UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

CONTRIBUCIONES A LA TEORIA DE LOS POLINOMIOS RALOS

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires en el área Ciencias Matemáticas

Martín Avendaño

Director de tesis: Dra. Teresa Krick.

Buenos Aires, 25 de Febrero de 2008

CONTRIBUCIONES A LA TEORIA DE LOS POLINOMIOS RALOS

Se presentan contribuciones al estudio de los polinomios ralos en tres diferentes aspectos. El primer resultado es un algoritmo que permite encontrar todos los factores irreducibles, de grado acotado por una constante prefijada, de un polinomio ralo multivariado con coeficientes algebraicos. El costo del algoritmo es polinomial en la longitud bit de su codificación rala y en la constante prefijada, y exponencial en el número de variables (esta dependencia exponencial siendo inevitable). El segundo es un algoritmo que permite interpolar un polinomio ralo univariado con coeficientes enteros, con t términos no nulos, a partir de $2t$ puntos enteros conocidos de altura chica. El último es una cota sobre la cantidad de soluciones reales que puede tener un sistema de ecuaciones ralas que consiste de un polinomio bivariado y una recta. A partir de esta se deriva un algoritmo sencillo para verificar si un polinomio lineal divide o no un polinomio ralo con coeficientes reales.

Palabras Clave: Polinomios Ralos, Factorización, Interpolación.

CONTRIBUTIONS TO THE THEORY OF LACUNARY POLYNOMIALS

We present contributions to the study of lacunary polynomials in three different aspects. The first result is an algorithm which finds all the factors, of degree bounded by a fixed constant, of a multivariate lacunary polynomial with algebraic coefficients. The cost of the algorithm is polynomial in the bit length of the lacunary encoding of the polynomial and in the fixed constant, and exponential in the number of variables (this last dependence being unavoidable). The second result is an algorithm which interpolates an univariate lacunary polynomial with integer coefficients and t non-zero terms from $2t$ known integer points of small height. The last result is a bound on the number of real roots of a system of lacunary polynomials consisting on a bivariate polynomial and a line. From this result, we derive a simple algorithm which decides whether a linear polynomial divides a bivariate lacunary polynomial with real coefficients or not.

Keywords: Lacunary Polynomials, Factorization, Interpolation.

Agradecimientos

A Teresa, por guiarme durante toda mi carrera, enseñándome matemática, dándome siempre ánimo para continuar frente a los problemas difíciles y ayudándome a evitar los irresolubles, por permitirme hacer investigación junto a ella, por su paciencia, comprensión y tolerancia, por la libertad con la que siempre me permitió trabajar, y por sobre todas la cosas, por su capacidad incansable de ayudarme con todo, excediendo largamente el trabajo de directora de tesis. Sin todo eso, estoy seguro de que nada de lo que sigue habría existido.

A Martín Sombra y Ariel Pacetti, por sus valiosos aportes en matemática, que dieron lugar a las Secciones 4 y 5 respectivamente, y además porque gracias a su ayuda esta tesis pudo ser presentada a tiempo.

A Daniel Perrucci y Gabriela Jeronimo, por su ayuda, especialmente con la Sección 6, introduciéndome en el tema y luego revisando una versión preliminar.

Al CONICET, por la beca que me permitió concentrarme en la investigación durante estos cinco años.

A Mariel, por ser la persona que ha compartido el mayor tiempo conmigo, porque en su compañía las cosas malas se convierten en buenas, la tristeza en alegría y la soledad no existe.

A Stella y Oscar, por haber estado siempre presentes, brindándome todo el soporte necesario para poder enfrentar cualquier dificultad sin preocuparme por el resultado.

Contents

Chapter 1

Introducción

El objetivo de esta tesis es contribuir a algunos temas centrales en la teoría de los polinomios ralos. Aquí "ralo" debe entenderse del siguiente modo: los únicos términos de los polinomios que son tomados en cuenta son aquellos no nulos. Hemos elegido la palabra "ralo" en lugar de "esparso", ya que esta última es usada actualmente con otro significado. Esta teoría también difiere de la teoría "densa" de polinomios, en donde, para un polinomio de grado d, todos los términos de grado hasta d, incluyendo los nulos, son tomados en cuenta.

En esta teoría de los polinomios ralos, la cantidad de términos no nulos reemplaza a la cantidad total de términos posibles, es decir, para un polinomio de grado d en n variables, esa cantidad jugará el papel del número $\binom{d+n}{n}$. Para cada uno de los problemas tratados en esta tesis, es importante tener en mente que las estimaciones deberán depender polinomialmente de esa cantidad (y de otros parámetros que surgirán naturalmente) y logarítmicamente del grado de los polinomios considerados. Por lo tanto, los polinomios interesantes en este contexto son aquellos cuya cantidad de términos no nulos es logarítmica en su grado.

Más precisamente, los temas que trataremos en esta tesis son los siguientes:

- Factorización de polinomios ralos multivariados con coeficientes en un cuerpo de números.
- Interpolación de polinomios ralos univariados con coeficientes enteros, donde tanto los coeficientes como los *exponentes* son desconocidos.
- Un primer intento de obtener cotas precisas para la cantidad de raíces reales aisladas de sistemas cuadrados de polinomios ralos multivariados con coeficientes reales.

A continuación daremos una breve reseña histórica y el estado actual de cada uno de esos temas y también detallaremos los avances conseguidos con este trabajo.

1.1 Factorización de polinomios ralos

Los resultados presentados en esta sección fueron obtenidos como parte de mi trabajo de doctorado junto con mi directora y con la colaboración de Martín Sombra. Estos se corresponden

esencialmente con el artículo [AKS07], en donde se trata el caso particular de polinomios bivariados. Aquí presentaremos su extensión al caso multivariado.

La factorización efectiva de polinomios, cuando es posible, es una tarea importante en álgebra computacional y teoría de números. Este problema tiene una larga historia, remontandose hasta I. Newton en 1707, y al astrónomo F. von Schubert quien en 1793 presentó un algoritmo para factorizar polinomios en una variable con coeficientes racionales, redescubierto más tarde y generalizado por L. Kronecker en 1882. Muchos otros algoritmos más eficientes fueron desarrollados desde entonces: citamos [Zas69], basado en [Ber70], entre los más famosos.

En 1982, A.K. Lenstra, H.W. Lenstra Jr. y L. Lovász lograron en [LLL82] un avance fundamental obteniendo el primer algoritmo determinístico de tiempo polinomial para factorizar polinomios univariados con coeficientes racionales. Basándose en ese trabajo y en la técnica de reducción de la base de un retículo introducida para su demostración, fueron obtenidos varios nuevos algoritmos de factorización [ChGr82, Len84, Kal85, Lan85, Hoe02, Len87, Lec05, BHKS05]. Estos algoritmos consiguieron satisfactoriamente traer a tiempo polinomial el problema de la factorización de polinomios univariados y multivariados sobre cuerpos de números cuando estos están codificados en forma *densa*, es decir, la entrada f del algoritmo consiste en la lista de todos sus términos de grado $\leq \deg(f)$ incluyendo a los que son nulos.

Para fines prácticos, es mejor considerar la *codificación rala* de los polinomios. Por ejemplo, para un polinomio univariado con coeficientes enteros, esto es la lista de los pares ordenados (a_i, α_i) —ambos enteros escritos en forma binaria— donde a_i es el coeficiente (no nulo) correspondiente al exponente α_i. De ahí que la codificación rala es lineal en la cantidad de términos no nulos, en el logaritmo del grado y en el logartimo del máximo valor absoluto de los coeficientes del polinomio. Dado que el grado del polinomio puede ser exponencial en su longitud rala, una aplicación directa de los algoritmos de factorización densos nos daría complejidad exponencial.

Aquí consideraremos el problema de factorizar un polinomio multivariado

$$f = \sum_{i=1}^{t} a_i X^{\alpha_i} \in K[X_1, \ldots, X_n]$$

con coeficientes en una extensión finita $K/\mathbb{Q}$, codificado en forma rala, es decir, por medio de la lista $(a_i, \alpha_i)_{1 \leq i \leq t}$ de sus coeficientes no nulos y sus correspondientes exponentes. Denotemos con $\ell(f)$ a la longitud bit de la codificación rala de f, la cual, como ya mencionamos antes, es la cantidad de bits que se necesitan para describir a los coeficientes y exponentes de f (ver Sección 4.3 para una definición precisa). Se obtendrá un algoritmo determinístico que calcula todos los factores de f de grado bajo, cuyo costo es polinomial en la longitud rala $\ell(f)$ y exponencial en el número de variables n:

Teorema 1.1.1. *Existe un algoritmo determinístico que, dado un polinomio $f \in K[X_1, \ldots, X_n]$ codificado en forma rala y un número natural d, calcula todos los factores irreducibles de f en $K[X_1, \ldots, X_n]$ de grado $\leq d$ con sus respectivas multiplicidades, en $(d \cdot \ell(f))^{O(n)}$ operaciones bit.*

Aquí $O(n)$ es la notación estándar para cn donde c es una constante universal.

Observemos que por un lado la restricción a factores de grado acotado es inevitable si pretendemos complejidad polinomial: el polinomio $f = X^p - 1$ (p primo) tiene longitud rala de orden $\log_2(p)$ pero tiene un factor irreducible denso $X^{p-1} + \cdots + 1$ que claramente tiene p téminos no nulos.

Por otra parte, el siguiente ejemplo, de J. von zur Gathen y E. Kaltofen [GaKa85], muestra que tampoco se puede conseguir una dependencia polinomial en el número de variables: para cualquier $n \in \mathbb{N}$ primo, el polinomio

$$f = \prod_{i=1}^{n}(X_i^n - 1) + n\prod_{i=1}^{n}(X_i - 1) \in \mathbb{Z}[X_1, \ldots, X_n]$$

es divisible por el polinomio irreducible

$$g = \prod_{i=1}^{n}(X_i^{n-1} + \cdots + 1) + n \in \mathbb{Z}[X_1, \ldots, X_n].$$

Pero f tiene 2^{n+1} términos, coeficientes pequeños (acotados por $n + 1$) y grado $\deg(f) = n^n$, mientras que g tiene $n^n = 2^{n\log_2(n)}$ términos y $\deg(g) = n(n - 1)$. Esto muestra que para n suficientemente grande, $\ell(g)$ tiene orden $\ell(f)^{\log_2(n)}$.

El primer resultado en la dirección del Teorema 1.1.1 apareció en 1998, cuando F. Cucker, P. Koiran y S. Smale mostraron cómo encontrar todas las raíces enteras de un polinomio univariado con coeficientes enteros en tiempo polinomial en su longitud rala, y preguntaron si también se podrían encontrar en un tiempo similar todas las raíces racionales [CKS99]. Esta pregunta (y más!) fue respondida afirmativamente por H.W. Lenstra Jr. quien obtuvo un algoritmo que, dado un cuerpo de números K y un polinomio univariado $f \in K[X]$, calcula todos los factores irreducibles de grado $\leq d$ con sus respectivas multiplicidades, en $(d + \ell(f))^{O(1)}$ operaciones bit [Len99b]. El primer e inspirador resultado en el caso multivariado fue obtenido por E. Kaltofen y P. Koiran [KaKo05, Thm. 3] en 2005, mostrando cómo calcular los factores *lineales* de un polinomio bivariado $f \in \mathbb{Q}[X, Y]$ en tiempo polinomial en $\ell(f)$. Un año despues, E. Kaltofen y P. Koiran [KaKo06] y T. Krick, M. Sombra junto con el autor de esta tesis [AKS07] extendieron independientemente ese resultado a un algoritmo que calcula todos los factores de grado $\leq d$. El primer artículo resolvía el problema en el caso multivariado, pero el algoritmo presentado allí requería conocer una cierta constante universal no explícita c [KaKo06, Thm. 1]. El otro sólo considera el caso bivariado (el cual es directamente generalizable al caso multivariado como mostraremos aquí) y hace explícitas todas las constantes, permitiendo de ese modo que el algoritmo sea implementado. Este último enfoque no sólo permite calcular los factores en un cuerpo de números, sino también los factores absolutos, es decir, los factores sobre la clausura algebraica de los números racionales.

Todos estos algoritmos (incluyendo al nuestro) están basados en el mismo principio *"the gap theorem"* usado primero por Cucker, Koiran y Smale para polinomios univariados con coeficientes enteros. La idea es tan simple y natural que merece ser explicada en esta introducción.

Dado $f \in \mathbb{Z}[X]$, ¿cómo podemos encontrar fácilmente sus raíces enteras ξ? El criterio de Gauss nos da los posibles valores de ξ; sin embargo, aún sin tener en cuenta la enorme cantidad de posibilidades para ξ, ¿cómo podríamos verificar si $f(\xi) = 0$? La evaluación directa no es posible, ya que el tamaño de $f(\xi)$ puede ser exponencialmente grande con respecto al de la entrada, excepto en los casos $\xi = 0, \pm 1$. También deberíamos evitar usar los algoritmos de factorización densos mencionados anteriormente, dado que su costo es polinomial en el grado de f.

Ahora veamos que es lo que el principio del "gap" hace: supongamos que $f = \sum_{i=1}^{t} a_i X^{\alpha_i} \in \mathbb{Z}[X]$ puede separarse

$$f = f_1 + X^{\beta} f_2$$

en polinomios no nulos f_1 de grado $\deg(f_1) = \alpha$ y f_2, de modo tal que hay un "gap" (brecha) entre los exponentes de f_1 y los de $X^{\beta} f_2$ de longitud

$$\beta - \alpha \geq \log_2 \|f\|_1$$

(aquí $\|f\|_1 = \sum_{i=1}^{t} |a_i|$ indica como es usual la *norma*-1 de f). Entonces, excepto en los casos $\xi = 0, \pm 1$, tenemos que $f(\xi) = 0$ si y sólo si $f_1(\xi) = f_2(\xi) = 0$: si esto no fuera así, digamos que $f(\xi) = 0$ pero $f_2(\xi) \neq 0$, entonces

$$|f_1(\xi)| \leq \|f_1\|_1 \cdot |\xi|^{\alpha} < \|f\|_1 \cdot |\xi|^{\alpha} \quad \text{y} \quad |f_1(\xi)| = |\xi|^{\beta} \cdot |f_2(\xi)| \geq |\xi|^{\beta}$$

nos daría que $\|f\|_1 > |\xi|^{\beta-\alpha} \geq 2^{\beta-\alpha}$ en contradicción con la suposición que hicimos sobre el gap! Por lo tanto, para verificar si f se anula en $\xi \neq 0, \pm 1$, se descompone a f en pequeños polinomios espaciados

$$f = \sum_{i} X^i f_i$$

y se chequea si $f_i(\xi) = 0$ para todo i. Más aún, dado que esa descomposición es independiente del punto ξ, las raíces enteras pueden encontrarse como las raíces comunes de un conjunto de polinomios de bajo grado, utilizando cualquier algoritmo de factorización denso.

El ingrediente clave que hace funcionar el argumento de arriba es que cualquier entero $\xi \neq 0, \pm 1$ satisface la cota inferior uniforme $|\xi| \geq 2$! Para poder aplicar la misma idea a $\xi \in \mathbb{Q}$, la correcta generalización del valor absoluto es la *altura*, definida como el máximo entre los valores absolutos del numerador y denominador de una fracción reducida. Imitando el razonamiento de arriba, pero esta vez utilizando el valor absoluto usual *y* todos los p-ádicos, se arriba a la misma conclusión, como consecuencia de que todos los números racionales excepto $0, \pm 1$ tienen altura al menos 2. Esto es esencialmente lo que Lenstra utilizó en [Len99b]; más generalmente, él fue capaz de tratar del mismo modo los factores no lineales, considerando la altura de sus raíces y aplicando una cota inferior adecuada: el Teorema de Dobrowolski [Dob79] en la versión de P. Voutier [Vou96]. En [KaKo05], los autores lograron la primera generalización del principio del gap a polinomios no univariados, más precisamente, para encontrar factores lineales de polinomios bivariados.

Como en todos los trabajos previos, la clave de nuestro algoritmo es un adecuado teorema del gap. Lo obtendremos como consecuencia de una cota inferior para la altura de Zariski de conjuntos

densos sobre una hipersuperficie debido a F. Amoroso y S. David [AmDa00] y luego refinado por C. Pontreau [Pon05, Thm. 1.9] haciendo explícitas las constantes. Esto es explicado en detalle en las Secciones 4.1 y 4.2. Este resultado nos permitirá descomponer al polinomio dado $f \in \mathbb{Q}[X_1, \ldots, X_n]$ en polinomios más pequeños; luego los factores de f serán calculados como los factores comunes de esos polinomios de bajo grado. Esta estrategia funciona bien para todos los factores excepto los monomios y los ciclotómicos (productos de binomios cuyos coeficientes son raíces de la unidad). Estos factores requieren un tratamiento separado, que haremos en la Sección 4.3.

Dado que nuestro algoritmo opera por reducción a los casos de polinomios densos multivariados y polinomios ralos univariados, nuestro interés será probar que esa reducción puede hacerse en tiempo polinomial en la longitud rala. No intentaremos calcular el exponente en la estimación de complejidad, el cual en principio podría ser bastante grande.

Como consecuencia del algoritmo, deduciremos que el número de factores irreducibles de grado $\leq d$ de $f \in \mathbb{Q}[X_1, \ldots, X_n]$ contados con multiplicidades (exceptuando a los factores monomiales) está acotado por $(d \cdot \ell(f))^{O(n)}$. Esto no es trivial ya que el grado de f puede ser exponencial en $\ell(f)$, pero de hecho algo mucho mejor puede decirse:

Proposición 1.1.2. *Sea $f \in \mathbb{Z}[X_1, \ldots, X_n]$ y consideremos la factorización*

$$f = q \cdot \prod_p p^{e_p}$$

donde q es un polinomio ciclotómico, $p \in \mathbb{Q}[X_1, \ldots, X_n]$ recorre todos los factores irreducibles no ciclotómicos de f y e_p es la correspondiente multiplicidad. Entonces

$$\sum_p e_p \leq 10^4 \cdot n^3 \cdot \log \|f\|_1 \cdot \log^3(n \max\{\deg(f), 16\}).$$

En particular, la cantidad total de factores irreducible no ciclotómicos de cualquier grado de f está acotada polinomialmente en función de la longitud rala de f. Esta propiedad generaliza a [Dob79, Thm. 2] y es una consecuencia más de la conexión con la teoría de alturas de la Geometría Diofántica.

La Proposición 1.1.2 debe ser comparada con otro resultado de H.J. Lenstra Jr.: el número total de factores irreducibles de grado $\leq d$ de $f \in \mathbb{Q}[X]$ contados con multiplicidades (que no sean X) está acotado por

$$c \cdot t^2 \cdot 2^d \cdot d \cdot \log(2dt)$$

donde t es la cantidad de términos no nulos de f [Len99a, Thm. 1]. Esta cota es exponencial, pero independiente del grado y coeficientes de f. En base a estos resultados, parece natural considerar la siguiente pregunta: ¿está la cantidad de factores irreducibles que no sean monomios (no ciclotómicos quizás?) de un t-nomio en $\mathbb{Q}[X]$ uniformemente acotado por alguna función $B(t)$ dependiendo sólo de t, y tal vez por algo como $t^{O(1)}$?

Tratando de ir más lejos, uno podría preguntarse si es posible calcular en tiempo polinomial la factorización *absoluta* de un polinomio codificado en forma rala, es decir, sus factores irreducibles sobre $\overline{\mathbb{Q}}$. Para el caso univariado la respuesta es claramente "no": un polinomio univariado se factoriza completamente como producto de factores lineales, y todos ellos no pueden calcularse en tiempo polinomial. Para el caso multivariado, puede verse que el cálculo de los factores binomiales es equivalente a la factorización de un polinomio univariado, así que estos factores sobre $\overline{\mathbb{Q}}$ tampoco pueden ser calculados en tiempo polinomial. Aquí probaremos que excepto por esos, se pueden calcular todos los otros factores irreducibles sobre $\overline{\mathbb{Q}}$ de grado bajo, en tiempo polinomial en la longitud rala.

Teorema 1.1.3. *Existe un algoritmo determinístico que, dado $f \in K[X_1, \ldots, X_n]$, donde K es un cuerpo de números, y $d \geq 1$, obtiene todos los factores irreducibles de f en $\overline{\mathbb{Q}}[X_1, \ldots, X_n]$ de grado $\leq d$, excepto los binomiales, con sus respectivas multiplicidades, en $(d \cdot \ell(f))^{O(n)}$ operaciones bit.*

Este algortimo se sigue de otro teorema del gap que se obtiene como consecuencia de otro resultado de Pontreau [Pon05, Thm. 1.22]. Más aún, deduciremos de ese resultado un análogo de la Proposición 1.1.2 para la cantidad de factores absolutos no binomiales de un polinomio dado $f \in \mathbb{Z}[X_1, \ldots, X_n]$.

Proposición 1.1.4. *Sea $f \in \mathbb{Z}[X_1, \ldots, X_n]$ y consideremos la factorización*

$$f = q \cdot \prod_p p^{e_p}$$

donde q es producto de binomios, $p \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ recorre todos los factores irreducibles de f con al menos tres términos, y e_p es la multiplicidad correspondiente. Entonces

$$\sum_p e_p \leq 10^{14} \cdot n^{13} \cdot \log \|f\|_1 \cdot \log^5(\max\{n \deg(f), 16\}).$$

Terminaremos esta sección notando que aunque el problema de encontrar todos los factores de grado bajo de polinomios multivariados sobre cuerpos de números en tiempo polinomial en la longitud de la codificación rala está ahora completamente resuelto, la solución presentada aquí es sólo un resultado teórico en el sentido que dado que las constantes involucradas son enormes, el algoritmo –si se lo implementa– sería absolutamente impracticable. Sin embargo, como sucede frecuentemente en temas de álgebra computacional, un primer resultado con la complejidad adecuada motiva la búsqueda de buenos algoritmos en la práctica. Por ejemplo, recordemos que durante la búsqueda de buenos algoritmos para la factorización densa de polinomios univariados sobre los racionales, el quiebre que produjo el resultado de Lenstra, Lenstra y Lovasz [LLL82] finalmente condujo al algoritmo de tiempo polinomial *y* eficiente de M. van Hoeij [Hoe02, BHKS05]. En este sentido, todavía queda mucho trabajo por hacerse aquí.

1.2 Interpolación de polinomios ralos univariados con coeficientes enteros

Los resultados presentados en esta sección fueron obtenidos conjuntamente, como parte de mi trabajo de doctorado, con mi directora y Ariel Pacetti; estos resultados han sido publicados en [AKP06].

La interpolación es un ingrediente crucial en la Matemática. La mayoría de los algoritmos para interpolar polinomios univariados requiere que la cantidad de puntos sea esencialmente igual al grado del polinomio buscado. La motivación de este trabajo es la búsqueda de un algoritmo eficiente de interpolación para polinomios enteros univariados, donde la cantidad de puntos de interpolación dependa de la cantidad de términos no nulos del polinomio y no de su grado. En esta versión del problema, sabremos que el polinomio buscado tiene exactamente (o a lo sumo) t términos no nulos, pero no sabremos cuáles son los exponentes a los que les corresponde un coeficiente no nulo. Esto ya no es más un problema básico de álgebra lineal, sino que se trata de reconstruir los pares (coeficiente, exponente) correspondientes a los términos de un polinomio, a partir de sus valores en una cantidad razonable de puntos de interpolación.

Diremos que un polinomio es *t-ralo* si tiene a lo sumo t términos no nulos. El problema de interpolar un polinomio t-ralo a partir de su valor en una lista particular de puntos de interpolación (donde la cantidad de esos puntos depende de t pero no del grado) es conocido como "interpolación rala". Este problema recibió mucha atención cerca de 1990 y de nuevo ahora, por ejemplo en [BeTi88, Zip90, KaLa88, KLW90, KLL00, Lee01, KaLe03], [BoTi91], [DrGr91, GKS91], [GKS90, CDGK91] y [GKS94].

Es un hecho conocido que, como consecuencia de la Regla de los Signos de Descartes (Teorema 6.1.2), un polinomio t-ralo $f \in \mathbb{R}[X]$ tiene a lo sumo $t-1$ raíces reales positivas distintas. De ahí que un polinomio univariado t-ralo en $\mathbb{C}[X]$ está unívocamente determinado por su valor en $2t$ puntos positivos en $\mathbb{R}$ (ya que para dos tales polinomios, la diferencia de sus partes reales (o sus partes imaginarias) es un polinomio $2t$-ralo que por lo tanto tiene a lo sumo $2t-1$ raíces reales positivas distintas).

En [BeTi88], M. Ben-Or y P. Tiwari consiguieron un hermoso algoritmo determinístico que reconstruye un polinomio t-ralo $f \in \mathbb{C}[X]$ a partir de $2t$ puntos distintos de interpolación de la forma

$$x_1 = 1,\ x_2 = a,\ x_3 = a^2, \ldots, x_{2t} = a^{2t-1}.$$

Ellos también plantearon el problema de producir un algoritmo que interpole a un polinomio t-ralo en $\mathbb{C}[X]$ a partir de $2t$ puntos reales positivos arbitrarios, que emule en algún sentido a los algoritmos de interpolación de Lagrange que no imponen ninguna restricción sobre los puntos de entrada, a diferencia del suyo, en donde estos en lugar de los puntos de partida son muy particulares.

Nuestro algoritmo se basa esencialmente en una variante original del levantamiento de Newton-Hensel que puede ser usado en problemas de interpolación. El tradicional levantamiento de

Newton-Hensel, conocido como el Lema de Hensel, es la contraparte algebraica (no arquimediana) del método de Newton. Este fue introducido por Hensel alrededor de 1900 y es la base de la teoría de los números p-ádicos y sus aplicaciones como en el principio local-global de Hasse-Minkowski para formas cuadráticas. Desde entonces, el "levantamiento de Newton-Hensel" ha estado presente en la computación simbólica exacta: por ejemplo en factorización de polinomios univariados con coeficientes racionales [Zas69, LLL82] y en factorización de polinomios multivariados [ChGr82, Chi84, Gri84, Kal85].

La versión que desarrollaremos aquí permite levantar polinomios en $\mathbb{Z}[X]$ a partir de información módulo un primo $p \neq 2$ a una potencia p^k para cualquier k. La clave es que no sólo se levantan los coeficientes del polinomio, sino que también sus *exponentes*. Esto se consigue gracias a la función $L_p : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ definida por $x^{p-1} \equiv 1 + p\,L_p(x) \pmod{p^2}$ para $p \nmid x$ y $L_p(x) = 0$ para $p \mid x$ (ver Definición 5.4.1), que juega el papel de la "función logarítmica módulo p" y nos permite linealizar ecuaciones cuyas incógnitas estén en los exponentes.

Teorema 1.2.1. *Sea $f = \sum_{j=1}^{t} a_j X^{e_j} \in \mathbb{Z}[X]$. Sea $p > t$ un primo impar tal que $p \nmid a_i$ para todo i y $p - 1 \nmid e_i - e_j$ para todos $i \neq j$.*
Supongamos que $x_1, \ldots, x_{2t}$ e $y_1, \ldots, y_{2t}$ son números enteros dados que satisfacen:

- $f(x_i) \equiv y_i \pmod{p}$ *para todo* $1 \leq i \leq 2t$,
- $$\det \begin{bmatrix} L_p(x_1)x_1^{e_1} & \ldots & L_p(x_1)x_1^{e_t} & x_1^{e_1} & \ldots & x_1^{e_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ L_p(x_{2t})x_{2t}^{e_1} & \ldots & L_p(x_{2t})x_{2t}^{e_t} & x_{2t}^{e_1} & \ldots & x_{2t}^{e_t} \end{bmatrix} \not\equiv 0 \pmod{p}.$$

Entonces, para cada $k \in \mathbb{N}$ existe un polinomio $f^{(k)} = \sum_{j=1}^{t} a_j^{(k)} X^{e_j^{(k)}} \in \mathbb{Z}[X]$, que satisface simultaneamente:

- $f^{(k)}(x_i) \equiv y_i \pmod{p^k} \qquad 1 \leq i \leq 2t$,
- $a_j^{(k)} \equiv a_j \pmod{p}$ *y* $e_j^{(k)} \equiv e_j \pmod{(p-1)} \qquad 1 \leq j \leq t$.

Más aún, si $f^{(k)} = \sum_{j=1}^{t} a_j^{(k)} X^{e_j^{(k)}}$ y $g^{(k)} = \sum_{j=1}^{t} b_j^{(k)} X^{d_j^{(k)}} \in \mathbb{Z}[X]$ son dos tales polinomios, entonces

$$a_j^{(k)} \equiv b_j^{(k)} \pmod{p^k} \quad y \quad e_j^{(k)} \equiv d_j^{(k)} \pmod{\varphi(p^k)} \quad \text{para todo} \quad 1 \leq j \leq t,$$

donde φ es la función de Euler.

De hecho, probaremos algo que es interesante en sí mismo, más allá de alguna posible aplicación a la interpolación: que este resultado corresponde exactamente a un levantamiento de Hensel de un sistema de $2t$ ecuaciones generalizadas con $2t$ incógnitas, siendo estas los t coeficientes de f en los enteros p-ádicos y los t exponentes de f en un conjunto apropiado E_p (ver Definición 5.2.1), y donde la condición que el determinante del teorema anterior no se anule módulo p es la correspondiente clásica condición sobre el Jacobiano del sistema.

Para este propósito, introducimos el anillo E_p de los "exponentes admisibles" (cuyo grupo aditivo resultará ser isomorfo al grupo de unidades $\mathbb{Z}_p^\times$), donde "admisibles" significa que para $x \in \mathbb{Z}_p^\times$ y $\alpha \in E_p$ tenemos una definición consistente de $x^\alpha \in \mathbb{Z}_p^\times$. Inmediatamente después de introducir este anillo, tiene sentido considerar expresiones polinomiales en $\mathbb{Z}_p$, donde las variables están en $\mathbb{Z}_p^\times$ y los exponentes en E_p.

Aquí, entre todas las descripciones equivalentes de $\mathbb{Z}_p$ adoptaremos la siguiente por ser más adecuada para nuestros enunciados:

$$\mathbb{Z}_p = \left\{ (a_i)_{i\geq 1} \in \mathbb{Z}^{\mathbb{N}} \ : \ a_i \equiv a_{i+1} \bmod p^i \ \forall\, i \right\} / \sim$$

donde $\sim$ es la relación de equivalencia dada por

$$(a_i)_{i\geq 1} \sim (b_i)_{i\geq 1} \iff a_i \equiv b_i \bmod p^i, \ \forall\, i.$$

Del mismo modo, definimos E_p como:

$$E_p = \left\{ (a_i)_{i\geq 1} \in \mathbb{Z}^{\mathbb{N}} \ : \ a_i \equiv a_{i+1} \bmod \varphi(p^i) \ \forall\, i \right\} / \simeq$$

donde $\simeq$ es la relación de equivalencia dada por

$$(a_i)_{i\geq 1} \simeq (b_i)_{i\geq 1} \iff a_i \equiv b_i \bmod \varphi(p^i), \ \forall\, i.$$

En ambos anillos, las operaciones (incluyendo la función exponencial) son coordenada a coordenada.

$$x = \overline{(x_i)_{i\geq 1}} \in \mathbb{Z}_p \ \text{ y } \ e = \overline{(e_i)_{i\geq 1}} \in E_p \ \longrightarrow \ x^e = \overline{(x_i^{e_i})_{i\geq 1}}$$

En las Secciones 5.1 y 5.2 haremos un estudio completo de estas estructuras de datos. Luego, en las dos secciones siguientes, consideraremos dos diferentes clases de ecuaciones polinomiales: la primera (llamada ecuaciones seudo-polinomiales) difiere de las ecuaciones polinomiales clásicas en que los exponentes son constantes de E_p en lugar de números naturales, y la segunda (llamada ecuaciones exponenciales) tiene como incógnitas a los exponentes de los monomios. Probaremos que la existencia de una solución módulo p más una condición razonable tipo Jacobiano (llamada condición de levantamiento) garantiza la existencia de una solución en el anillo correspondiente $\mathbb{Z}_p$ o E_p. También probaremos que estos dos tipos de ecuaciones están relacionados mediante un cambio de variables exponencial-logarítmico.

Volviendo a la interpolación, el Teorema 1.2.1 nos permite dar una respuesta satisfactoria al problema en el caso en que el polinomio buscado f cumpla la propiedad de la buena reducción módulo el primo elegido p y que los puntos de evaluación $x_1, \ldots, x_{2t}$ satisfagan la propiedad tipo Jacobiano (la no anulación del determinante) tal como se describe en las hipótesis. También, en el Teorema 5.6.4, produciremos familias grandes de puntos de tamaño pequeño que son adecuados en ese sentido.

Para poder responder a la pregunta de Ben-Or y Tiwari en toda su generalidad, todavía necesitamos de un criterio para elegir, en término de los valores $y_i = f(x_i)$, un primo p (pequeño)

tal que f tiene buena reducción módulo p. Esto es el análogo a la elección del primo en los algoritmos de factorización de polinomios con coeficientes enteros (en cuyo caso se elige un primo que no divida al discriminante del polinomio), y en el caso arquimediano, a un criterio (todavía desconocido) para elegir un cero aproximado. Más realísticamente necesitaríamos un argumento probabilístico para la elección de tal primo en un rango determinado, pero todavía no lo hemos conseguido.

1.3 Estimaciones para la cantidad de raíces de sistemas ralos

Los resultados presentados en esta sección corresponden a los resultados obtenidos durante el trabajo de doctorado, que aparecerán en [Ave08].

Ya hemos mencionado a la Regla de lo Signos de Descartes que establece que la cantidad de raíces reales positivas de un polinomio $f \in \mathbb{R}[X]$, contadas con multiplicidad, está acotada por la cantidad de cambios de signos en su vector de coeficientes, omitiendo los nulos. Como consecuencia directa, la cantidad de raíces reales de f está acotada por $2t-1$, donde t es la cantidad de términos no nulos de f (aquí las a lo sumo $t-1$ raíces positivas y a lo sumo $t-1$ raíces negativas están contadas con multiplicidad, mientras que la posible raíz 0 cuenta a lo sumo una vez).

Todavía no hay generalizaciones naturales de la Regla de los Signos de Descartes al caso multivariado, pero mucho trabajo se ha hecho y se está haciendo para estimar la cantidad de raíces (en el ortante positivo) aisladas o no degeneradas (es decir, donde el Jacobiano no se anula, condición que implica que la raíz es aislada) de sistemas cuadrados de polinomios reales multivariados, en términos de la cantidad de variables y de la cantidad de términos no nulos involucrados en el sistema.

El resultado principal en esa dirección es de A. Khovanskii [Kho91]. Una versión simplificada del mismo implica que un sistema cuadrado de n ecuaciones polinomiales reales en n variables, involucrando un total de t términos no nulos, tiene a lo sumo $(n+1)^t 2^{t(t-1)/2}$ raíces reales no degeneradas en el ortante positivo. Ciertos avances sobre el resultado de Khovanskii han sido obtenidos recientemente por F. Bihan y F. Sottile, pero sin embargo la dependencia exponencial en la cantidad de términos no nulos t no ha podido ser evitada [BiSo06, BBS07].

En [LRW03], T.Y. Li, M. Rojas y X. Wang (ver también D. Perrucci [Per05]) estudiaron casos particulares de sistemas cuadrados bivariados y mostraron que la cantidad de raíces aisladas o no degeneradas de un trinomio y un polinomio con a lo sumo t términos no nulos, $t \geq 3$, está acotada por $2^t - 2$.

Más aún, la Conjetura de Kushnirenko, formulada a mediados de la decada del 70 (que dice que un sistema cuadrado de n ecuaciones polinomiales reales en n variables, tal que la ecuación k-ésima tiene t_k términos, debe tener a lo sumo $(t_1-1)\cdots(t_n-1)$ raíces no degeneradas en el ortante positivo) resulto ser falsa, como lo muestra un contraejemplo presentado por B. Haas en 2002 para un sistema de dos trinomios en dos variables [Haa02].

El resultado principal de esta sección es un refinamiento del resultado en [LRW03] para el caso particular en que el trinomio es de grado uno. Sin perdida de generalidad, podemos suponer que el polinomio lineal es de la forma $Y - aX - b$ y por lo tanto estudiar la cantidad de raíces reales de un polinomio bivariado sobre la recta $Y = aX + b$:

Teorema 1.3.1. *Sea $f = \sum_{i=1}^{t} a_i X^{\alpha_i} Y^{\beta_i} \in \mathbb{R}[X, Y]$ un polinomio con a lo sumo t términos no nulos, y sean $a, b \in \mathbb{R}$. Sea $g(X) = f(X, aX + b)$. Entonces $g \equiv 0$ o g tiene a lo sumo $6t - 4$ raíces reales, contadas con multiplicidades excepto por las posibles raíces 0 y $-b/a$ que cuentan a lo sumo una vez.*

Aparentemente esta es la primera vez que una cota no exponencial se consigue para este tipo de sistemas: no había cotas polinomiales conocidas incluso para casos simples de familias de polinomios.

Como consecuencia de ese resultado, obtendremos un algoritmo alternativo para verificar si una forma lineal $Y - aX - b$ divide a un polinomio f en $K[X, Y]$, donde K es un cuerpo de números real. La cantidad de operaciones bit que necesita el algoritmo es polinomial en el grado $[K : \mathbb{Q}]$ de la extensión, en la cantidad t de términos no nulos de f, en el logaritmo del grado de f y en la altura logarítmica de a, b y f. El primer algoritmo para este propósito puede deducirse del resultado más general de E. Kaltofen y P. Koiran [KaKo05] mencionado en la Sección 2.1. Aquí, en lugar de utilizar el principio del gap, reduciremos el problema al caso univariado mediante especializaciones $f(X, X^n)$ para pequeños valores de n, que no destruyen la estructura rala de f.

Es importante mencionar que las herramientas utilizadas son completamente elementales: estamos ahora estudiando la posibilidad de extender estos resultados para sistemas más generales.

Chapter 2

Introduction

This thesis aims to contribute to some central topics in the theory of lacunary polynomials. Here "lacunary" has to be understood in the following sense: the only terms of the polynomials that are taken into account are the non-zero ones. We chose the word "lacunary" to distinguish it from the term "sparse", which is usually used nowadays in a different meaning. This is also different from the "dense" theory of polynomials, where for a polynomial of degree d, all the possible terms arising, even the zero ones, are taken into account.

In this theory of lacunary polynomials, the number of non-zero terms replaces the total number of possible terms, i.e. for a polynomial of degree at most d in n variables, this number will play the role of the number $\binom{d+n}{n}$. For each of the problems considered in this thesis, the important issue to keep in mind is that the estimates have to depend polynomially on this number (and on some other parameters that arise naturally) and logarithmically on the degree of the polynomials that are considered. Therefore the interesting polynomials in this setting are those whose number of non-zero terms is logarithmic in their degree.

More precisely, the topics we address in this thesis are the following ones:

- The factorization of lacunary multivariate polynomials with coefficients in a number field.
- The interpolation of lacunary univariate polynomials with integer coefficients, where both the coefficients *and the exponents* are unknown.
- A first attempt to obtain precise bounds for the number of real isolated roots of square systems of multivariate polynomials, with real coefficients.

We now summarize the history and the state of the art of each of these topics and the contributions achieved in our work.

2.1 Factorization of lacunary polynomials

The results presented in this section were obtained as a part of my candidacy research together with my advisor and with the collaboration of Martín Sombra. They mainly correspond to the

article [AKS07], where the particular case of a bivariate polynomial is treated. Here we present their extension to the full multivariate case.

Effective factorization of polynomials, when possible, is an important task in computational algebra and number theory. This problem has a long history, going back to I. Newton in 1707, and to the astronomer F. von Schubert who in 1793 presented an algorithm for factoring a univariate polynomial, later rediscovered and generalized by L. Kronecker in 1882. Many other more efficient algorithms were designed since then: we cite [Zas69], based on [Ber70], among the most famous ones.

In 1982, A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász made a fundamental advance by obtaining the first deterministic polynomial-time algorithm for factoring an univariate polynomial over the rational numbers. Based on [LLL82] and the technique of lattice basis reduction introduced for its proof, several new factorization algorithms were obtained [ChGr82, Len84, Kal85, Lan85, Len87, Lec05, BHKS05]. These algorithms succeeded in bringing to polynomial time the problem of factoring univariate and multivariate polynomials over algebraic number fields when given by their *dense* encoding, that is the input f is given by the list of all its terms of degree $\leq \deg(f)$ including the zero ones.

For practical purposes, it is worth considering the *lacunary encoding* of a polynomial. For instance, for an univariate polynomial with integer coefficients, it is the list of all pairs (a_i, α_i) —both integers written in binary encoding— where a_i is a non-zero coefficient corresponding to the exponent α_i. Thus the lacunary encoding is linear in the number of non-zero terms, in the logarithm of the degree and in the logarithm of the maximum absolute value of the coefficients of the considered polynomial. Since the degree of a polynomial can be exponentially big in its lacunary length, a direct application of the algorithms for factoring dense polynomials would give an exponential complexity.

Here we consider the problem of factoring a multivariate polynomial

$$f = \sum_{i=1}^{t} a_i X^{\alpha_i} \in K[X_1, \ldots, X_n]$$

with coefficients in a finite extension $K/\mathbb{Q}$, given in lacunary encoding, i.e. by the list $(a_i, \alpha_i)_{1 \leq i \leq t}$ of its non-zero coefficients and corresponding exponents. Let $\ell(f)$ denote the bit length of the lacunary encoding of f, which is, as mentioned above, the number of bits needed to spell out the data (see Section 4.3 for a precise definition in our setting). We obtain a deterministic algorithm for computing the low degree factors of the polynomial f, whose cost is polynomial in the lacunary length $\ell(f)$ and exponential in the number of variables n:

Theorem 2.1.1. *There is a deterministic algorithm that, given a multivariate (lacunary encoded) polynomial $f \in K[X_1, \ldots, X_n]$ and a natural number d, computes all irreducible factors of f in $K[X_1, \ldots, X_n]$ of degree $\leq d$ together with their multiplicities, within $(d \cdot \ell(f))^{O(n)}$ bit operations.*

Here we recall that $O(n)$ is the standard notation for cn for a universal constant c.

Let us observe on one hand that the restriction to bounded degree factors is unavoidable if we look for polynomial costs: the polynomial $f = X^p - 1$ (p a prime number) is of lacunary length of order $\log_2(p)$ but has the dense irreducible factor $X^{p-1} + \cdots + 1$ which clearly has p non-zero terms.

On the other hand, the following example, due to J. von zur Gathen and E. Kaltofen [GaKa85], shows that a polynomial dependence on the number of variables n is unfeasible: for any $n \in \mathbb{N}$, where n is a prime number, the polynomial

$$f = \prod_{i=1}^{n}(X_i^n - 1) + n\prod_{i=1}^{n}(X_i - 1) \in \mathbb{Z}[X_1, \ldots, X_n]$$

is divisible by the irreducible polynomial

$$g = \prod_{i=1}^{n}(X_i^{n-1} + \cdots + 1) + n \in \mathbb{Z}[X_1, \ldots, X_n].$$

But f has 2^{n+1} terms, small size coefficients (bounded by $n+1$), and its degree is $\deg(f) = n^n$, while g has $n^n = 2^{n\log_2(n)}$ terms and $\deg(g) = n(n-1)$. This shows that, for n sufficiently large, $\ell(g)$ has order $\ell(f)^{\log_2(n)}$.

The first result in the direction of Theorem 2.1.1 appeared in 1998, when F. Cucker, P. Koiran and S. Smale showed how to find all the integer roots of an univariate polynomial with integer coefficients in polynomial time in its lacunary encoding, and asked whether one can find in the same time the rational roots as well [CKS99]. This question (and more!) was affirmatively answered by H.W. Lenstra Jr. who presented an algorithm that, given a number field K and a univariate polynomial $f \in K[X]$, computes all its irreducible factors of degree $\leq d$ together with their multiplicities, in $(d + \ell(f))^{O(1)}$ bit operations [Len99b]. The first and inspiring result in the multivariate setting was obtained by E. Kaltofen and P. Koiran [KaKo05, Thm. 3] in 2005, who showed how to compute the *linear* factors of a bivariate polynomial $f \in \mathbb{Q}[X, Y]$ in polynomial time in $\ell(f)$. One year later, E. Kaltofen and P. Koiran [KaKo06] and T. Krick and M. Sombra together with the author of this thesis [AKS07] independently extended this result to an algorithm that computes all the factors of degree $\leq d$. The former paper solves the problem in the multivariate setting, however the algorithm presented there requires the a priori knowledge of an universal but non-explicit constant c [KaKo06, Thm. 1]. The latter only considers the bivariate case (which is straight-forward generalizable to the multivariate setting as we show here) and makes explicit all the constants, thus allowing the algorithm to be eventually implemented. Our approach also allows to compute not only the factors in a number field but also the absolute ones, i.e. the factors over the algebraic closure of the rational numbers.

All these algorithms (including ours) are based on a *gap* principle first applied by Cucker, Koiran and Smale for univariate integer polynomials. The idea is so strikingly simple and natural that it deserves to be explained in this introduction.

For $f \in \mathbb{Z}[X]$, how can we easily find its integer roots ξ? Gauss criterion gives us the possible values of a root ξ; however, even forgetting the huge number of possible choices for ξ, how can we test if $f(\xi) = 0$? Direct evaluation is not feasible, as the size of $f(\xi)$ can be exponentially big in the input size, except for the cases when $\xi = 0, \pm 1$. We also wish to avoid applying the dense factorization algorithms mentioned above since their cost depend polynomially on the degree of f.

So here is what the gap principle does: Assume that $f = \sum_{i=1}^{t} a_i X^{\alpha_i} \in \mathbb{Z}[X]$ can be split as

$$f = f_1 + X^{\beta} f_2$$

for non-zero polynomials f_1 of degree $\deg(f_1) = \alpha$ and f_2, where there is a gap between the exponents of f_1 and those of $X^{\beta} f_2$ of length

$$\beta - \alpha \geq \log_2 \|f\|_1$$

(here $\|f\|_1 = \sum_{i=1}^{t} |a_i|$ denotes as usual the 1-*norm* of f). Then, except for the cases $\xi = 0, \pm 1$, this implies that $f(\xi) = 0$ if and only $f_1(\xi) = f_2(\xi) = 0$: if this were not the case, namely $f(\xi) = 0$ but $f_2(\xi) \neq 0$, then

$$|f_1(\xi)| \leq \|f_1\|_1 \cdot |\xi|^{\alpha} < \|f\|_1 \cdot |\xi|^{\alpha} \quad \text{and} \quad |f_1(\xi)| = |\xi|^{\beta} \cdot |f_2(\xi)| \geq |\xi|^{\beta}$$

would lead us to $\|f\|_1 > |\xi|^{\beta-\alpha} \geq 2^{\beta-\alpha}$ in contradiction with the gap assumption! Therefore, to test if f vanishes at $\xi \neq 0, \pm 1$, one decomposes f into widely spaced short pieces

$$f = \sum_i X^i f_i$$

and tests if $f_i(\xi) = 0$ for all i. Furthermore, since the decomposition is independent from the point ξ, the integer roots can be found as the common roots of a set of low degree polynomials, applying any dense factorization algorithm.

The key ingredient that makes the above argument work is that any integer $\xi \neq 0, \pm 1$ satisfies a uniform lower bound $|\xi| \geq 2$! In order to apply the same idea to $\xi \in \mathbb{Q}$, the correct generalization of the absolute value is the *height*, defined as the maximum between relatively prime expressions for the numerator and denominator. By imitating the argument above, but this time for the usual absolute value *and* all the p-adic ones, we arrive at the same conclusion as a consequence that all rational numbers except $0, \pm 1$ have height at least 2. This is essentially what Lenstra applied in [Len99b]; more generally, he was able to handle in this way other factors besides the linear ones by considering the height of their roots after applying a suitable lower bound for them, namely Dobrowolski's theorem [Dob79] in the version of P. Voutier [Vou96]. In [KaKo05], the authors succeeded to present the first generalization of this gap principle for non-univariate polynomials, more precisely for linear factors of bivariate polynomials.

As in these previous works, the key of our algorithm is a suitable gap theorem. We obtain it as a consequence of a lower bound for the height of Zariski dense sets lying on a hypersurface due

to F. Amoroso and S. David [AmDa00] and further refined by C. Pontreau [Pon05, Thm. 1.9] in order to make the constants explicit. This is explained in detail in Sections 4.1 and 4.2. This result allows us to decompose the given polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ into short pieces; the factors of f are then computed as the common factors of these low degree pieces. This strategy works for all factors except the monomials and the cyclotomic ones, that is, factors which are a product of binomials whose coefficients are roots of the unity. These factors have to be handled separately, as explained in Section 4.3.

Since our algorithm operates by reducing to the cases of dense multivariate and lacunary univariate polynomials, our concern is only to prove that this reduction can be done in polynomial time in the lacunary encoding. We have not attempted to compute the exponent in the complexity estimate, which in principle can be quite big.

As a consequence of the algorithm, we derive that the number of irreducible factors of degree $\leq d$ of $f \in \mathbb{Q}[X_1, \ldots, X_n]$ counted with multiplicities (except for the monomial factors) is bounded by $(d \cdot \ell(f))^{O(n)}$. This is not trivial, as the degree of f can be exponential in $\ell(f)$, but in fact much better can be said:

Proposition 2.1.2. *Let $f \in \mathbb{Z}[X_1, \ldots, X_n]$ and consider the factorization*

$$f = q \cdot \prod_p p^{e_p}$$

where q is a cyclotomic polynomial, $p \in \mathbb{Q}[X_1, \ldots, X_n]$ runs over all non-cyclotomic irreducible factors of f, and e_p is the corresponding multiplicity. Then

$$\sum_p e_p \leq 10^4 \cdot n^3 \cdot \log \|f\|_1 \cdot \log^3(n \max\{\deg(f), 16\}).$$

In particular the total number of non-cyclotomic irreducible factors of any degree of f is polynomially bounded in terms of the lacunary length of f. This property generalizes [Dob79, Thm. 2] and is a further consequence of the connection with the theory of heights in Diophantine Geometry.

Proposition 2.1.2 should be compared with another result of H.J. Lenstra Jr.: the total number of irreducible factors of degree $\leq d$ of $f \in \mathbb{Q}[X]$ counted with multiplicities (different from X) is bounded by

$$c \cdot t^2 \cdot 2^d \cdot d \cdot \log(2dt)$$

where t is the number of non zero terms of f [Len99a, Thm. 1]. This bound is exponential, but independent of the degree and coefficients of f. Based on these two results, it seems natural to consider the following generalization: is the number of all irreducible (and non-cyclotomic maybe?) factors that are not monomials of a t-nomial in $\mathbb{Q}[X]$ uniformly bounded by some function $B(t)$ depending only on t, and maybe even by $t^{O(1)}$?

Trying to get further, one might ask if it is possible to compute in polynomial time the *absolute* factorization of a polynomial given in lacunary encoding, that is, its irreducible factors over $\overline{\mathbb{Q}}$.

For the univariate case the answer is clearly "no": an univariate polynomial splits completely as a product of linear factors, and this cannot be done in lacunary polynomial time. For the multivariate case, it can be shown that the computation of binomial factors is equivalent to the factorization of a univariate polynomial, so that binomials factors over $\overline{\mathbb{Q}}$ cannot be computed either. Here, we show that except for these, we can compute all other irreducible factors over $\overline{\mathbb{Q}}$ of low degree, in lacunary polynomial time.

Theorem 2.1.3. *There is a deterministic algorithm that, given $f \in K[X_1, \ldots, X_n]$, where K is a number field, and $d \geq 1$, computes all irreducible factors of f in $\overline{\mathbb{Q}}[X_1, \ldots, X_n]$ of degree $\leq d$, together with their multiplicities, except for the binomial ones, in $(d \cdot \ell(f))^{O(n)}$ bit operations.*

This algorithm follows from another suitable gap theorem that we obtain as a consequence of another refined result by Pontreau [Pon05, Thm. 1.22]. Furthermore, we deduce from his result an analogue of Proposition 2.1.2 for the number of non-binomial absolute factors of a given $f \in \mathbb{Z}[X_1, \ldots, X_n]$.

Proposition 2.1.4. *Let $f \in \mathbb{Z}[X_1, \ldots, X_n]$ and consider the factorization*

$$f = q \cdot \prod_p p^{e_p}$$

where q is a product of binomials, $p \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ runs over all irreducible factors of f with at least three terms, and e_p is the corresponding multiplicity. Then

$$\sum_p e_p \leq 10^{14} \cdot n^{13} \cdot \log \|f\|_1 \cdot \log^5(\max\{n \deg(f), 16\}).$$

Let us end this section by observing that although the problem of finding all small degree factors of multivariate polynomials over number fields in polynomial time in the lacunary encoding of the input is now completely solved, the solution given here is only theoretical in the sense that due to the huge size of the constants involved, the algorithm –if implemented– would be absolutely impracticable. However, since it appears so often in topics in computational algebra, a first promising complexity result motivates the search for good practical algorithms. For instance, let us recall that during the search for good dense factorization algorithms over the rational numbers, the break-through (but inefficient) result of Lenstra, Lenstra and Lovasz [LLL82] finally led to the polynomial-time *and* efficient algorithm of M. van Hoeij [Hoe02, BHKS05]. In this sense there is still much work to be done here!

2.2 Interpolation of univariate integer lacunary polynomials

The results presented in this section were jointly obtained, as a part of my candidacy research, together with my advisor and Ariel Pacetti; these results have appeared in [AKP06].

Interpolation is a crucial ingredient in Mathematics. But most algorithms that interpolate univariate polynomials require that the number of given values equals essentially the degree of

the polynomial. Our motivation for this work is the search of an efficient interpolation algorithm for an integer univariate polynomial, where the number of interpolation points depends on the number of non-zero terms and not on the degree on the polynomial. We insist on the fact that the setting is that we will know that a polynomial has exactly (or at most) t non-zero terms, but we don't know anything about the set of exponents that arise with a non-zero coefficient. We are not speaking here about solving a basic linear algebra problem, but about recovering which are the terms (coefficient, exponent) appearing in the polynomial from its values on a reasonable number of interpolation points.

A polynomial is called *t-lacunary* if it has at most t non-zero terms. The problem of interpolating a t-lacunary polynomial from its values in a list of specific interpolation points where the number of these points does not depend on the degree but on t is called "lacunary interpolation". It received a lot of attention around 1990 and again recently, for instance in [BeTi88, Zip90, KaLa88, KLW90, KLL00, Lee01, KaLe03], [BoTi91], [DrGr91, GKS91], [GKS90, CDGK91] and [GKS94].

It is a well-known fact that, as a consequence of Descartes' Rule of Signs (Theorem 6.1.2), a t-lacunary polynomial $f \in \mathbb{R}[X]$ has at most $t-1$ distinct real positive roots. Therefore, any univariate t-lacunary polynomial in $\mathbb{C}[X]$ is uniquely determined by its value in $2t$ different positive values in $\mathbb{R}$ (since for two such polynomials, the difference of their real parts (or their imaginary parts) is a $2t$-lacunary polynomial which has at most $2t-1$ different real positive roots).

In [BeTi88], M. Ben-Or and P. Tiwari produced a beautiful deterministic algorithm that recovers such a t-lacunary polynomial $f \in \mathbb{C}[X]$ from its value in $2t$ different interpolation points of the form

$$x_1 = 1,\ x_2 = a,\ x_3 = a^2, \ldots, x_{2t} = a^{2t-1}.$$

They also raised the problem of producing an algorithm that interpolates a t-lacunary polynomial in $\mathbb{C}[X]$ from $2t$ arbitrary different real positive values, to emulate in some sense Lagrange interpolation algorithms that do not require specific interpolation input values, instead of imposing the starting points as they did.

Our algorithm relies essentially on an original new version of Newton-Hensel lifting that can be related to interpolation questions. The traditional Newton-Hensel lifting, known as Hensel lemma, is the algebraic (non-archimedean) counterpart of Newton's method. It was introduced by Hensel around 1900 and is the basis of the theory of p-adic numbers and their applications as in the local-global Hasse-Minkowski principle for quadratic forms. Since then, "Newton-Hensel lifting" is present in exact symbolic computation: for example in univariate rational polynomial factorization in [Zas69, LLL82] and in multivariate polynomial factorization [ChGr82, Chi84, Gri84, Kal85].

The version we develop here allows to lift polynomials in $\mathbb{Z}[X]$ from information modulo a prime number $p \neq 2$ to a power p^k for any k. The key point is that it does not only lifts the coefficients of the polynomial but also its *exponents*. This is achieved thanks to the map $L_p : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ defined by $x^{p-1} \equiv 1 + p\, L_p(x) \pmod{p^2}$ for $p \nmid x$ and $L_p(x) = 0$ for $p \mid x$ (see Definition 5.4.1), that

plays the role of the "logarithmic function modulo p" and enables us to linearize the equations whose unknowns are in the exponents.

Theorem 2.2.1. *Let $f = \sum_{j=1}^{t} a_j X^{e_j} \in \mathbb{Z}[X]$. Let $p > t$ be an odd prime number such that $p \nmid a_i$ for all i and $p-1 \nmid e_i - e_j$ for all $i \neq j$.*
Suppose that are given integer numbers $x_1, \ldots, x_{2t}$ and $y_1, \ldots, y_{2t}$ satisfying:

- $f(x_i) \equiv y_i \pmod{p}$ *for all* $1 \leq i \leq 2t$,
- $$\det \begin{bmatrix} L_p(x_1)x_1^{e_1} & \ldots & L_p(x_1)x_1^{e_t} & x_1^{e_1} & \ldots & x_1^{e_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ L_p(x_{2t})x_{2t}^{e_1} & \ldots & L_p(x_{2t})x_{2t}^{e_t} & x_{2t}^{e_1} & \ldots & x_{2t}^{e_t} \end{bmatrix} \not\equiv 0 \pmod{p}.$$

Then for every $k \in \mathbb{N}$ there exists $f^{(k)} = \sum_{j=1}^{t} a_j^{(k)} X^{e_j^{(k)}} \in \mathbb{Z}[X]$, that satisfies simultaneously:

- $f^{(k)}(x_i) \equiv y_i \pmod{p^k} \qquad 1 \leq i \leq 2t$,
- $a_j^{(k)} \equiv a_j \pmod{p}$ *and* $e_j^{(k)} \equiv e_j \pmod{(p-1)} \qquad 1 \leq j \leq t$.

Moreover, if $f^{(k)} = \sum_{j=1}^{t} a_j^{(k)} X^{e_j^{(k)}}$ and $g^{(k)} = \sum_{j=1}^{t} b_j^{(k)} X^{d_j^{(k)}} \in \mathbb{Z}[X]$ are two such polynomials, then

$$a_j^{(k)} \equiv b_j^{(k)} \pmod{p^k} \quad \text{and} \quad e_j^{(k)} \equiv d_j^{(k)} \pmod{\varphi(p^k)} \quad \text{for all} \quad 1 \leq j \leq t,$$

where φ denotes the Euler map.

In fact we show something that we find interesting on its own, besides its possible application to interpolation: that this result corresponds exactly to a Hensel lifting of a system of $2t$ generalized equations in $2t$ unknowns, where the unknowns are the t coefficients of f in the p-adic integers $\mathbb{Z}_p$ and the t exponents of f in some suitable set E_p (see Definition 5.2.1), and where the condition that the defined determinant does not vanish modulo p is the corresponding classical condition on the Jacobian determinant of the system.

For this purpose we introduce the ring E_p of "allowed exponents" (whose additive group is isomorphic to the p-adic unit group $\mathbb{Z}_p^\times$), where "allowed" means that for $x \in \mathbb{Z}_p^\times$ and $\alpha \in E_p$ we have a consistent definition of $x^\alpha \in \mathbb{Z}_p^\times$. After introducing this ring, it make sense to consider generalized polynomial expressions in $\mathbb{Z}_p$, where the variables belong to $\mathbb{Z}_p^\times$ and the exponents belong to E_p.

Here, among all the equivalent descriptions of $\mathbb{Z}_p$ we adopt the following one that we consider more suitable for our formulations:

$$\mathbb{Z}_p = \left\{ (a_i)_{i \geq 1} \in \mathbb{Z}^{\mathbb{N}} \ : \ a_i \equiv a_{i+1} \bmod p^i \ \forall\, i \right\} / \sim$$

where $\sim$ is the equivalence relation given by

$$(a_i)_{i \geq 1} \sim (b_i)_{i \geq 1} \iff a_i \equiv b_i \bmod p^i, \ \forall\, i.$$

Likewise, we define E_p as:

$$E_p = \left\{ (a_i)_{i\geq 1} \in \mathbb{Z}^{\mathbb{N}} \ : \ a_i \equiv a_{i+1} \bmod \varphi(p^i) \ \forall\, i \right\} / \simeq$$

where $\simeq$ is the equivalence relation given by

$$(a_i)_{i\geq 1} \simeq (b_i)_{i\geq 1} \iff a_i \equiv b_i \bmod \varphi(p^i), \ \forall\, i.$$

In both rings, the operations (including the exponential map) are coordinate-wise.

$$x = \overline{(x_i)_{i\geq 1}} \in \mathbb{Z}_p \ \text{ and } \ e = \overline{(e_i)_{i\geq 1}} \in E_p \ \longrightarrow \ x^e = \overline{(x_i^{e_i})_{i\geq 1}}$$

A complete study of these data structure is given in Sections 5.1 and 5.2. In the following sections, two different kinds of systems of generalized polynomial equations are considered: the first one (called pseudo-polynomial equations) differs from the classical polynomial equations in the fact that the exponents are allowed to be constants in E_p instead of natural numbers, and the second one (called exponential equations) has as unknowns the exponents of the monomials. We show that the existence of a solution modulo p plus some reasonable Jacobian-like condition (called Lifting Condition) guarantee the existence of a solution in the corresponding ring $\mathbb{Z}_p$ or E_p. We also show that these two kinds of equations are related by a logarithmic-exponential change of variables.

Coming back to our interpolation problem, Theorem 2.2.1 enables us to give a satisfactory answer to the question in the case that the input polynomial f satisfies the good reduction property modulo the chosen prime number p and that the evaluation points $x_1, \ldots, x_{2t}$ chosen as starting evaluation points satisfy the Jacobian-like property (the non-vanishing of the determinant) described in the hypothesis. We also produce large families of short height suitable starting points in Theorem 5.6.4.

In order to answer Ben-Or and Tiwari question in its full generality, we still idealistically need a criterion to choose, in terms of the evaluation values $y_i = f(x_i)$, a (small) prime number p such that f has the good reduction property modulo p. This would be the analog of the choice of the prime in the univariate rational polynomial factorization algorithms (the condition in this case is given by the non-vanishing of a discriminant modulo p), and in the archimedean setting, a (still unknown) criterion for the choice of an approximate zero. More realistically, we would at least need a satisfactory probabilistic argument for the choice of such a prime in a given range (that we are still unable to produce).

2.3 Estimates for the number of roots of lacunary systems

The results presented in this section correspond to the results obtained by the author during his candidacy work in [Ave08].

We already mentioned Descartes' Rule of Signs, which establishes that the number of positive real roots of a polynomial $f \in \mathbb{R}[X]$, counted with multiplicities, is bounded by the number of

changes of signs in its ordered vector of coefficients, skipping the zeros. As a direct consequence, the number of real roots of f is bounded by $2t-1$, where t is its number of non-zero terms (here the at most $t-1$ positive roots and at most $t-1$ negative roots are counted with multiplicities, while the possible root 0 is counted at most once).

There are not yet natural generalizations of Descartes' Rule of Signs for the multivariate setting, but a lot of work has been and is being done for estimating the number of real isolated or non-degenerated roots (that is, where the Jacobian does not vanish, condition that implies that the root is isolated) of multivariate square systems of real polynomials in the positive orthant, in terms of the number of variables and the number of non-zero terms that the system involves.

The main result in that direction is due to A. Khovanskii [Kho91]. A simplified version of it implies that a square system of n real polynomial equations in n indeterminates, which involves in total t non-zero terms has at most $(n+1)^t 2^{t(t-1)/2}$ non-degenerated real roots in the positive orthant. Further improvements of Khovanskii's result have been obtained by F. Bihan and F. Sottile, however the exponential dependence on the number of non-zero terms t can not be avoided yet [BiSo06, BBS07].

In [LRW03], T.Y. Li, M. Rojas and X. Wang (see also D. Perrucci [Per05]) studied particular cases of bivariate square systems and showed that the number of common isolated or non-degenerated roots of a trinomial and a polynomial with at most t non-zero terms, $t \geq 3$, is bounded by $2^t - 2$.

Furthermore, Kushnirenko's Conjecture, formulated in the mid-1970' (which says that a square system of n real polynomial equations in n indeterminates such that the k-th polynomial has t_k non-zero terms should have at most $(t_1-1)\cdots(t_n-1)$ non-degenerate roots in the positive orthant) turned out to be false, by the counter-example provided by B. Haas in 2002 for a system of two trinomials in two variables [Haa02].

The main result of this article is a refinement of the result in [LRW03] for the particular case when the trinomial is a linear polynomial. Without loss of generality we can assume the linear polynomial to be of the form $Y - aX - b$ and we thus study the possible number of real roots of a bivariate polynomial on a line $Y = aX + b$:

Theorem 2.3.1. *Let $f = \sum_{i=1}^{t} a_i X^{\alpha_i} Y^{\beta_i} \in \mathbb{R}[X,Y]$ be a polynomial with at most t non-zero terms, and let $a, b \in \mathbb{R}$. Set $g(X) = f(X, aX+b)$. Then either $g \equiv 0$ or g has at most $6t-4$ real roots, counted with multiplicities except for the possible roots 0 and $-b/a$ that are counted at most once.*

To our knowledge, this is the first time a non-exponential bound is achieved for this kind of systems: there were no polynomial known bounds even for simple cases of families of polynomials.

As a consequence of our result we derive an alternative algorithm for checking whether a given linear form $Y - aX - b$ divides a polynomial f in in $K[X,Y]$, where K is a real number field. The number of bit operations performed by the algorithm is polynomial on the degree $[K : \mathbb{Q}]$

of the field extension, on the number t of non-zero terms of f, on the logarithm of the degree of f and on the logarithmic height of a, b and f. The first algorithm for this purpose can be deduced from the more general result by E. Kaltofen and P. Koiran [KaKo05] mentioned in Section 2.1. Here, instead of applying the gap principle, we reduce the problem to the univariate case by considering specializations $f(X, X^n)$ for small values of n, therefore without destroying the lacunary structure of f.

It is worth mentioning that the tools we use are completely elementary: we are now studying the possibility of extending the results for more general systems.

Chapter 3

Preliminaries

3.1 Absolute values

Definition 3.1.1. *Let K be a field. An absolute value v on K is a map $v : K \to \mathbb{R}_{\geq 0}$ satisfying the following three properties:*

- $v(x) = 0 \quad \Leftrightarrow \quad x = 0$,
- $v(xy) = v(x)\, v(y) \quad \forall\, x, y \in K$,
- $v(x + y) \leq v(x) + v(y) \quad \forall\, x, y \in K$ *(triangle inequality).*

We also use $|x|_v$ to denote $v(x)$. If the absolute value satisfies, in addition to the triangle inequality, the stronger condition:

- $v(x + y) \leq \max\{v(x), v(y)\} \quad \forall\, x, y \in K$ *(ultrametric inequality),*

then we say that it is non-Archimedean.

It is clear, from the definition, that every absolute value v on a field K satisfies $v(1) = v(-1) = 1$ and $v(x) = v(-x)$ for all $x \in K$.

Example. *1. On an arbitrary field K, the trivial absolute value:*

$$v(x) = \begin{cases} 0 & \text{if} \quad x = 0 \\ 1 & \text{if} \quad x \neq 0. \end{cases}$$

2. On $\mathbb{R}$ or $\mathbb{C}$, the standard absolute value $|x|$.

3. On $\mathbb{Q}$, for every integer prime number $p \in \mathbb{N}$, the p-adic absolute value v_p given by:

$$v_p\left(p^r \frac{a}{b}\right) = p^{-r},$$

where $a, b, r \in \mathbb{Z}$, $b > 0$, $p \nmid a$ and $p \nmid b$.

4. *On $K(T)$, the absolute value $v_\infty(F/G) = 2^{\deg(F)-\deg(G)}$, where F, G are non-zero polynomials in $K[T]$.*

5. *On $K(T)$, for every $P \in K[T]$ irreducible, the absolute value v_P given by:*

$$v_P\left(P^r \frac{F}{G}\right) = 2^{-r},$$

where $r \in \mathbb{Z}$, $F, G \in K[T] - \{0\}$, $P \nmid F$ and $P \nmid G$.

The absolute values given in items (1) to (5), except (2), are non-Archimedean. The standard absolute value on $\mathbb{C}$ is written v_∞, $|\cdot|$, $|\cdot|_\infty$ or $|\cdot|_{v_\infty}$ indistinctly, and the p-adic absolute value v_p on $\mathbb{Q}$ is also $|\cdot|_p$ or $|\cdot|_{v_p}$.

Lemma 3.1.2. *Let v be an absolute value on a field K. Then v is non-Archimedean if and only if $v(\mathbb{N})$ is bounded.*

Proof. If v is non-Archimedean, then for every natural number $n \in \mathbb{N}$ we have:

$$v(n) = v(1 + \cdots + 1) \leq \max\{v(1), \ldots, v(1)\} = 1,$$

and therefore $v(\mathbb{N})$ is bounded. Now suppose that $v(n) \leq C$ for all $n \in \mathbb{N}$. Then, for every $x, y \in K$,

$$v(x+y)^n \leq \sum_{i=0}^{n} \left|\binom{n}{i}\right|_v v(x)^i v(y)^{n-i} \leq nC \max\{v(x), v(y)\}^n,$$

and taking its n-th root,

$$v(x+y) \leq (nC)^{1/n} \max\{v(x), v(y)\}.$$

The ultrametric inequality follows taking limits in the previous expression. □

Lemma 3.1.3. *Let v be a non-Archimedean absolute value on a field K. Let $a_1, \ldots, a_n \in K$ be such that $v(a_1) > v(a_i)$ for all $i \neq 1$. Then $v(a_1 + \cdots + a_n) = v(a_1)$.*

Proof. It is enough to prove the case $n = 2$. Suppose $v(a_1) > v(a_2)$. The inequalities:

$$v(a_1) = v(a_1 + a_2 - a_2) \leq \max\{v(a_1 + a_2), v(a_2)\} \leq \max\{v(a_1), v(a_2), v(a_2)\} = v(a_1)$$

imply that $v(a_1) = \max\{v(a_1 + a_2), v(a_2)\}$. This maximum is not $v(a_2)$ because $v(a_1) > v(a_2)$. Then $v(a_1) = v(a_1 + a_2)$. □

An absolute value v on a field K, induces on it the metric $d(x, y) = v(x - y)$. The arithmetic operations (addition, additive inverse, multiplication and multiplicative inverse) are continuous with respect to this metric.

Lemma 3.1.4. *Let v_1 and v_2 be non-trivial absolute values on a field K. Then, the following statements are all equivalent:*

1. *v_1 and v_2 induce the same topology.*

2. *for all $x \in K$, if $v_1(x) < 1$ then $v_2(x) < 1$.*

3. *$\exists \lambda > 0$ such that $v_1(x) = v_2(x)^\lambda$ for every $x \in K$.*

Proof. $(1 \Rightarrow 2)$: Let $x \in K$ be such that $v_1(x) < 1$. Then $x^n \to 0$ with respect to the topology induced by v_1. Since both absolute values induce the same topology, we also have $x^n \to 0$ with respect to v_2, i.e. $v_2(x)^n \to 0$. This implies that $v_2(x) < 1$.
$(2 \Rightarrow 3)$: We know that $v_1(x) < 1$ implies $v_2(x) < 1$, and using this fact for x^{-1}, we have that $v_1(x) > 1$ implies $v_2(x) > 1$. Since v_1 is non-trivial, there exists $z \in K$ such that $v_1(z) > 1$. Let $a = v_1(z)$, $b = v_2(z)$ and $\lambda = \log(a)/\log(b)$. Note that $v_1(z) = v_2(z)^\lambda$. Now take any non-zero $x \in K$. Then $v_1(x) = v_1(z)^\alpha$ for some $\alpha \in \mathbb{R}$. It is enough to prove that $v_2(x) = v_2(z)^\alpha$, because in this case we have $v_1(x) = v_1(z)^\alpha = v_2(z)^{\alpha\lambda} = v_2(x)^\lambda$. If $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ satisfy $\alpha < m/n$, then $v_1(x) < v_1(z)^{m/n}$. This implies that $v_1(x^n/z^m) < 1$ and then $v_2(x^n/z^m) < 1$, i.e. $v_2(x) < v_2(z)^{m/n}$. Therefore $v_2(x) \leq v_2(z)^\alpha$ because we can freely choose m/n as close to α as we want. The other inequality follows using the same idea, but taking $\alpha > m/n$.
$(3 \Rightarrow 1)$: Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in K. Then: $x_n \to x$ with respect to the topology induced by $v_1 \Leftrightarrow v_1(x_n - x) = v_2(x_n - x)^\lambda \to 0 \Leftrightarrow v_2(x_n - x) \to 0 \Leftrightarrow x_n \to x$ with respect to v_2. □

Theorem 3.1.5. [Ostrowski] *Let v be a non-trivial absolute value on $\mathbb{Q}$. Then either v is Archimedean and there exists $0 < \lambda \leq 1$ such that $v(x) = |x|^\lambda$, or v is non-Archimedean and there exists a prime number $p \in \mathbb{N}$ and $\lambda > 0$ such that $v(x) = v_p(x)^\lambda$.*

Proof. For every integer $k \in \mathbb{Z}$ we have $v(k) = v(|k|) = v(1 + \cdots + 1) \leq v(1) + \cdots + v(1) = |k|$. Let $a, b, m \in \mathbb{Z}$ with $a > 1$, $b > 1$ and $m \geq 0$. Suppose that $b^m = c_0 + c_1 a + \cdots + c_n a^n$ is the a-adic representation of b^m, i.e. $0 \leq c_i < a$ for all i and $c_n \neq 0$. In particular, we have $a^n \leq b^m$ and then $n \leq m \log(b)/\log(a)$. Define $M = \max\{1, v(a)\}$.

$$\begin{aligned} v(b^m) &\leq v(c_0) + \cdots + v(c_n)v(a)^n \leq a(1 + \cdots + v(a)^n) \\ &\leq a(1 + \cdots + M^n) \leq a(n+1)M^n \end{aligned}$$

$$\Rightarrow \quad v(b)^m \leq a(n+1)M^n \leq a\left(1 + m\tfrac{\log(b)}{\log(a)}\right) M^{m\log(b)/\log(a)}$$

$$\Rightarrow \quad \left(\tfrac{v(b)}{M^{\log(b)/\log(a)}}\right)^m \leq a\left(1 + m\tfrac{\log(b)}{\log(a)}\right)$$

$$\Rightarrow \quad \tfrac{v(b)}{M^{\log(b)/\log(a)}} \leq \left(a\left(1 + m\tfrac{\log(b)}{\log(a)}\right)\right)^{1/m} \to 1$$

$$\Rightarrow \quad v(b) \leq M^{\log(b)/\log(a)} = \max\{1, v(a)^{\log(b)/\log(a)}\}. \qquad (*)$$

Case v Archimedean: By Lemma 3.1.3, there exists $b \in \mathbb{N}$ such that $v(b) > 1$. If we had $v(a) \leq 1$ for some integer $a > 1$, then $(*)$ would imply the contradiction $v(b) \leq 1$. Therefore $v(a) > 1$ for every integer $a > 1$. Then, for every $a, b \in \mathbb{N}$ with $a > 1$ and $b > 1$, the inequality $(*)$ is

$$v(b) \leq v(a)^{\log(b)/\log(a)}$$

or more simply $v(b)^{1/\log(b)} \leq v(a)^{1/\log(a)}$. By the symmetry of this expression, swapping a and b, we get the identity:

$$v(b)^{1/\log(b)} = v(a)^{1/\log(a)} \quad \forall\, a, b \in \mathbb{N},\ a > 1,\ b > 1.$$

Now take $b \in \mathbb{N}$, $b > 1$ and let $0 < \lambda \leq 1$ be such that $v(b) = b^{\lambda}$. For any $a \in \mathbb{N}$, $a > 1$ we have:

$$v(a) = v(b)^{\frac{\log(a)}{\log(b)}} = b^{\lambda \frac{\log(a)}{\log(b)}} = 2^{\log(b)\lambda \frac{\log(a)}{\log(b)}} = 2^{\lambda \log(a)} = a^{\lambda}.$$

This means that for all $k \in \mathbb{Z}$, $v(k) = v(|k|) = |k|^{\lambda}$ holds. We conclude taking $x = p/q \in \mathbb{Q}$ with $p \in \mathbb{N}$ and $q \in \mathbb{Z}$, and then

$$v(x) = v\left(\frac{p}{q}\right) = \frac{v(p)}{v(q)} = \frac{|p|^{\lambda}}{|q|^{\lambda}} = |x|^{\lambda}.$$

Case v non-Archimedean: Here we have $v(x) \leq 1$ for all $x \in \mathbb{Z}$. Define

$$I = \{x \in \mathbb{Z} \ :\ v(x) < 1\}.$$

By the multiplicativity of v and the ultrametric inequality, the set I is an ideal of Z. Moreover, if $x, y \in \mathbb{Z}$ and $xy \in I$, then $v(x) \leq 1$, $v(y) \leq 1$ and $v(xy) < 1$. This is only possible if $v(x) < 1$ or $v(y) < 1$, i.e. $x \in I$ or $y \in I$. Therefore I is a non-trivial prime ideal of $\mathbb{Z}$. Let $p \in \mathbb{N}$ be the prime number such that $I = p\mathbb{Z}$. For any $x = p^r \frac{a}{b} \in \mathbb{Q} - \{0\}$ with $a, b, r \in \mathbb{Z}$, $b > 0$, $p \nmid a$ and $p \nmid b$, we have that $a \notin I$ and $b \notin I$. Then $v(a) = 1$, $v(b) = 1$ and

$$v(x) = v(p)^r \frac{v(a)}{v(b)} = v(p)^r = p^{\frac{\log(p)}{\log(v(p))}\, r} = v_p(x)^{-\frac{\log(p)}{\log(v(p))}}.$$

Note that $\lambda = -\log(p)/\log(v(p)) > 0$, because $p \in I$ implies $v(p) < 1$. □

Theorem 3.1.6. *Let v be an absolute value on a field K. Then, there exists an extension K_v/K and an absolute value $\overline{v}$ on K_v extending v, such that K_v is complete and $K \subseteq K_v$ is dense. Moreover, if E/K is an extension with an absolute value w extending v, such that E is complete and $K \subseteq E$ is dense, then there exists a K-isomorphism of fields $\sigma : E \to K_v$ with $w = \overline{v} \circ \sigma$.*

Proof. See [Lan93, Ch. 12, Prop. 2.1]. □

The field K_v together with the absolute value $\overline{v}$ of Theorem 3.1.6 is called the completion of K with respect to v. For instance, the completion of $\mathbb{Q}$ with respect to $|\cdot|$ is $\mathbb{R}$, and the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is the field of p-adic numbers $\mathbb{Q}_p$.

Theorem 3.1.7. *Let K be a complete field with respect to a non-trivial absolute value v and let E/K be an algebraic extension. Then, there exists a unique absolute value w on E extending v. Moreover, if E/K is finite, then E is complete with respect to w.*

Proof. See [Lan93, Ch. 12, Prop. 2.5]. □

Let K be a complete field with respect to a non-trivial absolute value v and let E/K be a Galois extension. If w is an absolute value on E extending v and $\sigma \in \mathrm{Gal}(E/K)$, then $w \circ \sigma$ is also an absolute value on E extending v. By Theorem 3.1.7 (uniqueness), we have $w = w \circ \sigma$. Taking the product over all $\sigma \in \mathrm{Gal}(E/K)$, we get:

$$w(x)^{[E:K]} = \prod_{\sigma \in \mathrm{Gal}(E/K)} w(\sigma(x)) = w\left(N_K^E(x)\right) = v\left(N_K^E(x)\right),$$

i.e.,

$$w(x) = v\left(N_K^E(x)\right)^{1/[E:K]}. \tag{3.1}$$

For instance, if $(K, v) = (\mathbb{R}, |\cdot|)$, Theorem 3.1.7 and Formula (3.1) prove that the only extension of $|\cdot|$ to $\mathbb{C}$ is given by $|a + bi| = (a^2 + b^2)^{1/2}$.

Let v be a non-trivial absolute value on a field K, let K_v be the completion of K with respect to v and let $\overline{K_v}$ be the algebraic closure of K_v. The absolute value $\overline{v}$ on K_v, and the only absolute value on $\overline{K_v}$ extending $\overline{v}$ will all be written v for simplicity of notation.

Every finite extension E/K can be embedded in $\overline{K_v}$, and for every embedding $\sigma : E \to \overline{K_v}$, we get an absolute value $w = v \circ \sigma$ extending v. The converse is given by the following theorem.

Theorem 3.1.8. *Let v be a non-trivial absolute value on a field K and let E/K be a finite extension with an absolute value w extending v. Then, there exists an embedding $\sigma \in \mathrm{Hom}_K(E, \overline{K_v})$ such that $w = v \circ \sigma$.*

Proof. Let E_w be the completion of E with respect to w, let $\overline{E_w}$ be the algebraic closure of E_w and let K_w be the (topologic) closure of K in E_w. The composite EK_w is contained in E_w because $E \subseteq E_w$ and $K_w \subseteq E_w$. Besides, EK_w/K_w is finite (because E/K is finite) and K_w is complete (because it is a closed subset in the complete field E_w), thus EK_w is also complete (by Theorem 3.1.7). Since $E \subseteq EK_w$, we also have $E_w \subseteq EK_w$. Therefore $E_w = EK_w$ and E_w/K_w is a finite extension with $[E_w : K_w] = [EK_w : K_w] \leq [E : K]$. In particular, $\overline{E_w}$ is an algebraic closure of K_w.
The field K_w with the absolute value w satisfies the hypothesis of Theorem 3.1.6, i.e. K_w is complete, K is dense in K_w and $w|_K = v$. Then, there exists a K-isomorphism $\sigma : K_w \to K_v$ such that $w = v \circ \sigma$. We can extend σ to a K-isomorphism $\tilde{\sigma} : \overline{E_w} \to \overline{K_v}$, and by Formula (3.1), we still have $w = v \circ \tilde{\sigma}$ in $\overline{E_w}$. We conclude by restricting $\tilde{\sigma}$ to E. □

Definition 3.1.9. *Let v be a non-trivial absolute value on a field K and let E/K be a finite extension with an absolute value w extending v. The local degree of the extension is defined as $N_w = [E_w : K_w]$, where K_w is the topologic closure of K in E_w.*

For instance, suppose that $(K, v) = (\mathbb{Q}, |\cdot|)$ and $E = \mathbb{Q}(\xi_5)$ where $\xi_5 = \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})$ is a 5-th root of the unity. In this case we have $K_v = \mathbb{R}$ and $\overline{K_v} = \mathbb{C}$. According to Theorem 3.1.8, every absolute value w on $\mathbb{Q}(\xi_5)$ extending $|\cdot|$ is given by embedding $\mathbb{Q}(\xi_5)$ in $\mathbb{C}$ with the standard absolute value, i.e. $w(x) = |\sigma(x)|$ where $\sigma : \mathbb{Q}(\xi_5) \to \mathbb{C}$ is a $\mathbb{Q}$-embedding. Therefore there

are only 4 possible absolute values $w_1, \dots, w_4$ on $\mathbb{Q}(\xi_5)$ extending $|\cdot|$, given by the embeddings $\sigma_i(\xi_5) = \xi_5^i$ with $i = 1, \dots, 4$. It is clear that σ_1 is the identity and σ_4 is the complex conjugation, thus they induce the standard absolute value $w_1 = |\cdot|$ on $\mathbb{Q}(\xi_5)$. On the other hand, σ_2 and σ_3 induce a different absolute value w_2 on $\mathbb{Q}(\xi_5)$ because $w_2(1+\xi_5) = |1+\xi_5^2| = |1+\xi_5^3| < 1$ and $w_1(1+\xi_5) = |1+\xi_5| > 1$. As we will see in next theorem, this example generalizes to the general case.

Definition 3.1.10. *Two embeddings $\sigma, \tau : E \to \overline{K_v}$ are conjugated if there exists a K_v-isomorphism $\lambda : \overline{K_v} \to \overline{K_v}$ such that $\sigma = \lambda \circ \tau$.*

Theorem 3.1.11. *Let v be a non-trivial absolute value on a field K and let E/K be a finite extension. Two embeddings $\sigma, \tau : E \to \overline{K_v}$ induce the same absolute value on E if and only if they are conjugated.*

Proof. Suppose that σ and τ are conjugated, i.e. $\sigma = \lambda \circ \tau$ where $\lambda : \overline{K_v} \to \overline{K_v}$ is a K_v-isomorphism. They induce on E the absolute values $w_\sigma = v \circ \sigma$ and $w_\tau = v \circ \tau$ respectively. The absolute values v and $v \circ \lambda$ on $\overline{K_v}$ coincide on K_v. Therefore we have $v = v \circ \lambda$ by Theorem 3.1.7, and then $w_\sigma = v \circ \sigma = v \circ \lambda \circ \tau = v \circ \tau = w_\tau$.
Now suppose that σ and τ induce the same absolute value on E. We extend the K-isomorphism $\lambda = \sigma \circ \tau^{-1} : \tau E \to \sigma E$ to a K_v-isomorphism $\overline{\lambda} : \tau E \cdot K_v \to \sigma E \cdot K_v$ via sequences: since τE is dense in $\tau E \cdot K_v$, every $x \in \tau E \cdot K_v$ is a limit $x = \lim \tau(x_n)$ for some sequence $x_n \in E$, then we can define $\overline{\lambda}(x) = \lim \sigma(x_n)$ that converges because τ and σ induce the same absolute value and $\sigma E \cdot K_v$ is complete. It is clear that $\overline{\lambda}$ is well defined, i.e. it does not depend on the sequence, and $\sigma = \overline{\lambda} \circ \tau$. Besides, $\overline{\lambda} : \tau E \cdot K_v \to \sigma E \cdot K_v$ is an isomorphism because we can define an inverse $\gamma : \sigma E \cdot K_v \to \tau E \cdot K_v$ by extending $\lambda^{-1} : \sigma E \to \tau E$ using the same construction. Moreover, $\overline{\lambda}$ fixes K_v because for every $x \in K_v$ we have a sequence $x_n \in K$ such that $x = \lim x_n = \lim \tau(x_n) = \lim \sigma(x_n) = \overline{\lambda}(x)$. We conclude by extending $\overline{\lambda}$ to the algebraic closure $\overline{K_v}$. □

We write $w|v$ to indicate that w is an absolute value extending v.

Proposition 3.1.12. *Let v be an absolute value on a field K and let E/K be a separable finite extension. Then, for every absolute value w on E extending v, we have*

- $N_w = \#\{\sigma : E \to \overline{K_v},\ K\text{-embedding},\quad s.t.\ w = v \circ \sigma\}$
- $[E : K] = \sum_{w|v} N_w$.

Proof. Let $\alpha \in E$ such that $E = K(\alpha)$ and let $f \in K[X]$ be the minimal polynomial of α over K. Suppose that $f = f_1 \dots f_r$ is the factorization into irreducibles of f in $K_v[X]$, where because α is separable, $f_i \neq f_j$ for $i \neq j$. The embeddings of E in $\overline{K_v}$ are the K-morphisms that map α to a root of f, and two such embeddings are conjugated if and only if they map α to a root of the same factor f_i. This implies that there are exactly r absolute values $w_1, \dots, w_r$ on E extending v. Also, $E_{w_i} = EK_{w_i} = K_{w_i}(\alpha)$, and since K_v and K_{w_i} are isomorphic, f_i (up to this isomorphism) is also the minimal polynomial of α in $K_{w_i}[X]$. This means that $N_{w_i} = [E_{w_i} : K_{w_i}] = [K_{w_i}[\alpha] : K_{w_i}] = \deg(f_i)$ equals the number of embeddings that induce w_i. Moreover $\sum_{i=1}^r N_{w_i} = \sum_{i=1}^r \deg(f_i) = \deg(f) = [E : K]$. □

Corollary 3.1.13. *Let v be an absolute value on a field K and let E/K be a separable finite extension. Then, for every $x \in E$ we have*

$$\prod_{w|v} |x|_w^{N_w} = |N_K^E(x)|_v.$$

Proof. Let $\sigma_1, \dots, \sigma_n$ be all the embeddings of E in $\overline{K_v}$, then

$$v(N_K^E(x)) = \prod_{i=1}^{n} v(\sigma_i(x)) = \prod_{w|v} \prod_{\substack{i: \\ w=v\circ\sigma_i}} w(x) = \prod_{w|v} w(x)^{N_w}.$$

□

Notation. *We write $M_{\mathbb{Q}} = \{v_p \ : \ p \text{ prime or } p = \infty\}$ for the set of standard and p-adic absolute values on $\mathbb{Q}$. Moreover, if $K/\mathbb{Q}$ is a finite extension, we write M_K for the set of all the extension to K of the absolute values in $M_{\mathbb{Q}}$ and M_K^∞ for the subset of Archimedean absolute values in M_K.*

$$M_K = \{w \ : \ w|v \text{ for some } v \in M_{\mathbb{Q}}\} \qquad M_K^\infty = \{w \ : \ w|v_\infty\}.$$

A remarkable property of the absolute values in $M_{\mathbb{Q}}$ is that $\prod_{v\in M_{\mathbb{Q}}} |x|_v = 1$ for all $x \in \mathbb{Q}^\times$. This holds because if $x = \pm p_1^{n_1} \cdots p_r^{n_r} \in \mathbb{Q}^\times$ where $p_i \in \mathbb{N}$ are (distinct) primes and $n_i \in \mathbb{Z}$, then $v_{p_i}(x) = p_i^{-n_1}$ for $1 \le i \le r$ and $v_p(x) = 1$ for all $p \neq p_i$ for some i, and $v_\infty(x) = p_1^{n_1} \dots p_r^{n_r}$.
Moreover, this property holds over every finite extension $K/\mathbb{Q}$ if we take into account the local degrees N_w. More precisely, for every $x \in K^\times$ we have:

$$\prod_{w\in M_K} |x|_w^{N_w} = \prod_{v\in M_{\mathbb{Q}}} \prod_{w|v} |x|_w^{N_w} = \prod_{v\in M_{\mathbb{Q}}} |N_{\mathbb{Q}}^K(x)|_v = 1. \tag{3.2}$$

This identity is known as the "product formula".

Definition 3.1.14. *Let v be an absolute value on a field K and let $a = (a_1, \dots, a_d) \in K^d$ be a vector. We define the 1-norm, 2-norm and ∞-norm by:*

- $\|a\|_{1,v} = \sum_{i=1}^d |a_i|_v$,
- $\|a\|_{2,v} = \left(\sum_{i=1}^d |a_i|_v^2\right)^{1/2}$,
- $\|a\|_v = \|a\|_{\infty,v} = \max\{|a_i| \ : \ 1 \le i \le d\}$.

When $K \subseteq \mathbb{C}$ and v is not explicitly written, we assume $v = v_\infty$. These norms are also defined for polynomials $f = \sum_{i=0}^d a_i x^i \in K[X_1, \dots, X_n]$, using the vector of coefficients of f, i.e. as $\|f\|_{\cdot,v} = \|(a_0, \dots, a_d)\|_{\cdot,v}$.

Remark. *For every $a \in K^d$ we have:*

$$\|a\|_{\infty,v} \le \|a\|_{2,v} \le \|a\|_{1,v} \le d\,\|a\|_{\infty,v}.$$

3.2 Height of algebraic numbers

Definition 3.2.1. *Let $K/\mathbb{Q}$ be a finite extension. The* relative height *(with respect to K) is the map $H_K : K \to \mathbb{R}_{\geq 1}$ given by:*

$$H_K(r) = \prod_{v \in M_K} \max\{1, |r|_v\}^{N_v},$$

where $N_v = [K_v : \mathbb{Q}_v]$.

Proposition 3.2.2. *Let $L/K/\mathbb{Q}$ be a tower of finite extensions. Then*

$$H_L(r) = H_K(r)^{[L:K]}$$

for every $r \in K$.

Proof. Let $v \in M_K$ and $w \in M_L$ such that $w|v$. Since $r \in K$ and $N_w = [L_w : \mathbb{Q}_w] = [L_w : K_w]\,[K_v : \mathbb{Q}_v] = N_v\,[L_w : K_w]$, we have:

$$\max\{1, |r|_w\}^{N_w} = \max\{1, |r|_v\}^{N_v[L_w:K_w]}.$$

Besides, by proposition 3.1.12, we have $\sum_{w|v}[L_w : K_w] = [L : K]$. This implies that:

$$\prod_{\substack{w \in M_L \\ w|v}} \max\{1, |r|_w\}^{N_w} = \prod_{\substack{w \in M_L \\ w|v}} \max\{1, |r|_v\}^{N_v[L_w:K_w]} = \max\{1, |r|_v\}^{N_v \sum_{w|v}[L_w:K_w]} = \max\{1, |r|_v\}^{N_v[L:K]}.$$

We conclude by multiplying over all $v \in M_K$,

$$H_L(r) = \prod_{w \in M_L} \max\{1, |r|_w\}^{N_w} = \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max\{1, |r|_w\}^{N_w} = \prod_{v \in M_K} \max\{1, |r|_v\}^{N_v[L:K]} = H_K(r)^{[L:K]}.$$

□

Definition 3.2.3. *The* absolute height *is the map $H : \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 1}$, given by:*

$$H(r) = H_K(r)^{1/[K:\mathbb{Q}]},$$

where K is a finite extension of $\mathbb{Q}$ such that $r \in K$. The (logarithmic) height *is the map $h : \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$, defined by $h(r) = \log H(r)$.*

Proposition 3.2.2 guarantees that $H(r)$ is well defined, i.e. it does not depend on the field K.

Definition 3.2.4. *Let $f = a_d \prod_{i=1}^{d}(X - r_i) \in \mathbb{C}[X]$. The* Mahler measure *of f is:*

$$M(f) = |a_d| \prod_{i=1}^{d} \max\{1, |r_i|\}.$$

The logarithmic Mahler measure *of f is $m(f) = \log M(f)$.*

The Mahler measure is multiplicative, i.e. if $f, g \in \mathbb{C}[X]$ then $M(fg) = M(f)M(g)$ and $m(fg) = m(f) + m(g)$.

Lemma 3.2.5. *Let $f = a_d X^d + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ be a primitive polynomial of degree d and let $p \in \mathbb{N}$ be a prime. Suppose that $r_1, \ldots, r_d \in \overline{\mathbb{Q}_p}$ are all the roots of f. Then:*

$$|a_d|_p \prod_{i=1}^{d} \max\{1, |r_i|_p\} = 1.$$

Proof. Suppose that $|r_1|_p \leq 1, \ldots, |r_k|_p \leq 1$ y $|r_{k+1}|_p > 1, \ldots, |r_d|_p > 1$. The coefficient a_k can be written as $a_k = a_d(r_1 \cdots r_{d-k} + \cdots + r_{k+1} \cdots r_d)$, where the sum ranges over all possible products of $d-k$ roots of f. Among all these terms, the product $r_{k+1} \cdots r_d$ has (strictly) maximal absolute value. Then, by Lemma 3.1.3 we have:

$$|a_k|_p = |a_d|_p \prod_{i=k+1}^{d} |r_i|_p = |a_d|_p \prod_{i=1}^{d} \max\{1, |r_i|_p\}.$$

On the other hand, every coefficient $a_j = a_d(r_1 \cdots r_{d-j} + \cdots + r_{j+1} \cdots r_d)$ has a similar formula, but all these terms have absolute value less or equal than $|r_{k+1} \cdots r_d|_p$. Therefore $|a_j|_p \leq |a_k|_p$ for every j, i.e. a_k is a coefficient with maximal absolute value. Since $f \in \mathbb{Z}[X]$ is primitive, we have $|a_j|_p \leq 1$ for every j, but we cannot have $|a_j|_p < 1$ for every j because p does not divides all the coefficients of f. Thus, there is at least one coefficient which absolute value equals exactly 1. Hence, the maximum of the absolute values of the coefficients of f is 1, and then $|a_k|_p = 1$. □

Proposition 3.2.6. *Let $r \in \overline{\mathbb{Q}}$, let $K = \mathbb{Q}[r]$ and let $f \in \mathbb{Z}[X]$ be the primitive minimal polynomial of r. Then $M(f) = H_K(r)$.*

Proof. Let $p \in \mathbb{N}$ be a prime number and let $r_1, \ldots, r_d \in \overline{\mathbb{Q}_p}$ be the roots of f. By Proposition 3.1.12, the sequence $|r_1|_p, \ldots, |r_d|_p$ contains $|r|_w$ for every absolute value w on K extending v_p with multiplicity N_w. By Lemma 3.2.5, we have:

$$\prod_{w|v_p} \max\{1, |r|_w\}^{N_w} = \prod_{i=1}^{d} \max\{1, |r_i|_p\} = |a_d|_p^{-1}. \tag{3.3}$$

On the other hand, for the Archimedean absolute values, we have:

$$\prod_{w|v_\infty} \max\{1, |r|_w\}^{N_w} = \prod_{i=1}^{d} \max\{1, |r_i|\}. \tag{3.4}$$

Multiplying (3.3) for all prime $p \in \mathbb{N}$ and (3.4), we conclude:

$$\begin{aligned} H_K(r) &= \prod_{w \in M_K} \max\{1, |r|_w\}^{N_w} = \prod_{v \in M_\mathbb{Q}} \prod_{w|v} \max\{1, |r|_w\}^{N_w} \\ &= \prod_{p} |a_d|_p^{-1} \prod_{i=1}^{d} \max\{1, |r_i|\} = |a_d| \prod_{i=1}^{d} \max\{1, |r_i|\} = M(f). \end{aligned}$$

□

For instance, if $r = a/b \in \mathbb{Q} - \{0\}$ where $a \in \mathbb{Z}$, $b \in \mathbb{N}$ and $\gcd(a,b) = 1$, then the primitive minimal polynomial of r is $f = bX - a \in \mathbb{Z}[X]$. Therefore $H(r) = H_{\mathbb{Q}}(r) = M(f) = |b| \max\{1, |a/b|\} = \max\{|a|, |b|\}$.

Lemma 3.2.7. *Let $r, s \in \overline{\mathbb{Q}}$ and let $n \in \mathbb{Z}$. Then:*

1. $h(r^n) = |n| h(r)$.
2. $h(rs) \leq h(r) + h(s)$.
3. $h(r+s) \leq h(r) + h(s) + \log 2$.

Proof. Let $K = \mathbb{Q}[r, s]$.
(1) For every $x \geq 0$ and $n \in \mathbb{N}_0$, $\max\{1, x^n\} = \max\{1, x\}^n$ holds. If $n \in \mathbb{N}_0$, then:

$$H_K(r^n) = \prod_{v \in M_K} \max\{1, |r^n|_v\}^{N_v} = \prod_{v \in M_K} \max\{1, |r|_v^n\}^{N_v} = \prod_{v \in M_K} \max\{1, |r|_v\}^{nN_v} = H_K(r)^n.$$

On the other hand, if $r \neq 0$, then the relative height of r^{-1} is:

$$H_K(r^{-1}) = \prod_{v \in M_K} \max\{1, |r|_v^{-1}\}^{N_v} = \underbrace{\prod_{v \in M_K} |r^{-1}|_v^{N_v}}_{=1} \prod_{v \in M_K} \max\{1, |r|_v\}^{N_v} = H_K(r).$$

Using both identities we get $H_K(r^n) = H_K(r)^{|n|}$ for every $n \in \mathbb{Z}$.
(2) For every $x, y \geq 0$ we have $\max\{1, xy\} \leq \max\{1, x\} \max\{1, y\}$. Then:

$$H_K(rs) = \prod_{v \in M_K} \max\{1, |rs|_v\}^{N_v} \leq \prod_{v \in M_K} \max\{1, |r|_v\}^{N_v} \max\{1, |s|_v\}^{N_v} = H_K(r) H_K(s).$$

(3) For every $x, y \geq 0$ we have $\max\{1, x+y\} \leq 2 \max\{1, x\} \max\{1, y\}$ and $\max\{1, x, y\} \leq \max\{1, x\} \max\{1, y\}$. Then:

$$\begin{aligned} H_K(r+s) &= \prod_{v \in M_K} \max\{1, |r+s|_v\}^{N_v} \leq \prod_{v \in M_K^\infty} \max\{1, |r|_v + |s|_v\}^{N_v} \prod_{v \notin M_K^\infty} \max\{1, |r|_v, |s|_v\}^{N_v} \leq \\ &\leq \prod_{v \in M_K^\infty} 2 \max\{1, |r|_v\}^{N_v} \max\{1, |s|_v\}^{N_v} \prod_{v \notin M_K^\infty} \max\{1, |r|_v\}^{N_v} \max\{1, |s|_v\}^{N_v} \leq \\ &\leq 2^{|M_K^\infty|} H_K(r) H_K(s). \end{aligned}$$

We conclude by using that the number $|M_K^\infty|$ of Archimedean absolute values on K is bounded by the number $[K : \mathbb{Q}]$ of $\mathbb{Q}$-embeddings of K in $\mathbb{C}$. □

Theorem 3.2.8. [Jensen's Formula] *Let $f \in \mathbb{C}[X]$ be a non-zero polynomial. Then:*

$$m(f) = \frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\theta})| d\theta.$$

Proof. Due to the additivity of both sides of the formula, it is enough to prove it for polynomials $f = X - \alpha$ where $\alpha \in \mathbb{C}$, and up to a linear change of variables, this is equivalent to:

$$\int_0^1 \log|\alpha - e^{2\pi it}|dt = \max\{0, \log|\alpha|\}.$$

The map $\log|z|$ is harmonic in $\mathbb{C} - \{0\}$. Then $\log|z - \alpha|$ is harmonic in $\mathbb{C} - \{\alpha\}$. In particular, if $|\alpha| > 1$, then the map $\log|z - \alpha|$ is harmonic in the disc of radius 1 centered in the origin. Using the mean-value identity for harmonic maps, we get:

$$\log|\alpha| = \int_0^1 \log|\alpha - e^{2\pi it}|dt.$$

Now suppose that $|\alpha| < 1$. The map $\log|1 - \overline{\alpha}z|$ is harmonic in $\mathbb{C} - \{\beta\}$, where $\beta = 1/\overline{\alpha} = \alpha/|\alpha|^2$. Since $|\beta| > 1$, then this map is harmonic in the disc of radius 1 centered in the origin. On the other hand, for every $z \in \mathbb{C}$ such that $|z| = 1$ we have $|1 - \overline{\alpha}z| = |\alpha - z|$. Therefore, using again the mean-value identity, we get:

$$0 = \int_0^1 \log|1 - \overline{\alpha}e^{2\pi it}|dt = \int_0^1 \log|\alpha - e^{2\pi it}|dt.$$

It only remains to consider the case $|\alpha| = 1$. By rotational symmetry, we can further reduce to the case $\alpha = 1$, i.e. we have to prove that

$$\int_0^1 \log|1 - e^{2\pi it}|dt$$

converges and is equal to zero. Since $|1 - e^{2\pi it}| = 2\sin(\pi t)$ for every $0 \leq t \leq 1$, then we have to prove that

$$\int_0^1 \log\sin(\pi t)dt = -\log 2.$$

The convergence of the integral follows from

$$\int_0^1 \log\sin(\pi t)dt = 2\int_0^{1/2} \log\sin(\pi t)dt,$$

and the facts that $\sin(\pi t)$ behaves like πt for every t near zero and that $\int_0^{1/2} \log(\pi t)dt$ converges. To compute the value of the integral, note that:

$$\begin{aligned} I &= \int_0^{1/2} \log\sin(\pi t)dt \\ &= \int_0^{1/2} \log(2\sin(\pi t/2)\cos(\pi t/2))dt \\ &= \tfrac{1}{2}\log(2) + \int_0^{1/2} \log\sin(\pi t/2)dt + \int_0^{1/2} \log\cos(\pi t/2)dt. \end{aligned}$$

Making the changes of variables $t = 2u$ and $t = 1 - 2u$, we get $I = \frac{1}{2}\log(2) + 2I$. Therefore $I = -\frac{1}{2}\log(2)$. □

Proposition 3.2.9. *Let $f \in \mathbb{C}[X]$ be a non-zero polynomial of degree d. Then:*

$$2^{-d}\|f\|_1 \leq M(f) \leq \|f\|_1.$$

Proof. Let $f = \sum_{i=0}^{d} a_i X^i = a_d \prod_{i=1}^{d}(X - r_i)$. Then:

$$\|f\|_1 = \sum_{i=0}^{d} |a_i| \leq |a_d| \prod_{i=1}^{d}(1 + |r_i|) \leq 2^d |a_d| \prod_{i=1}^{d} \max\{1, |r_i|\} = 2^d M(f).$$

To prove the other inequality, we use Theorem 3.2.8 and the bound $|f(e^{2\pi i t})| \leq \|f\|_1$ and we get:

$$m(f) = \int_0^1 \log |f(e^{2\pi i t})| dt \leq \int_0^1 \log \|f\|_1 dt = \log \|f\|_1.$$

□

Theorem 3.2.10. [Kronecker] *Let $r \in \overline{\mathbb{Q}}^{\times}$ be such that $h(r) = 0$. Then $r \in \mu_\infty$.*

Proof. Let $f \in \mathbb{Z}[X]$ be the minimal primitive polynomial of r. By Proposition 3.2.6, we have that $M(f) = 1$. Let $r = r_1, r_2, \ldots, r_d \in \overline{\mathbb{Q}}$ be all the roots of f. Since $M(f) = 1$, then f is a monic polynomial and $|r_i| \leq 1 \; \forall i$. The polynomials $f_n = \prod_{i=1}^{d}(X - r_i^n)$ are all in $\mathbb{Z}[X]$ because the r_i's are algebraic integers and the coefficients of f_n are symmetric polynomials in $r_1, \ldots, r_d$. Since $M(f_n) \leq 1$ and $\deg(f_n) = d$, we have that $\|f_n\|_1 \leq 2^d$ for all $n \in \mathbb{N}$, by Proposition 3.2.9. Therefore, there are two polynomials $f_n = f_m$ with $n \neq m$. Then the sets $\{r_1^n, \ldots, r_d^n\}$ and $\{r_1^m, \ldots, r_d^m\}$ coincide. After a suitable permutation of the roots r_i's, we get a cycle $r_1^n = r_2^m$, $r_2^n = r_3^m$, …, $r_k^n = r_1^m$. This implies that $r_1^{n^k} = r_1^{m^k}$, and therefore $r = r_1$ is a root of the unity, because we are assuming $r \neq 0$. □

Theorem 3.2.11. *Let $r \in \overline{\mathbb{Q}}^{\times} \setminus \mu_\infty$ be an algebraic number of degree d over $\mathbb{Q}$, then*

$$h(r) \geq \frac{2}{d \, \log^3(3d)}.$$

Proof. See [Vou96, Corollary 2]. □

Now we extend the notion of height and Mahler measure to the multivariate setting.

Definition 3.2.12. *Let $\xi \in \overline{\mathbb{Q}}^t$. The* (logarithmic) height of ξ *is*

$$h(\xi) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} N_v \log \max\{1, \|\xi\|_v\},$$

where K is an (arbitrary) field containing ξ. We also define the (logarithmic) 1-height of ξ *as*

$$h_1(\xi) = \frac{1}{[K : \mathbb{Q}]} \left(\sum_{v \in M_K^\infty} N_v \log \max\{1, \|\xi\|_{1,v}\} + \sum_{v \notin M_K^\infty} N_v \log \max\{1, \|\xi\|_v\} \right).$$

We also define $H(\xi) = \exp h(\xi)$ *and* $H_1(\xi) = \exp h_1(\xi)$. *If* $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ *then we define* $h(f)$, $H(f)$, $h_1(f)$ *and* $H_1(f)$ *as the height and* 1*-height of the vector of coefficients of* f *respectively.*

Lemma 3.2.7 (items 2 and 3) extends to the multivariate setting with the same proofs. Item 1 only extends when $n \geq 0$ (also with the same proof). It cannot be extended for $n < 0$ because for $\xi \in (\overline{\mathbb{Q}}^\times)^t$, the heights $H(\xi)$ and $H(\xi^{-1})$ are not equal in general. For instance, if $\xi = (2, 3)$, then $H(\xi) = 3$ but $H(\xi^{-1}) = 6$.

Lemma 3.2.13. *Let* $\xi \in \overline{\mathbb{Q}}^t$. *Then* $h(\xi) \leq h_1(\xi) \leq h(\xi) + \log t$.

Proof. The first inequality is clear from the definition because $\|\xi\|_v \leq \|\xi\|_{1,v}$ for all $v \in M_K^\infty$. For the second inequality, we use the estimation $\|\xi\|_{1,v} \leq t \, \|\xi\|_v$, that implies $\max\{1, \|\xi\|_{1,v}\} \leq t \max\{1, \|\xi\|_v\}$ for all $v \in M_K^\infty$ and we get

$$h_1(\xi) \leq h(\xi) + \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K^\infty} N_v \log t.$$

We conclude by using that $\sum_{v \in M_K^\infty} N_v \leq \sum_{v \in M_K} N_v = [K : \mathbb{Q}]$. □

Lemma 3.2.14. *Let* $\xi \in \overline{\mathbb{Q}}^t$ *and* $\eta \in \overline{\mathbb{Q}}^u$. *Let us write* $(\xi, \eta) \in \overline{\mathbb{Q}}^{t+e}$ *to the concatenation of* ξ *and* η. *Then* $\max\{h(\xi), h(\eta)\} \leq h((\xi, \eta)) \leq h(\xi) + h(\eta)$.

Proof. Let $K/\mathbb{Q}$ be a finite extension containing both ξ and η. The first inequality follows directly from the definition and from the fact that $\|\xi\|_v$ and $\|\eta\|_v$ are both bounded above by $\|(\xi, \eta)\|_v$ for all $v \in M_K$. More precisely, we have that $\|(\xi, \eta)\|_v = \max\{\|\xi\|_v, \|\eta\|_v\}$, which implies $\max\{1, \|(\xi, \eta)\|_v\} \leq \max\{1, \|\xi\|_v\} \max\{1, \|\eta\|_v\}$ for all $v \in M_K$, and then $h((\xi, \eta)) \leq h(\xi) + h(\eta)$. □

Suppose that $\xi = (\xi_1, \ldots, \xi_t) \in (\overline{\mathbb{Q}}^\times)^t$. We have that $h(\xi_i^{-1}) = h(\xi_i)$ for all $1 \leq i \leq t$. By applying Lemma 3.2.14 we get the inequality

$$h(\xi^{-1}) \leq h(\xi_1^{-1}) + \cdots + h(\xi_t^{-1}) = h(\xi_1) + \cdots + h(\xi_t) \leq t \, h(\xi)$$

that controls the height of ξ^{-1} in terms of the height of ξ. This gives a generalization of item 1 of Lemma 3.2.7 (with $n < 0$) for the multivariate case.

Lemma 3.2.15. *Let* $f \in \overline{\mathbb{Q}}[X]$ *be an univariate polynomial and let* $r \in \overline{\mathbb{Q}}$ *be a root of* f. *Then* $h(r) \leq h_1(f)$.

Proof. Suppose that $f = \sum_{i=0}^d a_i X^i$ with $a_d \neq 0$. Let $K = \mathbb{Q}[a_0, \ldots, a_d, r]$. Let $v \in M_K$. If v is Archimedean, i.e. $v \in M_K^\infty$, we have

$$|a_d|_v |r|_v^d = |a_{d-1} r^{d-1} + \cdots + a_0|_v \leq (|a_{d-1}|_v + \cdots + |a_0|_v) \max\{1, |r|_v\}^{d-1}.$$

This implies that

$$|a_d|_v \max\{1,|r|_v\}^d \leq (|a_d|_v + \cdots + |a_0|_v)\max\{1,|r|_v\}^{d-1} = \|f\|_{1,v}\max\{1,|r|_v\}^{d-1}$$

$$|a_d|_v \max\{1,|r|_v\} \leq \|f\|_{1,v} \leq \max\{1,\|f\|_{1,v}\}. \tag{3.5}$$

On the other hand, if v is non-Archimedean, we have

$$|a_d|_v|r|_v^d = |a_{d-1}r^{d-1} + \cdots + a_0|_v \leq \max\{|a_{d-1}|_v,\ldots,|a_0|_v\}\max\{1,|r|_v\}^{d-1}.$$

This implies that

$$|a_d|_v \max\{1,|r|_v\}^d \leq \max\{|a_d|_v,\ldots,|a_0|_v\}\max\{1,|r|_v\}^{d-1} = \|f\|_v\max\{1,|r|_v\}^{d-1}$$

$$|a_d|_v \max\{1,|r|_v\} \leq \|f\|_v \leq \max\{1,\|f\|_v\}. \tag{3.6}$$

Raising equations 3.5 and 3.6 to the $N_v/[K:\mathbb{Q}]$ and multiplying over all $v \in M_K$, we get $H(r) \leq H_1(f)$ as desired. The terms $|a_d|_v$ cancel out when multiplying because of the product formula 3.2. □

Lemma 3.2.16. *Let $f \in \overline{\mathbb{Q}}[X_1,\ldots,X_n]$ and let $\xi \in \overline{\mathbb{Q}}^n$. Then*

$$h(f(\xi)) \leq h_1(f) + \deg(f)h(\xi).$$

Proof. Suppose that $f = \sum_{|\alpha|\leq d} a_\alpha X^\alpha$ where $d = \deg(f)$. Let $K = \mathbb{Q}[a_\alpha, \xi]$ be the extension of $\mathbb{Q}$ generated by the coefficients of f and the coordinates of ξ. Let $v \in M_K$. If v is Archimedean,

$$|f(\xi)|_v \leq \sum_{|\alpha|\leq d} |a_\alpha|_v|\xi_1|_v^{\alpha_1}\cdots|\xi_n|_v^{\alpha_n} \leq \left(\sum_{|\alpha|\leq d}|a_\alpha|_v\right)\max\{|\xi_1|_v,\ldots,|\xi_n|_n\}^d = \|f\|_{1,v}\|\xi\|_v^d,$$

and then $\max\{1,|f(\xi)|_v\} \leq \max\{1,\|f\|_{1,v}\}\max\{1,\|\xi\|_v\}^d$. Similarly, if v is non-Archimedean, the ultrametric inequality gives $\max\{1,|f(\xi)|_v\} \leq \max\{1,\|f\|_v\}\max\{1,\|\xi\|_v\}^d$. Raising these inequalities to the $N_v/[K:\mathbb{Q}]$ and multiplying over all $v \in M_K$, we obtain $H(f(\xi)) \leq H_1(f)H(\xi)^d$. □

Definition 3.2.17. *Let $f \in \mathbb{C}[X_1,\ldots,X_n]$. The* (logarithmic) Mahler measure of f *is*

$$m(f) = \frac{1}{(2\pi)^n}\int_0^{2\pi}\cdots\int_0^{2\pi}\log|f(e^{it_1},\ldots,e^{it_n})|dt_1\cdots dt_n.$$

We also define $M(f) = \exp m(f)$.

As in the univariate case, the Mahler measure is multiplicative, i.e. $M(fg) = M(f)M(g)$ and $m(fg) = m(f) + m(g)$ for all $f,g \in \mathbb{C}[X_1,\ldots,X_n]$. Moreover, the inequality $M(f) \leq \|f\|_1$ of Proposition 3.2.9 also holds in the multivariate case with the same proof.

Definition 3.2.18. *Let $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$. The* global Mahler measure of f *is*

$$m_{\overline{\mathbb{Q}}}(f) = \frac{1}{[K : \mathbb{Q}]} \left(\sum_{v|v_\infty} N_v m_v(f) + \sum_{v \nmid v_\infty} N_v \log \max |\mathrm{coeff}(f)|_v \right),$$

where K is a number field containing all the coefficients of f and $m_v(f) = m(\sigma(f))$ for the corresponding embedding $\sigma : K \to \mathbb{C}$.

If $f \in \mathbb{Z}[X_1, \ldots, X_n]$ is a primitive polynomial then $m_{\overline{\mathbb{Q}}}(f) = m(f)$. The global Mahler measure is also multiplicative, i.e. $m_{\overline{\mathbb{Q}}}(fg) = m_{\overline{\mathbb{Q}}}(f) + m_{\overline{\mathbb{Q}}}(g)$ for all $f, g \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$. We also have the inequality $m_{\overline{\mathbb{Q}}}(f) \leq h_1(f)$ for all $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$.

Definition 3.2.19. *Let V be a hypersurface of $\overline{\mathbb{Q}}^n$ given by $f \in K[X_1, \ldots, X_n]$, where $K/\mathbb{Q}$ is a finite extension. The* normalized height of V *is $\widehat{h}(V) = m_{\overline{\mathbb{Q}}}(f)$.*

In the case of a hypersurface V given by a primitive polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$, then the normalized height reduces to $\widehat{h}(V) = m(f)$.

Chapter 4

Factorization

4.1 The "gap" theorem

Theorem 4.1.1. *Let $f = f_1 + X_n^\beta f_2 \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ be a polynomial with $\deg_{X_n}(f_1) = \alpha < \beta$. Let $\eta \in \overline{\mathbb{Q}}$ and $\xi \in \mu_\infty^{n-1}$ be such that $f(\xi, \eta) = 0$. If the "gap" $\Delta = \beta - \alpha$ satisfies $h(\eta)\Delta > h_1(f)$, then $f_1(\xi, \eta) = f_2(\xi, \eta) = 0$.*

Proof. Let $K/\mathbb{Q}$ be a finite extension containing the coefficients of f, ξ and η. Let $v \in M_K$ be an absolute value. We consider four cases, depending whether v is Archimedean or not, and whether $|\eta|_v$ is ≥ 1 or < 1.

a. $v \in M_K^\infty$ and $|\eta|_v \geq 1$: $|\eta|_v^\beta |f_2(\xi, \eta)|_v = |f_1(\xi, \eta)|_v \leq |\eta|_v^\alpha \|f_1\|_{1,v}$. Dividing by $|\eta|_v^\alpha$ and using that $\|f_1\|_{1,v} \leq \|f\|_{1,v}$, we get:

$$|\eta|_v^\Delta |f_2(\xi, \eta)|_v \leq \|f\|_{1,v}.$$

b. $v \in M_K^\infty$ and $|\eta|_v < 1$:

$$|f_2(\xi, \eta)|_v \leq \|f_2\|_{1,v} \leq \|f\|_{1,v}.$$

ab. Writing these two cases ($v \in M_K^\infty$) together, we get:

$$\max\{1, |\eta|_v\}^\Delta |f_2(\xi, \eta)|_v \leq \|f\|_{1,v}. \tag{4.1}$$

c. $v \notin M_K^\infty$ and $|\eta|_v \geq 1$: $|\eta|_v^\beta |f_2(\xi, \eta)|_v = |f_1(\xi, \eta)|_v \leq |\eta|_v^\alpha \|f_1\|_v$. Therefore

$$|\eta|_v^\Delta |f_2(\xi, \eta)|_v \leq \|f\|_v.$$

d. $v \notin M_K^\infty$ and $|\eta|_v < 1$:

$$|f_2(\xi, \eta)|_v \leq \|f_2\|_v \leq \|f\|_v.$$

cd. Writing these two cases ($v \notin M_K^\infty$) together, we get:

$$\max\{1, |\eta|_v\}^\Delta |f_2(\xi, \eta)|_v \leq \|f\|_v. \tag{4.2}$$

Raising the inequalities (4.1) and (4.2) to the $[K_v : \mathbb{Q}_v]/[K : \mathbb{Q}]$ power and multiplying over all $v \in M_K$, we obtain:

$$H(\eta)^{\Delta} \prod_{v \in M_K} |f_2(\xi,\eta)|_v^{\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}} \leq \prod_{v \in M_K^{\infty}} \|f\|_{1,v}^{\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}} \prod_{v \notin M_K^{\infty}} \|f\|_v^{\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}} \leq H_1(f).$$

If $f_2(\xi,\eta) \neq 0$, then, by the product formula (3.2),

$$\prod_{v \in M_K} |f_2(\xi,\eta)|_v^{\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}} = 1.$$

This implies $H(\eta)^{\Delta} \leq H_1(f)$, in contradiction with our hypothesis. Thus we have $f_2(\xi,\eta) = 0$, and therefore $f_1(\xi,\eta) = 0$. □

Definition 4.1.2. *Let $p \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ be a polynomial with $\deg_{X_n}(p) \geq 1$. For each $\omega \geq 0$, we write*

$$C_{p,\omega} = \left\{ \xi \in \mu_{\infty}^{n-1} \,:\, \exists \eta \in \overline{\mathbb{Q}} \,:\, p(\xi,\eta) = 0 \,\wedge\, h(\eta) \geq \omega \right\}.$$

We define

$$\lambda(p) = \sup \left\{ \omega \geq 0 \,:\, C_{p,\omega} \text{ is Zariski dense in } \overline{\mathbb{Q}}^{n-1} \right\}.$$

Note that the condition $\deg_{X_n}(p) \geq 1$ guarantees that $\lambda(p)$ is well-defined, because if $p = \sum_{i=0}^{d} p_i(X_1, \ldots, X_{n-1}) X_n^i$ with $p_d \neq 0$ and $d \geq 1$, then $C_{p,0} \supseteq \mu_{\infty}^{n-1} \smallsetminus V_{\overline{\mathbb{Q}}}(p_d)$ and this set is Zariski dense in $\overline{\mathbb{Q}}^{n-1}$. Furthermore, next result shows that $\lambda(p)$ is finite.

Lemma 4.1.3. *Let $p = \sum_{i=0}^{d} p_i(X_1, \ldots, X_{n-1}) X_n^i \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ be a polynomial with $d = \deg_{X_n}(p) \geq 1$. Then*

$$\lambda(p) \leq \log(d+1) + \sum_{i=0}^{d} h_1(p_i).$$

Proof. Let $\xi \in \mu_{\infty}^{n-1}$ be such that $p_d(\xi) \neq 0$ and let $\eta \in \overline{\mathbb{Q}}$ be such that $p(\xi,\eta) = 0$. By Lemma 3.2.15 we have $h(\eta) \leq h_1(p(\xi, X_n))$, and by Lemmas 3.2.13 and 3.2.14 we get

$$h_1(p(\xi, X_n)) \leq h(p(\xi, X_n)) + \log(d+1) \leq \sum_{i=0}^{d} h(p_i(\xi)) + \log(d+1).$$

Besides, the point ξ has height zero (because its coordinates are roots of the unity), and then, by Lemma 3.2.16 we get $h(p_i(\xi)) \leq h_1(p_i)$. All these inequalities give

$$h(\eta) \leq \log(d+1) + \sum_{i=0}^{d} h_1(p_i).$$

In other words, we have proved that if $\omega > \log(d+1) + \sum_{i=0}^{d} h_1(p_i)$, then $C_{p,\omega} \subseteq V_{\overline{\mathbb{Q}}}(p_d)$ which is clearly not Zariski-dense in $\overline{\mathbb{Q}}^{n-1}$. We conclude immediately from the definition of $\lambda(p)$. □

Theorem 4.1.4. *Let $f = f_1 + X_n^\beta f_2 \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ with $\deg_{X_n}(f_1) = \alpha < \beta$ and let $\Delta = \beta - \alpha$. Let $p \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ be a polynomial with $\deg_{X_n}(p) \geq 1$. If $p|f$ and $\lambda(p)\Delta > h_1(f)$, then $\mathrm{Res}_{X_n}(p, f_1) = \mathrm{Res}_{X_n}(p, f_2) = 0$.*

Proof. The hypothesis $\lambda(p)\Delta > h_1(f) \geq 0$ implies $\lambda(p) > 0$. Let $0 < \omega < \lambda(p)$ be such that $\omega\Delta > h_1(f)$. By the definition of $\lambda(p)$, the set $C_{p,\omega}$ is Zariski dense in $\overline{\mathbb{Q}}^{n-1}$. Let $\xi \in C_{p,\omega}$ such that ξ does not annihilate the leading coefficient p_d (w.r.t. X_n) of p, and let $\eta \in \overline{\mathbb{Q}}$ be such that $p(\xi, \eta) = 0$ and $h(\eta) \geq \omega$. Since $p|f$, then $f(\xi, \eta) = 0$, and since $h(\eta)\Delta \geq \omega\Delta > h_1(f)$, we can apply Theorem 4.1.1 to get $f_1(\xi, \eta) = f_2(\xi, \eta) = 0$. Our assumption $p_d(\xi) \neq 0$ implies that $\mathrm{Res}_{X_n}(p, f_1)(\xi) = \mathrm{Res}_{X_n}(p(\xi, X_n), f_1(\xi, X_n)) = 0$ and similarly, $\mathrm{Res}_{X_n}(p, f_2)(\xi) = 0$. Since this holds for all the points in the Zariski dense set $C_{p,\omega} \setminus V_{\overline{\mathbb{Q}}}(p_d) \subseteq \overline{\mathbb{Q}}^{n-1}$, then $\mathrm{Res}_{X_n}(p, f_1) = \mathrm{Res}_{X_n}(p, f_2) = 0$. □

Corollary 4.1.5. *Let $L/\mathbb{Q}$ be an algebraic extension. Let $f = f_1 + X_n^\beta f_2 \in L[X_1, \ldots, X_n]$ with $\deg_{X_n}(f_1) = \alpha < \beta$ and let $\Delta = \beta - \alpha$. Let $p \in L[X_1, \ldots, X_n]$ be an irreducible polynomial with $\deg_{X_n}(p) \geq 1$. Suppose that $\lambda(p)\Delta > h_1(f)$. Then $p|f$ if and only if $p|f_1$ and $p|f_2$.*

Note that if $\deg_{X_n}(p) = 0$, then the conclusion of the previous corollary holds independently of the value of Δ.

4.2 Lower bounds for $\lambda(p)$

In this section we present several lower bounds for $\lambda(p)$ where $p \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ is a non-zero polynomial with $\deg_{X_n}(p) \geq 1$.

Lemma 4.2.1. *Let $p_1, p_2 \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ be non-zero polynomials with $\deg_{X_n}(p_1) \geq 1$.*

1. *If $\deg_{X_n}(p_2) = 0$, then $\lambda(p_1 p_2) = \lambda(p_1)$.*
2. *If $\deg_{X_n}(p_2) \geq 1$, then $\lambda(p_1 p_2) = \max\{\lambda(p_1), \lambda(p_2)\}$.*

Proof. 1. Since $C_{p_1 p_2, \omega} = C_{p_1, \omega} \cup \left[V_{\overline{\mathbb{Q}}}(p_2) \cap \mu_\infty^{n-1} \right]$, then $C_{p_1 p_2, \omega}$ is Zariski dense in $\overline{\mathbb{Q}}^{n-1}$ if and only if $C_{p_1,\omega}$ is. In particular, this implies that $\lambda(p_1 p_2) = \lambda(p_1)$.

2. Since $C_{p_1 p_2, \omega} = C_{p_1, \omega} \cup C_{p_2, \omega}$, then $C_{p_1 p_2, \omega}$ is Zariski dense in $\overline{\mathbb{Q}}^{n-1}$ if and only if at least one of $C_{p_1,\omega}$ and $C_{p_2,\omega}$ is. Therefore $\lambda(p_1 p_2) = \max\{\lambda(p_1), \lambda(p_2)\}$. □

Definition 4.2.2. *Let $V \subseteq \overline{\mathbb{Q}}^n$ be a non-empty set. The* essential minimum of V *is*

$$\mu^{\mathrm{ess}}(V) = \inf\{\omega \geq 0 \ : \ V(\omega) \text{ is Zariski dense in } V\},$$

where $V(\omega)$ denotes the set of points $\xi \in V$ such that $h(\xi) \leq \omega$.

Note that if $V \subseteq \overline{\mathbb{Q}}^n$ is an algebraic variety and $U \subseteq V$ is an open subset, then $\mu^{\mathrm{ess}}(V) = \mu^{\mathrm{ess}}(U)$.

Proposition 4.2.3. *Let $p \in K[X_1, \ldots, X_n]$ be an irreducible polynomial with $\deg_{X_n}(p) \geq 1$, and let $V = V_{\overline{\mathbb{Q}}}(p)$. Then $\mu^{\mathrm{ess}}(V) \leq \lambda(p)$.*

Proof. Let $\varepsilon > 0$ and let $\omega = \mu^{\mathrm{ess}}(V) - \varepsilon$. Then $V(\omega)$ is not Zariski dense in V. Since p is irreducible in $K[X_1, \ldots, X_n]$, then $V(\omega)$ is not Zariski dense in any of the irreducible components of V. This implies that $\dim \overline{V(\omega)} \leq n-2$. Write $p = \sum_{i=0}^{d} p_i(X_1, \ldots, X_{n-1}) X_n^i$, where $p_d \neq 0$ and $d \geq 1$. Then

$$C_{p,\omega} \supseteq \pi\left(V \smallsetminus V(\omega)\right) \cap \mu_\infty^{n-1} \supseteq \mu_\infty^{n-1} \smallsetminus \left(V_{\overline{\mathbb{Q}}}(p_d) \cup \pi\left(\overline{V(\omega)}\right)\right),$$

where π is the projection onto the first $n-1$ coordinates. Since $\dim(V_{\overline{\mathbb{Q}}}(p_d) \cup \pi(\overline{V(\omega)})) \leq n-2$, then $C_{p,\omega}$ is dense in $\overline{\mathbb{Q}}^{n-1}$, i.e. $\lambda(p) \geq \omega = \mu^{\mathrm{ess}}(V) - \varepsilon$. Therefore $\lambda(p) \geq \mu^{\mathrm{ess}}(V)$. □

Theorem 4.2.4. *Let $V \subseteq \mathbb{G}_m^n$ be a non-empty algebraic variety. Then*

$$\frac{\widehat{h}(V)}{(\dim(V)+1)\deg(V)} \leq \mu^{\mathrm{ess}}(V) \leq \frac{\widehat{h}(V)}{\deg(V)}.$$

Proof. See [Zha95a, Theorem 5.2] and [Zha95b, Theorem 1.10]. □

Theorem 4.2.5. *Let $V \subseteq \mathbb{G}_m^n$ be a hypersurface of degree d irreducible over $\mathbb{Q}$. If V is not the union of translates of algebraic subgroups by torsion points, then*

$$\widehat{h}(V) \geq 10^{-4} \cdot \left(\frac{\log(n\log(nd'))}{n\log(nd')}\right)^3,$$

where $d' = \max\{d, 16\}$.

Proof. See [Pon05, Theorem 1.9]. □

Theorem 4.2.6. *Let $V \subseteq \mathbb{G}_m^n$ be a hypersurface of degree d irreducible over $\overline{\mathbb{Q}}$. If V is not the translate of an algebraic subgroup of $\mathbb{G}_m^n$, then*

$$\widehat{h}(V) \geq \frac{10^{-14}}{n^8} \cdot \frac{(\log(n\log(d')))^4}{(n\log(d'))^5},$$

where $d' = \max\{nd, 16\}$.

Proof. See [Pon05, Theorem 1.22]. □

Lemma 4.2.7. *Let $V \subseteq \mathbb{G}_m^n$ be a hypersurface. Then V is an algebraic subgroup if and only if V is defined by a polynomial $X^b - X^c$ for some $b, c \in \mathbb{N}_0^n$ such that $b_i c_i = 0$ for all i.*

Proof. Since V is a hypersurface of $\mathbb{G}_m^n$, we can assume that $V = V_{\overline{\mathbb{Q}}}(p) \cap \mathbb{G}_m^n$ for some squarefree polynomial $p \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ such that $\deg(p) \geq 1$ and $X_i \nmid p$ for all i. In particular, p has at least two non-zero terms. If V is an algebraic subgroup of $\mathbb{G}_m^n$, then

$$\begin{aligned} u \in V &\iff V = u^{-1} \cdot V \\ &\iff V_{\overline{\mathbb{Q}}}(p) \cap \mathbb{G}_m^n = V_{\overline{\mathbb{Q}}}(p(u \cdot X)) \cap \mathbb{G}_m^n \\ &\iff V_{\overline{\mathbb{Q}}}(p) = V_{\overline{\mathbb{Q}}}(p(u \cdot X)) \\ &\iff p = \gamma(u)\, p(u \cdot X) \quad \text{for some } \gamma(u) \in \overline{\mathbb{Q}}^\times. \end{aligned}$$

Write $p = \sum_e a_e X^e$ where $a_e \neq 0 \; \forall\, e$. Then for any $u \in V$, we have

$$\begin{aligned} p(X) = \gamma(u) p(u \cdot X) &\iff \sum a_e X^e = \sum a_e \gamma(u) u^e X^e \\ &\iff a_e = a_e \gamma(u) u^e \quad \forall\, e \\ &\iff 1 = \gamma(u) u^e \quad \forall\, e. \end{aligned}$$

Now, we take two different terms $a_b X^b$ and $a_c X^c$ of p. We proved that $\gamma(u)u^b = 1 = \gamma(u)u^c$ for all $u \in V$, and then we also have $u^b = u^c$ for all $u \in V$. Therefore $V \subseteq V_{\overline{\mathbb{Q}}}(X^b - X^c)$, and since $V = V_{\overline{\mathbb{Q}}}(p) \cap \mathbb{G}_m^n$, we have that $p \mid X^b - X^c$. Since $\deg(X^b - X^c) \leq \deg(p)$, then there exists $\gamma \in \overline{\mathbb{Q}}^\times$ such that $p = \gamma(X^b - X^c)$. The condition $b_i c_i = 0$ follows immediately from $X_i \nmid p$. $\square$

As a consequence, if $V \subseteq \mathbb{G}_m^n$ is a hypersurface and V is the translate of an algebraic subgroup by a torsion point, that is $V = \varepsilon \cdot W$ where W is given by a polynomial $p = X^b - X^c$ for some $b, c \in \mathbb{N}_0^n$ and $\varepsilon \in \mu_\infty^n$, then V is defined by the polynomial $\varepsilon^b p(\varepsilon^{-1} \cdot X) = X^b - \theta\, X^c$ where $\theta = \varepsilon^{b-c} \in \mu_\infty$. Likewise, V is the translate of an algebraic subgroup by a point of $\mathbb{G}_m^n$ if and only if V is defined by an arbitrary binomial.

Corollary 4.2.8. *Let $p \in K[X_1, \ldots, X_n]$ be a polynomial of degree d with coefficients in a finite extension $K/\mathbb{Q}$ of degree e. Suppose that $\deg_{X_n}(p) \geq 1$.*

1. *If p is irreducible in $K[X_1, \ldots, X_n]$, p is not a monomial and p is not divisible by any binomial $X^b - \theta X^c$ where $\theta \in \mu_\infty$, then*

$$\lambda(p) \geq \frac{10^{-4}}{nde} \cdot \left(\frac{\log(n \log(nd'))}{n \log(nd')} \right)^3,$$

   where $d' = \max\{de, 16\}$.

2. *If p is irreducible in $\overline{\mathbb{Q}}[X_1, \ldots, X_n]$ and p has at least three terms, then*

$$\lambda(p) \geq \frac{10^{-14}}{n^9 d} \cdot \frac{(\log(n \log(d')))^4}{(n \log(d'))^5},$$

   where $d' = \max\{nd, 16\}$.

Proof. 1. Let $q \in \mathbb{Q}[X_1, \dots, X_n]$ be an irreducible polynomial such that $p \,|\, q$. It is clear that $\deg(q) \leq de$ because q is a factor of $\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(p)$. Besides, we have that $C_{\sigma(p),\omega} = \sigma(C_{p,\omega})$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, and then $\lambda(p) = \lambda(\sigma(p))$. By item 2 of Lemma 4.2.1, we get $\lambda(q) = \lambda(p)$. Since q is not a single monomial, then $V = V_{\overline{\mathbb{Q}}}(q) \cap \mathbb{G}_m^n$ is a hypersurface of $\mathbb{G}_m^n$ of degree $\leq de$ irreducible over $\mathbb{Q}$. Moreover, q is not divisible by any binomial $X^b - \theta X^c$ with $\theta \in \mu_\infty$. In particular, this means that V is not the union of translates of algebraic subgroups of $\mathbb{G}_m^n$ by torsion points. We conclude by using Proposition 4.2.3 and Theorems 4.2.4 and 4.2.5.

$$\lambda(p) = \lambda(q) \geq \mu^{\mathrm{ess}}(V) \geq \frac{\widehat{h}(V)}{nde} \geq \frac{10^{-4}}{nde} \cdot \left(\frac{\log(n \log(nd'))}{n \log(nd')} \right)^3$$

2. Write $V = V_{\overline{\mathbb{Q}}}(p) \cap \mathbb{G}_m^n$. Since p is neither a monomial nor a binomial, then V is a hypersurface of $\mathbb{G}_m^n$ that is not the translate of an algebraic subgroup. Besides, V is irreducible over $\overline{\mathbb{Q}}$, because it is defined by an irreducible polynomial in $\overline{\mathbb{Q}}[X_1, \dots, X_n]$. We conclude by using Proposition 4.2.3 and Theorems 4.2.4 and 4.2.6.

$$\lambda(p) \geq \mu^{\mathrm{ess}}(V) \geq \frac{\widehat{h}(V)}{nd} \geq \frac{10^{-14}}{n^9 d} \cdot \frac{(\log(n \log(d')))^4}{(n \log(d'))^5}$$

□

A polynomial satisfying item 1 of the previous corollary will be called non-cyclotomic.

Proof of Proposition 2.1.2. We know that $m(f) = m(q) + \sum_p e_p m(p)$, where the sum runs over all primitive irreducible non-cyclotomic factors of f in $\mathbb{Z}[X_1, \dots, X_n]$ and e_p is its corresponding multiplicity. By Theorem 4.2.5 we have that

$$m(p) = \widehat{h}(V_{\overline{\mathbb{Q}}}(p)) \geq 10^{-4} \cdot \left(\frac{\log(n \log(nd'_p))}{n \log(nd'_p)} \right)^3,$$

where $d'_p = \max\{\deg(p), 16\}$. Since this expression is decreasing in d'_p, we can freely replace d'_p by $d' = \max\{\deg(f), 16\}$. Besides, the numerator is ≥ 1 because $\log(\log(16)) \geq 1$. Then we can also neglect this term.

$$m(p) \geq \frac{10^{-4}}{n^3 \, \log^3(n \, \max\{\deg(f), 16\})}$$

Using the inequalities $m(f) \geq \log \|f\|_1$ and $m(q) \geq 0$, we conclude that

$$\log \|f\|_1 \geq m(f) \geq \sum_p e_p m(p) \geq \frac{10^{-4} \sum_p e_p}{n^3 \, \log^3(n \, \max\{\deg(f), 16\})}.$$

□

Proof of Proposition 2.1.4. We know that $m(f) = m_{\overline{\mathbb{Q}}}(f) = m_{\overline{\mathbb{Q}}}(q) + \sum_p e_p m_{\overline{\mathbb{Q}}}(p)$, where the sum runs over all absolute irreducible of f in $\overline{\mathbb{Q}}[X_1, \ldots, X_n]$ and e_p is its corresponding multiplicity. By Theorem 4.2.6 we have that

$$m_{\overline{\mathbb{Q}}}(p) = \widehat{h}(V_{\overline{\mathbb{Q}}}(p)) \geq \frac{10^{-14}}{n^8} \cdot \frac{(\log(n \log(d'_p)))^4}{(n \log(d'_p))^5},$$

where $d'_p = \max\{n \deg(p), 16\}$. Since this expression is decreasing in d'_p, we can freely replace d'_p by $d' = \max\{n \deg(f), 16\}$. Besides, the numerator is ≥ 1 because $\log(\log(16)) \geq 1$. Then we can also neglect this term.

$$m_{\overline{\mathbb{Q}}}(p) \geq \frac{10^{-14}}{n^{13} \log^5(\max\{n \deg(f), 16\})}$$

Using the inequalities $m(f) \geq \log \|f\|_1$ and $m_{\overline{\mathbb{Q}}}(q) \geq 0$, we conclude that

$$\log \|f\|_1 \geq m(f) = m_{\overline{\mathbb{Q}}}(f) \geq \sum_p e_p m_{\overline{\mathbb{Q}}}(p) \geq \frac{10^{-14} \sum_p e_p}{n^{13} \log^5(\max\{n \deg(f), 16\})}$$

□

Proposition 2.1.4 can be extended to polynomials $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ by replacing $\log \|f\|_1$ by $h_1(f)$ in the statement and in the previous proof.

4.3 Algorithms

Let $K = \mathbb{Q}[r]$ be a finite extension of $\mathbb{Q}$ of degree e and let $\phi \in \mathbb{Z}[X]$ be the primitive minimal polynomial of r. Let $f \in K[X_1, \ldots, X_n]$ be a lacunary polynomial with exactly t non-zero terms. Let $d \in \mathbb{N}$. Our goal is to find all the irreducible factors (in $K[X_1, \ldots, X_n]$ and $\overline{\mathbb{Q}}[X_1, \ldots, X_n]$) of f of degree $\leq d$.

Suppose that $p \in K[X_1, \ldots, X_n]$ is a non-cyclotomic irreducible factor of f such that $\deg(p) \leq d$. Define $d' = \max\{de, 16\}$ and set

$$\Delta > 10^4 h_1(f) nde \left(\frac{\log(n \log(nd'))}{n \log(nd')} \right)^3.$$

If $\deg_{X_n}(p) \geq 1$, then, by Corollary 4.1.5 and the lower bound of the item 1 of Corollary 4.2.8, we can cut f every time that the gap of degree between two consecutive monomials (w.r.t. X_n) is greater than or equal to Δ, and p is still a factor of each of the small polynomials. On the other hand, if $\deg_{X_n}(p) = 0$, then the previous assertion is true independently of the value of Δ.

Input: A polynomial $f \in K[X_1, \ldots, X_n]$ with exactly t non-zero terms, encoded as a list of t vectors $(a_1, \alpha_1), \ldots, (a_t, \alpha_t) \in K \times \mathbb{N}_0^n$ representing each of the monomials of f.
A bound d for the degree of the required factors.
Output: All the non-cyclotomic irreducible factors of f in $K[X_1, \ldots, X_n]$ of degree $\leq d$.

1: $B \leftarrow \text{Height1UpperBound}(f)$
2: $d' \leftarrow \max\{de, 16\}$
3: $\Delta \leftarrow 10^4 Bnde \left(\frac{n \log(nd')}{\log(n \log(nd'))}\right)^3 + 1$
4: $S_0 \leftarrow \{f\}$
5: **for** $i = 1$ to n **do**
6: $\quad S_i \leftarrow \emptyset$
7: $\quad$ **for all** $g \in S_{i-1}$ **do**
8: $\quad\quad S_i \leftarrow S_i \cup \text{Split}(g, X_i, \Delta)$ /* Cut g when the gap (w.r.t X_i) of degree is $\geq \Delta$ */
9: $\quad$ **end for**
10: **end for**
11: Take $g \in S_n$ and set $S_n \leftarrow S_n \setminus \{g\}$
12: $F \leftarrow \text{DenseFactor}(g)$
13: **for all** $g \in S_n$ **do**
14: $\quad F \leftarrow F \cap \text{DenseFactor}(g)$
15: **end for**
16: Discard all the polynomials in F of degree greater than d.
17: **return** F

Algorithm 1: Computes the non-cyclotomic factors of f in $K[X_1, \ldots, X_n]$ of degree $\leq d$

We can easily adapt this algorithm to compute all the absolute irreducible factors of degree $\leq d$ with at least three terms by replacing Δ in step 3 by the value

$$\Delta \leftarrow 10^{14}\, B\, n^{14}\, d\, \frac{\log^5(\max\{nd, 16\})}{\log^4(n\, \log(\max\{nd, 16\}))} + 1$$

given by the second item of Corollary 4.2.8. We also need to use an algorithm for the absolute dense factorization in steps 12 and 14.

This algorithm requires in it first step an upper bound for $h_1(f)$. In order to compute it, we need to deal with the internal representation of the coefficients of f.

We encode every $a \in K$ by its vector of coordinates in the $\mathbb{Q}$-basis $\{1, r, r^2, \ldots, r^{e-1}\}$ of K. It is clear that, once we have the primitive minimal polynomial $\phi \in \mathbb{Z}[X]$ of r, all the arithmetic operations in K can be performed from this representation. Next lemma shows that this representation is also compatible with the height.

Lemma 4.3.1. *Let $K = \mathbb{Q}[r]$ be a finite extension and let $\phi(X) \in \mathbb{Z}[X]$ be the primitive minimal polynomial of r over $\mathbb{Q}$. Let $a = (a_1, \ldots, a_t) \in K^t$ and suppose that each a_i is represented by the vector $(a_{i,0}, \ldots, a_{i,e-1}) \in \mathbb{Q}^e$. Let $\tilde{a} \in \mathbb{Q}^{et}$ be the concatenation of all those vectors. Then*

$$h(a) \leq h_1(a) \leq h_1(\tilde{a}) + e\, m(\phi) \leq h(\tilde{a}) + \log(et) + e\, m(\phi).$$

Proof. Since $a_i = \sum_{j=0}^{e-1} a_{i,j} r^j$, then we clearly have:

$$\max\{1, \|a\|_{1,v}\} \leq \max\{1, |r|_v\}^e \max\{1, \sum_{i,j} |a_{i,j}|_v\} = \max\{1, |r|_v\}^e \max\{1, \|\tilde{a}\|_{1,v}\} \quad \forall\, v \in M_K^\infty,$$

$$\max\{1, \|a\|_v\} \leq \max\{1, |r|_v\}^e \max\{1, \max_{i,j} |a_{i,j}|_v\} = \max\{1, |r|_v\}^e \max\{1, \|\tilde{a}\|_v\} \quad \forall\, v \notin M_K^\infty.$$

Raising this to the $N_v/[K:\mathbb{Q}]$ power and multiplying over all $v \in M_K$ we get

$$H_1(a) \leq H(r)^e H_1(\tilde{a}).$$

By Proposition 3.2.6 we have that $H(r) = M(\phi)$. We conclude by taking logarithms and using the inequalities $h(a) \leq h_1(a)$ and $h_1(\tilde{a}) \leq \log(et) + h(\tilde{a})$ of Lemma 3.2.13. □

Now we have all the tools needed to give a precise bound for $h_1(f)$. The computations are detailed in Algorithm 2. In its main loop, B is collecting an upper bound for the height of each number in the vector $\tilde{a} = (a_{1,0}, a_{1,1}, \ldots, a_{t,e-1}) \in \mathbb{Q}^{et}$. Then, according to Lemma 3.2.14, at the end of the loop B will contain an upper bound for $H(\tilde{a})$.

Input: A finite extension $K = \mathbb{Q}[r]$ of $\mathbb{Q}$ of degree e, given by the primitive minimal polynomial $\phi \in \mathbb{Z}[X]$ of r.
A list $(a_1, \ldots, a_t) \in K^t$ containing the t coefficients of the polynomial $f \in K[X_1, \ldots, X_n]$, each one encoded as a vector $(a_{i,0}, \ldots, a_{i,e-1}) \in \mathbb{Q}^e$.
Output: An upper bound for $h_1(f)$.

```
A ← ‖φ‖_1 /* Compute an upper bound for M(φ) via Proposition 3.2.9 */
B ← 1
for i = 1 to t do
    for j = 0 to e − 1 do
        B ← max{B, |num(a_{i,j})|, |den(a_{i,j})|}
    end for
end for
return log(B) + log(et) + e log(A) /* Lemma 4.3.1 */
```

Algorithm 2: Computes an upper bound for $h_1(f)$

Definition 4.3.2. *Let $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ be a non-zero polynomial. We define $f^{[1]}$ by*

$$f^{[1]} = \frac{\partial}{\partial X_n}\left(\frac{f}{X_n^s}\right)$$

where $s \in \mathbb{N}_0$ is the maximum integer such that X_n^s divides f. We set $f^{[1]} = 0$ if $f = 0$. We recursively define $f^{[n]} = (f^{[n-1]})^{[1]}$ for all $n \geq 2$. We also set $f^{[0]} = f$.

Note that if f has exactly t non-zero terms, then $f^{[1]}$ has at most $t-1$ non-zero terms. On the other hand, if $p \in \overline{\mathbb{Q}}$ is an irreducible factor of f of multiplicity r (with $\deg_{X_n}(p) \geq 1$ and $p \neq cX_n$ with $c \in \overline{\mathbb{Q}}^\times$), then p is a factor of $f^{[1]}$ of multiplicity $r-1$.

$$\mathrm{mult}(p, f) = \max\{s \in \mathbb{N}_0 \,:\, p \mid f^{[s]}\} \tag{4.3}$$

This implies that the factor p of f cannot have multiplicity greater than or equal to t.

We can simply use formula 4.3 to compute the multiplicities of the factors by running Algorithm 1 for f, $f^{[1]}$, ..., $f^{[t-1]}$, but there is a shortcut: the idea is to replace the first instruction by

$$B \leftarrow \text{Height1UpperBound}(f, f^{[1]}, \ldots, f^{[t-1]})$$

which produces a "gap" large enough to work with any of these polynomials, and then, instead of factoring f, $f^{[1]}$, ..., $f^{[t-1]}$ in steps 12 and 14, we can simply compute the factors of f *with multiplicities* and keeping track (in step 14) of the minimum multiplicy they arise. Note that this work for all the irreducible factors p of f with $\deg_{X_n}(p) \geq 1$ and $p \neq cX_n$ for all c. In order to compute the correct multiplicities of all irreducible factors (not a single monomial), we need to use an upper bound for the 1-height of the derivatives $f^{[1]},\ldots,f^{[t-1]}$ with respect to all variables.

By the multivariate version of item 2 of Lemma 3.2.7, we have $h(f^{[1]}) \leq h(f) + \log(\deg_{X_n}(f))$, and then $h_1(f^{[r]}) \leq h(f) + r\log(\deg_{X_n}(f))$ for all r. Here we are considering the derivative with respect to variable X_n. If we want an uniform bound for the derivatives with respect to any variable, we need $h_1(f^{[r]}) \leq h(f) + r\log(\deg(f))$. Therefore, it is enough to replace the first instruction of Algorithm 1 by

$$B \leftarrow \text{Height1UpperBound}(f) + t\log(\deg(f))$$

in order to compute all the non-cyclotomic irreducible factors with multiplicities. Of course steps 12 and 14 should also be modified as explained above.

Notation. *Let $v \in \mathbb{R}^n$. We write*

$$v^+ = (\max\{v_1, 0\}, \ldots, \max\{v_n, 0\}) \quad \textit{and} \quad v^- = (\max\{-v_1, 0\}, \ldots, \max\{-v_n, 0\})$$

to the only decomposition $v = v^+ - v^-$ with vectors $v^+, v^- \in \mathbb{R}^n_{\geq 0}$.

Now we focus our attention in the cyclotomic factors. We begin by analyzing when an irreducible binomial $X^b - \theta\, X^c \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ divides a lacunary polynomial $f \in \overline{\mathbb{Q}}$. Next lemma allow us to compute all the possible pairs $b, c \in \mathbb{N}_0^n$.

Lemma 4.3.3. *Let $f \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ and suppose that $X^b - \theta\, X^c$ is an irreducible factor of f for some $\theta \in \overline{\mathbb{Q}}^\times$. Then, there are two different non-zero monomials a_iX^i and a_jX^j of f such that*

$$c = \frac{(i-j)^+}{g} \qquad \textit{and} \qquad b = \frac{(i-j)^-}{g}$$

where $g = \gcd(r_1 - s_1, \ldots, r_n - s_n)$.

Proof. We can assume without loss of generality that $b_n \geq 1$ and $c_n = 0$. The irreducibility of the binomial $X^b - \theta\, X^c$ implies that $b_ic_i = 0$ for all $i = 1, \ldots, n$ and $\gcd(b_1 - c_1, \ldots, b_n - c_n) = 1$. It is clear that $X^b - \theta\, X^c \mid f$ in $\overline{\mathbb{Q}}[X_1, \ldots, X_n]$ is equivalent to

$$X_n^{b_n} - \theta\, X_1^{c_1 - b_1} \cdots X_{n-1}^{c_{n-1} - b_{n-1}} \mid f \qquad \text{in } \overline{\mathbb{Q}}[X_1^{\pm 1}, \ldots, X_{n-1}^{\pm 1}][X_n].$$

Write $f = \sum_{e \in E} a_e X^e$ where $a_e \neq 0$ for all $e \in E$. Dividing f by $X_n^{b_n} - \theta\, X_1^{c_1-b_1} \cdots X_{n-1}^{c_{n-1}-b_{n-1}}$ we get the following remainder:

$$\sum_{e \in E} a_e X_1^{e_1} \cdots X_{n-1}^{e_{n-1}} \left(\theta\, X_1^{c_1-b_1} \cdots X_{n-1}^{c_{n-1}-b_{n-1}}\right)^{\left[\frac{e_n}{b_n}\right]} X_n^{e_n \bmod b_n}.$$

If this expression is zero in $\overline{\mathbb{Q}}[X_1^{\pm 1}, \ldots, X_{n-1}^{\pm 1}][X_n]$, then there are at least two indexes $i, j \in E$ such that

$$X_1^{i_1} \cdots X_{n-1}^{i_{n-1}} \left(X_1^{c_1-b_1} \cdots X_{n-1}^{c_{n-1}-b_{n-1}}\right)^{\left[\frac{i_n}{b_n}\right]} X_n^{i_n \bmod b_n} =$$

$$= X_1^{j_1} \cdots X_{n-1}^{j_{n-1}} \left(X_1^{c_1-b_1} \cdots X_{n-1}^{c_{n-1}-b_{n-1}}\right)^{\left[\frac{j_n}{b_n}\right]} X_n^{j_n \bmod b_n}.$$

In particular this means that $i_n \equiv j_n \bmod d_n$, and then we can write $j_n = i_n + g b_n$ for some integer $g \in \mathbb{Z}$.

$$X_1^{i_1-j_1} \cdots X_{n-1}^{i_{n-1}-j_{n-1}} = \left(X_1^{c_1-b_1} \cdots X_{n-1}^{c_{n-1}-b_{n-1}}\right)^g.$$

This implies that $i_l - j_l = g\,(c_l - b_l)$ for all $l = 1, \ldots, n-1$. The same relation holds for $l = n$ because we are assuming $c_n = 0$ and $j_n = i_n + g b_n$. Writing all these relations together, we get $i - j = g\,(c - b)$ for some $g \in \mathbb{Z}$. By eventually swapping b and c, we can assume that g is positive, and since $\gcd(b_1 - c_1, \ldots, b_n - c_n) = 1$, then $g = \gcd(i_1 - j_1, \ldots, i_n - j_n)$. The conclusion follows easily from $b, c \in \mathbb{N}_0^n$. □

Although many of the pairs $b, c \in \mathbb{N}_0^n$ determined by the Lemma 4.3.3 may not necessarily lead to a $\theta \in \overline{\mathbb{Q}}^\times$ such that $X^b - \theta\, X^c \mid f$, the search is now reduced to at most $t(t-1)/2$ possibilities, where t is the number of non-zero terms of f.

This search is implemented in Algorithm 3. The main loop produces all the possible pairs of exponents (b, c) as in Lemma 4.3.3, then univariate equations for $\theta \in \overline{\mathbb{Q}}$ are generated and finally we use an univariate lacunary factorization algorithm to decide if there exists such θ. In this case, the algorithm outputs the vector (b, c, g), where g is the minimal polynomial of θ over K. In the current implementation we only look for $\theta \in \mu_\infty$ of degree $\leq d$ over K, that is, g is a cyclotomic polynomial of degree $\deg(g) \leq d$.

If we want the true factors in $K[X_1, \ldots, X_n]$, we can take each (b, c, g) that produces Algorithm 3 and compute $\mathrm{Res}_\theta(X^b - \theta\, X^c, g(\theta))$, where θ is considered as an unknown.

Since the univariate algorithm we use in step 14 also computes the multiplicity of the factors, then we can adapt our algorithm in order to compute the multiplicities too. The only change we need to do in this step is to compute the irreducible cyclotomic factors (with its corresponding multiplicities) of degree $\leq d$ of each of the equations found in step 13 and then keep only the common ones with the least multiplicity they arise.

Input: The coefficients and exponents of f, encoded as a list $(a_1, \alpha_1), \ldots, (a_t, \alpha_t) \in K \times \mathbb{N}_0^n$, and an integer $d \geq 1$.

Output: All the irreducible factors $X^b - \theta\, X^c$ of f with $\theta \in \mu_\infty$ and $\deg(\theta/K) \leq d$. Here θ is given by its minimal monic polynomial over K.

1: Initialize $F \leftarrow \emptyset$
2: **for** $i = 1$ to $t - 1$ **do** /* Loop over all pairs of terms of f */
3: **for** $j = i + 1$ to t **do**
4: $v \leftarrow \alpha_i - \alpha_j$ /* Compute b and c using Lemma 4.3.3 */
5: $g \leftarrow \gcd(v_1, \ldots, v_n)$
6: $c \leftarrow v^+/g$
7: $b \leftarrow v^-/g$
8: Set k to an index such that $b_k + c_k \geq 1$
9: **if** $b_k = 0$ **then**
10: Swap b and c /* Ensure that $b_k \geq 1$ */
11: **end if**
12: Reduce all the terms of f by dividing it by the binomial $X_k^{b_k} - \theta\, X^{c-b}$ in the ring $K[X_1^{\pm 1}, \ldots, \widehat{X_k^{\pm 1}}, \ldots, X_n^{\pm 1}, \theta][X_k]$ /* Here θ behaves as an unknown */
13: Extract a list of "lacunary" polynomial equations for θ, by looking the coefficients of the previous expression in the ring $K[\theta][X_1^{\pm 1}, \ldots, \widehat{X_k^{\pm 1}}, \ldots, X_n^{\pm 1}, X_k]$
14: Compute the irreducible cyclotomic factors of degree $\leq d$ of each of these equations for θ by using the univariate algorithm and keep only the common factors. /* An algorithm for this is given in [Len99b] */
15: Add $(b, c, g) \in \mathbb{N}_0^n \times \mathbb{N}_0^n \times K[X]$ to the list F for each common factor g found in the previous step.
16: **end for**
17: **end for**
18: **return** F

Algorithm 3: Computes the irreducible factors $X^b - \theta\, X^c$ of f with $\theta \in \mu_\infty$ and $\deg(\theta/K) \leq d$

Chapter 5

Interpolation

5.1 The ring of p-adic numbers $\mathbb{Z}_p$

In this section, we give several definitions of the ring of p-adic numbers $\mathbb{Z}_p$, together with a proof of their equivalence. We begin with the construction that most fits with the rest of the work.

Definition 5.1.1. *Let $p \in \mathbb{N}$ be a prime number. The ring of p-adic numbers $\mathbb{Z}_p$ is the set*

$$\mathbb{Z}_p = \left\{ (a_i)_{i\geq 1} \in \mathbb{Z}^{\mathbb{N}} \ : \ a_i \equiv a_{i+1} \bmod p^i \ \forall\, i \right\} / \sim$$

where $\sim$ is the equivalence relation given by

$$(a_i)_{i\geq 1} \sim (b_i)_{i\geq 1} \Leftrightarrow \ a_i \equiv b_i \bmod p^i, \ \forall\, i.$$

The operations are coordinate-wise, i.e.:

$$\overline{(a_i)_{i\geq 1}} + \overline{(b_i)_{i\geq 1}} = \overline{(a_i + b_i)_{i\geq 1}} \qquad \overline{(a_i)_{i\geq 1}} \cdot \overline{(b_i)_{i\geq 1}} = \overline{(a_i \cdot b_i)_{i\geq 1}}.$$

It is easy to see that the operations are well-defined and that $\mathbb{Z}_p$ is a ring with these operations. Note that this definition is equivalent to give $\mathbb{Z}_p$ as the quotient ring A_p/I_p, where A_p is the subring $A_p = \{(a_i)_{i\geq 1} \ : \ a_i \equiv a_{i+1} \bmod p^i \ \forall\, i\}$ of $\mathbb{Z}^{\mathbb{N}}$, and I_p is the ideal $I_p = \{(a_i)_{i\geq 1} \ : \ a_i \equiv 0 \bmod p^i \ \forall\, i\}$ of A_p.

Now we give a more natural definition of $\mathbb{Z}_p$ and we prove its equivalence with Definition 5.1.1.

Definition 5.1.2. *Let $p \in \mathbb{N}$ be a prime. Let $\rho_k : \mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ be the canonical projections $\rho_k(\overline{x}) = \overline{x}$. The ring of p-adic numbers (written $\widetilde{\mathbb{Z}_p}$ temporarily) is the subring of $\prod_{k\in\mathbb{N}} \mathbb{Z}/p^k\mathbb{Z}$ that contains all the sequences $(a_k)_{k\in\mathbb{N}}$ such that $\rho_k(a_{k+1}) = a_k \ \forall\, k$.*

Proposition 5.1.3. *The map $\pi : \mathbb{Z}_p \to \widetilde{\mathbb{Z}_p}$ given by $\overline{(a_i)_{i\geq 1}} \mapsto (\overline{a_i})_{i\geq 1}$ is well-defined ring isomorphism.*

Proof. Denote by $\pi_k : \mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}$ the map given by $\overline{(a_i)_{i\geq 1}} \mapsto \overline{a_k}$. It is well-defined because:

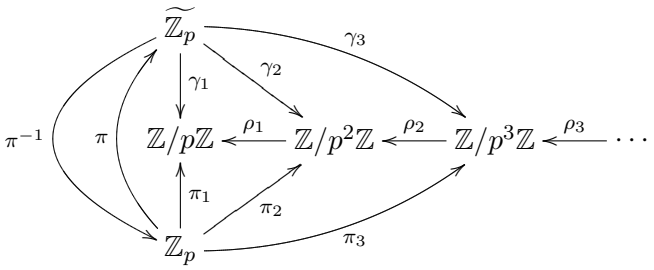
$$\overline{(a_i)_{i\geq 1}} = \overline{(b_i)_{i\geq 1}} \Leftrightarrow (a_i)_{i\geq 1} \sim (b_i)_{i\geq 1} \Leftrightarrow a_i \equiv b_i \bmod p^i \ \forall\, i \Rightarrow a_k \equiv b_k \bmod p^k \Rightarrow \overline{a_k} = \overline{b_k}.$$

Moreover, since the operations in $\mathbb{Z}_p$ are coordinate-wise, then π_k is a ring morphism. Besides, if $a = \overline{(a_i)_{i\geq 1}} \in \mathbb{Z}_p$, then $a_{k+1} \equiv a_k \bmod p^k$. Therefore $\rho_k(\pi_{k+1}(a)) = \rho_k(\overline{a_{k+1}}) = \overline{a_k} = \pi_k(a)$. This implies that $\rho_k \circ \pi_{k+1} = \pi_k$ for every k and guarantees that $\pi = (\pi_1, \pi_2, \ldots) : \mathbb{Z}_p \to \widetilde{\mathbb{Z}_p}$ is a well-defined ring morphism. In order to prove that it is injective, we only need to verify that $\ker(\pi) = \{0\}$. Actually, if $a = \overline{(a_k)_{k\geq 1}} \in \ker \pi$, then

$$\pi(a) = 0 \Rightarrow \pi_k(a) = 0 \ \forall\, k \Rightarrow a_k \equiv 0 \bmod p^k \ \forall\, k \Rightarrow \overline{(a_k)_{k\geq 1}} = \overline{(0)_{k\geq 1}} \Rightarrow a = 0.$$

Finally, if $b = (\overline{b_k})_{k\geq 1} \in \widetilde{\mathbb{Z}_p}$, then $\rho_k(\overline{b_{k+1}}) = \overline{b_k}$ for every k. Therefore $(b_k)_{k\geq 1} \in \mathbb{Z}^{\mathbb{N}}$ is a sequence such that $b_k \equiv b_{k+1} \bmod p^k$ for every k. Then, setting $a = \overline{(b_k)_{k\geq 1}}$, we have that $a \in \mathbb{Z}_p$ and $\pi(a) = b$. This implies that $\mathrm{Im}(\pi) = \widetilde{\mathbb{Z}_p}$, i.e. π is surjective. □

Denote by $\gamma_k : \widetilde{\mathbb{Z}_p} \to \mathbb{Z}/p^k\mathbb{Z}$ the projections to the coordinates. According to the proof of the previous proposition, we have the commutative diagram:



We also have that $\widetilde{\mathbb{Z}_p}$ with the projections γ_k is the usual construction for the inverse limit of this diagram (in the category of rings). Therefore, $\mathbb{Z}_p$ with the morphisms π_k is also the inverse limit. This lead us to the following definition of $\mathbb{Z}_p$:

Definition 5.1.4. *Let $p \in \mathbb{N}$ be a prime number. The ring of p-adic numbers is the inverse limit of the diagram:*

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\rho_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\rho_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\rho_3} \cdots.$$

Remark. *The map $i : \mathbb{Z} \to \mathbb{Z}_p$ given by $a \mapsto \overline{(a, a, \ldots)}$ is a ring monomorphism. Moreover, it is the only homomorphism such that $\pi_k \circ i = q_k \ \forall\, k$ where $q_k : \mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ is the projection to the quotient ring.*

In order to simplify the notation, we identify $x \in \mathbb{Z}$ with $i(x) \in \mathbb{Z}_p$, i.e. we think of the integers as included in $\mathbb{Z}_p$.

Lemma 5.1.5. *Let $a = \overline{(a_i)_{i\geq 1}} \in \mathbb{Z}_p$. Then $pa = \overline{(0, pa_1, pa_2, \ldots)}$. That is, multiplication by p is like a "shift to the right".*

Proof. Since $p = \overline{(p, p, \ldots)}$, then we only have to check that $(pa_1, pa_2, \ldots) \sim (0, pa_1, pa_2, \ldots)$, i.e. $pa_1 \equiv 0 \bmod p$ (trivial) and $pa_{k+1} \equiv pa_k \bmod p^{k+1}$ for every k. This holds because for every $a \in \mathbb{Z}_p$ and for every k we have $a_k \equiv a_{k+1} \bmod p^k$. □

Now we state some properties of $\mathbb{Z}_p$ that follow immediately from the definitions and a procedure called Hensel Lifting that consists in computing solutions of equations in $\mathbb{Z}_p$ by giving a recursive formula (called Hensel Step) for the coordinates of the solution.

Theorem 5.1.6. *Let $a = \overline{(a_i)_{i\geq 1}} \in \mathbb{Z}_p$. Then a is invertible in $\mathbb{Z}_p$ if and only if $p \nmid a_1$.*

Proof. If $p \mid a_1$, then for every $b = \overline{(b_i)_{i\geq 1}} \in \mathbb{Z}_p$ we have $a_1 b_1 \equiv 0 \bmod p$ and therefore $ab \neq 1$. This shows that a is not invertible. Now suppose that $p \nmid a_1$. We define recursively $b_1, b_2, \ldots \in \mathbb{Z}$ such that $b_i \equiv b_{i+1} \bmod p^i$ and $a_i b_i \equiv 1 \bmod p^i$ for every i. If this is possible, we will have $b = \overline{(b_i)_{i\geq 1}} \in \mathbb{Z}_p$ such that $ab = 1$ and therefore a is invertible. It is clear that we can choose $b_1 \in \mathbb{Z}$ such that $a_1 b_1 \equiv 1 \bmod p$ because p is prime to a_1. Suppose that we have already computed $b_1, \ldots, b_k \in \mathbb{Z}$ that satisfy all the conditions. We need $b_{k+1} = b_k + p^k \Delta$ such that $a_{k+1} b_{k+1} \equiv 1 \bmod p^{k+1}$. On the other hand, we know that $a_{k+1} = a_k + p^k \Gamma$ and $a_k b_k = 1 + p^k \Theta$ for some $\Gamma, \Theta \in \mathbb{Z}$. The equation to find Δ is:

$$(a_k + p^k \Gamma)(b_k + p^k \Delta) \equiv 1 \bmod p^{k+1}.$$

Simplifying, we get:

$$\begin{aligned} a_k b_k + p^k \Gamma + p^k \Delta &\equiv 1 \bmod p^{k+1} \\ p^k(\Theta + b_k \Gamma + a_k \Delta) &\equiv 0 \bmod p^{k+1} \\ a_k \Delta &\equiv -\Theta - b_k \Gamma \bmod p \\ a_1 \Delta &\equiv -\Theta - b_1 \Gamma \bmod p \end{aligned}$$

and this equation has a solution because $p \nmid a_1$. □

Using Theorem 5.1.6 and Lemma 5.1.5 we deduce the following properties of $\mathbb{Z}_p$:

- For every non-zero $x \in \mathbb{Z}_p$ there exist (unique) $r \in \mathbb{N}_0$ and $u \in \mathcal{U}(\mathbb{Z}_p)$ such that $x = p^r u$.
- $\mathbb{Z}_p$ is an integral domain, with field of fractions $\mathbb{Q}_p$. The non-zero elements of $\mathbb{Q}_p$ are $p^r u$ with $r \in \mathbb{Z}$ and $u \in \mathcal{U}(\mathbb{Z}_p)$.
- $\mathbb{Z}_p$ is a local ring with maximal ideal $\mathcal{M} = p\mathbb{Z}_p$. Its residue field is isomorphic to $\mathbb{F}_p$.

5.2 The ring of p-adic exponents E_p and the exponential map

First of all, we define the ring E_p of the numbers that we are going to use as exponents for the p-adic numbers. There are several equivalent definitions. We give first the definition that most fits with the rest of the work, then we give other possible constructions with no proof of equivalence (because these proofs are similar to those given in the previous section).

Definition 5.2.1. *Let $p \in \mathbb{N}$ be a prime number. The ring E_p of the p-adic "exponents" is the set*

$$E_p = \left\{(a_i)_{i\geq 1} \in \mathbb{Z}^{\mathbb{N}} \ : \ a_i \equiv a_{i+1} \bmod \varphi(p^i) \ \forall\, i\right\} / \simeq$$

where $\simeq$ is the equivalence relation given by

$$(a_i)_{i\geq 1} \simeq (b_i)_{i\geq 1} \Leftrightarrow a_i \equiv b_i \bmod \varphi(p^i), \ \forall\, i.$$

The operations are coordinate-wise, i.e.:

$$\overline{(a_i)_{i\geq 1}} + \overline{(b_i)_{i\geq 1}} = \overline{(a_i + b_i)_{i\geq 1}} \qquad \overline{(a_i)_{i\geq 1}} \cdot \overline{(b_i)_{i\geq 1}} = \overline{(a_i \cdot b_i)_{i\geq 1}}.$$

Here there is a list of other possible definitions of E_p:

- Let $B_p = \{(a_i)_{i\geq 1} \ : \ a_i \equiv a_{i+1} \bmod \varphi(p^i) \ \forall\, i\} \subset \mathbb{Z}^{\mathbb{N}}$ and let $J_p = \{(a_i)_{i\geq 1} \ : \ a_i \equiv 0 \bmod \varphi(p^i) \ \forall\, i\} \subset B_p$. Then J_p is an ideal of the ring B_p and $E_p \cong B_p/J_p$.
- Let $\tau_k : \mathbb{Z}/\varphi(p^{k+1})\mathbb{Z} \to \mathbb{Z}/\varphi(p^k)\mathbb{Z}$ be the canonical projections $\tau_k(\overline{x}) := \overline{x}$. Then E_p is the subring of $\prod_{k\in\mathbb{N}} \mathbb{Z}/\varphi(p^k)\mathbb{Z}$ containing all the sequences $(x_k)_{k\in\mathbb{N}}$ such that $\tau_k(x_{k+1}) = x_k, \ \forall\, k$.
- E_p is the inverse limit of the following diagram:

$$\mathbb{Z}/\varphi(p)\mathbb{Z} \xleftarrow{\tau_1} \mathbb{Z}/\varphi(p^2)\mathbb{Z} \xleftarrow{\tau_2} \mathbb{Z}/\varphi(p^3)\mathbb{Z} \xleftarrow{\tau_3} \cdots$$

We embed $\mathbb{Z}$ in E_p via constant sequences. More precisely, the map $j : \mathbb{Z} \to E_p$ given by $j(a) = \overline{(a, a, \ldots)}$ is a monomorphism of rings. For simplicity, we identify $a \in \mathbb{Z}$ with $j(a) \in E_p$, i.e. we think of the integers as included in E_p.

The structure of the ring E_p is closely related to that of $\mathbb{Z}_p$ as proven in the following theorem.

Theorem 5.2.2. *The map $\Gamma : E_p \to \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ given by*

$$\Gamma\left(\overline{(a_i)_{i\geq 1}}\right) = \left(\overline{a_1}, \overline{(a_i)_{i\geq 2}}\right)$$

is an isomorphism of rings.

Proof. First of all, we check that Γ is well-defined. Let $a = \overline{(a_i)_{i\geq 1}} \in E_p$. Then $a_i \equiv a_{i+1} \bmod \varphi(p^i)$ for all $i \geq 1$. Since $\varphi(p^i) = (p-1)p^{i-1}$ we have that $a_i \equiv a_{i+1} \bmod p^{i-1}, \ \forall\, i$, and then $\overline{(a_i)_{i\geq 2}}$ belongs to $\mathbb{Z}_p$. On the other hand, if we have two equivalent sequences $\overline{(a_i)_{i\geq 1}} = \overline{(b_i)_{i\geq 1}}$, then $a_i \equiv b_i \bmod \varphi(p^i)$ for all i. Therefore $a_1 \equiv b_1 \bmod (p-1)$ and $a_i \equiv b_i \bmod p^{i-1}, \ \forall\, i$, and then $\overline{a_1} = \overline{b_1}$ in $\mathbb{Z}/(p-1)\mathbb{Z}$ and $\overline{(a_i)_{i\geq 2}} = \overline{(b_i)_{i\geq 2}}$ in $\mathbb{Z}_p$.

Now that we know that Γ is well-defined, we immediately deduce that it is a homomorphism of rings, because the operations in E_p and $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ are coordinate-wise.

Monomorphism: Let $a = \overline{(a_i)_{i\geq 1}} \in \ker(\Gamma)$. Then $a_1 \equiv 0 \bmod (p-1)$ and $a_i \equiv 0 \bmod p^{i-1}$, $\forall\, i$. On the other hand, since $a \in E_p$, we have $a_i \equiv a_{i+1} \bmod (p-1)p^{i-1}$, $\forall\, i$, and then all the integers a_i have the same remainder modulo $p-1$, i.e. $a_i \equiv 0 \bmod (p-1)$, $\forall\, i$.

$$\left.\begin{array}{l} a_i \equiv 0 \bmod p^{i-1} \\ a_i \equiv a_1 \equiv 0 \bmod (p-1) \end{array}\right\} \Rightarrow\ a_i \equiv 0 \bmod \varphi(p^i) \ \Rightarrow\ a = 0.$$

Epimorphism: Given $\overline{a_1} \in \mathbb{Z}/(p-1)\mathbb{Z}$ and $\overline{(a_i)_{i\geq 2}} \in \mathbb{Z}_p$, we define $b_1 = a_1$ and b_i for $i \geq 2$ as an integer such that $b_i \equiv a_1 \bmod (p-1)$ and $b_i \equiv a_i \bmod p^{i-1}$. The existence of such a b_i is guaranteed by the Chinese Remainder's Theorem. By definition, we have that:

$$\left.\begin{array}{l} b_{i+1} \equiv a_1 \bmod p-1 \\ b_{i+1} \equiv a_{i+1} \bmod p^i \end{array}\right\} \Rightarrow \left.\begin{array}{l} b_{i+1} \equiv b_i \bmod (p-1) \\ b_{i+1} \equiv a_{i+1} \equiv a_i \equiv b_i \bmod p^{i-1} \end{array}\right\} \Rightarrow$$

$$\Rightarrow b_{i+1} \equiv b_i \bmod \varphi(p^i) \Rightarrow b = \overline{(b_i)_{i\geq 1}} \in E_p.$$

This means that $\Gamma(b) = a$. □

Thanks to the isomorphism of Theorem 5.2.2 we deduce the following properties of E_p:

- The invertible elements of E_p are the sequences $\overline{(a_i)_{i\geq 1}}$ such that $\gcd(a_2, \varphi(p^2)) = 1$.
- The zero-divisors in E_p are the sequences $a = \overline{(p^{i-1}d)_{i\geq 1}}$, where d divides $(p-1)$.

Now we introduce the p-adic exponential function and we state some of its elementary properties.

Definition 5.2.3. *Let $a = \overline{(a_i)_{i\geq 1}} \in \mathcal{U}(\mathbb{Z}_p)$ and let $b = \overline{(b_i)_{i\geq 1}} \in E_p$ be given by a sequence with $b_i \geq 0$, $\forall\, i$. We define*

$$a^b = \overline{(a_i^{b_i})_{i\geq 1}} \in \mathcal{U}(\mathbb{Z}_p).$$

If $a_{i+1} \equiv a_i \not\equiv 0 \bmod p^i$ and $b_{i+1} \equiv b_i \bmod \varphi(p^i)$, then $a_{i+1}^{b_{i+1}} \equiv a_{i+1}^{b_i} \equiv a_i^{b_i} \bmod p^i$. If $a_i \equiv c_i \not\equiv 0 \bmod p^i$ and $b_i \equiv d_i \bmod \varphi(p^i)$, then $a_i^{b_i} \equiv a_i^{d_i} \equiv c_i^{d_i} \bmod p^i$. This proves that the p-adic exponential is well-defined, i.e. does not depend on the sequence representing a and b. On the other hand, it is clear that for all $b \in E_p$, we can chose a sequence of non-negative integers representing b.

Notation. *We use the symbol $\wedge$ to denote the map*

$$\begin{array}{ccc} \mathcal{U}(\mathbb{Z}_p) \times E_p & \xrightarrow{\ \wedge\ } & \mathcal{U}(\mathbb{Z}_p) \\ (a, b) & \longmapsto & a^b \end{array}$$

Theorem 5.2.4. *Let $a, c \in \mathcal{U}(\mathbb{Z}_p)$ and let $b, d \in E_p$. Then:*

$$a^{b+d} = a^b a^d, \quad a^0 = 1, \quad (ac)^b = a^b c^b, \quad 1^b = 1 \ \text{ and } \ (a^b)^d = a^{bd}.$$

Proof. All these identities follow from the fact that the p-adic exponential function and the ring operations in $\mathbb{Z}_p$ and E_p are coordinate-wise. □

The first four identities of Theorem 5.2.4 mean that the map

$$(\mathcal{U}(\mathbb{Z}_p),\cdot)\times(E_p,+)\xrightarrow{\wedge}(\mathcal{U}(\mathbb{Z}_p),\cdot)$$

is a homomorphism of groups in each variable. The fifth identity means that $\wedge$ is a homomorphism of semigroups (in each variable) when E_p is given the product operation instead of the sum.

As usual, the exponential function has two possible "inverse" functions: logarithms and roots. Next we show how to define them in our context.

Definition 5.2.5. *Let $a\in\mathcal{U}(\mathbb{Z}_p)$ and let $b\in E_p$ invertible. We define the "b-root of a" by $\sqrt[b]{a}=a^{(b^{-1})}$. We denote $\sqrt[b]{\cdot}$ to the b-root function.*

$$\begin{array}{ccc}\mathcal{U}(\mathbb{Z}_p) & \xrightarrow{\sqrt[b]{\cdot}} & \mathcal{U}(\mathbb{Z}_p)\\ a & \longmapsto & \sqrt[b]{a}=a^{(b^{-1})}\end{array}$$

Proposition 5.2.6. *Let $a,c\in\mathcal{U}(\mathbb{Z}_p)$ and let $b,d\in E_p$. Suppose that b is invertible. Then:*

$$\sqrt[1]{a}=a,\quad \sqrt[b]{1}=1,\quad \sqrt[b]{a^b}=a=(\sqrt[b]{a})^b,\quad \sqrt[b]{ac}=\sqrt[b]{a}\sqrt[b]{c},\quad y\quad \sqrt[b]{a^d}=(\sqrt[b]{a})^d.$$

Besides, if d is also invertible, then:

$$\sqrt[d]{\sqrt[b]{a}}=\sqrt[b]{\sqrt[d]{a}}=\sqrt[bd]{a}.$$

Proof. It is clear from the properties of the p-adic exponential proven in Theorem 5.2.4. □

In order to define the logarithm, we need to be more careful. For an arbitrary $a\in\mathcal{U}(\mathbb{Z}_p)$, the map $E_p\to\mathcal{U}(\mathbb{Z}_p)$ given by $e\mapsto a^e$ is not necessarily bijective, and therefore it is not possible to define its inverse $\log_a:\mathcal{U}(\mathbb{Z}_p)\to E_p$. In the following definition and theorem, we give a precise characterization of all the $a\in\mathcal{U}(\mathbb{Z}_p)$ such that it is possible to define $\log_a$.

Definition 5.2.7. *Let $a=\overline{(a_i)_{i\geq 1}}\in\mathcal{U}(\mathbb{Z}_p)$. We say that a is a "good basis" if and only if a_i is a primitive root modulo p^i (i.e. a generator of the multiplicative group $\mathcal{U}(\mathbb{Z}/p^i\mathbb{Z})$) for all i.*

Theorem 5.2.8. *Let $a\in\mathcal{U}(\mathbb{Z}_p)$. Then the following statements are equivalent:*

1. *The map $E_p\to\mathcal{U}(\mathbb{Z}_p)$ given by $e\mapsto a^e$ is bijective.*
2. *a is a good basis.*

Proof. ($1 \Rightarrow 2$): Suppose that $a = \overline{(a_i)_{i\geq 1}}$ is not a good basis. Then there exists some $n \geq 1$ such that a_n is not a primitive root modulo p^n. Therefore, the set of powers of a_n does not contain all the remainders modulo p^n prime to p. This implies (looking at the n-th coordinate) that the map $e \mapsto a^e$ is not surjective.
($2 \Rightarrow 1$): Suppose that $a = \overline{(a_i)_{i\geq 1}} \in \mathcal{U}(\mathbb{Z}_p)$ satisfies that a_i is a primitive root modulo p^i for all i. From 5.2.4 we know that the map $(E_p, +) \to (\mathcal{U}(\mathbb{Z}_p), \cdot)$ given by $e \mapsto a^e$ is a homomorphism of groups. Therefore, in order to prove the injectivity, we only need to check that its kernel is trivial. Actually, if $e = \overline{(e_i)_{i\geq 1}} \in E_p$ satisfies $a^e = 1$, then $a_i^{e_i} \equiv 1 \bmod p^i$, $\forall\, i$, and hence $\varphi(p^i)|e_i$, $\forall\, i$, i.e. $e = 0$. Now we check the surjectivity. Let $b = \overline{(b_i)_{i\geq 1}} \in \mathcal{U}(\mathbb{Z}_p)$. For all i, we know that $b_i \equiv a_i^{e_i} \bmod p^i$ for some $e_i \in \mathbb{N}$. Doing:

$$b_{i+1} \equiv b_i \bmod p^i \Rightarrow a_{i+1}^{e_{i+1}} \equiv a_i^{e_i} \bmod p^i \Rightarrow a_i^{e_{i+1}} \equiv a_i^{e_i} \bmod p^i \Rightarrow \varphi(p^i)|(e_{i+1} - e_i)$$

we conclude that $e = \overline{(e_i)_{i\geq 1}}$ belongs to E_p and $a^e = b$. □

Note that in the case $p = 2$ there are no good bases, because of the lack of primitive roots modulo 2^i for $i > 2$.

For an odd prime p, the criteria to decide whether $a \in \mathcal{U}(\mathbb{Z}_p)$ is a good basis given in definition 5.2.7 is simplified in the following lemma.

Lemma 5.2.9. *Let p be an odd prime and let $a \in \mathbb{Z}$ such that $p \nmid a$. Then, the following statements are equivalent:*

1. *a is a primitive root modulo p^k for all $k \geq 1$.*
2. *a is a primitive root modulo p^i for some $i \geq 2$.*
3. *a is a primitive root modulo p^2.*

Any of these statements implies that a is a primitive root modulo p.

Proof. ($1 \Rightarrow 2$) and ($1 \Rightarrow 3$): Trivial.
($2 \Rightarrow 3$): Suppose that a is not a primitive root modulo p^k for some $k \geq 1$. Then there exists $1 \leq d < \varphi(p^k)$ such that $a^d \equiv 1 \bmod p^k$, i.e. $a^d = 1 + p^k r$ for some $r \in \mathbb{Z}$. Raising to the p-th power we have $a^{dp} = (1 + p^k r)^p$, and expanding we get:

$$a^{dp} = 1 + p^{k+1}r + \binom{p}{2}p^{2k}r^2 + \binom{p}{3}p^{3k}r^3 + \cdots \equiv 1 \bmod p^{k+1}.$$

Since $1 \leq dp < p\varphi(p^k) = \varphi(p^{k+1})$, we conclude that a is not a primitive root modulo p^{k+1}.
We have proven that if a is not a primitive root modulo p^k, then it is not a primitive root modulo p^{k+1}. In particular, if a is not a primitive root modulo p^2 we conclude that a is not a primitive root modulo p^i for any $i \geq 2$.
Using the same idea we get that (2) implies that a is a primitive root modulo p.
($3 \Rightarrow 1$): Suppose that a is a primitive root modulo p^2, but a is not a primitive root modulo p^k for some $k \geq 2$. Take $k > 2$ minimal such that a is not a primitive root modulo p^k. Then

there exists $1 \leq d < \varphi(p^k)$ such that $a^d \equiv 1 \bmod p^k$. Since $a^{\varphi(p^k)} \equiv 1 \bmod p^k$, then we also have $a^{\gcd(d,\varphi(p^k))} \equiv 1 \bmod p^k$, hence we can assume without loss of generality that $d|\varphi(p^k)$. On the other hand, we have that $a^d \equiv 1 \bmod p^{k-1}$, and since a is primitive modulo p^{k-1}, then $\varphi(p^{k-1})|d$. Therefore $d = \varphi(p^{k-1})$ and $a^{\varphi(p^{k-1})} \equiv 1 \bmod p^k$. Besides, $a^{\varphi(p^{k-2})} \not\equiv 1 \bmod p^{k-1}$, because a is primitive modulo p^{k-1}. Since $a^{\varphi(p^{k-2})} \equiv 1 \bmod p^{k-2}$ by the Euler-Fermat Theorem, then $a^{\varphi(p^{k-2})} = 1 + p^{k-2}r$ for some $r \in \mathbb{Z}$ prime to p. Raising this identity to the p-th power, we get

$$a^{\varphi(p^{k-1})} = a^{\varphi(p^{k-2})p} = (1+p^{k-2}r)^p = 1+p^{k-1}r+\binom{p}{2}p^{2(k-2)}r^2+\binom{p}{3}p^{3(k-2)}r^3+\cdots \equiv 1+p^{k-1}r \bmod p^k,$$

in contradiction to $a^{\varphi(p^{k-1})} \equiv 1 \bmod p^k$. □

From the lemma, it is clear that we only need to check if a_2 is a primitive root modulo p^2 in order to guarantee that $a = \overline{(a_i)_{i\geq 1}}$ is a good basis. In particular, if $a \in \mathbb{Z}$ is a primitive root modulo p^2, then $a = \overline{(a, a, \ldots)} \in \mathcal{U}(\mathbb{Z}_p)$ is a good basis.

Definition 5.2.10. *Let $a \in \mathcal{U}(\mathbb{Z}_p)$ be a good basis. We define the map $\log_a : \mathcal{U}(\mathbb{Z}_p) \to E_p$, "logarithm in basis a", as the inverse of the map $E_p \to \mathcal{U}(\mathbb{Z}_p)$ given by $e \mapsto a^e$.*

The following proposition contains a list of properties that can be obtained immediately from the definition of the logarithm and theorem 5.2.4. Note the similitude with the properties of the standard logarithm in $\mathbb{R}$.

Proposition 5.2.11. *Let p be an odd prime. Let $a, b \in \mathcal{U}(\mathbb{Z}_p)$ be good bases. Let $c, d \in \mathbb{Z}_p$ and $e \in E_p$. Then:*

- $\log_a(1) = 0$ *and* $\log_a(a) = 1$
- $\log_a(cd) = \log_a(c) + \log_a(d)$
- $\log_a(c^e) = e \log_a(c)$
- $\log_b(c) = (\log_a(b))^{-1} \log_a(c)$
- *Besides, if e is invertible, then* $\log_a(\sqrt[e]{c}) = e^{-1} \log_a(c)$.

The first two identities of the last proposition mean that the map

$$\begin{array}{rcl} (\mathcal{U}(\mathbb{Z}_p), \cdot) & \xrightarrow{\log_a} & (E_p, +) \\ u & \longmapsto & \log_a(u) \end{array}$$

is a homomorphism of groups. Moreover, it is an isomorphism with inverse $(E_p, +) \to (\mathcal{U}(\mathbb{Z}_p), \cdot)$ given by $e \mapsto a^e$.

A consequence of the previous remark is that, for any odd prime p, the additive group E_p is isomorphic to the (multiplicative) group of invertible elements of $\mathbb{Z}_p$. By Theorem 5.2.2 we have that

$$(\mathcal{U}(\mathbb{Z}_p), \cdot) \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +) \times (\mathbb{Z}_p, +).$$

5.3 Pseudo-polynomial equations

In this section, we consider equations

$$a_1 X^{e_1} + a_2 X^{e_2} + \cdots + a_t X^{e_t} = c$$

in the unknown X, where a_i and c belong to $\mathbb{Z}_p$, e_i belongs to E_p. We look for a solution X in $\mathcal{U}(\mathbb{Z}_p)$. We call "pseudo-polynomial" this kind of equations.

In order to avoid difficulties with two subindexes, we will use a supraindex when referring to a particular element in the sequence representing a_i, e_i, c or X. More precisely, we write:

$$a_i = \overline{(a_i^{(j)})_{j\geq 1}}, \quad e_i = \overline{(e_i^{(j)})_{j\geq 1}}, \quad c = \overline{(c^{(j)})_{j\geq 1}}, \quad X = \overline{(X^{(j)})_{j\geq 1}}.$$

We solve these equations using Hensel Lifting, that is, by finding a recursive formula (Hensel step) for the sequence $X^{(j)}$.

Hensel step: Suppose that, for some $k \geq 1$, we already got $X^{(k)} \in \mathbb{Z}$ such that

$$\sum_{i=1}^{t} a_i^{(k)} \left(X^{(k)}\right)^{e_i^{(k)}} \equiv c^{(k)} \bmod p^k \quad \text{and} \quad p \nmid X^{(k)}.$$

We look for $X^{(k+1)} = X^{(k)} + p^k \Delta$ that satisfies the corresponding equation modulo p^{k+1}. More precisely, this equation is

$$\sum_{i=1}^{t} a_i^{(k+1)} \left(X^{(k+1)}\right)^{e_i^{(k+1)}} \equiv \sum_{i=1}^{t} a_i^{(k+1)} \left(X^{(k)} + p^k \Delta\right)^{e_i^{(k+1)}} \equiv c^{(k+1)} \bmod p^{k+1}.$$

Expanding the second sum and keeping only the first two terms (all the terms containing p^{2k} are zero modulo p^{k+1}), we get:

$$\sum_{i=1}^{t} a_i^{(k+1)} \left[\left(X^{(k)}\right)^{e_i^{(k+1)}} + e_i^{(k+1)} p^k \Delta \left(X^{(k)}\right)^{e_i^{(k+1)}-1}\right] \equiv c^{(k+1)} \bmod p^{k+1}$$

Using that $a_i^{(k+1)} \equiv a_i^{(k)} \bmod p^k$, that $e_i^{(k+1)} \equiv e_i^{(k)} \bmod \varphi(p^k)$, that $c^{(k+1)} \equiv c^{(k)} \bmod p^k$ and that $X^{(k)}$ satisfies the equation modulo p^k, we have

$$c^{(k+1)} - \sum_{i=1}^{t} a_i^{(k+1)} \left(X^{(k)}\right)^{e_i^{(k+1)}} \equiv 0 \bmod p^k.$$

Therefore we can write this term as $p^k \Theta$ where $\Theta \in \mathbb{Z}$ depends only on the input data and $X^{(k)}$. Replacing this in our equation, we get

$$p^k \Delta \sum_{i=1}^{t} a_i^{(k+1)} e_i^{(k+1)} \left(X^{(k)}\right)^{e_i^{(k+1)}-1} \equiv p^k \Theta \bmod p^{k+1},$$

and dividing by p^k we obtain

$$\Delta \sum_{i=1}^{t} a_i^{(k+1)} e_i^{(k+1)} \left(X^{(k)}\right)^{e_i^{(k+1)}-1} \equiv \Theta \bmod p.$$

Therefore, in order to guarantee the existence and uniqueness of Δ (and $X^{(k+1)}$), we need that

$$\sum_{i=1}^{t} a_i^{(k+1)} e_i^{(k+1)} \left(X^{(k)}\right)^{e_i^{(k+1)}-1} \not\equiv 0 \bmod p.$$

Since this equation is modulo p, we can replace $a_i^{(k+1)}$ by $a_i^{(1)}$, $X^{(k)}$ by $X^{(1)}$ and the $e_i^{(k+1)}$ in the exponent by $e_i^{(1)}$. On the other hand, the $e_i^{(k+1)}$ that appears multiplying cannot be replaced by $e_i^{(1)}$, because we know that both have the same remainder modulo $p-1$, but we cannot control their remainders modulo p. This is the reason we replace this $e_i^{(k+1)}$ by $e_i^{(2)}$ (they are congruent modulo $\varphi(p^2) = p(p-1)$). Putting all this together, we conclude that

$$\text{[Lifting Condition]} \quad \sum_{i=1}^{t} a_i^{(1)} e_i^{(2)} \left(X^{(1)}\right)^{e_i^{(1)}-1} \not\equiv 0 \bmod p$$

is a necessary and sufficient condition on the input data and $X^{(1)}$ that guarantees that we can compute $X^{(k+1)}$ from $X^{(k)}$.

Theorem 5.3.1. *Consider the pseudo-polynomial equation*

$$a_1 X^{e_1} + a_2 X^{e_2} + \cdots + a_t X^{e_t} = c$$

where $a_i = \overline{(a_i^{(j)})_{j\geq 1}} \in \mathbb{Z}_p$, $c = \overline{(c^{(j)})_{j\geq 1}} \in \mathbb{Z}_p$ *and* $e_i = \overline{(e_i^{(j)})_{j\geq 1}} \in E_p$.
Let $X^{(1)} \in \mathbb{Z}$ *be such that*

- $p \nmid X^{(1)}$
- $\displaystyle\sum_{i=1}^{t} a_i^{(1)} \left(X^{(1)}\right)^{e_i^{(1)}} \equiv c^{(1)} \mod p$
- $\displaystyle\sum_{i=1}^{t} a_i^{(1)} e_i^{(2)} \left(X^{(1)}\right)^{e_i^{(1)}-1} \not\equiv 0 \mod p$

Then there exists a unique solution $X = \overline{(X^{(1)}, X^{(2)}, \ldots)} \in \mathcal{U}(\mathbb{Z}_p)$ *of the pseudo-polynomial equation.*

Proof. We compute the sequence $X^{(k)}$ iteratively using the Hensel step. □

Now we analyze (with the same technique) a system of pseudo-polynomial equations with several unknowns. We use the following notation:

$$\sum_{i=1}^{t_n} a_{in} X_1^{e_{1in}} X_2^{e_{2in}} \cdots X_m^{e_{min}} = c_n, \quad 1 \leq n \leq N$$

where N is the number of equations and m is the number of unknowns. The coefficients a_{in} and c_n belong to $\mathbb{Z}_p$, the exponents e_{min} belong to E_p and the unknowns belong to $\mathcal{U}(\mathbb{Z}_p)$.

Hensel step: Suppose that we already got $X_1^{(k)}, X_2^{(k)}, \ldots, X_m^{(k)} \in \mathbb{Z}$, prime to p, such that

$$\sum_{i=1}^{t_n} a_{in}^{(k)} \left(X_1^{(k)}\right)^{e_{1in}^{(k)}} \left(X_2^{(k)}\right)^{e_{2in}^{(k)}} \cdots \left(X_m^{(k)}\right)^{e_{min}^{(k)}} \equiv c_n^{(k)} \bmod p^k, \quad 1 \leq n \leq N.$$

We look for $\Delta_1, \Delta_2, \ldots, \Delta_m \in \mathbb{Z}$, such that $X_j^{(k+1)} = X_j^{(k)} + p^k \Delta_j$ with $1 \leq j \leq m$, give a solution modulo p^{k+1}.

$$\begin{aligned}
c_n^{(k+1)} &\equiv \sum_{i=1}^{t_n} a_{in}^{(k+1)} \prod_{j=1}^{m} \left(X_j^{(k+1)}\right)^{e_{jin}^{(k+1)}} \bmod p^{k+1} \\
&\equiv \sum_{i=1}^{t_n} a_{in}^{(k+1)} \prod_{j=1}^{m} \left(X_j^{(k)} + p^k \Delta_j\right)^{e_{jin}^{(k+1)}} \bmod p^{k+1} \\
&\equiv \sum_{i=1}^{t_n} a_{in}^{(k+1)} \prod_{j=1}^{m} \left[\left(X_j^{(k)}\right)^{e_{jin}^{(k+1)}} + p^k e_{jin}^{(k+1)} \left(X_j^{(k)}\right)^{e_{jin}^{(k+1)}-1} \Delta_j\right] \bmod p^{k+1} \\
&\equiv \sum_{i=1}^{t_n} a_{in}^{(k+1)} \left[\prod_{j=1}^{m} \left(X_j^{(k)}\right)^{e_{jin}^{(k+1)}} + p^k \sum_{j=1}^{m} e_{jin}^{(k+1)} \left(X_j^{(k)}\right)^{e_{jin}^{(k+1)}-1} \Delta_j \prod_{q \neq j} \left(X_q^{(k)}\right)^{e_{qin}^{(k+1)}}\right] \bmod p^{k+1} \\
&\equiv \sum_{i=1}^{t_n} a_{in}^{(k+1)} \prod_{j=1}^{m} \left(X_j^{(k)}\right)^{e_{jin}^{(k+1)}} \\
&\quad + p^k \sum_{i=1}^{t_n} \sum_{j=1}^{m} a_{in}^{(k+1)} e_{jin}^{(k+1)} \left(X_j^{(k)}\right)^{e_{jin}^{(k+1)}-1} \Delta_j \prod_{q \neq j} \left(X_q^{(k)}\right)^{e_{qin}^{(k+1)}} \bmod p^{k+1}.
\end{aligned}$$

Since $a_{in}^{(k+1)} \equiv a_{in}^{(k)} \bmod p^k$, $e_{jin}^{(k+1)} \equiv e_{jin}^{(k)} \bmod \varphi(p^k)$ and $c_n^{(k+1)} \equiv c_n^{(k)} \bmod p^k$, our hypothesis means that

$$c_n^{(k+1)} - \sum_{i=1}^{t_n} a_{in}^{(k+1)} \prod_{j=1}^{m} \left(X_j^{(k)}\right)^{e_{jin}^{(k+1)}} = p^k \Theta_n, \quad 1 \leq n \leq N,$$

for some $\Theta_n \in \mathbb{Z}$ that only depends on the given data. Replacing this in the equations for Δ_j we get:

$$\sum_{j=1}^{m} \sum_{i=1}^{t_n} a_{in}^{(k+1)} e_{jin}^{(k+1)} \left(X_j^{(k)}\right)^{e_{jin}^{(k+1)}-1} \Delta_j \prod_{q \neq j} \left(X_q^{(k)}\right)^{e_{qin}^{(k+1)}} \equiv \Theta_n \bmod p, \quad 1 \leq n \leq N.$$

Reducing modulo p, these equations become:

$$\sum_{j=1}^{m}\sum_{i=1}^{t_n} a_{in}^{(1)} e_{jin}^{(2)} \left(X_j^{(1)}\right)^{e_{jin}^{(1)}-1} \Delta_j \prod_{q\neq j} \left(X_q^{(1)}\right)^{e_{qin}^{(1)}} \equiv \Theta_n \bmod p, \quad 1 \leq n \leq N.$$

In order to simplify these expressions, we define for $1 \leq j \leq m$ and $1 \leq n \leq N$:

$$K_{nj} = \sum_{i=1}^{t_n} a_{in}^{(1)} e_{jin}^{(2)} \left(X_j^{(1)}\right)^{e_{jin}^{(1)}-1} \prod_{q\neq j} \left(X_q^{(1)}\right)^{e_{qin}^{(1)}}$$

and rewrite the equations as

$$\sum_{j=1}^{m} K_{nj}\Delta_j \equiv \Theta_n \bmod p, \quad 1 \leq n \leq N.$$

Therefore the condition that guarantees the existence of at least a solution $\Delta_1, \ldots, \Delta_m$ modulo p is:

$$\operatorname{rank} \begin{bmatrix} K_{11} & \cdots & K_{1m} \\ \vdots & & \vdots \\ K_{N1} & \cdots & K_{Nm} \end{bmatrix} = N \quad \text{en } \mathbb{Z}/p\mathbb{Z}.$$

If we also want the solution to be unique, then we need to impose the extra condition $m = N$. In this case, the rank of the matrix is N if and only if its determinant is non-zero modulo p.

Theorem 5.3.2. *Consider the system of pseudo-polynomial equations*

$$\sum_{i=1}^{t_n} a_{in} X_1^{e_{1in}} X_2^{e_{2in}} \cdots X_m^{e_{min}} = c_n, \quad 1 \leq n \leq N$$

with N equations and m unknowns $X_1, \ldots, X_m$, where

$$a_{in} = \overline{(a_{in}^{(k)})_{k\geq 1}} \in \mathbb{Z}_p, \quad e_{jin} = \overline{(e_{jin}^{(k)})_{k\geq 1}} \in E_p \quad \textit{and} \quad c_n = \overline{(c_n^{(k)})_{k\geq 1}} \in \mathbb{Z}_p$$

Let $X_1^{(1)}, \ldots, X_m^{(1)} \in \mathbb{Z}$ prime to p be such that

$$\sum_{i=1}^{t_n} a_{in}^{(1)} \left(X_1^{(1)}\right)^{e_{1in}^{(1)}} \left(X_2^{(1)}\right)^{e_{2in}^{(1)}} \cdots \left(X_m^{(1)}\right)^{e_{min}^{(1)}} \equiv c_n^{(1)} \bmod p, \quad 1 \leq n \leq N.$$

For all $1 \leq j \leq m$ and $1 \leq n \leq N$ we define

$$K_{nj} = \sum_{i=1}^{t_n} a_{in}^{(1)} e_{jin}^{(2)} \left(X_j^{(1)}\right)^{e_{jin}^{(1)}-1} \prod_{q\neq j} \left(X_q^{(1)}\right)^{e_{qin}^{(1)}}.$$

If we have

$$\operatorname{rank}\begin{bmatrix} K_{11} & \cdots & K_{1m} \\ \vdots & & \vdots \\ K_{N1} & \cdots & K_{Nm} \end{bmatrix} = N \quad \text{in } \mathbb{Z}/p\mathbb{Z},$$

then there exists a solution $X_1, \ldots, X_m \in \mathcal{U}(\mathbb{Z}_p)$ *of the system, that extends the given solution modulo* p*, i.e.* $X_j = \overline{(X_j^{(1)}, X_j^{(2)}, \ldots)}$*. Moreover, in the case* $N = m$*, that solution* $X_1, \ldots, X_m$ *is unique.*

5.4 Exponential equations

In this section we consider equations

$$a_1 x_1^e + a_2 x_2^e + \ldots + a_t x_t^e = c$$

in the unknown e, where the a_i and c belong to $\mathbb{Z}_p$, the x_i belong to $\mathcal{U}(\mathbb{Z}_p)$. We look for a solution e in E_p. We call "exponential" this kind of equations.

As in the previous section, we use supraindexes for the sequences representing the elements of $\mathbb{Z}_p$ and E_p.

$$a_i = \overline{(a_i^{(j)})_{j\geq 1}} \quad x_i = \overline{(x_i^{(j)})_{j\geq 1}} \quad c = \overline{(c^{(j)})_{j\geq 1}} \quad e = \overline{(e^{(j)})_{j\geq 1}}$$

We also use the Hensel Lifting technique here, but first of all, we need a couple of technical results.

Definition 5.4.1. *For every* $x \in \mathbb{Z}$ *such that* $p \nmid x$*, we define* $L_p(x)$ *the only integer satisfying* $x^{p-1} = 1 + pL_p(x)$*.*

Lemma 5.4.2. *Let* $x, y \in \mathbb{Z}$ *be prime to* p*. Then*

1. *If* $x \equiv y \bmod p^2$*, then* $L_p(x) \equiv L_p(y) \bmod p$*.*
2. $L_p(xy) \equiv L_p(x) + L_p(y) \bmod p$*.*

Proof. (1.) Suppose that $y = x + p^2\Delta$ for some integer Δ. Then

$$y^{p-1} = (x + p^2\Delta)^{p-1} = x^{p-1} + \left[\text{multiples of } p^2\right],$$

and by the definition of $L_p(x)$ and $L_p(y)$ we get

$$1 + pL_p(y) = 1 + pL_p(x) + \left[\text{multiples of } p^2\right].$$

We conclude $L_p(y) \equiv L_p(x) \bmod p$.
(2.) Since $x^{p-1} = 1 + pL_p(x)$ and $y^{p-1} = 1 + pL_p(y)$, then

$$1 + pL_p(xy) = (xy)^{p-1} \equiv 1 + p(L_p(x) + L_p(y)) \bmod p^2.$$

Therefore $L_p(xy) \equiv L_p(x) + L_p(y) \bmod p$. □

Lemma 5.4.3. *Let $p \in \mathbb{N}$ be an odd prime and let $x \in \mathbb{Z}$ be prime to p. Then $x^{\varphi(p^k)} \equiv 1 + p^k L_p(x) \bmod p^{k+1}$ for all $k \geq 1$.*

Proof. We proceed by induction on k. The case $k = 1$ is immediate by definition of $L_p(x)$. Now suppose that the result is proven for some $k \geq 1$, i.e. $x^{\varphi(p^k)} \equiv 1 + p^k L_p(x) \bmod p^{k+1}$. Then there exists an integer Δ such that

$$\begin{aligned}\left(x^{\varphi(p^k)}\right)^p &= \left(1 + p^k L_p(x) + p^{k+1}\Delta\right)^p \\ &= \left(1 + p^k L_p(x)\right)^p + p\left(1 + p^k L_p(x)\right)^{p-1} p^{k+1}\Delta + \left[\text{multiples of } p^{2(k+1)}\right].\end{aligned}$$

Since $2(k+1) \geq k+2$, we have

$$\begin{aligned}x^{\varphi(p^{k+1})} &\equiv \left(1 + p^k L_p(x)\right)^p \bmod p^{k+2} \\ &\equiv 1 + p^{k+1} L_p(x) + \binom{p}{2} p^{2k} L_p(x)^2 + \left[\text{multiples of } p^{3k}\right] \bmod p^{k+2} \\ &\equiv 1 + p^{k+1} L_p(x) \bmod p^{k+2},\end{aligned}$$

the last line since $p \mid \binom{p}{2}$, $2k + 1 \geq k + 2$ and $3k \geq k + 2$. □

Now we have all the tools needed to analyze the lifting condition for exponential equations.

Hensel step: Suppose we already got a solution modulo p^k for some $k \geq 1$, i.e. we have $e^{(k)} \in \mathbb{N}$ such that

$$a_1^{(k)} \left(x_1^{(k)}\right)^{e^{(k)}} + \cdots + a_t^{(k)} \left(x_t^{(k)}\right)^{e^{(k)}} \equiv c^{(k)} \bmod p^k.$$

We look for $e^{(k+1)} = e^{(k)} + \varphi(p^k)\nabla$, with $\nabla \in \mathbb{N}$, that verifies the corresponding equation modulo p^{k+1}.

$$\sum_{i=1}^{t} a_i^{(k+1)} \left(x_i^{(k+1)}\right)^{e^{(k+1)}} \equiv \sum_{i=1}^{t} a_i^{(k+1)} \left(x_i^{(k+1)}\right)^{e^{(k)} + \varphi(p^k)\nabla} \equiv c^{(k+1)} \bmod p^{k+1}.$$

Using Lemma 5.4.3, expanding and erasing all the powers of p greater than p^{k+1}, we get

$$\begin{aligned}\sum_{i=1}^{t} a_i^{(k+1)} \left(x_i^{(k+1)}\right)^{e^{(k)} + \varphi(p^k)\nabla} &\equiv \sum_{i=1}^{t} a_i^{(k+1)} \left(x_i^{(k+1)}\right)^{e^{(k)}} \left(1 + p^k L_p(x_i^{(k+1)})\right)^{\nabla} \\ &\equiv \sum_{i=1}^{t} a_i^{(k+1)} \left(x_i^{(k+1)}\right)^{e^{(k)}} \left(1 + p^k \nabla L_p(x_i^{(k+1)})\right) \\ &\equiv c^{(k+1)} \bmod p^{k+1}.\end{aligned}$$

Since $a_i^{(k+1)} \equiv a_i^{(k)}$, $x_i^{(k+1)} \equiv x_i^{(k)}$ and $c^{(k+1)} \equiv c^{(k)} \bmod p^k$, we can reformulate our hypothesis as

$$c^{(k+1)} - \sum_{i=1}^{t} a_i^{(k+1)} \left(x_i^{(k+1)}\right)^{e^{(k)}} \equiv 0 \bmod p^k.$$

Therefore we can write this term as $p^k\Theta$ for some $\Theta \in \mathbb{Z}$ that only depends on the given data. Replacing this in the equation for ∇ and dividing by p^k, we obtain

$$\nabla \sum_{i=1}^{t} a_i^{(k+1)} \left(x_i^{(k+1)}\right)^{e^{(k)}} L_p(x_i^{(k+1)}) \equiv \Theta \bmod p.$$

In order to guarantee the existence (and uniqueness) of ∇ (hence $e^{(k+1)}$), we need that the following condition

$$\sum_{i=1}^{t} a_i^{(k+1)} \left(x_i^{(k+1)}\right)^{e^{(k)}} L_p(x_i^{(k+1)}) \not\equiv 0 \bmod p$$

holds. We can simplify this expression, taking into account that $a_i^{(k+1)} \equiv a_i^{(1)} \bmod p$, $x_i^{(k+1)} \equiv x_i^{(1)} \bmod p$, $e^{(k)} \equiv e^{(1)} \bmod \varphi(p)$ and $L_p(x_i^{(k+1)}) \equiv L_p(x_i^{(2)}) \bmod p$ by Lemma 5.4.2.

$$\text{[Lifting Condition]} \quad \sum_{i=1}^{t} a_i^{(1)} \left(x_i^{(1)}\right)^{e^{(1)}} L_p(x_i^{(2)}) \not\equiv 0 \bmod p$$

Up to this point, we have proven that any solution $e^{(1)}$ of the exponential equation (modulo p) that satisfies the Lifting Condition, can be extended (iteratively) to a solution in E_p. We summarize this result in the following theorem.

Theorem 5.4.4. *Consider the exponential equation*

$$a_1 x_1^e + a_2 x_2^e + \cdots + a_t x_t^e = c$$

where $a_i = \overline{(a_i^{(j)})_{j\geq 1}} \in \mathbb{Z}_p$, $c = \overline{(c^{(j)})_{j\geq 1}} \in \mathbb{Z}_p$ *and* $x_i = \overline{(x_i^{(j)})_{j\geq 1}} \in \mathcal{U}(\mathbb{Z}_p)$.
Let $e^{(1)} \in \mathbb{Z}$ *be such that*

- $\sum_{i=1}^{t} a_i^{(1)} \left(x_i^{(1)}\right)^{e^{(1)}} \equiv c^{(1)} \bmod p$
- $\sum_{i=1}^{t} a_i^{(1)} \left(x_i^{(1)}\right)^{e^{(1)}} L_p(x_i^{(2)}) \not\equiv 0 \bmod p.$

Then there exists a unique solution $e = \overline{(e^{(1)}, e^{(2)}, \ldots)} \in E_p$ *of the exponential equation.*

5.5 Duality between pseudo-polynomial and exponential equations

In this section we will show the equivalence between pseudo-polynomial and exponential equations, up to a change of variables. We will also show that this duality preserves the Lifting Condition.

Suppose first that we have the pseudo-polynomial equation

$$a_1 X^{e_1} + \cdots + a_t X^{e_t} = c$$

where $a_i \in \mathbb{Z}_p$, $e_i \in E_p$, $c \in \mathbb{Z}_p$ and the unknown $X \in \mathcal{U}(\mathbb{Z}_p)$.
Let $a \in \mathcal{U}(\mathbb{Z}_p)$ be a good basis. Making the change of variables $X = a^e$ we obtain the exponential equation

$$a_1(a^{e_1})^e + \cdots + a_t(a^{e_t})^e = c$$

with unknown $e \in E_p$. Note that $a^{e_i} \in \mathcal{U}(\mathbb{Z}_p)$ for all i, as required in the definition of the exponential equation.

On the other hand, if we start with an exponential equation

$$a_1 x_1^e + \cdots + a_t x_t^e = c$$

where $a_i \in \mathbb{Z}_p$, $x_i \in \mathcal{U}(\mathbb{Z}_p)$, $c \in \mathbb{Z}_p$ and the unknown $e \in E_p$, then it is possible to obtain a pseudo-polynomial equation by making the change $x_i = a^{e_i}$ where $e_i = \log_a(x_i) \in E_p$ and $X = a^e \in \mathcal{U}(\mathbb{Z}_p)$.

$$a_1(a^{e_1})^e + \cdots + a_t(a^{e_t})^e = c$$
$$a_1(\underbrace{a^e}_{=X})^{e_1} + \cdots + a_t(\underbrace{a^e}_{=X})^{e_t} = c$$

Note that if $X \in \mathcal{U}(\mathbb{Z}_p)$ is a solution of this equation, then $e = \log_a(X) \in E_p$ is a solution of the initial exponential equation.

Now we prove that the Lifting Condition is preserved under this duality. Suppose that we have a pseudo-polynomial equation and its corresponding exponential equation (via the substitutions $X = a^e$ and $x_i = a^{e_i}$) where $a = \overline{(a^{(j)})_{j\geq 1}} \in \mathcal{U}(\mathbb{Z}_p)$ is a good basis.

$$a_1 X^{e_1} + \cdots + a_t X^{e_t} = c \ \rightsquigarrow \ a_1 x_1^e + \cdots + a_t x_t^e = c$$

We use the supraindex notation as in the previous two sections, i.e.

$$a_i = \overline{(a_i^{(j)})_{j\geq 1}}, \quad c = \overline{(c^{(j)})_{j\geq 1}}, \quad e_i = \overline{(e_i^{(j)})_{j\geq 1}}, \quad X = \overline{(X^{(j)})_{j\geq 1}}$$
$$x_i = a^{e_i} = \overline{(x_i^{(j)})_{j\geq 1}} = \overline{((a^{(j)})^{e_i^{(j)}})_{j\geq 1}}, \quad e = \log_a(X) = \overline{(e^{(j)})_{j\geq 1}}$$

where a_i and c belong to $\mathbb{Z}_p$, x_i and X belong to $\mathcal{U}(\mathbb{Z}_p)$ and e_i and e belong to E_p.
If $X^{(1)} \not\equiv 0 \bmod p$ satisfies the Lifting Condition of the pseudo-polynomial equation (Th. 5.3.1), i.e.

$$\sum_{i=1}^{t} a_i^{(1)} e_i^{(2)} \left(X^{(1)}\right)^{e_i^{(1)}-1} \not\equiv 0 \mod p,$$

then

$$\begin{aligned}
\sum_{i=1}^{t} a_i^{(1)} \left(x_i^{(1)}\right)^{e^{(1)}} L_p(x_i^{(2)}) &= \sum_{i=1}^{t} a_i^{(1)} \left(a^{(1)}\right)^{e^{(1)}e_i^{(1)}} L_p((a^{(2)})^{e_i^{(2)}}) \\
&\equiv \sum_{i=1}^{t} a_i^{(1)} \left(X^{(1)}\right)^{e_i^{(1)}} e_i^{(2)} L_p(a^{(2)}) \mod p \\
&\equiv X^{(1)} L_p(a^{(2)}) \left[\sum_{i=1}^{t} a_i^{(1)} e_i^{(2)} \left(X^{(1)}\right)^{e_i^{(1)}-1}\right] \mod p \\
&\not\equiv 0 \mod p
\end{aligned}$$

since $L_p(a^{(2)}) \not\equiv 0 \bmod p$, for if $p|L_p(a^{(2)})$, we would obtain $(a^{(2)})^{\varphi(p)} \equiv 1 \bmod p^2$ which contradicts the fact that $a^{(2)}$ is a primitive root modulo p^2. This proves that the Lifting Condition for the exponential equation (Th. 5.4.4) also holds.

Using this duality we can directly translate Theorem 5.3.2 into an equivalent theorem for systems of exponential equations.

Theorem 5.5.1. *Consider the system of exponential equations*

$$\sum_{i=1}^{t_n} a_{in} x_{1in}^{e_1} x_{2in}^{e_2} \cdots x_{min}^{e_m} = c_n \qquad 1 \le n \le N$$

with N equations and m unknowns, where $a_{in} \in \mathbb{Z}_p$, $x_{jin} \in \mathcal{U}(\mathbb{Z}_p)$, $c_n \in \mathbb{Z}_p$ and the unknowns $e_j \in E_p$. Let $e^{(1)}, \ldots, e^{(m)} \in \mathbb{Z}$ be such that

$$\sum_{i=1}^{t_n} a_{in}^{(1)} \left(x_{1in}^{(1)}\right)^{e_1^{(1)}} \cdots \left(x_{min}^{(1)}\right)^{e_m^{(1)}} \equiv c_n^{(1)} \mod p \quad 1 \le n \le N.$$

For all $1 \le j \le m$ and $1 \le n \le N$ we define

$$K_{nj} = \sum_{i=1}^{t_n} a_{in}^{(1)} \left(x_{1in}^{(1)}\right)^{e_1^{(1)}} \cdots \left(x_{min}^{(1)}\right)^{e_m^{(1)}} L_p(x_{jin}^{(2)}).$$

If we have

$$\operatorname{rank} \begin{bmatrix} K_{11} & \cdots & K_{1m} \\ \vdots & & \vdots \\ K_{N1} & \cdots & K_{Nm} \end{bmatrix} = N \quad \text{in } \mathbb{Z}/p\mathbb{Z},$$

then there exists a solution $e_1, \ldots, e_m \in E_p$ of the system, that extends the given solution modulo p, i.e. $e_j = \overline{(e_j^{(1)}, e_j^{(2)}, \ldots)}$. Moreover, in the case $N = m$, that solution is unique.

5.6 Interpolation lifting

In this section we study the systems of equations that arise in the problem of interpolation (of a pseudo-polynomial expression). First we prove a more general version of Theorem 2.2.1 of the Introduction that gives the lifting condition for the problem of interpolation of a pseudo-polynomial expression when the points are in $\mathcal{U}(\mathbb{Z}_p)$.

Theorem 5.6.1. *Consider a system of equations*

$$\sum_{i=1}^{t} a_i x_n^{e_i} = c_i \qquad 1 \le n \le 2t \tag{5.1}$$

where the interpolation points $x_n \in \mathcal{U}(\mathbb{Z}_p)$ and $c_i \in \mathbb{Z}_p$ are given, and the unknowns are both coefficients $a_i \in \mathcal{U}(\mathbb{Z}_p)$ and the exponents $e_i \in E_p$ (note that we have $2t$ equations and $2t$

unknowns). Let $a_i^{(1)} \in \mathbb{Z}$, *such that* $p \nmid a_i^{(1)}$, *and let* $e_i^{(1)} \in \mathbb{Z}$ *for all* $1 \leq i \leq t$ *be a solution of (5.1) modulo* p. *If the following Lifting Condition*

$$p \nmid \det \begin{bmatrix} (x_1^{(1)})^{e_1^{(1)}} L_p(x_1^{(2)}) & \cdots & (x_1^{(1)})^{e_t^{(1)}} L_p(x_1^{(2)}) & (x_1^{(1)})^{e_1^{(1)}} & \cdots & (x_1^{(1)})^{e_t^{(1)}} \\ \vdots & & \vdots & \vdots & & \vdots \\ (x_{2t}^{(1)})^{e_1^{(1)}} L_p(x_{2t}^{(2)}) & \cdots & (x_{2t}^{(1)})^{e_t^{(1)}} L_p(x_{2t}^{(2)}) & (x_{2t}^{(1)})^{e_1^{(1)}} & \cdots & (x_{2t}^{(1)})^{e_t^{(1)}} \end{bmatrix} \tag{5.2}$$

holds, then there exists unique $a_i \in \mathcal{U}(\mathbb{Z}_p)$ *and* $e_i \in E_p$ *for* $1 \leq i \leq t$ *solution of (5.1) that extends the given solution modulo* p.

Proof. Suppose that $a \in \mathcal{U}(\mathbb{Z}_p)$ is a good basis. Then we can write $a_i = a^{e_{i+t}}$ for some unknowns $e_{t+1}, \ldots, e_{2t} \in E_p$. This trick allow us to reformulate the interpolation problem as the system of exponential equations

$$\sum_{i=1}^{t} a^{e_{i+t}} x_n^{e_i} = c_i \qquad 1 \leq n \leq 2t$$

where the unknowns are $e_1, \ldots, e_{2t} \in E_p$. We use Theorem 5.5.1 to study this system. Here, the numbers K_{nj} adopt a very simple expression:

$$K_{nj} = \begin{cases} (a^{(1)})^{e_{j+t}^{(1)}} (x_n^{(1)})^{e_j^{(1)}} L_p(x_n^{(2)}) & 1 \leq j \leq t \\ \\ (a^{(1)})^{e_j^{(1)}} (x_n^{(1)})^{e_{j-t}^{(1)}} L_p(a^{(2)}) & t+1 \leq j \leq 2t. \end{cases}$$

Since the matrix $(K_{nj})_{1 \leq n,j \leq 2t}$ is square, then the condition to be full rank (in $\mathbb{Z}/p\mathbb{Z}$) is equivalent to its determinant to be non-zero modulo p.

$$\begin{bmatrix} (a^{(1)})^{e_{t+1}^{(1)}} (x_1^{(1)})^{e_1^{(1)}} L_p(x_1^{(2)}) & \cdots & (a^{(1)})^{e_{2t}^{(1)}} (x_1^{(1)})^{e_t^{(1)}} L_p(x_1^{(2)}) & (a^{(1)})^{e_{t+1}^{(1)}} (x_1^{(1)})^{e_1^{(1)}} L_p(a^{(2)}) & \cdots & (a^{(1)})^{e_{2t}^{(1)}} (x_1^{(1)})^{e_t^{(1)}} L_p(a^{(2)}) \\ \vdots & & \vdots & \vdots & & \vdots \\ (a^{(1)})^{e_{t+1}^{(1)}} (x_{2t}^{(1)})^{e_1^{(1)}} L_p(x_{2t}^{(2)}) & \cdots & (a^{(1)})^{e_{2t}^{(1)}} (x_{2t}^{(1)})^{e_t^{(1)}} L_p(x_{2t}^{(2)}) & (a^{(1)})^{e_{t+1}^{(1)}} (x_{2t}^{(1)})^{e_1^{(1)}} L_p(a^{(2)}) & \cdots & (a^{(1)})^{e_{2t}^{(1)}} (x_{2t}^{(1)})^{e_t^{(1)}} L_p(a^{(2)}) \end{bmatrix}$$

It is clear that we can take away all the $a^{e_{t+j}}$ in each column (because we known that they are not zero modulo p). We also known that $p \nmid L_p(a)$ since a is a primitive root modulo p^2, so we can also take them away. This lead us to the Lifting Condition (5.2). □

Note that we have restricted our analysis of the interpolation problem (5.1) to pseudo-polynomial expressions whose coefficients are in $\mathcal{U}(\mathbb{Z}_p)$. We needed this in order to apply the duality between pseudo-polynomial and exponential equations. On the other hand, it is clear that the condition (5.2) implies that $e_i^{(1)} \not\equiv e_j^{(1)} \pmod{\varphi(p)}$ for all $1 \leq i < j \leq t$. This motivates the following definition for polynomials with integer coefficients:

Definition 5.6.2. *Let* $f = \sum_{i=1}^{t} a_i x^{e_i} \in \mathbb{Z}[x]$ *be a* t*-lacunary polynomial and let* $p \in \mathbb{N}$ *be a prime. We say that* f *has a* good reduction modulo p *if* $p \nmid a_i$ *for all* $1 \leq i \leq t$ *and* $p - 1 \nmid e_i - e_j$ *for all* $1 \leq i < j \leq t$.

It is clear that every polynomial $f \in \mathbb{Z}[x]$ has bad reduction at only a finite set of primes.

We have also restricted the interpolation points $x_1, \ldots, x_{2t}$ to be in $\mathcal{U}(\mathbb{Z}_p)$. In the case of integer points this is equivalent to $p \nmid x_i$ for all $1 \leq i \leq 2t$.

Definition 5.6.3. *Let $f = \sum_{i=1}^{t} a_i x^{e_i} \in \mathbb{Z}[x]$ be a t-lacunary polynomial and let $p \in \mathbb{N}$ be a prime such that f has a good reduction modulo p. We say that the points $x_1, \ldots, x_{2t} \in \mathbb{Z}$ are* suitable for f (w.r.t. p) *if $p \nmid x_i$ for all $1 \leq i \leq 2t$ and condition (5.2) holds.*

In particular, the points $x_1, \ldots, x_{2t}$ are all different modulo p^2. Otherwise the matrix in (5.2) would have two identical rows modulo p.

It is not clear at all that a polynomial $f \in \mathbb{Z}[x]$ having a good reduction modulo a prime $p \in \mathbb{N}$ has necessarily a suitable set of points $x_1, \ldots, x_{2t} \in \mathbb{Z}$. The next theorem shows two families of points with this property.

Theorem 5.6.4. *Let $f = \sum_{i=1}^{t} a_i x^{e_i} \in \mathbb{Z}[x]$ be a t-lacunary polynomial and let $p \in \mathbb{N}$ be a prime such that f has a good reduction modulo p. The following $2t$ points are suitable for f (w.r.t. p):*

1. *$x_i \equiv \rho^{i-1} \pmod{p^2}$ for all $1 \leq i \leq 2t$, where ρ is a primitive root modulo p^2.*
2. *$x_i \equiv \rho^{i-1} \pmod{p}$ and $x_{i+t} = x_i + p$ for all $1 \leq i \leq t$, where ρ is a primitive root modulo p.*

Proof. (1.) Denote by $r = L_p(\rho)$. By Lemma 5.4.2 we have that $L_p(x_i) \equiv (i-1)r \pmod{p}$ for all $1 \leq i \leq 2t$, and since ρ is primitive modulo p^2 we have $r \not\equiv 0 \pmod{p}$. It is convenient to introduce the quantities $z_i = \rho^{e_i}$ for $1 \leq i \leq t$. We have that $z_i \not\equiv z_j \pmod{p}$ for all $i \neq j$, because f reduces well modulo p. We compute the determinant in (5.2) modulo p explicitly:

$$\det \begin{bmatrix} x_1^{e_1} L_p(x_1) & \cdots & x_1^{e_t} L_p(x_1) & x_1^{e_1} & \cdots & x_1^{e_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{2t}^{e_1} L_p(x_{2t}) & \cdots & x_{2t}^{e_t} L_p(x_{2t}) & x_{2t}^{e_1} & \cdots & x_{2t}^{e_t} \end{bmatrix} \equiv$$

$$\equiv \det \begin{bmatrix} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \rho^{e_1} r & \cdots & \rho^{e_t} r & \rho^{e_1} & \cdots & \rho^{e_t} \\ \rho^{2e_1} 2r & \cdots & \rho^{2e_t} 2r & \rho^{2e_1} & \cdots & \rho^{2e_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ \rho^{(2t-1)e_1}(2t-1)r & \cdots & \rho^{(2t-1)e_t}(2t-1)r & \rho^{(2t-1)e_1} & \cdots & \rho^{(2t-1)e_t} \end{bmatrix} \equiv$$

$$\equiv (-1)^t \det \begin{bmatrix} 1 & \cdots & 1 & 0 & \cdots & 0 \\ z_1 & \cdots & z_t & z_1 r & \cdots & z_t r \\ z_1^2 & \cdots & z_t^2 & 2z_1^2 r & \cdots & 2z_t^2 r \\ \vdots & & \vdots & \vdots & & \vdots \\ z_1^{2t-1} & \cdots & z_t^{2t-1} & (2t-1)z_1^{2t-1} r & \cdots & (2t-1)z_t^{2t-1} r \end{bmatrix} \equiv$$

$$\equiv (-1)^t r^t z_1 \cdots z_t \det \begin{bmatrix} 1 & \cdots & 1 & 0 & \cdots & 0 \\ z_1 & \cdots & z_t & 1 & \cdots & 1 \\ z_1^2 & \cdots & z_t^2 & 2z_1 & \cdots & 2z_t \\ \vdots & & \vdots & \vdots & & \vdots \\ z_1^{2t-1} & \cdots & z_t^{2t-1} & (2t-1)z_1^{2t-2} & \cdots & (2t-1)z_t^{2t-2} \end{bmatrix} \equiv$$

$$\equiv (-1)^{t(t+1)/2} r^t z_1 \cdots z_t \prod_{1 \le i < j \le t} (z_i - z_j)^4 \not\equiv 0 \pmod{p}$$

(2.) In this case, we have $L_p(x_{i+t}) = L_p(x_i) - x_i^{-1}$ for all $1 \le i \le t$, because

$$x_{i+t}^{p-1} = (x_i + p)^{p-1} \equiv x_i^{p-1} + p(p-1)x_i^{p-2} \equiv 1 + p(L_p(x_i) - x_i^{-1}) \pmod{p^2}.$$

Since $x_i \equiv x_{i+t} \pmod{p}$, the determinant in (5.2) becomes:

$$\det \begin{bmatrix} x_1^{e_1} L_p(x_1) & \cdots & x_1^{e_t} L_p(x_1) & x_1^{e_1} & \cdots & x_1^{e_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_t^{e_1} L_p(x_t) & \cdots & x_t^{e_t} L_p(x_t) & x_t^{e_1} & \cdots & x_t^{e_t} \\ x_1^{e_1}(L_p(x_1) - x_1^{-1}) & \cdots & x_1^{e_t}(L_p(x_1) - x_1^{-1}) & x_1^{e_1} & \cdots & x_1^{e_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_t^{e_1}(L_p(x_t) - x_t^{-1}) & \cdots & x_t^{e_t}(L_p(x_t) - x_t^{-1}) & x_t^{e_1} & \cdots & x_t^{e_t} \end{bmatrix} \equiv$$

$$\equiv \det \begin{bmatrix} x_1^{e_1} L_p(x_1) & \cdots & x_1^{e_t} L_p(x_1) & x_1^{e_1} & \cdots & x_1^{e_t} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_t^{e_1} L_p(x_t) & \cdots & x_t^{e_t} L_p(x_t) & x_t^{e_1} & \cdots & x_t^{e_t} \\ -x_1^{e_1-1} & \cdots & -x_1^{e_t-1} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ -x_t^{e_1-1} & \cdots & -x_t^{e_t-1} & 0 & \cdots & 0 \end{bmatrix} \equiv$$

$$\equiv x_1^{-1} \cdots x_t^{-1} \det \begin{bmatrix} x_1^{e_1} & \cdots & x_1^{e_t} \\ \vdots & & \vdots \\ x_t^{e_1} & \cdots & x_t^{e_t} \end{bmatrix}^2 \equiv x_1^{-1} \cdots x_t^{-1} \prod_{1 \le i < j \le t} (\rho^{e_i} - \rho^{e_j})^2 \not\equiv 0 \pmod{p}$$

□

Note that the points $x_1, \ldots, x_{2t}$ of the previous theorem are suitable for every t-lacunary polynomial having a good reduction modulo p.

5.7 Interpolation in $\mathbb{Z}[x]$ – Heuristics

Let $f = \sum_{i=1}^{t} a_i x^{e_i} \in \mathbb{Z}[x]$ be an unknown t-lacunary polynomial, let $x_1, \ldots, x_{2t} \in \mathbb{N}$ be arbitrary given points, and let $y_i = f(x_i)$ for all $1 \le i \le 2t$. We want to recover f from the interpolation points $(x_i, y_i)_{1 \le i \le 2t}$, that completely determine the polynomial by Descartes' Rule of Signs.

The first step consist in selecting a prime number $p \in \mathbb{N}$ such that f reduces well modulo p, such that $p \nmid x_i$ for all $1 \leq i \leq 2t$ and such that condition (5.2) holds. It is clear that the first two restrictions hold for almost every prime numbers, that is, all the prime numbers but finite. More precisely, any prime number greater than all the x_i, the $|a_i|$ and the $|e_i - e_j|$ satisfies these two properties. On the other hand, the last condition is more complicated: the determinant in (5.2) is not constant because $L_p(x_i)$ depends on p. It is still an open question how to find such p, or even to prove that such a prime exists. However, numerical experiments show that this determinant is "uniformly distributed" modulo p, when $e_1, \ldots, e_t \in \mathbb{N}$ and $x_1, \ldots, x_{2t} \in \mathbb{Z}$ are fixed, and p ranges over the prime numbers. If this evidence turns out to be true, then the "probability" for a prime to satisfy condition 5.2 would be very big (and increasing with p), so practically every prime number satisfying the first two conditions would also meet the third one. We propose here to go on, assuming that p is given (as part of the input).

The second step consists in computing the reduction of f modulo p, that is, the coefficients are reduced modulo p and the exponents modulo $\varphi(p)$. The idea is to determine it via the values x_i and y_i modulo p. Unfortunately, this is not possible if the points are arbitrary, for instance, $f = x^4 + 3$ and $g = 3x^3 + x$ coincide modulo 7 at $x = 1, 2, 3, 4$. We present here two partial solutions that allow us to go on:

A1. Assume that we know the values of f modulo p at the points $x = 1, 2, \ldots, p-1$, and then apply Lagrange Interpolation to recover the reduction of f modulo p.

A2. Assume that the points $x_1, \ldots, x_{2t}$ (when reduced modulo p) correspond to consecutive powers of a primitive root modulo p, i.e. $x_i \equiv \rho^{a+i} \pmod{p}$ for all $1 \leq i \leq 2t$ and some primitive root ρ modulo p. Next theorem shows that this is enough to recover the reduction of f modulo p.

Theorem 5.7.1. *Let $f = \sum_{i=1}^{t} a_i x^{e_i} \in \mathbb{F}_p[x]$ such that $0 \leq e_1 < e_2 < \cdots < e_t < p-1$ and $a_i \neq 0$ for all $1 \leq i \leq t$. Let $\rho \in \mathbb{F}_p$ be a given primitive root. Then f is uniquely determined by the values $f(1), f(\rho), \ldots, f(\rho^{2t-1})$.*

Proof. We derive the result by proving that a non-zero polynomial with at most $2t$ non-zero terms (and exponents $< p-1$) cannot vanish at all the points $x = 1, \rho, \ldots, \rho^{2t-1}$. Suppose on the contrary that there exists a non-zero polynomial $g = \sum_{i=1}^{2t} b_i x^{d_i} \in \mathbb{F}_p[x]$, with exponents $0 \leq d_1 < d_2 < \cdots < d_{2t} < p-1$, satisfies $g(1) = g(\rho) = \cdots = g(\rho^{2t-1}) = 0$. These relations can be written as:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \rho^{e_1} & \rho^{e_2} & \cdots & \rho^{e_{2t}} \\ \vdots & \vdots & & \vdots \\ \rho^{(2t-1)e_1} & \rho^{(2t-1)e_2} & \cdots & \rho^{(2t-1)e_{2t}} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{2t} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

This is a Vandermonde system of linear equations with determinant $\prod_{1 \leq i < j \leq 2t} (\rho^{e_i} - \rho^{e_j})$, which is not zero in $\mathbb{F}_p$ because ρ is primitive and the exponents cannot differ in $p-1$. □

If we take the primitive root $\rho = 3$ modulo 7, Theorem 5.7.1 proves that a binomial is determined by its value at the points $x = 1, 3, 3^2, 3^3$ modulo 7, i.e. $x = 1, 3, 2, 6$. We showed above two binomials $f, g \in \mathbb{F}_7[x]$ that coincide at $x = 1, 2, 3, 4$. Note that they differ when evaluated at $x = 6$: $f(6) = 4$ but $g(6) = 3$.

Theorem 5.7.1 proves that A2 makes sense, but it does not give any idea about how to compute the reduction of f modulo p. Of course, if p and t are small, we can try all the possible set of coefficients and exponents until we find the polynomial that interpolates, but this procedure is clearly not practical when p and t are big (the search space has $\binom{p-1}{t}(p-1)^t$ elements). Even if we reduce the search space to the exponents (and use linear algebra to recover the coefficients), the number of elements is $\binom{p-1}{t}$, which is still too big. This procedure can be useful when p is close to t, but in general we cannot guarantee this.

In order to reduce further the search space we use here a procedure developed by Ben-Or and Tiwari (see [BeTi88]). The idea is to compute the polynomial $H(x) = \prod_{i=1}^{t}(x - \rho^{e_i}) \in \mathbb{F}_p[x]$, then factorize it in order to recover $\rho^{e_1}, \ldots, \rho^{e_t}$ (we can do this in polynomial time in p and t, see [Ber70]) and finally reconstruct $e_1, \ldots, e_t$ by determining their discrete logarithm (we need at most pt trials here). It only remains to show how to efficiently compute $H(x)$.

Theorem 5.7.2. [Ben-Or, Tiwari] *Let $f = \sum_{i=1}^{t} a_i x^{e_i} \in \mathbb{F}_p[x]$ with $0 \leq e_1 < \cdots < e_t < p-1$ and $a_i \neq 0$ for all $1 \leq i \leq t$. Let $\rho \in \mathbb{F}_p$ be a primitive root. Let $H = \prod_{i=1}^{t}(x - \rho^{e_i}) = x^t - b_{t-1}x^{t-1} - \cdots - b_0 \in \mathbb{F}_p[x]$. Then the coefficients of H are the unique solution of*

$$\begin{bmatrix} f(1) & f(\rho) & \cdots & f(\rho^{t-1}) \\ f(\rho) & f(\rho^2) & \cdots & f(\rho^t) \\ \vdots & \vdots & & \vdots \\ f(\rho^{t-1}) & f(\rho^t) & \cdots & f(\rho^{2t-2}) \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{t-1} \end{bmatrix} = \begin{bmatrix} f(\rho^t) \\ f(\rho^{t+1}) \\ \vdots \\ f(\rho^{2t-1}) \end{bmatrix}.$$

Proof. We compute the following product of matrices:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \rho^{e_1} & \rho^{e_2} & \cdots & \rho^{e_t} \\ \vdots & \vdots & & \vdots \\ \rho^{(t-1)e_1} & \rho^{(t-1)e_2} & \cdots & \rho^{(t-1)e_t} \end{bmatrix} \begin{bmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_t \end{bmatrix} \begin{bmatrix} 1 & \rho^{e_1} & \cdots & \rho^{(t-1)e_1} \\ 1 & \rho^{e_2} & \cdots & \rho^{(t-1)e_2} \\ \vdots & \vdots & & \vdots \\ 1 & \rho^{e_t} & \cdots & \rho^{(t-1)e_t} \end{bmatrix} \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{t-1} \end{bmatrix}.$$

Since ρ^{e_i} is a root of $H(x)$, then $\rho^{te_i} = h_0 + h_1\rho^{e_i} + \cdots + h_{t-1}\rho^{(t-1)e_i}$ for all i. This implies that the product of the rightmost two matrices is $[\rho^{te_1}\ \rho^{te_2}\ \cdots\ \rho^{te_t}]^T$. Multiplying it by the diagonal of coefficients of f we get $[a_1\rho^{te_1}\ a_2\rho^{te_2}\ \cdots\ a_t\rho^{te_t}]^T$, and then the product of all the matrices is $[f(\rho^t)\ f(\rho^{t+1})\ \cdots\ f(\rho^{2t-1})]^T$. It is also a straight-forward computation that the product of the first three matrices is $M = [f(\rho^{i+j})]_{0 \leq i,j \leq t-1}$. Finally, the determinant of M is the product of three determinants (two of them correspond to Vandermonde matrices and the other to a diagonal matrix), i.e. $\det(M) = a_1 a_2 \cdots a_t \prod_{1 \leq i < j \leq t}(\rho^{e_i} - \rho^{e_j})^2 \neq 0$. □

The last step consists in applying the Interpolation Lifting of Section 5.6 to obtain the sequence of reductions of f modulo p^2, p^3, etc. If we choose the coefficients of these reductions

in $(-p^k/2, p^k/2)$, and the exponents in $[0, \varphi(p^k) - 1]$, the sequence is eventually constant (it stabilizes at f). We can stop the lifting when we produce a polynomial that coincides with f at the integer points $x_1, \ldots, x_{2t}$. We know that this determines f uniquely.

Next we estimate the number of bit operations required by both A1 and A2 and compare their performance.

In A1 we need to interpolate a polynomial in $\mathbb{F}_p$ of degree $p-2$, that is, we have to solve a Vandermonde linear system with $p-1$ equations and $p-1$ unknowns in $\mathbb{F}_p$. We need $O(p^3)$ operations in $\mathbb{F}_p$ to solve it (actually, there are superfast algorithms for Vandermonde systems that only need $O(p^2 \log^3(p))$ operations in $\mathbb{F}_p$ [Pan01]), and since each operation in $\mathbb{F}_p$ requires $O(\log^2(p))$ bit operations, the complexity of this case is of order $O(p^3 \log^2(p))$, which can be lowered to $O(p^2 \log^5(p))$ if we apply the superfast algorithm.

In A2 we need to solve a square system of $2t$ linear equations in $\mathbb{F}_p$. This requires $O(t^3)$ operations in $\mathbb{F}_p$, i.e. $O(t^3 \log^2(p))$ bit operations. After that, we need to solve t discrete logarithm problems in $\mathbb{F}_p$. There is no algorithm known yet to solve this problem efficiently, so we have to content ourselves with a straightforward search over all the possible exponents. This requires a single entry table $e \leftrightarrow \rho^e$ with $0 \le e < p$ for a fixed primitive root $\rho \in \mathbb{F}_p$, which can be computed in p operations in $\mathbb{F}_p$, that is, in $O(p \log^2(p))$ bit operations. The overall complexity of this case is $O((t^3 + p) \log^2(p))$.

It is clear from the analysis above that A2 is preferable over A1, unless p is of order $O(t^{3/2})$ or less. Another reason to prefer A2 over A1 is that the former needs consecutive powers of a primitive root modulo p as starting points, which can be chosen as the same as those in the first family of Theorem 5.6.4, since a primitive root modulo p^2 is also primitive modulo p, thus reducing the number of evaluations of f. However, there seems to be more room for improvements in the problem of solving a Vandermonde system of linear equations than in the discrete logarithm problem (there are already relevant results in that direction modulo some extra hypothesis). If such an improvement were achieved, then both strategies would be comparable.

Chapter 6

The number of roots of a bivariate polynomial on a line

6.1 Changes of signs

Definition 6.1.1. *Let $f \in \mathbb{R}[x]$ be a non-zero polynomial. We denote by $V(f)$ the number of changes of signs in the sequence of coefficients of f skipping the zeros. We also set $V(0) = -2$.*

Remark. *Let $f \in \mathbb{R}[x]$. Then $V(kf(rx)) = V(f)$ for all $k \neq 0$ and $r > 0$.*

Theorem 6.1.2. [Descartes' rule of signs] *Let $f \in \mathbb{R}[x]$ be a non-zero polynomial. Then f has at most $V(f)$ positive roots counted with multiplicities.*

Let us point out here that this famous theorem is a consequence of the following fact: if $f \in \mathbb{R}[x]$ is a non-zero polynomial and $r > 0$, then $V((x-r)f) \geq V(f) + 1$, i.e. if we add a positive root to a polynomial, then its number of changes of signs increases at least by 1. Next lemma gives an analogue of this property for negative roots.

Lemma 6.1.3. *Let $f \in \mathbb{R}[x]$ and let $r > 0$. Then $V((x+r)f) \leq V(f)$.*

Proof. By the previous remark, we have $V((x+r)f) = V((rx+r)f(rx)) = V((x+1)f(rx))$ and $V(f(rx)) = V(f)$. Therefore we only need to consider the case $r = 1$. We proceed by induction in the number t of non-zero terms of f. The theorem is trivial for $t = 0$ and $t = 1$. Now let us suppose that it holds for all $t \leq n$. Let $f \in \mathbb{R}[x]$ with $n+1$ non-zero monomials.

$$f = \sum_{i=1}^{n+1} a_i x^{\alpha_i} \quad \text{where} \quad a_i \neq 0 \, \forall \, i \quad \text{and} \quad 0 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_{n+1} = d = \deg(f)$$

Let $g = \sum_{i=1}^{n} a_i x^{\alpha_i}$. By inductive hypothesis we have $V((x+1)g) \leq V(g)$. First, we consider the case $\alpha_n < d-1$, i.e. when the terms of $(x+1)g$ do not overlap with those of $a_{n+1}x^d(x+1)$. There are two possibilities: if $a_n a_{n+1} > 0$, then $V((x+1)f) = V((x+1)g) \leq V(g) = V(f)$, and

if $a_n a_{n+1} < 0$, then $V((x+1)f) = V((x+1)g) + 1 \leq V(g) + 1 = V(f)$. In both cases we have $V((x+1)f) \leq V(f)$. Now the only remaining case is $\alpha_n = d - 1$. Here $(x+1)f$ and $(x+1)g$ only differ in their terms of degree d and $d+1$, as shown in the following table.

	x^d	x^{d+1}
$(x+1)g$	a_n	0
$(x+1)f$	$a_n + a_{n+1}$	a_{n+1}

If $a_n a_{n+1} > 0$, then $V(f) = V(g)$, and according to the table, we have $V((x+1)f) = V((x+1)g)$. Therefore $V((x+1)f) \leq V(f)$. On the other hand, if $a_n a_{n+1} < 0$, then $V(f) = V(g) + 1$, but we have three different possibilities for the table, depending whether $|a_n|$ is greater, equal or less than $|a_{n+1}|$. Set s for the sign of a_n.

	x^d	x^{d+1}
$(x+1)g$	s	0
$(x+1)f$	s	$-s$

Case $|a_n| > |a_{n+1}|$

	x^d	x^{d+1}
$(x+1)g$	s	0
$(x+1)f$	0	$-s$

Case $|a_n| = |a_{n+1}|$

	x^d	x^{d+1}
$(x+1)g$	s	0
$(x+1)f$	$-s$	$-s$

Case $|a_n| < |a_{n+1}|$

The tables above show that $V((x+1)f) \leq V((x+1)g) + 1$ for each of the three cases. Using the inductive hypothesis and $V(f) = V(g) + 1$, we conclude that $V((x+1)f) \leq V(f)$. □

Remark. *Let $f, g \in \mathbb{R}[x]$ and suppose that g has t terms. Then $V(f+g) \leq V(f) + 2t$.*

Note that the value of $V(0)$ is not relevant for Theorem 6.1.2 and Lemma 6.1.3. The only reason for defining $V(0) = -2$ is the previous remark (in the case $f = 0$ and $t = 1$).

Proposition 6.1.4. *Let $f \in \mathbb{R}[x, y]$ with t non-zero terms. Let $p = (x + r_1) \cdots (x + r_n) \in \mathbb{R}[x]$ where $r_i > 0$ for all $i = 1, \ldots, n$. Then*

$$V(f(x, p(x))) \leq 2t - 2.$$

Proof. We write $f = \sum_{i=1}^{n} a_i(x) y^{\alpha_i}$, where $0 \leq \alpha_1 < \cdots < \alpha_n$ and $a_i(x) \in \mathbb{R}[x]$, and we set $t_i > 0$ the number of non-zero terms of a_i. It is clear that $t = t_1 + \ldots + t_n$.
We define $f_k = \sum_{i=k}^{n} a_i(x) y^{\alpha_i - \alpha_k}$ for $k = 1, \ldots, n$ and $f_{n+1} = 0$. Lemma 6.1.3 and the previous remark imply that the polynomials f_k satisfy:

- $f_{n+1} = 0 \quad \Rightarrow \quad V(f_{n+1}(x, p(x))) = -2$
- $f_k = y^{\alpha_{k+1} - \alpha_k} f_{k+1} + a_k(x) \quad \Rightarrow \quad f_k(x, p(x)) = p(x)^{\alpha_{k+1} - \alpha_k} f_{k+1}(x, p(x)) + a_k(x) \quad \Rightarrow$ $V(f_k(x, p(x))) \leq V(f_{k+1}(x, p(x))) + 2t_k$
- $f = y^{\alpha_1} f_1 \quad \Rightarrow \quad f(x, p(x)) = p(x)^{\alpha_1} f_1(x, p(x)) \quad \Rightarrow \quad V(f(x, p(x))) \leq V(f_1(x, p(x)))$.

Thus, we conclude that $V(f(x,p(x))) \leq -2 + 2(t_1 + \ldots + t_n) = 2t - 2$. □

Now we have all the tools needed to give a proof of the Theorem 2.3.1 stated in the Introduction:

Proof. If $a = 0$ or $b = 0$, then $g \in \mathbb{R}[x]$ is a polynomial with at most t non-zero terms. Descartes' rule of signs implies that, either $g \equiv 0$ or g has at most $2t - 1 \leq 6t - 4$ real roots (counted with multiplicities except for the possible root 0). In the case $a \neq 0$ and $b \neq 0$, the real roots of $f(x, ax + b)$ correspond one to one to the roots of $f(bx/a, b(x + 1)) = \widehat{f}(x, x + 1)$, where $\widehat{f} = \sum_{i=1}^{t} a_i a^{-\alpha_i} b^{\alpha_i+\beta_i} x^{\alpha_i} y^{\beta_i}$. Since this bijection preserves the multiplicity of the roots and maps the possible roots 0 and $-b/a$ of g to the roots 0 and -1 of $\widehat{f}(x, x + 1)$, we only need to consider the case $a = b = 1$, i.e. $g = f(x, x + 1)$. Suppose that $g \not\equiv 0$. Descartes' rule of signs and Proposition 6.1.4 imply that the number of positive roots of g counted with multiplicities is at most $2t - 2$. On the other hand, the roots of g in $(-\infty, -1)$ correspond to the positive roots of $0 \not\equiv g(-1-x) = f(-1-x, -x) = f_1(x, x+1)$, where $f_1 = \sum_{i=1}^{t} a_i (-1)^{\alpha_i+\beta_i} x^{\beta_i} y^{\alpha_i}$. Therefore the number of roots (with multiplicities) of g in $(-\infty, -1)$ is also bounded by $2t - 2$. Finally, the roots of g in $(-1, 0)$ correspond to the positives roots of

$$0 \not\equiv (x+1)^{\deg(g)} g\left(\frac{-x}{x+1}\right) = (x+1)^{\deg(g)} f\left(\frac{-x}{x+1}, \frac{1}{x+1}\right) = f_2(x, x+1)$$

where $f_2 = \sum_{i=1}^{t} a_i (-1)^{\alpha_i} x^{\alpha_i} y^{\deg(g)-\alpha_i-\beta_i}$. Therefore there are at most $2t - 2$ of such roots. Taking into account the possible roots 0 and -1, counted each one at most once, we conclude that g has at most $6t - 4$ real roots. □

6.2 Linear factors of a bivariate polynomial

Proposition 6.2.1. *Let $f = \sum_{i=1}^{t} a_i x^{\alpha_i} y^{\beta_i} \in \mathbb{R}[x, y]$. Let $a, b \in \mathbb{R}$ such that $b \neq |1 - a|$. Then $y - ax - b \,|\, f \;\Leftrightarrow\; x^n - ax - b \,|\, f(x, x^n)$ for at least $6t - 3$ odd integers $n \geq 3$.*

Proof. ($\Leftarrow$) : Suppose that $3 \leq n_1 < n_2 < \cdots < n_{6t-3}$ are $6t - 3$ odd numbers such that $x^n - ax - b \,|\, f(x, x^n)$. Let $w_i \in \mathbb{R}$ be a root of $x^{n_i} - ax - b$ for each $1 \leq i \leq 6t - 3$. Then $f(w_i, aw_i + b) = f(w_i, w_i^{n_i}) = 0$ for all $1 \leq i \leq 6t - 3$. This means that $f(x, ax + b)$ has at least $6t - 3$ real roots. Applying Theorem 2.3.1 we conclude that $f(x, ax + b) \equiv 0$, or simply $y - ax - b \,|\, f$. It only remains to proof that $w_i \neq w_j$ for all $i \neq j$. Actually, if $x^{n_i} - ax - b$ and $x^{n_j} - ax - b$ had a common root $w = w_i = w_j \in \mathbb{R}$, then $w^{n_i - n_j} = 1$ and therefore $w = \pm 1$. This would imply that $0 = w^{n_i} - aw - b = -b \pm (1 - a)$, in contradiction with the hypothesis $b \neq |1 - a|$. □

Corollary 6.2.2. *If $f \in \mathbb{R}[x, y]$ has t non-zero terms, then there is and odd integer $3 \leq n \leq 12t - 5$ such that $f(x, x^n) \neq 0$.*

Proof. Otherwise, by Proposition 6.2.1 (there are exactly $6t - 3$ odd integers between 3 and $12t - 5$), every polynomial $y - ax - b \in \mathbb{R}[x, y]$ with $b \neq |1 - a|$ would divide f. □

Note that if $(a, b) \neq (0, 1)$, then either $b \neq |1 - a|$ or $b \neq |1 + a|$.

Input: A lacunary polynomial $f = \sum_{i=1}^{t} a_i x^{\alpha_i} y^{\beta_i} \in K[x, y]$ with t terms, encoded as a list of vectors $(a_i, \alpha_i, \beta_i) \in K \times \mathbb{N}_0 \times \mathbb{N}_0$ representing the monomials of f, and two numbers $a, b \in K$.
Output: **TRUE** or **FALSE** depending whether $y - ax - b \,|\, f(x, y)$ or not.

1: **if** $(a, b) = (0, 1)$ **then**
2: **return** $f(x, 1) = 0$
3: **end if**
4: **if** $b = |1 - a|$ **then**
5: $f \leftarrow f(-x, y)$
6: $a \leftarrow -a$
7: **end if**
8: **for all** $n = 3, 5, \ldots, 12t - 5$ **do**
9: **if** $f(x, x^n) \neq 0$ **then**
10: $A \leftarrow \text{DenseFactor}(x^n - ax - b)$ /* Irreducible factors (with multiplicities) of $x^n - ax - b$ in $K[x]$ */
11: $B \leftarrow \text{LacunFactor}(f(x, x^n), n)$ /* Irreducible factors (with multiplicities) of $f(x, x^n)$ in $K[x]$ of degree $\leq n$ */
12: **if** $A \not\subseteq B$ **then**
13: **return FALSE**
14: **end if**
15: **end if**
16: **end for**
17: **return TRUE**

Algorithm 4: Test if $y - ax - b$ divides a lacunary polynomial $f(x, y)$ in $\mathbb{R}[x, y]$

The correctness of the algorithm is a consequence of Proposition 6.2.1. In order to estimate its complexity, we first state the following two famous results on the factorization of polynomials of univariate polynomials.

Dense Factorization Given $f \in K[x]$ of degree d and absolute height H, it is possible to compute all its irreducible factors in $K[x]$ with multiplicities in $(d\,[K : \mathbb{Q}] \log H)^{O(1)}$ bit operations (see [LLL82] for the rational case and [Lan85] for the general case).

Lacunary Factorization Given $f \in K[x]$ a lacunary polynomial of degree d, with at most t monomials and absolute height H, it is possible to find all its irreducible factors (with multiplicities) in $K[x]$ of degree bounded by s in $(t\,s\,[K : \mathbb{Q}] \log d \log H)^{O(1)}$ bit operations (see [Len99b]).

The complexity of the algorithm is clearly dominated by its main loop (steps 8–16), where it performs $6t - 3$ calls to the dense and lacunary factorization algorithms in order to factorize $x^n - ax - b$ completely and find all the factors of degree bounded by n of $f(x, x^n)$. We

have that $\deg(x^n - ax - b) = n \leq 12t - 5$ and $H(x^n - ax - b) \leq H(a)H(b)$, therefore the step 10 requires at most $((6t-3)\,(12t-5)\,[K:\mathbb{Q}]\,\log(H(a)\,H(b)))^{O(1)}$ bit operations. On the other hand, we have that $f(x, x^n)$ is a lacunary polynomial with at most t non-zero terms, of degree bounded by $nd \leq (12t-5)d$ and absolute height bounded by $(2H(f))^t$ because the coefficients of $f(x, x^n)$ are sums of at most t coefficients of f. Thus, step 11 requires no more than $\big((6t-3)\,t\,(12t-5)[K:\mathbb{Q}]\,\log(d(12t-5))\,\log(2H(f))^t\big)^{O(1)}$ bit operations. This proves that the total number of bit operations performed by the algorithm is polynomial in t, $\log(d)$, $[K:\mathbb{Q}]$ and $\log(H(a)H(b)H(f))$.

List of Algorithms

Bibliography

[Ave08] M. Avendaño, *The number of roots of a bivariate polynomial on a line.* Accepted for publication in J. Symb. Comput. (2008). Preliminary version in Effective Methods in Algebraic Geometry Digital Proceedings (2007).

[AKP06] M. Avendaño, T. Krick, A. Pacetti, *Newton-Hensel interpolation lifting.* Found. Comp. Math. **6(1)** Special Vol. dedicated to Steve Smale on his 75th birthday (2006), 81–120.

[AKS07] M. Avendaño, T. Krick, M. Sombra, *Factoring bivariate sparse (lacunary) polynomials.* Journal of Complexity **23** (2007), 193–216.

[AmDa00] F. Amoroso, S. David, *Minoration de la hauteur normalisée des hypersurfaces.* Acta Arith. **92** (2000), 339–366.

[BBS07] D.J. Bates, F. Bihan, F. Sottile, *Bounds on the number of real solutions to polynomial equations.* IMRN, to appear.

[BeTi88] M. Ben-Or, P. Tiwari, *A deterministic algorithm for sparse multivariate polynomial interpolation. Extended abstract.* STOC (1988) 301–309.

[Ber70] E.R. Berlekamp, *Factoring polynomials over large finite fields.* Math. Comp. **24** (1970), 713–735.

[BHKS05] K. Belabas, M. van Hoeij, J. Klüners, A. Steel, *Factoring polynomials over global fields.* Preprint (2005).

[BiSo06] F. Bihan, F. Sottile, *New fewnomial upper bounds from Gale dual polynomial systems.* Moscow Mathematics Journal **7(3)** (2007), 387–407.

[BoTi91] A. Borodin, P. Tiwari, *On the decidability of sparse univariate polynomial interpolation.* Comput. Complexity **1** (1991) 67–90. STOC (1988), 301–309.

[Chi84] A. Chistov, *Factoring polynomials over a finite field and solution of systems of algebraic equations.* (Russian. English summary.) Theory of the complexity of computations, II. Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984) 124–188.

[ChGr82] A. Chistov, D. Grigoriev, *Polynomial time factoring of the multivariate polynomials over a global field.* Preprint LOMI E-5-82 (1982) 39 p.

[CDGK91] M. Clausen, A. Dress, J. Grabmeier, M. Karpinski, *On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields.* Theoretical Computer Science **84** (1991), 151–164.

[CKS99] F. Cucker, P. Koiran, S. Smale, *A polynomial time algorithm for Diophantine equations in one variable.* J. Symbolic Comput. **27** (1999), 21–29.

[Dob79] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial.* Acta Arith. **34** (1979), 391–401.

[DrGr91] A. Dress, J. Grabmeier, *The interpolation problem for k-sparse polynomials and character sums.* Adv. in Appl. Math. **12** (1991), 57–75.

[GaKa85] J. von Zur Gathen, E. Kaltofen, *Factoring sparse multivariate polynomials.* Journal of Computer and System Sciences **31(2)** (1985), 265–287

[Gri84] D. Grigoriev, *Factoring polynomials over a finite field and solution of systems of algebraic equations.* (Russian. English summary.) Theory of the complexity of computations, II. Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984) 20–79.

[GKS90] D. Grigoriev, M. Karpinski, M. Singer, *Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields.* Siam J. Comput. Vol. **19(6)** (1990), 1059–1063.

[GKS91] D. Grigoriev, M. Karpinski, M. Singer, *The interpolation problem for k-sparse sums of eigenfunctions of operators.* Adv. in Appl. Math. **12** (1991), 76–81.

[GKS94] D. Grigoriev, M. Karpinski, M. Singer, *Computational complexity of sparse rational function interpolation.* SIAM J. Comput. **23** (1995), 1–11.

[Haa02] B. Haas, *A simple counter-example to Koushnirenko's conjecture.* Beiträge zur Algebra und Geometrie **43(1)** (2002), 1–8.

[Hoe02] M. van Hoeij, *Factoring polynomials and the knapsack problem.* Journal of Number Theory **95** (2002), 167–189.

[Kal85] E. Kaltofen, *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization.* SIAM J. Comput. **14** (1985), 469–489.

[KaKo05] E. Kaltofen, P. Koiran, *On the complexity of factoring bivariate supersparse (lacunary) polynomials.* ISSAC'05, Proc. 2005 Internat. Symp. Symbolic Algebraic Comput. (2005), 208–215.

[KaKo06] E. Kaltofen, P. Koiran, *Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields.* ISSAC'06, Proc. 2006 Internat. Symp. Symbolic Algebraic Comput. (2006), 162–168.

[KaLa88] E. Kaltofen, Y.N. Lakshman *Improved sparse multivariate polynomial interpolation algorithms.* ISSAC'88, Proc. 1988 Internat. Symp. Symbolic Algebraic Comput., Lecture Notes in Comput. Sci **358**, Springer-Verlag, New York (1988), 467–474.

[KLW90] E. Kaltofen, Y.N. Lakshman, J.-M. Wiley, *Modular rational sparse multivariate polynomial interpolation.* ISSAC'90, Proc. 1990 Internat. Symp. Symbolic Algebraic Comput. (S. Watanabe and M. Nagata, eds.), ACM Press, New York (1990), 135–139.

[KaLe03] E. Kaltofen, W.-s Lee, *Early termination in sparse interpolation algorithms.* J. Symbolic Computation **36(3-4)** (2003), 365–400.

[KLL00] E. Kaltofen, A. Lobo, W.-s Lee, *Early termination in Ben-Or/Tiwari sparse interpolation and a hybrid of Zippel's algorithm.* ISSAC'00, Proc. 2000 Internat. Symp. Symbolic Algebraic Comput. (C. Travero, ed.), ACM Press, New York (2000), 192–201.

[Kho91] A. Khovanskii, *Fewnomials.* AMS press, Providence, Rhode Island (1991).

[Lan85] S. Landau, *Factoring polynomials over algebraic number fields.* SIAM J. Comput. **14** (1985), 184–195.

[Lan93] S. Lang, *Algebra.* Addison Wesley (1993).

[Lec05] G. Lecerf, *Improved dense multivariate polynomial factorization algorithms.* To appear in J. Symb. Comput.

[Lee01] W.-s. Lee, *Early Termination Strategies in Sparse Interpolation Algorithms.* Ph.D. Dissertation, North Carolina State University (2001).

[Len84] A.K. Lenstra, *Factoring multivariate integral polynomials.* Theoret. Comput. Sci. **34** (1984), 207–213.

[Len87] A.K. Lenstra, *Factoring multivariate polynomials over algebraic number fields.* SIAM J. Comput. **16** (1987), 591–598.

[Len99a] H.W. Lenstra Jr., *On the factorization of lacunary polynomials.* Number theory in progress **1** (1999), 277–291.

[Len99b] H.W. Lenstra Jr., *Finding small degree factors of lacunary polynomials.* Number theory in progress **1** (1999), 267–276.

[LLL82] A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, *Factoring polynomials with rational coefficients.* Math. Ann. **261** (1982), 515–534.

[LRW03] T.Y. Li, J.M. Rojas, X. Wang, *Counting real connected components of trinomial curves intersections and m-nomial hypersurfaces.* Discrete and computational geometry **30(3)** (2003), 379–414.

[Pan01] V. Pan, *Structured matrices and polynomials. Unified superfast algorithms.* Birkhuser Boston, Inc., Boston, MA; Springer-Verlag, New York, 2001.

[Per05] D. Perruci, *Some bounds for the number of connected components of real zero sets of sparse polynomials.* Discrete and computational geometry **34(3)** (2005), 475–495.

[Pon05] M. Corentin Pontreau, *Minoration de la hauteur normalisée en petite codimension.* Université de Caen, Doctoral Thesis (2005).

[Vou96] P. Voutier, *An effective lower bound for the height of algebraic numbers.* Acta Arith. **74** (1996), 81–95.

[Zas69] H.Zassenhaus, *On Hensel Factorization I.* J. Number Theory **1** (1969), 291–311.

[Zha95a] S. Zhang, *Positive line bundles on arithmetic varieties.* J. Amer. Math. Soc. **8** (1995), 187–221.

[Zha95b] S. Zhang, *Small points and adelic metrics.* J. Algebraic Geom. **4** (1995), 281–300.

[Zip90] R. Zippel, *Interpolating polynomials from their values.* J. Symbolic Computation **9** (1990), 375–403.