UNIVERSIDAD DE CONCEPCIÓN
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
PROGRAMA DE DOCTORADO EN MATEMÁTICA

Problemas de definibilidad e indecidibilidad en algunos anillos de funciones

Profesor Guía: Xavier Vidaux
Codirector: Antonio Laface
Codirector: Thanases Pheidas (University of Crete-Heraklion, Greece)
Dpto. de Matemática
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

UNIVERSIDAD DE CONCEPCIÓN
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
PROGRAMA DE DOCTORADO EN MATEMÁTICA

Problemas de definibilidad e indecidibilidad en algunos anillos de funciones

Xavier Vidaux (Profesor Guía)
Antonio Laface (Codirector)
Thanases Pheidas (Codirector)
Ricardo Baeza Rodriguez (evaluador externo, miembro del jurado)
Angus Macintyre (evaluador externo, miembro del jurado)
Thomas Scanlon (evaluador externo)

Dpto. de Matemática
Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Tesis Defendida el 13 de Septiembre 2010

HÉCTOR HARDY PASTÉN VÁSQUEZ
CONCEPCIÓN-CHILE
2010

Problemas de Definibilidad e Indecidibilidad en algunos Anillos de Funciones
Definability and Undecidability Problems in some Rings of Functions

Héctor Pastén Vásquez
Universidad de Concepción

En estas breves palabras me gustaría expresar mi gratitud hacia el Departamento de Matemática de la Universidad de Concepción por darme las herramientas para llegar a esta instancia, especialmente a Cesar Flores por presentarme la opción de la Matemática profesional, el cual yo no conocía. Agradezco a Xavier Vidaux por supervisar esta Tesis y a Antonio Laface y Thanases Pheidas por co-supervisar. También aprovecho este espacio para agradecer a todos los matemáticos que dedicaron tiempo en revisar distintas partes de este trabajo en sus versiones previas, como Alain Escassut, Jacqueline Ojeda y Ricardo Baeza. Me disculpo desde ya si algún nombre escapa de mi memoria en este momento.

Agradezco especialmente a mis padres quienes desde siempre han fomentado mi gusto por las matemáticas y me dieron un enorme apoyo para llevar a cabo el cumplimiento de muchas de mis metas. Su apoyo fue fundamental.

Finalmente, agradezco de forma especial a Natalia, quien me ha acompañado en gran parte de este camino y ha significado un apoyo emocional y personal invaluable.

Dedico esta Tesis y todo el trabajo que significó a mis padres Olga y Héctor, mis hermanos Sofía y Johan, y a mi querida Natalia.

Contents

Chapter 1

Presentación - Presentation

1.1 En español

Nota Importante: Las notationes en los Capítulos 3 y 4 son independientes.

1.1.1 Plan de contenidos

El presente trabajo se estructura de la siguiente forma:

- En la sección 1.1.2 de este capítulo se entrega un resumen general del contenido de la investigación desarrollada, mientras que en la sección 1.1.3 del mismo se presenta brevemente un resumen de los resultados existentes relativos a los problemas estudiados, y de los resultados nuevos obtenidos en el transcurso de la investigación. Ambos puntos están es español y serán extendidos en los capítulos 3 y 4.

- En el capítulo 2 se entrega un resumen en español de las herramientas necesarias para abordar los problemas estudiados en los capítulos 3 y 4 y se fijan algunas convenciones.

- El capítulo 3 contiene una investigación desarrollada por el autor de esta Tesis. Se encuentra en inglés y cuenta con una introducción propia donde se explica de manera completa el contexto de la investigación y se presentan los resultados ya existentes. Además, cuenta con una sección donde se presentan los resultados nuevos. El objetivo central es estudiar la representación de cuadrados por medio de polinomios

de segundo grado en varios campos, principalmente sobre las funciones meromorfas p-ádicas, y deducir consecuencias en Lógica.

- El capítulo 4 contiene una investigación en conjunto desarrollada por Thanases Pheidas (codirector de la Tesis), Xavier Vidaux (director de la Tesis) y por el autor de esta Tesis. Al igual que el Capítulo 3, se encuentra en inglés y cuenta con una introducción propia donde se explica de manera completa el contexto de la investigación y los resultados nuevos. El objetivo central es estudiar definibilidad y codificación uniforme sobre familias de estructuras, para obtener algunos resultados fuertes de indecidibilidad.

- Finalmente, en el Capítulo 5 se entrega una lista de problemas abiertos relativos a la investigación y se presentan posibles direcciones en las que el trabajo se puede extender. Este capítulo se encuentra en español y en inglés.

1.1.2 Resumen

En el Capítulo 3 demostraremos un resultado sobre representación de cuadrados mediante polinomios mónicos de segundo grado en el campo de las funciones meromorfas p-ádicas (los polinomios considerados tienen sus coeficientes en este mismo campo), para así resolver el problema de Büchi de los n cuadrados en este campo. Usando este resultado, demostramos la no existencia de un algoritmo para decidir si un sistema de formas cuadráticas diagonales sobre $\mathbb{Z}[z]$ representa o no en el anillo de funciones enteras p-ádicas (con variable z) un vector dado de polinomios de $\mathbb{Z}[z]$, y un resultado similar para funciones meromorfas p-ádicas cuando los sistemas admiten condiciones de anulamiento sobre las incógnitas. Esto mejora la ya conocida respuesta negativa al análogo del Décimo Problema de Hilbert para estas estructuras. También mejoramos algunos resultados de Vojta relativos al caso de funciones meromorfas complejas, campos de funciones algebraicas y finalmente campos de números, y mostramos una directa conexión de esto último con la conjetura de Bombieri para superficies sobre campos de números.

Por otro lado, en el capítulo 4 se demuestran algunos resultados sobre definibilidad y codificación uniforme en familias de estructuras, y se obtienen a partir de ellos resultados de indecibilidad uniforme. Por ejemplo, la relación "$x \neq y$" se puede definir de manera uniforme sobre el lenguaje de anillos en

la familia de todos los campos, por medio de la fórmula

$$\exists u\, xu = 1 + yu.$$

El estudio del concepto de uniformidad nos permitirá obtener técnicas para probar resultados del siguiente tipo: no existe un algoritmo para saber si un sistema de ecuaciones diofantinas con condiciones del tipo "x no constante" sobre algunas variables x, admite o no solución en $\mathbb{F}_p[z]$ para infinitos p. Ésto contrasta fuertemente con la situación análoga sobre $\mathbb{F}_p$, donde es sabido que *si* existe un algoritmo para saber si o no un sistema de ecuaciones diofantinas tiene solución en $\mathbb{F}_p$ para infinitos p (en efecto, basta verificar si el sistema tiene alguna solución compleja, lo cual se puede decidir algorítmicamente). Además, obtenemos una definición de la relación "existe un número natural s tal que $x = y^{p^s}$ o $y = x^{p^s}$" sobre una amplia clase de anillos de funciones en característica p, donde la fórmula que se obtiene es positiva existencial y no utiliza el número p (en particular, para clases de anillos de funciones algebraicas cuyo campo de constante es algebraico sobre $\mathbb{F}_p$).

1.1.3 Introducción

This section is a short Spanish version of the introductions (in English) of Chapters 3 and 4.
Esta sección es un resumen extendido de las introducciones (en inglés) de los capítulos 3 y 4.

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, fue respondido negativamente por Matijasevich 70 años más tarde [Mat] 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 lenguaje moderno, lo que realmente se demostró es que los conjuntos recursivos de $\mathbb{Z}$ son diofantinos, y como consecuencia la teoría positiva existencial de $\mathbb{Z}$ es indecidible en el lenguaje de anillos $\{0, 1, +, \cdot\}$. A partir del Décimo Problema de Hilbert aparecen dos problemas naturales:

P1: Resolver análogos en otras estructuras.

P2: Si hay una respuesta negativa para un análogo del Décimo Problema en una $\mathcal{L}$-estructura $\mathfrak{M}$, debilitar el lenguaje $\mathcal{L}$ manteniendo la respuesta negativa.

Para el problema P1, una técnica que surge es tratar de codificar existencialmente $\mathbb{Z}$ en la estructura $\mathfrak{M}$ que nos interesa. De esta forma se puede responder negativamente el análogo del Décimo Problema en $\mathfrak{M}$ utilizando el resultado para $\mathbb{Z}$. En el Capítulo 4, esta idea será extendida a codificaciones uniformes sobre familias de estructuras, para obtener indecidibilidad en situaciones más generales.

Por otra parte, relativo al problema P2, J. R. Büchi estudió la posibilidad de debilitar el lenguaje de anillos y mantener el resultado de indecidibilidad para la teoría positiva existencial de enteros sobre el nuevo lenguaje. Concretamente, Büchi formuló una conjetura en teoría de números y probó (en un trabajo no publicado y comunicado póstumamente por Lipshitz [L]) que suponiendo que dicha conjetura era correcta, entonces la teoría positiva existencial de $\mathbb{Z}$ sobre $\mathcal{L}_2$ es indecidible, con el lenguaje

$$\mathcal{L}_2 = \{0, 1, +, P_2\},$$

donde P_2 es un símbolo de relación unaria que se interpreta de la siguiente forma: $P_2(k)$ sí y sólo si "*k es un cuadrado*". El problema aritmético que condiciona este resultado actualmente es conocido como el Problema de Büchi para enteros ($\mathbf{BP}_2(\mathbb{Z})$) y es el siguiente:

Problema. *Decidir si existe algún entero $N \geq 3$ 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 $x_i^2 = (x+i)^2, i = 1, \ldots, N$ para algún entero x.

Análisis numéricos del problema y argumentos heurísticos (ver [BB, Pi, He]) sugieren que $N = 5$ serviría, pero no se ha logrado probar siquiera que tal N exista. La conjetura es que $\mathbf{BP}_2(\mathbb{Z})$ tiene respuesta positiva, y en esta dirección Vojta [Vo2] demostró usando técnicas de Bogomolov que $\mathbf{BP}_2(\mathbb{Z})$ tiene respuesta positiva si asumimos una conjetura de Lang sobre puntos racionales en superficies de tipo general.

En muchos casos, dado un anillo $\mathfrak{M}$ y un lenguaje $\mathcal{L}$, si la teoría positiva existencial de $\mathfrak{M}$ sobre $\mathcal{L}$ es indecidible y si el análogo del problema de Büchi es cierto en $\mathfrak{M}$, entonces es posible utilizar el argumento de Büchi para debilitar $\mathcal{L}$ y mantener la indecidibilidad; por esto en particular nace el interés de resolver un análogo de $\mathbf{BP}_2(\mathbb{Z})$ sobre otros anillos.

Se sabe que tienen respuesta positiva análogos del problema de Büchi en varias estructuras, como por ejemplo $\mathbf{BP}_2(\mathcal{M})$, donde $\mathcal{M}$ es el campo de funciones meromorfas complejas, y $\mathbf{BP}_2(K)$, donde K es el campo de funciones de una curva algebraica en característica cero (ver [Vo2]), $\mathbf{BP}_2(F(z))$ donde F es un campo de característica cero o mayor que 18 (ver [PV1, PV2]), y recientemente $\mathbf{BP}_2(K)$ donde K es el campo de funciones de una curva algebraica en característica positiva y suficientemente grande (ver [SV]).

Representation of squares by monic second degree polynomials in the field of p-adic meromorphic functions

En el Capítulo 3 se resuelve un análogo del problema de Büchi para $\mathcal{M}_p$ (funciones meromorfas p-ádicas) con el objetivo de mejorar los resultados existentes de indecidibilidad para el anillo de funciones enteras p-ádicas y el campo de funciones meromorfas p-ádicas. También se estudiarán generalizaciones al problema de Büchi para campos de funciones de curvas en característica cero, para el campo de funciones meromorfas complejas, y consecuencias de la conjetura de Lang en generalizaciones al problema de Büchi para extensiones finitas de $\mathbb{Q}$ adaptando las técnicas de Vojta.

Más precisamente, consideremos los lenguajes

$$\begin{aligned}\mathcal{L}_R^z =&\{0,1,+,\cdot,z\},\\ \mathcal{L}_R^* =&\{0,1,+,\cdot,z,\mathrm{ord}\},\\ \mathcal{L}_2^z =&\{0,1,+,P_2,f_z\},\text{ and}\\ \mathcal{L}_2^* =&\{0,1,+,P_2,f_z,\mathrm{ord}\},\end{aligned}$$

donde P_2 y ord son símbolos de relaciones unarias, y f_z es un símbolo de función unaria. En anillos de funciones en la variable z, el símbolo z se interpreta como la variable, $P_2(x)$ se interpreta como "x es un cuadrado", $f_z(x)$ se interpreta como "$x \mapsto zx$", e interpretamos $\mathrm{ord}(x)$ como "$\mathrm{ord}_z(x) \geq 0$" (siempre y cuando tenga sentido en el anillo considerado).

Definimos $\mathcal{A}_p$ como el anillo de funciones analíticas p-ádicas y $\mathcal{M}_p$ como el campo de funciones meromorfas p-ádicas en la variable z. El siguiente resultado fue probado en [LP].

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

El siguiente resultado fue probado en [Vi].

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

Con el objetivo de poder obtener resultados similares en los lenguajes $\mathcal{L}_2^z$ y $\mathcal{L}_2^*$ respectivamente, se resuelven en el Capítulo 3, los análogos del Problema de Büchi en $\mathcal{A}_p$ y $\mathcal{M}_p$.

Teorema. *Sea $P \in \mathcal{A}_p[X]$ un polinomio mónico de grado 2. Si $P(a)$ es un cuadrado en $\mathcal{A}_p$ para al menos 13 valores de $a \in \mathbb{C}_p$, entonces o bien P tiene coeficientes constantes o bien P es un cuadrado en $\mathcal{A}_p[X]$*

Teorema. *Sea $P \in \mathcal{M}_p[X]$ un polinomio mónico de grado 2. Si $P(a)$ es un cuadrado en $\mathcal{M}_p$ para al menos 35 valores de $a \in \mathbb{C}_p$, entocnes o bien P tiene coeficientes constantes o bien P es un cuadrado en $\mathcal{M}_p[X]$.*

Nota que el resultado para funciones analíticas es una consecuencia (pero con otra constante) del resultado para funciones meromorfas. Este resultado para funciones analíticas era parte de mi tesis de magíster [P], pero decidí incluirlo en este trabajo por la conveniencia del lector ya que su demostración es mucho más simple que el resultado para meromorfas.

También en el Capítulo 3 se demuestran resultados análogos a lo anterior para el campo de funciones meromorfas complejas y para el campo de funciones de una curva algebraica en característica cero. Además, se exploran análogos para campos de números asumiendo una conjetura de Lang-Bombieri. Estos resultados extienden los resultados en [Vo2].

Para campos de números, los resultados que se obtienen (bajo la Conjetura de Bombieri-Lang) tienen consecuencias directas en investigaciones de autores de computación y de teoría de números (ver [Al, Bre, BB, Pi]) que buscan secuencias largas de cuadrados de enteros con segundas diferencias constantes no necesariamente 2, implicando (asumiendo que la conjetura de Bombieri-Lang es cierta para superficies) que para una constante D dada, hay un largo acotado para secuencias no triviales de cuadrados con segundas diferencias iguales a D.

Definibilidad Uniforme e Indecidibilidad en Clases de Estructuras

Otro mejoramiento posible al Décimo Problema de Hilbert en otros anillos es considerar una familia de anillos sobre un mismo lenguaje $\mathcal{L}$ y tratar de mostrar la (no) existencia de un algoritmo para decidir si una $\mathcal{L}$-fórmula se satisface para todos ellos, para alguno de ellos o para infinitos de ellos, entre otros casos. Una de las principales motivaciones desde el punto de vista lógico para considerar un problema de esta naturaleza es que en una situación así es necesario estudiar definiciones y codificaciones uniformes sobre una familia de estructuras.

Este campo de investigación parece haber sido poco explorado. Pueden ser considerados como relevantes los trabajos [Ax, AxK12, AxK3, CHr, Hr, Mac, Rum].

En el Capítulo 4 abordamos problemas de (in)decibilidad uniforme para familias de estructuras. Por ejemplo, es sabido que dado un sistema de ecuaciones diofantinas S sobre $\mathbb{Z}$, existe un algoritmo para saber si S posee o no soluciones módulo p para infinitos primos p (basta con chequear si el sistema tiene alguna solución compleja o no - ver [Nav]). Extendiendo este resultado cabe preguntarse si existe o no un algoritmo para saber si un sistema diofantino S como el anterior admite (o no) soluciones en $\mathbb{F}_p[z]$ para infinitos primos p, cuando se permiten condiciones de "no constante" sobre algunas de las incógnitas. En realidad, la condición 'para infinitos primos p' podría reemplazarse por condiciones como "para al menos un p" o "para todo primo p". En el Capítulo 4 se considerarán estos problemas y extensiones a los mismos para familias más generales de anillos de funciones.

En particular se demuestra el siguiente teorema:

Teorema *No existe algoritmo alguno que permita resolver los siguientes problemas:*

Decidir si un sistema diofantino con condiciones de 'no constante' sobre algunas de las incógnitas tiene solución en $\mathbb{F}_p[z]$ para

1. *algún primo p,*
2. *todo primo p impar,*
3. *infinitos primos p,*
4. *todos los primos p, posiblemente salvo un número finito,*

5. *todos los primos p de la forma $4k+1$.*

Ver Corolario 4.1.20 para un enunciado más general.

Para conseguir ésto, una herramienta central son las definiciones uniformes, y con particular importancia la definición uniforme positivo existencial sobre clases de anillos de funciones en característica positiva de la relación "existe un número natural s tal que $x = y^{p^s}$ o $y = x^{p^s}$" (donde p es la característica del respectivo anillo). Esto se consigue sobre una amplia clase de anillos de funciones en característica p y de manera uniforme. Así, en particular, en la fórmula que se obtiene no aparece el parámetro p. Definir esta relación ha sido desde hace tiempo un punto central para varios autores al momento de codificar los enteros en un anillo de funciones en característica positiva (ver por ejemplo, en orden cronológico, [De2], [Ph1], [Ph2], [KR], [S1], [PZ1], [S2], [Ei] y [ES]) y esta es la primera vez que se consigue hacer con fórmulas positivo existenciales que no dependen de p. Para mayores detalles, ver el Capítulo 4.

Conclusion

En resumen, los resultados que se consiguen en los capítulos 3 y 4 se relacionan principalmente con las siguientes problemáticas:

1. Resolver el análogo del Problema de Büchi para $\mathcal{M}_p$.

2. A partir de los resultados que obtenemos relativos al Problema de Büchi en $\mathcal{M}_p$, demostrar la indecidibilidad de la teoría positiva existencial de $\mathcal{M}_p$ en el lenguaje $\mathcal{L}_2^*$.

3. Asumiendo la conjetura de Lang, resolver generalizaciones del problema de Büchi sobre extensiones finitas de $\mathbb{Q}$ y, en general, estudiar la representación de cuadrados en K por polinomios mónicos de segundo grado que no son cuadrados de $K[x]$.

4. Desarrollar y estudiar un concepto adecuado de definibilidad uniforme sobre familias de estructuras.

5. Desarrollar técnicas de codificación uniforme sobre familias de estructuras, para obtener resultados fuertes de indecidibilidad sobre clases de estructuras.

6. Definición uniforme de la relación "existe un número natural s tal que $x = y^{p^s}$ o $y = x^{p^s}$" sobre clases amplias de anillos de funciones en característica positiva.

1.2 In English

Important Note: Notation in Chapters 3 and 4 are independent.

1.2.1 Description of Contents

The present work is structures in the following way:

- In Section 1.1.2 of this Chapter we give a general abstract of results obtained in the thesis. Specific introductions are given at the beginning of Chapters 3 and 4.

- In Chapter 2 we introduce some preliminary material of Mathematical Logic which will be necessary in Chapters 3 and 4 and we fix notation.

- Chapter 3 contains new results. It is written in English and has its own introduction where we detail the context of this research work and we present several known results. It also contains a section with new results. There we study the representation of squares by means of polynomials of degree two in various fields, mainly over p-adic meromorphic functions, and deduce consequences in Logic.

- Chapter 4 corresponds to a joint work with Thanases Pheidas (coadvisor of this Thesis) and Xavier Vidaux (advisor). As in Chapter 3, it is written in English and it contains its own introduction explaining the context and giving various new results. There we study uniform definability and encodability over families of structures, in order to obtain some strong undecidability results.

- Finally, Chapter 5 contains a list of open problems that naturally arise from this work. It is written in Spanish and in English.

1.2.2 Abstract

In Chapter 3 we prove a result on the representation of squares by monic second degree polynomials in the field of p-adic meromorphic functions in order to solve positively Büchi's n squares problem in this field. Using this result, we prove the non-existence of an algorithm to decide whether a system of diagonal quadratic forms over $\mathbb{Z}[z]$ represents or not in the ring of p-adic entire functions (in the variable z) a given vector of polynomials in $\mathbb{Z}[z]$, and a similar result for p-adic meromorphic functions when the systems allow vanishing conditions on the unknowns. This improves the negative answers for the analogue of Hilbert's Tenth Problem for these structures, for the cases in which such answers have been given. We also improve some results by Vojta concerning the case of complex meromorphic functions, the case of function fields and finally the case of number fields, and show an intimate relation of the latter with Bombieri's conjecture for surfaces over number fields.

In Chapter 4 we obtain several definability and uniform encodability results in various families of structures, and from those, we deduce several uniform undecidability results. For example, the relation "$x \neq y$" can be defined in a uniform way over the language of rings in the family of all fields by means of the formula

$$\exists u\, xu = 1 + yu.$$

The study of the general concept of uniformity will allow us to obtain techniques for proving results of the following type: There is no algorithm to decide whether or not a system of Diophantine equations with conditions of the type "x is non constant" over some variables x, admits a solution in $\mathbb{F}_p[z]$ for infinitely many p. This contrasts strongly with the analogous situation over $\mathbb{F}_p$, where it is known that there is an algorithm to decide whether or not a system of Diophantine equations has a solution in $\mathbb{F}_p$ for infinitely many p (actually, it is enough to verify whether or not the system has a solution in $\mathbb{C}$, which can be done effectively). Moreover, we obtain a definition of the relation "there exists a natural number s such that $x = y^{p^s}$ or $y = x^{p^s}$" over a wide class of rings of functions of positive characteristic p, such that the obtained formula is positive existential and does not use the number p (in particular, for some classes of rings of algebraic functions whose field of constants is algebraic over $\mathbb{F}_p$).

Chapter 2

Material preliminar - Preliminary Concepts

2.1 Material preliminar

Con respecto al análisis complejo p-ádico (en particular, la Teoría Nevanlinna no-Arquimediana), el material necesario será introducido en el mismo Capítulo 3. A continuación, introducimos los conceptos básicos de la Lógica Matemática que usaremos a lo largo de este trabajo. Seguimos la terminología de Cori y Lascar [CL].

Dado un lenguaje $\mathcal{L}$, una *$\mathcal{L}$-estructura* es un conjunto M junto con

- una constante por cada símbolo de constante en $\mathcal{L}$,
- una función n-aria por cada símbolo de función n-aria en $\mathcal{L}$, y
- una relación n-aria por cada símbolo de relación n-aria en $\mathcal{L}$.

Usualmente asumimos que los lenguajes tienen un símbolo "=" que se interpreta como la igualdad.

Cuando hablamos de *fórmulas sobre un lenguaje* $\mathcal{L}$ (o de *$\mathcal{L}$-fórmulas*) entenderemos siempre que se trata de fórmulas bien formadas sobre $\mathcal{L}$ (por ejemplo, la cadena de símbolos $\exists\forall x$ no es una fórmula para nosotros). Escribiremos $F(x_1, \ldots, x_n)$ (o en ocasiones $F[x_1, \ldots, x_n]$ cuando la otra notación es ambigua) para indicar que la fórmula F tiene sus variables no cuantificadas (o variables libres) entre las variables $x_1, \ldots, x_n$. Si una fórmula no tiene variables libres, decimos que es un *enunciado* o una *fórmula cerrada*.

Una fórmula es positiva existencial si sus únicos cuantificadores (de haber) son $\exists$ y sus únicos conectores son $\wedge$ y $\vee$, sin negaciones.

Si F es un $\mathcal{L}$-enunciado y $\mathfrak{M}$ es una $\mathcal{L}$-estructura, decimos que $\mathfrak{M}$ *satisface* F o que F *es cierta en* $\mathfrak{M}$ (se escribe $\mathfrak{M} \models F$) si al interpretar F en $\mathfrak{M}$ se obtiene una afirmación verdadera en $\mathfrak{M}$. Por ejemplo, con el lenguaje $\mathcal{L} = \{0, 1, +, \cdot\}$ tenemos

$$\mathbb{Z} \models \exists x \exists y \, x \cdot y = x + 1$$

(tomar $x = 1, y = 2$) y

$$\mathbb{Z} \not\models \exists x \forall y \, x + y = y + y.$$

Si $\mathfrak{M}$ es una $\mathcal{L}$-estructura con conjunto base M y si $C \subseteq M^n$ diremos que una fórmula $F(x_1, \ldots, x_n)$ define el conjunto C si para todo $(a_1, \ldots, a_n) \in M^n$ se tiene: la fórmula $F(a_1, \ldots, a_n)$ es cierta en $\mathfrak{M}$ si y sólo si $(a_1, \ldots, a_n)$ pertenece a C (donde $F(a_1, \ldots, a_n)$ es el enunciado obtenido a partir de $F(x_1, \ldots, x_n)$ al reemplazar cada x_i por a_i). Diremos que $C \subseteq M^n$ es (positiva existencialmente) definible en $\mathfrak{M}$ sobre $\mathcal{L}$ si hay una fórmula (positiva existencial) que lo define. Una función es definible si su gráfico es definible.

Por ejemplo, el teorema de Lagrange asegura que la relación $x \leq y$ es positiva existencialmente definible en $\mathbb{Z}$ sobre el lenguaje de anillos $\mathcal{L}_A = \{0, 1, +, \cdot\}$ por medio de la fórmula

$$F(x, y) \colon \exists x_1 \exists x_2 \exists x_3 \exists x_4 \, y = x + x_1^2 + x_2^2 + x_3^2 + x_4^2$$

donde cada símbolo de tipo "z^2" es solamente una notación para "$z \cdot z$".

Una *teoría* de una $\mathcal{L}$-estructura $\mathfrak{M}$ es un conjunto de enunciados de $\mathcal{L}$ que son verdaderos en $\mathfrak{M}$. En particular la teoría positiva existencial de $\mathfrak{M}$ sobre $\mathcal{L}$ es el conjunto de todos los $\mathcal{L}$-enunciados positivo existenciales que son ciertos en $\mathfrak{M}$.

Un conjunto $C \subseteq \mathbb{N}^n$ es decidible si hay un algoritmo (una máquina de Turing) que calcula su función característica. Es posible codificar de manera efectiva (computable) todos los $\mathcal{L}_A$-enunciados dentro del conjunto $\mathbb{N}$, es decir, asociar un número natural único (número de Gödel) a cada $\mathcal{L}_A$-enunciado. Sea G el conjunto de números de Gödel. La respuesta negativa del Décimo Problema de Hilbert implica que el subconjunto G^{pe} de G de números que son números de Gödel de un enunciado positivo existencial cierto en $\mathbb{N}$, es indecidible. De esta forma, no hay un algoritmo para decidir si una

fórmula positiva existencial sobre $\mathcal{L}_A$ es cierta en $\mathbb{N}$. Como el símbolo "$\geq$" es positivo existencialmente $\mathcal{L}_A$-definible sobre $\mathbb{Z}$, es posible transformar de manera efectiva una $\mathcal{L}_A$-fórmula F positiva existencial en otra F' (cambiando cada ocurrencia de tipo "$\exists x$" por "$\exists x \geq 0$") tal que $\mathbb{N} \models F$ sí y sólo si $\mathbb{Z} \models F'$. Así, se deduce que la teoría positiva existencial de $\mathbb{Z}$ es indecidible (no hay un algoritmo para decidir si una fórmula positiva existencial sobre $\mathcal{L}_A$ es cierta en $\mathbb{Z}$, pues si lo hubiera lo aplicamos a F'). Se concluye (observando como son constituidas las fórmulas positivas existenciales sobre $\mathcal{L}_A$) que no hay un algoritmo para decidir si un sistema de ecuaciones diofantinas tiene o no una solución entera. Un argumento similar (aunque generalmente mucho más complicado) de definibilidad y/o codificación nos permitirá demostrar indecidibilidad para otros problemas.

2.2 Preliminary Concepts

With respect to p-Adic Complex Analysis (and in particular, for the non-Archimedean Nevanlinna Theory), the necessary basic concepts will be introduced as they are needed in Chapter 3. In the rest of this section, we introduce the basic concepts from Mathematical Logic that we will use all along this work. We follow the terminology of Cori and Lascar [CL].

Given a language $\mathcal{L}$, an *$\mathcal{L}$-structure* is a set M together with

- an element of M for each constant symbol in $\mathcal{L}$,
- an n-ary function for each n-ary function symbol in $\mathcal{L}$, and
- an n-ary relation for each n-ary relation symbol in $\mathcal{L}$.

Usually we assume that the languages have a symbol "=" which is interpreted as equality.

By a *formula over a language $\mathcal{L}$* (or *$\mathcal{L}$-formula*), we mean a well-formed formula over $\mathcal{L}$ (for example, the string of symbols $\exists\forall x$ is not a formula for us). We will write $F(x_1, \ldots, x_n)$ (or sometimes $F[x_1, \ldots, x_n]$ when the other notation is ambiguous) to indicate that the formula F has all its non-quantified variables (or free variables) among $x_1, \ldots, x_n$. If a formula does not have free variables, we call it a *sentence* or a *closed formula*. A formula is positive existential if all its quantifiers (if any) are existential and $\wedge$ and $\vee$ are the only connectives, with no negation symbols.

If F is an $\mathcal{L}$-sentence and $\mathfrak{M}$ is an $\mathcal{L}$-structure, we say that $\mathfrak{M}$ *satisfies* F or that F *is true in* $\mathfrak{M}$ (written $\mathfrak{M} \models F$) if the interpretation of F in $\mathfrak{M}$ is true in $\mathfrak{M}$. For example, with the language $\mathcal{L} = \{0, 1, +, \cdot\}$ we have

$$\mathbb{Z} \vDash \exists x \exists y \, x \cdot y = x + 1$$

(choose $x = 1, y = 2$) and

$$\mathbb{Z} \nvDash \exists x \forall y \, x + y = y + y.$$

If $\mathfrak{M}$ is an $\mathcal{L}$-structure with base set M and if $C \subseteq M^n$, we will say that a formula $F(x_1, \ldots, x_n)$ defines the set C if for each $(a_1, \ldots, a_n) \in M^n$ we have: the formula $F(a_1, \ldots, a_n)$ is true in $\mathfrak{M}$ if and only if $(a_1, \ldots, a_n)$ belongs to C (where $F(a_1, \ldots, a_n)$ is the sentence obtained from $F(x_1, \ldots, x_n)$ after replacing each x_i by a_i). We will say that $C \subseteq M^n$ is (positive existentially) definable in $\mathfrak{M}$ over $\mathcal{L}$ if there exists a formula (positive existential) that defines it. A function is definible if its graph is definable.

For example, the theorem of the four squares of Lagrange implies that the relation $x \leq y$ is positive existentially definable in $\mathbb{Z}$ over the language of rings $\mathcal{L}_A = \{0, 1, +, \cdot\}$ by means of the formula

$$F(x, y) \colon \exists x_1 \exists x_2 \exists x_3 \exists x_4 \, y = x + x_1^2 + x_2^2 + x_3^2 + x_4^2$$

where each symbol of the type "z^2" is just a notation for "$z \cdot z$".

A *theory* of an $\mathcal{L}$-structure $\mathfrak{M}$ is a set of sentences of $\mathcal{L}$ which are true in $\mathfrak{M}$. In particular, the positive existential theory of $\mathfrak{M}$ over $\mathcal{L}$ is the set of all positive existential $\mathcal{L}$-sentences which are true in $\mathfrak{M}$.

A set $C \subseteq \mathbb{N}^n$ is decidable if there is an algorithm (a Turing machine) that computes its characteristic function. It is possible to code in an effective way all $\mathcal{L}_A$-sentences within the set $\mathbb{N}$, namely, to mechanically associate a unique natural number (*Gödel number*) to each $\mathcal{L}_A$-sentence. Let G be the set of Gödel numbers. The negative answer to Hilbert's Tenth Problem implies that the subset G^{pe} of G of numbers which are Gödel numbers of positive existential sentences true in $\mathbb{N}$, is undecidable. Therefore, there is no algorithm to decide whether or not a positive existential formula over $\mathcal{L}_A$ is true in $\mathbb{N}$. Since the symbol "$\geq$" is positive existentially $\mathcal{L}_A$-definable over $\mathbb{Z}$, it is possible to transform in an effective (mechanical) way a positive existential $\mathcal{L}_A$-formula F into another such formula F' (by replacing each occurrence of "$\exists x$" by "$\exists x \geq 0$"), such that $\mathbb{N} \models F$ if and only if $\mathbb{Z} \models F'$. Hence, we

deduce that the positive existential theory of $\mathbb{Z}$ is undecidable (there is no algorithm to decide whether or not a positive existential formula over $\mathcal{L}_A$ is true in $\mathbb{Z}$, as otherwise we would apply it to F'). We conclude (observing how are made up positive existential formulas over $\mathcal{L}_A$) that there is no algorithm to decide whether or not a system of Diophantine equations has an integral solution. A similar argument (though usually much more complicated) of definability and/or codification will allow us to prove undecidability results for a variety of other problems.

Chapter 3

Representation of squares by monic second degree polynomials in the field of p-adic meromorphic functions

3.1 Introduction

In 1970, after the work developed by M. Davis, H. Putnam and J. Robinson, Hilbert's Tenth Problem was answered negatively by Y. Matiyasevic (see [Mat] or [Da]). In logical terms, it was shown that the positive existential theory of $\mathbb{Z}$ in the language of rings $\mathcal{L}_R = \{0, 1, +, \cdot\}$ is undecidable, which means that there exists no algorithm to decide whether a system of diophantine equations (or equivalently, a single diophantine equation) has integer solutions or not. For a general survey on Hilbert's Tenth Problem and extensions of it, see for example [PZ2] or [Po] (see [S3] for results about number fields and function fields).

Soon after the problem was solved, J. R. Büchi proved in an unpublished work (see [L] or [Maz]) that a positive answer to a certain problem in Number Theory (which we write here $\mathbf{BP}(\mathbb{Z})$) would allow to show that there exists no algorithm to decide whether a system of diagonal quadratic forms over $\mathbb{Z}$ represents or not a given vector of integers.

The number-theoretical problem $\mathbf{BP}(\mathbb{Z})$ is based on the following observation. If we consider the first difference of a sequence of consecutive integer

squares (for example $1, 4, 9, 16$), we obtain a sequence of consecutive odd integers (in our example $3, 5, 7$). Hence, the second difference is the constant sequence (2). One may ask whether a sequence of squares having second difference equal to the constant sequence (2) must be a sequence of consecutive squares. The sequence $6^2, 23^2, 32^2, 39^2$ shows that it is not true in general.

Problem 3.1.1 (**BP**($\mathbb{Z}$))**.** *Does there exist an integer M such that the following happens:*
If the second difference of a sequence $(x_i^2)_{i=1}^M$ of integer squares is constant and equal to 2, then there exists an integer ν such that $x_i^2 = (\nu + i)^2$ for $i = 1, \ldots, M$ (that is, the squares must be consecutive).

This problem became known as the *n Squares Problem* or *Büchi's Problem*. Numerical evidence suggests that $M = 5$ should work (see for example [Pi]), but **BP**($\mathbb{Z}$) still is an open problem.

Assuming a positive answer to **BP**($\mathbb{Z}$), Büchi was able to prove, using the negative answer given to Hilbert's tenth problem and assuming a positive answer to **BP**($\mathbb{Z}$), the non-existence of an algorithm for the problem of representation of a vector of integers by diagonal quadratic forms. The problem of the existence of such an algorithm can be shown to be equivalent to the problem of decidability of the positive existential theory of $\mathbb{Z}$ over the language $\mathcal{L}_2 = \{0, 1, +, P_2\}$, where $P_2(x)$ is interpreted as "x is a square".

In order to get similar consequences in Logic for other rings of interest, and motivated by the arithmetical interest of the problem, several authors have studied variants of **BP**($\mathbb{Z}$). A natural thing to do is to replace the ring $\mathbb{Z}$ by another commutative ring A with unit. Depending on the ring, we sometimes need to make additional hypothesis in the statement of **BP**(A):

- If A is a ring of functions of characteristic zero in the variable z, then we ask for at least one x_i to be non-constant.
- If A is a ring of positive characteristic, then we ask M to be at most the characteristic of A.

For variants on Büchi's problem (for example, considering sequences whose second difference is a constant sequence (m) for some m not necessarily $= 2$), see [Al] and [BB]. For the problem **BP**(A) with A a ring, we know that the following cases (among various others) have a positive answer: **BP**$^2(\mathbb{F}_p)$ with $p > 2$ (see [He]), **BP**$^2(\mathcal{M})$ where $\mathcal{M}$ is the field of complex meromorphic functions (see [Vo2]), **BP**$^2(F(z))$ where $F(z)$ is the field of rational functions

over a field of characteristic 0 or $p \geq 19$ (see [PV1, PV2]). Moreover, Büchi's problem has a positive answer even in the case of function fields of curves (see [Vo2] for the characteristic zero case and see [SV] for 'large enough' positive characteristic). Under a conjecture in Diophantine Geometry, Vojta showed in [Vo2] that $\mathbf{BP}^2(\mathbb{Q})$ would have a positive answer (hence $\mathbf{BP}^2(\mathbb{Z})$ would have a positive answer). See [PPV] for a survey on Büchi's problem and its variants.

The positive existential $\mathcal{L}_2$-theory of a ring is usually much weaker than its positive existential $\mathcal{L}_R$-theory. But when Büchi's problem has a positive answer for a ring A then those theories for A are (in general) equivalent. This is what happens for example for p-adic analytic functions and for p-adic meromorphic functions (see Section 3.2.2).

We will solve $\mathbf{BP}(A)$ for some rings of functions, namely, the field of p-adic meromorphic functions, the field of complex meromorphic functions and function fields of curves in characteristic zero by showing in each case a somewhat stronger result on representation of squares by polynomials, in the spirit of the following:

Given a ring B and a subset A of B, there exists a constant M satisfying the following condition:
For any set $\{a_1, \ldots, a_M\}$ of M elements in A, there exists a 'small' set $E \subseteq B[X]$ such that, if a monic polynomial of degree two $P \in B[X]$ has the property that each $P(a_i)$ is a square in B, then $P \in E$ or P is a square in $B[X]$.

We will prove such a result for number fields, but assuming that the following conjecture by Bombieri holds for surfaces.

Conjecture 3.1.2 (Bombieri)**.** *If X is a smooth projective variety of general type defined over a number field $K/\mathbb{Q}$, then $X(K)$ is contained in a proper Zariski closed set of X.*

The results for function fields, complex meromorphic functions and number fields are based on Vojta's work on Büchi's problem (see [Vo2]), where he solved Büchi's problem for complex meromorphic functions, function fields and (assuming the above conjecture) for number fields. The results related to the p-adic setting are proved in a completely different way from Vojta's proof for the complex meromorphic case, and indeed, our proof is closer to the ideas in [PV1, PV2].

On the one hand, from an arithmetic point of view, our interest is not only in solving Büchi's problem in some structures, but also understand *how*

many times a second degree polynomial which is not a square, can represent a square.

On the other hand, from the point of view of Logic, our main interest in solving Büchi's problem for p-adic meromorphic functions is that some analogues of Hilbert's Tenth Problem for the ring of p-adic analytic functions (see [LP]) and the field of p-adic meromorphic functions (see [Vi]) have been proved to be undecidable (those problems are open in the complex case). Those results allow us, in the p-adic case, to derive consequences in Logic from Büchi's problem. This will be explained below in Section 3.2.2.

We also refer the reader to [De1] where is developed a general method used to solve negatively analogues of Hilbert's Tenth Problem for rings of functions.

3.2 Main results

In this section, we present the statements of the results proven in this work.

3.2.1 Representation of squares in the field of p-adic meromorphic functions

Let p be a prime number and let $\mathbb{C}_p$ be the field of p-adic complex numbers (the completion of the algebraic closure of the field $\mathbb{Q}_p$ of p-adic numbers). Throughout the paper, one can replace $\mathbb{C}_p$ by any algebraically closed field of characteristic zero, complete with respect to a non-trivial non-Archimedean valuation.

Let $\mathcal{A}_p$ be the ring of entire functions over $\mathbb{C}_p$ and let $\mathcal{M}_p$ be the field of meromorphic functions over $\mathbb{C}_p$. We prove the following theorem on representation of squares by polynomials.

Theorem 3.2.1. *Let $P \in \mathcal{M}_p[X]$ be a monic polynomial of degree two. If $P(a)$ is a square in $\mathcal{M}_p$ for at least 35 values of $a \in \mathbb{C}_p$, then either P has constant coefficients or P is a square in $\mathcal{M}_p[X]$.*

By solving the second order recurrence implied in the statement of Büchi's problem, we can use the above theorem to show the following.

Corollary 3.2.2. *The problems $\mathbf{BP}(\mathcal{A}_p)$ and $\mathbf{BP}(\mathcal{M}_p)$ have a positive answer.*

Theorem 3.2.1 can be improved for the ring $\mathcal{A}_p$ of p-adic entire functions in the following way.

Theorem 3.2.3. *Let $P \in \mathcal{A}_p[X]$ be a monic polynomial of degree two. If $P(a)$ is a square in $\mathcal{A}_p$ for at least 13 values of $a \in \mathbb{C}_p$, then either P has constant coefficients or P is a square in $\mathcal{A}_p[X]$.*

The proof of Theorem 3.2.3 is shorter and simpler than the proof of Theorem 3.2.1. Indeed, the method used in the proof of Theorem 3.2.3 essentially is a p-adic simplified version of the method in [PV1, PV2]. Unfortunately, several technical difficulties arise when we consider the problem for $\mathcal{M}_p$, and this requires the use of Nevanlinna theory and some combinatoric arguments.

We will prove these results in Section 3.4 and Section 3.5. In Section 3.3, the reader will find some general results from p-adic Complex Analysis that we will need later in the proofs.

3.2.2 Undecidability for p-adic entire and meromorphic functions in Büchi's language

Corollary 3.2.2 allows us to obtain very strong undecidability results for p-adic analytic and meromorphic functions, improving results by Lipshitz and Pheidas, and by Vidaux. In order to state the theorems, we need to introduce some notation.

Recall that $\mathcal{A}_p$ stands for the ring of entire functions over $\mathbb{C}_p$, and $\mathcal{M}_p$ stands for the field of meromorphic functions over $\mathbb{C}_p$, with variable z.

By a *diagonal quadratic equation over a ring A* we will mean an equation of the form

$$a_1x_1^2 + \cdots + a_nx_n^2 = b$$

where the a_i and b are elements of A and the x_i are the unkowns.

Define the following languages:

$$\begin{aligned}
\mathcal{L}_R^z &= \{0, 1, +, \cdot, z\},\\
\mathcal{L}_R^* &= \{0, 1, +, \cdot, z, \mathrm{ord}\},\\
\mathcal{L}_2^z &= \{0, 1, +, P_2, f_z\}, \text{ and}\\
\mathcal{L}_2^* &= \{0, 1, +, P_2, f_z, \mathrm{ord}\},
\end{aligned}$$

where P_2 and ord are unary predicate symbols, and f_z is a unary function symbol. In $\mathcal{A}_p$ and $\mathcal{M}_p$, $P_2(x)$ is interpreted as "x is a square", $f_z(x)$ is

interpreted as "$x \mapsto zx$", and we interpret $\mathrm{ord}(x)$ as "$x(0) = 0$" (all other symbols are interpreted in the obvious way).

Theorem 3.2.4. *Multiplication is positive existentially definable in $\mathcal{M}_p$ and in $\mathcal{A}_p$ over the language $\mathcal{L}_2^z$.*

See Section 3.6 for a proof.

We recall that the following two theories are undecidable: the positive existential theory of $\mathcal{A}_p$ in the language $\mathcal{L}_R^z$ (see [LP]) and the positive existential theory of $\mathcal{M}_p$ in the language $\mathcal{L}_R^*$ (see [Vi]). From this and Theorem 3.2.4 we deduce:

Theorem 3.2.5. *The positive existential theory of $\mathcal{A}_p$ in the language $\mathcal{L}_2^z$ and the positive existential theory of $\mathcal{M}_p$ in the language $\mathcal{L}_2^*$ are undecidable.*

This result allows us to prove the following (see Section 3.6).

Theorem 3.2.6. *There is no algorithm to solve any of the following problems:*

1. *Given a system of diagonal quadratic equations*

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

with all the a_{ij} and b_j in $\mathbb{Z}[z]$, to decide whether or not the system has a solution in $\mathcal{A}_p$.

2. *Given a system of diagonal quadratic equations*

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

with all the a_{ij} and b_j in $\mathbb{Z}[z]$, and given a set $I \subseteq \{1, \ldots, r\}$, to decide whether or not the system has a solution in $\mathcal{M}_p$ satisfying $x_i(0) = 0$ for each $i \in I$.

3.2.3 Representation of squares in number fields

The statements given below will be proved in Section 3.9.

Theorem 3.2.7. *Assume Bombieri's Conjecture 3.1.2 holds for surfaces. Let K be a number field and $\{a_1, \dots, a_8\}$ a set of eight elements in K. There exists a finite (possibly empty) set $E = E(K, (a_i)_i)$ of polynomials in $K[x]$ such that the following holds: for each polynomial f of the form*

$$x^2 + ax + b \in K[x],$$

if $f(a_i)$ are squares in K for each i then either $f \in E$, or $f = (x + c)^2$ for some $c \in K$.

This theorem is an extension of Theorem 0.5 in [Vo2]. The method used to obtain this result is essentially an adaptation of the method by Vojta in [Vo2].

It is an obvious but remarkable fact that, if one could find a number field K and a sequence $a = (a_1, \dots, a_8)$ of distinct elements of K such that the set $E(K, (a_i))$ is infinite, then one would automatically obtain a counterexample to Bombieri's Conjecture. On the other hand, showing finiteness for $E(K, (a_i))$ for some K and some sequence (a_i) would give a new example of a surface (over K) where Bombieri's question has a positive answer. We are not able to prove nor disprove the finiteness of the set $E(K, (a_i))$ in any case.

From the finiteness of the sets $E(K, (a_i))$ one can easily derive the following (see Section 3.9).

Corollary 3.2.8. *Assume that Bombieri's conjecture holds for surfaces defined over $\mathbb{Q}$. Let $a_1, a_2, \dots$ be a sequence of integers without repeated terms. There exists a constant M (depending on the sequence $(a_i)_i$) such that: if a polynomial $f = x^2 + ax + b \in \mathbb{Q}[x]$ satisfies the property "$f(a_i)$ is a square in $\mathbb{Z}$ for $i = 1, \dots, M$", then f is of the form $f = (x + c)^2$, for some $c \in \mathbb{Z}$.*

Observe that the dependence of M on the sequence cannot be dropped. Consider for example the polynomial $f_N = x^2 - 4(2N)!$, where N is a positive integer, and define

$$a_i = i! + \frac{(2N)!}{i!}.$$

Then it is obvious that $(a_i)_{i=1}^N$ is a strictly decreasing sequence in $\mathbb{Z}$ and each $f_N(a_i)$ is a square in $\mathbb{Z}$.

Note that, if in Corollary 3.2.8 we set $a_n = n$ for each n, then we obtain a positive answer to Büchi's Problem for $\mathbb{Z}$ (under Bombieri's Conjecture).

3.2.4 Representation of squares for function fields and for complex meromorphic functions

The geometric results in Section 3.7 will be used in Section 3.9 to prove the following theorems, analogues to Theorem 3.2.1.

Theorem 3.2.9. *Let F be a field of characteristic zero and C a non-singular projective curve defined over F. Define the integer $M = \max\{8, 4(g+1)\}$ where g is the genus of C. Write $K(C)$ for the function field of C and let X be transcendental over $K(C)$. Let $P \in K(C)[X]$ be a monic polynomial of degree two. If $P(a)$ is a square in $K(C)$ for at least M values of $a \in F$, then either P has constant coefficients or P is a square in $K(C)[X]$.*

Theorem 3.2.10. *Write $\mathcal{M}$ for the field of meromorphic functions on $\mathbb{C}$. Let $P \in \mathcal{M}[X]$ be a monic polynomial of degree two. If $P(a)$ is a square in $\mathcal{M}$ for at least 8 values of $a \in \mathbb{C}$, then either P has constant coefficients or P is a square in $\mathcal{M}[X]$.*

These theorems give as a direct consequence a positive answer to Büchi's problem in the respective cases, but such a positive answer is not new since it was proved in [Vo2] for both cases. Moreover, Büchi's problem for this kind of rings was solved recently by a new method in characteristic zero and (large enough) positive characteristic in [SV].

3.3 Some results in p-adic Nevanlinna Theory

First we present the notation we use for the usual functions in p-adic Nevanlinna Theory.

We will work over the field $\mathbb{C}_p$ with absolute value $|\cdot|_p$. Write $\mathcal{A}_p$ for the ring of entire functions over $\mathbb{C}_p$ and $\mathcal{M}_p$ for the field of meromorphic functions over $\mathbb{C}_p$. We denote by F^+ the positive part of a function F whose image is included in $\mathbb{R}$, that is $F^+ = \max\{F, 0\}$. We adopt the following notation for the standard functions in p-adic Nevanlinna theory, where $f = \frac{h}{g} \in \mathcal{M}_p$ is

non-zero, and where $g, h \in \mathcal{A}_p$ are coprime:

$$\begin{aligned}
B[r] &= \{z \in \mathbb{C}_p \colon |z|_p \leq r\} \\
n(r,h,0) &= \text{number of zeros of } h \text{ in } B[r] \text{ counting multiplicity} \\
n(r,f,0) &= n(r,h,0) \\
n(r,f,\infty) &= n(r,g,0) \\
N(r,h,0) &= \int_0^r \frac{n(t,h,0) - n(0,h,0)}{t} dt + n(0,h,0)\log r \\
N(r,f,0) &= N(r,h,0) \\
N(r,f,a) &= N(r,f-a,0) \\
N(r,f,\infty) &= N(r,g,0) \\
|h|_r &= \max_{n\geq 0} |a_n|_p r^n, \text{ where } h(z) = a_0 + \sum_{n\geq 1} a_n z^n \\
|f|_r &= \frac{|h|_r}{|g|_r} \\
m(r,f,a) &= \log^+ \frac{1}{|f-a|_r} \\
m(r,f) = m(r,f,\infty) &= \log^+ |f|_r
\end{aligned}$$

We recall to the reader that for each $r > 0$, the function $|\cdot|_r : \mathcal{M} \to \mathbb{R}$ is a non-archimedean absolute value satisfying $|a|_r = |a|_p$ when a is constant.

We will need the following standard results from p-adic Nevanlinna Theory. For a general presentation of p-adic complex analysis, see for example [Ro, Es]. For references on p-adic Nevanlinna Theory (in particular, for a proof of the following results) see for example [ChY], [Ru] or the Chapter II of [HY].

First we have the *Logarithmic Derivative Lemma*:

Lemma 3.3.1. *If n is a positive integer and $f \in \mathcal{M}_p$ then*

$$\left|\frac{f^{(n)}}{f}\right|_r \leq \frac{1}{r^n}$$

where $f^{(n)}$ stands for the n-th derivative.

We will also need the *Poisson-Jensen Formula*:

Theorem 3.3.2. *Given $f \in \mathcal{M}_p$, there exists a constant C depending only on f such that*

$$\log |f|_r = N(r, f, 0) - N(r, f, \infty) + C.$$

As a consequence of the Poisson-Jensen Formula, we get the *First Main Theorem*:

Theorem 3.3.3. *Let $f \in \mathcal{M}_p$ be a non-constant meromorphic function and $a \in \mathbb{C}_p$. As $r \to \infty$ we have*

$$m(r, f, a) + N(r, f, a) = m(r, f, \infty) + N(r, f, \infty) + O(1).$$

Finally, we state the *Second Main Theorem*:

Theorem 3.3.4. *Let $f \in \mathcal{M}_p$ be a non-constant meromorphic function and let $a_1, \ldots, a_q \in \mathbb{C}_p$ be distinct. Then, as $r \to \infty$ we have*

$$\sum_{i=1}^{q} m(r, f, a_i) \leq N(r, f, \infty) + O(1).$$

3.4 p-adic Meromorphic Functions

In this section we prove Theorem 3.2.1.

The following equality will be used many times without mention within this section:

$$N(r, f, x) = K + \int_1^r \frac{n(t, f, x)}{t} dt, \quad \text{for large } r. \tag{3.1}$$

It will be used systematically in order to deduce inequalities (for large r) about N when we know inequalities about n (the point is that the integral is a linear and monotone operator).

In order to simplify the proof of Theorem 3.2.1, we actually will prove the following equivalent result.

Theorem 3.4.1. *Let $h_1, \ldots, h_M$ be elements of $\mathcal{M}_p$ such that at least one h_i is non-constant. Let $a_1, \ldots, a_M$ be M distinct elements of $\mathbb{C}_p$. If there exist $f, g \in \mathcal{M}_p$, with g non-zero, such that*

$$h_j^2 = (a_j + f)^2 - g \qquad j = 1, \ldots, M \tag{3.2}$$

then $M \leq 34$.

For the rest of this section, we will assume that we are under the hypothesis of Theorem 3.4.1. Assuming $M \geq 35$ we will obtain a contradiction.

First, we observe that

$$h_i^2 - h_j^2 = (a_i - a_j)(2f + a_i + a_j). \tag{3.3}$$

Lemma 3.4.2. *The function f is not constant.*

Proof. If f is constant then so is $c_i = (a_i + f)^2$. Note that since some h_i is non-constant, g is non-constant. Taking i, j and k such that c_i, c_j, and c_k are pairwise distinct constants, the following equality

$$(h_i h_j h_k)^2 = (c_i - g)(c_j - g)(c_k - g)$$

gives a non-constant meromorphic parametrization of an elliptic curve over $\mathbb{C}_p$, which is impossible by a theorem of Berkovich (see [Ber]). □

Lemma 3.4.3. *Let $x \in \mathbb{C}_p$ be a pole of some h_i. There exists an index k depending on x such that for each $i \neq k$ we have (simultaneously)*

1. $\mathrm{ord}_x h_k \geq \mathrm{ord}_x h_i$;
2. $\mathrm{ord}_x f \geq 2\mathrm{ord}_x h_i$;
3. $\mathrm{ord}_x g \geq 4\mathrm{ord}_x h_i$;
4. $\mathrm{ord}_x h_i = \mathrm{ord}_x h_j$ *for all* $j \neq k$; *and*
5. $\mathrm{ord}_x h_i \leq -1$.

Moreover, for each i we have

$$\min\{\mathrm{ord}_x h_i, 0\} \geq \frac{1}{M-1} \sum_l \min\{\mathrm{ord}_x h_l, 0\} \tag{3.4}$$

and, there exists a positive constant K such that for large enough r and for each i we have

$$N(r, h_i, \infty) \leq \frac{1}{M-1} \sum_l N(r, h_l, \infty) + K. \tag{3.5}$$

Proof. Let i_0 be an index such that h_{i_0} has a pole at x.

First suppose that *all* h_i have the same order at x (hence negative). In this case, Items (1), (4) and (5) hold trivially, Item (2) comes from Equation (3.3), and Item (3) comes from Equation (3.2). Indeed for Item (3) we have

$$\begin{aligned}\mathrm{ord}_x(g) &\geq 2\min\{\mathrm{ord}_x(h_i), \mathrm{ord}_x(f+a_i)\}\\ &= 2\min\{\mathrm{ord}_x(h_i), \mathrm{ord}_x(f)\}\\ &= 2\min\{\mathrm{ord}_x(h_i), 2\mathrm{ord}_x(h_i)\}\\ &\geq 4\mathrm{ord}_x h_i,\end{aligned}$$

where the last inequality comes from Item (2).

The other case is when not all h_i have the same order at x. Choose k such that item (1) holds true. By Equation (3.3) for indices k and any $i \neq k$, Item (4) holds true. If $i_0 = k$ then all h_i have a pole at x (by maximality of k), and if $i_0 \neq k$ then by Item (4), for all $i \neq k$, h_i has a pole at x. Hence Item (5) holds true. Items (2) and (3) for $i \neq k$ follow as in the previous case.

Finally, by Items (1), (4) and (5), and observing that $\mathrm{ord}_x h_k$ could be positive, we have for each i

$$(M-1)\min\{\mathrm{ord}_x h_i, 0\} = \sum_{l\neq k} \min\{\mathrm{ord}_x h_l, 0\} \geq \sum_l \min\{\mathrm{ord}_x h_l, 0\}.$$

Summing for $x \in B[r]$ we obtain

$$(M-1)n(r, h_i, \infty) \leq \sum_l n(r, h_l, \infty).$$

which gives the inequality (3.5), using Equation (3.1). □

Lemma 3.4.4. *The following inequality holds*

$$\sum_{n=1}^{M} \log|h_n|_r + \frac{1}{M-1}\sum_{n=1}^{M} N(r, h_n, \infty) + \frac{1}{2}N(r, f, \infty) + \mathcal{O}(1) \geq 0.$$

Proof. By the Second Main Theorem 3.3.4, we have for each $i = 1, \ldots, M$

$$-N(r, f, \infty) + \mathcal{O}(1) \leq -\sum_{j\neq i} \log^+ \left|\frac{1}{f + \frac{a_i+a_j}{2}}\right|_r \leq \sum_{j\neq i} \log\left|f + \frac{a_i+a_j}{2}\right|_r.$$

Since by Equation (3.3) we have

$$h_i^2 - h_j^2 = 2(a_i - a_j)\left(f + \frac{a_i + a_j}{2}\right),$$

we deduce

$$-N(r, f, \infty) + \mathcal{O}(1) \leq \sum_{j \neq i} \log \left|h_i^2 - h_j^2\right|_r .$$

If for a given r, i_r is an index such that $|h_i|_r$ is minimal, then

$$\begin{aligned}
\frac{1}{2}\sum_{j \neq i_r} \log \left|h_{i_r}^2 - h_j^2\right|_r &\leq \sum_{j \neq i_r} \log |h_j|_r \\
&= C + \sum_{j \neq i_r} \left(N(r, h_j, 0) - N(r, h_j, \infty)\right) \\
&\leq C + N(r, h_{i_r}, \infty) + \sum_n \left(N(r, h_n, 0) - N(r, h_n, \infty)\right) \\
&= C' + N(r, h_{i_r}, \infty) + \sum_n \log |h_n|_r \\
&\leq C'' + \frac{1}{M-1}\sum_n N(r, h_n, \infty) + \sum_n \log |h_n|_r
\end{aligned}$$

where the first and second equalities are given by the Poisson-Jensen Formula 3.3.2, the third inequality is given by Lemma 3.4.3 (see Equation (3.5)), and C, C', C'' are fixed constants (not depending on r nor on i_r).

Finally we have

$$\begin{aligned}
-\frac{1}{2}N(r, f, \infty) + \mathcal{O}(1) &\leq \frac{1}{2}\sum_{j \neq i_r} \log \left|h_{i_r}^2 - h_j^2\right|_r \\
&\leq \sum \log |h_n|_r + \frac{1}{M-1}\sum N(r, h_n, \infty) + C''
\end{aligned}$$

for each r large enough, and the lemma is proven. □

Lemma 3.4.5. *The following inequalities hold:*

$$n(r, f, \infty) \leq \frac{2}{M-1}\sum_n n(r, h_n, \infty) \tag{3.6}$$

and

$$\sum_n N(r, h_n, 0) \geq \frac{M-3}{M-1}\sum_n N(r, h_n, \infty) + \mathcal{O}(1).$$

Proof. Observe that by Lemma 3.4.3 (Item (2) and Equation (3.4)) we have

$$(M-1)n(r,f,\infty) \leq 2\sum n(r,h_j,\infty),$$

hence

$$(M-1)N(r,f,\infty) \leq 2\sum N(r,h_n,\infty) + \mathcal{O}(1).$$

The second formula comes immediately by Lemma 3.4.4 and the Poisson-Jensen Formula 3.3.2. □

The equations

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

are directly deduced by reordering and differentiating the one given in the hypothesis. From this we deduce

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

hence

$$g'^2 - 4f'^2 g = 4h_n(h_n f'^2 - h_n'^2 h_n - h_n' g').$$

Writing

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

we have

$$\Delta = 4h_n\Delta_n. \tag{3.7}$$

Lemma 3.4.6. *If Δ is not identically zero, then*

$$N(r,\Delta,0) \geq \frac{1}{2}\sum N(r,h_n,0) - \frac{8}{M-1}\sum N(r,h_n,\infty) + \mathcal{O}(1).$$

Proof. On the one hand, for a given $x \in \mathbb{C}_p$ suppose f has a pole at x and $h_j(x) = 0$ for some index j. Set $l = \mathrm{ord}_x(h_j)$ and $m = \mathrm{ord}_x(f)$. Note that $\mathrm{ord}_x(g) = 2m$ because $h_j(x) = 0$ (see Equation (3.2)). Write

$$h_j = u_l(z-x)^l + u_{l+1}(z-x)^{l+1} + \cdots,$$

$$f = v_m(z-x)^m + v_{m+1}(z-x)^{m+1} + \cdots$$

and

$$g = w_{2m}(z-x)^{2m} + w_{2m+1}(z-x)^{2m+1} + \cdots$$

for the Laurent series of h_j, f and g at x. Observe that

$$w_{2m} = v_m^2.$$

The first term of the Laurent series at x for respectively $h_j f'^2$, $h_j'^2 h_j$ and $h_j' g'$ is, respectively,

$$m^2 u_l v_m^2 (z-x)^{l+2m-2}$$

$$l^2 u_l^3 (z-x)^{3l-2}$$

and

$$2lmu_l v_m^2 (z-x)^{l+2m-2}$$

hence

$$\mathrm{ord}_x \Delta_j = l + 2m - 2$$

since $2l \neq m$. Therefore, we have

$$\mathrm{ord}_x \Delta = 2(l+m-1).$$

On the other hand, if $x \in \mathbb{C}_p$ is not a pole of f and is a zero of some h_j, then we have

$$\mathrm{ord}_x \Delta \geq \mathrm{ord}_x(h_j)$$

because by Equation (3.2), g does not have a pole, hence Δ_j does not have a pole and we conclude by Equation (3.7).

Let A_r be the set of $x \in B[r]$ such that f has not a pole at x and $h_j(x) = 0$ for some index j, and let B_r be the set of $x \in B[r]$ such that f has a pole at x and $h_j(x) = 0$ for some index j. Observe that, by Equation (3.3), no three of the h_n can share a zero (we use it for the fifth inequality below). We have

then

$$\begin{aligned}
n(r,\Delta,0) &\geq \sum_{x\in A_r} \operatorname{ord}_x\Delta + \sum_{x\in B_r} \operatorname{ord}_x\Delta \\
&\geq \sum_{x\in A_r} \max_{h_i(x)=0} \operatorname{ord}_x(h_i) + \sum_{x\in B_r} \max_{h_i(x)=0} 2(\operatorname{ord}_x(h_i)+\operatorname{ord}_x(f)-1) \\
&\geq \sum_{x\in A_r\cup B_r} \max_{h_i(x)=0} \operatorname{ord}_x(h_i) + 2\sum_{x\in B_r} \max_{h_i(x)=0} (\operatorname{ord}_x(f)-1) \\
&= \sum_{x\in A_r\cup B_r} \max_{h_i(x)=0} \operatorname{ord}_x(h_i) + 2\sum_{x\in B_r} (\operatorname{ord}_x(f)-1) \\
&\geq \sum_{x\in A_r\cup B_r} \max_{h_i(x)=0} \operatorname{ord}_x(h_i) + 4\sum_{x\in B_r} \operatorname{ord}_x(f) \\
&\geq \frac{1}{2}\sum_i n(r,h_i,0) - 4n(r,f,\infty) \\
&\geq \frac{1}{2}\sum_i n(r,h_i,0) - \frac{8}{M-1}\sum n(r,h_i,\infty)
\end{aligned}$$

where the last inequality comes from Lemma 3.4.5. The result follows. □

Lemma 3.4.7. *If Δ is not identically zero, then*

$$N(r,\Delta,\infty) \leq \frac{8}{M-1}\sum N(r,h_n,\infty) + \mathcal{O}(1).$$

Proof. Suppose that some $x \in \mathbb{C}_p$ is a pole of Δ. Then, by definition of Δ, it is a pole of f or of g. If none of the h_i has a pole at x then by Equation (3.3) f does not have a pole, and by Equation (3.2), g does not have a pole, which contradicts our hypothesis. Therefore, some h_i has a pole at x. Take k as in Lemma 3.4.3. For each index $i \neq k$ we have (observing that $\operatorname{ord}_x(h_i) \leq -1$ and that if $g' = 0$ then $\operatorname{ord}_x h_i' g'$ is infinite)

$$\begin{aligned}
\operatorname{ord}_x\Delta &\geq \operatorname{ord}_x h_i + \min\{\operatorname{ord}_x h_i f'^2, \operatorname{ord}_x h_i'^2 h_i, \operatorname{ord}_x h_i' g'\} \\
&\geq \operatorname{ord}_x h_i + \min\{7\operatorname{ord}_x h_i, 5\operatorname{ord}_x h_i, 7\operatorname{ord}_x h_i\} \\
&= 8\operatorname{ord}_x h_i.
\end{aligned}$$

Hence, using the Lemma 3.4.3 (Equation (3.4)) we have

$$\operatorname{ord}_x\Delta \geq \frac{8}{M-1}\sum_l \min\{\operatorname{ord}_x h_l, 0\}.$$

Write D_r for the set of poles of Δ in $B[r]$. We have

$$\begin{aligned} n(r,\Delta,\infty) &= \sum_{x\in D_r} -\mathrm{ord}_x\Delta \\ &\leq \frac{8}{M-1}\sum_{x\in D_r}\sum_{l}\max\{-\mathrm{ord}_x h_l, 0\} \\ &\leq \frac{8}{M-1}\sum_{l}\sum_{x\in B[r]}\max\{-\mathrm{ord}_x h_l, 0\} \\ &= \frac{8}{M-1}\sum_{l} n(r,h_l,\infty). \end{aligned}$$

and the result follows. □

Lemma 3.4.8. *For each $r>0$ and each i we have*

1. $\log|g|_r \leq \max\{2\log|h_i|_r, 0, 2\log|f|_r\} + \log\max\{|a_i^2|_r\}$; *and*
2. $2\log|h_i|_r \leq \max\{2\log|f|_r, 0, \log|g|_r\} + \log\max\{|a_i^2|_r\}$.

Proof. Since

$$|2a_i f|_r \leq |a_i|_r|f|_r \leq \frac{|a_i^2|_r + |f^2|_r}{2} \leq \max\{|a_i^2|_r, |f^2|_r\}$$

we have

$$\begin{aligned} \log|g|_r &= \log|(f+a_i)^2 - h_i^2|_r \\ &\leq \log\left(\max\{|h_i^2|_r, |f^2|_r, |2a_i f|_r, |a_i^2|_r\}\right) \\ &\leq \log\left(\max\{|h_i^2|_r, |f^2|_r, |a_i^2|_r\}\right) \\ &\leq \max\{2\log|h_i|_r, 0, 2\log|f|_r\} + \log\max\{|a_i^2|_r\}. \end{aligned}$$

The other inequality is proved in a similar way.

□

Lemma 3.4.9. 1. *For each $r>0$, there exists an index k_r such that $|h_{k_r}|_r$ is minimal.*

2. *There exists a positive constant K_f such that, for any $r>0$ and for all $i \neq k_r$, we have*

$$\log|f|_r \leq \max\{0, 2\log|h_i|_r\} + K_f.$$

3. *There exists a positive constant K_g such that, for any $r > 0$ and for all $i \neq k_r$, we have*

$$\log |g|_r \leq \max\{0, 4 \log |h_i|_r\} + K_g.$$

Proof. Item (1) is immediate since for each r, the set $\{|h_i|_r \colon i = 1, \ldots, M\}$ is finite. Let us prove Item (2). There exists a positive constant $K' > 1$ such that for each $r > 0$, i and j, we have

$$|2f|_r \leq |2f + a_i + a_j|_r + |a_i + a_j|_r \leq K' + |2f + a_i + a_j|_r. \tag{3.8}$$

On the other hand, by Equation (3.3) there exists a constant $K'' > 1$ such that, for any $r > 0$, $i \neq k_r$ and j, we have

$$\begin{aligned} |2f + a_i + a_j|_r &= \left| \frac{h_i^2 - h_{k_r}^2}{a_i - a_{k_r}} \right|_r \\ &\leq \left| \frac{h_i^2}{a_i - a_{k_r}} \right|_r \qquad \text{(by Item (1))} \\ &\leq K'' |h_i^2|_r \end{aligned}$$

hence by Equation (3.8)

$$|2f|_r \leq K'' |h_i^2|_r + K' \leq K'' \max\{|h_i^2|_r, 1\} + K'.$$

Therefore, we have

$$\begin{aligned} \log |f|_r &\leq \log(K'' \max\{|h_i^2|_r, 1\} + K') - \log |2|_r \\ &\leq \log(K'' \max\{|h_i^2|_r, 1\}) + \log K' + \log 2 - \log |2|_r \\ &\leq \max\{2 \log |h_i|_r, 0\} + K_f \end{aligned}$$

with K_f is a positive constant greater than $\log K'' + \log K' + \log 2 - \log |2|_r$, and where the second inequality comes from the fact that for all real numbers $x, y \geq 1$, we have $\log(x+y) \leq \log x + \log y + \log 2$ (just write $(1-x)(y-1) \leq 0$).

Finally, we prove Item (3). By Lemma 3.4.8 and Item (2), for each $i \neq k_r$ we have

$$\begin{aligned} \log |g|_r &\leq \max\{2 \log |h_i|_r, 0, 2 \log |f|_r\} + \log \max\{|a_i^2|_r\} \\ &\leq \max\{2 \log |h_i|_r, 0, 2 \max\{0, 2 \log |h_i|_r\} + 2K_f\} + \log \max\{|a_i^2|_r\} \\ &\leq \max\{2 \log |h_i|_r + 2K_f, 2K_f, 4 \log |h_i|_r + 2K_f\} + \log \max\{|a_i^2|_r\} \\ &\leq \max\{0, 4 \log |h_i|_r\} + K_g \end{aligned}$$

where K_g is a fixed positive constant bigger than $2K_f + \log \max\{|a_i^2|_r\}$. □

Lemma 3.4.10. *If Δ is not identically zero, then*

$$\log|\Delta|_r \leq \frac{6M-2}{M(M-1)}\sum \log|h_n|_r + \frac{8}{(M-1)^2}\sum N(r,h_n,\infty) - 2\log r + \mathcal{O}(1).$$

Proof. By the Poisson-Jensen Formula 3.3.2 and Lemma 3.4.3 (Equation (3.5)) we have for r large enough and for each i

$$\begin{aligned}\log|h_i|_r &= N(r,h_i,0) - N(r,h_i,\infty) + C\\ &\geq -N(r,h_i,\infty) + C\\ &\geq -\frac{1}{M-1}\sum_n N(r,h_n,\infty) + C'\end{aligned}$$

for some constant C and negative constant C'. So we have

$$\log|h_i|_r + \frac{1}{M-1}\sum_n N(r,h_n,\infty) - C' \geq 0. \tag{3.9}$$

Given $r > 0$ take k_r as in Lemma 3.4.9. Choose i_r such that $|h_{i_r}|_r$ is minimal in $\{|h_i|_r : i \neq k_r\}$, and note that

$$\log|h_{i_r}|_r \leq \frac{1}{M-1}\sum_{i\neq k_r}\log|h_i|_r.$$

By Item (2) in Lemma 3.4.9, we have for each r large enough

$$\begin{aligned}\log|f|_r &\leq \max\{0, 2\log|h_{i_r}|_r\} + K_f\\ &\leq \max\left\{0, \frac{2}{M-1}\sum_{i\neq k_r}\log|h_i|_r\right\} + K_f\\ &\leq_{(3.9)} \max\left\{0, \frac{2}{M-1}\sum_{i\neq k_r}\log|h_i|_r + \right.\\ &\qquad \left.\frac{2}{M-1}\left(\log|h_{k_r}|_r + \frac{1}{M-1}\sum_i N(r,h_i,\infty) - C'\right)\right\} + K_f\\ &\leq \max\left\{0, \frac{2}{M-1}\sum_i \log|h_i|_r + \right.\\ &\qquad \left.\frac{2}{(M-1)^2}\sum_i N(r,h_i,\infty)\right\} - \frac{2C'}{M-1} + K_f.\end{aligned}$$

Similarly, by Item (3) in Lemma 3.4.9 we have for each r large enough

$$\log|g|_r \leq \max\left\{0, \frac{4}{M-1}\sum_i \log|h_i|_r + \frac{4}{(M-1)^2}\sum_i N(r,h_i,\infty)\right\} - \frac{4C'}{M-1} + K_g.$$

Hence, for large enough r we get

$$\log|f|_r \leq \max\left\{0, \frac{2}{M-1}\sum_n \log|h_n|_r + \frac{2}{(M-1)^2}\sum_n N(r,h_n,\infty)\right\} + \mathcal{O}(1) \tag{3.10}$$

$$\log|g|_r \leq \max\left\{0, \frac{4}{M-1}\sum_n \log|h_n|_r + \frac{4}{(M-1)^2}\sum_n N(r,h_n,\infty)\right\} + \mathcal{O}(1). \tag{3.11}$$

From Lemma 3.3.1 (Logarithmic Derivative Lemma) we have for large enough r and each index n

$$|\Delta|_r \leq |h_n|_r \max\{|h_n f'^2|_r, |h_n'^2 h_n|_r, |h_n' g'|_r\} \leq \frac{1}{r^2}|h_n|_r^2 \max\{|f|_r^2, |h_n|_r^2, |g|_r\}.$$

By Lemma 3.4.8, we have

$$2\log|h_n|_r \leq \max\{2\log|f|_r, 0, \log|g|_r\} + \mathcal{O}(1),$$

hence, since Δ is not the zero function

$$\log|\Delta|_r \leq \log\left(\frac{1}{r^2}|h_n|_r^2\right) + \max\{2\log|f|_r, 0, \log|g|_r\} + \mathcal{O}(1).$$

Since this last expression is true *for each* n, we have

$$\log|\Delta|_r \leq \frac{2}{M}\sum \log|h_n|_r - 2\log r + \max\{2\log|f|_r, 0, \log|g|_r\} + \mathcal{O}(1). \tag{3.12}$$

Note that by equations (3.10) and (3.11) we have

$$\max\{2\log|f|_r, 0, \log|g|_r\} \leq \max\left\{0, \frac{4}{M-1}\sum \log|h_n|_r + \frac{4}{(M-1)^2}\sum N(r,h_n,\infty)\right\} + \mathcal{O}(1)$$

where the right-hand part is of the form $\max\{0, A\} + \mathcal{O}(1)$, and, by Lemma 3.4.4, we have

$$A + \frac{2}{M-1} N(r, f, \infty) + \mathcal{O}(1) \geq 0.$$

Hence,

$$\begin{aligned}\max\{0, A\} + \mathcal{O}(1) = \max \Bigg\{ & \frac{2}{M-1} N(r, f, \infty), A + \\ & \frac{2}{M-1} N(r, f, \infty) \Bigg\} - \frac{2}{M-1} N(r, f, \infty) \\ \leq & \left(\frac{2}{M-1} N(r, f, \infty) + A + \frac{2}{M-1} N(r, f, \infty) + \mathcal{O}(1) \right) \\ & - \frac{2}{M-1} N(r, f, \infty)\end{aligned}$$

and replacing A by its expression we get

$$\begin{aligned}\max\{2 \log |f|_r, 0, \log |g|_r\} \leq & \frac{4}{M-1} \sum \log |h_n|_r + \frac{4}{(M-1)^2} \sum N(r, h_n, \infty) \\ & + \frac{2}{M-1} N(r, f, \infty) + \mathcal{O}(1).\end{aligned}$$

Therefore, by Equation (3.12), we find that $\log |\Delta|_r$ is less than or equal to

$$\begin{aligned}& \left(\frac{2}{M} + \frac{4}{M-1} \right) \sum \log |h_n|_r - 2 \log r + \\ & \frac{4}{(M-1)^2} \sum N(r, h_n, \infty) + \frac{2}{M-1} N(r, f, \infty) + \mathcal{O}(1).\end{aligned}$$

Finally, we bound $N(r, f, \infty)$ using Lemma 3.4.5 and the result follows. □

Lemma 3.4.11. *We have* $\Delta = 0$.

Proof. Assume that Δ is not identically zero. By the Poisson-Jensen Formula 3.3.2, we have

$$\log |\Delta|_r = N(r, \Delta, 0) - N(r, \Delta, \infty) + \mathcal{O}(1).$$

Lemmas 3.4.6, 3.4.7 and 3.4.10 allow us to bound $\log |\Delta|_r$ above and below, obtaining

$$\begin{aligned}\frac{6M-2}{M(M-1)} \sum \log |h_n|_r + \frac{8}{(M-1)^2} I - 2 \log r \geq \\ \frac{1}{2} Z - \frac{8}{M-1} I - \frac{8}{M-1} I + \mathcal{O}(1)\end{aligned}$$

where we write $Z = \sum N(r, h_n, 0)$ and $I = \sum N(r, h_n, \infty)$. Using again the Poisson-Jensen Formula 3.3.2 we have

$$\sum \log |h_n|_r = Z - I + \mathcal{O}(1).$$

Together with Lemma 3.4.5, it gives

$$\begin{aligned}
-2\log r &\geq \left(\frac{1}{2} - \frac{6M-2}{M(M-1)}\right) Z + \\
&\quad \left(\frac{6M-2}{M(M-1)} - \frac{16}{M-1} - \frac{8}{(M-1)^2}\right) I + \mathcal{O}(1) \\
&\geq \left(\left(\frac{1}{2} - \frac{6M-2}{M(M-1)}\right)\frac{M-3}{M-1} - \frac{10M^2-2}{M(M-1)^2}\right) I + \\
&\quad \left(\frac{1}{2} - \frac{6M-2}{M(M-1)}\right)\mathcal{O}(1) + \mathcal{O}(1) \\
&\geq \left(\left(\frac{1}{2} - \frac{6M-2}{M(M-1)}\right)\frac{M-3}{M-1} - \frac{10M^2-2}{M(M-1)^2}\right) I + \mathcal{O}(1) \\
&= \frac{M^2-35M+8}{2M(M-1)} I + \mathcal{O}(1).
\end{aligned}$$

Since

- $-2\log r$ goes to $-\infty$ as r goes to ∞,
- $I + \mathcal{O}(1) \geq 0$, and
- $\dfrac{M^2-35M+8}{2M(M-1)} \geq 0$ for $M \geq 35$,

we obtain a contradiction. □

As a number of methods have been developped for other analogues of Büchi's problem, at this point we may use various different techniques in order to finish the proof of the theorem. We present the method from [PV1, PV2] using elliptic curves, since by a theorem by Berkovich we know that those are not parametrizable by meromorphic functions over $\mathbb{C}_p$.

Since Δ is the zero function, we have

$$g'^2 = 4f'^2 g. \tag{3.13}$$

Hence there exists a meromorphic function u such that $g = u^2$ and Equation (3.13) becomes

$$4u'^2u^2 = 4f'^2u^2.$$

Since g is non-zero by hypothesis, this implies $u'^2 = f'^2$. Hence $u = \alpha f + b$ for some $\alpha \in \{-1, 1\}$ and $b \in \mathbb{C}_p$, and we obtain

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

Choosing three distinct indices i, j and k such that $a_n - \alpha b \neq 0$ for $n = i, j, k$, we obtain

$$\left(\frac{h_i h_j h_k}{\sqrt{(a_i - \alpha b)(a_j - \alpha b)(a_k - \alpha b)}} \right)^2 = (a_i + \alpha b + 2f)(a_j + \alpha b + 2f)(a_k + \alpha b + 2f).$$

Since f is not a constant (by Lemma 3.4.2), we obtain a non-constant parametrization of the elliptic curve

$$Y^2 = (a_i + X)(a_j + X)(a_k + X)$$

which is impossible by Berkovich's Theorem. This finishes the proof.

3.5 p-adic Entire Functions

In this section we prove Theorem 3.2.3.

The purpose of this section is to prove Theorem 3.2.3. Up to some adaptations for the p-adic setting, the proof goes along essentially the same lines as the solution of Büchi's problem for $\mathbb{C}[z]$ using the method of Pheidas and Vidaux (see for example [PV1] for the paper where this method was used by first time, or [PPV] for a quite simplified exposition in the particular case $\mathbb{C}[x]$, which is closer to the case of p-adic entire functions) and we include it here just for the sake of completeness.

We prefer to avoid the use of Berkovich's theorem and replace it by an elementary argument on factorization.

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

Theorem 3.5.1. *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 3.5.2. *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

$$2 \max_n m(r, h_n) \geq m(r, h_i^2 - h_j^2) = m(r, f) + \mathcal{O}(1) \tag{3.14}$$

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

$$\begin{aligned} m(r, g) &\leq 2 \max\{m(r, a_j + f), m(r, h_j)\} + \mathcal{O}(1) \\ &\leq 4 \max_n m(r, h_n) + \mathcal{O}(1). \end{aligned} \tag{3.15}$$

As in the previous section, we define

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

and these functions satisfy the same equation as in the previous section (see Equation (3.7))

$$\Delta = 4h_n \Delta_n.$$

Lemma 3.5.3. *The function Δ is the zero function.*

The point is that, if Δ is not the zero function then we can apply to it the function $m(r,\cdot)$, and we will obtain a contradiction by bounding above and below $m(r,\Delta)$. We we will need the following three claims.

Claim 3.5.4. *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 3.5.4. 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 (3.14) and (3.15) and Lemma 3.3.1 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

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

□

Claim 3.5.5. *For each r large enough, we have*

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

Proof of Claim 3.5.5. 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

$$|2f|_r = |a_i + a_j + 2f|_r$$

because of Lemma 3.5.2 and the definition of $|\cdot|_r$, 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

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

□

Claim 3.5.6. *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 3.5.6. 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 inequality and Theorem 3.3.2 applied to Δ (which is an entire function) lead to

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

□

Proof of Lemma 3.5.3. We suppose Δ is not identically zero. We apply to it $m(r, \cdot)$ and use the bounds given in the above Claims to get:

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

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

From the equation $\Delta = 0$ we have

$$g'^2 = 4f'^2 g. \tag{3.16}$$

By Lemma 3.5.2 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 (3.16) 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 3.5.2 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 3.5.1 is complete.

3.6 Undecidability Results

In this section we prove Theorem 3.2.4.

We will use the positive answer to Problems $\mathbf{BP}(\mathcal{M}_p)$ and $\mathbf{BP}(\mathcal{A}_p)$. First we define the following $\mathcal{L}_2^z$-formulas:

$$\begin{aligned} \mathrm{Bu}[x, y] &: \exists u_1 \ldots \exists u_{35} \left(\wedge_{i=1}^{35} P_2(u_i)\right) \wedge \left(\wedge_{i=2}^{34} u_{i-1} + u_{i+1} = 2u_i + 2\right) \\ &\qquad \wedge x = u_1 \wedge 2y + 1 = u_2 - u_1 \\ \mathrm{Sq}[x, y] &: \mathrm{Bu}[x, y] \wedge \mathrm{Bu}[f_z x, f_z f_z y] \\ \mathrm{Prod}[x, y, w] &: \exists u \exists v P_2(u) \wedge P_2(v) \wedge \\ &\qquad (\mathrm{Sq}[x + y, u] \wedge \mathrm{Sq}[x - y, v] \wedge u = v + 4w)\,. \end{aligned}$$

Note that all the above formulas are positive existential.

Next we define the following systems of equations:

$$\mathrm{Bu}_{\mathrm{sys}}(a,b): \begin{cases} q_3^2 - 2q_2^2 + q_1^2 = 2 \\ \vdots \\ q_{35}^2 - 2q_{34}^2 + q_{33}^2 = 2 \\ q_1^2 = b \\ q_2^2 - q_1^2 = 2a + 1 \end{cases}$$

$$\mathrm{Sq}_{\mathrm{sys}}(a,b): \begin{cases} \mathrm{Bu}_{\mathrm{sys}}(a,b) \\ \mathrm{Bu}_{\mathrm{sys}}(za, z^2 b) \end{cases}$$

and

$$\mathrm{Prod}_{\mathrm{sys}}(a,b,c): \begin{cases} \mathrm{Sq}(a, x^2) \\ \mathrm{Sq}(b, y^2) \\ \mathrm{Sq}(a+b, w^2) \\ w^2 = x^2 + 2c + y^2 \end{cases}$$

where it is understood that, if we consider a system of equations built up by several of these systems, then the unknowns in each of them are distinct. For example, in the definition of $\mathrm{Sq}_{\mathrm{sys}}$, since we use twice $\mathrm{Bu}_{\mathrm{sys}}$, it is understood that the variables q_i in the first $\mathrm{Bu}_{\mathrm{sys}}$ are distinct from the variables q_i appearing in the second $\mathrm{Bu}_{\mathrm{sys}}$.

Note that the system $\mathrm{Prod}_{\mathrm{sys}}(x^2, y^2, z^2)$ (where x, y, z also are considered as unknowns) is a system of diagonal quadratic equations with coefficients in $\mathbb{Z}[z]$.

From the definition of the above formulas and systems of equations, it is clear that given $a, b, c \in R$, where $R = \mathcal{A}_p$ or $\mathcal{M}_p$, we have the following:

- $R \models \mathrm{Bu}[a,b]$ if and only if the system $\mathrm{Bu}_{\mathrm{sys}}(a,b)$ has a solution in R
- $R \models \mathrm{Sq}[a,b]$ if and only if the system $\mathrm{Sq}_{\mathrm{sys}}(a,b)$ has a solution in R
- $R \models \mathrm{Prod}[a,b,c]$ if and only if the system $\mathrm{Prod}_{\mathrm{sys}}(a,b,c)$ has a solution in R.

Lemma 3.6.1. *If $a, b, c \in R$, where $R = \mathcal{A}_p$ or $R = \mathcal{M}_p$, then the following statements are equivalent:*

i. $ab = c$

ii. $R \models \mathrm{Prod}[a, b, c]$

iii. $\mathrm{Prod}_{\mathrm{sys}}(a, b, c)$ *has a solution in* R.

Proof. Because of the above discussion, it is enough to prove that item i is equivalent to item ii. By Corollary 3.2.2 we have: R satisfies $\mathrm{Bu}[a, b]$ if and only if $b = a^2$ or a and b are constants. Thus, R satisfies $\mathrm{Sq}[a, b]$ if and only if $b = a^2$. Therefore, R satisfies $\mathrm{Prod}[a, b, c]$ if and only if $c = ab$. □

Proof of Theorem 3.2.4. This is a consequence of the equivalence of items i and ii in Lemma 3.6.1, and the fact that $\mathrm{Prod}[x, y, z]$ is a positive existential $\mathcal{L}_2^z$-formula. □

Proof of Theorem 3.2.6. From Theorem 3.2.4 we obtain the non-existence of an algorithm to solve any of the following problems:

1. Given a system

$$\sum_{i=1}^{r} a_{ik} x_i^2 + \sum_{j=1}^{s} b_{jk} y_j = c_k, \quad k = 1, \ldots, t \tag{3.17}$$

   with all the a_{ik}, b_{jk}, c_k in $\mathbb{Z}[z]$, to decide whether or not the system has a solution in $\mathcal{A}_p$.

2. Given a system

$$\sum_{i=1}^{r} a_{ik} x_i^2 + \sum_{j=1}^{s} b_{jk} y_j = c_k, \quad k = 1, \ldots, t \tag{3.18}$$

   with all the a_{ik}, b_{jk}, c_k in $\mathbb{Z}[z]$, and given two sets $I \subseteq \{1, \ldots, r\}$ and $J \subseteq \{1, \ldots, s\}$, to decide whether or not the system has a solution in $\mathcal{M}_p$ satisfying $x_i(0) = 0$ for each $i \in I$ and $y_j(0) = 0$ for each $k \in J$.

To prove item (1) of the theorem, consider the diagonal quadratic system

$$\sum_{i=1}^{r} a_{ik} x_i^2 + \sum_{k=1}^{s} b_{jk} (u_j^2 - v_j^2) = c_k, \quad k = 1, \ldots, t. \tag{3.19}$$

System (3.19) has a solution in $\mathcal{A}_p$ if and only if System (3.17) has, because of the identity

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

In order to prove item (2) of the theorem, we cannot perform the same substitution as before in order to eliminate the degree-one part, because a technical problem arises with the vanishing conditions. Namely, if we replace an unknown y_j with condition $y_j(0) = 0$ by $(u_j^2 - v_j^2)$ as in the previous case, then the vanishing condition becomes $(u_j^2 - v_j^2)(0) = 0$, which is useless because we want vanishing conditions on the *unknowns*, not on *polynomial expressions* of the unknowns. To fix this problem, we will use again the positive answer to Büchi's problem in order to perform a substitution in such a way that vanishing conditions on unknowns become vanishing conditions on the new unknowns. We will obtain not one but several diagonal quadratic systems, but this will be enough to prove the Theorem.

Consider the following $2^{|J|}$ diagonal quadratic systems S_α indexed by $\alpha \subseteq J$:

$$\begin{cases} \displaystyle\sum_{i=1}^{r} a_{ik}x_i^2 + \sum_{j\in\alpha} b_{jk}(u_{j2}^2 - u_{j1}^2 - 1) + \sum_{\substack{1\le j\le s\\ j\notin J}} b_{jk}(w_{j2}^2 - w_{j1}^2) = c_k,\ k = 1,\dots,t \\ u_{j3}^2 - 2u_{j2}^2 + u_{j1}^2 = 2,\ j \in \alpha \\ \vdots \\ u_{j35}^2 - 2u_{j34}^2 + u_{j33}^2 = 2,\ j \in \alpha \\ \mathrm{Prod}(u_{j1}^2, v_j^2, 1),\ j \in \alpha \end{cases}$$

with conditions $x_i(0) = 0$ for each $i \in I$ and $u_{j1}(0) = 0$ for each $j \in \alpha$.

We make the following two obvious observations about functions in $\mathcal{M}_p$:

(A) $f(0) = 0$ and f is constant if and only if $f = 0$.

(B) $f(0) = 0$ and f is non-constant if and only if $f(0) = 0$ and f is invertible.

We will prove now that System (3.18) has a solution in $\mathcal{M}_p$ satisfying its corresponding vanishing conditions if and only at least one of the Systems S_α has a solution in $\mathcal{M}_p$ satisfying its vanishing conditions.

First, assume that System (3.18) has a solution $x_i = f_i$, $y_j = g_j$ satisfying the vanishing conditions and define

$$\alpha = \{j \in J\colon g_j \text{ is non-constant}\}.$$

Then S_α has the following solution satisfying its vanishing conditions (by Lemma 3.6.1):

$$\begin{array}{rcll} x_i & = & f_i & \\ u_{jl} & = & \frac{g_j}{2} + l - 1 & \text{for } j \in \alpha \\ v_j & = & \frac{1}{u_{jl}} & \text{for } j \in \alpha \\ w_{j1} & = & \frac{g_j - 1}{2} & \text{for } 1 \leq j \leq s \text{ and } j \notin J \\ w_{j2} & = & \frac{g_j + 1}{2} & \text{for } 1 \leq j \leq s \text{ and } j \notin J. \end{array}$$

Observe that the y_j with $j \in J - \alpha$ have been replaced by 0 (observation (A)).

Assume now that System S_α has the following solution satisfying its vanishing conditions:

$$\begin{array}{rcll} x_i & = & \chi_i & \\ u_{jl} & = & \mu_{jl} & \text{for } j \in \alpha \\ v_j & = & \nu_j & \text{for } j \in \alpha \\ w_{j1} & = & \omega_{j1} & \text{for } 1 \leq j \leq s \text{ and } j \notin J \\ w_{j2} & = & \omega_{j2} & \text{for } 1 \leq j \leq s \text{ and } j \notin J. \end{array}$$

Then the following is a solution of System (3.18):

$$\begin{array}{rcll} x_i & = & \chi_i & \\ y_j & = & 0 \text{ for } j \in J - \alpha & \\ y_j & = & \mu_{j2}^2 - \mu_{j1}^2 - 1 & \text{for } j \in \alpha \\ y_j & = & \omega_{j2}^2 - \omega_{j1}^2 & \text{for } 1 \leq j \leq s \text{ and } j \notin J. \end{array}$$

It only remains to show that this solution satisfies the vanishing conditions of System (3.18). Indeed, the condition $x_i(0) = 0$ for $i \in I$ holds because it is the same vanishing condition on the x_i as in S_α. For $j \in J$ we have $y_j(0) = 0$, which is trivially true for $j \in J - \alpha$. For $j \in \alpha$ we have $\mu_{j1}(0) = 0$ (this is a condition on S_α) and μ_{j1} is invertible (its inverse is $\pm\nu_j$). Therefore, by observation (B) the function μ_{j1} is non-constant. Observe that $(\mu_{jl})_{l=1}^{35}$ is a Büchi sequence with a non-constant term, hence, by Corollary 3.2.2 there exists a non-cosntant γ_j such that $\mu_{jl}^2 = (\gamma_j + l)^2$. This implies that

$$y_j = \mu_{j2}^2 - \mu_{j1}^2 - 1 = 2(\gamma_j + 1) = 2\mu_{j1}$$

hence, using the condition $\mu_{j1}(0) = 0$ for $j \in \alpha$ on S_α, we obtain $y_j(0) = 2\mu_{j1}(0) = 0$. □

3.7 Some geometric results

This section contains most of the geometric results that we will use in the next two sections. The arguments given here essentially are adaptations of the arguments given by Vojta in [Vo2]. For the sake of completeness, we will perform most of the computations.

During the whole section, we assume that the base field is $\mathbb{C}$, and we write $g(X)$ for the genus of the curve X.

Let $S = (\delta_2, \delta_3, \ldots)$ be a sequence in $\mathbb{C}^*$ with pairwise distinct terms. Set $X_2 = \mathbb{P}^2(\mathbb{C})$ and for $n > 2$ let $X_n \subset \mathbb{P}^n(\mathbb{C})$ be the algebraic set defined by the equations

$$\delta_2 x_i^2 = \delta_i \delta_2 (\delta_i - \delta_2) x_0^2 - (\delta_i - \delta_2) x_1^2 + \delta_i x_2^2 \tag{3.20}$$

as the index i ranges from 3 to n. If $[x_0 : \cdots : x_n] \in X_n$, it is easy to see that at most 2 of the x_i can be zero, hence $X_n \subseteq U_0 \cup U_1 \cup U_2$ where U_i is the open set $\{x_i \neq 0\}$.

Lemma 3.7.1. *The variety X_n is a smooth surface in $\mathbb{P}^n$, contains the lines*

$$\pm x_1 = \pm x_2 - \delta_2 x_0 = \cdots = \pm x_n - \delta_n x_0 \tag{3.21}$$

and has canonical sheaf $\mathcal{O}_{X_n}(n-5)$. In particular, X_n is of general type for $n \geq 6$.

Proof. Observe that, for $[x_0 : \cdots, x_n] \in X_n \cap U_0$ the matrix

$$\begin{bmatrix} (\delta_3 - \delta_2)x_1 & -\delta_3 x_2 & \delta_2 x_3 & 0 & \cdots & 0 \\ (\delta_4 - \delta_2)x_1 & -\delta_4 x_2 & 0 & \delta_2 x_4 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ (\delta_n - \delta_2)x_1 & -\delta_n x_2 & 0 & 0 & \cdots & \delta_2 x_n \end{bmatrix} \tag{3.22}$$

has rank $n-2$. Indeed, there are 3 cases depending on the number of zeroes among $x_3, \ldots, x_n$:

1. No zero: trivial.

2. One zero: at least one of the first two columns has no zero.

3. Two zeroes: suppose that $x_i = x_j = 0$ where $3 \leq i < j \leq n$, then no entry in the first two columns is zero. Therefore

$$\begin{vmatrix} (\delta_i - \delta_2)x_1 & -\delta_i x_2 \\ (\delta_j - \delta_2)x_1 & -\delta_j x_2 \end{vmatrix} = \delta_2 x_1 x_2 (\delta_j - \delta_i) \neq 0.$$

hence, X_n is nonsingular at each point in $X_n \cap U_0$. The verification that X_n is nonsingular at each point in $X_n \cap U_1$ and $X_n \cap U_2$ is quite similar, but the determinants in case (3) are

$$\begin{vmatrix} -\delta_i\delta_2(\delta_i - \delta_2)x_0 & -\delta_i x_2 \\ -\delta_j\delta_2(\delta_j - \delta_2)x_0 & -\delta_j x_2 \end{vmatrix} = \delta_2\delta_i\delta_j x_0 x_2 (\delta_j - \delta_i) \neq 0$$

and

$$\begin{vmatrix} -\delta_i\delta_2(\delta_i - \delta_2)x_0 & (\delta_i - \delta_2)x_1 \\ -\delta_j\delta_2(\delta_j - \delta_2)x_0 & (\delta_j - \delta_2)x_1 \end{vmatrix} = \delta_2 x_0 x_1 (\delta_j - \delta_i)(\delta_j - \delta_2)(\delta_i - \delta_2) \neq 0$$

respectively. Therefore X_n is a smooth surface in $\mathbb{P}^n$.

The claim about the lines (3.21) is an easy computation (looking at $U_0 \cap X_n$).

Finally, since X_n is a complete intersection surface in $\mathbb{P}^n$ defined as the intersection of $n-2$ smooth hypersurfaces of degree 2, its canonical sheaf is

$$\mathcal{O}(2(n-2) - n - 1) = \mathcal{O}(n-5).$$

□

Definition 3.7.2. *Define the trivial lines of X_n as the lines* (3.21).

Observe that for $n \geq 3$ the rational map

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

induces a finite morphism

$$\pi_n \colon X_n \to X_{n-1}$$

of degree 2 ramified along the curve $C_n \subset X_n$ defined by $x_n = 0$. This curve is nonsingular. Indeed, if

$$[x_0 : \cdots : x_n] \in C_n = X_n \cap \{x_n = 0\}$$

then at most one of the $x_0, \ldots, x_{n-1}$ can be zero and the remaining verification can be performed as in the proof of Lemma 3.7.1 for cases (2) and (3) since $x_n = 0$, but adding the extra row $(0, \ldots, 0, 1)$ to each matrix.

Define $\phi_n = \pi_3 \circ \cdots \circ \pi_n$. We note that the image of C_n in X_2 via ϕ_n is

$$\delta_n \delta_2 (\delta_n - \delta_2) x_0^2 - (\delta_n - \delta_2) x_1^2 + \delta_n x_2^2 = 0. \tag{3.23}$$

Definition 3.7.3. *Let X be a smooth surface over $\mathbb{C}$ and let $\mathcal{L}$ be an invertible sheaf on X. Take a section*

$$\omega \in H^0(X, \mathcal{L} \otimes S^2(\Omega^1_X)).$$

Let $Y \subset X$ be a curve with normalization $i : \tilde{Y} \to Y$. We say that Y is ω-integral *if*

$$i^*\omega \in H^0(\tilde{Y}, i^*(\mathcal{L}) \otimes S^2(\Omega^1_{\tilde{Y}}))$$

vanishes identically on $\tilde{Y}$.

On $U_0 \subset \mathbb{P}^2 = X_2$ define

$$\omega = x_1 x_2 dx_1 \otimes dx_1 + (\delta_2^2 - x_1^2 - x_2^2) dx_1 \otimes dx_2 + x_1 x_2 dx_2 \otimes dx_2.$$

Note that, after the change of variables $y_0 = x_0/x_1$ and $y_2 = x_2/x_1$, on $U_0 \cap U_1$, we have

$$\omega = \frac{1}{y_0^5} \left(\delta_2^2 y_0 y_2 dy_0 \otimes dy_0 + (1 - \delta_2^2 y_0^2 - y_2^2) dy_0 \otimes dy_2 + y_0 y_2 dy_2 \otimes dy_2 \right)$$

hence ω extends to a section

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

Lemma 3.7.4. *Write $[x_0 : x_1 : x_2]$ for homogeneous coordinates on $\mathbb{P}^2 = X_2$. The only ω_2-integral curves on X_2 are*

1. *$x_0 = 0$, $x_1 = 0$, and $x_2 = 0$*
2. *the four trivial lines*
3. *the conics $\delta_2 c(c - \delta_2) x_0^2 - (c - \delta_2) x_1^2 + c x_2^2 = 0$ for $c \neq 0, \delta_2$.*

Moreover, if $f \colon \mathbb{C} \to X_2(\mathbb{C})$ is a non-constant holomorphic map satisfying $f^*\omega_2 = 0$ then its image is contained in one of these curves.

Proof. It is easy to see that curves of type (1) and (2) are ω_2-integral. Let's show that curves of type (3) are ω_2-integral. If we look at the affine chart U_0, on a curve of type (3) we have

$$(c-\delta_2)x_1dx_1 = cx_2dx_2$$

hence

$$\begin{aligned}
\omega_2 &= \left(\frac{c^2x_2^3}{(c-\delta_2)^2x_1} + \frac{cx_2}{(c-\delta_2)x_1}(\delta_2^2 - x_1^2 - x_2^2) + x_1x_2\right) dx_2 \otimes dx_2 \\
&= \left(c^2x_2^2 + c(c-\delta_2)(\delta_2^2 - x_1^2 - x_2^2) + (c-\delta_2)^2x_1^2\right) \frac{x_2dx_2 \otimes dx_2}{(c-\delta_2)^2x_1} \\
&= \left(\delta_2^2c(c-\delta_2) - \delta_2(c-\delta_2)x_1^2 + \delta_2cx_2^2\right) \frac{x_2dx_2 \otimes dx_2}{(c-\delta_2)^2x_1} \\
&= \delta_2\left(\delta_2c(c-\delta_2) - (c-\delta_2)x_1^2 + cx_2^2\right) \frac{x_2dx_2 \otimes dx_2}{(c-\delta_2)^2x_1} = 0.
\end{aligned}$$

Conversely, let Y be an ω_2-integral curve on X_2 not of type (1) or (2). We will show that Y is of type (3). Let $P \in Y$ be a regular point of Y not in a line of type (1) nor (2). As Y is regular at P, in some neighborhood of P one can assume that one affine coordinate is function of the other, say $x_1 = x_1(x_2)$. Since Y is ω_2-integral, we get a quadratic ordinary differential equation for x_1. Hence there are 2 local solutions at P. But exactly 2 curves of type (3) pass through P. Therefore, Y is locally of type (3) on a dense set of points, and so Y is of type (3).

A similar computation proves the assertion about holomorphic maps. □

Observe that the image of C_n in X_2 is ω_2-integral (see Equation (3.23)). Write $\omega_n' = \phi_n^*\omega_2$ and note that

$$\omega_n' \in H^0(X_n, \mathcal{O}_{X_n}(5) \otimes S^2(\Omega^1_{X_n}))$$

because $\pi_n^*\mathcal{O}_{X_{n-1}}(1) = \mathcal{O}_{X_n}(1)$ for each $n \geq 3$.

Lemma 3.7.5. *Let $n \geq 6$ be an integer. The only ω_n'-integral curves on X_n are*

1. *the pull-backs via ϕ_n of the coordinate axes on X_2 to X_n*
2. *the trivial lines*

3. *the pull-backs via* ϕ_n *of the conics* $\delta_2 c(c-\delta_2)x_0^2 - (c-\delta_2)x_1^2 + cx_2^2 = 0$ *for* $c \neq 0, \delta_2$.

These curves are nonsingular and the only one with genus $\leq 2^{n-3}$ *are the trivial lines, with genus* 0. *Moreover, if* $h : \mathbb{C} \to X_n(\mathbb{C})$ *is a non-constant holomorphic map satisfying* $h^*\omega_n' = 0$ *then the image of* h *is contained in one of these curves.*

Proof. Let $Y \subseteq X_n$ be a ω_n'-integral curve. Write

$$Z = \phi_n(Y) \quad \text{and} \quad Y' = \phi_n^*(Z).$$

Note that Z is ω_2-integral. Hence we have 3 cases by Lemma 3.7.4.

Suppose that

$$Z = \{x_j = 0\} \subseteq X_2$$

is a coordinate axe. Then

$$Y' = X_n \cap \{x_j = 0\}$$

is nonsingular by a verification similar to the one done for C_n. Since Z meets all the curves $\phi(C_i)$ for $i = 3, \ldots, n$ and they form the branch divisor, Y' is connected. Hence $Y' = Y$ and Y is nonsingular. Note that

$$\phi_n|_Y : Y \to Z$$

has degree 2^{n-2} and is ramified at $2^{n-2}(n-2)$ points, hence

$$g(Y) = 2^{n-3}(n-4) + 1$$

by the Hurwitz formula.

Now suppose that Z is a trivial line in X_2. Replacing the value of x_2 in terms of x_1 in the defining equations of X_n we obtain that Y is a trivial line, with genus 0.

Finally suppose that Z is a curve of type (3) in Lemma 3.7.4. By the same argument as in the first case, Y' is connected. One can show that Y' is nonsingular by a direct computation (on the affine chart U_0 we add the row

$$((c-\delta_2)x_1, -cx_2, 0, \ldots, 0)$$

in 3.22, and for U_1, U_2 the computation is similar) therefore $Y = Y'$. Consider the map $\phi_n|_Y : Y \to Z$. This map induces a morphism $\psi_n : Y \to Z$. If Y lies

above one of the curves C_i then $\deg(\psi_n) = 2^{n-3}$ and if Y does not lie above any C_i then $\deg(\psi_n) = 2^{n-2}$. Anyway, ϕ_n is ramified at least in

$$(n-3) \cdot 4 \cdot 2^{n-4} = 2^{n-2}(n-3)$$

points and $g(Z) = 0$, thus for $n \geq 6$ by the Hurwitz formula we have

$$g(Y) > -2^{n-2} + 2^{n-3}(n-3) = 2^{n-3}(n-5) \geq 2^{n-3}.$$

The assertion about holomorphic maps follows from taking $f = \phi_n \circ h$ in Lemma 3.7.4 and noting that f is not constant since ϕ_n is finite, and

$$f^*\omega_2 = h^*\psi_n^*\omega_2 = h^*\omega_n' = 0.$$

□

Lemma 3.7.6. *Let $\pi : X' \to X$ be a finite morphism of smooth projective surfaces over $\mathbb{C}$, ramified along a curve $Y \subset X'$. Let $\mathcal{L}$ be a invertible sheaf on X, and take a section*

$$\omega \in H^0(X, \mathcal{L} \otimes S^2(\Omega^1_X)).$$

If $\pi(Y)$ is ω-integral, then

$$\pi^*\omega \in H^0(X', \pi^*\mathcal{L} \otimes S^2(\Omega^1_{X'}))$$

vanishes identically on Y.

Proof. This is a particular case of [Vo2] Lemma 2.10. □

We recall to the reader that $\omega_n' = \phi_n^*\omega_2$.

Lemma 3.7.7. *Define $\omega_2' = \omega_2$. The sections ω_n' determine sections*

$$\omega_n \in H^0(X_n, \mathcal{O}_{X_n}(7-n) \otimes S^2(\Omega^1_{X_n}))$$

such that each ω_n-integral curve is a ω_n'-integral curve. Moreover, the ω_n-integral curves are the same as the ω_n'-integral curves, with the only possible exception of ω'-integral curves lying over $C_3, \ldots, C_n$.

Proof. By induction. The case $n = 2$ is clear. Assume it for $n = m - 1$ with $m > 2$. Note that $\pi_m(C_m)$ does not lie over any of the curves $C_3, \ldots, C_{m-1}$ because they have different images in X_2, hence $\pi_m(C_m)$ is ω_{m-1}-integral by Lemma 3.7.5 and induction hypothesis. Consider the section

$$\begin{aligned}\pi_m^*\omega_{m-1} &\in H^0(X_m, \pi_m^*\mathcal{O}_{X_{m-1}}(7-(m-1)) \otimes S^2(\Omega^1_{X_m})) \\ &= H^0(X_m, \mathcal{O}_{X_m}(7-(m-1)) \otimes S^2(\Omega^1_{X_m}))\end{aligned}$$

(recall that $\pi_n^*\mathcal{O}_{X_{n-1}}(1) = \mathcal{O}_{X_n}(1)$). By Lemma 3.7.6 we have that $\pi_m^*\omega_{m-1}$ vanishes identically on C_m, thus $\pi_m^*\omega_{m-1}$ determines a global section ω_m in

$$\mathcal{O}_{X_m}(7-m) \otimes S^2(\Omega^1_{X_m})$$

by taking

$$\omega_m = \frac{1}{x_m}\pi_m^*\omega_{m-1}.$$

Call U_m the open set of X_m obtained by deleting the curves lying over any of the $C_3, \ldots, C_m$. The sections ω'_m and ω_m agree on U_m up to a non-vanishing factor, therefore the ω'_m-integral curves and the ω_m-integral curves are the same on U_m. A curve lying over some C_i is of type (3) in Lemma 3.7.5 (see Equation 3.23), hence it is ω'_m-integral, and we are done. □

Corollary 3.7.8. *For $n \geq 6$, the only ω_n-integral curves with genus $\leq 2^{n-3}$ on X_n are the trivial lines, with genus 0. Moreover, if $h : \mathbb{C} \to X_n(\mathbb{C})$ is a non-constant holomorphic map such that $h^*\omega_n = 0$ then the image of h lies in a trivial line.*

Proof. From Lemma 3.7.5 and Lemma 3.7.7 we deduce the first part of the Lemma, and the fact that the image of h lies in a curve with genus $> 2^{n-3}$ or in a trivial line. Use Picard's Theorem to conclude. □

Theorem 3.7.9. *For $n \geq 8$, the only curves of genus 0 or 1 on X_n are the trivial lines.*

Proof. Let $Y \subseteq X_n$ be a curve of genus 0 or 1 and write $i : \tilde{Y} \to Y$ for its normalization. On the one hand, the curve $\tilde{Y}$ has genus 0 or 1, hence $\mathcal{K}_{\tilde{Y}}$ has non-positive degree. On the other hand, the sheaf $i^*\mathcal{O}_{X_n}(7-n)$ has negative degree because $n \geq 8$. Therefore,

$$i^*\mathcal{O}_{X_n}(7-n) \otimes \mathcal{K}_{\tilde{Y}}^{\otimes 2}$$

has no nonzero global section on $\tilde{Y}$, hence $i^*\omega_n$ vanishes identically on $\tilde{Y}$. From this we deduce that Y is a ω_n-integral curve with genus ≤ 1 on X_n, and we are done by Corollary 3.7.8. □

3.8 Correspondence between polynomials and points

We understand that, given a sequence $\delta_2, \delta_3, \ldots$ of distinct non-zero elements in $K/\mathbb{Q}$, the surfaces X_n are defined by Equation (3.20).

Lemma 3.8.1. *Fix a sequence $(a_1, a_2, \ldots a_n)$ in $K/\mathbb{Q}$, with $n \geq 3$ and pairwise distinct a_i. Set $\delta_i = a_i - a_1$ for $i \geq 2$. There is an injective map from the set of monic polynomials $f \in K[x]$ of degree two satisfying that $f(a_i)$ is a square for $i = 1, \ldots, n$, to the set*

$$X_n(K) \cap \{x_0 \neq 0\}.$$

The map is

$$j(f) = [1 : \sqrt{f(a_1)} : \cdots : \sqrt{f(a_n)}]$$

(for a fixed choice of square roots) and has the property that f is a square in $K[x]$ if and only if $j(f)$ lies in a trivial line of X_n.

Proof. Take a polynomial

$$f = x^2 + ax + b \in K[x]$$

with the property that

$$f(a_1) = b_1^2, \ldots, f(a_n) = b_n^2$$

are squares in K, then

$$\begin{aligned} \delta_2 b_i^2 &= (a_2 - a_1) f(a_i) = (a_2 - a_1)(a_i^2 + u a_i + v) \\ &= (a_i - a_1)(a_2 - a_1)(a_i - a_2) \cdot 1 - (a_i - a_2)(a_1^2 + u a_1 + v) + \\ &\quad (a_i - a_1)(a_2^2 + u a_2 + v) \\ &= \delta_i \delta_2 (\delta_i - \delta_2) 1^2 - (\delta_i - \delta_2) b_1^2 + \delta_i b_2^2 \end{aligned} \tag{3.24}$$

Therefore, for each polynomial

$$f = x^2 + ux + v \in K[x]$$

with the property that $f(a_1), \ldots, f(a_n)$ are squares in K, we have that

$$j(f) \in X_n(K) \cap \{x_0 \neq 0\}.$$

Now we check injectivity. Given a point

$$p = [1 : b_1 : \cdots : b_n] \in X_n(K) \cap \{x_0 \neq 0\},$$

define

$$f_p = x^2 + \frac{b_2^2 - b_1^2 - a_2^2 + a_1^2}{a_2 - a_1}x + \frac{a_1a_2(a_2 - a_1) - a_1b_2^2 + a_2b_1^2}{a_2 - a_1} \in K[x]$$

The polynomial f_p is the *only* monic polynomial of degree two satisfying $f_p(a_1) = b_1^2$ and $f_p(a_2) = b_2^2$. Moreover, after a standard computation we get

$$\delta_2 f_p(a_1 + \delta_i) = \delta_i\delta_2(\delta_i - \delta_2) - (\delta_i - \delta_2)b_1^2 + \delta_i b_2^2$$

and, since

$$p \in X_n(K) \cap \{x_0 \neq 0\},$$

we obtain

$$\delta_2 f_p(a_1 + \delta_i) = \delta_2 b_i^2.$$

Therefore, we have $f_p(a_i) = b_i^2$ for each i. The uniqueness of f_p proves that j is injective.

Assume that

$$j(g) = [1 : b_1 : \cdots : b_n]$$

lies in a trivial line for some

$$g = x^2 + ux + v \in K[x].$$

Thus we have an equation of the kind $\pm b_2 - \delta_2 = \pm b_1$, say

$$\epsilon' b_2 = \epsilon b_1 + a_2 - a_1$$

for $\epsilon, \epsilon' \in \{1, -1\}$. Therefore, we have

$$b_2^2 = b_1^2 + 2\epsilon(a_2 - a_1)b_1 + (a_2 - a_1)^2$$

and we get

$$\left(\frac{b_2^2 - b_1^2 - a_2^2 + a_1^2}{a_2 - a_1}\right)^2 - 4\left(\frac{a_1a_2(a_2 - a_1) - a_1b_2^2 + a_2b_1^2}{a_2 - a_1}\right) = 4b_1^2(\epsilon^2 - 1) = 0$$

So, using the above definition of f_p, we have

$$g = f_{j(g)} = \left(x + \frac{u}{2}\right)^2.$$

□

3.9 Number and function fields, meromorphic functions

We use the same notation as in Section 3.7. First we prove Theorem 3.2.7.

Proof. We follow the notation of Section 3.7. For $i = 2, \dots, 8$ set $\delta_i = a_i - a_1$ and note that $X_2, \dots, X_8$ are defined over K. If Conjecture 3.1.2 holds then there exists a proper Zariski closed subset $Z \subsetneq X_8$ such that all the K-rational points of X_8 belong to Z. Given an irreducible curve $Y \subseteq X_n$, if $Y(K)$ is dense in $Y(\mathbb{C})$ then Y is defined over K and, by Faltings' Theorem, Y has genus at most 1. Therefore we can take Z as the union of a finite number of curves on X_8 with genus 0 or 1, up to a finite number of K-rational points. We conclude by Theorem 3.7.9 and Lemma 3.8.1. □

Let us prove Corollary 3.2.8.

Proof. Since the set $E(\mathbb{Q}, (a_i)_i)$ is finite, it is enough to show that a monic polynomial $f \in \mathbb{Z}[z]$ which is not a square, is such that $f(n)$ is a square at most for a finite number of $n \in \mathbb{Z}$. Indeed, the graph of

$$y = \sqrt{f(x)}$$

is asymptotic to the graph of $y = |x|$, and hence has no integer point for large enough $|x|$. □

The next proposition will be useful to prove Theorem 3.2.9.

Proposition 3.9.1. *Let $n \geq 8$. If $Y \subseteq X_n$ is a curve, its normalization is $i : \tilde{Y} \to Y$ and $g(\tilde{Y}) < \frac{n-3}{4}$, then Y is an ω_n-integral curve.*

Proof. Let $i : \tilde{Y} \to Y$ be the normalization map. We have

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

As $\deg i^*\mathcal{O}_{X_n}(1) \geq 1$, for $n \geq 8$ we get

$$\begin{aligned} \deg\left(i^*\mathcal{O}_{X_n}(7-n) \otimes \mathcal{K}_{\tilde{Y}}^{\otimes 2}\right) &= (7-n)\deg i^*\mathcal{O}_{X_n}(1) + 4g(\tilde{y}) - 4 \\ &\leq 7 - n + 4g(\tilde{Y}) - 4 \\ &= 4g(\tilde{Y}) + 3 - n < 0. \end{aligned}$$

Therefore, $i^*\omega_n$ is zero in $\tilde{Y}$. □

Now we present the proof of Theorem 3.2.9.

Proof. We can assume $F = \mathbb{C}$. Suppose P has some non-constant coefficient and

$$P(a_i) = h_i^2, i = 1, \ldots, M$$

for some $a_i \in \mathbb{C}$ and $h_i \in K(C)$. Using Lemma 3.8.1 with $K = K(C)$, one can verify that

$$h = [1 : h_1 : \ldots : h_M]$$

defines a non-constant morphism $h : C \to X_M$, where we consider $\delta_i = a_i - a_1$ in the definition of X_M. Since C is a complete variety we obtain that $\mathrm{im}(h)$ is algebraic. Let Y be an irreducible curve containing $\mathrm{im}(h)$, since h is dominant on Y, we conclude that h factors through $\tilde{Y}$. By Riemann-Hurwitz Formula, we have

$$g(\tilde{Y}) \leq g(C) \leq \frac{M}{4} - 1 < \frac{M-3}{4}$$

hence Y is a ω_M integral curve by the previous Lemma. Finally, Lemma 3.7.8 implies that $\mathrm{im}(h)$ is contained in a trivial line, and the conclusion follows from Lemma 3.8.1. □

Before proving Theorem 3.2.10 we need to fix some notation in complex Nevanlinna theory. We refer the reader to the notes [Vo3] on Diophantine Approximation and Complex Nevanlinna Theory, where Vojta gives a concise and self-contained introduction to this topic. We follow the notation used there.

Let X be a smooth projective variety over $\mathbb{C}$. For each divisor $D \in \mathrm{Div}(X)$ and for each holomorphic map $f : \mathbb{C} \to X$ whose image is not contained in the support of D, we denote by

$$T_{D,f} : \mathbb{R}^+ \to \mathbb{R}$$

the *Nevanlinna height function* associated to D and f. Moreover, one can define (up to a bounded term as r varies) a *Nevanlinna height function* for line sheaves by letting $T_{\mathcal{L},f} = T_{D,f}$, where $D \in \mathrm{Div}(X)$ can be any divisor such that $\mathcal{L} = \mathcal{O}(D)$ and the image of f is not contained in D. There is a formal analogy between these height functions and the ones produced by the Weil Height Machine in the context of heights for algebraic points on varieties. Indeed, this is part of a deep formal analogy between Nevanlina Theory for holomorphic maps and Diophantine Approximation; see for example [O] or [Vo1].

We need the following result:

Theorem 3.9.2 (See [Vo2] Prop. 6.1)**.** *Let X be a complex non-singular projective variety, $f : \mathbb{C} \to X$ an holomorphic curve, $d > 0$ an integer, $\mathcal{L}$ a line sheaf on X, ω a global section of*

$$\mathcal{L}^\vee \otimes S^d \Omega^1_X,$$

and $\mathcal{A}$ an ample line sheaf on X. If $f^*\omega$ is not identically zero, then there exists a set $U \subseteq \mathbb{R}^+$ of finite Lebesgue measure such that for any $r \notin U$ we have

$$T_{\mathcal{L},f}(r) \leq O(\log T_{\mathcal{A},f}(r)) + o(\log r).$$

Proof of Theorem 3.2.10. Let $P \in \mathcal{M}[X]$ be a monic second degree polynomial, with some non-constant coefficient, which is not a square in $\mathcal{M}[X]$, and assume that there exists $a_1, a_2, \ldots, a_8 \in \mathbb{C}$ such that $P(a_i)$ is a square in $\mathcal{M}$ for each i, say

$$\sqrt{P(a_i)} = h_i \in \mathcal{M}.$$

Since P has some non-constant coefficient, some of the h_i is non-constant. By Lemma 3.8.1 we have that

$$h = [1 : h_1 : \cdots : h_8]$$

does not belong to a trivial line of $X_8(\mathcal{M})$, that is, the image of the non-constant holomorphic map $h : \mathbb{C} \to X_8(\mathbb{C})$ is not contained in the trivial lines.

Now take $\mathcal{L} = \mathcal{O}(1)$. Since $\mathcal{L}$ is the line sheaf associated to a hyperplane divisor on X_8, it is very ample. Note that

$$\mathcal{O}(1)^\vee \simeq \mathcal{O}(-1)$$

and consider the section ω_8 of

$$\mathcal{O}(-1) \otimes S^2 \Omega^1_{X_8}.$$

Taking

$$\mathcal{L} = \mathcal{A} = \mathcal{O}(1),$$

$f = h$, $d = 2$ and $\omega = \omega_8$ in Theorem 3.9.2 we conclude that $h^*\omega_8 = 0$ because h is non-constant. By Corollary 3.7.8, the image of h must be contained in the trivial lines, a contradiction. □

Chapter 4

Uniform Definability and Undecidability in Classes of Structures

This is joint work with Thanases Pheidas and Xavier Vidaux.

4.1 Introduction

It is well known that a system of Diophantine equations has a complex solution if and only if it has a solution modulo infinitely many primes (see [Nav]). Since there is an algorithm to solve the former problem, there is also an algorithm to decide whether an arbitrary system of diophantine equations has a solution in the finite field $\mathbb{F}_p$ for infinitely many primes p. In this work we show that the situation is completely different if we replace the fields $\mathbb{F}_p$ by rings of functions of positive characteristic and consider analogous diophantine problems. For example, we show that the following problems are undecidable: decide whether or not a system of diophantine equations together with conditions of the form "x is non constant", for some of the unknowns x, has a solution in $\mathbb{F}_p[z]$ for

1. some odd prime p,
2. all odd primes p,
3. infinitely many odd primes p,

4. all but possibly a finite number of odd primes p,

5. all primes p of the form $6k + 5$, etc.

Indeed we prove such very general *uniform* undecidability results for large classes of subrings of function fields of curves (of large enough characteristic) - for example, for the class of all polynomial rings of odd positive characteristic.

There seems to be rather few results of this kind in the bibliography, but there are several results on *asymptotic (un)decidability*: given a class of structures, to decide whether or not a given formula is true for all but finitely many of them. For example, in [CHr], Chatzidakis and Hrushovski prove that a certain class of differential fields, each of them separately having a decidable theory, has an asymptotic undecidable theory. On the other hand, Hrushovski [Hr] and Macintyre [Mac] (independently) show that the class of algebraically closed fields in positive characteristic, together with the Frobenius map, is asymptotically decidable. Other results of the same flavour can be found in [AxK12, AxK3, Ax, Rum].

In this work, we will be interested in positive existential theories, because of the obvious connection with Hilbert's tenth problem, but the general method that we develop is straightforward adaptable to decidability questions about full theories.

On the way, we define positive existentially the relation "y is a p^s-th power of x" in a class of algebraic function fields whose fields of constants are algebraic over $\mathbb{F}_p$, for p large enough with respect to the genus.

Hilbert's tenth problem (the tenth in the famous list that Hilbert gave at the International Conference of Mathematicians in Sorbonne, in 1900) was:

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 1971 when Y. Matijasevich, 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 foundational work of K. Goedel and A. Turing who laid the necessary foundations in Logic. Later various authors asked similar questions for rings other than the integers (starting with J. Denef and L. Lipshitz). One such question is the following: What if we replace the *integers* by *polynomials*, say in one

variable, with coefficients in a finite field $\mathbb{F}_q$, with $q = p^n$ elements, where p is the (prime) characteristic. The problem was answered by J. Denef in [De1] and [De2], negatively again. In the modern terminology of Logic the result is phrased *The positive existential theory of a ring $F[z]$ of polynomials of the variable z over a field F, in the language $\mathcal{L}_z = \{0, 1, +, \cdot, z\}$, is undecidable*. In this problem the considered polynomial equations are those with coefficients in the natural image of $\mathbb{Z}[z]$ in $F[z]$.

Later, a large number of similar results (mostly of a negative nature) were established. The general flavor of these results is: if in place of $\mathbb{Z}$ in Hilbert's tenth problem we substitute a global ring or field, such as a ring of polynomials or rational functions (or a finite extension), all the existing results are negative (the positive existential theory is undecidable); almost always in the language $\mathcal{L}_z$ or an extension of it by a finite list of symbols for certain elements of the structure. In contrast, in local domains, such as a field of p-adic numbers or power series, the results tend to be positive (decidable existential theory, even decidable first order theory). But there are many open problems, for example the question asked for $\mathbb{C}(z)$, the field of rational functions with complex coefficients (or coefficients in any algebraically closed field) and the field of formal power series over any reasonable field of positive characteristic (e.g. over a finite field).

In order to state our results, we need to introduce a few notation. All languages considered will be first order languages. Also, the word *class* will always refer to a non-empty class of structures over a common language.

Notation 4.1.1. *1. We consider* 0 *to be a natural number.*

2. All languages considered will be first order and equalitarian.

3. If $\mathcal{L}$ is a language, we will denote by $\mathcal{F}_\mathcal{L}$ (respectively $\mathcal{F}^{\mathrm{e}}_\mathcal{L}$, $\mathcal{F}^{\mathrm{pe}}_\mathcal{L}$) the set of (respectively existential, positive existential) $\mathcal{L}$-sentences, and if $\mathfrak{M}$ is an $\mathcal{L}$-structure $T_\mathcal{L}(\mathfrak{M})$ (respectively $T^{\mathrm{e}}_\mathcal{L}$, $T^{\mathrm{pe}}_\mathcal{L}$) will stand for the (respectively existential, positive existential) $\mathcal{L}$-theory of $\mathfrak{M}$.

4. If $\mathfrak{U}$ is an $\mathcal{L}$-structure and X is a subset of $\mathcal{L}$, we will denote by $\mathfrak{U}_X$ the $\mathcal{L} \setminus X$-structure in which we forget *the interpretation of the symbols of X. If $\mathcal{U}$ is a class of such $\mathcal{L}$-structures, we will denote by $\mathcal{U}_X$ the class of corresponding $\mathcal{L} \setminus X$-structures.*

5. If $\mathfrak{U}$ is an $\mathcal{L}$-structure and X is a set of symbols which are not in $\mathcal{L}$ and which have a given interpretation in $\mathfrak{U}$, we will denote by $\mathfrak{U}^X$ the

corresponding $\mathcal{L} \cup X$-structure. If $\mathcal{U}$ is a class of such $\mathcal{L}$-structures we will denote by $\mathcal{U}^X$ the corresponding class of $\mathcal{L} \cup X$-structures.

6. *All classes of structures are by default non-empty.*

7. *We define the following languages:*

   (a) $\mathcal{L}_A = \{0, 1, +, \cdot\}$ *is the language of rings;*

   (b) $\mathcal{L}_z = \mathcal{L}_A \cup \{z\}$, *where z is a symbol of constant;*

   (c) $\mathcal{L}_{z,\mathrm{ord}} = \mathcal{L}_z \cup \{\mathrm{ord}\}$, *where* ord *is a unary predicate symbol;*

   (d) $\mathcal{L}_T = \mathcal{L}_A \cup \{T\}$, *where T is a unary predicate symbol;*

   (e) $\mathcal{L}_T^* = \{0, 1, +, |, R, T\}$, *where $|$ and R are binary relation symbols;*

   (f) $\mathcal{L}^{*,+} = \{0, 1, +, R\}$.

   (g) $\mathcal{L}^* = \{0, 1, +, \mathrm{pos}, R\}$, *where* pos *is a unary relation symbol interpreted in $\mathbb{Z}$ as: "$\mathrm{pos}(x)$ if and only if x is non-negative". We will freely write $x \geq 0$ when working over this language.*

8. *For each prime p, consider the following equivalence relation $|_p$ over $\mathbb{Z}$:*

   $$x \mid_p y \text{ if and only if there exists } s \in \mathbb{Z} \text{ such that } y = \pm x p^s.$$

   We will refer to it as p-divisibility *and denote its restriction to the natural numbers by the same symbol.*

9. *Let $\mathfrak{D}_p$ be the $\mathcal{L}_T^*$-structure $(\mathbb{Z}; 0, 1, +, |, |_p, \mathbb{Z} \setminus \{-1, 0, 1\})$ and*

   $$\mathcal{D} = \{\mathfrak{D}_p \colon p \text{ is prime}\}.$$

10. *Let $\mathfrak{N}_p$ be the $\mathcal{L}^{*,+}$-structure $(\mathbb{N}; 0, 1, +, |_p)$ and*

    $$\mathcal{N} = \{\mathfrak{N}_p \colon p \text{ is prime}\}.$$

11. *Let $\mathfrak{Z}_p$ be the $\mathcal{L}^*$-structure $(\mathbb{Z}; 0, 1, +, \geq 0, |_p)$ and*

    $$\mathcal{Z} = \{\mathfrak{Z}_p \colon p \text{ is prime}\}.$$

12. *All function fields will be considered as structures over $\mathcal{L}_{z,\mathrm{ord}}$, where z is interpreted as a local parameter at a prime divisor $\mathfrak{p}$ of the field over its field of constants, and* $\mathrm{ord}(x)$ *will be interpreted as "the valuation of x at $\mathfrak{p}$ is non-negative". The symbol z will just be the variable z in the case of a rational function field $F(z)$, and in this case* $\mathrm{ord}(x)$ *will be interpreted as "the order of x at 0 is non-negative".*

13. *Any subring B of a rational function field $F(z)$, whose elements are regular at 0, will be considered as an $\mathcal{L}_z$-structure, where the symbol z is interpreted as the variable z, or, in the case that B is a ring of polynomials $F[z]$, it will also be considered as an $\mathcal{L}_T$-structure, where $T(x)$ will be interpreted as "x is non-constant".*

Definition 4.1.2. *Let $\mathcal{L}$ be a first order language, X be a non-empty proper subset of $\mathcal{L}$, and let $\mathcal{U}$ be a class of $\mathcal{L}$-structures. We will say that a symbol $\alpha \in X$ is* uniformly $\mathcal{L} \setminus X$-definable in $\mathcal{U}_X$ *(or in $\mathcal{U}$ if there is no ambiguity), if there exists an $\mathcal{L} \setminus X$-formula which defines the interpretation of α in each element of $\mathcal{U}$. If moreover the formula is existential, respectively positive existential, then we will say* uniformly existentially $\mathcal{L} \setminus X$-definable, *respectively* uniformly positive existentially $\mathcal{L} \setminus X$-definable ($\mathcal{L} \setminus X$-uped), *instead of just uniformly $\mathcal{L} \setminus X$-definable.*

If the symbol α has the same name 'x' across its interpretations in elements of $\mathcal{U}$, we will say that 'x' is uniformly $\mathcal{L} \setminus \{\alpha\}$-definable. Also we may say that the family of interpretations of α is uniformly definable in $\mathcal{U}$ instead of saying that α is.

Let us give a few trivial examples to illustrate the definition:

- With the language $\{R, \cdot\}$ and the class of all groups (where $R(x)$ is interpreted as "x is in the center" and the symbol $\cdot$ is interpreted as the group law), the formula $\forall y(xy = yx)$ uniformly $\{\cdot\}$-defines R in the class of all groups.

- With the language $\{\mathrm{e}, \cdot\}$ and the class of all groups (where e is interpreted as the identity element and $\cdot$ is interpreted as the group law), the formula $\exists y(x \cdot y = y)$ uniformly positive existentially $\{\cdot\}$-defines e in $\mathcal{U}$ over the language $\{\cdot\}$. So we shall say that the identity element is $\{\cdot\}$-uped in the class of all groups.

Another elementary example is given by the following lemma which we will prove in Section 4.2.

Lemma 4.1.3. *The relation $\neq$ is $\mathcal{L}_z$-uped in the class of all polynomial rings over fields, where z is interpreted as the variable.*

Moret-Bailly in [MB] gives very general criteria for positive existential (un)definability of the relation $\neq$ in rings.

As a non-trivial example, we prove the following proposition in Section 4.2.

Proposition 4.1.4. *Consider the language*

$$\mathcal{L} = \{0, +, \leq, R_2\}$$

and the structures

$$\mathfrak{C}_r = (\mathbb{Z}; 0, +, \leq, P_2^r)$$

where $P_2^r(x)$ stands for "x is a square and r does not divide x". The relation $\leq$ is $\{0, +, R_2\}$-uped in the class $\mathcal{U}$ of all structures $\mathfrak{C}_r$ with $r \geq 2$.

Let us give an example where we do not have uniformity. Consider the language $\mathcal{L} = \mathcal{L}_A \cup \{\alpha\}$, where α is a symbol of constants. Consider the $\mathcal{L}$-structures $\mathfrak{M}^k = (\mathbb{Z}; 0, 1, +, \cdot, k)$, where α is interpreted as k in each $\mathfrak{M}^k$. The formula $x = k$ defines k over $\mathcal{L}_A$ in each $\mathfrak{M}^k$, but there is no formula that uniformly $\mathcal{L}_A$-defines α in the set $\{\mathfrak{M}^k \colon k \in \mathbb{Z}\}$: such a formula $\varphi(x)$ would $\mathcal{L}_A$-define 2 in $\mathfrak{M}^2_{\{\alpha\}}$ and 3 in $\mathfrak{M}^3_{\{\alpha\}}$, which is absurd as these two structures are the same (the ring of integers). Note that with this example, it is enough to consider two distinct structures. Next proposition shows that one can have uniformity in each finite subfamily of a family of structures but not in the whole family. The proof will be given in Section 4.2.

Proposition 4.1.5. *Let $\mathcal{C}$ be the set of all finite fields $\mathbb{F}_p$ of prime characteristic p. The relation "to be a square" is $\{0, 1, +\}$-uped in any finite subfamily of $\mathcal{C}$, but there is no infinite subfamily of $\mathcal{C}$ where it is $\{0, 1, +\}$-uped. Hence, in particular, multiplication is not $\{0, 1, +\}$-uped in $\mathcal{C}$.*

A highly relevant result can be found in [CDM], where it is shown that there is no formula in the language of rings that defines $\mathbb{F}_q$ in $\mathbb{F}_{q^2}$ for all but finitely q (here q is any power of any prime).

We will now present one of the main tools that will allow us to obtain several uniform definitions. We first define a relation that has often been a key point to codify the integers in rings of functions of positive characteristic (see for example, by chronological order, [De2], [Ph1], [Ph2], [KR], [S1], [PZ1], [S2], [Ei] and [ES]).

Definition 4.1.6. *Let R_A be the equivalence relation defined on A by:*

$R_A(x,y)$ if and only if there exists $s \in \mathbb{N}$ such that either $y = x^{p^s}$ or $x = y^{p^s}$,

where p is the characteristic of A. For short we will say that "there exists $s \in \mathbb{Z}$ such that $y = x^{p^s}$.

In order to show that the above relation is uped in several classes of structures, we need to introduce Büchi's problem.

Let A be a commutative ring with unit and of positive characteristic $p > 2$. Let C be a subring of A. If $M \geq 3$, let us call an *M-term Büchi sequence for (A,C)* a sequence of M elements of A, not all in C, whose second difference of squares is the constant sequence (2).

Büchi's Problem for Rings of Characteristic $p > 2$:
BP(A,C,M) *Is it true that for all $N \geq M$, any N-term Büchi sequence (x_n) of (A,C) satisfies*

$$x_n^2 = (x+n)^{p^s+1}, \qquad n = 1, \ldots, N,$$

for some $x \in A$ and some non-negative integer s?

Notation 4.1.7. *If* **BP**(A,C,M) *has a positive answer for some M then we will denote by $M_0(A,C)$ the least such M.*

Note that $M_0(A,C)$, if it exists, is always at most the characteristic p of A (as if there exists an M greater than p then the Büchi sequence is p-periodic; see [PPV]).

We prove:

Theorem 4.1.8. *If* **BP**(A,C,M) *has a positive answer then there exists a positive existential $\mathcal{L}_A$-formula $\varphi_{M_0(A,C)}(x,y)$ with the following properties:*

1. *If $R_A(x,y)$ holds then A satisfies $\varphi_{M_0(A,C)}(x,y)$; and*

2. *if either xy or $x+y$ is not in C then: $R_A(x,y)$ holds if and only if A satisfies $\varphi_{M_0(A,C)}(x,y)$.*

In the cases relevant to this work, Büchi's problem is known to have a positive answer when (A, C, M) is

1. $(F[z], F, 14)$ for any field F of characteristic $p \geq 17$;
2. $(F(z), F, 18)$ for any field F of characteristic $p \geq 19$;
3. $(K, F, 312g + 169)$ for any function field of a curve K of genus g, with field of constants F, and of characteristic $p \geq 312g + 169$.

For a reference, see [PV1] and [PV2] for Items 1 and 2, and [SV] for Item 3.

In order to uniformly define the relation R_A in some classes of structures, we need to introduce the following definition.

Definition 4.1.9. *Let us call* Büchi class *any class $\mathcal{C}$ of pairs of rings such that there exists an integer M so that $\mathbf{BP}(A, C, M)$ has a positive answer for any (A, C) in the class. If $\mathcal{C}$ is a Büchi class, we denote by $M(\mathcal{C})$ the maximum of the set*

$$\{M_0(A, C) \colon (A, C) \text{ in the class } \mathcal{C}\}$$

and by $\bar{\mathcal{C}}$ the class of structures A such that (A, C) is in $\mathcal{C}$ for some C (so $\bar{\mathcal{C}}$ is the projection on the first component).

Note that $M(\mathcal{C})$ may be greater than some of the characteristics of the A in $\bar{\mathcal{C}}$ but this can happen for at most a finite number of characteristics.

Theorem 4.1.10. *Let $\mathcal{C}$ be a Büchi class such that C is a field for each pair (A, C) in the class. Suppose that for each pair (A, C) in the class $\mathcal{C}$, A is both an $\mathcal{L}_T$-structure and an $\mathcal{L}_z$-structure, where $T(x)$ is interpreted as "x is transcendental over C" and z is a symbol of constant interpreted by an element of A transcendental over C. There exist a positive existential $\mathcal{L}_T$-formula $\varphi^T_{\mathcal{C}}(x, y)$ and a positive existential $\mathcal{L}_z$-formula $\varphi^z_{\mathcal{C}}(x, y)$ with the following properties:*

1. *$\varphi^T_{\mathcal{C}}(x, y)$ uniformly defines R_A in $\bar{\mathcal{C}}$ (hence the collection of relations R_A is $\mathcal{L}_T$-uped in $\bar{\mathcal{C}}$); and*

2. *$\varphi^z_{\mathcal{C}}(x,y)$ uniformly defines R_A in $\bar{\mathcal{C}}$ (hence the collection of relations R_A is $\mathcal{L}_z$-uped in $\bar{\mathcal{C}}$).*

Here are some known Büchi classes where Theorem 4.1.10 applies:

1. Any non-empty subclass of the class of pairs $(F[z], F)$ where $F[z]$ is a polynomial ring over a field F of characteristic at least 17.
2. Any non-empty subclass of the class of pairs $(F(z), F)$ where $F(z)$ is a rational function field over a field F of characteristic at least 19.
3. Given an integer $g_0 \geq 0$, any non-empty subclass of the class of pairs (A, C) where A is a function field of a curve of genus $g \leq g_0$ and of positive characteristic at least $312g + 169$, with C the field of constants of A.

Theorem 4.1.10 is enough for our purposes but, for sake of completeness, we prove an analogous result for a relation weaker than R_A, but which can be applied in more general classes.

Theorem 4.1.11. *Let $\mathcal{C}$ be a Büchi class. For each pair (A, C) in the class $\mathcal{C}$, suppose that A is an $\mathcal{L}_T$-structure where $T(x)$ is interpreted as "$x \notin C$" and C has the following properties:*

- *for all $x \in A$, if $2x \in C$ then $x \in C$; and*
- *for all $x \in A$, if $x^2 \in C$ then $x \in C$.*

Let R^C_A be the relation defined by

$$R_A(x, y) \text{ holds, and either } x \text{ or } y \text{ is not in } C.$$

There exists a positive existential $\mathcal{L}_T$-formula $\psi^T_{\mathcal{C}}(x, y)$ with the following property: $\psi^T_{\mathcal{C}}(x, y)$ uniformly defines R^C_A in $\bar{\mathcal{C}}$ (hence the collection of relations R^C_A is $\mathcal{L}_T$-uped in $\bar{\mathcal{C}}$).

Notation 4.1.12. *We will denote by Ω any class of $\mathcal{L}_{z,\mathrm{ord},\neq}$-structures such that there exists a Büchi class $\mathcal{C}$ of pairs (K, C), where K is a function field of a curve of genus at most some fixed integer g_0 and C is the constant field of K, such that for each $\mathcal{L}_{z,\mathrm{ord},\neq}$-structure $\mathfrak{M}$ in Ω, there exists a pair (K, C) in $\mathcal{C}$ such that:*

- *the base set M of $\mathfrak{M}$ is a subring of K and contains C;*
- *M contains some local parameter ξ at some prime divisor $\mathfrak{p}$;*
- *z is interpreted as ξ;*
- $\mathrm{ord}(x)$ *is interpreted as "the order of x at $\mathfrak{p}$ is non-negative";*
- *$\neq$ is interpreted as usual.*

Note that in the above notation, since there can be more than one choice of ξ for a pair (K, C), several $\mathcal{L}_{z,\mathrm{ord},\neq}$-structures $\mathfrak{M}$ may correspond to the same pair (K, C) in the Büchi class. Note also that Theorem 4.1.10 applies to the class of pairs (A, C) where A ranges in Ω and is seen as a ring.

Next theorem gives uniform definitions in other types of classes of structures.

Theorem 4.1.13. *Multiplication is uniformly positive existentially*

1. *$\mathcal{L}^{*,+}$-definable in $\mathcal{N} = \{(\mathbb{N}; 0, 1, +, |_p) : p \text{ is prime}\}$;*
2. *$\mathcal{L}^{*}$-definable in $\mathcal{Z} = \{(\mathbb{Z}; 0, 1, +, \leq, |_p) : p \text{ is prime}\}$; and*
3. *$\mathcal{L}^{*}_{T}$-definable in $\mathcal{D} = \{(\mathbb{Z}; 0, 1, +, |, |_p, \mathbb{Z} \setminus \{-1, 0, 1\}) : p \text{ is prime}\}$.*

Before stating our main results, we need to introduce the following definition.

Definition 4.1.14. *Consider two languages $\mathcal{L}$ and $\mathcal{L}'$. Let $\mathfrak{M}$ be an $\mathcal{L}$-structure and $\mathcal{U}$ be a class of $\mathcal{L}'$-structures. Let $\mathcal{G}$ be a set of $\mathcal{L}$-sentences and $\mathcal{G}'$ a set of $\mathcal{L}'$-sentences. We will say that $(\mathcal{G}, \mathfrak{M})$ is* uniformly encodable *in $(\mathcal{G}', \mathcal{U})$ if there exists an algorithm $\mathcal{A}$ that, given a formula $F \in \mathcal{G}$, returns a formula $\mathcal{A}(F) \in \mathcal{G}'$ such that the following are equivalent:*

- *$\mathfrak{M}$ satisfies F.*
- *Any structure $\mathfrak{U}$ in $\mathcal{U}$ satisfies $\mathcal{A}(F)$.*
- *There exists a structure $\mathfrak{U}$ in $\mathcal{U}$ that satisfies $\mathcal{A}(F)$.*

Remark 4.1.15. *Let $\mathcal{A}$ be an algorithm that uniformly encodes a pair $(\mathcal{G}, \mathfrak{M})$ in a pair $(\mathcal{G}', \mathcal{U})$, where $\mathcal{G}$ is a set of sentences over a language $\mathcal{L}$ and $\mathcal{G}'$ is a set of sentences over a language $\mathcal{L}'$.*

1. *For any non-empty subset $\mathcal{G}_0$ of $\mathcal{G}$, the algorithm $\mathcal{A}$ uniformly encodes $(\mathcal{G}_0, \mathfrak{M})$ in $(\mathcal{G}', \mathcal{U})$.*

2. *For any set $\mathcal{G}'_0$ of $\mathcal{L}'$-sentences that contains $\mathcal{G}'$, the algorithm $\mathcal{A}$ uniformly encodes $(\mathcal{G}, \mathfrak{M})$ in $(\mathcal{G}'_0, \mathcal{U})$.*

3. *For any non-empty subclass $\mathcal{U}_0$ of $\mathcal{U}$, the algorithm $\mathcal{A}$ uniformly encodes $(\mathcal{G}, \mathfrak{M})$ in $(\mathcal{G}', \mathcal{U}_0)$.*

4. *For any language $\mathcal{L}'' = \mathcal{L}' \cup X$, with $\mathcal{L}' \cap X = \varnothing$, the algorithm $\mathcal{A}$ uniformly encodes $(\mathcal{G}, \mathfrak{M})$ in $(\mathcal{G}', \mathcal{U}^X)$, no matter the interpretation of the elements of X given in the structures $\mathfrak{U}^X$ of $\mathcal{U}^X$.*

5. *For any language $\mathcal{L}'' = \mathcal{L} \setminus X \neq \varnothing$, if the set of $\mathcal{L}''$-formulas $\mathcal{G}''$ which are in $\mathcal{G}$ is non-empty, then the algorithm $\mathcal{A}$ uniformly encodes $(\mathcal{G}'', \mathfrak{M}_X)$ in $(\mathcal{G}', \mathcal{U})$.*

Uniform encodability can be used to show very strong undecidability results in the following way (the proof will be given in Section 4.3).

Theorem 4.1.16. *Suppose that a pair $(\mathcal{G}, \mathfrak{M})$ is uniformly encodable in a pair $(\mathcal{G}', \mathcal{U})$ and that there is no algorithm to decide whether or not a formula F in $\mathcal{G}$ is true in $\mathfrak{M}$. Let $\mathcal{C}$ be a non-empty collection of non-empty subclasses of $\mathcal{U}$. There is no algorithm to solve the following problem:*

> ***(P)*** *Given $F \in \mathcal{G}'$, decide whether or not there exists a class $\mathcal{V}$ in the collection $\mathcal{C}$ such that every structure $\mathfrak{U}$ in $\mathcal{V}$ satisfies F.*

Theorem 4.1.17. *The pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{N})$ is uniformly encodable in*

1. *$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^*}, \mathcal{Z})$;*

2. *$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^{*,+}}, \mathcal{N})$; and*

3. *$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_{z,\mathrm{ord},\neq}}, \Omega)$ (where Ω is any class as defined in Notation 4.1.12).*

4. *$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}}, \Omega)$ with*

   (a) *$\mathcal{L} = \mathcal{L}_{z,\mathrm{ord}}$ if $\neq$ is $\mathcal{L}_{z,\mathrm{ord}}$-uped in Ω.*

   (b) *$\mathcal{L} = \mathcal{L}_{z,\neq}$ if* ord *is $\mathcal{L}_{z,\neq}$-uped in Ω.*

   (c) *$\mathcal{L} = \mathcal{L}_z$ if $\neq$ and* ord *are $\mathcal{L}_z$-uped in Ω.*

In the following corollary, we specify some classes Ω for which we do have uniform definition of $\neq$ or ord (for Item 1, we use Lemma 4.1.3).

Corollary 4.1.18. *The pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{N})$ is uniformly encodable in the pairs*

1. *$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_z}, \bar{\mathcal{C}})$, where $\mathcal{C}$ is any Büchi class of pairs (A, C) where C is a field and A is a polynomial ring over C (in particular for the class of all polynomial rings of characteristic at least 17).*

2. *$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_{z,\mathrm{ord}}}, \bar{\mathcal{C}})$, where $\mathcal{C}$ is any Büchi class of pairs (A, C) where C is a field and A is a rational function field over C (in particular for the class of all rational function fields of characteristic at least 19).*

3. *$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_{z,\mathrm{ord}}}, \bar{\mathcal{C}})$, where $\mathcal{C}$ is any Büchi class of pairs (A, C) where C is a field and A is a function field of a curve of genus at most some fixed integer g_0, with constant field C (in particular for the class of all such function fields of genus at most g_0 whose characteristic is at least $312g + 169$, where g is the genus of the function field).*

Theorem 4.1.19. *The pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{Z})$ is uniformly encodable in*

1. *$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^*}, \mathcal{Z})$;*

2. *$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^*_T}, \mathcal{D})$;*

3. *$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_T}, \mathcal{C})$, where $\mathcal{C}$ is the class of all polynomial rings over a field of odd positive characteristic, where $T(x)$ is interpreted in each structure as "x is non-constant".*

Actually, the proof of Item 3 works (with only notational changes) in a similar way to prove that the pair $(\mathcal{F}_{\mathcal{L}_A}, \mathbb{Z})$ is uniformly encodable in $(\mathcal{F}_{\mathcal{L}_A}, \mathcal{C})$, where $\mathcal{C}$ is the class of all polynomial rings over a field of odd positive characteristic.

We obtain the following corollary from Theorem 4.1.16 (choosing suitably the class $\mathcal{C}$ of subclasses of $\mathcal{U}$).

Corollary 4.1.20. *Let $\mathcal{L}$ and $\mathcal{U}$ be such that the conclusion of Theorems 4.1.17 or 4.1.19 hold and suppose that $\mathcal{U}$ is infinite. There is no algorithm to decide whether or not a positive existential $\mathcal{L}$-sentence is true for (for example):*

1. *some $\mathfrak{U}$ in $\mathcal{U}$ (this item does not require $\mathcal{U}$ to be infinite),*

2. *all* $\mathfrak{U}$ *in* $\mathcal{U}$,
3. *infinitely many* $\mathfrak{U}$ *in* $\mathcal{U}$,
4. *all but possibly finitely many* $\mathfrak{U}$ *in* $\mathcal{U}$,
5. *each structure in a given subclass of* $\mathcal{U}$.

4.2 Examples of (non-)uniform definitions

The proof of Lemma 4.1.3 is an easy adaptation of the proof of the analogous result over the integers (which we got from a talk by A. Shlapentokh).

Proof of Lemma 4.1.3. Consider the following positive existential $\mathcal{L}_z$-formula

$$\varphi_{\neq}(t)\colon \exists x, u, v((zu-1)((z+1)v-1) = tx).$$

We prove that $\varphi_{\neq}(t)$ is satisfied in a polynomial ring $F[z]$, where F is a field, if and only if t is distinct from 0. First note that it is clear that if the formula is satisfied then t is not 0 (since neither z nor $z+1$ is invertible).

Suppose that t is non-zero. Since $F[z]$ is a unique factorization domain, we can write t as t_0t_1 in such a way that z does not divide t_0 and $z+1$ does not divide t_1. By Bézout's identity, there exist polynomials u, x_u, v and x_v such that $zu + t_0x_u = 1$ and $(z+1)v + t_1x_v = 1$. Therefore, we have

$$(zu-1)((z+1)v-1) = t_0x_ut_1x_v = tx_ux_v,$$

hence we can choose $x = x_ux_v$ for the formula to be satisfied. □

Proof of Proposition 4.1.5. Let X be a non-empty finite set of prime numbers and let q be its maximum. The quantifier free $\{0,1,+\}$-formula

$$\bigvee_{i=0}^{q-1} x = i^2$$

is satisfied in $\mathbb{F}_p$ if and only if x is a square, for each p in X.

Suppose that $\varphi(x)$ is a positive existential $\{0,1,+\}$-formula that defines the relation "x is a square" in $\mathbb{F}_p$ for all primes p in an infinite set X. The formula $\varphi(x)$ is logically equivalent to a formula of the form

$$\exists y_1 \ldots \exists y_n \bigvee_{i=1}^{r} L_i(x, y_1, \ldots, y_n)$$

where each L_i is a formal system of linear equations. Hence, for each $p \in X$, the set of x such that $\varphi(x)$ is true in $\mathbb{F}_p$, namely, the set of squares in $\mathbb{F}_p$, is the union of the projections on the variable x of the zero locus H_i^p of each L_i. Each H_i^p is an affine linear subspace of $\mathbb{F}_p^{n+1}$ or the empty set. Since the projection K_i^p of each H_i^p on x is an affine linear subspace of $\mathbb{F}_p$, it is either the whole of $\mathbb{F}_p$, a point or the empty set. From now on assume that p is bigger than 2. Since there are $\frac{p+1}{2}$ squares in $\mathbb{F}_p$, none of the K_i^p can be the whole of $\mathbb{F}_p$ (as the union of the K_i^p is the set of squares in $\mathbb{F}_p$). Hence the number r of disjunctions in the formula φ is at least $\frac{p+1}{2}$, which is absurd. □

The rest of this section is dedicated to the proof of Proposition 4.1.4. If A is a set of non-negative integers, then we define

$$A(n) = |A \cap \{1, 2, \ldots, n\}|$$

and

$$\sigma(A) = \inf_{n>0} \frac{A(n)}{n}.$$

The function σ is known as the *Shnirel'man density*. If $n \geq 2$ and $A, A_1, \ldots, A_n$ are sets of positive integers, we will write

$$\sum_{i=1}^{n} A_i = \left\{ \sum_{i=1}^{n} \alpha_i \colon \alpha_i \in A_i \right\}$$

and nA is the sum of n copies of A.

The two following fundamental results on Shnirel'man density can be found in [Na, Chapter 11, Section 3].

Lemma 4.2.1. *[Na, Lemma 11.2] If A and B are sets of non-negative integers such that $0 \in A \cap B$, $\sigma(A) > \frac{1}{2}$ and $\sigma(B) > \frac{1}{2}$ then $A + B$ is the set of non-negative integers.*

Theorem 4.2.2. *[Na, Theorem 11.2] If $A_1, \ldots, A_t$ are sets of non-negative integers containing 0, then we have*

$$1 - \sigma\left(\sum_{i=1}^{t} A_i\right) \leq \prod_{i=1}^{t} (1 - \sigma(A_i)).$$

By a theorem of Linnik, given any set B of non-negative integers with $\sigma(B) > 0$, the set $A = \{x^2 \colon x \in B\}$ is a basis of finite order, that is, each positive integer is a (uniformly) bounded sum of elements in A. We want to show that the bound is the same for certain family of sets B.

Theorem 4.2.3. *Let $u \geq 2$ be an integer, and*

$$C(u) = \{n \in \mathbb{Z} \colon u \nmid n\}.$$

Each non-negative integer is the sum of at most 5940 squares of elements in $C(u)$.

Using this result (proven below), Proposition 4.1.4 follows easily:

Proof of Proposition 4.1.4. By Theorem 4.2.3, the following positive existential $\{0, +, R_2\}$-formula uniformly defines the relation $x \geq 0$ in the class of structures $\mathfrak{C}_r$ (which is enough to prove the result):

$$\phi(x) : \exists x_1, \ldots, x_{5940} \bigwedge_{i=1}^{5940} (R_2(x_i) \vee x_i = 0) \wedge x = \sum_{i=1}^{5940} x_i$$

where we recall that $R_2(x)$ is interpreted as "x is a square and r does not divide x" in $\mathfrak{C}_r$. □

We need two lemmas before we can prove Theorem 4.2.3.

Lemma 4.2.4. *Let d, k be positive integers, let*

$$A_i = \{z_i + 1, \ldots, z_i + k\}$$

for $1 \leq i \leq d$ be sets of k consecutive integers and let

$$B_i = \{z_i + 1, \ldots, z_i + k - 1\}$$

(take B_i empty if $k = 1$). Suppose that we have a set $U \subseteq \mathbb{R}^d$ satisfying the following:

(1) U is non-empty,

(2) U is convex,

(3) $\pi_i(U) = \pi_i(H^i_{z_i+1} \cap U)$ for $1 \leq i \leq d$, where $\pi_i : \mathbb{R}^d \to \mathbb{R}^{d-1}$ deletes the i-th coordinate and $H^i_x \subseteq \mathbb{R}^d$ is the hyperplane $x_i = x$.

Then we have

$$(k-1)^d|U \cap \prod_{i=1}^{d} A_i| \leq k^d|U \cap \prod_{i=1}^{d} B_i|.$$

Proof. We fix $k \geq 1$. Up to translation by the vector $(z_1, \ldots, z_d)$ we can assume $z_i = 0$ for each i, hence

$$A_i = A = \{1, \ldots, k\}$$

and

$$B_i = B = \{1, \ldots, k-1\}$$

for each i. Define

$$1_d = (1, \ldots, 1)$$

and observe that 1_d belongs to U (otherwise U would be empty by the hypothesis (3)). Let $a_d \geq 1$ be a real number such that

$$(1, \ldots, 1, a_d) \in U$$

(this is possible because $1_d \in U$) and such that, if

$$(1, \ldots, 1, l) \in U$$

for $l \in A$ then $a_d \geq l$ (this can be done because U is convex).

The proof goes by induction on d. Observe that for $d = 1$ the set U is just an interval containing 1, thus the desired inequality clearly holds. Assume that the result is true for $d = n-1 \geq 1$ and consider a set $U \subseteq \mathbb{R}^n$ satisfying the hypotheses. For the rest of the proof, the set H_x^n will be considered inside $\mathbb{R}^n$. It is easy to see that, for any $x \in [1, a_n]$ the set

$$U_x = \pi_n(U \cap H_x^n) \subseteq \mathbb{R}^{n-1}$$

satisfies the hypotheses of the Lemma with $d = n-1$ and $z = 0$, hence

$$(k-1)^{n-1}|A^{n-1} \cap U_x| \leq k^{n-1}|B^{n-1} \cap U_x|.$$

For $x \in A$ we have

$$\pi_n(H_x^n \cap A^n \cap U) = A^{n-1} \cap U_x$$

hence

$$|H_x^n \cap A^n \cap U| = |A^{n-1} \cap U_x|$$

and similarly for $x \in B$ we have

$$|H_x^n \cap B^n \cap U| = |B^{n-1} \cap U_x|.$$

In particular, for $x \in B$ (hence also $x \in A$), we have

$$(k-1)^{n-1}|H_x^n \cap A^n \cap U| \leq k^{n-1}|H_x^n \cap B^n \cap U|. \tag{4.1}$$

The hypothesis (2) and (3) on U implies

$$\pi_n \left(H_k^n \cap A^n \cap U\right) \times A \subseteq A^n \cap U$$

which gives us

$$|H_k^n \cap A^n \cap U| \leq \frac{1}{k}|A^n \cap U|. \tag{4.2}$$

Using the Inequalities (4.1) and (4.2) we obtain:

$$\begin{aligned}
(k-1)^n|A^n \cap U| &= (k-1)\sum_{x\in A}(k-1)^{n-1}|H_x^n \cap A^n \cap U| \\
&= (k-1)^n|H_k^n \cap A^n \cap U| + \\
&\quad (k-1)\sum_{x\in B}(k-1)^{n-1}|H_x^n \cap A^n \cap U| \\
&\leq (k-1)^n\frac{1}{k}|A^n \cap U| + (k-1)\sum_{x\in B}k^{n-1}|H_x^n \cap B^n \cap U| \\
&= (k-1)^n\frac{1}{k}|A^n \cap U| + (k-1)k^{n-1}|B^n \cap U|
\end{aligned}$$

hence

$$(k(k-1)^n - (k-1)^n)|A^n \cap U| \leq (k-1)k^n|B^n \cap U|$$

and we obtain finally

$$(k-1)^n|A^n \cap U| \leq k^n|B^n \cap U|.$$

□

Let d and k be positive integers, and r a positive real number. We let

$$\begin{aligned}
L_d(r) &= \{v = (v_1, \ldots, v_d) \in \mathbb{Z}^d \colon \|v\|_2 \leq r, v_i > 0 \text{ for } 1 \leq i \leq d\} \\
L_{d,k}(r) &= \{v = (v_1, \ldots, v_d) \in \mathbb{Z}^d \colon \|v\|_2 \leq r, v_i > 0, k \nmid v_i \text{ for } 1 \leq i \leq d\}.
\end{aligned}$$

Lemma 4.2.5. *We have*

$$k^d|L_{d,k}(r)| \geq (k-1)^d|L_d(r)|.$$

Proof. Let $U = D(0,r)$ be the d-dimensional closed euclidean ball of radius r. Take integers $z_i \geq 0$ congruent to 0 modulo k for $1 \leq i \leq d$ such that

$$(z_1+1,\ldots,z_d+1) \in U,$$

(if this is not possible - for r being too small - then the conclusion follows). Write $z = (z_1,\ldots,z_d)$ and define the sets $A_i = A_i(z)$ and $B_i = B_i(z)$ as in Lemma 4.2.4. It is clear that, as z ranges over all the possible choices then the sets

$$U \cap \prod_{i=1}^{d} A_i(z)$$

form a partition of $L_d(r)$ and the sets

$$U \cap \prod_{i=1}^{d} B_i(z)$$

form a partition of $L_{d,k}(r)$. For each fixed z, let

$$U_z = U \cap \{(x_1,\ldots,x_d)\colon x_i \geq z_i \text{ for each } i\}.$$

Note that

$$\left|U \cap \prod_{i=1}^{d} A_i\right| = \left|U_z \cap \prod_{i=1}^{d} A_i\right| \quad \text{and} \quad \left|U \cap \prod_{i=1}^{d} B_i\right| = \left|U_z \cap \prod_{i=1}^{d} B_i\right|$$

and note also that the hypothesis in Lemma 4.2.4 are satisfied for U_z, $A_i(z)$ and $B_i(z)$. The result follows. □

Proof of Theorem 4.2.3. Let $r(n)$ be the number of ordered 6-tuples of integers $(x_1,\ldots,x_6)$ such that

$$n = \sum x_i^2,$$

and let $r'(n)$ be the number of ordered 6-tuples of integers having their non-zero coordinates in $C(u)$ and satisfying the same condition. Write

$$R(n) = \sum_{k=0}^{n} r(k) \quad \text{and} \quad R'(n) = \sum_{k=0}^{n} r'(k).$$

Observe that $R(n)$ is the number of integer points in the 6-dimensional closed euclidean ball $B(0, \sqrt{n})$ of radius $\sqrt{n}$.

If $z \in \mathbb{R}^6$ define the *box centered at* z as the closed ball of radius $1/2$ in the ∞-norm centered at z and write it B_z. Observe that, if V is a set of N integer points in $\mathbb{R}^6$, then

$$N = \mathrm{Vol}\left(\bigcup_{z \in V} B_z\right).$$

Given $n > 0$ define

$$I(n) = \mathbb{Z}^6 \cap B(0, \sqrt{n})$$

and

$$I'(n) = \{v \in I_n \colon u \text{ does not divide the nonzero coordinates of } v\}$$

hence we have

$$R(n) = |I(n)| = \mathrm{Vol}\left(\bigcup_{z \in I(n)} B_z\right)$$

and

$$R'(n) = |I'(n)| = \mathrm{Vol}\left(\bigcup_{z \in I'(n)} B_z\right)$$

Moreover, decomposing $I(n)$ and $I'(n)$ in lower dimensional parts we have

$$R(n) = 1 + \sum_{d=1}^{6} 2^d \binom{6}{d} |L_d(\sqrt{n})|$$

and

$$R'(n) = 1 + \sum_{d=1}^{6} 2^d \binom{6}{d} |L_{d,u}(\sqrt{n})|,$$

where $\binom{6}{d}$ counts the number of non-zero components and 2^d the distribution

of the signs. Hence, by Lemma 4.2.5 we get

$$\begin{aligned} R'(n) &= 1 + \sum_{d=1}^{6} 2^d \binom{6}{d} |L_{d,u}(\sqrt{n})| \\ &\geq 1 + \sum_{d=1}^{6} \left(\frac{u-1}{u}\right)^d 2^d \binom{6}{d} |L_d(\sqrt{n})| \\ &\geq \left(\frac{u-1}{u}\right)^6 R(n). \end{aligned}$$

We have

$$B\left(0, \sqrt{n} - \frac{\sqrt{6}}{2}\right) \subseteq \bigcup_{z \in I(n)} B_z \tag{4.3}$$

since if

$$||v||_2 \leq \sqrt{n} - \frac{\sqrt{6}}{2}$$

then the nearest lattice point to v is at a distance at most $\sqrt{6}/2$. Therefore, we have

$$R(n) \geq \mathrm{Vol}\left(B\left(0, \sqrt{n} - \frac{\sqrt{6}}{2}\right)\right) = \frac{\pi^3}{6}\left(\sqrt{n} - \frac{\sqrt{6}}{2}\right)^6$$

which gives a lower bound that will allow us to conclude.

$$R'(n) \geq \left(\frac{u-1}{u}\right)^6 \frac{\pi^3}{6}\left(\sqrt{n} - \frac{\sqrt{6}}{2}\right)^6.$$

Let us now look for an upper bound. Given $n \geq 1$, let $m(n)$ be the number of integers k in $\{0, 1, \ldots, n\}$ satisfying $r'(k) = 0$ and write $X(n)$ for the set of these integers. Note that

- $r'(0) = 1 \neq 0$,
- for $n > 0$ we have $r(n) < 40n^2$ (see [Na, Theorem 14.6]) and
- $r'(n) \leq r(n)$.

Therefore, we have the following upper bound for $n \geq 1$:

$$\begin{aligned} R'(n) &\leq 1 + \sum_{\substack{1 \leq k \leq n \\ k \notin X(n)}} r(k) \\ &< 1 + 40 \sum_{\substack{1 \leq k \leq n \\ k \notin X(n)}} k^2 \\ &\leq 1 + 40 \sum_{k=m(n)+1}^{n} k^2 \\ &= 1 + 40 \left(\frac{2n^3 + 3n^2 + n}{6} - \frac{2m(n)^3 + 3m(n)^2 + m(n)}{6} \right) \end{aligned}$$

Set

$$S = \{x^2 \colon x \in C(u)\} \cup \{0\}$$

and $A = 6S$. Since $m(n) = n - A(n)$, we use for $n \geq 1$ the upper and lower bounds obtained for $R'(n)$ to get

$$40 \left(\frac{2n^3 + 3n^2 + n}{6} - \frac{2(n - A(n))^3 + 3(n - A(n))^2 + n - A(n)}{6} \right) + 1 > \left(\frac{u-1}{u} \right)^6 \frac{\pi^3}{6} (\sqrt{n} - \sqrt{6}/2)^6.$$

Working out the left hand side one obtains

$$\frac{40}{3} A(n)^3 - 20(2n+1)A(n)^2 + \frac{20(6n^2 + 6n + 1)}{3} A(n) + 1 > \left(\frac{u-1}{u} \right)^6 \frac{\pi^3}{6} (\sqrt{n} - \sqrt{6}/2)^6.$$

Let σ_n be such that $A(n) = \sigma_n n$. Note that $0 < \sigma_n \leq 1$ (recall that $n \geq 1$ and $1 \in A$). Since $u \geq 2$ we have

$$\left(\frac{u-1}{u} \right)^6 \frac{\pi^3}{6} > 0.08,$$

hence for $n > 3$

$$\frac{40}{3} \sigma_n (\sigma_n^2 - 3\sigma_n + 3) n^3 + 20\sigma_n (2 - \sigma_n) n^2 + \frac{20\sigma_n}{3} n + 1 > 0.08 \left(\sqrt{n} - \frac{\sqrt{6}}{2} \right)^6. \tag{4.4}$$

If for some $n \geq 500$ we have $\sigma_n \leq 0.0014$ then the above inequality and elementary calculus gives a contradiction. Hence $\sigma_n > 0.0014$ for each $n \geq 500$. On the other hand, as $1 \in A$ we have

$$\sigma_n \geq \frac{1}{499} > 0.0014$$

for $n = 1, 2, \ldots, 499$. Note that these bounds are far from being optimal, but they are enough for our purposes.

This proves that $\sigma_n > 0.0014$ for each $n \geq 1$. Therefore we have $\sigma(A) \geq 0.0014$ and Theorem 4.2.2 implies

$$\sigma(495A) \geq 1 - (1 - 0.0014)^{495} > 0.5.$$

By Lemma 4.2.1,

$$5940S = 990A = 2(495A)$$

is the set of non-negative integers. □

4.3 Uniform encodings

4.3.1 Proof of Theorem 4.1.16 and Corollary 4.1.20

Proof of Theorem 4.1.16. Suppose that under the hypothesis of the theorem there exists an algorithm $\mathcal{A}$ to solve Problem (P), and let $\mathcal{B}$ be the algorithm that uniformly encodes $(\mathcal{G}, \mathfrak{M})$ in $(\mathcal{G}', \mathcal{U})$. Let us show that the algorithm obtained by first applying $\mathcal{B}$ and then $\mathcal{A}$ decides whether or not a formula in $\mathcal{G}$ is satisfied by $\mathfrak{M}$ (which is absurd). Let F be a formula in $\mathcal{G}$ and apply $\mathcal{A}$ to the output G of F after applying $\mathcal{B}$.

- if the answer is YES then there exists a non-empty class $\mathcal{V}$ in the collection $\mathcal{C}$ such that every structure $\mathfrak{U}$ in $\mathcal{V}$ satisfies G. In particular, there exists at least one structure in $\mathcal{U}$ satisfying G. Therefore, $\mathfrak{M}$ satisfies F (by definition of uniform encodability).

- if the answer is NO then for each class $\mathcal{V}$ in the non-empty collection $\mathcal{C}$, there exists at least one structure $\mathfrak{U}$ in $\mathcal{V}$ not satisfying G. In particular, there exists at least one structure in $\mathcal{U}$ not satisfying G. Therefore, $\mathfrak{M}$ does not satisfy F (by definition of uniform encodability).

□

Proof of Corollary 4.1.20. We list by item the collection $\mathcal{C}$ needed to apply Theorem 4.1.16. The collection $\mathcal{C}$ consists respectively of:

1. all classes containing exactly one structure in $\mathcal{U}$;
2. the class $\mathcal{U}$
3. all infinite subclasses of $\mathcal{U}$,
4. all cofinite subclasses of $\mathcal{U}$,
5. the given subclass of $\mathcal{U}$.

□

4.3.2 Techniques for uniform encodings

Following Cori and Lascar [CL] we recall the following notation and definitions.

Notation 4.3.1. *1. If $\mathfrak{U}$ is an $\mathcal{L}$-structure, then for each symbol α of $\mathcal{L}$, we will write $\alpha^{\mathfrak{U}}$ for the interpretation of α in $\mathfrak{U}$.*

2. Let $f\colon \mathfrak{U} \to \mathfrak{W}$ be a morphism of $\mathcal{L}$-structures. We will say that f is an $\mathcal{L}$-monomorphism *if for each relation symbol R we have: for all $x_1, \ldots, x_n \in \mathfrak{U}$*

$$R^{\mathfrak{U}}(x_1, \ldots, x_n) \text{ holds if and only if } R^{\mathfrak{W}}(f(x_1), \ldots, f(x_n)) \text{ holds.}$$

3. An $\mathcal{L}$-isomorphism is an $\mathcal{L}$-monomorphism which is onto.

Note that sometimes $\mathcal{L}$-monomorphisms are called $\mathcal{L}$-embeddings.

Definition 4.3.2. *Let $\mathfrak{U}$ be an $\mathcal{L}$-structure and $\mathcal{L}'$ be a language. Suppose that there exists a bijection $f\colon \mathcal{L} \to \mathcal{L}'$ which sends symbols of constants to symbols of constants, and for each natural number $n \geq 1$, symbols of n-ary relations to symbols of n-ary relations, and symbols of n-ary functions to symbols of n-ary functions. Let $\mathfrak{U}'$ be the $\mathcal{L}'$-structure with same base set as $\mathfrak{U}$ and where each symbol $f(\alpha)$ from $\mathcal{L}'$ is interpreted by $\alpha^{\mathfrak{U}}$. Given $\mathfrak{U}$ and $f\colon \mathcal{L} \to \mathcal{L}'$ as above, we will refer to $\mathfrak{U}'$ as to the $(\mathfrak{U}, f)$-induced $\mathcal{L}'$-structure. Moreover, in this context, we will denote by $\mathcal{A}_{\mathcal{L}}^{\mathcal{L}'}$ the algorithm that transforms a formula over $\mathcal{L}$ into a formula over $\mathcal{L}'$ (simply using the bijection f). Note that for every formula F over $\mathcal{L}$, we have: $\mathfrak{U}$ satisfies F if and only if $\mathfrak{U}'$ satisfies $\mathcal{A}_{\mathcal{L}}^{\mathcal{L}'}(F)$.*

Proposition 4.3.3. *Let $\alpha \in \mathcal{L}$ be uniformly $\mathcal{L} \setminus X$-definable in a class $\mathcal{U}$ of $\mathcal{L}$-structures. There exists an algorithm $\mathcal{A}_X^\alpha$ that, given an $\mathcal{L}$-sentence F, returns an $\mathcal{L} \setminus X$-sentence $\mathcal{A}_X^\alpha(F)$ such that $\mathfrak{U}$ satisfies F if and only if $\mathfrak{U}_X$ satisfies $\mathcal{A}_X^\alpha(F)$ for all structures $\mathfrak{U} \in \mathcal{U}$. Moreover, if α is (respectively, positive) existentially definable and F is (respectively, positive) existential then $\mathcal{A}_X^\alpha(F)$ is (respectively, positive) existential.*

Proof. In each $\mathcal{L}$-sentence F, replace α by the formula that defines it uniformly. □

Notation 4.3.4. *1. If $\mathcal{A}$ and $\mathcal{B}$ are two algorithms such that the set of outputs of $\mathcal{B}$ is included in the set of inputs of $\mathcal{A}$, we will denote by $\mathcal{A} \circ \mathcal{B}$ the algorithm that first applies $\mathcal{B}$ and then $\mathcal{A}$.*

2. Let $\alpha_1, \ldots, \alpha_n \subset \mathcal{L}$ be uniformly $\mathcal{L} \setminus X$-definable in a class $\mathcal{U}$ of $\mathcal{L}$-structures. We will denote by

$$\mathcal{A}_X^{\alpha_1,\ldots,\alpha_n}$$

the algorithm $\mathcal{A}_X^{\alpha_1} \circ \cdots \circ \mathcal{A}_X^{\alpha_n}$.

Proposition 4.3.5. *Let $\mathcal{G}$, $\mathcal{G}'$ and $\mathcal{G}''$ be sets of sentences over $\mathcal{L}$, $\mathcal{L}'$ and $\mathcal{L}''$ respectively. Let $\mathfrak{M}$ be an $\mathcal{L}$-structure, $\mathcal{U}$ a class of $\mathcal{L}'$-structures and $\mathcal{V}$ a class of $\mathcal{L}''$-structures. Let $(\mathcal{V}_\mathfrak{U})$ be a partition of $\mathcal{V}$ indexed by a subclass $\mathcal{U}_{\text{ind}}$ of $\mathcal{U}$. If*

- *$(\mathcal{G}, \mathfrak{M})$ is uniformly encodable in $(\mathcal{G}', \mathcal{U})$ by an algorithm $\mathcal{A}$; and*
- *there exists an algorithm $\mathcal{B}$ such that for each $\mathfrak{U}$ in $\mathcal{U}_{\text{ind}}$, the pair $(\mathcal{G}', \mathfrak{U})$ is uniformly encodable in $(\mathcal{G}'', \mathcal{V}_\mathfrak{U})$ by $\mathcal{B}$*

then $(\mathcal{G}, \mathfrak{M})$ is uniformly encodable in $(\mathcal{G}'', \mathcal{V})$ by the algorithm $\mathcal{B} \circ \mathcal{A}$.

Proof. We may visualize the statement schematically as

$$(\mathcal{G}, \mathfrak{M}) \xrightarrow{\mathcal{A}} (\mathcal{G}', \mathcal{U}) \supseteq (\mathcal{G}', \mathcal{U}_{\text{ind}}) \xrightarrow{\mathcal{B}} \left(\mathcal{G}'', \bigcup_{\mathfrak{U} \in \mathcal{U}} \mathcal{V}_\mathfrak{U}\right) = (\mathcal{G}'', \mathcal{V})$$

and observe that by Item 3 of Remark 4.1.15, $\mathcal{A}$ uniformly encodes $(\mathcal{G}, \mathfrak{M})$ in $(\mathcal{G}', \mathcal{U}_{\text{ind}})$. Let F be an $\mathcal{L}$-sentence.

Let us prove that if $\mathfrak{M}$ satisfies F then each $\mathfrak{V}$ in $\mathcal{V}$ satisfies $\mathcal{B}(\mathcal{A}(F))$. Since $\mathfrak{V}$ is in $\mathcal{V}$, it is in some $\mathcal{V}_{\mathfrak{U}}$, for some $\mathfrak{U}$ in $\mathcal{U}_{\text{ind}}$. Since $\mathfrak{M}$ satisfies F and $(\mathcal{G}, \mathfrak{M})$ is uniformly encodable in $(\mathcal{G}', \mathcal{U})$ by $\mathcal{A}$, $\mathfrak{U}$ satisfies $\mathcal{A}(F)$, and since $(\mathcal{G}', \mathfrak{U})$ is uniformly encodable in $(\mathcal{G}'', \mathcal{V}_{\mathfrak{U}})$ by $\mathcal{B}$, $\mathfrak{V}$ satisfies $\mathcal{B}(\mathcal{A}(F))$.

Let us prove that if $\mathfrak{V}$ satisfies $\mathcal{B}(\mathcal{A}(F))$ for some $\mathfrak{V}$ in $\mathcal{V}$ then $\mathfrak{M}$ satisfies F. Let $\mathfrak{U}$ in $\mathcal{U}$ be such that $\mathfrak{V}$ is in $\mathcal{V}_{\mathfrak{U}}$. Since $\mathfrak{V}$ satisfies $\mathcal{B}(\mathcal{A}(F))$, also $\mathfrak{U}$ satisfies $\mathcal{A}(F)$, hence $\mathfrak{M}$ satisfies F. □

We see from the proof that the above proposition actually requires only a covering of $\mathcal{V}$ instead of a partition.

We now describe the general strategy that we will use several times in order to uniformly encode the natural numbers in classes of structures. Depending on the class in which we want to encode we will sometimes need two steps.

One step encoding process. Let $\mathfrak{M}$ be a $\bar{\mathcal{L}}$-structure. In order to prove that a pair $(\mathcal{F}^{\text{pe}}_{\bar{\mathcal{L}}}, \mathfrak{M})$ is uniformly encodable in a pair $(\mathcal{F}^{\text{pe}}_{\mathcal{L}}, \mathcal{U})$ we will enlarge the language $\mathcal{L}$ by a set of symbols $X = \{\alpha_1, \ldots, \alpha_n\}$ and consider an interpretation of each element of X in each $\mathfrak{U} \in \mathcal{U}$ so that

1. it is easy to prove that $(\mathcal{F}^{\text{pe}}_{\bar{\mathcal{L}}}, \mathfrak{M})$ is uniformly encodable in $(\mathcal{F}^{\text{pe}}_{\mathcal{L}\cup X}, \mathcal{U}^X)$, say by an algorithm $\mathcal{A}$; and

2. each α in X is uniformly positive existentially $\mathcal{L}$-definable in $\mathcal{U}$.

From Item 2 we can apply Proposition 4.3.3, and we will then be able to conclude by using Item 2 of Remark 4.1.15 since

$$\mathcal{A}_X^{\alpha_1,\ldots,\alpha_n}(\mathcal{F}^{\text{pe}}_{\mathcal{L}\cup X})$$

is included in $\mathcal{F}^{\text{pe}}_{\mathcal{L}}$. Schematically, we perform (with some obvious abuses of notation):

$$(\mathcal{F}^{\text{pe}}_{\bar{\mathcal{L}}}, \mathfrak{M}) \xrightarrow{\mathcal{A}} (\mathcal{F}^{\text{pe}}_{\mathcal{L}\cup X}, \mathcal{U}^X) \xrightarrow{\mathcal{A}_X^{\alpha_1,\ldots,\alpha_n}} (\mathcal{A}_X^{\alpha_1,\ldots,\alpha_n}(\mathcal{F}^{\text{pe}}_{\mathcal{L}}), \mathcal{U}) \subseteq (\mathcal{F}^{\text{pe}}_{\mathcal{L}}, \mathcal{U})$$

and we deduce that the algorithm $\mathcal{A}_0 = \mathcal{A}_X^{\alpha_1,\ldots,\alpha_n} \circ \mathcal{A}$ uniformly encodes $(\mathcal{F}^{\text{pe}}_{\bar{\mathcal{L}}}, \mathfrak{M})$ in $(\mathcal{F}^{\text{pe}}_{\mathcal{L}}, \mathcal{U})$.

Two steps encoding process. Let $\mathfrak{M}$ be a $\bar{\mathcal{L}}$-structure. Suppose that we have an algorithm $\mathcal{A}_0$ given by the "one step encoding process" to uniformly

encode $(\mathcal{F}^{\mathrm{pe}}_{\bar{\mathcal{L}}}, \mathfrak{M})$ in a pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}}, \mathcal{U})$ and that we want to encode it in another pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}'}, \mathcal{V})$, for some class $\mathcal{V}$ of $\mathcal{L}'$-structures. Assume that we can find a partition $(\mathcal{V}_{\mathfrak{U}})$ of $\mathcal{V}$ indexed by a subclass $\mathcal{U}_{\mathrm{ind}}$ of $\mathcal{U}$ (note that by Item 1 of Remark 4.1.15, $\mathcal{A}_0$ uniformly encodes $(\mathcal{F}^{\mathrm{pe}}_{\bar{\mathcal{L}}}, \mathfrak{M})$ in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}}, \mathcal{U}_{\mathrm{ind}})$). In order to apply Proposition 4.3.5, we need to find an algorithm $\mathcal{B}$ such that for each $\mathfrak{U} \in \mathcal{U}_{\mathrm{ind}}$, $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}}, \mathfrak{U})$ is uniformly encodable in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}'}, \mathcal{V}_{\mathfrak{U}})$ by $\mathcal{B}$. We then need to enlarge the language $\mathcal{L}'$ by a set of symbols $Y = \{\beta_1, \ldots, \beta_n\}$ and consider an interpretation of each element of Y in each $\mathfrak{V} \in \mathcal{V}$ so that we can easily find an algorithm $\mathcal{B}'$ such that

1. for each $\mathfrak{U} \in \mathcal{U}_{\mathrm{ind}}$, $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}}, \mathfrak{U})$ is uniformly encodable in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}'\cup Y}, \mathcal{V}_{\mathfrak{U}})$ by $\mathcal{B}'$; and
2. each β in Y is uniformly positive existentially $\mathcal{L}'$-definable in $\mathcal{V}$.

At this point, the algorithm $\mathcal{B}$ is the composition

$$\mathcal{A}_Y^{\beta_1,\ldots,\beta_n} \circ \mathcal{B}'.$$

We will then be able to conclude using Item 2 of Remark 4.1.15 since

$$\mathcal{A}_Y^{\beta_1,\ldots,\beta_n}(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}'\cup Y})$$

is included in $\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}'}$. So the composition $\mathcal{B} \circ \mathcal{A}_0$ uniformly encodes $(\mathcal{F}^{\mathrm{pe}}_{\bar{\mathcal{L}}}, \mathfrak{M})$ in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}'}, \mathcal{V})$. Schematically we obtain:

$$(\mathcal{F}^{\mathrm{pe}}_{\bar{\mathcal{L}}}, \mathfrak{M}) \xrightarrow{\mathcal{A}_0} (\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}}, \mathcal{U}) \supseteq (\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}}, \mathcal{U}_{\mathrm{ind}})$$

$$\xrightarrow{\mathcal{B}'} \left(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}'\cup Y}, \bigcup_{\mathcal{U}_{\mathrm{ind}}} \mathcal{V}_{\mathfrak{U}}^{Y}\right) \xrightarrow{\mathcal{A}_Y^{\beta_1,\ldots,\beta_n}} (\mathcal{A}_Y^{\beta_1,\ldots,\beta_n}(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}'\cup Y}), \mathcal{V}) \subseteq (\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}'}, \mathcal{V})$$

and we deduce that the algorithm

$$\mathcal{A}_Y^{\beta_1,\ldots,\beta_n} \circ \mathcal{B}' \circ \mathcal{A}_0$$

uniformly encodes $(\mathcal{F}^{\mathrm{pe}}_{\bar{\mathcal{L}}}, \mathfrak{M})$ in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}'}, \mathcal{V})$.

In order to find the algorithm $\mathcal{B}'$ in the above process, we will need the following lemmas. They are certainly well known, but we decided to include them as we could not find a reference with the precise statements we needed. Let us introduce first some notation.

Notation 4.3.6. *Given a map $f\colon X \to Y$, we will denote by*

- $\sim_f$ *the equivalence relation on X defined by: $a \sim_f b$ if and only if $f(a) = f(b)$;*
- X_f *the quotient set $\frac{X}{\sim_f}$;*
- π_f *the canonical projection*

$$\pi_f\colon X \to X_f;$$

- $\bar{f}$ *the unique map*

$$\bar{f}\colon X_f \to Y$$

such that $\bar{f} \circ \pi_f = f$; and

- *if R is an n-ary relation on X then R_f will denote the n-ary relation on X_f defined by: $R_f(\pi_f(x_1), \ldots, \pi(x_n))$ if and only if there exist $u_1 \in \pi_f(x_1)$, $\ldots$, $u_n \in \pi_f(x_n)$ such that $R(u_1, \ldots, u_n)$.*

Lemma 4.3.7. *Let X and Y be sets together with n-ary relations R on X and S on Y. Let $f\colon X \to Y$ be a function. If the function f satisfies:*

1. *if $R(x_1, \ldots, x_n)$ holds then $S(f(x_1), \ldots, f(x_n))$ and*
2. *if $S(f(x_1), \ldots, f(x_n))$ holds then $R_f(\pi_f(x_1), \ldots, \pi_f(x_n))$,*

then the relation R_f satisfies:

$$R_f(\bar{x}_1, \ldots, \bar{x}_n) \text{ holds if and only if } S(\bar{f}(\bar{x}_1), \ldots, \bar{f}(\bar{x}_n)) \text{ holds}$$

for all $\bar{x}_1, \ldots, \bar{x}_n \in X_f$.

Proof. We need only to prove the implication from left to right. Let

$$\bar{x}_1, \ldots, \bar{x}_n \in X_f$$

and suppose that

$$R_f(\bar{x}_1, \ldots, \bar{x}_n)$$

holds. By definition of R_f, there exist

$$u_1 \in \bar{x}_1, \ \ldots, \ u_n \in \bar{x}_n$$

such that

$$R(u_1, \ldots, u_n)$$

holds. By Condition 1,

$$S(f(u_1), \ldots, f(u_n))$$

holds, and since $f = \bar{f} \circ \pi$,

$$S(\bar{f}(\bar{u}_1), \ldots, \bar{f}(\bar{u}_n))$$

holds, hence also

$$S(\bar{f}(\bar{x}_1), \ldots, \bar{f}(\bar{x}_n))$$

holds. □

Definition 4.3.8. *Let $f \colon \mathfrak{U} \to \mathfrak{W}$ be a morphism of structures over a language $\mathcal{L}$. We will say that f is* relation-onto *if for every relation symbol R of $\mathcal{L}$ we have: for all $x_1, \ldots, x_n \in \mathfrak{U}$, if $\mathfrak{W}$ satisfies $R(f(x_1), \ldots, f(x_n))$ then there exist $u_1 \sim_f x_1$, …, $u_n \sim_f x_n$ such that $\mathfrak{U}$ satisfies $R(u_1, \ldots, u_n)$.*

Note that the condition of being relation-onto does not need to be checked for the equality (as it is trivially satisfied).

Definition 4.3.9. *Given a morphism of $\mathcal{L}$-structures $f \colon \mathfrak{U} \to \mathfrak{W}$, where $\mathfrak{U}$ has base set U, the quotient $\mathcal{L}$-structure $\mathfrak{U}_f$ is defined as follows:*

- *the base set of $\mathfrak{U}_f$ is U_f;*
- *for each function symbol h (including constant symbols), the interpretation of h in $\mathfrak{U}_f$ is given by:*

$$h^{\mathfrak{U}_f}(\bar{x}_1, \ldots, \bar{x}_n) = h^{\mathfrak{U}}(x_1, \ldots, x_n);$$

- *for each relation symbol R, the interpretation of R in $\mathfrak{U}_f$ is given by: $R^{\mathfrak{U}_f}(\bar{x}_1, \ldots, \bar{x}_n)$ holds if and only if there exist $u_1 \in \bar{x}_1, \ldots, u_n \in \bar{x}_n$ such that $R^{\mathfrak{U}}(u_1, \ldots, u_n)$ holds.*

Proposition 4.3.10. *Let $f \colon \mathfrak{U} \to \mathfrak{W}$ be a morphism of $\mathcal{L}$-structures. We have:*

1. *The quotient structure $\mathfrak{U}_f$ is indeed an $\mathcal{L}$-structure.*
2. *The canonical map $\pi_f \colon \mathfrak{U} \to \mathfrak{U}_f$ is a $\mathcal{L}$-morphism.*

3. *The induced map* $\bar{f}\colon \mathfrak{U}_f \to \mathfrak{W}$ *is an injective* $\mathcal{L}$*-morphism.*

4. *The morphism* f *is relation-onto if and only if* $\bar{f}$ *is a* $\mathcal{L}$*-monomorphism.*

5. *The morphism* f *is onto and relation-onto if and only if* $\bar{f}$ *is a* $\mathcal{L}$*-isomorphism.*

Proof. The proof is easy and left to the reader (it comes from Lemma 4.3.7). □

The following lemma is well known.

Lemma 4.3.11. *Let* $\mathfrak{U}$ *be an* $\mathcal{L}$*-structure,* $\asymp$ *a binary relation symbol, and* $T_{\asymp}$ *the theory of the equality for the symbol* $\asymp$*. The quotient structure* $\mathfrak{U}/\asymp^{\mathfrak{U}}$ *is an* $\mathcal{L}$*-structure which satisfies* $T_{\asymp}$ *(hence it is a* equalitarian structure*) and is elementarily equivalent to* $\mathfrak{U}$*.*

Proposition 4.3.12. *Let* $\mathcal{L}_0$ *be a first order language. Let* $\mathcal{U}_0$ *be a class of* $\mathcal{L}_0$*-structures and* $\mathfrak{W}$ *be an* $\mathcal{L}_0$*-structure. Assume that for each structure* $\mathfrak{U} \in \mathcal{U}_0$ *there exists a morphism* $f_{\mathfrak{U}}\colon \mathfrak{U} \to \mathfrak{W}$ *which is onto and relation-onto. Let* $\mathcal{L}_1$ *be a language that contains* $\mathcal{L}_0$ *and, given an interpretation for each symbol of* $\mathcal{L}_1 \smallsetminus \mathcal{L}_0$ *in each structure* $\mathfrak{U}$ *of* $\mathcal{U}_0$*, we denote by* $\mathfrak{U}_1$ *the new structure, and* $\mathcal{U}_1$ *denotes the class of* $\mathcal{L}_1$*-structures* $\mathfrak{U}_1$*. If the collection of relations* $\sim_{f_{\mathfrak{U}}}$ *is uniformly definable by an* $\mathcal{L}_1$*-formula* $\varphi(a,b)$ *in* $\mathcal{U}_1$*, then the algorithm* $\mathcal{A}$ *which does the following:*
`In any` $\mathcal{L}_0$`-sentence` F`, for each relation symbol` R `(including the symbol of equality) that occurs in` F`, replace` $R(x_1,\dots,x_n)$ `by`

$$\exists u_1,\dots,u_n \left(\bigwedge_{i=1}^{n} \varphi(u_i,y_i) \wedge R(u_1,\dots,u_n) \right);$$

uniformly encodes $(\mathcal{F}_{\mathcal{L}_0},\mathfrak{W})$ *in* $(\mathcal{F}_{\mathcal{L}_1},\mathcal{U}_1)$*. Moreover,*

- *if the formula* $\varphi(a,b)$ *is existential then* $\mathcal{A}$ *uniformly encodes* $(\mathcal{F}^{\mathrm{e}}_{\mathcal{L}_0},\mathfrak{W})$ *in* $(\mathcal{F}^{\mathrm{e}}_{\mathcal{L}_1},\mathcal{U}_1)$*;*

- *if the formula* $\varphi(a,b)$ *is positive existential then* $\mathcal{A}$ *uniformly encodes* $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_0},\mathfrak{W})$ *in* $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_1},\mathcal{U}_1)$*.*

Proof. Let us show that the algorithm $\mathcal{A}$ uniformly encodes $(\mathcal{F}_{\mathcal{L}_0}, \mathfrak{W})$ in $(\mathcal{F}_{\mathcal{L}_1}, \mathcal{U}_1)$ (the same algorithm works analogously for the two other cases). By Proposition 4.3.10, Item 5, for each $\mathfrak{U}$ in the class $\mathcal{U}_0$, $\mathfrak{W}$ satisfies F if and only if $\mathfrak{U}_{f_\mathfrak{U}}$ satisfies F. Let us define the $\mathcal{L}_0$-structure $\mathfrak{U}^{f_\mathfrak{U}}$ by

- the base set of $\mathfrak{U}^{f_\mathfrak{U}}$ is the base set of $\mathfrak{U}$;
- function symbols are interpreted in $\mathfrak{U}^{f_\mathfrak{U}}$ as in $\mathfrak{U}$;
- for each relation symbol R (including the equality) of $\mathcal{L}_0$,

  $$R^{\mathfrak{U}^{f_\mathfrak{U}}}(x_1, \ldots, x_n)$$

  holds if and only if there exists $u_1, \ldots, u_n \in \mathfrak{U}$ such that $u_1 \sim_{f_\mathfrak{U}} x_1$, …, $u_n \sim_{f_\mathfrak{U}} x_n$ and $R^{\mathfrak{U}}(u_1, \ldots, u_n)$ holds.

In particular, the symbol of equality is interpreted in $\mathfrak{U}^{f_\mathfrak{U}}$ as the relation $\sim_{f_\mathfrak{U}}$. By Proposition 4.3.10, Item 2, the $\mathcal{L}_0$-structure $\mathfrak{U}^{f_\mathfrak{U}}$ satisfies the theory of equality $T_=$. By Lemma 4.3.11, the structure $\mathfrak{U}_{f_\mathfrak{U}}$ satisfies F if and only if $\mathfrak{U}^{f_\mathfrak{U}}$ satisfies F. Therefore, $\mathfrak{U}_{f_\mathfrak{U}}$ satisfies F if and only if $\mathfrak{U}_1$ satisfies $\mathcal{A}(F)$. □

4.4 Case of integers

4.4.1 Some general uniform definitions in $\mathcal{N}$ and $\mathcal{D}$

In this section we will show in particular that squaring powers of a prime is uniformly positive existentially definable in $\mathcal{N}$ and in $\mathcal{D}$ - see Notation 4.1.1, Items 8, 9, and 10.

When working with the structures $\mathfrak{N}_p$, the string '$a \leq b$' stands for

$$\exists c(b = a + c).$$

Notation 4.4.1. *1. for each prime number p we define*

$$P_p^{>} = \{p^h : h \in \mathbb{N}\} \qquad P_p^{\pm} = \{\pm p^h : h \in \mathbb{N}\}$$

$$P_{p,0}^{>} = \{p^h : h \in \mathbb{N}_{>0}\} \qquad P_{p,0}^{\pm} = \{\pm p^h : h \in \mathbb{N}_{>0}\}$$

Lemma 4.4.2. *The formula $P(n) = R(1, n)$ uniformly positive existentially*

1. *$\mathcal{L}^{*,+}$-defines the collection of sets $P_p^>$ in $\mathcal{N}$ (hence in particular $P_p^>$ is $\mathcal{L}^{*,+}$-uped in $\mathcal{N}$);*

2. *$\mathcal{L}_T^*$-defines the collection of sets $P_p^\pm$ in $\mathcal{D}$ (hence in particular $P_p^\pm$ is $\mathcal{L}_T^*$-uped in $\mathcal{D}$).*

Proof. This comes immediately from the definitions. □

Lemma 4.4.3. *The formula*

$$P_0^\varepsilon(n)\colon \begin{cases} R(1,n) \wedge (n \geq 2) & \text{if } \varepsilon \text{ is } > \\ R(1,n) \wedge T(n) & \text{if } \varepsilon \text{ is } \pm \end{cases}$$

uniformly positive existentially

1. *$\mathcal{L}^{*,+}$-defines the collection of sets $P_{p,0}^>$ in $\mathcal{N}$ if ε is $>$ (hence $P_{p,0}^>$ is $\mathcal{L}^{*,+}$-uped in $\mathcal{N}$).*

2. *$\mathcal{L}_T^*$-defines the collection of sets $P_{p,0}^\pm$ in $\mathcal{D}$ if ε is $\pm$ (hence $P_{p,0}^\pm$ is $\mathcal{L}_T^*$-uped in $\mathcal{D}$).*

Proof. This comes immediately from the definitions. □

Lemma 4.4.4. *Consider the positive existential formula*

$$\bar{\theta}_P^\varepsilon(m,n)\colon P_0^\varepsilon(m) \wedge P_0^\varepsilon(n) \wedge R(m-1, n-m)$$

over $\mathcal{L}^{*,+}$ if ε is $>$, and over $\mathcal{L}_T^*$ if ε is $\pm$. For each prime p, we have

1. *$\mathfrak{N}_p$ satisfies $\bar{\theta}_P^>$ if and only if $m, n \in P_{p,0}^>$ and $n = m^2$; and*

2. *$\mathfrak{D}_p$ satisfies $\bar{\theta}_P^\pm$ if and only if $m, n \in P_{p,0}^\pm$ and*

   - *either $n = m^2$; or*
   - *$p = 2$ and $(m,n) \in \{(-2,-8),(2,-2),(4,-2),(4,-8)\}$; or*
   - *$p = 3$ and $(m,n) = (3,-3)$.*

Proof. We leave to the reader the verification of the implications from the right to the left. Suppose that $\bar{\theta}_P^\varepsilon$ is satisfied in $\mathfrak{D}_p$ or $\mathfrak{N}_p$ (depending on ε). There exist integers r, s, ℓ such that $r > 0$ and $s > 0$ and there exist ρ, σ, λ in $\{-1, 1\}$ (or $= 1$ if working in $\mathfrak{N}_p$) so that

$$m = \rho p^r \qquad n = \sigma p^s \qquad n - m = \lambda p^\ell (m-1).$$

By direct substitution we obtain

$$\sigma p^s - \rho p^r = \lambda p^\ell (\rho p^r - 1)$$

and deduce

$$\sigma p^s + \lambda p^\ell = \rho p^r (\lambda p^\ell + 1)$$

which implies that ℓ is positive (looking at the latter equation modulo p). Write the above equation as

$$\sigma p^s = \rho p^r - \lambda p^\ell + \rho\lambda p^{r+\ell} \tag{4.5}$$

and consider it over the ring $\mathbb{Z}_p$ of p-adic integers (or simply as an equation written in base p).

In the case of $\mathfrak{N}_p$, Equation (4.5) gives

$$p^s + p^\ell = p^r + p^{r+\ell}. \tag{4.6}$$

Since the right-hand side has two non-zero p-adic digits (for some choice of digits containing 1), we have either $s = r$ and $\ell = r + \ell$, or $s = r + \ell$ and $\ell = r$. But the former case is impossible since $r > 0$. Hence $s = 2r$ and we deduce that $n = m^2$.

Let us come back to the general case of integers. Note that by Equation (4.5), if $\rho = \lambda$ then $\sigma = \lambda\rho = 1$ and $s = 2r$, hence $n = m^2$.

If $p \geq 3$ then, since the coefficients lie between -1 and 1 and since $r + \ell > \max\{r, \ell\}$, we deduce, from the uniqueness of the p-adic expansion, choosing for example representative "digits" within

$$D = \left\{ -\frac{p-1}{2}, \ldots, \frac{p-1}{2} \right\},$$

that $r = \ell$. Therefore, we have

$$\sigma p^s = (\rho - \lambda) p^r + \lambda\rho p^{2r} \tag{4.7}$$

and if $\rho = \lambda$ then $\sigma = \lambda\rho = 1$ and $s = 2r$, hence $n = m^2$. If ρ is distinct from λ then p must be 3 since otherwise the right-hand side would have two non-zero digits while the left-hand side has only one. Equation (4.7) becomes

$$\sigma 3^s = 2\rho 3^r - 3^{2r}$$

hence

$$\sigma 3^{s-r} = 2\rho - 3^r$$

which implies $s = r$ (looking at the equation modulo 3). Therefore we have

$$\sigma = 2\rho - 3^r$$

which can happen only if $\sigma = -1$, $\rho = 1$ and $r = 1$, hence $(m, n) = (3, -3)$.

Suppose that $p = 2$. Note that if $r = \ell$ and $\rho = \lambda$ then we conclude that $n = m^2$ as before.

Case $\rho = -\lambda$. Equation (4.5) becomes

$$2^{r+\ell} + \sigma 2^s = \rho(2^r + 2^\ell). \tag{4.8}$$

If $\sigma = 1$ then $\rho = 1$, which gives

$$2^{r+\ell} + 2^s = 2^r + 2^\ell.$$

Since $r+\ell > \max\{r, \ell\}$, by the uniqueness of the 2-adic expansion with digits $\{0, 1\}$, we have $r = \ell$, hence

$$2^{2r} + 2^s = 2^{r+1}.$$

Hence $s = 2r$ and $2^{2r+1} = 2^{r+1}$, which is impossible since $r > 0$.

Therefore, $\sigma = -1$. If $\rho = -1$ then Equation (4.8) becomes

$$2^{r+\ell} + 2^r + 2^\ell = 2^s,$$

which gives $r = \ell$ (again by uniqueness), hence

$$2^{2r} + 2^{r+1} = 2^s$$

and we deduce that $2r = r + 1$, hence $r = 1$ and $s = 3$, which corresponds to the pair $(m, n) = (-2, -8)$. If $\rho = 1$ then Equation (4.8) becomes

$$2^{r+\ell} = 2^s + 2^r + 2^\ell,$$

which implies (again by uniqueness of the expansion) that either $s = r$, or $s = \ell$, or $r = \ell$.

- If $s = r$ then $2^{r+\ell} = 2^{r+1} + 2^\ell$, hence $r + 1 = \ell$, hence $2^{2r+1} = 2^{r+2}$ and $r = 1$. This case corresponds to the pair $(m, n) = (2, -2)$.

- If $s = \ell$ then $2^{r+s} = 2^{s+1} + 2^r$, hence $s + 1 = r$, hence $2^{2s+1} = 2^{s+2}$ and $s = 1$. This case corresponds to the pair $(m, n) = (4, -2)$.
- If $r = \ell$ then $2^{2r} = 2^s + 2^{r+1}$, hence $s = r + 1$, hence $2^{2r} = 2^{r+2}$ and $r = 2$. This case corresponds to the pair $(m, n) = (4, -8)$.

Case $\rho = \lambda$ and $r \neq \ell$. Equation (4.5) becomes

$$\sigma 2^s = \rho 2^r - \rho 2^\ell + 2^{r+\ell}. \tag{4.9}$$

If $\rho = 1$ then

$$\sigma 2^s = 2^r - 2^\ell + 2^{r+\ell} > 2^r > 0,$$

hence $\sigma = 1$. Therefore, we have

$$2^s + 2^\ell = 2^r + 2^{r+\ell},$$

which we know from the analysis of Equation (4.6) that it has no solution unless $\ell = r$. □

Corollary 4.4.5. *There exists a positive existential formula*

1. *$\theta_P^>(m, n)$ that uniformly $\mathcal{L}^{*,+}$-defines the collection of sets $\{(p^h, p^{2h}) \colon h \in \mathbb{N}\}$ in $\mathcal{N}$ (hence squaring in $P_p^>$ is $\mathcal{L}^{*,+}$-uped in $\mathcal{N}$).*
2. *$\theta_P^\pm(m, n)$ that uniformly $\mathcal{L}_T^*$-defines the collection of sets $\{(\pm p^h, p^{2h}) \colon h \in \mathbb{N}\}$ in $\mathcal{D}$ (hence squaring in $P_p^\pm$ is $\mathcal{L}_T^*$-uped in $\mathcal{D}$).*

Proof. Choose

$$\theta_P^>(m, n) \colon \bar{\theta}_P^>(m, n) \vee (m = 1 \wedge n = 1),$$

for Item 1 and

$$\theta_P^\pm(m, n) \colon ((m = 1 \vee m = -1) \wedge n = 1) \vee (\bar{\theta}_P^\pm(m, n) \wedge n \neq -2 \wedge n \neq -3 \wedge n \neq -8)$$

for Item 2. □

Remark 4.4.6. *Corollary 4.4.5 allows us to write in our formulas terms like a^2, a^4, a^8,... whenever a is an element of P_p, $P_{p,0}$, P_p^+ or $P_{p,0}^+$.*

4.4.2 Multiplication uniformly in $\mathcal{N}$ and $\mathcal{Z}$

In this section we will first prove Item 1 of Theorem 4.1.13 and then deduce Item 2 from it.

Lemma 4.4.7. *The collections of sets*

$$M_p = \{(n, p^a, np^a) \colon n \geq 0 \text{ and } a \geq 0\}$$

are $\mathcal{L}^{*,+}$-uped in $\mathcal{N}$.

Proof. Following the strategy of the second author in [Ph1, Section 2], we show that the following formula $\varphi(x, y, z)$

$$P^{>}(y) \wedge z \geq x \wedge R(x, z) \wedge R(x + 1, z + y) \wedge R(x + y, z + y^2)$$

is true in $\mathfrak{N}_p$ if and only if $(x, y, z) \in M_p$.

If $z = xy$ and $y = p^a$ for some non-negative integer a, then we have

- $z \geq x$;
- $z = xp^a$;
- $z + y = xp^a + p^a = p^a(x + 1)$; and
- $z + y^2 = xp^a + p^{2a} = p^a(x + y)$,

hence $\mathfrak{N}_p$ satisfies $\varphi(x, y, z)$.

Suppose that $\mathfrak{N}_p$ satisfies $\varphi(x, y, z)$. There exist integers a, α, β, γ such that $a \geq 0$ and

$$y = p^a \tag{4.10}$$

$$z = p^\alpha x \tag{4.11}$$

$$z + y = p^\beta(x + 1) \tag{4.12}$$

$$z + y^2 = p^\gamma(x + y). \tag{4.13}$$

First note that if $x = 0$ then $z = 0$ and we are done, hence we suppose that x is positive. From $z = p^\alpha x$, $z \geq x$ and $x \geq 1$ we deduce that α is non-negative. Also we have β and γ non-negative (since from Equation (4.12) we have

$$x + 1 \leq z + y = p^\beta(x + 1)$$

and from Equation (4.13) we have $x + y \leq z + y^2 = p^\gamma(x + y))$.

From Equation (4.11), (4.12) and (4.13) we obtain

$$x(p^\alpha - p^\beta) = p^\beta - p^a \tag{4.14}$$

and from Equation (4.10), (4.11) and (4.13) we obtain

$$x(p^\alpha - p^\gamma) = p^{a+\gamma} - p^{2a}. \tag{4.15}$$

Let us prove that if two elements of $\{a, \alpha, \beta, \gamma\}$ are equal then $z = xy$.

- If $a = \alpha$ then we conclude from Equations (4.10) and (4.11).
- If $a = \beta$ then we conclude that $\alpha = \beta$ from Equation (4.14) and $x > 0$.
- If $a = \gamma$ then we conclude that $\alpha = \gamma$ from Equation (4.15) and $x > 0$.
- If $\alpha = \beta$ then we conclude that $a = \beta$ from Equation (4.14) and $x > 0$.
- If $\alpha = \gamma$ then we conclude that $a = \gamma$ from Equation (4.15) and $x > 0$.
- If $\beta = \gamma$ then from Equations (4.14) and (4.15) we have $p^\beta - p^a = p^{a+\beta} - p^{2a}$, hence $p^\beta(1 - p^a) = p^a(1 - p^a)$, hence either $a = \beta$, in which case we can conclude as above, or $a = 0$ and $\beta > 0$. In the latter case, from Equation (4.14) we obtain $x(p^\alpha - p^\beta) = p^\beta - 1 > 0$, hence $\alpha > \beta > 0$, which is impossible since p does not divide $p^\beta - 1$.

From now on, we may suppose that a, α, β, and γ are pairwise distinct. From Equation (4.14), we have

$$\alpha > \beta \text{ if and only if } \beta > a \tag{4.16}$$

hence either $\alpha > \beta > a$ or $\alpha < \beta < a$. Similarly, from Equation (4.15), we have

$$\alpha > \gamma \text{ if and only if } \gamma > a \tag{4.17}$$

hence either $\alpha > \gamma > a$ or $\alpha < \gamma < a$. So we have four possible orders:

1. $\alpha > \beta > \gamma > a$;
2. $\alpha > \gamma > \beta > a$;
3. $\alpha < \beta < \gamma < a$; or

4. $\alpha < \gamma < \beta < a$.

From Equations (4.14) and (4.15) we have

$$(p^\alpha - p^\gamma)(p^\beta - p^a) = (p^\alpha - p^\beta)(p^\gamma - p^a)p^a. \tag{4.18}$$

Hence the orders 2 and 4 are impossible (otherwise the left-hand side would have smaller absolute value than the right-hand side). In case of order number 1, the valuation at p in Equation (4.18) gives

$$\gamma + a = \beta + 2a,$$

hence

$$\gamma = \beta + a > \gamma + a,$$

which is absurd. In case of order number 3, we obtain

$$\alpha + \beta = \alpha + \gamma + a,$$

hence

$$\beta = \gamma + a > \beta + a,$$

which is absurd. □

Next corollary proves Item 1 of Theorem 4.1.13.

Corollary 4.4.8. *Multiplication is $\mathcal{L}^{*,+}$-uped in $\mathcal{N}$.*

Proof. The proof is identical to the proof of [Ph1, Lemma 3] using Lemma 4.4.7 instead of [Ph1, Lemma 2]. □

Next corollary proves Item 2 of Theorem 4.1.13.

Corollary 4.4.9. *Multiplication is $\mathcal{L}^*$-uped in $\mathcal{Z}$.*

Proof. Let $\mu(x, y, z)$ be a positive existential $\mathcal{L}^{*,+}$-formula that uniformly defines multiplication $z = xy$ in $\mathcal{N}$ (it exists from Corollary 4.4.8). Let $\bar{\mu}(x, y, z)$ be the $\mathcal{L}^*$-formula obtained from μ by replacing (syntactically) all occurences of the form $\exists u$ (where u is a variable) by $\exists u \geq 0$. The (positive existential) $\mathcal{L}^*$-formula

$$\mu_1(x, y, z) = \bar{\mu}(x, y, z) \wedge x \geq 0 \wedge y \geq 0 \wedge z \geq 0$$

uniformly defines the set

$$\{(x, y, z) \colon z = xy \text{ and } x, y, z \geq 0\}$$

in $\mathcal{Z}$. The (positive existential) $\mathcal{L}^*$-formula

$$\mu_2(x, y, z) = \bigvee_{\varepsilon \in \{-1,1\}^3} \varepsilon_1 x \geq 0 \wedge \varepsilon_2 y \geq 0 \wedge \varepsilon_3 z \geq 0 \wedge \mu_1(\varepsilon_1 x, \varepsilon_2 y, \varepsilon_3 z)$$

uniformly defines $\{(x, y, z) \colon z = xy\}$ in $\mathcal{Z}$. □

4.4.3 Multiplication uniformly in $\mathcal{D}$

In this section we prove Item 3 of Theorem 4.1.13.

Lemma 4.4.10. *There is a positive existential $\mathcal{L}_T^*$-formula $CO(x)$ that defines uniformly the collection of sets*

$$CO_p = \{n \in \mathbb{Z} \colon p \nmid n\}$$

in $\mathcal{D}$ (hence the sets CO_p are $\mathcal{L}_T^*$-uped in $\mathcal{D}$).

Proof. Consider the formula

$$\exists m(P_0^{\pm}(m) \wedge n | m - 1).$$

If $n \in CO_p$, then we can take $m = p^{\varphi(|n|)}$, since by Euler's theorem we know that $p^{\varphi(|n|)}$ is congruent to 1 mod n.

Conversely, if the formula is satisfied in some $\mathfrak{D}_p$, then there exists $k \in \mathbb{Z}$ such that $nk = m - 1$. Since p divides m, it does not divide n. □

The next lemma defines squaring uniformly in each CO_p.

Lemma 4.4.11. *The collection of sets*

$$\left\{(n, n^2) \colon n \in CO_p\right\}$$

is $\mathcal{L}_T^*$-uped in $\mathcal{D}$. More precisely, for any integer prime p we have: $n = m^2$ with $m, n \in CO_p$ if and only if $\mathfrak{D}_p$ satisfies the following $\mathcal{L}_T^*$-formula $\theta_{CO}(m, n)$

$$CO(m) \wedge CO(n) \wedge \exists a(P_0^{\pm}(a) \wedge m | a^2 - 1 \wedge n | a^2 - 1 \wedge a^8 - m \mid a^{16} - n).$$

Proof. If $n = m^2$ and $m, n \in CO_p$ we have two cases; if $|m| = n = 1$ then any $a \in P^{\pm}_{p,0}$ works, and if $T(m)$ then $n > 2$ and we can choose $a = p^{\phi(m)\phi(n)/2}$, where ϕ stands for Euler's function (recall that $\phi(n)$ is even for $n > 2$).

Suppose that $\mathfrak{D}_p$ satisfies $\theta_{CO}(m, n)$ for some $m, n \in CO_p$. Since $a \in P^{\pm}_{p,0}$ we have $a \geq 2$. Since m and n divide $a^2 - 1$, we have $|m| < a^2$ and $|n| < a^2$. Since $a^8 - m$ divides

$$a^{16} - n = a^{18} - m^2 + m^2 - n,$$

we have:

1. $a^8 - m$ divides $m^2 - n$;
2. $|m^2 - n| < a^4 + a^2$ (since $|m| < a^2$ and $|n| < a^2$); and
3. $|a^8 - m| > a^8 - a^2$ (since $|m| < a^2$).

By 1, we have that either $m^2 - n = 0$ or $|a^8 - m| \leq |m^2 - n|$. For the sake of contradiction, suppose that the latter is true. Then we have

$$a^8 - a^2 < |a^8 - m| \leq| m^2 - n| < a^4 + a^2$$

hence, since $a \geq 2$ we get

$$a^8 < a^4 + 2a^2 < a^4 + a^4 < a^8$$

which is impossible. Therefore $m^2 = n$. □

Lemma 4.4.12. *The collection of sets*

$$\{(x, y, z) \colon z = xy \text{ and } x \in CO_p \text{ and } y \in P^{\pm}_p\}$$

is $\mathcal{L}^*_T$-uped in $\mathcal{D}$. More precisely, for any integer prime p, we have: $x = mn$ with $m \in CO_p$ and $n \in P^{\pm}_p$, if and only if $\mathfrak{D}_p$ satisfies the formula $\rho_{CP}(m, n, x)$

$$(n = -1 \wedge m = -x) \vee (n = 1 \wedge m = x) \vee$$
$$\left(CO(m) \wedge P^{\pm}_0(n) \wedge \exists a, b(\theta_{CO}(m, a) \wedge \theta^{\pm}_P(n, b) \wedge \theta_{CO}(m + n, a + 2x + b))\right).$$

Proof. Note that if p does not divide m and $n \in P^{\pm}_{p,0}$ then p does not divide $m + n$, and note that $(m + n)^2 = a + 2mn + b$. □

We are now ready to show that squaring is $\mathcal{L}_T^*$-uped in $\mathcal{D}$.

Lemma 4.4.13. *For any integer prime p and for any $m, n \in \mathbb{Z}$ the following holds: $n = m^2$ if and only if $\mathfrak{D}_p$ satisfies*

$$\exists a, b, u, v (P(a) \wedge P(b) \wedge CO(u) \wedge CO(v) \wedge \rho_{CP}(u, a, m) \wedge \rho_{CP}(v, b, n) \wedge \theta_P^{\pm}(a, b) \wedge \theta_{CO}(u, v))$$

Proof. Choose

$$a = p^{\mathrm{ord}_p m} \qquad \text{and} \qquad u = \frac{m}{a}$$

and do the same for n. □

It is standard to define multiplication using squaring: for any $m, n, h \in \mathbb{Z}$ the following holds:

$$h = m \cdot n \text{ if and only if } (m+n)^2 = m^2 + 2h + n^2.$$

Hence multiplication is $\mathcal{L}_T^*$-uped in $\mathcal{D}$ and Item 3 of Theorem 4.1.13 follows.

4.5 Pell equations uniformly

If x and a are polynomials in z, we will denote by $x(a)$ the composition $x \circ a$.

Let us first remind some known facts about Pell equations.

Theorem 4.5.1. *Let F be a field of characteristic $p \neq 2$ and let z be a variable. Let $a \in F[z] \setminus F$. Any solution $(X, Y) = (x, y)$ in $F[z]$ of the equation*

$$X^2 - (a^2 - 1)Y^2 = 1 \tag{4.19}$$

is of the form $(x, y) = (\pm x_n(a), y_n(a))$ where the pairs $(x_n(z), y_n(z))$ are defined by

$$x_n(z) + \sqrt{z^2 - 1}\, y_n(z) = \left(z + \sqrt{z^2 - 1}\right)^n \tag{4.20}$$

by separating rational and irrational parts over $F(z)$.

Moreover, for any $m, n \in \mathbb{Z}$ we have

1. $x_{m+n}(a) = x_m(a)x_n(a) - (a^2 - 1)y_m(a)y_n(a)$;
2. $y_{m+n}(a) = x_m(a)y_n(a) + x_n(a)y_m(a)$;

3. *The integer m divides in $\mathbb{Z}$ the integer n if and only if the polynomial $y_m(a)$ divides in $F[z]$ the polynomial $y_n(a)$;*

4. *If $p \neq 0$ then for any $s \in \mathbb{Z}$ we have: $n = \pm mp^s$ if and only if $x_n(a) = x_m^{p^s}(a)$.*

5. *$y_n(a)$ is non constant if and only if $n \notin \{-1, 0, 1\}$.*

Proof. See [PZ1]. □

Theorem 4.5.1 tells us essentially that the structure of the set of solutions of the Pell equation (4.19) does not depend on the parameter a, not only as a group, but also as a structure with the relation of divisibility and the function that takes p^s-th powers.

Notation 4.5.2. *We consider the following two groups:*

1. *$(\mathbb{Z} \times \mu_2, \oplus)$, where μ_2 is the multiplicative group with two elements, has its law defined by*

$$(m, v) \oplus (n, w) = (wm + vn, vw).$$

2. *If F is a field of characteristic $p \neq 2$, then*

$$\Sigma_a(F) \subseteq F[z] \times F[z]$$

denotes the set of solutions of

$$X^2 - (a^2 - 1)Y^2 = 1,$$

where $a \in F[z] \smallsetminus F$. It is well known that the operation

$$(x, y) \oplus (x', y') = (xx' - (a^2 - 1)yy', xy' + x'y)$$

defines a group law on $\Sigma_a(F)$.

Let us define the class $\mathcal{Q}$ as the set

$$\{\mathfrak{Q}_p \colon p \text{ is prime}\}$$

where the $\mathcal{L}_T^*$-structures $\mathfrak{Q}_p$ are defined as follows

- the base set is $\mathbb{Z} \times \mu_2$;

- 0 is interpreted as $(0,1)$;
- 1 is interpreted as $(1,1)$;
- $+$ is interpreted as $\oplus$;
- $(u,v) \mid (x,y)$ is interpreted as "u divides x";
- $R((u,v),(x,y))$ is interpreted as "$u \mid_p x$;
- $T((u,v))$ is interpreted as "u is not in $\{-1,0,1\}$".

Let β be a unary predicate symbol interpreted in each $\mathcal{L}_T^*$-structure $\mathfrak{Q}_p$ as

$$\beta^{\mathfrak{Q}_p}((v_1,v_2)) \text{ if and only if } v_2 = 1.$$

Lemma 4.5.3. *The symbol β is $\mathcal{L}_T^*$-uped in $\mathcal{Q}$ by*

$$\zeta(v)\colon \exists w(v = w + w \vee v = w + w + 1)$$

Proof. The formula $\zeta(v)$ is satisfied in $\mathfrak{Q}_p$ if and only if there exist $w_1 \in \mathbb{Z}$ and $w_2 \in \mu_2$ such that

$$(v_1,v_2) = 2(w_1,w_2) = (2w_1w_2,1)$$

or

$$(v_1,v_2) = 2(w_1,w_2) + (1,1) = (2w_1w_2 + 1,1),$$

and the latter happens if and only if $v_2 = 1$. □

It is well known that $\Sigma_a(F)$ is isomorphic to the additive group $\mathbb{Z} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$. We will use this fact in the following form:

Lemma 4.5.4. *The map*

$$\begin{array}{rccc} \xi_{a,F}\colon & \mathbb{Z} \times \mu_2 & \to & \Sigma_a(F) \\ & (n,\varepsilon) & \mapsto & (\varepsilon x_n, y_n). \end{array}$$

is an isomorphism of groups.

Notation 4.5.5. *Let F be a field of characteristic $p \neq 2$ and $a \in F[z]$ non-constant. We consider the following $\mathcal{L}_T^*$-structure*

$$\mathfrak{G}_a(F) = \Big(\Sigma_a(F); (1,0), (a,1), \oplus, |, \tilde{R}, \tilde{T}\Big)$$

where

- $(x,y) \mid (u,v)$ *means "y divides v";*
- $\tilde{R}((x,y),(u,v))$ *means "there exists $s \in \mathbb{Z}$ such that $x^{p^s} = u$"*
- $\tilde{T}(x,y)$ *means "y is not a constant".*

Lemma 4.5.6. *For any field F of characteristic $p \neq 2$, and for each $a \in F[z] \smallsetminus F$, the $\mathcal{L}_T^*$-structures $\mathfrak{G}_a(F)$ and $\mathfrak{Q}_p$ are isomorphic through $\xi_{a,F}$.*

Proof. It is an immediate consequence of Theorem 4.5.1. □

Notation 4.5.7. *Consider the $\mathcal{L}_A$-formula*

$$\delta(\alpha, v, w) \colon v^2 + (\alpha^2 - 1)w^2 = 1$$

and note that it is satisfied in $F[z]$ if and only if the pair (v,w) is a solution of the Pell equation with parameter α.

Lemma 4.5.8. *If α is interpreted as a non-constant element of $F[z]$ then the positive existential $\mathcal{L}_A$-formula*

$$\eta(\alpha, v, w) \colon \delta(\alpha, v, w) \wedge (\exists x, y(\delta(\alpha, x, y) \wedge (v = x^2 - (\alpha^2 - 1)y^2 \wedge w = 2xy) \vee (v = (x^2 - (\alpha^2 - 1)y^2)\alpha - (\alpha^2 - 1)2xy \wedge w = x^2 - (\alpha^2 - 1)y^2 + 2\alpha xy))).$$

is satisfied in $F[z]$ if and only if (u,v) is a solution of the Pell equation with parameter α and $u = x_n$ for some integer n.

Proof. This is trivial from Lemmas 4.5.3 and then 4.5.6. □

Lemma 4.5.9. *For each ε in $\{\pm 1\}$, let us consider the following positive existential $\mathcal{L}_A$-formula $\Delta^\varepsilon(\alpha, x, x')$:*

$$\eta(\varepsilon x, \varepsilon x') \wedge \exists y, y', y_1, y_2(\delta(\alpha, \varepsilon x, y) \wedge \delta(\alpha, \varepsilon x', y') \wedge \delta(\varepsilon x, \varepsilon x', y_1) \wedge \delta(\varepsilon x + 1, \varepsilon x' + 1, y_2))$$

and write

$$\Delta(\alpha, x, x') \colon \bigvee_{\varepsilon \in \{\pm 1\}} \Delta^{\varepsilon}(\alpha, x, x').$$

Whenever α is assigned a non-constant element of $F[z]$, the formula $\Delta(\alpha, x, x')$ is satisfied in $F[z]$ if and only if $R_{F[z]}(x, x')$ holds (see Definition 4.1.6).

Proof. Note that Δ^1 is analogous to the formula of Lemma 2.4 in [PZ1]. □

4.6 The relation "y is a p^s-th power of x"

In this section, we prove Theorems 4.1.8, 4.1.10 and 4.1.11.

Lemma 4.6.1. *Let A be a commutative ring with unit. Let $x, y \in A$ such that $y = x^{p^s}$ for some non-negative integer s. Write*

$$x_n^2 = (x - 1 + n)^{p^s+1},$$

where $n = 1, \ldots, M$ for some integer $M \geq 2$. We have

$$xy = x_1^2 \qquad \text{and} \qquad x + y = x_2^2 - x_1^2 - 1.$$

Proof. Let us show that the second equation holds. We have:

$$\begin{aligned} x + y &= x + x^{p^s} \\ &= x^{p^s+1} + x + x^{p^s} + 1 - x^{p^s+1} - 1 \\ &= (x+1)(x^{p^s} + 1) - x^{p^s+1} - 1 \\ &= (x+1)(x+1)^{p^s} - x^{p^s+1} - 1 \\ &= (x+1)^{p^s+1} - x^{p^s+1} - 1 \\ &= x_2^2 - x_1^2 - 1 \end{aligned}$$

which proves the lemma. □

Proof of Theorem 4.1.8. Suppose that Büchi's problem has a positive answer for a triple (A, C, M) and write $M_0 = M_0(A, C)$, so that we have: *any M-term Büchi sequence (x_n) of (A, C), with $M \geq M_0$, is of the form*

$$x_n^2 = (f + n)^{p^s+1}$$

for some non-negative integer s and $f \in A$.

Consider the following formulas from the language of rings

$$\varphi_0(x_1,\dots,x_{M_0},x,y)\colon \Delta^{(2)}(x_1^2,\dots,x_{M_0}^2)=(2)\wedge xy=x_1^2\wedge x+y=x_2^2-x_1^2-1,$$

$$\varphi_1(x,y)\colon \exists x_1\dots\exists x_{M_0}\varphi_0(x_1,\dots,x_{M_0},x,y)$$

and

$$\varphi_{M_0}(x,y)\colon \varphi_1(x,y)\vee\varphi_1(y,x).$$

For short, we might write

$$\text{"there exists } s\in\mathbb{Z} \text{ such that } y=x^{p^s}\text{"}$$

instead of " there exists $s\in\mathbb{N}$ such that either $y=x^{p^s}$ or $x=y^{p^s}$".

Let us prove Item 1 of Theorem 4.1.8. Let $x,y\in A$ be such that $R_A(x,y)$ holds. By definition of R_A we have $y=x^{p^s}$ for some integer s. If $s\geq 0$, taking $x_n\in A$ such that $x_n^2=(x-1+n)^{p^s+1}$ the formula $\varphi_{M_0}(x,y)$ is satisfied in A by Lemma 4.6.1. Analogously if $s\leq 0$ then by taking $x_n^2=(y-1+n)^{p^{-s}+1}$ the formula $\varphi_1(y,x)$ is true in A by Lemma 4.6.1.

Let us prove Item 2 of Theorem 4.1.8 (note that one implication comes directly from Item 1). Let $x,y\in A$ be such that A satisfies $\varphi_{M_0}(x,y)$ and xy or $x+y$ is not in C. On the one hand, if xy is not in C then x_1^2 is not in C. On the other hand, if $x+y$ is not in C then $x_2^2-x_1^2-1$ is not in C, hence one of x_1^2 and x_2^2 is not in C. Therefore, the sequence $(x_1,\dots,x_{M_0})$ is a Büchi sequence with at least one term non-constant and by hypothesis, there exists $f\in A$ such that

$$x_n^2=(f+n)^{p^s+1}$$

for some non-negative integer s. Therefore we have a system of equations in x and y

$$\begin{cases} xy=(f+1)^{p^s+1}\\ x+y=(f+2)^{p^s+1}-(f+1)^{p^s+1}-1\end{cases}$$

whose unique solutions are

$$(x,y)=(f+1,(f+1)^{p^s})\qquad\text{and}\qquad(x,y)=((f+1)^{p^s},f+1)$$

(the verification is easy and is left to the reader). Hence either $y=x^{p^s}$ or $x=y^{p^s}$, i.e. $R_A(x,y)$ holds. □

Proof of Theorem 4.1.10. Within this proof, "transcendental" will always mean "transcendental over C", and "algebraic" will always mean "algebraic over C".

The positive existential formula from the language $\mathcal{L}_T = \{0, 1, +, \cdot, T\}$

$$\begin{aligned}\varphi_{\mathcal{C}}^T(x,y)\colon\ &((T(xy) \vee T(x+y)) \wedge \varphi_{M(\mathcal{C})}(x,y)) \vee \\ &\exists u \exists v((T(uv) \vee T(u+v)) \wedge \varphi_{M(\mathcal{C})}(ux,vy) \wedge \varphi_{M(\mathcal{C})}(u,v))\end{aligned}$$

uniformly defines R_A in $\mathcal{C}$ over $\mathcal{L}_T$.

Indeed, if $R_A(x,y)$ holds then there exists an integer s such that $y = x^{p^s}$. If either xy or $x+y$ is transcendental then A satisfies

$$(T(xy) \vee T(x+y)) \wedge \varphi_{M(\mathcal{C})}(x,y),$$

by Theorem 4.1.8. If none of xy and $x+y$ is transcendental then choose u transcendental and $v = u^{p^s}$ if $s \geq 0$, or choose v transcendental and $u = v^{p^{-s}}$ if $s < 0$. For these choices of u and v, A satisfies

$$(T(uv) \vee T(u+v)) \wedge \varphi_{M(\mathcal{C})}(ux,vy) \wedge \varphi_{M(\mathcal{C})}(u,v).$$

Suppose now that A satisfies $\varphi_{\mathcal{C}}^T(x,y)$. If A satisfies

$$(T(xy) \vee T(x+y)) \wedge \varphi_{M(\mathcal{C})}(x,y)$$

then $R_A(x,y)$ holds by Theorem 4.1.8. If not then there in particular both of xy and $x+y$ are algebraic, hence both of x and y are algebraic. Also there exist $u, v \in A$ such that

- uv or $u+v$ is transcendental (hence u or v is transcendental);
- there exists $r \in \mathbb{Z}$ such that $v = u^{p^r}$ (by Theorem 4.1.8 and the previous item); and
- A satisfies $\varphi_{M(\mathcal{C})}(ux,vy)$.

Note that the first and second items imply that both u and v are transcendental.

Suppose that x or y is not 0 (otherwise $R_A(x,y)$ holds trivially).
Case 1: If $uxvy$ or $ux+vy$ is transcendental then, by the third item and Theorem 4.1.8, there exists $s \in \mathbb{Z}$ such that $vy = (ux)^{p^s}$, hence none of x and y is 0 and

$$u^{p^r} y = (ux)^{p^s},$$

which implies

$$yu^{p^r-p^s} = x^{p^s}$$

and therefore, $r = s$ (since u is transcendental but none of x and y is transcendental nor 0). Hence $R_A(x, y)$ holds.

Case 2: If both $uxvy$ and $ux + vy$ are algebraic then both ux and vy are algebraic, hence they are 0 (since u and v are transcendental but x and y are algebraic), which contradicts the fact that x or y is non-zero.

This finishes the proof of Item 1 of Theorem 4.1.10.

Let us prove Item 2, namely, let us prove that the positive existential formula $\varphi^z_{\mathcal{C}}(x, y)$ from the language $\mathcal{L}_z = \{0, 1, +, \cdot, z\}$

$$\varphi^z_{\mathcal{C}}(x, y) \colon \varphi_{M(\mathcal{C})}(x, y) \vee \exists u(\varphi_{M(\mathcal{C})}(z, u) \wedge (\varphi_{M(\mathcal{C})}(zx, uy) \vee \varphi_{M(\mathcal{C})}(ux, zy)))$$

uniformly defines R_A in $\mathcal{C}$ over $\mathcal{L}_z$.

Suppose first that $R_A(x, y)$ holds. There exists an integer s such that $y = x^{p^s}$. If $s \geq 0$, then by taking $u = z^{p^s}$ the formula $\varphi_{M(\mathcal{C})}(zx, uy)$ holds in A by Theorem 4.1.8. If $s \leq 0$, then by taking $u = z^{p^{-s}}$ the formula $\varphi_{M(\mathcal{C})}(ux, zy)$ holds in A by Theorem 4.1.8.

Suppose now that A satisfies $\varphi^z_{\mathcal{C}}(x, y)$. If xy or $x + y$ is transcendental then as A satisfies $\varphi_{M(\mathcal{C})}(x, y)$ we are done by Theorem 4.1.8. So suppose that both xy and $x + y$ are algebraic (hence both x and y are algebraic).

Suppose that A satisfies

$$\exists u(\varphi_{M(\mathcal{C})}(z, u) \wedge \varphi_{M(\mathcal{C})}(zx, uy))$$

(the other case is done similarly). Since A satisfies $\varphi_{M(\mathcal{C})}(z, u)$ and z is transcendental (hence zu or $z + u$ is transcendental), by Theorem 4.1.8, there exists an integer r such that

$$u = z^{p^r} \tag{4.21}$$

and in particular u is transcendental. Note that if both x and y are 0 then we are done. So we may assume that one of the two is non-zero.

Case 1: If $uy + zx$ or $uyzx$ is transcendental, as A satisfies $\varphi_{M(\mathcal{C})}(zx, uy)$, there exists an integer k such that $uy = (zx)^{p^k}$ by Theorem 4.1.8. In particular, none of x and y is 0. By Equation (4.21) we have $z^{p^r}y = (zx)^{p^k}$, hence

$$z^{p^r-p^k}y = x^{p^k}$$

which implies $k = r$ (since x and y are algebraic and non-zero and z is transcendental) and the result follows.

Case 2: If both $uy + zx$ and $uyzx$ are algebraic then both uy and zx are algebraic, which is impossible since u and z are transcendental, x and y are algebraic, and at least one of x or y is non-zero. □

Proof of Theorem 4.1.11. Consider the positive existential $\mathcal{L}_T$-formulas

$$\psi_1(x,y)\colon \exists x_1 \dots \exists x_{M(\mathcal{C})} \left((T(x_1^2) \vee T(x_2^2 - x_1^2 - 1)) \wedge \varphi_0(x_1, \dots, x_{M(\mathcal{C})}, x, y) \right).$$

and

$$\psi_{\mathcal{C}}^T(x,y)\colon \psi_1(x,y) \vee \psi_1(y,x)$$

where φ_0 is defined at the beginning of this section (note that we have replaced M_0 by $M(\mathcal{C})$ in the definition of φ_0).

Let $x, y \in A$ be such $R_A^C(x,y)$ holds. By definition of R_A^C we have $y = x^{p^s}$ for some integer s. As in the proof of Theorem 4.1.8, if $s \geq 0$, taking $x_n \in A$ such that

$$x_n^2 = (x - 1 + n)^{p^s + 1}$$

the formula

$$\varphi_0(x_1, \dots, x_{M(\mathcal{C})}, x, y)$$

is satisfied in A by Lemma 4.6.1. Analogously if $s \leq 0$ then by taking

$$x_n^2 = (y - 1 + n)^{p^{-s} + 1}$$

the formula

$$\varphi_0(x_1, \dots, x_{M(\mathcal{C})}, y, x)$$

is true in A by Lemma 4.6.1. Let us show that with these elections of the x_n, the structure A satisfies

$$T(x_1^2) \vee T(x_2^2 - x_1^2 - 1).$$

Suppose that it is not the case (i.e. x_1^2 and $x_2^2 - x_1^2 - 1$ are in C) and that $s \geq 0$. By Lemma 4.6.1, $xy = x_1^2$ and

$$x + y = x_2^2 - x_1^2 - 1$$

are in C, hence

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

is in C and we deduce that

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

is in C. By hypothesis on C, it follows that $x - y \in C$, hence also

$$2x = (x+y) + (x-y)$$

is in C and

$$2y = (x+y) - (x-y)$$

is in C. Therefore, again by hypothesis on C, x and y are in C, which gives a contradiction. Hence A satisfies $\psi_1(x,y)$. Similarly, if $s \leq 0$ then A satisfies $\psi_1(y,x)$. Hence A satisfies $\psi_{\mathcal{C}}^T(x,y)$.

Suppose that A satisfies $\psi_{\mathcal{C}}^T(x,y)$. Since the sequence $(x_1, \ldots, x_{M(\mathcal{C})})$ is a Büchi sequence with either x_1^2 or x_2^2 not in C, hence either x_1 or x_2 is not in C, and since $\mathcal{C}$ is a Büchi class, there exists $f \in A$ such that

$$x_n^2 = (f+n)^{p^s+1}$$

for some non-negative integer s. We conclude as in the proof of Theorem 4.1.8. □

4.7 Uniform encoding of the natural numbers

In this section we will prove Theorem 4.1.17.

Let us call an algorithm *identity algorithm* if it returns the input data.

Proof of Item 1 of Theorem 4.1.17. We want to prove that the pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{N})$ is uniformly encodable in the pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^*}, \mathcal{Z})$. Following the strategy described in Section 4.3, we will follow the "One step encoding process" for natural numbers, for the language $\mathcal{L} = \mathcal{L}^*$, the class $\mathcal{U} = \mathcal{N}$ and where the set X is $\{\cdot\}$.

The following algorithm $\mathcal{A}$ uniformly encodes $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{N})$ in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^* \cup X}, \mathcal{Z}^X)$ (hence Item 1 of the process is fullfiled): given a sentence F in $\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}$, replace each occurrence in F of $\exists x$ by $\exists x \geq 0$ (or more formally "$\exists x(\mathrm{pos}(x) \wedge$" and taking care of where should close the parenthesis). It is clear that F is true in $(\mathbb{N}; 0, 1, +, \cdot)$ if and only if $\mathcal{A}(F)$ is true in $(\mathbb{Z}; 0, 1, +, \cdot, \geq 0, |_p)$.

By Corollary 4.4.9, multiplication is $\mathcal{L}^*$-uped in the class $\mathcal{Z}$, hence also Item 2 is fulfilled. □

Proof of Item 2 of Theorem 4.1.17. We want to prove that the pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{N})$ is uniformly encodable in the pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^{*,+}}, \mathcal{N})$. Following the strategy described in Section 4.3, we will follow the "One step encoding process" for natural numbers, for the language $\mathcal{L} = \mathcal{L}^{*,+}$, the class $\mathcal{U} = \mathcal{N}$ and where the set X is $\{\cdot\}$. Item 1 of the process comes trivially in this case: the required algorithm to uniformly encode $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{N})$ in

$$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^{*,+}\cup X}, \mathcal{N}^X)$$

is the identity algorithm, because a formula in $\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}$ is true in $(\mathbb{N}; 0, 1, +, \cdot)$ if and only if it is true in $\mathfrak{N}_p^X = (\mathbb{N}; 0, 1, +, \cdot, |_p)$. Item 2 asks for multiplication to be $\mathcal{L}^{*,+}$-uped in the class $\mathcal{N}$, but this is Item 1 of Theorem 4.1.13. □

Proof of Item 3 of Theorem 4.1.17. We want to prove that the pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{N})$ is uniformly encodable in the pair

$$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_{z,\mathrm{ord},\neq}}, \Omega)$$

where Ω has been defined in Notation 4.1.12. We will follow the "two steps encoding process" for natural numbers, where

- $\mathcal{L} = \mathcal{L}^*$ and $\mathcal{U} = \mathcal{N}$
- $\mathcal{A}_0$ is the algorithm that uniformly encodes $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{N})$ in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^{*,+}}, \mathcal{N})$
- $\mathcal{L}' = \mathcal{L}_{z,\mathrm{ord},\neq}$ and $\mathcal{V} = \Omega$
- $\mathcal{U}_{\mathrm{ind}} = \{\mathfrak{N}_p \colon p \in \mathcal{P}\}$, where $\mathcal{P}$ is the set of primes for which there exists at least one structure in Ω of characteristic p.
- Ω is partitionned into subclasses $\Omega_{\mathfrak{N}_p}$ where $\Omega_{\mathfrak{N}_p}$ is the class of all structures in Ω of characteristic p.
- Y is the set of symbols $\{R, S\}$
- R is interpreted in each $\mathcal{L}_{z,\mathrm{ord},\neq}$-structure $\mathfrak{U}$ of Ω by the relation $R_{\mathfrak{U}}$ defined by "$R_{\mathfrak{U}}(x, y)$ if and only if there exists an integer s such that $y = x^{p^s}$", where p is the characteristic of $\mathfrak{U}$
- $S(x, y)$ is interpreted in each $\mathfrak{U}$ in Ω as "$\mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}}(y)$" (recalling that to each structure in Ω is associated exactly one local parameter z at a prime divisor $\mathfrak{p}$ - see Notation 4.1.12)

We will apply Proposition 4.3.12 for each prime number in $\mathcal{P}$. Fix such a prime p. Following the notation of Proposition 4.3.12, consider:

- $\mathcal{L}_0 = \{1, z, \cdot, R\}$
- $\mathcal{L}_1 = \mathcal{L}_0 \cup \{S\}$
- $\mathcal{U}_0^p = \Omega^{*,\mathrm{reg}}_{\mathfrak{N}_p}$ is the class of $\mathcal{L}_0$-structures with base set $\{f \in U \colon f \neq 0 \text{ and } \mathrm{ord}_{\mathfrak{p}}(f) \geq 0\}$ as U ranges among the base sets of structures of characteristic p in Ω, and where R is interpreted as $R_{\mathfrak{U}}$ restricted to $U \setminus \{0\}$. Note that there can be more than one structure in $\mathcal{U}_0$ with a given base set (depending on the choice of the local parameter).
- $\mathcal{U}_1^p$ is the class of $\mathcal{L}_1$-structures obtained from $\mathcal{U}_0^p$ when interpreting $S(x, y)$ by "$\mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}}(y)$".
- $\mathfrak{W}^p$ is the $(\mathfrak{N}_p, j)$-induced $\mathcal{L}_0$-structure, where $j \colon \mathcal{L}^{*,+} \to \mathcal{L}_0$ is the bijection

α	0	1	$+$	R
$j(\alpha)$	1	z	$\cdot$	R

- For each $\mathfrak{U}$ in $\mathcal{U}_0^p$, let $f_{\mathfrak{U}} \colon \mathfrak{U} \to \mathfrak{W}^p$ be the map that sends $x \in \mathfrak{U}$ to its order at $\mathfrak{p}$.

Let us prove that the hypothesis of Proposition 4.3.12 are satisfied. First, $f_{\mathfrak{U}}$ is trivially a morphism for each $\mathfrak{U}$ in $\mathcal{U}_0^p$, and it is onto because in each structure in $\mathcal{U}_0^p$ we have only regular functions.

Let us prove that $f_{\mathfrak{U}}$ is relation-onto. Let $x_1, x_2 \in \mathfrak{U}$ be such that

$$\mathrm{ord}_{\mathfrak{p}}(x_1) \mid_p \mathrm{ord}_{\mathfrak{p}}(x_2).$$

Taking

$$u_1 = z^{\mathrm{ord}_{\mathfrak{p}}(x_1)} \qquad \text{and} \qquad u_2 = z^{\mathrm{ord}_{\mathfrak{p}}(x_2)},$$

we have $u_1 \sim_{f_{\mathfrak{U}}} x_1$ and $u_2 \sim_{f_{\mathfrak{U}}} x_2$ and $R^{\mathfrak{U}}(u_1, u_2)$ holds.

The collection of relations $\sim_{f_{\mathfrak{U}}}$ is trivially $\mathcal{L}_1$-uped in $\mathcal{U}_1^p$. Therefore, we can apply Proposition 4.3.12 to obtain the algorithm $\mathcal{A}_p = \mathcal{A}$ that actually does not depend on p.

At this point we have the algorithms $\mathcal{A}_0$, $\mathcal{A}^{\mathcal{L}^0}_{\mathcal{L}^{*,+}}$ and $\mathcal{A}$.

Let $\mathcal{A}'$ be the algorithm that transforms an $\mathcal{L}_1$-sentence into a sentence over the language $\mathcal{L}_{z,\mathrm{ord},\neq} \cup Y$ by replacing each occurrence of the form Qx,

where Q is a quantifier, by $Qx \neq 0$. It is clear that for each $\mathcal{L}_1$-sentence F and for each $\mathfrak{U}$ in the class $\mathcal{U}_1^p$, the corresponding structure in $\Omega^Y_{\mathfrak{N}_p}$ satisfies $\mathcal{A}'(F)$ if and only if $\mathfrak{U}$ satisfies F.

In order to conclude, it is now enough to give uniform positive existential $\mathcal{L}_{z,\mathrm{ord},\neq}$-definitions of the elements of $Y = \{R, S\}$ in the class Ω.

For the symbol R, this is Item 2 of Theorem 4.1.10. The positive existential formula

$$\exists u, v(x = uy \wedge y = vx \wedge \mathrm{ord}(u) \wedge \mathrm{ord}(v))$$

uniformly $\mathcal{L}_{z,\mathrm{ord},\neq}$-defines S in the class Ω.

Schematically, following the "two steps encoding process", we performed:

$$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{N}) \xrightarrow{\mathcal{A}_0} (\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^{*,+}}, \mathcal{N}) \supseteq (\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^{*,+}}, \{\mathfrak{N}_p \colon p \in \mathcal{P}\}) \xrightarrow{\mathcal{A}^{\mathcal{L}_0}_{\mathcal{L}^{*,+}}} (\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_0}, \{\mathfrak{W}^p \colon p \in \mathcal{P}\})$$

$$\xrightarrow{\mathcal{A}} \left(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_1}, \bigcup_{p\in\mathcal{P}} \Omega^{*,\mathrm{reg}}_{\mathfrak{N}_p}\right) \xrightarrow{\mathcal{A}'} \left(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_{z,\mathrm{ord},\neq\cup Y}}, \bigcup_{p\in\mathcal{P}} \Omega^{Y}_{\mathfrak{N}_p}\right) \xrightarrow{\mathcal{A}^{R,S}_Y} (\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_{z,\mathrm{ord},\neq}}, \Omega)$$

□

Proof of Item 4 of Theorem 4.1.17. This comes immediately from Proposition 4.3.3 and Item 4 of Theorem 4.1.17. □

4.8 Uniform encoding of $\mathbb{Z}$ in the language $\mathcal{L}_T$

In this section we will prove Theorem 4.1.19.

Proof of Item 1 of Theorem 4.1.19. We want to prove that $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{Z})$ is uniformly encodable in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^*}, \mathcal{Z})$. We proceed as in the proof of Item 2 of Theorem 4.1.17 (following the "one step encoding process") with $\mathcal{L} = \mathcal{L}^*$, $\mathcal{U} = \mathcal{Z}$ and $X = \{\cdot\}$. Multiplication is $\mathcal{L}^*$-uped in the class $\mathcal{Z}$ by Item 3 of Theorem 4.1.13. □

Proof of Item 2 of Theorem 4.1.19. We prove that $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{Z})$ is uniformly encodable in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^*_T}, \mathcal{D})$. Follow the "one step encoding process") with $\mathcal{L} = \mathcal{L}^*_T$, $\mathcal{U} = \mathcal{D}$ and $X = \{\cdot\}$. Multiplication is $\mathcal{L}^*_T$-uped in the class $\mathcal{D}$ by Item 2 of Theorem 4.1.13. □

Proof of Item 3 of Theorem 4.1.19. We prove that $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{Z})$ is uniformly encodable in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_T}, \mathcal{C})$, where $\mathcal{C}$ is the class of all polynomial rings over a field of odd positive characteristic.

We will first follow the "two steps encoding process" to uniformly encode $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{Z})$ in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^*_T}, \mathcal{Q})$, with

- $\mathcal{L} = \mathcal{L}^*_T$ and $\mathcal{U} = \mathcal{D}$
- $\mathcal{A}_0$ is the algorithm that uniformly encodes $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{Z})$ in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^*_T}, \mathcal{D})$
- $\mathcal{L}' = \mathcal{L} = \mathcal{L}^*_T$ and $\mathcal{V} = \mathcal{Q}$
- $\mathcal{U}_{\mathrm{ind}} = \mathcal{U}$
- $\mathcal{Q}$ is partitionned into one-element subsets $\{\mathfrak{Q}_p\}$
- Y has only one symbol β
- β is interpreted in each $\mathcal{L}^*_T$-structure $\mathfrak{Q}_p$ of $\mathcal{Q}$ as "$\beta((u, v))$ if and only if $v = 1$".

Note that β is $\mathcal{L}^*_T$-uped in $\mathcal{Q}$ by Lemma 4.5.3. In this context $\mathcal{B}'$ is the algorithm that transforms each occurrence of Qx in an $\mathcal{L}^*_T$-sentence by $Qx(\beta x)\wedge$ (with the usual abuse of notation). Schematically, we have:

$$(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}, \mathbb{Z}) \xrightarrow{\mathcal{A}_0} (\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}}, \mathcal{D}) = (\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}}, \mathcal{D}_{\mathrm{ind}})$$

$$\xrightarrow{\mathcal{B}'} \left(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}\cup Y}, \bigcup_p \{\mathfrak{Q}_p\}^Y \right) \xrightarrow{\mathcal{A}^\beta_Y} (\mathcal{A}^\beta_Y(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}\cup Y}), \mathcal{Q}) \subseteq (\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}}, \mathcal{Q}).$$

We will now use Proposition 4.3.5 with

- $\mathcal{G} = \mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_A}$ and $\mathfrak{M} = \mathbb{Z}$
- $\mathcal{G}' = \mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^*_T}$ and $\mathcal{U} = \mathcal{Q}$
- $\mathcal{G}'' = \mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_T}$ and $\mathcal{V} = \mathcal{C}$
- $\mathcal{U}_{\mathrm{ind}} = \mathcal{U}$
- $\mathcal{C}$ is partitioned into subclasses $\mathcal{C}_{\mathfrak{Q}_p}$, where $\mathcal{C}_{\mathfrak{Q}_p}$ is the class of all polynomial rings of characteristic p.

In order to conclude we need to find an algorithm $\mathcal{B}$ such that for each $\mathfrak{Q}_p \in \mathcal{Q}$, the pair $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}^*_T}, \mathfrak{Q}_p)$ is uniformly encodable in $(\mathcal{F}^{\mathrm{pe}}_{\mathcal{L}_T}, \mathcal{C}_{\mathfrak{Q}_p})$. Fix a prime p and let

$$F = Q_1 u_1 \dots Q_n u_n G(u_1, \dots, u_n)$$

be an $\mathcal{L}^*_T$-sentence in normal prenex form (in our case we need only to consider existential quantifiers, but the whole proof actually goes through when universal quantifiers are allowed).

Write $G^1, \dots, G^m$ the atomic formulas that appear in F and let us describe the algorithm (following the syntax as in Cori and Lascar [CL]):

1. **Term by term substitution of constants and function symbols.** In each term of G, formally replace (in the following order)

   (a) each occurrence of 0 by $(1, 0)$;

   (b) each occurrence of 1 by $(\alpha, 1)$, for some new (fixed) variable α;

   (c) each u_i by (v_i, w_i), for some new (fixed) variables v_i and w_i;

   (d) each string of the form $(x, y) + (x', y')$ by

   $$(xx' - (\alpha^2 - 1)yy', xy' + x'y)$$

   until the whole term becomes a single pair.

   Call G_0 the word resulting from G, and $G^1_0, \dots, G^m_0$ the words resulting from the corresponding atomic formulas $G^1, \dots, G^m$.

2. **Substitution of the relation symbols: first component**:

   (a) In G_0, delete any of the G^1_i (and its corresponding connective if any) where appears $|$ or T.

   (b) Replace each pair by its first component.

   (c) Replace each $R(x, x')$ by the formula $\Delta(\alpha, x, x')$ from Lemma 4.5.9 and write

   $$G_1(\alpha, u_1, \dots, u_n, v_1, \dots, v_n)$$

   the resulting $\mathcal{L}_T$-formula.

3. **Substitution of the relation symbols: second component**:

   (a) In G_0, delete any of the G^1_i (and its corresponding connective if any) where appears R.

(b) Replace each pair by its second component.

(c) Replace each $x \mid y$ by $\exists t(y = tx)$ (and don't do anything to T) and write

$$G_2(\alpha, u_1, \ldots, u_n, v_1, \ldots, v_n)$$

the resulting $\mathcal{L}_T$-formula.

4. Define $\mathcal{B}(F)$ as

$$Q_1 u_1 Q_1 v_1 \ldots Q_n u_n Q_n v_n \exists \alpha \left(T(\alpha) \wedge G_1 \wedge G_2 \wedge \bigwedge_{i=1}^{n} \delta(\alpha, u_i, v_i) \right)$$

Observe that one of G_1 and G_2 must be non-empty: if no relations except equality appear in G, then we did not delete anything, and if a relation that is not equality appears in G then it can be deleted only in one of G_1 or G_2.

The algorithm $\mathcal{B}$ works thanks to Lemma 4.5.6.

□

Chapter 5

Conclusión - Conclusion

5.1 Conclusión

A continuación presentamos una lista de problemas que aparecen de forma natural a raíz del presente trabajo.

Con respecto al Capítulo 3:

1. Bajar las cotas en los Teoremas 3.2.3 y 3.2.1.

2. Estudiar el problema de representacion de cuadrados por polinomios de segundo grado sobre

   (a) el campo de las funciones meromorfas p-ádicas sobre un disco; o

   (b) algún anillo de funciones meromorfas p-ádicas en característica positiva.

3. Consideremos el siguiente enunciado: "Dados A anillo conmutativo unitario, un entero $k \geq 2$ y un conjunto $S \subseteq A$, si un polinomio $f \in A[X]$ de grado k representa potencias k-ésimas para *demasiados* valores de X en S, entonces f es una potencia k-ésima, salvo un conjunto *pequeño* de excepciones". Convertir este enunciado en algo preciso (dependiendo del caso) y estudiarlo en algunos anillos A (por ejemplo: si A es un anillo de polinomios, S es su campo base y $k \geq 3$, o A es un anillo de funciones análiticas etc.).

4. Sea $K/\mathbb{Q}$ un campo de números. Fijamos ocho elementos $a_1, \ldots, a_8$ de K y definimos el conjunto $E \subseteq K[X]$ de polinomios mónicos de segundo grado $f \in K[X]$ que no son cuadrados pero sus valores en los a_i son cuadrados. Demuestre o refute: *E es finito.* Si la afirmación fuera cierta para alguna elección de K y de los a_i, entonces se obtendría un nuevo ejemplo no-trivial donde la pregunta de Bombieri tiene respuesta positiva. Por otro lado, si la afirmación es falsa para alguna elección de K y de los a_i entonces tendríamos un contra-ejemplo a la conjetura de Bombieri-Lang.

Con respecto al Capítulo 4:

1. Encontrar una clase de campos de funciones racionales de característica positiva, con infinitas características distintas, y donde el orden se puede definir uniformemente sobre el lenguaje $\mathcal{L}_z$ (o mostrar que no existe tal clase).

2. Bajar las cotas sobre las características.

3. Demuestre o refute que existe una definición uniforme para la multiplicación sobre la clase de estructuras $\mathbb{F}_p$ sobre el lenguaje $\{0, 1, +, P_2\}$, donde $P_2(x)$ se interpreta en cada $\mathbb{F}_p$ por "x es un cuadrado" (al parecer no es difícil mostrar que no existe una definición positiva existencial - ver la demostración de la Proposición 4.1.5 en la Sección 4.2).

4. Extender los resultados sobre el símbolo "$\neq$" en el Lema 4.1.3 a clases más amplias de anillos de funciones algebraicas.

5.2 Conclusion

Here is a short list of problems which naturally arise from this work.

With respect to Chapter 3:

1. Lower the bounds in Theorems 3.2.3 and 3.2.1.

2. Study the problem of representation of squares by degree two polynomials over

   (a) the field of p-adic meromorphic functions over a disc; or

(b) some ring of p-adic meromorphic functions in positive characteristic.

3. Consider the following statement: "Given a commutative unitary ring A, an integer $k \geq 2$ and a subset $S \subseteq A$, if a polynomial $f \in A[X]$ of degree k represents a k-th power for *too many* values of X in the set S, then f itself is a k-th power, up to a *small* set of exceptions". Make the statement precise (depending on the case) and study it for some rings A (for example: if A is a ring of polynomials, S is its ring of constants and $k \geq 3$, or A is a ring of analytic functions, and so on).

4. Let $K/\mathbb{Q}$ be a number field, take eight elements $a_1, \ldots, a_8$ of K and define the set $E \subseteq K[X]$ of monic second degree polynomials $f \in K[X]$ that are not squares but take square values at the a_i's. Prove or disprove: *E is finite*. If one would prove this for some choice of K and the a_i's, then one would obtain a new non-trivial example where Bombieri's question has a positive answer. If one would disprove it for some choice of K and the a_i's, then one would get a counter-example to Bombieri-Lang conjecture.

With respect to Chapter 4:

1. To find a class of rational function fields in positive characteristic, with infinitely many distinct characteristics, where we can define uniformly the order over the language $\mathcal{L}_z$ (or show that there is no such class).

2. Lower the bounds on the characteristic.

3. Prove or disprove that there is a uniform definition of multiplication for the class of structures $\mathbb{F}_p$ over the language $\{0, 1, +, P_2\}$, where $P_2(x)$ is interpreted in each $\mathbb{F}_p$ by "x is a square" (it does not seem too difficult to prove the non-existence of a positive existential definition - see the proof of Proposition 4.1.5 in Section 4.2).

4. Extend the result about $\neq$ in Lemma 4.1.3 to bigger classes of rings of algebraic functions.

Bibliography

[Al] D. Allison, *On square values of quadratics*, Math. Proc. Camb. Philos. Soc. **99-3**, 381-383 (1986).

[Ax] J. Ax, *Solving diophantine problems modulo every prime*, Annals of Mathematics **85-2**, 161-183 (1967).

[AxK12] J. Ax and S. Kochen, *Diophantine problems over finite fields I and II*, American Journal of Mathematics **87-3**, 605-648 (1965).

[AxK3] J. Ax and S. Kochen, *Diophantine problems over finite fields III*, Annals of Mathematics **83-3**, 437-456 (1966).

[Ber] W. Berkovich, *Spectral theory and analytic geometry over non-Archimedean fields*, Math. Surveys and Monographs, Coll. Amer. Math Soc. (1990).

[Bre] A. Bremner, *On square values of quadratics*, Acta Arith. **108-2**, 95-111 (2003).

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

[CDM] Z. Chatzidakis, L. van den Dries and A. Macintyre, *Definable sets over finite fields*, J. reine u. ang. Math. **427**, 107-135 (1992).

[CHr] Z. Chatzidakis and E. Hrushovski, *Asymptotic theories of differential fields*, Illinois Journal of Mathematics **47-3**, 593-618 (2003).

[ChY] 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).

[CL] R. Cori and D. Lascar *Logique mathématique 1 - Calcul propositionnel; algèbre de Boole; calcul des prédicats*, Masson - Collection Axiomes (1993). ISBN : 2-225-84079-2.

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

[De1] J. Denef, *The Diophantine Problem for polynomial rings and fields of rational functions*, Transactions of the American Mathematical Society, **242** 391-399 (1978).

[De2] —— *The diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium 78, M. Boffa, D. van Dalen, K. McAloon (eds.), North Holland, 131-145 (1979).

[Ei] K. Eisenträger, *2003-Hilbert's tenth problem for algebraic function fields of characteristic 2*, Pacific Journal of Mathematics, **210-2** 261-281 (2003).

[ES] K. Eisenträger and A. Shlapentokh, *Undecidability in Function Fields of Positive Characteristic*, International Mathematics Research Notices (2009) 2009:4051-4086.

[Es] A. Escassut, *Analytic elements in p-adic analysis*, World Scientific (1995).

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

[Hr] E. Hrushovski, *The elementary theory of the Frobenius automorphisms*, http://arxiv.org/pdf/math.LO/0406514 (2006).

[HY] P. C. Hu and C. C. Yang, *Meromorphic functions over non-Archimedean fields*, Mathematics and Its Applications 522, Kluwer Academic Publishers, 2000. MR 1794326 — Zbl 0984.30027

[KR] K.H. Kim and F.W. Roush, *Diophantine unsolvability for function fields over certain infinite fields of positive characterisitic p*, Journal of Algebra, **152-1** 230-239 (1992).

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

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

[Mac] A. Macintyre, *Nonstandard Frobenius*, In preparation.

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

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

[MB] L. Moret-Bailly, *Sur la dfinissabilit existentielle de la non-nullit dans les anneaux*, Algebra and Number Theory **1-3**, 331-346 (2007).

[Na] M. B. Nathanson, *Elementary Methods in Number Theory*, Springer, Graduate Texts in Mathematics, **195** (2000).

[Nav] J. A. Navarro, *Álgebra conmutativa básica* (2010). Downloadable from http://matematicas.unex.es/∼navarro/ACB.pdf

[O] C. Osgood, *A number theoretic-differential equations approach to generalizing Nevanlinna theory*, Indian J. of Math. 23 (1981), 1-15.

[P] H. Pasten, *Extensiones del problema de Büchi a distintas estructuras y potencias más altas*, Tesis del Departamento de Matemática de la Universidad de Concepción (2010) http://dmat.cfm.cl/colloquium-tesis.php.

[PPV] H. Pasten, T. Pheidas and X. Vidaux, *A survey on Büchi's problem: new presentations and open problems*, to appear as Proceedings of the Hausdorff Institute of Mathematics, in Zapiski POMI, Steklov Institute of Mathematics, and in the Journal of Mathematical Sciences (2010).

[Ph1] T. Pheidas, *An undecidability result for power series rings of positive characteristic II*, Proceedings of the American Mathematical Society **100-3**, 526-530 (1987).

[Ph2] T. Pheidas, *Hilbert's Tenth Problem for fields of rational functions over finite fields*, Inv. Math. **103**, 1-8 (1991).

[Ph3] —— *Endomorphisms of elliptic curves and undecidability in function fields of positive characteristic*, Journal of Algebra **273-1**, 395-411 (2004).

[PV1] T. Pheidas and X. Vidaux, *The analogue of Büchi's problem for rational functions*, Journal of The London Mathematical Society **74-3**, 545-565 (2006).

[PV2] —— *Corrigendum: The analogue of Büchi's problem for rational functions*, Journal of The London Mathematical Society, to appear in the Journal of the London Mathematical Society.

[PZ1] T. Pheidas and K. Zahidi, *Undecidable existential theories of polynomial rings and function fields*, Communications in Algebra, **27-10** 4993-5010 (1999).

[PZ2] T. Pheidas and K. Zahidi, *Undecidability of existential theories of rings and fields: A survey*, Contemporary Mathematics **270**, 49-106 (1999).

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

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

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

[Ru] M. Ru, *A note on p-adic Nevanlinna Theory*, Proceedings of the American Mathematical Society, **129(5)**, 1263-1269 (2000).

[Rum] R. Rumely, *Undecidability and definability for the theory of global fields*, Transactions of the American Mathematical Society, **262-1** 195-217 (1980).

[S1] A. Shlapentokh, *Diophantine Undecidability over Algebraic Function Fields over Finite Fields of Constants*, Journal of Number Theory **58** 317-342 (1996).

[S2] A. Shlapentokh, *Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic*, Pacific Journal of Mathematics **193-2** (2000).

[S3] —— *Hilbert's tenth problem - Diophantine classes and extensions to global fields*, New Mathematical Monographs **7**, Cambridge University Press (2007).

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

[Vi] 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).

[Vo1] P. Vojta, *Diophantine Approximations and Value Distribution Theory, Lecture Notes in Mathematics 1239*, Springer-Verlag, 1987.

[Vo2] —— *Diagonal quadratic forms and Hilbert's Tenth Problem*, Contemporary Mathematics **270**, 261-274 (2000).

[Vo3] —— *Diophantine Approximation and Nevanlinna Theory*, available on line http://math.berkeley.edu/∼vojta/cime/cime.pdf