d_f \tag{3.3}$$

hence

$$d_f \leq \frac{r}{r-1} d \tag{3.4}$$

From Equations (3.1) and (3.4) follows

$$d_h \leq \text{máx}\{rd, rd_f\} \leq \frac{r^2}{r-1} d \ ,$$

thus, after an easy computation,

$$\deg(\Delta) \leq \frac{r(dr^2 - r + 1)}{r-1} \ .$$

Note that from Equation (3.3) we have

$$\deg(x_\alpha^r - x_\omega^r) = \deg(x_n^r - x_\omega^r)$$

as long as $n \in I'$. So, if $d > d_0$ then all x_n but possibly x_ω have degree d, otherwise all x_n have the same degree d, and from the hypothesis of some x_n being non-constan we have $d > 0$. ■

Notation 18 *We will be writing* Λ *for a least common multiple of* $\{x_n | n \in I'\}$.

Note that Λ is not constant since, by Lemma 17 (1), none of the x_n's, for $n \in I'$, is constant.

Lemma 19 *The polynomial Λ^{r-1} divides Δ.*

Proof. From Equation (3.2) we deduce that x_n^{r-1} divides Δ for each $n \in I'$ and the result follows. ∎

Lemma 20 *No $\xi+1$ polynomials in $\{x_n | n \in I'\}$ have a common non-constant factor.*

Proof. By Lemma 17 (1), the polynomials in $\{x_n | n \in I'\}$ are non-constant.

Suppose that for some distinct $\xi+1$ indices $i(1), i(2), ..., i(\xi+1) \in I'$, there exists $\rho \in F$ such that ρ is a common zero for all $x_{i(l)}$. Consider the following equations derived from Equation (3.1)

$$\begin{aligned} x_{i(1)}^r - x_{i(2)}^r &= (z_{i(1)} + f)^r - (z_{i(2)} + f)^r \\ x_{i(2)}^r - x_{i(3)}^r &= (z_{i(2)} + f)^r - (z_{i(3)} + f)^r \\ &\cdots \\ x_{i(\xi)}^r - x_{i(\xi+1)}^r &= (z_{i(\xi)} + f)^r - (z_{i(\xi+1)} + f)^r. \end{aligned}$$

Evaluating at ρ we obtain

$$(z_{i(1)} + f(\rho))^r = (z_{i(2)} + f(\rho))^r = \cdots = (z_{i(\xi+1)} + f(\rho))^r = c$$

for some $c \in F$. It follows that the equation $(z + f(\rho))^r = c$ has at least $\xi+1$ distinct roots, since by hypothesis of Theorem 11, $i \neq j$ implies $z_i \neq z_j$. This contradicts the definition of ξ. ∎

Lemma 21 *We have $\Delta = 0$.*

Proof. Let $p \in F[t]$ be a prime polynomial. From Lemma 20, p divides at most ξ polynomials in $\{x_n | n \in I'\}$, so we have

$$\text{máx}\{\nu_p(x_n) | n \in I'\} \geq \frac{1}{\xi} \sum_{n \in I'} \nu_p(x_n) = \frac{1}{\xi} \nu_p \left(\prod_{n \in I'} x_n \right)$$

where ν_p denotes the function *"order at p"*.

Summing the left and right hand sides of this last inequality over the primes dividing $\prod_{n \in I'} x_n$, from Lemma 17 (1) we obtain

$$\deg\left(\text{lcm}\{x_n | n \in I'\}\right) \geq \frac{1}{\xi} \deg \left(\prod_{n \in I'} x_n \right) = \frac{M-1}{\xi} d$$

where "lcm" means *"least common multiple"*. Therefore we have

$$\deg(\Lambda) \geq \frac{M-1}{\xi} d.$$

Note that if Δ is not the zero polynomial then from Lemma 19, we deduce

$$(r-1)\deg(\Lambda) \leq \deg(\Delta) \ .$$

Thus, by Lemma 17 (2), we have

$$\frac{M-1}{\xi}d \leq \deg(\Lambda) \leq \frac{1}{r-1}\deg(\Delta) \leq \frac{r(dr^2-(r-1))}{(r-1)^2}.$$

As $0 < d$ (Lemma 17 (1)) this implies

$$\begin{aligned} M &\leq \frac{\xi}{d}\frac{r(dr^2-(r-1))}{(r-1)^2}+1 \leq \frac{r^3\xi}{(r-1)^2} - \frac{r\xi}{(r-1)d}+1 \\ &< \frac{r^3\xi}{(r-1)^2}+1 \leq \left\lceil \frac{r^3\xi}{(r-1)^2} \right\rceil + 1 = M \end{aligned}$$

hence gives us a contradiction. So we have $\Delta = 0$ ∎

3.4. Proof of Theorem 11

In order to prove the Main Result, we will suppose that

Assumption 22 *h is not the zero polynomial.*

and obtain a contradiction

The next four Lemmas will be under Assumption 22.

From Lemma 21 we have

$$\Delta = h'^r - r^r f'^r h^{r-1} = 0 \Rightarrow h'^r = r^r f'^r h^{r-1} \tag{3.5}$$

Since some of the x_n's are not constant, from 3.1 we note that f, g are not both constant. Therefore, from Equation 3.5 and Assumption 22 we have that, if h is a non-zero constant then $f' = 0$ so f is constant, thus h is a non-constant polynomial. Moreover, if f is constant then we have $h' = 0$ from 3.5, hence f is a non-constant polynomial. So, under Assumption 22, h and f are non-constant polynomials.

Notation 23 *Let φ, η be the leading coefficients of f, h respectively.*

Lemma 24 *We have $d < d_f$.*

Proof. From Assumption 22 we have f non-constant, thus from Equation (3.5) we deduce

$$r(d_h - 1) = r(d_f - 1) + d_h(r-1) \Rightarrow d_h = rd_f \neq 0$$

and

$$(d_h\eta)^r = r^r(d_f\varphi)^r\eta^{r-1} \Rightarrow \eta = \left(\frac{rd_f}{d_h}\right)^r \varphi^r = \varphi^r \ .$$

It follows that $(z_n + f)^r$ and h must have the same degree and leading coefficient for each $n \in I$. Hence, by Equation (3.1), we have $rd < rd_f$, hence $d < d_f$. ∎

Lemma 25 *We have*

$$r \deg(x_n) = rd = (r-1)d_f$$

for each $n \in I'$.

Proof. By Equation (3.1), for each $n \in I'$ we have $h = (z_n + f)^r - x_n^r$. Plugging this expression for h in Equation (3.5) we obtain

$$(rf'(z_n + f)^{r-1} - rx_n' x_n^{r-1})^r = r^r f'^r((z_n + f)^r - x_n^r)^{r-1}$$

hence

$$(f'(z_n + f)^{r-1} - x_n' x_n^{r-1})^r = f'^r((z_n + f)^r - x_n^r)^{r-1}. \tag{3.6}$$

Expanding each side of this equation we get

$$\sum_{i=0}^{r}(-1)^i \binom{r}{i}(f'(z_n + f)^{r-1})^{r-i}(x_n' x_n^{r-1})^i = \\ = \sum_{j=0}^{r-1}(-1)^j \binom{r-1}{j} f'^r (z_n + f)^{r(r-1-j)} x_n^{rj}$$

and canceling terms for $i = 0 = j$ we have

$$\sum_{i=1}^{r}(-1)^i \binom{r}{i}(f'(z_n + f)^{r-1})^{r-i}(x_n' x_n^{r-1})^i = \\ = \sum_{j=1}^{r-1}(-1)^j \binom{r-1}{j} f'^r (z_n + f)^{r(r-1-j)} x_n^{rj} \ .$$

Since $d < d_f$ (by Lemma 24) and $0 < d = \deg x_n, \forall n \in I'$ (by Lemma 17 (1)), the sequence of polynomials in each sum of the last equation has decreasing positive degree. Therefore, by observing the leading coefficients at $i = 1 = j$ we have

$$r(d_f \varphi)^{r-1} \varphi^{(r-1)^2} d_n X_n^r = (r-1)(d_f \varphi)^r \varphi^{r(r-2)} X_n^r$$

where $d_n = d$ and X_n are the degree and the leading coefficient of x_n for each $n \in I'$, respectively. Hence we have

$$rd_n = (r-1)d_f \ .$$

■

Notation 26 *Write* $\Gamma = \gcd\{x_n' x_n^{r-1} | n \in I'\}$, *where* gcd *means "greatest common divisor".*

Note that Γ is well defined since $0 < d = \deg x_n, \forall n \in I'$, and is not the zero polynomial.

Lemma 27 *We have* $\deg \Gamma \geq d_f - 1$.

Proof. From Equation (3.6)

$$(f'(z_n + f)^{r-1} - x'_n x_n^{r-1})^r = f'^r((z_n + f)^r - x_n^r)^{r-1}$$

we see that f' divides $x'_n x_n^{r-1}$ for all $n \in I'$. ∎

Recall that we have $d_f \geq 1$ and $r \geq 2$. So Lemma 25 implies that r divides d_f, hence the degree of f' is $d_f - 1 \geq 1$. We conclude that Γ is not constant by Lemma 27.

Lemma 28 *The following inequality holds*

$$d - 1 \geq \frac{M - 1 - \xi}{M - 1} \deg \Gamma.$$

Proof. Write $\prod_{p_i|\Gamma} p_i^{a_i}$ for the prime factorization of Γ (up to factors in F). Since Γ is not constant this product is not empty, and since F is assumed to be algebraically closed we have $\deg p_i = 1$ for each i.

We claim that each $p_i^{a_i}$ in the factorization of Γ divides at least $M - 1 - \xi$ elements in $\{x'_n \mid n \in I'\}$. Indeed, recall that $|I'| = M - 1$ and notice that each $p_i^{a_i}$ must divide $x'_n x_n^{r-1}$ for each $n \in I'$ by definition of Γ. But from Lemma 20 we know that each p_i can divide at most ξ polynomials in $\{x_n^{r-1} \mid n \in I'\}$, hence each $p_i^{a_i}$ must divide at least $M - 1 - \xi$ polynomials in $\{x'_n \mid n \in I'\}$.

Therefore we have that for each p_i, $p_i^{a_i(M-1-\xi)}$ divides $\prod_{n \in I'} x'_n$. Hence $\Gamma^{M-1-\xi}$ divides $\prod_{n \in I'} x'_n$ and we have

$$(M - 1)(d - 1) = \deg \left(\prod_{n \in I'} x'_n \right) \geq (M - 1 - \xi) \deg \Gamma$$

which proves the lemma, since $M > 1$. ∎

Proof of Main Result. Suppose that Assumption 22 is true. By Lemma 27 and Lemma 28 we have

$$d - 1 \geq \frac{M - 1 - \xi}{M - 1} \deg \Gamma \geq \frac{M - 1 - \xi}{M - 1}(d_f - 1) \ .$$

Thus, by Lemma 25 and the definition of M we have

$$\begin{aligned} d - 1 &\geq \frac{M - 1 - \xi}{M - 1} \left(\frac{rd}{r - 1} - 1 \right) = \frac{\left\lceil \frac{r^3}{(r-1)^2} \xi \right\rceil + 1 - 1 - \xi}{\left\lceil \frac{r^3}{(r-1)^2} \xi \right\rceil + 1 - 1} \left(\frac{r}{r - 1} d - 1 \right) \\ &= \frac{\left\lceil \frac{r^3}{(r-1)^2} \xi \right\rceil - \xi}{\left\lceil \frac{r^3}{(r-1)^2} \xi \right\rceil} \left(\frac{r}{r - 1} d - 1 \right) \ . \end{aligned}$$

Since $\lceil y \rceil \geq y$ by definition, and $y \mapsto (y - \xi)/y = 1 - \frac{\xi}{y}$ is an increasing positive function for $y > \xi$, we have

$$d - 1 \geq \frac{\frac{r^3}{(r-1)^2} \xi - \xi}{\frac{r^3}{(r-1)^2} \xi} \left(\frac{r}{r - 1} d - 1 \right)$$

hence

$$d-1 \geq \frac{\frac{r^3}{(r-1)^2}-1}{\frac{r^3}{(r-1)^2}}\left(\frac{r}{r-1}d-1\right) = \left(1-\frac{1}{\frac{r^3}{(r-1)^2}}\right)\left(\frac{r}{r-1}d-1\right)$$
$$= \frac{r}{r-1}d-1-\frac{(r-1)^2}{r^3}\left(\frac{r}{r-1}d-1\right)$$

hence

$$\frac{(r-1)^2}{r^3}\left(\frac{r}{r-1}d-1\right) \geq \frac{r}{r-1}d-d = \frac{d}{r-1}$$

hence

$$\frac{(r-1)^2}{r^3}(rd-r+1) \geq d\ .$$

Therefore, as $r \geq 2$ we have

$$d \leq \frac{(r-1)^2}{r^3}(rd-r+1) < \frac{(r-1)^2}{r^3}(rd-1+1) = \frac{(r-1)^2}{r^3}rd < d$$

which gives us a contradiction. Hence Assumption 22 is false and g is the zero polynomial. ∎

3.5. Equivalence of Büchi's Problem and Hensley's Formulation

Proposition 29 *Let A be a commutative ring with unit, of characteristic different from 2.*

1. *If $\mathrm{BP}_2(A)$ has a positive answer then $\mathrm{HP}_2(A)$ has a positive answer.*
2. *Suppose that $2 \in A$ is invertible or $A/4A \simeq \mathbb{Z}/4\mathbb{Z}$. If $\mathrm{HP}_2(A)$ has a positive answer then $\mathrm{HP}_2(A)$ has a positive answer.*

Proof. For (1), it is easy to check that a sequence $(x_k)_{k=1}^N$ in A with terms of the form $x_k^2 = (k+f)^2+g$ for fixed $f, g \in A$, is also a sequence with constant second difference equal to 2.

For (2), let $(x_k)_{k=1}^N$ be a sequence in A with constant second difference equal to 2, then we have $x_{k-2}^2 - 2x_{k-1}^2 + x_k^2 = 2$ for $k = 3, ..., N$. The sequence of second partial sums of this last expression gives $(x_1^2-x_2^2)(k-2)-x_2^2+x_k^2 = (k-2)(k-1)$, hence $x_k^2 = k^2 + (x_2^2 - x_1^2 - 3)k + (2 + 2x_1^2 - x_2^2)$.

If 2 is invertible we take $f = (x_2^2 - x_1^2 - 3)/2, g = (2+2x_1^2 - x_2^2) - f^2$ and the result follows. Otherwise, if $A/4A \simeq \mathbb{Z}/4\mathbb{Z}$ then $A/2A \simeq \mathbb{Z}/2\mathbb{Z}$ and the equation $(x_1^2-x_2^2)-(x_2^2-x_3^2) = 2$ seen modulo $4A$ easily gives $x_1^2 - x_2^2 = 1$ or 3 mód $4A$, hence $x_1^2 - x_2^2 \notin 2A$. Therefore $(x_2^2 - x_1^2 - 3) \in 2A$ and we can take f, g as before. ∎

Capítulo 4

Büchi's problem in any Power for Finite Fields

Abstract: For any $k \geq 2$ and p prime of the form $p = kl + 1$, we show that there exists a constant M (of size p/c, where c is the least prime divisor of k) such that, if a monic polynomial $f \in \mathbb{F}_p[x]$ of degree k has the property that $f(n) \in \mathbb{F}_p$ is a k-th power for at least M values of $n \in \mathbb{F}_p$, then f is a k-th power in $\mathbb{F}_p[x]$.

In particular, any sequence of length M formed by k-th powers in $\mathbb{F}_p$ and whose sequence of k-th differences is the constant sequence $(k!)$, must be a sequence of the form $((\nu + n)^k)_n$ for some $\nu \in \mathbb{F}_p$. This is the first example of a positive answer to Büchi's problem for any power.

4.1. Introduction

In an unpublished work of J. R. Büchi communicated by Lipshitz (see [14]), it was shown that, in order to define in a positive existential way the multiplication in $\mathbb{Z}$ over the language $\mathcal{L}_2 = \{0, 1, +, P_2\}$ (where $P_2(x)$ stands for 'x is a square'), hence improving strongly the negative answer of Hilbert's tenth problem by Matiyasevich (see [16]), it is enough to have a positive answer to the following number-theoretical question:

Question 30 $\mathrm{BP}_2(\mathbb{Z})$ *: Does there exist an integer M such that the following holds?*

If a sequence of integers $(x_i)_{i=1}^M$ satisfies

$$\Delta^{(2)}(x_i^2)_{i=1}^M = (2, \ldots, 2)$$

(that is, $(x_i^2)_{i=1}^M$ has 2nd differences constant and equal to 2) then there exists an integer ν such that $x_i^2 = (\nu + i)^2$ for each i.

Büchi believed that one can take $M = 5$, and numerical evidence suggests that this is indeed the case, but nowadays the *existence* of such an M is still

an open problem. The problem $\mathrm{BP}_2(\mathbb{Z})$ is known as the *n Squares Problem* or *Büchi's Problem.*

In general, we will use the notation $\Delta^{(k)}$ to indicate the k-th differences of a sequence; so for example $\Delta^{(1)}(a,b,c,d) = (b-a, c-b, d-c)$ and $\Delta^{(3)}(a,b,c,d) = (d-3c+3b-a)$.

In [20] it was proposed the following natural generalization to $\mathrm{BP}_2(A)$ for higher powers.

Question 31 $\mathrm{BP}_k(\mathbb{Z})$ *: Does there exist an integer M such that the following holds?*

If a sequence of integers $(x_i)_{i=1}^M$ satisfies

$$\Delta^{(k)}(x_i^k)_{i=1}^M = (k!, \ldots, k!)$$

then there exists an integer ν such that $x_i^k = (\nu+i)^k$ for each i.

This is an open problem for all $k \geq 2$.

Given a commutative ring A with unit, one can formulate a similar question in a natural way by considering A instead of $\mathbb{Z}$ in the statement of $\mathrm{BP}_k(\mathbb{Z})$. Sometimes it is necessary to consider additional requirements on the x_i. For example, in the case of a ring of functions on the variable z we require for at least one x_i to depend on z. Another example, which will be relevant in our situation, is when A has positive characteristic. In this case, we require M to be at most the characteristic. Let us refer to such analogues as $\mathrm{BP}_k(A)$ (the word 'analogue' then depends on the ring).

In [20] it was shown that, in several cases, a positive answer to the the problem $\mathrm{BP}_k(A)$ allows us to define multiplication in the language $\mathcal{L}_k = \{0, 1, +, P_k\}$ where $P_k(x)$ stands for 'x is a k-th power'.

In the case $k = 2$ a lot of progress has been achieved. For example, we know the the following cases (among various others) have a positive answer: $\mathrm{BP}_2(\mathbb{F}_p)$ with $p > 2$ (see [12]), $\mathrm{BP}_2(\mathcal{M})$ where $\mathcal{M}$ is the field of complex meromorphic functions (see [32]), $\mathrm{BP}_2(F(z))$ where $F(z)$ is the field of rational functions over a field of characteristic 0 or $p \geq 19$ (see [21, 22]). Actually Büchi's problem has a positive answer even in the case of function fields of curves (see [32] for the characteristic zero case and see [29] for 'large enough' positive characteristic). Moreover, under a conjecture in Diophantine Geometry, Vojta showed in [32] that $\mathrm{BP}_2(\mathbb{Q})$ would have a positive answer (hence $\mathrm{BP}_2(\mathbb{Z})$ would have a positive answer).

On the other hand, though in [19] an 'intermediate' problem between $\mathrm{BP}_2(A)$ and $\mathrm{BP}_k(A)$ (known as Hensley's problem for k-th powers) is shown to have a positive answer for any k when $A = F[z]$ with F a field of characteristic zero, the *only* known example of a positive answer to $\mathrm{BP}_k(A)$ with $k > 2$ is for $A = F[z]$ and $k = 3$ (see [23]).

The aim of this paper is to provide, for any $k \geq 2$, examples of rings A where $\mathrm{BP}_k(A)$ has a positive answer. Unfortunately, the examples shown below do not give new results in Logic (in an obvious way) since the rings considered are finite.

Before stating our results, let us introduce a few notation.

Notation 32 *1. If S is a set, $|S|$ denotes the cardinal of S.*

2. $P(K,k)$ is the set of k-th powers in the field K.

3. If F is a polynomial, $\mathbb{V}(F)$ is the zero locus of F.

We prove the following theorem on the representation of k-th powers in certain finite fields, by monic polynomials of degree k. As a consequence, we get Büchi's problem in higher powers for some finite fields (see Section 4.2).

Theorem 33 *Let $k \geq 2$ be an integer, c its least prime factor and p a prime of the form $kl+1$ such that $p > 4k^2$. Consider the constant*

$$M = \left\lfloor \frac{1}{c}p + (k-1)\sqrt{p} - k \right\rfloor$$

and let $f \in \mathbb{F}_p[x]$ be a monic polynomial of degree k. We have $M \leq p$ and, if $f(n)$ is a k-th power for at least M values of $n \in \mathbb{F}_p$ then f is a k-th power in $\mathbb{F}_p[x]$.

Moreover, in the particular case $k = 2$ the result holds with $M = (p+3)/2$ and for any odd prime.

Corollary 34 *Let $k \geq 2$ be an integer. The problem $\mathrm{BP}_k(\mathbb{F}_p)$ has a positive answer for any prime $p > 4k^2$ of the form $kl+1$, taking*

$$M = \left\lfloor \frac{1}{c}p + (k-1)\sqrt{p} - k \right\rfloor$$

where c is the least prime divisor of k. Moreover, $\mathrm{BP}_2(\mathbb{F}_p)$ has a positive answer for any prime $p > 2$, with $M = (p+3)/2$.

We remark that Hensley proved in [12] that $\mathrm{BP}_2(\mathbb{F}_p)$ has a positive answer with $M = p$ for $p > 2$.

Observe that, by Dirichlet's Theorem on primes in arithmetic progressions, for each k we have infinitely many primes p satisfying the conditions in Theorem 33 and Corollary 34.

Theorem 33 can be refined in the following way in the case of squares (see Section 4.3).

Proposition 35 *Let $p > 2$ be a prime and $f = x^2 + ux + v \in \mathbb{F}_p[x]$ a monic polynomial of degree 2 which is not a square in $\mathbb{F}_p[x]$. If $S = \{n \in \mathbb{F}_p : f(n)$ is a square$\}$ then*

$$|S| = \frac{1}{2}\left(p + \left(\frac{\frac{u^2}{4} - v}{p}\right)\right)$$

where $\left(\frac{-}{p}\right)$ is the Legendre symbol.

This work is part of the MS Thesis of the author at the Universidad de Concepción, Chile. I thank the professors of the Math Department (Departamento de Matemática) for their useful comments, especially Antonio Laface and Xavier Vidaux. I also would like to express my gratitude to Athanases Pheidas and Bjorn Poonen for their valuable suggestions.

4.2. Representation of k-th powers by a polynomial of degree k.

The purpose of this section is to prove Theorem 33.

Notation 36 *Let $k \geq 2$ be an integer and let A be an integral domain such that the polynomial $x^k - 1 \in A[x]$ has all its zeros in A. We define μ_k as the multiplicative group formed by the zeros of $x^k - 1$. It is clear that μ_k is cyclic. Note that, if d divides k then $x^d - 1$ has all its zeros in A and μ_d is a subgroup of μ_k.*

Lemma 37 *Let $k \geq 2$ be an integer, let A be an integral domain of characteristic $p > 0$ containing μ_k, and let $a \in A$ be a non-zero element. Let $d \geq 1$ be the largest integer dividing k such that a is a d-th power in A and fix a root $b = \sqrt[d]{a} \in A$. Write $e = k/d$. Consider the following factorization of $y^k - a$ in $A[y]$*

$$y^k - a = \prod_{\epsilon^d = 1} (y^e - \epsilon b) \tag{4.1}$$

where the product takes into account the multiplicities of the zeros of $x^k - 1$. Then (4.1) is the factorization of $y^k - a$ in irreducible elements of $A[y]$.

Proof. We have that each irreducible factor in $A[y]$ is non-constant because $y^k - a$ is a monic polynomial. Write F for the field of fractions of A. Since we have the factorization given in (4.1), it is enough to show that each irreducible factor of $y^k - a$ in $F[y]$ has degree e.

Let K be the splitting field of $y^k - a$ and let $\alpha \in K$ be a fixed root of it. Since $\mu_k \subseteq F$ we have $K = F(\alpha)$. We define $e' = [K : F]$. Note that if g is an irreducible factor of $y^k - a$ in $F[y]$ then the splitting field of g also is K because the roots of g in K are of the form $\epsilon\alpha$ for some $\epsilon \in \mu_k$, and we have $\mu_k \subseteq F$. Hence all the irreducible factors of $y^k - a$ have the same degree e', and we conclude that $d' = k/e'$ is an integer.

Let g be an irreducible factor of $y^k - a$ in $F[y]$. Observe that $e' \leq e$ because we have the factorization given in (4.1). Write $\alpha_1, \ldots, \alpha_{e'}$ for the (possibly repeated) zeros of g in K. Since the α_i are zeros of $y^k - a$, and the zeros of $y^k - a$ are of the form $\epsilon\alpha$ for some $\epsilon \in \mu_k$, we conclude that

$$\prod_{i=1}^{e'} \alpha_i = \epsilon_0 \alpha^{e'} = \epsilon_0 \sqrt[k]{a}^{e'}$$

for some $\epsilon_0 \in \mu_k$. In particular, by the Vieta's Formula and using the fact that $\epsilon_0 \in F$ we have that $\sqrt[d']{a} = \sqrt[k]{a}^{e'} \in F$, where $d' = k/e' \geq k/e = d$. By maximality of d we conclude that $d' = d$ and $e' = e$. ∎

Lemma 38 *Let $k \geq 2$ be an integer, let K be a field of characteristic $p > 0$ and choose an algebraic closure Ω_p for K. If a polynomial $h \in K[x]$ is a k-th power*

in $\Omega_p[x]$, then h can be written in the form $h = \alpha g^k u$ where $\alpha \in K$, $g \in K[x]$ is monic, and $u \in K[x^p]$ is a monic polynomial not divisible by a non-constant k-th power in $K[x]$.

Proof. Write h in the form $h = \alpha g^k u$ where $\alpha \in K$, $g \in K[x]$ is monic and has degree as large as possible, and $u \in K[x]$ is monic. If u is constant we are done, so we assume u non constant. Write the factorization of u in the form $u = h_1^{a_1} \cdots h_r^{a_r}$ with all the h_i distinct, monic and irreducible, and note that $0 < a_i < k$ for each i because of the choice of g. Since the h_i are coprime in $K[x]$, they are coprime in $\Omega_p[x]$ and therefore each $h_i^{a_i}$ is a k-th power in $\Omega_p[x]$ (since h is a k-th power by hypothesis). From this we conclude that for each i the polynomial h_i splits in $\Omega_p[x]$ as $h_i = \prod_j (x - \alpha_{ij})^{b_{ij}}$ where k divides each $a_i b_{ij}$. Each b_{ij} is strictly greater than 1 because $a_i < k$ and k divides $a_i b_{ij}$. Therefore, for each i the polynomial h_i is not separable, which means that each h_i belongs to $K[x^p]$. ∎

Corollary 39 *Let $k \geq 2$ be an integer, let K be a field of characteristic $p > k$ containing exactly k different k-th roots of 1, and let $f \in K[x]$ be a monic polynomial of degree k. Write d for the largest integer dividing k such that f is a d-th power in $K[x]$, fix $g \in K[x]$ satisfying $f = g^d$ and define $e = k/d$. The polynomial g can be chosen monic and the factorization of the polynomial $y^k - f \in K[x, y]$ in irreducible elements of $K[x, y]$ is*

$$y^k - f = \prod_{\epsilon \in \mu_d} (y^e - \epsilon g)$$

where each factor is absolutely irreducible.

Proof. Since f is monic, its d-th roots have as leading coefficients the elements of μ_d, hence we can take g monic.

Write $F = y^k - f$. Since the total degree of F is the same as the degree in x and in y, each non-constant factor of F must depend on both x and y. Hence, instead of considering the factorization of F in $K[x, y]$ we will rather consider the factorization of F in $K[x][y]$. By Lemma 37, the only remaining part is to show that the factors $y^e - \epsilon g$ are absolutely irreducible.

Assume that $y^e - \epsilon g$ is reducible in $\Omega_p[x, y]$ where Ω_p is an algebraic closure of K. Since the total degree of $y^e - \epsilon g$ is the same as the degree in x and in y, each non-constant factor of it must depend on both x and y. Hence $y^e - \epsilon g$ is reducible in $\Omega_p[x][y]$ and Lemma 37 implies that ϵg is a r-th power in $\Omega_p[x]$ for some $r > 1$ dividing e. Note that ϵg has no non-constant factor in $K[x^p]$ because $k < p$ and, moreover, g is monic and the only s dividing e such that g is an s-th power in $K[x]$ is $s = 1$, by maximality of d. This contradicts Lemma 38. ∎

Since the multiplicative group of a finite field is cyclic, the following is clear.

Lemma 40 *If $k \geq 2$ is an integer and $p > 2$ is a prime number of the form $kl + 1$, then*

$$|P(\mathbb{F}_p, k)| = \frac{p-1}{k} + 1.$$

More precisely, in $\mathbb{F}_p$ the element 0 has only one k-th root, and the number of k-th roots for each nonzero $n \in P(\mathbb{F}_p, k)$ is k. In particular, the field $\mathbb{F}_p$ (under the same hypotheses for p) has exactly k different k-th roots of 1.

Definition 41 *If K is a field, k an integer and $f \in K[x]$ a polynomial, then we define the set*

$$S(K, k, f) = \{x \in \mathbb{F}_p \colon f(x) \in P(K, k)\}.$$

Proposition 42 *Let $k \geq 2$ be an integer and p be a prime of the form $kl + 1$. Let $f \in \mathbb{F}_p[x]$ be a monic polynomial of degree k and let d be the largest integer such that f is a d-th power in $\mathbb{F}_p[x]$. If we write $e = k/d$ then we have*

$$|S(\mathbb{F}_p, k, f)| \leq \frac{1}{e}(p+1) + \frac{(e-1)(e-2)}{e}\sqrt{p} + k - 2.$$

Proof. The field $\mathbb{F}_p$ has k different k-th roots of 1 because p is of the form $kl+1$, by lemma 40. Define $F = y^k - f(x) \in \mathbb{F}_p[x, y]$ and let $Z = \mathbb{V}(F) \subseteq \mathbb{A}^2$ be the zero locus of F in the affine plane. By Corollary 39, Z has d reduced absolutely irreducible components $X_1, \ldots, X_d$ each one of degree e. By the Riemann Hypothesis for curves (see [2] for the case of singular curves) we conclude that the number of $\mathbb{F}_p$-rational points of the projective closure of each X_i is at most

$$p + 1 + (e-1)(e-2)\sqrt{p}.$$

The projective closure of Z meets the line at infinity at the points $[1 : \epsilon : 0]$ where ϵ ranges in μ_k, therefore we get

$$|Z(\mathbb{F}_p)| \leq d(p+1) + d(e-1)(e-2)\sqrt{p} - k. \tag{4.2}$$

Let us now estimate $|Z(\mathbb{F}_p)|$ in a different way. We write $P = P(\mathbb{F}_p, k)$ and $S = S(\mathbb{F}_p, k, f)$. Note that a point $(x, y) \in Z(\mathbb{F}_p)$ is a solution of the system

$$\begin{cases} f(x) = r \\ y^k = r \end{cases}$$

where $r \in P$. Let us write

$$S_r = \{x \colon f(x) = r\}.$$

It is clear that the sets S_r are disjoint. Indeed they form a partition of S because by hypothesis we have $f(x) \in P$ if and only if $x \in S$. Since $\deg f = k$, for each $r \in P$ we have $|S_r| \leq k$. Also, by Lemma 40 the second equation has k solutions for each nonzero $r \in P$ and just one solution for $r = 0$. Hence the total number of solutions of the system is

$$\begin{aligned} |Z(\mathbb{F}_p)| &\geq |S_0| + \sum_{r \in P \smallsetminus \{0\}} k|S_r| = (1-k)|S_0| + \sum_{r \in P} k|S_r| \\ &\geq (1-k)k + k|S| \end{aligned}$$

therefore we have

$$k|S| - k(k-1) \leq |Z(\mathbb{F}_p)| \leq d(p+1) + d(e-1)(e-2)\sqrt{p} - k$$

which gives the desired bound. ∎

Proof of Theorem 33. Under the definitions and the hypotheses of Theorem 33 we will prove that, if f is not a k-th power in $\mathbb{F}_p[x]$ then $|S(\mathbb{F}_p, k, f)| < M$. We write $S = S(\mathbb{F}_p, k, f)$. From the previous proposition we have

$$|S| \leq \frac{1}{e}(p+1) + \frac{(e-1)(e-2)}{e}\sqrt{p} + k - 2$$

where e is a divisor of k depending on f. Note that $e \geq 2$ because f is not a k-th power. When $k = 2$ the conclusion follows, so we consider the general case with $p > 4k^2$. Since the constant M does not depend on f we have to find a bound for $|S|$ not depending on f, therefore we have

$$\begin{aligned}
|S| &\leq \frac{1}{e}(p+1) + \frac{(e-1)(e-2)}{e}\sqrt{p} + k - 2 \\
&\leq \frac{1}{c}(p+1) + (k-2)\sqrt{p} + k - 2 \\
&\leq \frac{1}{c}p + (k-1)\sqrt{p} + k + \frac{1}{c} - 2 - 2k \qquad \text{because } \sqrt{p} > 2k \\
&< \frac{1}{c}p + (k-1)\sqrt{p} - (k+1) \\
&< \left\lfloor \frac{1}{c}p + (k-1)\sqrt{p} - k \right\rfloor = M
\end{aligned}$$

(we recall to the reader that c stands for the least prime divisor of k). Observe that

$$M < \frac{1}{c}p + (k-1)\sqrt{p} \leq \frac{1}{2}p + \left(\frac{1}{2}\sqrt{p} - 1\right)\sqrt{p} = p - \sqrt{p}$$

hence the obtained upper bound for $|S|$ still is smaller than p. ◇

Proof of Corollary 34. Let $(x_n)_{n=1}^M$ be a sequence in $\mathbb{F}_p$ satisfying

$$\Delta^{(k)}(x_n^k)_{n=1}^M = (k!, \ldots, k!),$$

with M as in the hypothesis. Solving the recurrence for the x_i^k in terms of the index i and the first initial values $x_1^k, \ldots, x_k^k$, we get $x_n^k = f(n)$ where $f \in \mathbb{F}_p[x]$ is a monic polynomial of degree k. Hence Theorem 33 implies that there exists $\nu \in \mathbb{F}_p$ such that $x_n^k = (\nu + n)^k$. ◇

4.3. The case of squares

Theorem 33 can be improved for the case $k = 2$. Given a degree 2 polynomial f, we can count the exact number of $n \in \mathbb{F}_p$ such that $f(n)$ is a square. This

refinement does not give more information for $\mathrm{BP}_2(\mathbb{F}_p)$.

Proof of Proposition 35: We use the notation given in the statement. Since we have

$$f = \left(x + \frac{u}{2}\right)^2 - \frac{u^2}{4} + v,$$

up to a linear change of variable, we can assume that $f = x^2 + a$ (note that $a \neq 0$ because f is not a square by hypothesis). Define $F = y^2 - f(x) \in \mathbb{F}_p[x, y]$ and $Z = \mathbb{V}(F) \subseteq \mathbb{A}^2$. The projective closure of Z is a smooth projective conic defined over $\mathbb{F}_p$ hence it has $p + 1$ rational points over $\mathbb{F}_p$. Note that it meets the line at infinity at $[1 : 1 : 0]$ and $[1 : -1 : 0]$, therefore $|Z(\mathbb{F}_p)| = p - 1$.

Define $\pi : Z \to \mathbb{A}^1$ as the restriction of the projection $(x, y) \mapsto x$. Since the map π has degree 2, if we define $R \subseteq \mathbb{A}^1(\mathbb{F}_p)$ to be the set of points having exactly one $\mathbb{F}_p$-rational preimage via π then we obtain

$$|\pi(Z(\mathbb{F}_p))| = \frac{1}{2}\left(|Z(\mathbb{F}_p)| + |R|\right) = \frac{1}{2}\left(p - 1 + |R|\right).$$

We note that $S = \pi(Z(\mathbb{F}_p))$, thus we have to compute $|R|$. Given $q = (u, v) \in Z$, the point $q' = (u, -v)$ satisfies $\pi(q) = u = \pi(q')$, thus $u \in R$ if and only if $v = 0$. Therefore the number $|R|$ is the number of solutions of the equation $x^2 + a = 0$, that is $1 + \left(\frac{-a}{p}\right)$. Finally

$$|S| = \frac{1}{2}\left((p - 1) + 1 + \left(\frac{-a}{p}\right)\right).$$

$\diamond$

Capítulo 5

Büchi's problem for the ring of p-adic entire functions and consequences in Logic

5.1. Background

In this section we present the results we need from p-adic Analysis, and, in doing this, we will fix the notation we are going to use throughout this chapter. The results in this section are well known. For a general reference on non-archimedean Complex Analysis see for example [27].

All the results in this section (and this chapter) remain valid if we consider an algebraically closed field of characteristic zero, complete with respect to a non-trivial non-archimedean valuation. However, in order to simplify the statements of the results, we will work with $\mathbb{C}_p$, which is the completion of the algebraic closure of $\mathbb{Q}_p$ (and satisfies all the requirements we said). Since we are going to work with entire functions only, the results stated in this section are not in there general forms, but they are enough for our purposes.

The expression

$$h(z) = \sum_{n \geq 0} a_n z^n$$

defines a function $h : \mathbb{C}_p \to \mathbb{C}_p$ whenever for all $z \in \mathbb{C}_p$ we have $|a_n z^n|_p \to 0$ as $n \to \infty$. We define $\mathcal{A}_p$ as the set of all such functions. They are called global analytic functions over $\mathbb{C}_p$ or entire functions. One can prove that $\mathcal{A}_p$ is an integral domain. Let $\mathcal{M}_p$ be the field of fractions of $\mathcal{A}_p$. It is called the field of (global) meromorphic functions.

Proposition 43 *Any entire function h is differentiable, its analytic derivative coincides with its formal derivative, and h' is entire. If $h' = 0$ then h is constant.*

If h is entire and $a \in \mathbb{C}_p$, then h admits a convergent Taylor power series at a. This power series allows us to define the order at a of h, denoted by $\operatorname{ord}_a h$, as in the complex case. It can be proved that a meromorphic function without poles is actually analytic.

For $h \in \mathcal{A}_p$ and $r > 0$ we define

$$|h|_r = \max_{n \geq 0} |a_n|_p r^n$$

and, for non-zero h,

$$\nu(r, h) = \max\{n \colon |a_n|_p r^n = |h|_r\}$$

We also define $\nu(0, h) = \lim_{r \to 0^+} \nu(r, h)$.

Proposition 44 *Let $r > 0$. The function $|\cdot|_r : \mathcal{A}_p \to \mathbb{R}$ defines a non-Archimidean absolute value, and if h is constant then $|h|_r = |h|_p$.*

One can easily prove the following.

Proposition 45 *If $h \in \mathcal{A}$ is non-constant, then there exists R such that $|h|_r > 1$ for $r > R$. Moreover, there exists a positive constant C such that $|h|_r \geq Cr$ as $r \to \infty$.*

Theorem 46 *(Poisson-Jensen Formula) Let $h = \sum_n a_n z^n$ be an entire non-constant function. The function $\nu(r, h)$ increases as $r \to \infty$ and*

$$\log |h|_r = \log |a_{\nu(0,h)}|_p + \int_0^r \frac{\nu(t, h) - \nu(0, h)}{t} + \nu(0, h) \log r.$$

Theorem 47 *(Weierstrass Preparation Theorem) Given $h \in \mathcal{A}_p$ non-zero there exist a unique monic polynomial P of degree $\nu(r, h)$ and a function g analytic on $B[r]$ such that $f = Pg$, g does not have any zero in $B[r]$, and P has exactly $\nu(r, h)$ zeros on $B[r]$ (counting multiplicity).*

For $r \geq 0$ and $h \in \mathcal{A}_p$ define $n(r, h, 0)$ as the number of zeros of f in $B[r]$ counting multiplicity. Then $n(r, h, 0) = \nu(r, h)$ by Theorem 47. We define

$$N(r, h, 0) = \int_0^r \frac{n(t, h, 0) - n(0, h, 0)}{t} + n(0, h, 0) \log r.$$

Hence by Theorem 46 we have

$$N(r, h, 0) = \log |h|_r - \log |a_{n(0,h,0)}|_p \tag{5.1}$$

for each entire non-constant function $h = \sum_n a_n z^n$. Actually this last equation holds for all non-zero entire function (the constant case is trivial). For $h \in \mathcal{A}_p, r > 0$ define

$$m(r, h) = \log^+ |h|_r$$

where $\log^+ s = \max\{\log s, 0\}$. As $n(r, h, 0) = \nu(r, h)$, Theorem 46 implies that $n(r, h, 0)$ is a non-decreasing function on r for each entire function $h \neq 0$. Thus, by Equation (5.1) we have

Proposition 48 *For $h \in \mathcal{A}_p$ non-zero holds*

$$N(r,h,0) = m(r,h) + \mathcal{O}(1).$$

The following result is proved in [7]

Theorem 49 *(Logarithmic Derivative Lemma) Let $h \in \mathcal{A}_p$ be non-zero, and $l \in \mathbb{Z}$ a positive integer. Then $r^l |h^{(l)}|_r \leq |h|_r$.*

Corollary 50 *If $h \in \mathcal{A}_p$ is non-zero and $r > 1$ then*

$$m(r,h') \leq m(r,h) - \log r + \mathcal{O}(1)$$

as $r \to \infty$.

As a final remark, observe that

$$N(r,h,0) = C + \int_1^r \frac{n(r,h,0)}{t} dt$$

thus, inequalities related to $n(r,\cdot,0)$ can be translated to inequalities about $N(r,\cdot,0)$ up to a bounded term.

5.2. Representation of squares by a polynomial of degree two in $\mathcal{A}_p[X]$.

The purpose of this section is to prove the following result.

Theorem 51 *Let $F = X^2 + uX + v \in \mathcal{A}_p[X]$ be a polynomial having a non-constant coefficient. If $F(a)$ is a square in $\mathcal{A}_p$ for at least 13 values of $a \in \mathbb{C}_p$ then F is a square in $\mathcal{A}_p[x]$.*

In order to simplify the proof, we will prove the Theorem in the following equivalent form:

Theorem 52 *Let $h_j \in \mathcal{A}_p, j = 1, \ldots, M$ with at least one of them non-constant, and let $a_j \in \mathbb{C}_p$ be distinct for $j = 1, \ldots, M$. Assume we have $f, g \in \mathcal{A}_p$ with f, g non-zero, such that $h_j^2 = (a_j + f)^2 - g$ for $j = 1, \ldots, M$. Then $M \leq 12$.*

We will assume $M > 12$ to obtain a contradiction.

Lemma 53 *The function f is non-constant.*

Proof. Suppose that f is constant. Then $(h_i - h_j)(h_i + h_j) = (a_i - a_j)(a_i + a_j + 2f)$ also is constant for $i \neq j$, hence each $h_i = \frac{1}{2}\left((h_i - h_j) + (h_i + h_j)\right)$ is constant, which contradicts the hypothesis. ∎

For $i \neq j$ we have

$$h_i^2 - h_j^2 = \big((a_i + f)^2 - g\big) - \big((a_j + f)^2 - g\big) = 2(a_i - a_j)f + (a_i^2 - a_j^2)$$

hence, for each r we have

$$2 \max_n m(r, h_n) \geq m(r, h_i^2 - h_j^2) = m(r, f) + \mathcal{O}(1) \tag{5.2}$$

and the equality $g = (a_j + f)^2 - h_j^2$ implies

$$m(r, g) \leq 2 \max\{m(r, a_j + f), m(r, h_j)\} + \mathcal{O}(1) \leq 4 \max_n m(r, h_n) + \mathcal{O}(1). \tag{5.3}$$

From the hypothesis, we obtain

$$\begin{aligned} h_n^2 + g &= (a_n + f)^2 \\ 2h_n' h_n + g' &= 2f'(a_n + f) \end{aligned}$$

where the second equation is obtained from the first one differentiating. From this we deduce

$$(2h_n' h_n + g')^2 = 4f'^2(h_n^2 + g)$$

and reordering we get

$$g'^2 - 4f'^2 g = 4h_n(h_n f'^2 - {h_n'}^2 h_n - h_n' g'). \tag{5.4}$$

We define

$$\begin{aligned} \Delta &= g'^2 - 4f'^2 g \\ \Delta_n &= h_n f'^2 - {h_n'}^2 h_n - h_n' g' \end{aligned}$$

hence, from 5.4 we derive

$$\Delta = 4h_n \Delta_n$$

Lemma 54 *The function Δ is the zero function.*

Proof. We suppose Δ is not identically zero. The point is that, in this case, we can apply the function $m(r, \cdot)$ to Δ, and we will obtain a contradiction by bounding above and below $m(r, \Delta)$. We split the proof in three claims.

Claim 55 *For each r large enough, we have*

$$m(r, \Delta) \leq 6 \max_n m(r, h_n) - 2 \log r + \mathcal{O}(1).$$

Proof of Claim 55. By definition of Δ we have

$$\begin{aligned} m(r, \Delta) &= m(r, h_n) + m(r, \Delta_n) + \mathcal{O}(1) \\ &\leq m(r, h_n) + \max\{m(r, h_n f'^2), m(r, {h_n'}^2 h_n), m(r, h_n' g')\} + \mathcal{O}(1) \end{aligned}$$

In order to estimate an upper bound for this last expression, by the inequalities (5.2) and (5.3) and Corollary 50 we obtain for each r large enough

$$\begin{aligned} m(r, h_n f'^2) &\leq m(r, h_n) + 2m(r, f) - 2\log r + \mathcal{O}(1) \\ &\leq 5 \max_n m(r, h_n) - 2\log r + \mathcal{O}(1) \\ m(r, h_n'^2 h_n) &\leq m(r, h_n) + 2m(r, h_n) - 2\log r + \mathcal{O}(1) \\ &\leq 3 \max_n m(r, h_n) - 2\log r + \mathcal{O}(1) \\ m(r, h_n' g') &\leq m(r, h_n) + m(r, g) - 2\log r + \mathcal{O}(1) \\ &\leq 5 \max_n m(r, h_n) - 2\log r + \mathcal{O}(1) \end{aligned}$$

Therefore, for each r large enough we have

$$m(r, \Delta) \leq 6 \max_n m(r, h_n) - 2\log r + \mathcal{O}(1).$$

$\diamond$

Claim 56 *For each r large enough, we have*

$$\max m(r, h_n) \leq \frac{1}{M-1} \sum_n m(r, h_n) + \mathcal{O}(1)$$

Proof of Claim 56. Given an r, if all the $m(r, h_n)$ are equal the result is obvious, so let us assume that we have two indices s, t such that $m(r, h_s)$ is minimal, $m(r, h_t)$ is maximal and $m(r, h_s) \neq m(r, h_t)$. For r large enough and for all $i \neq j$ we have $|2f|_r = |a_i + a_j + 2f|_r$ by Lemma 53 and Proposition 45, moreover, $|2f|_r > 1$ for large r. Write $C = \log^+ \max_{i \neq j} |a_i - a_j|_p$ and note that this constant does not depend on r. Since $h_i^2 - h_j^2 = (a_i - a_j)(a_i + a_j + 2f)$ we have for r large enough

$$m(r, f) \leq m(r, h_i^2 - h_j^2) \leq m(r, f) + C.$$

On the one hand, by the strong triangle inequality of $|\cdot|_r$ we have for each n

$$m(r, f) + C \geq m(r, h_t^2 - h_s^2) = 2m(r, h_t) = 2 \max_n m(r, h_n).$$

On the other hand, for each $n \neq s$ we have

$$2m(r, h_n) \geq m(r, h_n^2 - h_s^2) \geq m(r, f).$$

adding these inequalities as long as $n \neq s$ we get

$$2 \sum_n m(r, h_n) \geq 2 \sum_{n \neq s} m(r, h_n) \geq (M-1) m(r, f).$$

Therefore

$$2 \sum_n m(r, h_n) \geq (M-1) m(r, f) \geq (M-1)(2 \max_n m(r, h_n) - C).$$

$\diamond$

Claim 57 *For each r large enough, we have*

$$\frac{1}{2}\sum_n m(r,h_n) \leq m(r,\Delta) + \mathcal{O}(1)$$

Proof of Claim 57. Define

$$n(r) = \sum_{|\rho|\leq r} \max_n \operatorname{ord}_\rho h_n$$

and note that this sum is always finite because the h_n are entire. Since $4h_n\Delta_n = \Delta$ holds for each n and Δ is not identically zero, we have $\operatorname{ord}_\rho h_n \leq \operatorname{ord}_\rho \Delta$ for each n and each ρ, therefore $n(r) \leq n(r,\Delta,0)$.

Observe that no three of the h_i can share a zero (if ρ is a common zero of h_i, h_j, h_k for distinct indices, then the polynomial $(f(\rho)+X)^2 - g(\rho)$ has three roots, namely a_i, a_j, a_k), hence

$$\sum_n n(r,h_n,0) \leq 2n(r)$$

and we arrive to

$$\sum_n n(r,h_n,0) \leq 2n(r,\Delta,0)$$

hence

$$\sum_n N(r,h_n,0) \leq 2N(r,\Delta,0) + \mathcal{O}(1).$$

This and Proposition 48 lead to

$$\sum_n m(r,h_n) \leq 2m(r,\Delta) + \mathcal{O}(1).$$

◇

Therefore, by the previous Claims we have

$$2\log r + \frac{1}{2}\sum_n m(r,h_n) \leq \frac{6}{M-1}\sum_n m(r,h_n) + \mathcal{O}(1)$$

which is a contradiction for $M > 12$. This proves that $\Delta = 0$. ■

From the equation $\Delta = 0$ we have

$$g'^2 = 4f'^2 g. \tag{5.5}$$

By Lemma 53 we have that f is non-constant, hence the equation $g'^2 = 4f'^2 g$ implies that g is a square in $\mathcal{M}_p$, but $g \in \mathcal{A}_p$ implies that g is a square in $\mathcal{A}_p$. Thus $g = u^2$ for some $u \in \mathcal{A}_p$ and replacing in Equation (5.5) we get $u'^2 = f'^2$. Therefore there exists $b \in \mathbb{C}_p$ and $\alpha \in \{-1,1\}$ such that $g = (\alpha f + b)^2$, hence

$$\begin{aligned} h_n^2 &= (a_n+f)^2 - (\alpha f + b)^2 \\ &= (a_n+f)^2 - (f+\alpha b)^2 \\ &= (a_n - \alpha b)(a_n + \alpha b + 2f). \end{aligned}$$

Observe that this and Lemma 53 imply h_n non-constant for all n such that $a_n \neq \alpha b$, and this is the case for al but at most one index m since the a_n are pairwise distinct. Define

$$v_n = \frac{f_n}{a_n - \alpha b}$$

for each $n \neq m$, and note that each v_i is non-constant. Take any two indices $i \neq j$ such that $i, j \neq m$. We have

$$(v_i - v_j)(v_i + v_j) = v_i^2 - v_j^2 = (a_i + \alpha b + 2f) - (a_j + \alpha b + 2f) = a_i - a_j$$

and this implies that $v_i - v_j$ and $v_i + v_j$ are constant, therefore each $v_i = \frac{1}{2}((v_i + v_j) + (v_i - v_j))$ is constant. This is the desired contradiction, and the proof of Theorem 52 is complete.

5.3. Büchi's Problem and consequences in Logic

We begin this section stating and proving the Büchi's Problem for $\mathcal{A}_p$.

Theorem 58 *If a sequence of p-adic entire functions $(x_i)_{i=1}^{13}$, satisfies*

$$\Delta^{(2)}(x_i^2)_{i=1}^{13} = (2, \ldots, 2)$$

(that is, $(x_i^2)_{i=1}^{13}$ has 2nd differences constant and equal to 2) and not all the x_i are constant, then there exists a p-adic entire function ν such that $x_i^2 = (\nu + i)^2$ for each i.

Proof. Let $(x_n)_{n=1}^{13}$ be a sequence in $\mathcal{A}_p$ satisfying

$$\Delta^{(2)}(x_n^2)_{n=1}^{13} = (2, \ldots, 2),$$

Solving the recurrence for the x_i^2 in terms of the index i and the first initial values x_1^2, x_2^2, we get $x_n^2 = F(n)$ where $F \in \mathcal{A}_p[X]$ is a monic polynomial of degree 2. Moreover, F has some non-constant coefficient because not all the x_i are constant. Hence Theorem 52 implies that there exists $\nu \in \mathcal{A}_p$ such that $x_n^2 = (\nu + n)^2$. ∎

Consider the language $\mathcal{L}_2^z = \{0, 1, +, f_z, P_2\}$ where P_2 is a symbol of relation such that $P_2(x)$ is interpreted in $\mathcal{A}_p$ as 'x is a square' and f_z is a symbol of function such that $f_z(x)$ is interpreted in $\mathcal{A}_p$ as '$x \mapsto zx$'. Clearly $\mathcal{A}_p$ is a $\mathcal{L}_2^z$-structure. We have:

Theorem 59 *Multiplication is positive existentially definable in $\mathcal{A}_p$ over the language $\mathcal{L}_2^z$.*

Proof. By Theorem 58, the following $\mathcal{L}_2$-formula

$$F[x, y] : \exists u_1 \cdots \exists u_{35} \left(\wedge_{i=1}^{35} P_2(u_i)\right) \wedge \left(\wedge_{i=2}^{34} u_{i-1} + u_{i+1} = 2u_i + 2\right) \wedge x = u_1 \wedge 2y + 1 = u_2 - u_1$$

is satisfied in $\mathcal{A}_p$ if and only if $y = x^2$ or $x, y \in \mathbb{C}_p$. Then the $\mathcal{L}_2^z$-formula

$$G[x, y] : F[x, y] \wedge F[f_z x, f_z f_z y]$$

is satisfied in $\mathcal{A}_p$ if and only if $y = x^2$.

Therefore, the $\mathcal{L}_2^z$-formula

$$H[x, y, w] : \exists u \exists v \left(G[x + y, u] \wedge G[x - y, v] \wedge u = v + 4w \right)$$

is satisfied in $\mathcal{A}_p$ if and only if $w = xy$. Note that all the formulas are positive existential. ∎

Define the language $\mathcal{L}_R^z = \{0, 1, +, \cdot, z\}$. We recall that the positive existential theory of $\mathcal{A}_p$ in the language $\mathcal{L}_R^z$ is undecidable (see [15]). From this, the fact that $f_z 1 = z$, and Theorem 59 we conclude

Theorem 60 *The positive existential theory of $\mathcal{A}_p$ in the language $\mathcal{L}_2^z$ is undecidable.*

One can state this result in terms of systems of equations. A *system of diagonal quadratic equations with coefficients in* $\mathbb{Z}[z]$, is a system of equations of the form

$$\sum_{i=1}^{r} a_{ij} x_i^2 = b_j \quad j = 1, \ldots, s$$

where the a_{ij} and b_j belong to $\mathbb{Z}[z]$.

Theorem 61 *There is no algorithm to do the following: Given a system of diagonal quadratic equations with coefficients in $\mathbb{Z}[z]$, to decide whether it has solution in $\mathcal{A}_p$ or not.*

Proof. From Theorem 60 we obtain directly the non-existence of an algorithm to solve the following problem:

Given a finite number of systems of the form

$$\sum_{i=1}^{r} a_{ij} x_i^2 + \sum_{k=1}^{t} c_{kj} y_k = b_j \quad j = 1, \ldots, s \tag{5.6}$$

with all the a_{ij}, c_{kj}, b_j in $\mathbb{Z}[z]$, to decide whether at least one of these systems has solution in $\mathcal{A}_p$.

So we can assume we are dealing with a single system (if we had an algorithm to decide in this case, we could apply it several times to get a contradiction).

In the System (5.6) we replace each y_k by $u_k^2 - v_k^2$ to obtain

$$\sum_{i=1}^{r} a_{ij} x_i^2 + \sum_{k=1}^{t} c_{kj} (u_k^2 - v_k^2) = b_j \quad j = 1, \ldots, s. \tag{5.7}$$

System (5.7) has solutions if and only if System (5.6) has, because of the identity

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

Therefore there is no algorithm to decide whether a general system of the form (5.7) has solutions in $\mathcal{A}_p$ or not. ∎

Bibliografía

[1] D. Allison, *On square values of quadratics*, Math. Proc. Camb. Philos. Soc. **99**, no. 3, 381-383 (1986).

[2] Y. Aubry and M. Perret, *A Weil theorem for singular curves*, Proceedings of Arithmetic, Geometry and Coding Theory IV, ed. Pellikaan, Perret, Vladut, De Gruyter, 1-7 (1995).

[3] A. Bremner, *On square values of quadratics*, Acta Arith. **108**, no. 2, 95-111 (2003).

[4] J. L. Britton, *Integers solutions of systems of quadratic equations*, Math. Proc. of the Cambridge Phil. Soc. **86**, 385-389 (1979).

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

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

[7] W. Cherry and Z. Ye, *Non-Archimedean Nevanlinna theory in several variables and non-Archimedean Nevanlinna inverse problem*, Transactions of the American Mathematical Society **349**, 5047-5071, (1997).

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

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

[10] 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).

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

[12] D. Hensley, *Sequences of squares with second difference of two and a problem of logic*, unpublished (1980-1983).

[13] —— *Sequences of squares with second difference of two and a conjecture of Büchi*, unpublished (1980-1983).

[14] 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, 677-680, (1990).

[15] L. Lipshitz and T. Pheidas, *An analogue of Hilbert's tenth problem for p-adic entire functions*, Jour. Symb. Logic **60**, no. 4 (1995).

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

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

[18] L. Moret-Bailly and A. Shlapentokh, *Diophantine Undecidability of Holomorphy Rings of Function Fields of Characteristic Zero*, Annales de l'Institut Fourier **59-5**, 2103-2118 (2009).

[19] H. Pasten, *An extension of Büchi's Problem for polynomial rings in zero characteristic*, Proc. Amer. Math. Soc. **138**, 1549-1557 (2010).

[20] T. Pheidas and X. Vidaux, *Extensions of Büchi's problem: Questions of decidability for addition and n-th powers*, Fundamenta Mathmaticae **185**, 171-194 (2005).

[21] —— *The analogue of Büchi's problem for rational functions*, Journal of The London Mathematical Society **74-3**, 545-565 (2006).

[22] —— *Corrigendum: The analogue of Büchi's problem for rational functions*, submitted to the Journal of the London Mathematical Society (2009).

[23] —— *The analogue of Büchi's problem for cubes in rings of polynomials*, Pacific Journal of Mathematics **238** (2), 349-366 (2008).

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

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

[26] B. Poonen, *Hilbert's Tenth Problem over rings of number-theoretic interest*, downloadable from http://math.mit.edu/∼poonen/papers/aws2003.pdf

[27] A. M. Robert, *A course in p-adic analysis*, Springer, Graduate Texts in Mathematics **198**.

[28] A. Shlapentokh, *Hilbert's tenth problem - Diophantine classes and extensions to global fields*, New Mathematical Monographs **7**, Cambridge University Press (2007).

[29] A. Shlapentokh and X. Vidaux *The analogue of Büchi's problem for function fields*, preprint.

[30] Th. Skolem, *Diophantische Gleichungen*, Ergebnisse d. math. u. Ihrer Grenzgebiete, Bd. 5, Julius Springer (1938).

[31] X. Vidaux, *An analogue of Hilbert's tenth problem for fields of meromorphic functions over non-Archimedean valued fields*, Journal of Number Theory **101**, Issue 1, 48-73 (2003).

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

[33] H. Yamagishi, *On the solutions of certain diagonal quadratic equations and Lang's conjecture*, Acta Arithmetica **109-2** (2003).