Universidad de Concepción
Dirección de Postgrado
Facultad de Ciencias Físicas y Matemáticas -Programa de Magíster en Matemática

# Potencias en subsucesiones de progresiones aritméticas en anillos de funciones y un problema de indecidibilidad

# (Powers in subsequences of arithmetic progressions in rings of functions and a problem of undecidability)

NATALIA CRISTINA GARCÍA FRITZ
CONCEPCIÓN-CHILE
2011

Profesor Guía: Xavier Vidaux
Dpto. de Matemática, Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Universidad de Concepción
Dirección de Postgrado
Facultad de Ciencias Físicas y Matemáticas -Programa de Magíster en Matemática

# Potencias en subsucesiones de progresiones aritméticas en anillos de funciones y un problema de indecidibilidad

# (Powers in subsequences of arithmetic progressions in rings of functions and a problem of undecidability)

Xavier Vidaux (profesor guía de tesis)
Pablo Sáez (evaluador externo, miembro del jurado)
Andrea Tironi (evaluador interno, miembro del jurado)
Carlos Videla (evaluador externo, miembro del jurado)

TESIS DEFENDIDA EL 15 DE ABRIL DE 2011

NATALIA CRISTINA GARCÍA FRITZ
CONCEPCIÓN-CHILE
2011

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

# Potencias en subsucesiones de progresiones aritméticas en anillos de funciones y un problema de indecidibilidad

Natalia García
Universidad de Concepción

**Agradecimientos**

En primer lugar quiero agradecer a mi profesor guía, Xavier Vidaux, por todo el tiempo que me dedicó durante el desarrollo de esta tesis, por su paciencia, y por las buenas conversaciones que me ayudaron a orientar el trabajo de manera de alcanzar estos resultados.

También quiero agradecer a Pablo Sáez, Andrea Tironi y Carlos Videla por aceptar corregir esta tesis a pesar del poco tiempo disponible y por sus muy útiles sugerencias que me ayudaron a mejorar la matemática y la escritura de este trabajo.

Gracias al Departamento de Matemática de la Universidad de Concepción por entregarme la preparación para llegar a esta instancia, en especial a José Aguayo, César Flores y Antonio Laface, quienes con su entusiasmo me motivaron a estudiar otros temas de interés en matemática más allá de los contenidos de los cursos que estoy segura que me servirán durante mis futuros estudios y toda mi carrera.

Agradezco a mi familia por fomentar en mí el deseo de aprender y por apoyarme incondicionalmente en esta y en las demás metas que me he trazado en la vida. Sin ellos no habría podido llegar a este punto.

Gracias a Héctor Pastén por recomendarme leer el paper de Hajdu que me ha traído tantas sorpresas, y por estar ahí siempre que necesitaba contarle a alguien sobre mis avances en este trabajo, incluso antes de revisar si estaban correctos. Te quiero mucho.

# Contents

# Introducción y Resultados Principales

Esta tesis consiste de dos teoremas principales (Teoremas 2 y 6) de la aritmética de polinomios y algunas consecuencias en Lógica Matemática.

Un corolario simple de deducir de nuestro teorema principal, inspirado por un paper sobre potencias en progresiones aritméticas de Hajdu [10], establece que en particular, dado cualquier campo $F$,

*la cantidad $a\lambda+b$, donde $a$ y $b$ son polinomios coprimos en $F[t]$, no puede ser una potencia en $F[t]$ para más de $M = 4$ valores distintos de $\lambda \in F$, a menos que $a$ y $b$ tengan derivada nula.*

Aquí por *potencia*, nos referimos a *una potencia $k$-ésima para algún $k \geq 2$*. Este corolario fue en realidad nuestro primer resultado e inspiró el resto de la tesis. Por un lado, uno podría naturalmente tratar de generalizarlo de las siguientes maneras:

1. ¿Es la condición de coprimalidad realmente necesaria? Si no, ¿qué tan *pequeño* debería ser el máximo común divisor de $a$ y $b$ de manera de asegurar la existencia de un $M$? (suponiendo que mientras más factores en común tienen $a$ y $b$, mayor será $M$);

2. ¿Qué ocurre en otros anillos de funciones? (tales como subanillos de campos de funciones, anillos de funciones analíticas o meromorfas, ...);

3. ¿Qué ocurre al considerar expresiones de la forma $a\lambda^2 + b\lambda + c$ en vez de $a\lambda + b$? ¿Y para exponentes superiores?

En el trabajo aquí presentado, tratamos las generalizaciones del tipo 1 (Teorema 2) y del tipo 3 (Teorema 6).

Por otro lado, el enunciado anterior y sus posibles generalizaciones *deberían* decir algo sobre el lenguaje de primer orden $\mathcal{L}_P = \{0, 1, +, P\}$ (o lenguajes que lo contengan), donde $P$ es un predicado de relación unaria en el cual $P(x)$ se interpreta como "$x$ es una potencia".

Hasta donde nos ha sido posible averiguar, este lenguaje no ha sido estudiado previamente por lógicos (aunque el lenguaje de Macintyre [12] está un tanto relacionado, pues contiene un predicado $P^k$ para cada $k \geq 2$ interpretado como "$P^k(x)$ si y sólo si $x$ es una potencia $k$-ésima"). Sin embargo,

el estudio de potencias consecutivas y potencias en progresiones aritméticas sobre los enteros tiene una larga historia. En 1640, Fermat conjeturó que no hay 4 cuadrados en progresión aritmética, y esto fue demostrado posteriormente por Euler. Unos siglos después, en 1844, Catalan [3] conjeturó que las únicas potencias consecutivas son 8 y 9. En 1997, Darmon y Merel [6] demostraron que no hay tres potencias $k$-ésimas en progresión aritmética con $k$ mayor o igual que 3, completando el estudio de progresiones aritméticas formadas por potencias del mismo exponente. Actualmente, los estudios se están enfocando en progresiones aritméticas formadas por potencias sin la restricción de tener el mismo exponente. En 2004, Hajdu [10] demostró bajo la conjetura ABC que si

$$(x_1^{l_1}, x_2^{l_2}, \ldots, x_k^{l_k})$$

es una progresión aritmética con $x_1$ y $x_2$ coprimos y $l_i \geq 2$ para cada $i$, entonces $k$ y $\max\{l_i\}$ están acotados (sin depender de los $x_i$). El también demostró, incondicionalmente, que si existe una constante $C$ mayor que cualquier $l_i$, entonces $k$ está acotado.

A continuación presentamos algunas notaciones antes de establecer nuestros resultados principales.

**Notación 1.** *1. Si $F$ es un campo, denotamos por $\tilde{F}$ a la clausura algebraica de $F$.*

*2. Si $a$ es un polinomio, denotamos por $a'$ la derivada formal de $a$ y $\deg(a)$ el grado de $a$.*

*3. Si $a$ y $b$ son polinomios a coeficientes en un campo $F$, denotamos por $\gcd(a,b)$ al máximo común divisor (mónico) de $a$ y $b$ en $F$, y $\operatorname{lcm}(a,b)$ al mínimo común múltiplo (mónico) de $a$ y $b$ en $F$.*

*4. Si $r$ es un número real, la notación $\lceil r \rceil$ se refiere a la función techo aplicada a $r$ (es decir, el menor entero que es mayor o igual que $r$).*

*5. Dados $a, b \in F[t]$, escribimos*

$$\gamma(a,b) = \frac{\deg(\gcd(a,b))}{\max\{\deg(a), \deg(b)\}}$$

*al cual llamamos* el índice de coprimalidad de $a$ y $b$. *Notemos que $0 \leq \gamma(a,b) \leq 1$ mide precisamente que tan coprimos son $a$ y $b$: si $\gamma(a,b)$ es cercano a 0, entonces $a$ y $b$ tienen pocos factores en común, y si*

*$\gamma(a,b)$ es cercano a 1, entonces a y b tienen muchos factores en común. Observemos que $\gamma(a,b)$ no varia con el campo de base considerado (ya que el máximo común divisor sólo depende del campo primo de $F$).*

6. *Si $a$ y $b$ son polinomios tales que $\gamma = \gamma(a,b) < \frac{1}{2}$, denotamos*

$$M(a,b) = \begin{cases} \left\lceil \frac{1}{1-2\gamma} \right\rceil + 1 & \text{si } a' = 0 \\ \left\lceil \frac{1}{1-2\gamma} \right\rceil + 2 & \text{si } b' = 0 \\ \left\lceil \frac{3}{1-2\gamma} \right\rceil + 1 & \text{si } a' \neq 0 \text{ y } b' \neq 0. \end{cases}$$

*Observe que la condición sobre $\gamma$ implica que $M(a,b)$ es positivo.*

Ahora estamos en condiciones de establecer nuestro primer teorema principal.

**Teorema 2.** *Sea $F$ un campo. Sean $a, b \in F[t]$ polinomios no nulos tales que*

1. *el cuociente $\frac{a}{b}$ no tiene derivada nula; y*
2. *alguno entre $a$ o $b$ tiene derivada no nula.*

*Si $\gamma(a,b)$ es estrictamente menor que $\frac{1}{2}$ entonces la expresión $a\lambda + b$ es una potencia en $F[t]$ para a lo más $M(a,b)$ valores distintos de $\lambda$ en $F$.*

En el Lema 19 verificamos que dado cualquier número real $\gamma$ tal que

$$0 \leq \gamma < \frac{1}{2}$$

tenemos

$$\left\lceil \frac{3}{1-2\gamma} \right\rceil + 1 > \left\lceil \frac{1}{1-2\gamma} \right\rceil + 2 > \left\lceil \frac{1}{1-2\gamma} \right\rceil + 1,$$

y por lo tanto podemos reemplazar en el Teorema 2 la cota $M(a,b)$ por

$$\left\lceil \frac{3}{1-2\gamma} \right\rceil + 1$$

que depende sólo de $\gamma$. Por lo tanto tenemos una cota que solamente depende del índice de coprimalidad. No sabemos que tan optimales son nuestras cotas.

Observemos que en característica cero, la condición que la derivada de $\frac{a}{b}$ es distinta de 0 se cumple trivialmente cuando $\gamma(a,b) < 1$. También observemos que si $F$ es algebraicamente cerrado y $a' = b' = 0$, entonces para cada $\lambda \in F$ la expresión $a\lambda + b$ es potencia, independientemente de la característica. Por lo tanto no podemos eliminar la hipótesis "alguno entre $a$ y $b$ tiene derivada no nula". Finalmente, observemos que para un campo algebraicamente cerrado $F$ (de cualquier característica), si $a$ es potencia y $\frac{a}{b}$ es constante, entonces $a\lambda + b$ es potencia en $F[t]$ independientemente del valor de $\lambda \in F$.

El siguiente teorema muestra que, en característica positiva, la hipótesis que la derivada de $\frac{a}{b}$ debe ser distinta de cero no puede ser reemplazada por la hipótesis "el cuociente $\frac{a}{b}$ no es constante".

**Teorema 3.** *Dado un entero positivo $n$ y un número real positivo $\varepsilon$, hay infinitos números primos $p$ tales que en cualquier campo $K$ de característica $p$, existen polinomios $a$ y $b$ en $K[t]$ tales que*

1. *$a' \neq 0$ y $b' \neq 0$;*
2. *$\frac{a}{b}$ no es constante;*
3. *$\gamma(a,b) < \varepsilon$; y*
4. *$a\lambda + b$ es potencia para $n$ valores de $\lambda$ en $K$.*

Cuando $a$ y $b$ son coprimos, obtenemos el siguiente corolario a partir del Teorema 2 (observando que la condición $(\frac{a}{b})' \neq 0$ se cumple trivialmente cuando $a$ y $b$ son coprimos, incluso en característica positiva).

**Corolario 4.** *Sea $F$ un campo. Sean $a, b \in F[t]$ polinomios coprimos. En el conjunto $\{a\lambda + b : \lambda \in F\}$ hay a lo más*

*i.* 4 *potencias, si $a'$ y $b'$ son no nulos;*

*ii.* 3 *potencias, si $a' \neq 0$ y $b' = 0$; y*

*iii.* 2 *potencias, si $a' = 0$ y $b' \neq 0$.*

Antes de establecer nuestro segundo teorema principal, hagamos notar una consecuencia del corolario 4 en Lógica Matemática: si $F$ es algebraicamente cerrado entonces la siguiente $\mathcal{L}_P$-fórmula

$$\mathrm{der}_1(x)\colon \bigwedge_{n=1}^{4} P(n+x)$$

es cierta en $F[t]$ si y sólo si $x$ tiene derivada nula. Luego, la propiedad de "tener derivada nula" es definible sin cuantificadores en $F[t]$, de forma uniforme en la característica. Usando el teorema de Mason-Stothers, mostramos en la sección 5 que la siguiente fórmula más simple $\mathrm{der}(x)$ también define esta propiedad.

**Proposición 5.** *Sea $F$ un campo algebraicamente cerrado. La $\mathcal{L}_P$-fórmula (libre de cuantificadores)*

$$\mathrm{der}(x)\colon P(x) \wedge P(x+1)$$

*define a los polinomios con derivada nula en el anillo de polinomios $F[t]$.*

En particular, para característica 0, la proposición anterior muestra que las constantes son definibles (sin cuantificadores) en el lenguaje $\mathcal{L}_P$ en cualquier anillo de polinomios sobre un campo algebraicamente cerrado.

Enunciamos ahora nuestro segundo teorema principal[1] (demostrado en la Sección 4).

**Teorema 6.** *Sea $F$ un campo, y $b$ y $c$ polinomios a coeficientes en $F$. En el caso de característica positiva, suponemos que $b''c' - b'c''$ es distinto de cero. Si $b$ o $c$ no es constante, entonces la expresión $\lambda^2 + b\lambda + c$ es un cubo o una potencia de exponente mayor para a lo más 12 valores de $\lambda$ en $F$.*

Es imposible no poner en paralelo nuestro resultado con la siguiente versión fuerte de la solución del problema de Büchi para anillos de polinomios en característica cero (ver una discusión del problema de Büchi al final de la introducción).

[1] Al momento de imprimir esta tesis, Prof. Andrea Tironi nos sugirió una manera de debilitar la hipótesis de este teorema en el caso de característica positiva - la versión de la tesis que será sometida a publicación contendrá esta versión más fuerte de este teorema.

**Teorema 7.** *Sea $F$ un campo de característica 0, y $b$ y $c$ polinomios sobre $F$, al menos uno de ellos no constante. Si para $M = 8$ valores distintos de $\lambda \in F$ la cantidad $\lambda^2+b\lambda+c$ es un cuadrado en $F[t]$, entonces es un cuadrado como un polinomio en la variable $\lambda$.*

De hecho, este teorema es también válido para funciones meromorfas complejas (así como para campos de números, y también para campos de funciones en característica 0, pero con una cota $M$ que depende del género) en lugar de polinomios y fue demostrado por H. Pasten, después de la solución de P. Vojta al problema de Büchi para esos campos. También hay una versión de este teorema por H. Pasten para funciones meromorfas complejas $p$-ádicas (ver [15, 26]).

Combinando los teoremas 6 y 7, obtenemos lo siguiente:

**Corolario 8.** *Sea $F$ un campo de característica 0, y $b$ y $c$ polinomios a coeficientes en $F$, al menos uno de ellos no constante. Si para 20 valores distintos de $\lambda \in F$ la cantidad $\lambda^2 + b\lambda + c$ es una potencia en $F[t]$, entonces es un cuadrado como polinomio en la variable $\lambda$.*

Este corolario implica lo que necesitamos para obtener nuevos resultados de indecidibilidad sobre algunos lenguajes que contienen $\mathcal{L}_P$, porque implica el siguiente teorema "en el estilo Büchi".

**Teorema 9.** *Sea $F$ un campo de característica 0 y $(q_n)_{q=1}^{20}$ una sucesión de polinomios con segunda diferencia igual a la sucesión constante (2). Si todos los $q_n$ son potencias entonces, o todos los $q_n$ son constantes, o existe $q \in F[t]$ tal que $q_n = (q + n)^2$ para cada $n$.*

De hecho, como la sucesión $(q_n)$ de polinomios tiene segunda diferencia (2), existen $b, c \in F[t]$ tales que

$$q_n = n^2 + bn + c.$$

Como los $q_n$ no son todos constantes, entonces $b$ o $c$ no es constante. Del corolario 8, como los $q_n$ son todos potencias, $\lambda^2+\lambda b+c$ es un cuadrado como polinomio en $\lambda$. Por lo tanto, el polinomio $\lambda^2+\lambda b+c$ es de la forma $r(\lambda+q)^2$ con $q, r \in F[t]$, y el teorema se demuestra porque el coeficiente de $\lambda$ es 1 (por lo tanto $r = 1$).

Para poder obtener resultados de indecidibilidad a partir del Teorema 9, utilizamos resultados de indecidibilidad basados en la insolubilidad del

*Décimo Problema de Hilbert*, demostrado por Martin Davis, Yuri Matiyasevich, Hilary Putnam y Julia Robinson [13, 7]. El Décimo Problema de Hilbert era el siguiente:

**(H10)** *Encontrar un algoritmo para decidir si un sistema arbitrario de ecuaciones diofantinas tiene o no solución en los enteros.*

Por *ecuación diofantina*, nos referimos a una ecuación polinomial sobre los enteros (con grado y número de variables arbitrarios). Éste problema es insoluble porque un algoritmo como el que se pide no existe. En términos lógicos, esto significa que la teoría positiva existencial de $\mathbb{Z}$ en el lenguaje de anillos (de primer orden) $\mathcal{L}_R = \{0, 1, +, \cdot\}$ es indecidible (es decir, no existe un algoritmo para decidir si un enunciado positivo existencial sobre los enteros, escrito sólo con símbolos para la suma, multiplicación, 0 y 1, es cierto en $\mathbb{Z}$ - *positivo existencial* significa que el enunciado es equivalente a uno con sólo cuantificadores existenciales, todos al comienzo, y sin negación).

¿Cómo se pueden obtener resultados de indecidibilidad basándonos en lo anterior? Vamos a recordar rápidamente dos maneras clásicas de hacer esto. Supongamos que $\mathcal{L}$ es un lenguaje que contiene $\mathcal{L}_R$ y sea $\mathcal{M}$ una $\mathcal{L}$-estructura. De esto, $\mathcal{M}$ es un anillo (posiblemente con más estructura). Por ejemplo, si $(F[t]; 0, 1, +, \cdot)$ es un anillo de polinomios, entonces podemos considerar la estructura $(F[t]; 0, 1, +, \cdot, t)$, donde $t$ juega un papel similar a 0 y 1, en el sentido que es un elemento específico de $F[t]$ que consideramos ser parte de la estructura. La $\mathcal{L}$-teoría positiva existencial de $\mathcal{M}$ es el conjunto de enunciados positivo-existenciales que pueden ser escritos usando sólamente símbolos de $\mathcal{L}$. En el ejemplo anterior, $\exists y \exists z(y^2 + yz = t)$ es un enunciado de este tipo. Para poder mostrar que la teoría positiva existencial de $\mathcal{M}$ en $\mathcal{L}$ es indecidible, es suficiente demostrar que $\mathbb{Z}$ es positivo existencialmente definible en $\mathcal{M}$, lo que significa que existe un enunciado $\phi(x)$ sobre $\mathcal{L}$, con una variable libre $x$, que es cierta si y sólo si $x$ pertenece a $\mathbb{Z}$. Esto porque si existiera un algoritmo para decidir si un enunciado sobre $\mathcal{L}$ fuese cierto en $\mathcal{M}$, entonces utilizando el enunciado $\phi(x)$, habría un algoritmo para resolver H10. De hecho, tendríamos:

"Existen $x_1, \ldots, x_n$ en $\mathbb{Z}$ tales que $P(x_1, \ldots, x_n) = 0$."

es equivalente a

"Existen $y_1, \ldots, y_n$ en $\mathcal{M}$ tales que $P(y_1, \ldots, y_n) = 0$ y $\phi(y_j)$ es cierto en $\mathcal{M}$ para cada $j$."

Esto contradice la insolubilidad de H10.

Supongamos ahora que se sabe que la $\mathcal{L}$-estructura $\mathcal{M}$ tiene teoría positiva existencial indecidible. Si uno puede definir de manera positiva existencial la interpretación en $\mathcal{M}$ de algún símbolo $s$ de $\mathcal{L}$ usando sólamente los símbolos de $\mathcal{L} \setminus \{s\}$, entonces utilizando un argumento análogo al dado anteriormente, uno obtiene la indecidibilidad de la teoría positiva existencial de $\mathcal{M}$ vista como una $\mathcal{L} \setminus \{s\}$-estructura. Esto es precisamente lo que hacemos en esta tesis. Para un survey de resultados de extensiones y análogos de H10, ver por ejemplo [9].

Antes de enunciar nuestros resultados de definibilidad/indecidibilidad, debemos establecer más notaciones.

**Notación 10.** *Nos referiremos a los siguientes lenguajes de primer orden:*

- $\mathcal{L}_R = \{0, 1, +, \cdot\}$ *es el lenguaje de anillos.*
- $\mathcal{L}_R^t = \mathcal{L}_R \cup \{f_t\}$ *y* $\mathcal{L}_P^t = \mathcal{L}_P \cup \{f_t\}$*, donde* $f_t$ *es un símbolo de función unaria de multiplicación por el elemento trascendental* $t$*.*
- $\mathcal{L}_R^T = \mathcal{L}_R \cup \{T\}$ *y* $\mathcal{L}_P^T = \mathcal{L}_P \cup \{T\}$*, donde* $T$ *es un símbolo de relación unaria. Interpretaremos* $T(x)$ *por "*$x$ *no es un polinomio constante" (lenguaje introducido por L. Rubel [22]).*

Siguiendo el método de Büchi (ver Sección 6), no es muy difícil deducir el siguiente teorema a partir del Teorema 9.

**Teorema 11.** *Si* $F[t]$ *es un anillo de polinomios sobre un campo* $F$ *de característica* 0*, entonces la multiplicación es definible de manera positiva existencial sobre los lenguajes* $\mathcal{L}_P^t$ *y* $\mathcal{L}_P^T$*.*

Como la teoría positiva existencial de $F[t]$ sobre los lenguajes $\mathcal{L}_R^t$ y $\mathcal{L}_R^T$ son indecidibles (ver Denef [8] para $\mathcal{L}_R^t$, y Pheidas y Zahidi [21] para $\mathcal{L}_R^T$), y como $T$ es $\mathcal{L}_P$-definible en $F[t]$ (por la Proposición 5, la fórmula $\neg P(x) \vee \neg P(x+1)$ define los polinomios no constantes), finalmente obtenemos:

**Teorema 12.** *Sea* $F$ *un campo de característica* 0*. La teoría positiva existencial de* $F[t]$ *es indecidible sobre* $\mathcal{L}_P^t$ *y sobre* $\mathcal{L}_P^T$*.*

**Teorema 13.** *Si* $F$ *es un campo algebraicamente cerrado de característica* 0 *entonces la teoría de* $F[t]$ *sobre* $\mathcal{L}_P$ *es indecidible.*

No sabemos si la hipótesis "$F$ algebraicamente cerrado" puede ser eliminada en el Teorema 13.

En vista de los teoremas demostrados en este trabajo sería bueno obtener análogos del Teorema 6 para cualquier anillo para el cual el análogo del Teorema 7 ha sido demostrado, o se cree que sea cierto. Pero si estamos interesados sólo en las implicaciones en lógica, lo que realmente necesitamos son análogos del Teorema 9, que son algún tipo de generalizaciones del problema de Büchi. Lo mencionamos a continuación:

**Problema de Büchi** ($\mathbf{B^k}$) *Sea $k$ un entero mayor o igual que 2. Sea $A$ un anillo de funciones de característica 0, y $B$ un subanillo de $A$. Existe un entero $M$, tal que si una sucesión de largo $M$ formada por potencias $k$-ésimas en $A$ tiene diferencia $k$-ésima igual a la sucesión constante $(k!)$ entonces, o es una sucesión de potencias consecutivas, o es una secuencia de elementos de $B$.*

Usualmente, para $B$ se puede elegir el campo de *constantes* (en campos de funciones, funciones meromorfas, etc).

Terminamos esta introducción con un breve survey de resultados sobre el problema de Büchi, para motivar a seguir investigando de manera de obtener análogos del Teorema 9 en otras estructuras y para potencias más altas.

El problema de Büchi para funciones meromorfas complejas y para $k = 2$ fue resuelto en primer lugar por P. Vojta [26] en 2001. El Problema ($\mathbf{B^k}$) para funciones racionales fue también resuelto por Pheidas y Vidaux para $k = 2$ (con un método que da una cota menos buena, pero que funciona también en característica positiva, y que inspiró algunas de las demostraciones de esta tesis - cabe destacar que en característica positiva el problema de Büchi debe ser formulado de una manera un poco distinta) y para $k = 3$ (ver [18, 19, 20], y ver [17] donde el problema es introducido. Debemos mencionar que un versión más débil del problema ($\mathbf{B^k}$) (llamado problema de Hensley) fue resuelto para cualquier $k$ por Pasten [14] para polinomios en característica 0, y por Shlapentokh y Vidaux [24] para campos de funciones (en característica positiva, ellos sólo obtienen el problema de Büchi para cuadrados, pero es fácil deducir de su teorema principal la solución al problema de Hensley, usando una versión del teorema de Mason para campos de funciones). Notar también que han sido anunciados varios resultados por Julie Tzu-Yueh Wang, Ta Thi Haoi An y Hsiu-Lien Huang, donde los títulos sugieren que ellos resolvieron el problema de Hensley para funciones meromorfas (J. T. Y. Wang y T. T.

H. An) y campos de funciones (J. T. Y. Wang) y el problema de Büchi para cubos sobre campos de funciones (J. T. Y. Wang y H. L. Huang). Ver [1].

Hay muchos otros resultados fuertemente relacionados a estos problemas (por ejemplo sobre el problema de Büchi - o sus implicaciones en lógica - para subanillos de campos de números) que podríamos citar aquí, pero mejor sugeriremos a los lectores interesados ver más detalles en el survey [16] y desde una perspectiva diferente en el paper [2].

# Introduction and Main Results

This thesis consists of two main theorems (Theorems 2 and 6) on the arithmetic of polynomials and some consequences in Mathematical Logic.

A simple corollary of our first main theorem, inspired by a paper on powers in arithmetic progressions by Hajdu [10], states in particular that given any field $F$

*the quantity $a\lambda+b$, where $a$ and $b$ are coprime polynomials in $F[t]$, cannot be a power in $F[t]$ for more than $M = 4$ distinct values of $\lambda \in F$, unless both $a$ and $b$ have zero derivative.*

Here by *power*, we mean *a $k$-th power for some $k \geq 2$*. This corollary was actually our very first result and inspired the rest of the thesis. On the one hand, one could naturally try to generalize it in the following ways:

1. Is the condition on coprimality really necessary? If not, how *small* should the degree of the greatest common divisor of $a$ and $b$ be in order to ensure the existence of an $M$ (guessing that the more $a$ and $b$ have factors in common, the bigger should be $M$);

2. What about other rings of functions? (such that subrings of function fields, rings of analytic or meromorphic functions, ...)

3. What about considering expressions of the form $a\lambda^2 + b\lambda + c$ instead of $a\lambda + b$? What about higher powers?

In the work presented here, we deal with generalizations of type 1 (Theorem 2) and of type 3 (Theorem 6).

On the other hand, the statement above and its possible generalizations *should* say something about the first order language $\mathcal{L}_P = \{0, 1, +, P\}$ (or languages containing $\mathcal{L}_P$), where $P$ is a unary relation symbol and $P(x)$ is interpreted as "$x$ is a power".

Though to the best of our knowledge this language has not been previously studied by logicians (though Macintyre's language [12] is somewhat related to it, as it contains a predicate $P^k$ for each $k \geq 2$ interpreted as "$P^k(x)$ if and only if $x$ is a $k$-th power"), the study of consecutive powers and powers in arithmetic progression over the integers has a long history. In 1640, Fermat conjectured that there does not exist four squares in arithmetic progression, and this was proved later on by Euler. A few centuries

later, in 1844, Catalan [3] conjectured that the only consecutive powers are 8 and 9. In 1997, Darmon and Merel [6] proved that there does not exist three $k$-th powers in arithmetic progression with $k$ greater than or equal to 3, completing the study of arithmetic progressions formed by powers with the same exponent. Nowadays, the study is focusing in arithmetic progressions formed by powers without the restriction of having the same exponent. In 2004, Hajdu [10] proved under the ABC conjecture that if

$$(x_1^{l_1}, x_2^{l_2}, \ldots, x_k^{l_k})$$

is an arithmetic progression with $x_1$ and $x_2$ coprime and $l_i \geq 2$ for every $i$, then $k$ and $\max\{l_i\}$ are bounded (not depending on the $x_i$). He also proves, unconditionally, that if there exists a constant $C$ greater than every $l_i$, then $k$ is bounded.

Let us introduce some notation before we state our main results.

**Notation 1.** *1. If $F$ is a field, we denote by $\tilde{F}$ the algebraic closure of $F$.*

2. *If $a$ is a polynomial, we will write $a'$ for the formal derivative of $a$ and* $\deg(a)$ *for the degree of $a$.*

3. *If $a$ and $b$ are polynomials over a field $F$, we write* $\gcd(a,b)$ *for the (monic) greatest common divisor of $a$ and $b$ in $F$, and* $\operatorname{lcm}(a,b)$ *for the (monic) least common multiple of $a$ and $b$ in $F$.*

4. *If $r$ is a real number, the notation $\lceil r \rceil$ will refer to the ceiling function applied to $r$ (this is the smallest integer which is greater than or equal to $r$).*

5. *Given $a, b \in F[t]$, we will write*

$$\gamma(a,b) = \frac{\deg(\gcd(a,b))}{\max\{\deg(a), \deg(b)\}}$$

*and refer to it as to* the index of coprimality of $a$ and $b$. *Observe that $0 \leq \gamma(a,b) \leq 1$ measures precisely how far are $a$ and $b$ of being coprime: the closer $\gamma(a,b)$ is to 0, the less factors $a$ and $b$ have in common, and the closer $\gamma(a,b)$ is to 1, the more factors $a$ and $b$ have in common. Note that $\gamma(a,b)$ does not vary with the base field considered (as the greatest common divisor depends only on the prime field of $F$).*

*6. If $a$ and $b$ are polynomials such that $\gamma = \gamma(a,b) < \frac{1}{2}$, we let*

$$M(a,b) = \begin{cases} \left\lceil \frac{1}{1-2\gamma} \right\rceil + 1 & \text{if } a' = 0 \\ \left\lceil \frac{1}{1-2\gamma} \right\rceil + 2 & \text{if } b' = 0 \\ \left\lceil \frac{3}{1-2\gamma} \right\rceil + 1 & \text{if } a' \neq 0 \text{ and } b' \neq 0. \end{cases}$$

*Observe that the condition on $\gamma$ implies that $M(a,b)$ is positive.*

We are now in condition to state our first main theorem.

**Theorem 2.** *Let $F$ be a field. Let $a, b \in F[t]$ be non-zero polynomials such that*

1. *the quotient $\frac{a}{b}$ has non-zero derivative; and*
2. *either $a$ or $b$ has non-zero derivative.*

*If $\gamma(a,b)$ is strictly less than $\frac{1}{2}$, then the expression $a\lambda + b$ is a power in $F[t]$ for at most $M(a,b)$ distinct values of $\lambda$ in $F$.*

In Lemma 19 we will verify that for any real number $\gamma$ such that

$$0 \leq \gamma < \frac{1}{2}$$

we have

$$\left\lceil \frac{3}{1-2\gamma} \right\rceil + 1 > \left\lceil \frac{1}{1-2\gamma} \right\rceil + 2 > \left\lceil \frac{1}{1-2\gamma} \right\rceil + 1,$$

hence we could replace in Theorem 2 the bound $M(a,b)$ by the quantity

$$\left\lceil \frac{3}{1-2\gamma} \right\rceil + 1$$

which depends only on $\gamma$. So we do have actually a bound that is uniform up to the index of coprimality. We do not know how far our bounds are from being optimal.

Observe that in characteristic zero, the condition on the derivative of $\frac{a}{b}$ to be distinct from 0 is trivially satisfied when $\gamma(a,b) < 1$. Also observe that if

$F$ is algebraically closed and $a' = b' = 0$, then for every $\lambda \in F$ the expression $a\lambda + b$ is a power, independently of the characteristic. Hence we cannot take out the hypothesis "either $a$ or $b$ has non-zero derivative". Finally, observe that for $F$ an algebraically closed field (of any characteristic), if $a$ is a power and $\frac{a}{b}$ is constant, then $a\lambda + b$ is a power in $F[t]$ independently of the value of $\lambda \in F$.

Next theorem shows that, in positive characteristic, the hypothesis that the derivative of $\frac{a}{b}$ must be distinct from zero cannot be replaced by the hypothesis "the quotient $\frac{a}{b}$ is non-constant".

**Theorem 3.** *Given a positive integer $n$ and a positive real number $\varepsilon$, there are infinitely many primes $p$ such that in any field $F$ of characteristic $p$, there exist polynomials $a$ and $b$ in $F[t]$ such that*

1. *$a' \neq 0$ and $b' \neq 0$;*
2. *$\frac{a}{b}$ is non-constant;*
3. *$\gamma(a, b) < \varepsilon$; and*
4. *$a\lambda + b$ is a power for $n$ values of $\lambda$ in $F$.*

When $a$ and $b$ are coprime, we obtain the following statement as an immediate corollary of Theorem 2 (observing that the condition $(\frac{a}{b})' \neq 0$ is automatically fulfilled when $a$ and $b$ are coprime, even in positive characteristic).

**Corollary 4.** *Let $F$ be a field. Let $a, b \in F[t]$ be coprime polynomials. In the set $\{a\lambda + b \colon \lambda \in F\}$ there are at most*

*i.* *4 powers, if $a'$ and $b'$ are non-zero;*

*ii.* *3 powers, if $a' \neq 0$ and $b' = 0$; and*

*iii.* *2 powers, if $a' = 0$ and $b' \neq 0$.*

Before we state our second main theorem, we would like to point out an easy consequence of Corollary 4 in Mathematical Logic: if $F$ is algebraically closed then the following $\mathcal{L}_P$-formula

$$\mathrm{der}_1(x) \colon \bigwedge_{n=1}^{4} P(n + x)$$

is true in $F[t]$ if and only if $x$ has zero derivative. Hence, the property "to have zero derivative" is quantifier free $\mathcal{L}_P$-definable in $F[t]$, uniformly in the characteristic. Using Mason-Stothers Theorem, we will show in Section 5 that the following simpler formula $\mathrm{der}(x)$ also defines that property.

**Proposition 5.** *Let $F$ be an algebraically closed field. The $\mathcal{L}_P$ (quantifier free) formula*

$$\mathrm{der}(x)\colon P(x) \wedge P(x+1)$$

*defines the polynomials with zero derivative in the polynomial ring $F[t]$.*

So in particular in characteristic 0, the above proposition says that constants are (quantifier free) definable over the language $\mathcal{L}_P$ in any ring of polynomials over an algebraically closed field.

Let us now state our second main theorem[2] (proven in Section 4).

**Theorem 6.** *Let $F$ a field and $b$ and $c$ polynomials with coefficients in $F$. In the case of positive characteristic, assume that $b''c' - b'c''$ is non-zero. If $b$ or $c$ is non-constant then the expression $\lambda^2 + b\lambda + c$ is a cube or higher power for at most 12 values of $\lambda \in F$.*

It is impossible not to put in parallel our result with the following strong version of the solution to Büchi's problem for polynomial rings in characteristic zero (see a discussion on Büchi's problem at the end of the introduction).

**Theorem 7.** *Let $F$ be a field of characteristic 0 and $b$ and $c$ polynomials over $F$, at least one of them non-constant. If for $M = 8$ distinct values of $\lambda \in F$ the quantity $\lambda^2 + b\lambda + c$ is a square in $F[t]$, then it is a square as a polynomial in the variable $\lambda$.*

Indeed this theorem is valid for complex meromorphic functions (as well as for number fields, and also for function fields in characteristic 0 but with a bound $M$ that depends on the genus) instead of polynomials and it was proved by H. Pasten, after the solution by P. Vojta to Büchi's problem for those fields. There is also a version of this theorem by H. Pasten for $p$-adic complex meromorphic functions (see [15, 26]).

Combining Theorems 6 and 7, we obtain the following:

[2]Just before we print this thesis, Prof. Andrea Tironi suggested us a way to weaken the hypothesis of this theorem in the case of positive characteristic - the version of the thesis that will be submitted for publication will contain this stronger version of this theorem.

**Corollary 8.** *Let $F$ be a field of characteristic 0 and $b$ and $c$ polynomials with coefficients in $F$, at least one of them non-constant. If for 20 distinct values of $\lambda \in F$ the quantity $\lambda^2 + b\lambda + c$ is a power in $F[t]$, then it is a square as a polynomial in the variable $\lambda$.*

This corollary implies what we actually need in order to obtain new undecidability results over some languages containing $\mathcal{L}_P$, as it implies the following "Büchi-like theorem".

**Theorem 9.** *Let $F$ be a field of characteristic 0 and $(q_n)_{q=1}^{20}$ be a sequence of polynomials with second difference equal to the constant sequence (2). If all the $q_n$ are powers then either all the $q_n$ are in $F$, or there exists $q \in F[t]$ such that $q_n = (q+n)^2$ for each $n$.*

Indeed, since the sequence $(q_n)$ of polynomials has second difference (2), there exist $b, c \in F[t]$ such that

$$q_n = n^2 + bn + c.$$

Since the $q_n$ are not all constant, either $b$ or $c$ is non-constant. From Corollary 8, since the $q_n$ are all powers, $\lambda^2 + \lambda b + c$ is a square as a polynomial in $\lambda$. Therefore, the polynomial $\lambda^2 + \lambda b + c$ is of the form $r(\lambda + q)^2$ with $q, r \in F[t]$, and the theorem is proven because the coefficient of $\lambda$ is 1 (hence $r = 1$).

In order to obtain undecidability results from Theorem 9, we will use known undecidability results based on the unsolvability of *Hilbert's Tenth Problem* proved by Martin Davis, Yuri Matiyasevich, Hilary Putnam and Julia Robinson [13, 7]. Hilbert's Tenth Problem was the following:

**(H10)** *Find an algorithm to decide whether or not an arbitrary system of diophantine equations has an integer solution.*

By *diophantine equation*, we mean a polynomial equation over the integers (with arbitrary degree and number of variables). This problem is *unsolvable* because such an algorithm does not exist. In logical terms, this means that the positive existential theory of $\mathbb{Z}$ in the (first order) language of rings, $\mathcal{L}_R = \{0, 1, +, \cdot\}$, is undecidable (i. e., there is no algorithm to decide whether or not a positive existential statement about the integers, written only with symbols for addition, multiplication, 0 and 1, is true in $\mathbb{Z}$ - *positive existential* means that the statement is equivalent to one with only existential quantifiers, all in front, and no negation).

How can one obtain undecidability results based on the above? Suppose that $\mathcal{L}$ is a language that contains $\mathcal{L}_R$ and let $\mathcal{M}$ be an $\mathcal{L}$-structure. So $\mathcal{M}$ is indeed a ring with maybe some extra-structure. For example, if $(F[t]; 0, 1, +, \cdot)$ is a ring of polynomials, then we may consider the richer structure $(F[t]; 0, 1, +, \cdot, t)$, where $t$ is playing a role similar to that of 0 and 1, in the sense that it is a specific element of $F[t]$ that we consider as being *part* of the structure. The positive existential $\mathcal{L}$-theory of $\mathcal{M}$ is the set of positive existential statements that can be written using only symbols from $\mathcal{L}$. In the example, $\exists y \exists z(y^2 + yz = t)$ is such a statement. In order to show that the positive existential theory of $\mathcal{M}$ in $\mathcal{L}$ is undecidable, it is enough to show that $\mathbb{Z}$ is positive existentially definable in $\mathcal{M}$, which means that there exists a statement $\varphi(x)$ over $\mathcal{L}$, with one free variable $x$, which is true if and only if $x$ belongs to $\mathbb{Z}$. This is because if there would be an algorithm to decide whether or not a statement over $\mathcal{L}$ would be true in $\mathcal{M}$, then, using the statement $\varphi(x)$, there would be an algorithm to solve H10. Indeed, we would have:

"There exist $x_1, \ldots, x_n$ in $\mathbb{Z}$ such that $P(x_1, \ldots, x_n) = 0$"

is equivalent to

"There exist $y_1, \ldots, y_n$ in $\mathcal{M}$ such that $P(y_1, \ldots, y_n) = 0$ and $\varphi(y_j)$ is true in $\mathcal{M}$ for each $j$."

This would contradict the unsolvability of H10.

Suppose now that it is already known that the $\mathcal{L}$-structure $\mathcal{M}$ has undecidable positive existential theory. If one can define in a positive existential way the interpretation in $\mathcal{M}$ of some symbol $s$ of $\mathcal{L}$ using only symbols from $\mathcal{L} \setminus \{s\}$, then using an argument analogous to the one given above, one obtains the undecidability of the positive existential theory of $\mathcal{M}$ seen as an $\mathcal{L} \setminus \{s\}$-structure. This is precisely what we will do in this thesis. For a survey of results on extensions and analogues of H10, see for example [9].

Before we can state our undecidability results, we need to introduce a few more notation.

**Notation 10.** *We will refer to the following first order languages:*

- $\mathcal{L}_R = \{0, 1, +, \cdot\}$ *is the language of rings.*
- $\mathcal{L}_R^t = \mathcal{L}_R \cup \{f_t\}$ *and* $\mathcal{L}_P^t = \mathcal{L}_P \cup \{f_t\}$ *where* $f_t$ *is a symbol of unary function for multiplication by the transcendental element* $t$*.*

- $\mathcal{L}_R^T = \mathcal{L}_R \cup \{T\}$ *and* $\mathcal{L}_P^T = \mathcal{L}_P \cup \{T\}$*, where* $T$ *is a symbol of unary relation. We will interpret* $T(x)$ *as "*$x$ *is not a constant polynomial" (language introduced by L. Rubel [22]).*

Following Büchi's method (see Section 6), it is not too hard to derive the following theorem from Theorem 9.

**Theorem 11.** *If* $F[t]$ *is a polynomial ring over a field* $F$ *of characteristic* 0*, then multiplication is positive existentially definable over the languages* $\mathcal{L}_P^t$ *and* $\mathcal{L}_P^T$*.*

Since the positive existential theory of $F[t]$ over the languages $\mathcal{L}_R^t$ and $\mathcal{L}_R^T$ are undecidable (see Denef [8] for $\mathcal{L}_R^t$, and Pheidas and Zahidi [21] for $\mathcal{L}_R^T$), and because $T$ is $\mathcal{L}_P$-definable in $F[t]$ (from Proposition 5, the formula $\neg P(x) \vee \neg P(x+1)$ defines the non-constant polynomials), we finally obtain:

**Theorem 12.** *Let* $F$ *be a field of characteristic* 0*. The positive existential theory of* $F[t]$ *is undecidable over* $\mathcal{L}_P^t$ *and over* $\mathcal{L}_P^T$*.*

**Theorem 13.** *If* $F$ *is an algebraically closed field of characteristic* 0 *then the full theory of* $F[t]$ *over* $\mathcal{L}_P$ *is undecidable.*

We do not know whether the hypothesis on $F$ being algebraically closed can be removed in Theorem 13.

In view of the theorems proven above it would be nice to obtain analogues of Theorem 6 for whatever rings for which the analogue of Theorem 7 has been proven, or is believed to be true. But if we are only interested in the implications in logic, what we want really are analogues of Theorem 9, which are some kind of generalizations of Büchi's problem. Let us recall it now:

**Büchi's Problem** ($\mathbf{B^k}$) *Let* $k$ *be an integer greater than or equal to* 2*. Let* $A$ *be a ring of functions of characteristic* 0*, and* $B$ *a subring of* $A$*. Does there exist an integer* $M$*, such that if a sequence of length* $M$ *made of* $k$*-th powers in* $A$ *has* $k$*-th difference equal to the constant sequence* $(k!)$*, then either it is a sequence of consecutive powers or it is a sequence of elements of* $B$*.*

Usually, one can choose for $B$ the set of *constants* (in function fields, meromorphic functions etc).

We will finish this introduction with a quick survey of results about Büchi's Problem, as to motivate further research in order to obtain analogues of Theorem 9 in other structures and for higher powers.

Büchi's problem for complex meromorphic functions and for $k = 2$ was first solved by P. Vojta [26] in 2001. Problem $(\mathbf{B^k})$ for rational functions was also solved by Pheidas and Vidaux for $k = 2$ (with a method that gives a higher bound, but that works also in positive characteristic, and that inspired some of the proofs of this thesis - we should stress that in positive characteristic Büchi's problem has to be formulated in a slightly different way) and for $k = 3$ (see [18, 19, 20], and see [17] where the problem is introduced). We should mention that a weak version of Problem $(\mathbf{B^k})$ (called Hensley's problem) was solved for any $k$ by Pasten [14] for polynomials in characteristic 0, and by Shlapentokh and Vidaux [24] for function fields (in positive characteristic, they only obtain Büchi's Problem for squares, but it is easy to derive from their main theorem the solution to Hensley's problem, using a version of Mason's theorem for function fields). Also note that various new results are being announced by Julie Tzu-Yueh Wang, Ta Thi Haoi An and Hsiu-Lien Huang, where the titles suggest that they solve Hensley's problem for meromorphic functions (J. T. Y. Wang and T. T. H. An) and function fields (J. T. Y. Wang) and Büchi's problem for cubes over function fields (J. T. Y. Wang and H. L. Huang). See [1].

There are many other results highly related to these problems (for example around Büchi's problem - or its implications in logic - for subrings of number fields) and that we could have cited here, but we will rather suggest to the interested reader to look for further details in the survey [16], and from a different perspective in the paper [2].

# 1 Preliminaries

In this section we will state a few well known theorems that we will need in the thesis. For other general facts used in this work, we refer the reader to [11] for algebra, [4, 5] for basic facts about Logic, and [9] and [23] for more specific results on Hilbert's Tenth Problem.

We will use the following two theorems for the proof of Theorem 3.

**Theorem 14** (Chinese remainder theorem)**.** *Let $k \geq 2$. If $a_1, a_2, \ldots, a_k$ are integers and $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers, then there exists an integer $x$ such that*

$$x \equiv a_i \pmod{m_i}, \qquad i = 1, \ldots, k.$$

*If $x$ is any solution of this set of congruences, then an integer $y$ is also a solution if and only if*

$$x \equiv y \pmod{m_1 \cdots m_k}.$$

**Theorem 15** (Dirichlet's theorem on primes in arithmetic progressions)**.** *Let $a$ and $d$ be two positive integers. If $a$ and $d$ are coprime, then in the arithmetic progression*

$$an + d$$

*there are infinitely many primes.*

**Definition 16.** *Let $f \in F[t]$ and $K$ a splitting field of $f$ over $F$. We define the* radical *of $f$ (with respect to $K$)*

$$\mathrm{rad}(f) = \prod_{i=1}^{n} (x - a_i)$$

*where the $a_i$ are all the different zeros of $f$ in $K$.*

We will need (a weak version of) the following theorem for the proof of Proposition 5 (see [25] for a proof).

**Theorem 17** (Mason-Stothers Theorem)**.** *Let $F$ be a field. Let $a, b, c \in F[t]$ be relatively prime polynomials such that $a + b = c$. If $a'$, $b'$ and $c'$ are not all zero, then we have*

$$\max\{\deg(a), \deg(b), \deg(c)\} \leq \deg(\mathrm{rad}(abc)) - 1.$$

# 2 Polynomials in arithmetic progressions

This section is entirely dedicated to the proof of Theorem 2.

Fix a field $F$ and polynomials $a$ and $b$ in $F[t]$ for the whole section.

First observe that if $a\lambda+b$ is not a power in $\tilde{F}[t]$ for more than $M$ values of $\lambda$ in $\tilde{F}$, then it cannot be a power in $F[t]$ for more than $M$ values of $\lambda$ in $F$. Hence we can make the following assumption without loss of generality:

**Assumption 18.** *The field $F$ is algebraically closed.*

For the whole section, we suppose that the hypothesis of Theorem 2 are satisfied, namely,

1. either $a' \neq 0$ or $b' \neq 0$;
2. $\left(\frac{a}{b}\right)' \neq 0$; and
3. $\gamma(a,b) < \frac{1}{2}$;

and assume that there are $M$ distinct $\lambda \in F$ such that

$$a\lambda + b = x_\lambda^{k_\lambda} \tag{1}$$

for some polynomials $x_\lambda \in F[t]$ and some integers $k_\lambda \geq 2$. We shall prove that $M$ is smaller than $M(a,b)$ (see Notation 1).

**Lemma 19.** *For any real number $\gamma$ such that*

$$0 \leq \gamma < \frac{1}{2}$$

*we have*

$$\left\lceil \frac{3}{1-2\gamma} \right\rceil + 1 > \left\lceil \frac{1}{1-2\gamma} \right\rceil + 2 > \left\lceil \frac{1}{1-2\gamma} \right\rceil + 1.$$

*Proof.* We need only prove the first inequality. Note first that since

$$0 \leq \gamma < \frac{1}{2},$$

we have

$$0 < 1 - 2\gamma \leq 1$$

hence

$$\frac{3}{1-2\gamma} - \frac{1}{1-2\gamma} = \frac{2}{1-2\gamma} \geq 2.$$

So we have

$$\frac{3}{1-2\gamma} + 1 \geq \frac{1}{1-2\gamma} + 3,$$

hence, since the ceiling function is an increasing function we obtain

$$\begin{aligned}
\left\lceil \frac{3}{1-2\gamma} \right\rceil + 1 &= \left\lceil \frac{3}{1-2\gamma} + 1 \right\rceil \\
&\geq \left\lceil \frac{1}{1-2\gamma} + 3 \right\rceil \\
&= \left\lceil \frac{1}{1-2\gamma} \right\rceil + 3 \\
&> \left\lceil \frac{1}{1-2\gamma} \right\rceil + 2.
\end{aligned}$$

□

**Notation 20.** *From now on we will write $\gamma$ for $\gamma(a, b)$.*

Differentiating each side of Equation (1) we obtain

$$a'\lambda + b' = k_\lambda x_\lambda^{k_\lambda - 1} x'_\lambda. \tag{2}$$

Let $\lambda_1$, $\lambda_2$, …, $\lambda_M$ be $M$ distinct values of $\lambda$ for which $a\lambda + b$ is a power and write

$$d = \max\left\{\deg a, \deg b\right\}.$$

Note that $d$ is at least 1.

Since $\deg(a\lambda + b) = d$ excepting for at most one value of $\lambda$, we can assume that in the set

$$H = \{\lambda_1, \lambda_2, \ldots, \lambda_{M-1}\}$$

every $a\lambda_i + b$ has degree $d$.

For every $\lambda \in H$ we can write Equation (1) as

$$a\lambda + b = \gcd(a, b) p_\lambda$$

for some polynomial $p_\lambda$ in $F[t]$. Defining

$$c = \deg(\gcd(a, b))$$

we obtain

$$\deg(p_\lambda) = d - c.$$

**Lemma 21.** *We have $d > 2c$.*

*Proof.* We have

$$\frac{1}{2} > \gamma = \frac{c}{d}.$$

□

**Notation 22.** *We will write*

$$g = \frac{1}{\gcd(a, b)}$$

*and observe that it is a rational function over $F$ with no zeroes.*

**Lemma 23.** *Given $\mu$ and $\nu$ in $H$, if $\mu$ is distinct from $\nu$ then $p_\mu$ and $p_\nu$ are coprime.*

*Proof.* If $\rho$ is a common zero of both

$$p_\mu = (a\mu + b)g \quad \text{and} \quad p_\nu = (a\nu + b)g,$$

then $\rho$ is a zero of $(a\mu - a\nu)g$. This implies that $\rho$ is a zero of $ag$. Since $\rho$ is a zero of $(a\mu + b)g$ and of $ag$ we get that $\rho$ is a zero of $bg$. Therefore, the polynomial $t - \rho$ divides the greatest common divisor of $ag$ and $bg$, which is 1, hence leading to a contradiction. □

**Lemma 24.** *We have:*

$$\gcd(a, b) \prod_{\mu \in H} p_\mu \quad \textit{divides} \quad (a'b - ab') \prod_{\mu \in H} x_\mu.$$

*Proof.* Multiplying Equation (2) by $a$ we have

$$a'a\lambda + ab' = ak_\lambda x_\lambda^{k_\lambda - 1} x'_\lambda$$

hence by Equation (1)

$$a'(x_\lambda^{k_\lambda} - b) + ab' = ak_\lambda x_\lambda^{k_\lambda - 1} x'_\lambda$$

which finally gives

$$a'b - ab' = x_\lambda^{k_\lambda - 1}(a'x_\lambda - ak_\lambda x'_\lambda).$$

Hence

$$x_\lambda^{k_\lambda} = \gcd(a,b)p_\lambda \quad \text{divides} \quad (a'b - ab')x_\lambda$$

for each $\lambda$ in $H$. Therefore, for each $\lambda \in H$, the polynomial $\gcd(a,b)p_\lambda$ divides

$$(a'b - ab')x_\lambda \prod_{\substack{\mu \in H \\ \mu \neq \lambda}} x_\mu = (a'b - ab') \prod_{\mu \in H} x_\mu.$$

Hence the least common multiple of the polynomials $\gcd(a,b)p_\mu$, which is

$$\gcd(a,b) \prod_{\mu \in H} p_\mu$$

because the $p_\mu$ are coprime by Lemma 23, divides

$$(a'b - ab') \prod_{\mu \in H} x_\mu.$$

□

**Lemma 25.** *The expression $a\lambda + b$ is a power in $F[t]$ for at most $M(a,b)$ values of $\lambda$ in $F$.*

*Proof.* First observe that by Lemma 19 and the definition of $M(a,b)$, it is enough to prove that $M$ is at most

$$\left\lceil \frac{3}{1 - 2\gamma} \right\rceil + 1.$$

Also note that for each $\lambda \in H$ we have

$$\deg(x_\lambda) \leq \frac{d}{2}$$

(since $k_\lambda \geq 2$ and $\deg(x_\lambda^{k_\lambda}) = d$).

Since $a'b - ab'$ is non-zero (by hypothesis, because the quotient $\frac{a}{b}$ has non-zero derivative) we have from Lemma 24

$$\deg(\gcd(a,b)) + \deg\left(\prod_{\mu \in H} p_\mu\right) \leq \max\left\{\deg(a'b), \deg(ab')\right\} + \deg\left(\prod_{\mu \in H} x_\mu\right)$$

which implies

$$c + (M-1)(d-c) \leq 2d - 1 + (M-1)\frac{d}{2}$$

hence

$$2c + (M-1)(2d-2c) \leq 4d - 2 + (M-1)d$$

which gives

$$(M-1)(d-2c) \leq 4d - 2 - 2c,$$

hence, noting that $d - 2c$ is positive - see Lemma 21, we have

$$\begin{aligned} M &\leq \frac{3d-2+d-2c}{d-2c} + 1 \\ &= \frac{3d-2}{d-2c} + 2 \\ &< \frac{3d}{d-2c} + 2 \\ &= \frac{3}{1-2\gamma} + 2 \\ &\leq \left\lceil \frac{3}{1-2\gamma} \right\rceil + 2. \end{aligned}$$

□

**Lemma 26.** *If $a' = 0$, then $M \leq M(a,b)$.*

*Proof.* If $a' = 0$ then Equation (2) becomes

$$b' = k_\lambda x_\lambda^{k_\lambda - 1} x'_\lambda.$$

As $b'$ is not 0 (by hypothesis, not both $a'$ and $b'$ can be zero), the polynomial

$$x_\lambda^{k_\lambda} = \gcd(a,b) p_\lambda$$

divides $b' x_\lambda$ for every $\lambda \in H$. Hence, as in the proof of Lemma 24,

$$\gcd(a,b) \prod_{\mu \in H} p_\mu \quad \text{divides} \quad b' \prod_{\mu \in H} x_\mu.$$

We obtain

$$c + (M-1)(d-c) \leq d - 1 + (M-1)\frac{d}{2}$$

which implies

$$2c + (M-1)(2d-2c) \leq 2d - 2 + (M-1)d$$

hence

$$(M-1)(d-2c) \leq 2d - 2c - 2$$

and

$$\begin{aligned} M &\leq \frac{2d-2c-2}{d-2c} + 1 \\ &= \frac{d-2}{d-2c} + 2 \\ &< \frac{d}{d-2c} + 2 \\ &= \frac{1}{1-2\gamma} + 2 \\ &\leq \left\lceil \frac{1}{1-2\gamma} \right\rceil + 2. \end{aligned}$$

Hence we finally have

$$M \leq \left\lceil \frac{1}{1-2\gamma} \right\rceil + 1.$$

□

**Lemma 27.** *If $b' = 0$, then $M \leq M(a,b)$.*

*Proof.* Since $b' = 0$, Equation (2) becomes

$$a'\lambda = k_\lambda x_\lambda^{k_\lambda - 1} x'_\lambda.$$

Since for each non-zero $\lambda$, the polynomial $x_\lambda^{k_\lambda} = \gcd(a,b)p_\lambda$ divides $a'x_\lambda$, we have

$$\gcd(a,b) \prod_{\mu \in H - \{0\}} p_\mu \quad \text{divides} \quad a' \prod_{\mu \in H - \{0\}} x_\mu.$$

Since

$$a' \prod_{\mu \in H - \{0\}} x_\lambda$$

is not zero, we obtain

$$c + (M-2)(d-c) \leq d - 1 + (M-2)\frac{d}{2}$$

which implies

$$2c + (M-2)(2d-2c) \leq 2d - 2 + (M-2)d$$

hence

$$(M-2)(d-2c) \leq 2d - 2c - 2$$

and

$$\begin{aligned} M &\leq \frac{2d-2c-2}{d-2c} + 2 \\ &= \frac{d-2}{d-2c} + 3 \\ &< \frac{d}{d-2c} + 3 \\ &= \frac{1}{1-2\gamma} + 3 \\ &\leq \left\lceil \frac{1}{1-2\gamma} \right\rceil + 3. \end{aligned}$$

We finally have

$$M \leq \left\lceil \frac{1}{1-2\gamma} \right\rceil + 2.$$

□

# 3 Counterexamples in positive characteristic

This section is dedicated to the proof of Theorem 3.

Let $a_1, a_2, \ldots, a_n$ be different prime numbers. By the Chinese Remainder Theorem, there is an integer $x$ which solves the system of congruences

$$x \equiv -a_1 \ldots a_{i-1} a_{i+1} \ldots a_n \pmod{a_i} \qquad i = 1, \ldots, n. \tag{3}$$

Note that $y = x + ka_1 a_2 \ldots a_n$ is also a solution of this system for every $k \in \mathbb{Z}$.

Since the product

$$\prod_{j \neq i} a_j$$

is coprime with $a_i$ for each $i$, we deduce from the system (3) that $x$ and $a_1 \ldots a_n$ are coprime. By Dirichlet's Theorem we conclude that there exist infinitely many prime solutions $x + ka_1 a_2 \ldots a_n$ for the system of equations.

Given $\varepsilon > 0$, we can choose a prime solution $p > n$ of the system to be large enough in order to ensure that the following inequality holds:

$$\frac{\sum_{i=1}^{n} \left( \prod_{j \neq i} a_j \right)}{p + \sum_{i=1}^{n} \left( \prod_{j \neq i} a_j \right)} < \varepsilon.$$

Given a field $F$ of characteristic $p$, consider the following polynomials in $F[t]$:

$$a = (1+t)^{a_2 a_3 \cdots a_n} (2+t)^{a_1 a_3 \cdots a_n} \cdots (n+t)^{a_1 a_2 \cdots a_{n-1}},$$

and

$$b = at^p.$$

Observe that $\frac{a}{b}$ is non-constant.

If $g$ is a prime in the ring $F[t]$ and $f$ is a polynomial, we will write $\mathrm{ord}_g(f)$ for the largest integer $n$ such that $g^n$ divides $f$.

Since $p > n$, we have then, by the Little Fermat Theorem,

$$\begin{aligned} \mathrm{ord}_{(i+t)}(ai + b) &= \mathrm{ord}_{(i+t)}(ai + at^p) \\ &= \mathrm{ord}_{(i+t)}(i+t)^p + \mathrm{ord}_{(i+t)}(a) \\ &= p + a_1 \ldots a_{i-1} a_{i+1} \ldots a_n \end{aligned}$$

which is a multiple of $a_i$. Since by construction of $a$, for any $j$ distinct from $i$, the order of $ai+b$ at $j+t$ is a multiple of $a_i$, we deduce that $ai+b$ is an $a_i$-th power.

We deduce that $a\lambda+b$ is a power for $n$ values of $\lambda \in K$, and

$$\begin{aligned}\gamma(a,b) &= \frac{\deg(\gcd(a,b))}{\max\{\deg(a),\deg(b)\}} \\ &= \frac{\deg(a)}{\deg(at^p)} \\ &= \frac{\sum_{i=1}^{n}\left(\prod_{j\neq i} a_j\right)}{p+\sum_{i=1}^{n}\left(\prod_{j\neq i} a_j\right)} < \varepsilon.\end{aligned}$$

# 4 The case of monic quadratic polynomials

This section is dedicated to the proof of Theorem 6.

Fix a field $F$ and non-constant polynomials $b$ and $c$. In the case of positive characteristic, we assume moreover that $b''c' - b'c''$ is non-zero. Since "$\lambda^2 + b\lambda + c$ is not a power of exponent $\geq 3$ in $\tilde{F}$ for more than $M$ values of $\lambda$ in $\tilde{F}$" implies that "$\lambda^2 + b\lambda + c$ is not a power of exponent $\geq 3$ for more than $M$ values of $\lambda$ in $F$", without loss of generality, we can make the following assumption.

**Assumption 28.** *$F$ is algebraically closed.*

Suppose that $\lambda^2 + b\lambda + c$ is a power in $F[t]$, with exponent greater than or equal to 3, for $M$ distinct values of $\lambda$. Define

$$d = \max\{\deg(b), \deg(c)\}.$$

Since

$$\deg(\lambda^2 + b\lambda + c) = d$$

except for at most 1 value of $\lambda$ in $F$, we can define $H$ as a subset of $M - 1$ values of $\lambda$ for which the degree of $\lambda^2 + b\lambda + c$ is exactly $d$. Write

$$\lambda^2 + b\lambda + c = x_\lambda^{k_\lambda} \tag{4}$$

with $x_\lambda \in F[t]$ and $k_\lambda \geq 3$.

**Lemma 29.** *If $m$, $n$ and $\ell$ are pairwise distinct elements in $H$, then $x_m$, $x_n$ and $x_\ell$ are coprime.*

*Proof.* Suppose that $\rho \in F$ is a common zero of $x_m^{k_m}$, $x_n^{k_n}$ and $x_\ell^{k_\ell}$. Hence $\rho$ is a zero of $m^2 + bm + c$, $n^2 + bn + c$ and $\ell^2 + b\ell + c$. From this we obtain that

$$(m^2 - n^2) + (m - n)b(\rho) = 0$$

and

$$(n^2 - \ell^2) + (n - \ell)b(\rho) = 0.$$

Since $m \neq n$ and $n \neq \ell$ we obtain

$$(m + n) + b(\rho) = 0$$

and

$$(n+\ell)+b(\rho)=0.$$

From the above we obtain

$$m+n=n+\ell$$

which implies $m=\ell$, obtaining a contradiction with the hypothesis. Therefore $x_m^{k_m}$, $x_n^{k_n}$ and $x_\ell^{k_\ell}$ are coprime and we can conclude that $x_m$, $x_n$ and $x_\ell$ are coprime as well. □

Differentiating each side of Equation (4) we have

$$b'\lambda+c'=(x_\lambda^{k_\lambda})'. \tag{5}$$

Differentiating each side of Equation (5) we obtain

$$b''\lambda+c''=(x_\lambda^{k_\lambda})''. \tag{6}$$

Combining (5) and (6) to eliminate $\lambda$ we obtain

$$b''c'-b'c''=b''(x_\lambda^{k_\lambda})'-b'(x_\lambda^{k_\lambda})''. \tag{7}$$

Write

$$\Lambda=\operatorname{lcm}\left\{x_\mu^{k_\mu-2}\colon \mu\in H\right\}.$$

**Lemma 30.** *The polynomial $\Lambda$ divides $b''c'-b'c''$.*

*Proof.* This is immediate from Equation (7) since each $x_\lambda^{k_\lambda-2}$ divides $b''c'-b'c''$. □

Note that, as $k_\lambda$ is at least 3 and each $x_\lambda^{k_\lambda}$ has degree $d$ for $\lambda\in H$, we have

$$\deg(x_\lambda)\leq\frac{d}{3}$$

for each $\lambda\in H$.

**Lemma 31.** *We have*

$$\deg(\Lambda)\geq(M-1)\frac{d}{6}.$$

*Proof.* Given $(t-u)$ any prime polynomial, there exist $r_1$ and $r_2$ non-negative integers such that $(t-u)^{r_1}$ divides $x_\lambda^{k_\lambda-2}$ and $(t-u)^{r_2}$ divides $x_\nu^{k_\nu-2}$, for some $\lambda$ and $\nu$. From Lemma 29, $(t-u)$ does not divide any other $x_\mu^{k_\mu-2}$. From the above, since $(t-u)^{r_1+r_2}$ divides

$$(t-u)^{2\max\{r_1,r_2\}},$$

it also divides $\Lambda^2$. This implies that

$$\prod_{\mu\in H} x_\mu^{k_\mu-2}$$

divides $\Lambda^2$.

Therefore, since by hypothesis the $x_\mu$ are non-constant, the polynomial $\Lambda$ is not zero and we can deduce

$$\begin{aligned}
\deg(\Lambda) &\geq \frac{1}{2}\sum_{\mu\in H}\deg(x_\mu^{k_\mu-2}) \\
&\geq \frac{1}{2}\sum_{\mu\in H}(k_\mu-2)\deg(x_\mu) \\
&= \frac{1}{2}\sum_{\mu\in H}\deg(x_\mu^{k_\mu}) - 2\deg(x_\mu) \\
&\geq \frac{1}{2}(M-1)\left(d-2\frac{d}{3}\right) \\
&\geq (M-1)\frac{d}{6}.
\end{aligned}$$

□

**Lemma 32.** *If $M \geq 8$ then we have: $b'' = 0$ if and only if $c'' = 0$.*

*Proof.* Suppose first that $c''$ is zero, so that Equation (6) becomes

$$b''\lambda = (x_\lambda^{k_\lambda})''.$$

Hence, for every $\lambda$ distinct from 0, every $x_\lambda^{k_\lambda-2}$ divides $b''$. Therefore, the polynomial

$$\Lambda_0 = \operatorname{lcm}\left\{x_\lambda^{k_\lambda-2} \colon \lambda \in H \smallsetminus \{0\}\right\}.$$

divides $b''$. We proceed as for Lemma 31 in order to obtain a lower bound for the degree of $\Lambda_0$. We have

$$\begin{aligned}
\deg(\Lambda_0) &\geq \frac{1}{2} \sum_{\mu \in H \setminus \{0\}} \deg(x_\mu^{k_\mu - 2}) \\
&\geq \frac{1}{2} \sum_{\mu \in H \setminus \{0\}} (k_\mu - 2) \deg(x_\mu) \\
&= \frac{1}{2} \sum_{\mu \in H \setminus \{0\}} \deg(x_\mu^{k_\mu}) - 2 \deg(x_\mu) \\
&\geq \frac{1}{2}(M-2) \left( d - \frac{2d}{3} \right) \\
&\geq (M-2)\frac{d}{6}.
\end{aligned}$$

If $b''$ is non-zero we obtain

$$(M-2)\frac{d}{6} \leq \deg(\Lambda) \leq \deg(b'') \leq d-2.$$

Therefore if $M \geq 8$ then we obtain $d \leq d-2$, which is impossible. Therefore, we have $b'' = 0$.

Now suppose that $b''$ is zero. Equation (6) becomes

$$c'' = (x_\lambda^{k_\lambda})''.$$

Hence $\Lambda$ divides $c''$, and by Lemma 31 we have

$$(M-1)\frac{d}{6} \leq \deg(\Lambda) \leq \deg(c'') \leq d-2,$$

which gives a contradiction if $M \geq 7$. Hence $c''$ is zero. □

In the case of zero characteristic we do not need such an hypothesis on $b''c' - b'c''$ thanks to the following lemma.

**Lemma 33.** *If $F$ has characteristic 0 and $M \geq 8$ then neither $b''$ nor $c''$ is zero.*

*Proof.* Since $b'$ or $c'$ are not both zero, for every $\lambda$ in $H$, the polynomial

$$x_\lambda^{k_\lambda} = \lambda^2 + b\lambda + c \in F[t]$$

is non-constant. Since $k_\lambda \geq 3$ we have then

$$\deg(x_\lambda^{k_\lambda}) \geq 3.$$

If both $b''$ and $c''$ are zero, then we have

$$3 \leq \deg(x_\lambda^{k_\lambda}) = \deg(n^2 + bn + c) \leq 1,$$

which is not possible. We conclude with Lemma 32. □

**Lemma 34.** *If $F$ has characteristic 0 and $M \geq 8$ then the polynomial $b''c' - b'c''$ is non-zero.*

*Proof.* First note that since by Lemma 33 neither $b''$ nor $c''$ is zero, we deduce that neither $b'$ nor $c'$ is zero. If $b''c' - b'c'' = 0$ then

$$\left(\frac{b'}{c'}\right)' = 0,$$

hence there exists a (non-zero) constant $K$ such that $c' = Kb'$. Hence there is a constant $L$ such that $b = Kc + L$ and

$$\lambda^2 + b\lambda + c = \lambda^2 + b(\lambda + K) + L$$

is a power in $F[t]$. Therefore, also

$$\frac{\lambda^2 + L}{\lambda + K} + b$$

is a power in $F[t]$ whenever $\lambda$ is distinct from $-K$ (because $\lambda + K$ is in $F$ which is algebraically closed). Writing

$$q(\lambda) = \frac{\lambda^2 + L}{\lambda + K},$$

by Corollary 4, this can happen for at most for 3 distinct values of $q(\lambda)$, hence for at most 6 distinct values of $\lambda$ (since, given $c \in F$, the equation $q(\lambda) = c$ has at most two solutions in $\lambda$). Note that when $\lambda = -K$ we have

$$\lambda^2 + b\lambda + c = \lambda^2 + L$$

which is a constant, hence a power. Therefore, the quantity $\lambda^2 + b\lambda + c$ can be a power for at most 7 values of $\lambda$, which contradicts our assumption on $M$. □

*Proof of Theorem 6.* In order to get a contradiction, assume that $M$ is at least 13. Since $b''c'-b'c''$ is non-zero (by Lemma 34 in the case of characteristic zero, and by hypothesis in the case of positive characteristic) and since $M \geq 13$, we have

$$2d \leq (M-1)\frac{d}{6} \leq \deg(\Lambda) \leq \deg(b''c' - b'c'') \leq 2d - 3,$$

where the second inequality comes from Lemma 31 and the third inequality comes from Lemma 30. This is impossible.

□

# 5 Definability of zero derivative polynomials

This section is dedicated to the proof of Proposition 5.

If $x$ is a polynomial in $F[t]$ with zero derivative, since $F$ is algebraically closed, $x$ and $x+1$ are powers, hence the formula

$$\mathrm{der}(x)\colon P(x) \wedge P(x+1)$$

is satisfied in $F[t]$. Suppose now that $\mathrm{der}(x)$ is satisfied in $F[t]$. Let us show that $x$ has zero derivative.

Since $x$ is a power, it can be written as $f^m$ for some $f$ in $F[t]$ and some $m \geq 2$. Since $x+1$ is also a power, we can write

$$g^n = f^m + 1$$

for some $g$ in $F[t]$ and $n \geq 2$. In order to get a contradiction, we suppose that $x$ has non-zero derivative.

Since $f^m$, $g^n$ and 1 are coprime, and since $x = f^m$ has non zero derivative, we can apply Mason-Stothers Theorem. So we have

$$\max\{\deg(f^m), \deg(1), \deg(g^n)\} \leq \deg(fg) - 1$$

hence

$$\max\{m\deg(f), n\deg(g)\} \leq \deg(f) + \deg(g) - 1.$$

Therefore, we have

$$(m-1)\deg(f) \leq \deg(g) - 1 \tag{8}$$

and

$$(n-1)\deg(g) \leq \deg(f) - 1. \tag{9}$$

Multiplying Equation (8) by $(n-1)$, we obtain

$$\begin{aligned}(n-1)(m-1)\deg(f) &\leq (n-1)\deg(g) - (n-1)\\ &\leq \deg(f) - 1 - (n-1)\\ &= \deg(f) - n.\end{aligned}$$

We get a contradiction because $n$ and $m$ are greater than 1.

# 6 Definability and Undecidability Results

This section is dedicated to the proof of Theorem 11.

First of all note that in order to define existentially multiplication in $F[t]$ over a language $\mathcal{L}$ that contains $\{+\}$, it is enough to show that the binary relation "$y = x^2$" is existentially definable in $F[t]$ over $\mathcal{L}$. Indeed, we have $z = xy$ if and only if

$$4z = (x+y)^2 - (x-y)^2.$$

Most of this section is essentially an adaptation of an argument by Büchi to the case of rings of functions (see [24] for the language $\mathcal{L}_R^t$, where it is also done in positive characteristic - the argument is essentially taken from [18], in which there is a gap in the case of the language $\mathcal{L}_P^T$ - we fill it here).

Write $\psi(z, w, w_1, \ldots, w_{20})$ for the positive existential $\mathcal{L}_P$-formula

$$\bigwedge_{i=3,\ldots,20} w_i - 2w_{i-1} + w_{i-2} = 2 \bigwedge_{i=1,\ldots,20} P(w_i) \wedge w = w_1 \wedge 2z = w_2 - w_1 - 1$$

in the free variables $z, w, w_1, \ldots, w_{20}$. Also, write

$$\phi(z, w) \colon \exists w_1, \ldots, w_{20} \psi(z, w, w_1, \ldots, w_{20}).$$

**Lemma 35.** *Let $F$ be a field of characteristic 0. If the formula $\phi(z, w)$ is satisfied in $F[t]$ then, either $z^2 = w$, or both $z$ and $w$ are in $F$. Moreover, if $z^2 = w$ then the formula $\phi(z, w)$ holds.*

*Proof.* If the formula is satisfied then there are $w_1$, ..., $w_{20}$ in $F[t]$ which are powers and with second difference 2. By Theorem 9, either each $w_i$ is constant, which implies that both $z$ and $w$ are constant, or there exists $q \in F[t]$ such that $w_n = (q+n)^2$ for each $n$. In this case we have

$$2z = (q+2)^2 - (q+1)^2 - 1 = 2q + 2$$

hence $z^2 = (q+1)^2 = w_1 = w$.

Suppose now that $z^2 = w$ and write $z = q+1$. Choosing $w_1 = w = (q+1)^2$, we have

$$\begin{aligned} w_2 &= 2z + w_1 + 1 \\ &= 2(q+1) + (q+1)^2 + 1 \\ &= (q+2)^2. \end{aligned}$$

We can choose $w_n = (q+n)^2$ for each $n \geq 3$ in order for the formula to be satisfied. □

**Lemma 36.** *If $F$ has characteristic 0, then $F[t]$ satisfies the positive existential formula of the language $\mathcal{L}_P^t$*

$$\phi(tz, t^2w)$$

*if and only if $z^2 = w$.*

*Proof.* If $z^2 = w$, then $(tz)^2 = t^2z^2 = t^2w$, hence $\phi(tz, t^2w)$ holds in $F[t]$ by Lemma 35.

If $\phi(tz, t^2w)$ holds, then either $(tz)^2 = t^2w$, which implies $z^2 = w$, or both $tz$ and $t^2w$ are constant, in which case $z = w = 0$ (hence also $z^2 = w$). □

**Lemma 37.** *If $F[t]$ is a polynomial ring over a field $F$ of characteristic 0, then squaring over $F[t]$ is positive existentially definable in the language $\mathcal{L}_P^T$.*

*Proof.* We will show that the formula

$$\nu(x, y) : \exists u, v, y_1, y_2 \phi(x, y) \wedge \phi(x + u, y_1) \wedge \\ \phi(x - u, y_2) \wedge \phi(u, v) \wedge T(u) \wedge y_1 + y_2 - 2v = 2y$$

defines $y = x^2$.

If $x^2 = y$ in $F[t]$, then we can choose

$$\begin{aligned} u &= t, \\ v &= t^2, \\ y_1 &= (x + t)^2, \text{ and} \\ y_2 &= (x - t)^2, \end{aligned}$$

for the formula to be satisfied.

Now let $x$ and $y$ be polynomials in $F[t]$ such that $\nu(x, y)$ holds. First note that since $u$ is non-constant, if $x + u$ (or $x - u$) is constant then $x$ is non-constant and since $\phi(x, y)$ is satisfied, this implies that $y = x^2$ by Lemma 35. Suppose now that $x + u$ and $x - u$ are non-constant. We have

$$y_1 = (x + u)^2,$$

$$y_2 = (x - u)^2,$$

and

$$v = u^2$$

by Lemma 35. Therefore, we have

$$\begin{aligned} 2y &= y_1 + y_2 - 2v \\ &= (x+u)^2 + (x-u)^2 - 2u^2 \\ &= 2x^2, \end{aligned}$$

hence $y = x^2$. □

# References


[1] Ta Thi Hoai An and Julie Tzu-Yueh Wang, *Hensley's problem for complex and non-Archimedean meromorphic functions*, to appear in Journal of Mathematical Analysis and Applications, doi 10.1016/j.jmaa.2011.03.025 (2011).

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

[3] E. Catalan, *Note extraite d'une lettre adressée à l'éditeur*, J. Reine Angew. Math. **27-192** (1844).

[4] R. Cori and D. Lascar, *Logique Mathématique I*, Masson, Axiomes (1993).

[5] ——, *Logique Mathématique II*, Masson, Axiomes (1993).

[6] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. **490**, 81-100 (1997).

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

[8] J. Denef, *The Diophantine Problem for polynomial rings and fields of rational functions*, Transactions of the American Mathematical Society **242**, 391-299 (1978).

[9] J. Denef, L. Lipshitz, T. Pheidas, J. Van Geel Eds. *Hilbert's tenth problem : relations with arithmetic and algebraic geometry, Ghent 1999*, Contemporary Mathematics **270** (2000).

[10] L. Hajdu, *Perfect powers in arithmetic progression. A note on the inhomogeneous case*, Acta Arith. **113**, 343-349 (2004).

[11] S. Lang, *Algebra*, Springer.

[12] A. Macintyre, *On definable subsets of p-adic fields*, Journal of Symbolic Logic **41-3**, 605-610 (1976).

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

[14] H. Pasten, *An extension of Büchi's Problem for polynomial rings in zero characteristic*, Proceedings of the American Mathematical Society **138**, 1549-1557 (2010).

[15] —— *Representation of squares by monic second degree polynomials in the field of p-adic meromorphic functions*, to appear in Transactions of the AMS.

[16] H. Pasten, T. Pheidas, X. Vidaux, *A survey on Büchi's problem : new presentations and open problems*, Zapiski Nauchn. Sem. POMI, **377**, 111-140 (2010).
Published online http://www.pdmi.ras.ru/znsl/2010/v377.html

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

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

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

[20] T. Pheidas and X. Vidaux, *The analogue of Büchi's problem for cubes in rings of polynomials*, Pacific Journal of Mathematics **238 (2)**, 349-366 (2008).

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

[22] L. Rubel, *An essay on diophantine equations for analytic functions*, Exposiciones Mathematicae, **14**, 81-82 (1995).

[23] A. Shlapentokh, *Hilbert's Tenth Problem: Diophantine classes and extensions to global fields*, New Mathematical Monographs (2007).

[24] A. Shlapentokh and X. Vidaux, *The analogue of Büchi's problem for function fields*, Journal of Algebra **330-1**, 482-506 (2011).

[25] N. Snyder, *An alternate proof of Mason's Theorem*, Elemente der Mathematik **55-3**, 93-94 (2000).

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