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

Sobre la complejidad de la resolución de sistemas de ecuaciones polinomiales y de la interpolación polinomial multivariada

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

Nardo Giménez

Directores: Guillermo Matera y Pablo Solernó
Consejero de estudios: Pablo Solernó

Lugar de trabajo: Universidad Nacional de General Sarmiento. Instituto del Desarrollo Humano.

Buenos Aires, 2017

Sobre la complejidad de la resolución de sistemas de ecuaciones polinomiales y de la interpolación polinomial multivariada

Resumen

La resolución de sistemas de ecuaciones polinomiales y la interpolación polinomial multivariada se analizan desde el punto de vista algorítmico y de la complejidad computacional.

Desde el punto de vista algorítmico se exhibe un algoritmo probabilístico que resuelve un sistema polinomial cuya complejidad bit es esencialmente cuadrática en el número de Bézout del sistema y lineal en su talla bit. Este algoritmo resuelve el sistema de entrada módulo un número primo p y aplica levantamiento p–ádico. Para esto, se establecen una serie de resultados sobre la longitud bit de un primo "lucky" p, es decir un primo para el cual la reducción del sistema de entrada módulo p preserva ciertas propiedades geométricas y algebraicas fundamentales del sistema original. Luego este algoritmo se aplica al problema de la interpolación polinomial cuando el conjunto de nodos está dado como el conjunto de ceros de un sistema polinomial, dando como resultado un procedimiento que calcula intepolantes de "bajo grado". La complejidad bit de estos algoritmos es similar a la de los algoritmos que usan bases de Gröbner o H–bases en el peor caso y en ciertos casos de interés práctico puede resultar considerablemente menor.

Desde el punto de vista de la complejidad computacional se demuestran cotas inferiores para la complejidad de los problemas de interpolación polinomial. Se introduce un nuevo modelo computacional para la interpolación de Hermite–Lagrange que incluye clases no lineales de interpolantes. Este modelo incluye fenómenos de coalescencia y captura una gran variedad de conocidos problemas y algoritmos de interpolación. En este contexto, se exhiben ejemplos de problemas de interpolación con clases no lineales de interpolantes cuya complejidad es intrínsecamente exponencial, mostrando que nuestro algoritmo para interpolación polinomial multivariada es esencialmente asintóticamente óptimo para los problemas seleccionados y que nada se gana admitiendo no linealidad.

Palabras clave Resolución de sistemas polinomiales sobre $\mathbb{Q}$; complejidad bit; sucesión regular reducida; forma de Chow; fibras de levantamiento; levantamiento de Hensel; primos "lucky"; interpolación de Hermite–Lagrange; problema de interpolación; algoritmo de interpolación; complejidad computacional; cota inferior de complejidad; aplicación construible; aplicación racional; aplicación topológicamente robusta; aplicación geométricamente robusta.

On the complexity of polynomial system solving and multivariate polynomial interpolation

Abstract

Polynomial system solving and multivariate polynomial interpolation over the rationals are considered from both the algorithmic and computational point of view.

From the algorithmic point of view a probabilistic algorithm is developed which solves a polynomial system whose bit complexity is roughly quadratic in the Bézout number of the system and linear in its bit size. Our algorithm solves the input system modulo a prime number p and applies p–adic lifting. For this purpose, we establish a number of results on the bit length of a "lucky" prime p, namely one for which the reduction of the input system modulo p preserves certain fundamental geometric and algebraic properties of the original system. Then this algorithm is applied to polynomial interpolation when the set of nodes is given as the set of zeros of a polynomial system, yielding a procedure which computes "low degree" interpolants. The bit complexity of these algorithms is similar to that of the algorithms that use Gröbner or H–bases in the worst case, and in certain cases of particular interest can be significantly lower.

From the computational complexity point of view lower complexity bounds for the complexity of interpolation algorithms by polynomials are shown. A new computational model for Hermite–Lagrange interpolation with nonlinear classes of interpolants is introduced, which includes coalescence phenomena and captures a large variety of known Hermite–Lagrange interpolation problems and algorithms. In this context examples of interpolation problems are exhibited with nonlinear classes of interpolants whose complexity is intrinsically exponential, showing that our algorithm for multivariate polynomial interpolation is essentially asymptotically optimal for the problems under consideration and that nothing is gained by admitting nonlinearity.

Key words Polynomial system solving over $\mathbb{Q}$; bit complexity; reduced regular sequence; Chow form; lifting fibers; Hensel lifting; lucky primes; Hermite–Lagrange interpolation; interpolation problem; interpolation algorithm; computational complexity; lower complexity bound; constructible map; rational map; topologically robust map; geometrically robust map.

Agradecimientos

Deseo expresar mi mayor agradecimiento a Guillermo Matera, Pablo Solernó y a Joos Heintz por la dedicación y el entusiasmo demostrados durante el desarrollo de este trabajo.

A mis padres Guillermo y Alfreda y a mi hermano Julián por su apoyo siempre incondicional.

A mis amigos, Jorge Flolasco, Antonio Cafure, Eda Cesaratto, Ezequiel Dratman, Mariana Pérez, Melina Privitelli, que de distintas maneras también estuvieron presentes.

Finalmente, a mi esposa Cecilia, que con amorosa paciencia siempre estuvo a mi lado en estos años de trabajo y a quien dedico esta tesis.

Índice general

Capítulo 1

Introducción

En este trabajo de tesis se consideran dos problemas centrales de la geometría algebraica computacional: la resolución de sistemas de ecuaciones polinomiales y la interpolación polinomial multivariada.

Más precisamente el trabajo se focaliza en el costo binario de la resolución de sistemas polinomiales y de la interpolación polinomial. En relación con el primer problema, se determina una cota superior sobre el costo binario de una clase de algoritmos à la Kronecker para intersecciones completas definidas sobre $\mathbb{Q}$. La cantidad de operaciones aritméticas en $\mathbb{Q}$ que realizan este tipo de algoritmos es esencialmente polinomial (más precisamente, cuadrática) en un invariante denominado el "grado del sistema", que se acota superiormente por el número de Bezout del mismo. Sin embargo el costo binario podría ser mucho mayor, debido al eventual crecimiento de los enteros que aparecen en los cálculos intermedios. Para evitar este fenómeno, siguiendo una sugerencia de [GLS01], en esta tesis se desarrolla una versión modular de estos algoritmos que consiste en realizar los cálculos módulo un primo p "lucky", a fin de obtener la salida mediante un proceso de levantamiento p–ádico. Un aspecto crucial de este enfoque reside en la determinación de un primo p lucky para obtener una "buena" reducción modular. Esto implica que ciertas características geométricas y algebraicas, como la dimensión y el grado de la variedad de entrada, se preserven en la reducción módulo p. En este sentido se obtienen resultados sobre la longitud bit de un primo p lucky. De este modo se obtiene un algoritmo probabilístico, con probabilidad acotada a priori, que resuelve un sistema de ecuaciones polinomiales con coeficientes en racionales con un costo binario esencialmente cuadrático en el grado del sistema y lineal en el tamaño bit del mismo, mejorando significativamente los resultados de complejidad binaria conocidos.

Con respecto a la interpolación polinomial, se consideran dos problemas principales. En primer lugar, y de acuerdo con el paradigma del cálculo simbólico, se considera un problema de interpolación "implícita" en donde el conjunto (finito) de nodos de interpolación está descripto como el conjunto de soluciones de un sistema de ecuaciones polinomiales con coeficientes en $\mathbb{Q}$. A este conjunto de nodos asociamos un espacio de interpolantes que resulta unívocamente determinado por los polinomios de entrada y que se compone de polinomios de grado a lo sumo $n(d-1)$ donde d es una cota superior para los grados de los polinomios de entrada y n es

la cantidad de indeterminadas. Exhibimos un algoritmo que resuelve este problema de interpolación con un costo binario esencialmente cúbico en el grado del sistema de entrada y lineal en el tamaño bit del mismo, resultando una alternativa a los métodos que usan bases de Gröbner o H–bases.

Por último se considera la complejidad computacional de la interpolación polinomial multivariada. La salida de los algoritmos clásicos de interpolación polinomial es la representación densa o rala de los polinomios interpolantes, por lo que la dimensión (finita) del espacio de interpolantes en consideración resulta una cota inferior para la complejidad de estos procedimientos. En esta tesis se plantea la cuestión de la complejidad intrínseca de los algoritmos de interpolación que admiten representaciones más generales de los interpolantes, como por ejemplo su codificación por medio de esquemas de evaluación, lo que a su vez motiva la consideración de clases no lineales de interpolantes. Para responder a esta cuestión se describe un modelo general de problema y algoritmo de interpolación de "Hermite–Lagrange" mediante argumentos geométricos. Se introduce además una noción de robustez geométrica que permite capturar en el modelo fenómenos de coalescencia, incluyendo de este modo los algoritmos de interpolación multivariada usuales. Finalmente se presentan dos familias naturales de problemas de interpolación del tipo Hermite–Lagrange cuya complejidad, bajo la mencionada restricción de "robustez geométrica", es intrínseca alta, aún si se admiten técnicas de interpolación no lineales. En particular todo algoritmo geométricamente robusto que resuelve estos problemas de interpolación realiza una cantidad de operaciones ariméticas que es polinomial en el número de nodos en consideración, demostrando que nuestro algoritmo de interpolación implícita es esencialmente óptimo.

En las secciones siguientes se discuten en más detalle los resultados conocidos hasta el momento en relación con los problemas anteriores así como los resultados obtenidos en esta tesis. Salvo mención explícita de lo contrario, estos últimos son originales y se encuentran en los artículos [GHMS11] y [Gim14] ya publicados y en el artículo [GM16] en proceso de revisión.

1.1. Antecedentes

1.1.1. Resolución de sistemas de ecuaciones polinomiales

La resolución de sistemas polinomiales definidos sobre $\mathbb{Q}$ es una tarea fundamental de la geometría algebraica computacional, que ha sido el motivo de trabajo intensivo desde la década de 1970. Enfoques simbólicos a este problema incluyen bases de Gröbner, descomposición triangular, resultantes, matrices de Macaulay y algoritmos à la Kronecker (ver, por ejemplo, [Mor05] y [Mor15] para un repaso de los métodos existentes). La correspondiente **complejidad aritmética**, es decir el número de operaciones aritméticas en $\mathbb{Q}$ requerido por estos algoritmos, ha sido analizada en, por ejemplo, [Laz81], [Giu89], [DFGS91], [FGS95], [GHH$^+$97], [GLS01], [Lec03] y [DL08], entre otros. El paradigma de complejidad que surge de estos trabajos es que los sistemas polinomiales se pueden resolver con un número de operaciones aritméticas que es **polinomial** en el **número de Bézout** del sistema, esto es, en el producto

de los grados de los polinomios del sistema de entrada. Esta conclusión esencialmente coincide con las cotas inferiores de [CGH$^+$03], [GHMS11] y [BHM$^+$16], bajo la hipótesis de que los correspondientes algoritmos son "geométricamente robustos", es decir, son universales y permiten la resolución de ciertos problemas "límite".

Por otro lado, existen pocos resultados sobre el costo binario o **complejidad bit** de estos algoritmos. En relación con las bases de Gröbner, el trabajo [HL11] de Hashemi y Lazard muestra que, en el caso de dimensión cero, éstas pueden calcularse con un número de operaciones bit que es esencialmente polinomial en el tamaño binario de la entrada y D^n, donde n es la cantidad de indeterminadas y D es el promedio de los grados de los polinomios que definen el sistema de entrada.

En la presente tesis se analiza la complejidad bit una familia de algoritmos à la Kronecker, originalmente debidos a [GHH$^+$97] y [GHM$^+$98] y cuya versión más reciente es la de Giusti, Lecerf y Salvy [GLS01] (ver también [DL08]). Estos algoritmos suponen como hipótesis que los polinomios de entrada $F_1, \ldots, F_r \in \mathbb{Z}[X_1, \ldots, X_n]$ definen una **intersección completa**, es decir que el conjunto solución $\mathcal{V} \subset \mathbb{C}^n$ del sistema $F_1 = 0, \ldots, F_r = 0$ es una subvariedad afín de $\mathbb{C}^n$ de dimensión $n - r$ y el ideal $(F_1, \ldots, F_r)$ es radical. Otra hipótesis de estos algoritmos es que $F_1, \ldots, F_r$ forman una sucesión regular reducida, es decir que ningún F_s es divisor de cero en el anillo cociente $\mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_{s-1})$ y el ideal $(F_1, \ldots, F_s)$ es radical para $1 \leq s \leq r$. Esta condición implica que la subvariedad afín $\mathcal{V}_s$ de $\overline{\mathbb{K}}^n$ definida por $F_1, \ldots, F_s$ tiene dimensión $n - s$ para $1 \leq s \leq r$. Esta segunda hipótesis de regularidad y reducción no es realmente restrictiva ya que esta situación se puede obtener por medio de una combinación lineal genérica de los polinomios $F_1, \ldots, F_r$, como se demuestra en [KP94]. Los polinomios $F_1, \ldots, F_r$ se suponen representados por un *straight-line program*, que informalmente hablando es un esquema de computación de las operaciones aritméticas requeridas para evaluar los polinomios, y cuya longitud L se define como el número total de operaciones (ver el Capítulo 2 para las definiciones formales). Estos algoritmos entregan en la salida una adecuada "parametrización" de una **fibra finita** de $\mathcal{V}$, esto es, de la subvariedad cero–dimensional $\mathbb{Q}$–definible de $\mathbb{C}^n$ determinada por la intersección de $\mathcal{V}$ con una subvariedad lineal genérica de dimensión complementaria r. Más precisamente, esta parametrización está definida por una "solución geométrica" o "representación univariada" de la fibra. Una **representación univariada** de una subvariedad cero–dimensional $\mathbb{Q}$–definible $\mathcal{W}$ de $\mathbb{C}^n$ es una "parametrización" de la misma definida por una forma lineal $U \in \mathbb{Q}[X_1, \ldots, X_n]$ y polinomios univariados $Q, V_1, \ldots, V_n \in \mathbb{Q}[T]$, con Q libre de cuadrados, tales que U induce un isomorfismo entre $\mathcal{W}$ y el conjunto de ceros en $\mathbb{C}$ del polinomio $Q(T)$, y cuya inversa está dada por $(V_1(T), \ldots, V_n(T))$. Un parametrización alternativa también utilizada es la denominada **representación de Kronecker** de $\mathcal{W}$, en la que $V_1, \ldots, V_n$ se sustituyen por polinomios $W_1, \ldots, W_n \in \mathbb{Q}[T]$ tales que el morfismo inverso anterior está dado por la tupla de funciones racionales $\left(\frac{W_1(T)}{Q'(T)}, \ldots, \frac{W_n(T)}{Q'(T)}\right)$ (ver el Capítulo 2 para las definiciones precisas de solución geométrica y representación univariada). Estas formas de representación de una variedad se remontan a los trabajos de Kronecker [Kro82] y König [Kön03] (ver también [HP68a]) y varios trabajos muestran que éstas constituyen una buena representación de $\mathcal{V}$, es decir una "solución" del sistema $F_1 = 0, \ldots, F_r = 0$, tanto desde el punto de vista numérico

como simbólico (ver, por ejemplo, [HKP$^+$00], [Sch03], [Lec03], [CM06], [SW05]).

Supóngase que los polinomios de entrada $F_1, \ldots, F_r$ tienen grado a lo sumo d y están dados por un straight–line program de longitud a lo sumo L y parámetros enteros de longitud bit a lo sumo h. En [GHH$^+$97] y [HMPS00] se demuestra que en tal caso el sistema $F_1 = 0, \ldots, F_r = 0$ puede resolverse con un número de operaciones bit que es polinomial en $rdL\delta h$. Aquí δ es un invariante introducido por Giusti et al. [GHM$^+$98] denominado el **grado del sistema** y que se define como $\delta := \text{máx}_{1 \leq s \leq r} \deg \mathcal{V}_s$, donde $\deg \mathcal{V}_s$ es el grado de la subvariedad afín de $\mathbb{C}^n$ definida por $F_1, \ldots, F_s$ para $1 \leq s \leq r$.

Asimismo [GHH$^+$97] provee una cota inferior sobre el tamaño binario de la salida si se utilizan representaciones "estándar". Además, el trabajo reciente de Schost y Safey El Din [SS16] considera la complejidad bit de sistemas cero–dimensionales multi–homogéneos y demuestra que tales sistemas pueden resolverse con complejidad cuadrática en el número de Bézout multi–homogéneo y un correspondiente análogo aritmético de éste.

Por último, en [GLS01] se demuestra que la complejidad aritmética de los algoritmos à la Kronecker es cuadrática en grado del sistema.

Expresaremos las medidas de complejidad de los algoritmos en términos de la cantidad $\mathcal{U}(n) = n \log^2(n) \log\log(n)$.

Teorema 1.1.1. *([GLS01, Theorem 1]) Sea $\mathbb{K}$ un cuerpo de característica cero y $F_1, \ldots, F_n$ polinomios en $\mathbb{K}[X_1, \ldots, X_n]$ de grado a lo sumo d que definen una sucesión regular reducida y dados por un straight–line program de longitud a lo sumo L. Sea $\mathcal{V}_s$ la subvariedad afín de $\overline{\mathbb{K}}^n$ definida por $F_1, \ldots, F_s$ para $1 \leq s \leq n$ y sea $\mathcal{V} := \mathcal{V}_n$. Existe un algoritmo probabilístico que calcula una representación univariada de $\mathcal{V}$ con $\mathcal{O}\big(n(nL + n^4)(\mathcal{U}(d\delta))^2\big)$ operaciones aritméticas en $\mathbb{K}$, donde $\delta := \text{máx}_{1 \leq s \leq n-1} \deg \mathcal{V}_s$. Su probabilidad de éxito depende de elecciones de elementos de $\mathbb{K}$ fuera de ciertos subconjuntos algebraicos estrictos.*

No obstante, cuando $\mathbb{K} = \mathbb{Q}$ esta estimación no necesariamente refleja adecuadamente el costo binario del algoritmo, que podría ser mucho mayor, debido al eventual crecimiento de los enteros en los cálculos intermedios. Por tal motivo en [GLS01] se sugiere realizar todos los cálculos módulo un primo p "lucky", para luego obtener la salida por medio de un procedimiento de levantamiento p–ádico. En consecuencia, la determinación de un primo p con "buena" reducción modular es crucial para poder estimar la complejidad bit del procedimiento.

1.1.2. Interpolación implícita

El problema de interpolación implícita puede tratarse por medio de bases de Gröbner y H-bases como se describe por ejemplo en [MS00a] y [Sau01] (ver también [MMM91], [MMM93], [MS00a], [GS00b]). En lo que respecta al conocimiento del autor de esta tesis, la cota de complejidad más fina para bases de Gröbner cero–dimensionales es la del trabajo [HL11] citado anteriormente. Supongamos que tenemos $r = n$ polinomios de entrada $F_1, \ldots, F_n$ que definen una sucesión regular reducida. En la Sección 8.3.1 mostramos que el cálculo de una base de Gröbner

del ideal $(F_1, \ldots, F_n)$ por medio del procedimiento descripto en [HL11] requiere $\mathcal{O}(n^3(3d)^n)$ operaciones aritméticas en $\mathbb{Q}$.

En el caso especial que las partes homogéneas de grado máximo de los polinomios $F_1, \ldots, F_n$ tengan solo el punto $(0, \ldots, 0)$ como cero común, los mismos polinomios $F_1, \ldots, F_n$ ya forman una H–base [MS00a]. Por otra parte, algunos de los procedimientos existentes para construir H–bases de ideales arbitrarios se basan en el cálculo de una base de Gröbner (con respecto a un orden monomial compatible con el grado) o bien implican el cálculo de una base de Gröbner del ideal dado como resultado derivado [AL94] (ver también [Buc85]). En consecuencia, el costo de aplicar estos procedimientos a nuestro problema es al menos el mencionado más arriba. Un enfoque más directo para construir H–bases que no se basa en ordenes monomiales se discute en [MS00b], [Sau01] y [PS07]. Una adaptación de este procedimiento al caso cero–dimensional se describe en [MS00b], pero sin enunciar su complejidad. Consecuentemente, en la Sección 8.3.1 discutimos la complejidad de este procedimiento, que es de $d^{\mathcal{O}(n^2)}$ operaciones aritméticas en $\mathbb{Q}$.

1.2. Resultados obtenidos y organización del trabajo

1.2.1. Resolución de sistemas polinomiales

Desarrollamos un algoritmo probabilístico à la Kronecker para intersecciones completas definidas sobre $\mathbb{Q}$ cuya complejidad bit es esencialmente cuadrática en el número de Bézout del sistema de entrada y lineal en su tamaño bit. Para esto, seguimos la sugerencia de [GLS01] antes mencionada, que consiste en realizar los cálculos módulo un primo p para luego recuperar los enteros de la salida por medio de un procedimiento de levantamiento p–ádico.

Sean $F_1, \ldots, F_r \in \mathbb{Z}[X_1, \ldots, X_n]$ polinomios que forman una sucesión regular reducida. Denotemos por $\mathcal{V}_s$ la subvariedad afín de $\mathbb{C}^n$ definida por los polinomios $F_1, \ldots, F_s$ y por $\delta_s := \deg \mathcal{V}_s$ su grado para $1 \leq s \leq r$. Sea $\mathcal{V} := \mathcal{V}_r$ y $\delta := \max_{1 \leq s \leq r} \delta_s$ el grado del sistema definido por $F_1, \ldots, F_r$. El algoritmo entrega en la salida una representación de Kronecker de una "fibra de levantamiento" de $\mathcal{V}$, esto es una fibra (cero–dimensional) definida sobre $\mathbb{Q}$ de una proyección lineal genérica $\pi : \mathcal{V} \to \mathbb{C}^{n-r}$ definida sobre $\mathbb{Q}$.

El cálculo de la representación de Kronecker de tal fibra de levantamiento procede en r etapas. En la etapa s–ésima calculamos una representación de Kronecker de una fibra de levantamiento de $\mathcal{V}_{s+1}$ a partir de una de $\mathcal{V}_s$. Para nuestros propósitos, la reducción modular definida por un primo p es "buena", y el correspondiente primo p es "lucky", si características geométricas y algebraicas básicas de la variedad $\mathcal{V}_s$ y su ideal de definición $(F_1, \ldots, F_s)$ se preservan bajo la reducción modular para $1 \leq s \leq r$. Entre otras, podemos mencionar la dimensión, el grado y la suavidad genérica. Además, nuestro algoritmo también requiere que la reducción modular de las fibras de levantamiento en consideración preserve dimensión, grado y no ramificación. Resultados parciales en esta dirección han sido obtenidos en [Sch00] (ver

también [MS16]), sobre la reducción modular de fibras suaves de familias paramétricas de variedades cero–dimensionales, y en [DOSS15], sobre la reducción modular de variedades cero–dimensionales definidas sobre $\mathbb{Z}$. Desafortunadamente, estos resultados no son suficientes para nuestros propósitos.

Para el análisis de la longitud bit de primos lucky, establecemos condiciones sobre los coeficientes de formas lineales que definen una proyección $\pi_s : \mathcal{V}_s \to \mathbb{C}^{n-s}$, y las coordenadas de un punto $\boldsymbol{p} \in \mathbb{C}^{n-s}$, que implican que π_s es "genérica" en el sentido arriba mencionado y que $\boldsymbol{p}$ es un "punto de levantamiento", esto es, define una fibra de levantamiento, para $1 \leq s \leq r$. Como necesitamos analizar tanto las condiciones para proyecciones y fibras definidas sobre $\mathbb{Z}$ como para sus reducciones modulares, un contexto natural para este análisis es el de una variedad afín definida sobre un cuerpo perfecto, infinito $\mathbb{K}$. El resultado principal que obtenemos en este contexto general es el siguiente (ver la Proposición 3.1.1 y el Teorema 4.2.5).

Teorema 1.2.1. *Sea $\mathbb{K}$ un cuerpo perfecto, infinito y $V \subset \overline{\mathbb{K}}^n$ una variedad intersección completa definida sobre $\mathbb{K}$ de dimensión $n-s$ y grado δ_s. Sean Λ_{ij} $(1 \leq i \leq n-s+1, 1 \leq j \leq n)$ y $Z_1, \ldots, Z_{n-s}$ indeterminadas sobre $\mathbb{K}[V]$. Notemos $\boldsymbol{Z} := (Z_1, \ldots, Z_{n-s})$, $\boldsymbol{\Lambda} := (\Lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n}$, $\boldsymbol{\Lambda}^* := (\Lambda_{ij})_{1 \leq i \leq n-s, 1 \leq j \leq n}$ y $\boldsymbol{\Lambda}_i := (\Lambda_{i1}, \ldots, \Lambda_{in})$ para $1 \leq i \leq n-s+1$. Existen polinomios $A_V \in \mathbb{K}[\boldsymbol{\Lambda}^*]$ y $\rho_V \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$, con $\deg_{\boldsymbol{\Lambda}_i} A_V = \delta_s$ $(1 \leq i \leq n-s)$, $\deg_{\boldsymbol{\Lambda}_i} \rho_V \leq \delta_s(2\delta_s - 1)$ $(1 \leq i \leq n-s+1)$, $\deg_{\boldsymbol{Z}} \rho_V \leq \delta_s(2\delta_s - 1)$, y tales que satisfacen las siguientes propiedades: para todo $\boldsymbol{\lambda} \in \mathbb{K}^{(n-s+1)n}$ y $\boldsymbol{p} \in \mathbb{K}^{n-s}$ con $A_V(\boldsymbol{\lambda}^*)\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$, si $(Y_1, \ldots, Y_{n-s+1}) := \boldsymbol{\lambda}\boldsymbol{X}$ (donde $\boldsymbol{X} := (X_1, \ldots, X_n)$), entonces*

1. *la aplicación $\pi : V \to \mathbb{A}^{n-s}$ definida por $\boldsymbol{Y} := (Y_1, \ldots, Y_{n-s})$ es un morfismo finito;*
2. *Y_{n-s+1} induce un elemento primitivo de la extensión de anillos $\mathbb{K}[\boldsymbol{Y}] \hookrightarrow \mathbb{K}[V]$;*
3. *$\operatorname{rank}_{\mathbb{K}[\boldsymbol{Y}]} \mathbb{K}[V] = \delta_s$;*
4. *$\boldsymbol{p}$ es un punto de levantamiento de π e Y_{n-s+1} induce un elemento primitivo de $\pi^{-1}(\boldsymbol{p})$.*

La principal herramienta técnica que utilizamos para obtener el resultado anterior es el análisis de la forma de Chow de V. Un análisis similar se obtiene en [CM06] bajo hipótesis más fuertes, a saber que $\mathbb{K}$ sea un cuerpo finito $\mathbb{F}_q$ y V una intersección completa absolutamente irreducible.

Luego comparamos las condiciones que subyacen al Teorema 1.2.1 para $\mathbb{K} = \mathbb{Q}$ y $\mathbb{K} = \overline{\mathbb{F}}_p$, donde $\mathbb{F}_p$ es un cuerpo primo. Esto proporciona un múltiplo entero $\mathfrak{N}$ de todos los primos p que no son lucky en el sentido arriba mencionado. Obtenemos una cota superior para la longitud bit de este entero $\mathfrak{N}$ usando las estimaciones de alturas de variedades equidimensionales de [DKS13]. A partir de esta cota y resultados conocidos sobre la existencia de primos que no dividen un entero dado (ver el Lema 2.2.2) podemos obtener un primo lucky p de "baja" longitud bit. El siguiente enunciado resume los resultados obtenidos en esta tesis sobre reducción modular (ver los Teoremas 5.3.1 y 6.3.5). Utilizamos la notación Soft-Oh $\mathcal{O}^{\sim}$ estándar que omite términos logarítmicos.

Teorema 1.2.2. *Sean $F_1, \ldots, F_r \in \mathbb{Z}[X_1, \ldots, X_n]$ polinomios de grado a lo sumo d con coeficientes de longitud bit a lo sumo h. Supóngase que $F_1, \ldots, F_r$ forman una sucesión regular reducida y denótese $\mathcal{V}_s := \mathcal{V}(F_1, \ldots, F_s) \subset \mathbb{C}^n$ y $\delta_s := \deg \mathcal{V}_s$ para $1 \leq s \leq r$. Sea $\delta := \max_{1 \leq s \leq r} \delta_s$. Sean $\boldsymbol{\lambda} \in \mathbb{Z}^{n^2} \setminus \{0\}$ y $\boldsymbol{p} := (p_1, \ldots, p_{n-1}) \in \mathbb{Z}^{n-1}$ elementos elegidos aleatoriamente con entradas de longitud bit $\mathcal{O}^{\sim}\big(\log(nd^r)\big)$. Sean $(Y_1, \ldots, Y_n) := \boldsymbol{\lambda} \boldsymbol{X}$ y $\boldsymbol{p}^s := (p_1, \ldots, p_{n-s})$ para $1 \leq s \leq r$.*

Sea p un primo aleatorio de longitud bit $\mathcal{O}^{\sim}\big(\log(nd^r h)\big)$. Denótese por $F_{1,p}, \ldots, F_{r,p}$, $Y_{1,p}, \ldots, Y_{n,p}$ y $\boldsymbol{p}_p$ las correspondientes reducciones módulo p. Entonces las siguientes condiciones se satisfacen para $1 \leq s \leq r$ con probabilidad al menos $2/3$:

1. *los polinomios $F_{1,p}, \ldots, F_{s,p}$ generan un ideal radical en $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ y definen una variedad equidimensional $\mathcal{V}_{s,p} \subset \overline{\mathbb{F}}_p^n$ de dimensión $n - s$ y grado δ_s;*

2. *la aplicación $\pi_{s,p} : \mathcal{V}_{s,p} \to \overline{\mathbb{F}}_p^{n-s}$ definida por $Y_{1,p}, \ldots, Y_{n-s,p}$ es un morfismo finito, $\boldsymbol{p}_p^s \in \mathbb{F}_p^{n-s}$ es un punto de levantamiento de $\pi_{s,p}$, e $Y_{n-s+1,p}$ induce un elemento primitivo de $\pi_{s,p}^{-1}(\boldsymbol{p}_p^s)$;*

3. *todo $\boldsymbol{q} \in \pi_{s,p}\big(\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^{s+1})\big)$ es un punto de levantamiento de $\pi_{s,p}$ e $Y_{n-s+1,p}$ induce un elemento primitivo de $\pi_{s,p}^{-1}(\boldsymbol{q})$.*

Se observa que el análisis de los primos lucky resulta mucho más simple si sólo se requieren las condiciones (1) y (2). Un análisis en esta línea se puede deducir de [Sch00] (compárese con [MS16]). Sin embargo, la condición (3), que es crítica para demostrar la correctitud de nuestro algoritmo para resolver el sistema $F_1 = 0, \ldots, F_r = 0$, requiere una extensión significativa de estas técnicas.

Finalmente, se combina el algoritmo de [CM06] con levantamiento p–ádico, como en [GLS01], para obtener un algoritmo que resuelve el sistema $F_1 = 0, \ldots, F_r = 0$ con buena complejidad bit. Se demuestra el siguiente resultado (ver los Teoremas 7.3.1 y 7.3.2 para enunciados precisos), que mejora significativamente los resultados de [GHH$^+$97] y [HMPS00].

Teorema 1.2.3. *Sean $F_1, \ldots, F_r$ polinomios de $\mathbb{Z}[X_1, \ldots, X_n]$ como en el Teorema 1.2.2. Existe un algoritmo probabilístico que toma como entrada un straight–line program de longitud a lo sumo L que representa $F_1, \ldots, F_r$, y entrega como salida una representación de Kronecker de una fibra de levantamiento de $\mathcal{V}(F_1, \ldots, F_r)$ con $\mathcal{O}^{\sim}\big(n^{\mathcal{O}(1)} L\delta(d\delta + d^r h)\big)$ operaciones bit. En los mismos términos, el cálculo de una representación univariada de una fibra de levantamiento de $\mathcal{V}(F_1, \ldots, F_r)$ requiere $\mathcal{O}^{\sim}\big(n^{\mathcal{O}(1)} L\delta(d\delta + d^{2r} h)\big)$ operaciones bit.*

1.2.2. Interpolación implícita

Sean $F_1, \ldots, F_n \in \mathbb{Z}[X_1, \ldots, X_n]$ polinomios que definen una subvariedad cero–dimensional $V \subset \mathbb{C}^n$ y generan un ideal radical $(F_1, \ldots, F_n)$. Decimos que un subespacio $\Pi_V \subset \mathbb{Q}[x_1, \ldots, X_n]$ es un **espacio de interpolantes** para el conjunto de nodos V si para todo $F \in \mathbb{Q}[X_1, \ldots, X_n]$ existe un único interpolante $P_F \in \Pi_V$ con $P_F(x) = F(x)$ para todo $x \in V$. Exhibimos un procedimiento simbólico efectivo para

construir, a partir de $F_1, \ldots, F_n$, una base $\{G_1, \ldots, G_D\}$ de un espacio de interpolantes Π_V y, a partir de un polinomio adicional $F \in \mathbb{Q}[X_1, \ldots, X_n]$, las coordenadas del interpolante P_F en dicha base. Nuestra construcción proporciona un espacio de interpolantes Π_V que está unívocamente determinado por la sucesión $F_1, \ldots, F_n$ y tal que el grado de los interpolantes es a lo sumo $n(d-1)$, donde d es una cota superior para los grados de $F_1, \ldots, F_n$. Por lo tanto, aunque nuestro espacio no es un espacio de interpolantes de "grado mínimo" en el sentido de [dBR90] (ver también [dBR92], [MS00a], [GS00b], [Sau01]), obtenemos interpolantes de grado "razonable".

Nuestra construcción de la base $\{G_1, \ldots, G_D\}$ no se obtiene a partir de la base monomial del álgebra residual de una base de Gröbner de $(F_1, \ldots, F_n)$ como en [MMM93] o la base de polinomios "reducidos" módulo una H–base del mismo ideal como en [MS00b], sino que combina la noción de respresentación univariada de la variedad V con herramientas de dualidad en álgebras de Gorenstein en el espíritu de [GHH$^+$97] y [HMPS00]. En particular, combinando la demostración del Teorema 21 con la fórmula (12) más abajo en [GHH$^+$97] se obtiene un interpolante P_F de "grado bajo". Sin embargo, el procedimiento allí descripto evita explícitamente el cálculo de una base del correspondiente espacio de interpolantes (lo que por otra parte no es necesario en el contexto de dicho trabajo). En nuestro caso, para obtener una base $\{G_1, \ldots, G_D\}$ de un espacio de interpolantes Π_V, consideramos una solución geométrica $Q, V_1, \ldots, V_n \in Q[T]$ de V con elemento primitivo $U \in \mathbb{Q}[X_1, \ldots, X_n]$. Los polinomios $G_1, \ldots, G_D$ se obtienen entonces sustituyendo adecuadamente $V_1, \ldots, V_n$ en el polinomio **Bezoutiano** de $F_1, \ldots, F_n$ (ver la identidad 8.1 para la definición de Bezoutiano). Luego, dado un polinomio $F \in \mathbb{Q}[X_1, \ldots, X_n]$ arbitrario, obtenemos el correspondiente interpolante P_F calculando sus coordenadas en la base $\{G_1, \ldots, G_D\}$ como se describe a continuación. Sea $J \in \mathbb{Q}[X_1, \ldots, X_n]$ el Jacobiano de $F_1, \ldots, F_n$ con respecto a $X_1, \ldots, X_n$. Denótense se por $\mathcal{J}$, u y f las imágenes en el anillo cociente $\mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_n)$ del Jacobiano J, del elemento primitivo U y del polinomio F respectivamente. Para cada $g \in \mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_n)$ denotemos por $Tr(g)$ la traza del endomorfismo de multiplicación por g en $\mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_n)$. Entonces el interpolante $P_F \in \Pi_V$ de cada $F \in \mathbb{Q}[X_1, \ldots, X_n]$ se puede escribir de la siguiente manera (Corolario 8.2.2):

$$P_F = \sum_{j=1}^{D} Tr(\mathcal{J}^{-1} f u^{j-1}) G_j.$$

Finalmente consideramos una versión algorítmica de esta construcción cuando $F_1, \ldots, F_n$ forman una sucesión regular reducida. Combinando el algoritmo para el cálculo de una representación univariada de V del Teorema 1.2.3 con las técnicas de dualidad antes mencionadas obtenemos un algoritmo probabilístico que, a partir de $F_1, \ldots, F_n$ y un polinomio adicional $F \in \mathbb{Q}[X_1, \ldots, X_n]$, calcula $\{G_1, \ldots, G_D\}$ y P_F (una representación por straight–line programs de los mismos).

Para controlar la longitud bit de los enteros durante los cálculos intermedios, al igual que en el caso de la resolución de sistemas polinomiales, nuestro algoritmo calcula aproximaciones p–ádicas adecuadas de los coeficientes $Tr(\mathcal{J}^{-1} f u^{j-1})$ $(1 \leq j \leq D)$ del interpolante P_F. Para esto usamos el primo p previamente calculado

para la etapa modular del cálculo de la representación univariada de V. Luego, por medio de las estimaciones para las alturas de [KPS01] y un algoritmo para reconstrucción racional (ver, por ejemplo, [vzGG99]), podemos recuperar, a partir de sus aproximaciones p–ádicas, las representaciones por numerador y denominador de las trazas. Se demuestra el siguiente resultado (ver el Teorema 8.3.20 para un enunciado detallado)

Teorema 1.2.4. *Sean $F_1, \ldots, F_n \in \mathbb{Z}[\boldsymbol{X}]$ polinomios de grado a lo sumo d que forman una sucesión regular reducida y definen la variedad cero–dimensional $V \subset \mathbb{A}^n$. Sea $F \in \mathbb{Z}[\boldsymbol{X}]$ un polinomio arbitrario. Denótese con δ el grado del sistema de entrada y con h una cota superior para la longitud bit de los coeficientes de $F_1, \ldots, F_n$ y F. Existe un algoritmo probabilístico que toma como entrada un straight–line program de longitud a lo sumo L que evalúa $F_1, \ldots, F_n$ y F y entrega en la salida una base $\{G_1, \ldots, G_D\}$ de un espacio de interpolantes Π_V con interpolantes de grados a lo sumo $n(d-1)$ y el correspondiente interpolante $P_F \in \Pi_V$ de F. La cantidad de operaciones bit que realiza el algoritmo es esencialmente*

$$\mathcal{O}^{\sim}\Big(n^{\mathcal{O}(1)} L\delta\big(d\delta + nd^n h\big(d^n + \deg(F)\big)\big)\Big).$$

Observamos que nuestro algoritmo realiza esencialmente $\mathcal{O}^{\sim}\big(n^{\mathcal{O}(1)} L(d\delta)^2\big)$ operaciones aritméticas en $\mathbb{Q}$. Para comparar la complejidad del mismo con la de los algoritmos que utilizan bases de Gröbner o H–bases, supóngase que los polinomios de entrada $F_1, \ldots, F_n$ y F están dados por su representación densa. La longitud L del straight–line program que subyace a esta representación es del orden $\mathcal{O}\big(n\binom{d+n}{n}\big)$. Puesto que, suponiendo que $d \geq n$, $n\binom{d+n}{n}$ es del orden $d^{n+\mathcal{O}(1)}$ y, por la desigualdad de Bézout, $d\delta$ está acotado superiormente por d^n, concluimos que para sistemas de entrada densos la complejidad aritmética de nuestro algoritmo es del orden $\mathcal{O}^{\sim}(d^{3(n+\mathcal{O}(1))})$. Así, nuestro algoritmo no mejora la complejidad del peor caso de bases de Gröbner para sistemas de entrada en codificación densa. Sin embargo, subrayamos que la eficiencia de nuestro algoritmo se manifiesta claramente cuando, o bien la longitud L del straight–line program que representa los polinomios de entrada es pequeña, o bien el grado δ es pequeño con respecto a la cota d^n. En este sentido, nuestro algoritmo puede ser una alternativa interesante a los algoritmos que usan bases de Gröbner o H–bases.

1.2.3. Cotas inferiores para algoritmos de interpolación

Un marco universal para los aspectos **matemáticos** de la interpolación se desarrolla en [dBR92, Section 2]. Por nuestra parte nos ocupamos de los aspectos **algorítmicos**, y en particular de la **complejidad computational** de los problemas y procedimientos de interpolación. Por lo tanto es preciso considerar no sólo los conceptos estructurales como los funcionales e interpolantes, sino también las (posibles) estructuras de datos que los representan. Aunque este punto de vista algorítmico puede combinarse con el marco general para la interpolación de [dBR92], el resultado sería un formalismo más bien aparatoso, difícil o imposible de descifrar para el no especialista, ocultando en vez de revelar las ideas detrás de nuestra argumentación. En

consecuencia focalizamos la atención en los problemas y algoritmos de interpolación de Hermite–Lagrange. Los interpolantes que consideramos son siempre polinomios multivariados sobre los números complejos $\mathbb{C}$. Esto hace las formulaciones matemáticas estructurales mucho más simples y que el contexto sea mejor conocido a los no especialistas que el modelo general de interpolación introducido en [dBR92].

Los algoritmos de interpolación clásicos devuelven los polinomios interpolantes en representación densa o rala y la dimensión (finita) del espacio vectorial en que se hallan resulta por lo tanto una cota inferior para la complejidad de estos procedimientos. Por nuestra parte planteamos la cuestión de la complejidad intrínseca de los algoritmos de interpolación de Hermite–Lagrange que admiten representaciones más generales de los interpolantes, por ejemplo, su codificación por straight–line programs. Para responder a esta cuestión, describimos un modelo general de problema y algoritmo de interpolación de "Hermite–Lagrange" que incluye los problemas y algoritmos de interpolación multivariada usuales.

Una característica general de los problemas y algoritmos de interpolación consiste en la identidad del **objeto de entrada** y la **representación de entrada** (ver [CGH$^+$03] para una motivación y una discusión matemática de la distinción de estos conceptos). En la interpolación de Hermite–Lagrange, el objeto y la representación de entrada son siempre dados por una lista finita de nodos y los correspondientes valores funcionales. Este planteo se mantendrá a lo largo de nuestro trabajo. Sin embargo se admitirá una libertad mayor que la usual en la representación de los **objetos de salida**, esto es, de los interpolantes, que siempre serán polinomios de grados acotados, los cuales sin embargo pueden resultar exponenciales en el número de nodos.

Se hará un uso sustancial de la identidad del objeto de entrada y de la representación de entrada para establecer un modelo matemático general que capture la noción intuitiva de problema y algoritmo de interpolación de Hermite–Lagrange con interpolantes polinomiales (ver la discusión en la Sección 9.2.1 y la Definición 9.2.1). En nuestro modelo, un **problema de interpolación** está determinado por una clase $\mathcal{D}$ de **datos de interpolación** y una clase $\mathcal{O}$ de **interpolantes**. El conjunto $\mathcal{D}$ que llamaremos la **estructura de datos de entrada** será un subconjunto "construible" de un espacio afín adecuado $\mathbb{C}^N$. El conjunto de interpolantes $\mathcal{O}$ será un subconjunto "construible" del espacio vectorial $\prod_D^{(n)}$ de polinomios n–variados con coeficientes complejos de grado a lo sumo D, para n y D adecuados, tal que para todo dato de interpolación $d \in \mathcal{D}$ existe exactamente un interpolante $f \in \mathcal{O}$ que resuelve el problema de interpolación para d. Para incluir en el modelo la noción de **algoritmo de interpolación** consideramos una **estructura de datos de salida** $\mathcal{D}^*$ que codifica la clase de objetos de salida $\mathcal{O}$ que definen los interpolantes. En la interpolación de Lagrange y de Hermite clásica $\mathcal{D}^*$ es siempre la representación densa o rala de los interpolantes. En nuestro caso, admitimos estructuras de datos $\mathcal{D}^*$ más generales para incluir por ejemplo la representación por straight–line programs de los interpolantes. Así, $\mathcal{D}^*$ será en general un subconjunto "construible" adecuado de un espacio afín $\mathbb{C}^M$. Finalmente consideramos una aplicación construible $\Psi : \mathcal{D} \to \mathcal{D}^*$ tal que para cada $d \in \mathcal{D}$ "calcula" el código $d^* \in \mathcal{D}^*$ que representa el interpolante $f \in \mathcal{O}$ que resuelve el problema de interpolación para d. El tamaño

M de la estructura de datos $\mathcal{D}^*$ es la "complejidad" del algoritmo. La "complejidad" del problema de interpolación determinado por los datos de interpolación $\mathcal{D}$ y la clase de interpolantes $\mathcal{O}$ se define como el mínimo M tal que existe un algoritmo con complejidad M que resuelve que resuelve el problema de interpolación. Por otra parte, los algoritmos y problemas de interpolación multivariada usuales admiten fenómenos de coalescencia (ver, por ejemplo, [dBR90] o [dBR92]). Con el fin de capturar estos fenómenos de coalescencia introducimos la noción fundamental de "robustez geométrica" en nuestro modelo.

Se podría esperar que estructuras de datos y técnicas algorítmicas no lineales permitan mejorar la complejidad de los procedimientos de interpolación. Sin embargo, mostramos que la no linealidad no es una panacea. En este espíritu exhibimos problemas particulares (y naturales) de interpolación de Hermite–Lagrange que bajo la mencionada restricción de "robustez geométrica" requieren para su resolución algorítmica procedimientos de alta complejidad intrínseca, aún si se admiten técnicas de interpolación no lineales. Para estos problemas probamos cotas inferiores de complejidad expresadas en términos del número K de nodos involucrados en el problema de interpolación en consideración y pueden ser lineales en K (resultados de incompresibilidad) o exponenciales en K.

Como primer ejemplo de problema incompresible consideramos un problema de interpolación de Lagrange "genérico", es decir, en donde el conjunto $\mathcal{D}$ de datos de interpolación es un subconjunto denso Zariski del espacio ambiente afín en el que está inmerso. Se demuestra el siguiente resultado (ver la Proposición 11.1.1 para el enunciado preciso).

Proposición 1.2.5. *Sean $n, K, D \in \mathbb{N}$. Sea $\mathcal{D}$ un subconjunto denso Zariski de $\mathbb{C}^{(n+1)\times K}$ que actúa como estructura de datos de entrada para un problema de interpolación con conjunto de interpolantes (no necesariamente lineal) $\mathcal{O} \subset \prod_D^{(n)}$. Es decir, para cada dato de interpolación $d = (x_1, y_1, \ldots, x_K, y_K) \in \mathcal{D}$, donde $x_1, \ldots, x_K \in \mathbb{C}^n$ y $y_1, \ldots, y_K \in \mathbb{C}$, existe $f \in \mathcal{O}$ tal que $f(x_i) = y_i$ para $1 \leq i \leq K$. Entonces todo algoritmo "geométricamente robusto" que resuelve el problema de interpolación determinado por $\mathcal{D}$ y $\mathcal{O}$ tiene complejidad al menos K.*

Sin embargo, el fenómeno anterior no se limita sólo a los problemas de interpolación genéricos, como lo muestra el siguiente problema interpolación de Lagrange con interpolantes "fáciles evaluar"(ver la Proposición 11.1.2 para el enunciado preciso).

Proposición 1.2.6. *Sean $K, M \in \mathbb{N}$, $K \geq 2$, y $F(X,T) \in \mathbb{C}[X,T]$ el polinomio bivariado $F(X,T) := (T^{D+1} - 1)\sum_{k=0}^{D} T^k X^k$ con $D := K - 1$. Sea $\mathcal{D} \subset \mathbb{C}^{2K}$ el conjunto $\mathcal{D} := \{(x_1, y_1, \ldots, x_K, y_K) \in \mathbb{C}^{2K} :$ existe $t \in \mathbb{C}$ con $F(x_i, t) = y_i$ para $1 \leq i \leq K$ y $x_i \neq x_j$ para $1 \leq i < j \leq K\}$. Nótese que la clausura Zariski $\overline{\mathcal{D}}$ es una subvariedad propia de dimensión $K+1$ de $\mathbb{C}^{2K}$. Consideremos a $\mathcal{O} := \{F(X,t) : t \in \mathbb{C}\}$ como conjunto de interpolantes. Nótese que todo interpolante $f \in \mathcal{O}$ puede ser evaluado por un straight–line program de longitud $\mathcal{O}(\log D)$ (ver [BCS97]). Entonces todo algoritmo "geométricamente robusto" que resuelve el problema de interpolación determinado por $\mathcal{D}$ y $\mathcal{O}$ tiene complejidad al menos K.*

Por último consideramos un problema de interpolación de Lagrange cuya complejidad es exponencial en el número de nodos si se admiten sólo algoritmos geométricamente robustos.

Sea $\mathcal{O}$ el subconjunto de $\mathbb{C}[X_1, \ldots, X_n]$ formado por los polinomios que se pueden evaluar con a lo sumo L operaciones aritméticas no escalares (es decir, las sumas, restas y multiplicaciones por constantes de $\mathbb{C}$ no se cuentan). Se puede ver que todo elemento de $\mathcal{O}$ tiene grado a lo sumo 2^L (ver [HS82, Theorem 3.2] o [BCS97, Exercise 9.18]). De acuerdo con [CGH$^+$03, Corollary 2] (ver también [HS82, Theorem 4.4]) existen puntos $\gamma_1, \ldots, \gamma_K \in \mathbb{C}^n$ con coordenadas enteras de longitud bit a lo sumo $\mathcal{O}(\sqrt{K})$, donde $K \in \mathcal{O}((L+n)^2)$, tales que para todo $f, g \in \mathcal{O}$ las igualdades $f(\gamma_i) = g(\gamma_i)$ para $1 \leq i \leq K$ implican $f = g$. Una tal sucesión $\gamma_1, \ldots, \gamma_K$ se llama una "sucesión de identificación" para la clase de polinomios $\mathcal{O}$. Sea $\mathcal{D}$ el subconjunto de $\mathbb{C}^K$ definido por $\mathcal{D} := \{(f(\gamma_1), \ldots, f(\gamma_K)) : f \in \mathcal{O}\}$. El par $\mathcal{D}$, $\mathcal{O}$ define de manera natural un problema de interpolación de Lagrange con nodos fijos $\gamma_1, \ldots, \gamma_K$, tal que para todo punto $\boldsymbol{y} = (y_1, \ldots, y_K) \in \mathcal{D}$ existe único interpolante $f \in \mathcal{O}$ que resuelve el problema de interpolación de Lagrange para el dato de interpolación $\boldsymbol{y}$. Se demuestra el siguiente resultado (ver el Teorema 11.2.1 para el enunciado preciso).

Teorema 1.2.7. *Todo algoritmo geométricamente robusto que resuelve el problema de interpolación determinado por la estructura de datos $\mathcal{D}$ y el conjunto de interpolantes $\mathcal{O}$ definidos como arriba tiene complejidad al menos $2^{\Omega(Ln)} = 2^{\Omega(\sqrt{K})}$. Es decir, todo algoritmo geométricamente robusto, que reconstruye los polinomios n–variados que pueden ser evaluados por un straight–line program de longitud no escalar a lo sumo L a partir de sus valores en una sucesión de identificación de longitud K, utiliza una cantidad de operaciones aritméticas que es exponencial en $\sqrt{K}$.*

El resultado anterior implica que la interpolación de Lagrange tradicional en $\binom{2^L+n}{n} = 2^{\mathcal{O}(Ln)}$ nodos es esencialmente óptima para esta clase muy especial de polinomios.

Por último observamos que en los ejemplos anteriores un algoritmo geométricamente robusto que resuelve el correspondiente problema de interpolación debe realizar una cantidad de operaciones aritméticas al menos polinomial en el número de nodos en consideración, demostrando que nuestro algoritmo para el problema de interpolación implícita es esencialmente óptimo.

1.2.4. Organización de la tesis

La tesis está organizada como sigue. En el Capítulo 2 se recuerdan las nociones y resultados de geometría algebraica y álgebra conmutativa que se usarán en esta tesis, y se discuten la representación de polinomios multivariados por straight–line programs y de variedades algebraicas por representaciones de Kronecker. En el Capítulo 3 se recuerda la noción de forma de Chow de una variedad equidimensional, se discuten sus propiedades básicas y se obtienen las condiciones (1)–(3) del Teorema 1.2.1. En el Capítulo 4 se discute la noción de punto de levantamiento y se termina de demostrar el Teorema 1.2.1. En el Capítulo 5 se demuestra el Teorema

1.2.2. El Capítulo 6 contiene las estimaciones de altura de las variedades que subyacen a la demostración de este resultado. En el Capítulo 7 se describe un algoritmo para resolver el sistema de entrada $F_1 = 0, \ldots, F_r = 0$ y se analiza su complejidad bit, demostrando así el Teorema 1.2.3. En el Capítulo 8 se describe un algoritmo para el problema de interpolación implícita definido por un sistema cero–dimensional $F_1 = 0, \ldots, F_n = 0$ y se analiza su complejidad, demostrando así el Teorema 1.2.4. Por último, los Capítulos 9, 10 y 11 están dedicados al tema de la complejidad de la interpolación multivariada. En el Capítulo 9 se presenta el modelo de computación para la interpolación que será la base para la determinación de las cotas inferiores de complejidad. En el contexto de este modelo se discuten en detalle tanto problemas de interpolación clásicos como también otros problemas de interpolación menos usuales, de tipo no lineal como los arriba mencionados. En el Capítulo 10 se introduce la noción de algoritmo geométricamente robusto. Finalmente el Capítulo 11 contiene los resultados sobre complejidad de la interpolación, demostrando las Proposiciones 1.2.5 y 1.2.6 y el Teorema 1.2.7.

Capítulo 2

Preliminares

Este capítulo contiene todas las definiciones, notaciones y resultados básicos de geometría algebraica y álgebra conmutativa que usaremos a lo largo de esta tesis. Como referencia para estos resultados utilizamos principalmente los textos [Eis95], [Kun85], [Sha94] y [Har77]. También contiene las definiciones de las estructuras de datos y los resultados de complejidad de los algoritmos básicos que se utilizarán, para lo cual tomamos como referencia principalmente los textos [vzGG99] y [BCS97].

2.1. Definiciones y resultados básicos de geometría algebraica y álgebra conmutativa

En lo que sigue un anillo es siempre un anillo conmutativo con unidad.

Sea R un anillo y M un R–módulo. Si $U \subset R$ es un subconjunto multiplicativo de R denotamos con $U^{-1}R$ y $U^{-1}M$ las respectivas localizaciones de R y M en U. Como es usual, llamamos **anillo de fraccciones total** de R a la localización de R en el conjunto U formado por todos los elementos de R que no son divisores de cero. Si P es un ideal primo de R denotamos con R_P y M_P las respectivas localizaciones de R y M en $U := R \setminus P$. En tal caso R_P es un anillo local cuyo ideal maximal es la imagen de P en R_P. Si $a \in R$, denotamos con R_a la localización de R en $U := \{a^k : k \geq 0\}$. Si R es un anillo local con ideal maximal $\mathfrak{M}$ llamamos al cuerpo cociente $R/\mathfrak{M}$ el **cuerpo de clases residuales** de R.

Por la **dimensión** $\dim R$ de un anillo R entendemos la dimensión de Krull del anillo, es decir, $\dim R$ es la longitud máxima r de una cadena de ideales primos $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r \subsetneq R$ contenida en R.

Un subconjunto $\{a_1, \ldots, a_n\} \subseteq A$ de n elementos de una $\mathbb{K}$–álgebra A se dice **algebraicamente independiente** si para todo polinomio no nulo $F \in \mathbb{K}[X_1, \ldots, X_n]$ se tiene que $F(a_1, \ldots, a_n) \neq 0$. El **grado de trascendencia** $\operatorname{trdeg}(A)$ de A se define como el supremo del conjunto de cardinales $|T|$, siendo $T \subseteq A$ un subconjunto finito y algebraicamente independiente. Si A es una $\mathbb{K}$–álgebra afín, es decir, una $\mathbb{K}$–álgebra finitamente generada, denotamos con $\dim A$ la dimensión de A como anillo. El siguiente resultado es útil para calcular la dimensión de una $\mathbb{K}$–álgebra afín.

Teorema 2.1.1. *Sea A una $\mathbb{K}$–álgebra afín. Entonces* $\dim A = \operatorname{trdeg}(A)$. *Además,*

si $S \subseteq A$ es un conjunto de generadores, entonces

$$\dim A = \text{máx}\{|T| : \ T \subseteq S \text{ es finito y algebraicamente independiente}\}.$$

Sea R un anillo Noetheriano, $I \subset R$ un ideal propio. Sea $I = \cap_{i=1}^{n} Q_i$ una descomposición primaria minimal de I, con Q_i un ideal P_i–primario para $1 \leq i \leq n$. Recordemos que los primos P_i $(1 \leq i \leq n)$ se llaman los primos **asociados** de I. Los elementos minimales del conjunto $\{P_1, \ldots, P_n\}$ son los primos **minimales** o **aislados** de I y los restantes son los llamados primos **inmersos**.

Sea $P \subset R$ un ideal primo y R_P la localización de R en P. La **codimensión** de P se define como $\text{codim}\,(P) := \dim(R_P)$. Equivalentemente $\text{codim}\,(P)$ es la máxima longitud n de una cadena de ideales primos $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$. En el caso general, si $I \subset R$ es un ideal, $I \neq R$, la **codimensión** de I se define como $\text{codim}\,(I) := \text{mín}\{\text{codim}\,(P) : \quad P \subset R \ \text{ es un ideal primo con } \ I \subseteq P\}$. También definimos la **dimensión** de I como $\dim(I) := \dim(R/I)$.

Un anillo Noetheriano R se dice **equidimensional** si todos sus primos minimales tienen la misma dimensión. Si A es una $\mathbb{K}$–álgebra afín equidimensional, para todo ideal $I \subseteq A$ se satisface $\dim(I) + \text{codim}\,(I) = \dim(A)$ (ver, por ejemplo, [Kun85, Corollary 3.6, b)]).

Sea $\mathbb{K}$ un cuerpo arbitrario y $\overline{\mathbb{K}}$ su clausura algebraica. Denotamos con $\mathbb{A}^n := \mathbb{A}^n(\overline{\mathbb{K}})$ y $\mathbb{P}^n := \mathbb{P}^n(\overline{\mathbb{K}})$ al espacio afín y proyectivo de dimensión n definido sobre $\overline{\mathbb{K}}$ respectivamente. Ambos son espacios topológicos con la **topología de Zariski** sobre $\mathbb{K}$, cuyos conjuntos cerrados son los **conjuntos algebraicos** definidos sobre $\mathbb{K}$, también llamados $\mathbb{K}$–subvariedades, de $\mathbb{A}^n$ y $\mathbb{P}^n$ respectivamente.

Definición 2.1.2. *Sea $\mathbb{K}$ un cuerpo arbitrario.*

i) Un subconjunto $V \subseteq \mathbb{A}^n$ es una $\mathbb{K}$–(sub)variedad afín *o una* (sub)variedad afín de $\mathbb{A}^n$ definida sobre $\mathbb{K}$ *si es el conjunto de ceros comunes en $\mathbb{A}^n$ de un subconjunto $S \subseteq \mathbb{K}[X_1, \ldots, X_n]$. En particular, una $\mathbb{K}$–*hipersuperficie afín *de $\mathbb{A}^n$ es el conjunto de ceros en $\mathbb{A}^n$ de un único polinomio $F \in \mathbb{K}[X_1, \ldots, X_n]$ no nulo.*

ii) Un subconjunto $V \subseteq \mathbb{P}^n$ es una $\mathbb{K}$–(sub)variedad proyectiva *o una* (sub)variedad proyectiva de $\mathbb{P}^n$ definida sobre $\mathbb{K}$ *si es el conjunto de ceros comunes en $\mathbb{P}^n$ de un subconjunto $S \subseteq \mathbb{K}[X_0, \ldots, X_n]$ de polinomios homogéneos. En particular, una $\mathbb{K}$–*hipersuperficie proyectiva *de $\mathbb{P}^n$ es el conjunto de ceros en $\mathbb{P}^n$ de un único polinomio homogéneo $F \in \mathbb{K}[X_0, \ldots, X_n]$ no nulo.*

Usaremos las notaciones $\mathcal{V}(S)$, respectivamente $\{F_1 = 0, \ldots, F_s = 0\}$, para denotar la $\mathbb{K}$–variedad afín o proyectiva definida por el conjunto de polinomios S, respectivamente $\{F_1, \ldots, F_s\}$.

Notemos que los conjuntos abiertos en la topología de Zariski de $\mathbb{A}^n$ o $\mathbb{P}^n$ son densos. En tal sentido, decimos que una propiedad sobre los elementos de $\mathbb{A}^n$ o $\mathbb{P}^n$ es **genérica** si la satisfacen todos los puntos que pertenecen a un abierto Zariski de $\mathbb{A}^n$ o $\mathbb{P}^n$.

Sea X un subconjunto de $\mathbb{A}^n$ o $\mathbb{P}^n$. Denotamos por $\mathcal{I}(X)$ al **ideal anulador** de V, es decir el conjunto de polinomios en $\mathbb{K}[X_1, \ldots, X_n]$ o en $\mathbb{K}[X_0, \ldots, X_n]$ que se

anulan en todos los puntos de X. Es claro que $\mathcal{I}(X)$ es un ideal radical. Si $V \subseteq \mathbb{A}^n$ es una subvariedad afín, el **anillo coordenado afín** de V se define como el anillo cociente $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}(V)$. El siguiente resultado fundamental es conocido como el Nullstellensatz o Teorema de los ceros de Hilbert (ver, por ejemplo, [Kun85, Chapter I, §3, Proposition 3.7]).

Teorema 2.1.3. *La asignación $V \mapsto \mathcal{I}(V)$ define una biyección del conjunto de todas las $\mathbb{K}$–subvariedades afines V de $\mathbb{A}^n$ sobre el conjunto de todos los ideales radicales I de $\mathbb{K}[X_1, \ldots, X_n]$. Para todo ideal I de $\mathbb{K}[X_1, \ldots, X_n]$, es $\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$*

En vista del teorema anterior, si V es una $\mathbb{K}$–subvariedad afín o proyectiva, $\mathcal{I}(V)$ suele denominarse también el **ideal de definición** de V.

Recordemos que un subconjunto de un espacio topológico es **localmente cerrado** si es un subconjunto abierto de su clausura, o equivalentemente si es la intersección de un abierto con un cerrado. Un subconjunto localmente cerrado de $\mathbb{A}^n$ o $\mathbb{P}^n$ en la correspondiente topología de Zariski sobre $\mathbb{K}$ será llamado una $\mathbb{K}$–subvariedad afín o proyectiva **abierta** de $\mathbb{A}^n$ o $\mathbb{P}^n$ respectivamente (otro término que se encuentra en la literatura para tales conjuntos es el de subvariedad "cuasi–afín" o "cuasi–proyectiva"). Ocasionalmente utilizaremos la expresión $\mathbb{K}$–subvariedad (afín o proyectiva) **cerrada** para denotar una $\mathbb{K}$–subvariedad afín o proyectiva de acuerdo con la Definición 2.1.2 enfatizando el hecho de que se trata de un conjunto cerrado de $\mathbb{A}^n$ o $\mathbb{P}^n$ según corresponda.

Por brevedad, en lo que sigue usamos el término $\mathbb{K}$–**variedad** para denotar indistintamente una $\mathbb{K}$–subvariedad afín o proyectiva tanto abierta como cerrada, siendo las definiciones y propiedades que damos a continuación válidas en cualquiera de estos casos. Consideraremos a toda $\mathbb{K}$–variedad V como un espacio topológico con la topología de Zariski inducida de $\mathbb{A}^n$ o de $\mathbb{P}^n$ según corresponda. Llamamos a esta topología la **topología de Zariski sobre $\mathbb{K}$ de V**.

Recordemos que un espacio topológico X no vacío se dice **irreducible** si no es la unión de dos subconjuntos cerrados propios. Una condición equivalente es que todo subconjunto abierto no vacío de X es denso en X.

Definición 2.1.4. *Una $\mathbb{K}$–variedad V se dice* irreducible sobre $\mathbb{K}$ *si es irreducible como espacio topológico con la topología de Zariski sobre $\mathbb{K}$.*

Una $\mathbb{K}$–variedad V es irreducible sobre $\mathbb{K}$ si y solo si su ideal anulador $\mathcal{I}(V)$ es un ideal primo de $\mathbb{K}[X_1, \ldots, X_n]$ o $\mathbb{K}[X_0, \ldots, X_n]$ según corresponda.

Toda $\mathbb{K}$–variedad V se puede descomponer como una unión irredundante de $\mathbb{K}$–variedades irreducibles, es decir, $V = C_1 \cup \cdots \cup C_s$ donde cada C_i es una $\mathbb{K}$–variedad irreducible que cumple que $C_i \not\subset C_j$ para todo $i \neq j$. A esta descomposición se la conoce como **descomposición en componentes irreducibles** y es única salvo reordenamiento. Cada C_i se denomina una componente $\mathbb{K}$–**irreducible** de V.

Dada una $\mathbb{K}$–variedad V, por la **dimensión** de V, que notamos $\dim V$, entendemos la dimensión de Krull del espacio topológico V en su topología de Zariski sobre $\mathbb{K}$. Por lo tanto la dimensión r de V es la longitud máxima de una cadena de $\mathbb{K}$–variedades cerradas irreducibles no vacías $V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_r \subseteq V$ contenida en V. Por el Teorema 2.1.3, si $V \subseteq \mathbb{A}^n$ es una $\mathbb{K}$–subvariedad afín, se tiene que

$\dim V = \dim \mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}(V)$. La dimensión de V coincide con el máximo de las dimensiones de sus componentes $\mathbb{K}$–irreducibles. Decimos que una $\mathbb{K}$–variedad es **equidimensional de dimensión r** o que tiene **dimensión pura r** si toda componente $\mathbb{K}$–irreducible de dicha variedad tiene dimensión r. Observemos que una $\mathbb{K}$–hipersuperficie es una $\mathbb{K}$–variedad de $\mathbb{A}^n$ o $\mathbb{P}^n$ de dimensión pura $n-1$.

Las siguientes son propiedades básicas de la dimensión (ver, por ejemplo, [Sha94, Chapter 1, Section §6.1, Theorem 1] y [Har77, Proposition 1.10 and Exercise 2.7]):

Teorema 2.1.5. *Sean V y W $\mathbb{K}$–variedades.*

- *Si $V \subseteq W$, entonces $\dim V \leq \dim W$.*
- *Si W es irreducible y $V \subseteq W$ tal que $\dim V = \dim W$, entonces $\overline{V} = W$, donde $\overline{V}$ es la clausura de V en W.*
- *Si V es una $\mathbb{K}$–subvariedad afín (respectivamente proyectiva) abierta de $\mathbb{A}^n$ (respectivamente de $\mathbb{P}^n$) entonces $\dim V = \dim \overline{V}$, donde $\overline{V}$ es la clausura de V en $\mathbb{A}^n$ (respectivamente en $\mathbb{P}^n$).*

A continuación recordamos la noción de morfismo entre variedades. Para los fines de esta tesis bastará restringirnos al caso afín. Así en lo que sigue el término $\mathbb{K}$–(sub)variedad designa una $\mathbb{K}$–variedad afín abierta o cerrada.

Definición 2.1.6. *Sea V una $\mathbb{K}$–subvariedad de $\mathbb{A}^n$. Una función $f : V \to \overline{\mathbb{K}}$ es* regular en un punto *$\boldsymbol{y} \in V$ si existe un entorno abierto y denso U con $\boldsymbol{y} \in U \subseteq V$ y polinomios $G, H \in \mathbb{K}[X_1, \ldots, X_n]$ tales que H no se anula en ningún punto de U y $f(\boldsymbol{x}) = G(\boldsymbol{x})/H(\boldsymbol{x})$ para todo $\boldsymbol{x} \in U$. Decimos que f es* regular en *V si es regular en todo punto de V.*

Observemos que, si identificamos $\overline{\mathbb{K}}$ con $\mathbb{A}^1$ en su topología de Zariski sobre $\mathbb{K}$, una función regular es continua. Denotamos por $\mathbb{K}[V]$ al anillo de todas las funciones regulares en una $\mathbb{K}$–variedad V.

Si V es una $\mathbb{K}$–subvariedad afín *cerrada* de $\mathbb{A}^n$, una función $f : V \to \overline{\mathbb{K}}$ es regular en V si y solo si existe $F \in \mathbb{K}[X_1, \ldots, X_n]$ con $f(\boldsymbol{x}) = F(\boldsymbol{x})$ para todo $\boldsymbol{x} \in V$ y $\mathbb{K}[V]$ resulta isomorfo al anillo cociente $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}(V)$. Si además $g \in \mathbb{K}[V] \setminus \{0\}$ y V_g es el subconjunto abierto Zariski de V definido por $\{g \neq 0\}$, el anillo $\mathbb{K}[V_g]$ de las funciones regulares en V_g es isomorfo a la localización $\mathbb{K}[V]_g$ de $\mathbb{K}[V]$.

Definición 2.1.7. *Sean V y W dos $\mathbb{K}$–variedades. Un* morfismo *$\varphi : V \to W$ es una aplicación continua tal que para todo subconjunto abierto y denso $U \subseteq W$ y para toda función regular $f : W \to \overline{\mathbb{K}}$, la función $f \circ \varphi : \varphi^{-1}(U) \to \overline{\mathbb{K}}$ es regular.*

El siguiente resultado se deduce fácilmente de la definición anterior (ver, por ejemplo, [Har77, Chapter 1, Lemma 3.6])

Lema 2.1.8. *Sea V una $\mathbb{K}$–variedad y $W \subseteq \mathbb{A}^n$ una $\mathbb{K}$–subvariedad afín* cerrada. *Una aplicación $\varphi : V \to W$ es un* morfismo *si y solo si $x_i \circ \varphi$ es una una función regular en V para cada i, donde $x_1, \ldots, x_n$ son las funciones coordenadas de $\mathbb{A}^n$ inducidas por las variables $X_1, \ldots, X_n$.*

Un **isomorfismo** $\varphi : V \to W$ de $\mathbb{K}$–variedades es un morfismo que admite un morfismo inverso $\psi : W \to V$ con $\psi \circ \varphi = \mathrm{id}_V$ y $\varphi \circ \psi = \mathrm{id}_W$.

Definición 2.1.9. *Sean V y W dos $\mathbb{K}$–variedades. Una* aplicación racional $\varphi : V \to W$ *es una aplicación parcialmente definida tal que su dominio de definición* $\operatorname{dom}\varphi$ *es un subconjunto abierto y denso U de V y $\varphi : U \to W$ es un morfismo de $\mathbb{K}$–variedades con la siguiente propiedad de maximalidad: si U' es un subconjunto abierto y denso de V con $U \subseteq U' \subseteq V$ y $\varphi' : U' \to W$ un morfismo tal que $\varphi' = \varphi$ en U, entonces $U' = U$.*

Observación 2.1.10. *En los Capítulos 9 y siguientes el significado del término* ***aplicación racional*** *difiere del dado en la Definición 2.1.9 en que no se requiere que el dominio U de φ sea maximal.*

Sean $\varphi : X \to Y$ y $\psi : Y \to Z$ aplicaciones racionales de $\mathbb{K}$–variedades, con $U := \operatorname{dom}\varphi$ y $V := \operatorname{dom}\psi$, tales que $\varphi^{-1}(V) \subseteq U$ es un subconjunto abierto y denso de X. En tal caso la composición $\psi\circ\varphi : \varphi^{-1}(V) \to Z$ es un morfismo de $\mathbb{K}$–variedades que se extiende a una única aplicación racional $\psi \circ \varphi : X \to Z$, que llamamos la **composición** de las aplicaciones racionales φ **y** ψ. Una aplicación racional $\varphi : X \to Y$ se dice **birracional** si admite una inversa, es decir una aplicación racional $\psi : Y \to X$ tal que $\psi \circ \varphi = \mathrm{id}_X$ y $\varphi \circ \psi = \mathrm{id}_Y$ como aplicaciones racionales. Equivalentemente $\varphi : X \to Y$ es una aplicación birracional si existen subconjuntos abiertos densos $U' \subseteq U$ y $V' \subseteq Y$ tales que $\varphi : U' \to V'$ es un isomorfismo de $\mathbb{K}$–variedades.

Una **función racional** sobre una $\mathbb{K}$–variedad V es una aplicación racional $f : V \to \overline{\mathbb{K}}$, donde identificamos $\overline{\mathbb{K}}$ con $\mathbb{A}^1$. Las funciones racionales sobre V forman una $\mathbb{K}$–álgebra que denotamos por $\mathbb{K}(V)$. Si además V es irreducible, $\mathbb{K}(V)$ es un cuerpo llamado el **cuerpo de las funciones racionales** sobre V. En este caso $\mathbb{K}[V]$ no posee divisores de cero y $\mathbb{K}(V)$ es isomorfo al cuerpo de fracciones del dominio íntegro $\mathbb{K}[V]$. Para una $\mathbb{K}$–variedad arbitraria V, la $\mathbb{K}$–álgebra $\mathbb{K}(V)$ es isomorfa al anillo total de fracciones de $\mathbb{K}[V]$ y también al producto directo de los cuerpos de funciones racionales de las componentes irreducibles de V.

Un morfismo de $\mathbb{K}$–variedades $\varphi : V \to W$ induce, por composición, un homomorfismo de anillos $\varphi^* : \mathbb{K}[W] \to \mathbb{K}[V]$ llamado el **homomorfismo dual** de φ. Decimos que φ es un **morfismo dominante** si $\overline{\varphi(V)} = W$, donde $\overline{\varphi(V)}$ es la clausura de $\varphi(V)$ con respecto a la topología Zariski de W. En esta situación, el homomorfismo dual φ^* resulta inyectivo e induce una extensión de anillos $\mathbb{K}[W] \hookrightarrow \mathbb{K}[V]$. Si φ es un morfismo dominante decimos que es **finito** si la extensión de anillos $\mathbb{K}[W] \hookrightarrow \mathbb{K}[V]$ es entera, es decir, si cada elemento $\eta \in \mathbb{K}[V]$ satisface una ecuación mónica con coeficientes en $\mathbb{K}[W]$.

A continuación damos una propiedad importante de los morfismos finitos (ver, por ejemplo, [Dan94, §4.2, Proposition]).

Teorema 2.1.11. *Sean V y W $\mathbb{K}$–variedades y sea $f : V \to W$ un morfismo finito. Si $S \subset W$ es una subvariedad irreducible entonces la preimagen $f^{-1}(S)$ es una variedad de dimensión pura* $\dim S$.

El siguiente resultado se conoce como el Teorema de la dimensión de la fibra [Sha94, Chapter 1, Section §6.3, Theorem 7].

Teorema 2.1.12. *Sea $f : V \to W$ un morfismo entre $\mathbb{K}$–variedades irreducibles. Supongamos que f es sobreyectivo, y que $\dim V = n$ y $\dim W = m$. Entonces $m \leq n$ y además,*

1. *$\dim C \geq n - m$ para todo $w \in W$ y para toda componente C de la fibra $f^{-1}(w)$;*
2. *existe un subconjunto abierto no vacío $U \subset W$ tal que $\dim f^{-1}(w) = n - m$ para todo $w \in U$.*

Tenemos también la siguiente propiedad de morfismos entre $\mathbb{K}$–variedades (ver, por ejemplo, [Kun85, Chapter §III. 2, Exercise 6]).

Teorema 2.1.13. *Sea $f : V \to W$ un morfismo entre $\mathbb{K}$–variedades. Entonces:*

- *si Z es una subvariedad irreducible de V, entonces $\overline{f(Z)}$ es irreducible, donde $\overline{f(Z)}$ denota la clausura de $f(Z)$ con respecto a la topología Zariski de W;*
- *$\dim \overline{f(V)} \leq \dim V$.*

Sea $V \subset \mathbb{A}^n$ una $\mathbb{K}$–variedad afín cerrada, $\mathcal{I}(V) \subset \mathbb{K}[X_1, \ldots, X_n]$ el ideal de definición de V y $\boldsymbol{x} \in V$. La **dimensión** $\dim_{\boldsymbol{x}} V$ de V en $\boldsymbol{x}$ es el máximo de las dimensiones de las componentes $\mathbb{K}$–irreducibles de V que contienen a $\boldsymbol{x}$. Si $\mathcal{I}(V) = (F_1, \ldots, F_r)$, el **espacio tangente** $\mathcal{T}_{\boldsymbol{x}}V$ de V en $\boldsymbol{x}$ se define como el núcleo de la matriz Jacobiana $(\partial F_i/\partial X_j)_{1\leq i\leq r, 1\leq j\leq n}(\boldsymbol{x})$ de $F_1, \ldots, F_r$ con respecto a $X_1, \ldots, X_n$ en $\boldsymbol{x}$.

Se satisface la siguiente desigualdad (ver, por ejemplo, [Sha94, página 94]):

$$\dim_{\boldsymbol{x}} V \leq \dim \mathcal{T}_{\boldsymbol{x}}V.$$

Un punto $\boldsymbol{x}$ se dice **regular** si $\dim_{\boldsymbol{x}} V = \dim \mathcal{T}_{\boldsymbol{x}}V$. En caso que $\dim_{\boldsymbol{x}} V < \dim \mathcal{T}_{\boldsymbol{x}}V$, decimos que $\boldsymbol{x}$ es un punto **singular** de V. El conjunto Σ de puntos singulares de V se denomina el **lugar singular** de V; se tiene que Σ es una $\mathbb{K}$–subvariedad cerrada de V. Una $\mathbb{K}$–variedad se dice **no singular o regular** si el conjunto de puntos singulares es vacío.

Sea V una $\mathbb{K}$–variedad afín cerrada cuya descomposición en componentes $\mathbb{K}$–irreducibles es $V = \cup_{i=1}^{N} \mathcal{C}_i$. Se tiene que $\mathcal{C}_i \cap \mathcal{C}_j \subset \Sigma$ para todo $i \neq j$ y que Σ no contiene componentes irreducibles de V. Además si consideramos el lugar singular Σ_i de cada componente irreducible C_i, se tiene que $\Sigma = \bigcup_{i\neq j}(C_i \cap C_j) \cup \bigcup_i \Sigma_i$.

Sea $V \subseteq \mathbb{A}^n$ una $\mathbb{K}$–variedad afín y $\boldsymbol{x} \in V$. Notamos con $\mathfrak{M}_{\boldsymbol{x}} \subset \mathbb{K}[V]$ el ideal $\mathfrak{M}_{\boldsymbol{x}} := \{f \in \mathbb{K}[V] : f(\boldsymbol{x}) = 0\}$. Si $\mathbb{K}$ es algebraicamente cerrado, $\mathfrak{M}_{\boldsymbol{x}}$ es un ideal maximal de $\mathbb{K}[V]$, llamado **el ideal maximal en $\boldsymbol{x}$**.

Definición 2.1.14. *Supóngase que $\mathbb{K}$ es algebraicamente cerrado. Sea $V \subseteq \mathbb{A}^n$ una $\mathbb{K}$–subvariedad afín y $\boldsymbol{x} \in V$. Decimos que $\boldsymbol{x}$ es un punto* normal *de V o que V es* normal en $\boldsymbol{x}$ *si el anillo local $\mathbb{K}[V]_{\mathfrak{M}_{\boldsymbol{x}}}$ es normal. Llamamos a V* normal *si es normal en cada uno de sus puntos.*

El siguiente resultado reúne los hechos sobre puntos normales que utilizaremos en esta tesis (ver, por ejemplo, [Bro89, Satz 8.5 y Satz 10.20]).

Proposición 2.1.15. *Supóngase que $\mathbb{K}$ es algebraicamente cerrado. Sea $V \subseteq \mathbb{A}^n$ una $\mathbb{K}$–subvariedad afín y $\boldsymbol{x} \in V$. Entonces valen las siguientes condiciones:*

1. *$\mathbb{K}[V]_{\mathfrak{M}_{\boldsymbol{x}}}$ es un dominio íntegro si y sólo si $\boldsymbol{x}$ pertenece a una única componente irreducible de V.*

2. *el conjunto $U \subset V$ de los puntos normales de V es un subconjunto abierto y denso Zariski de V.*

A cada $\mathbb{K}$–subvariedad afín $V \subset \mathbb{A}^n$ podemos asociarle una $\mathbb{K}$–subvariedad proyectiva $\overline{V} \subset \mathbb{P}^n$, que llamamos la **clausura proyectiva** de V y definimos de la siguiente manera. Consideramos la inmersión de $\mathbb{A}^n$ en $\mathbb{P}^n$ que a cada $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{A}^n$ le asigna el punto $(1 : x_1 : \cdots : x_n) \in \mathbb{P}^n$. La clausura proyectiva $\overline{V}$ es entonces la clausura con respecto a la topología Zariski en $\mathbb{P}^n$ de la imagen de V vía esta inmersión . Así, $\overline{V}$ es la menor $\mathbb{K}$–variedad proyectiva que contiene a V. Dado un ideal $I \subseteq \mathbb{K}[X_1, \ldots, X_n]$, se define $I^h \subseteq \mathbb{K}[X_0, \ldots, X_n]$ como el ideal homogéneo generado por las homogeneizaciones $F^h \in \mathbb{K}[X_0, \ldots, X_n]$ de todos los polinomios $F \in I$. Se satisfacen las siguientes propiedades [Kun85, §I.5, Proposition 5.17 y Exercise 6; y §II.4, Proposition 4.1].

Teorema 2.1.16. *Sea $V \subset \mathbb{A}^n$ una $\mathbb{K}$–subvariedad afín y sea $\overline{V} \subset \mathbb{P}^n$ la clausura proyectiva de V. Entonces:*

(i) V es irreducible si y sólo si $\overline{V}$ lo es.

(ii) Si $V = V_1 \cup V_2 \cup \cdots \cup V_r$ es la descomposición de V en $\mathbb{K}$–variedades irreducibles entonces $\overline{V} = \overline{V}_1 \cup \overline{V}_2 \cup \cdots \cup \overline{V}_r$ es la descomposición de $\overline{V}$ en componentes $\mathbb{K}$–irreducibles.

(iii) V y $\overline{V}$ tienen la misma dimensión.

(iv) $\mathcal{I}(\overline{V}) = \mathcal{I}(V)^h$.

2.1.1. La condición de pureza

El siguiente resultado clásico es conocido como el Teorema de los ideales principales (ver, por ejemplo, [Eis95, Theorem 10.2]).

Teorema 2.1.17. *Sea R un anillo Noetheriano y P un ideal primo de R que es minimal sobre un ideal $(a_1, \ldots, a_r) \subseteq R$ generado por r elementos. Entonces* $\operatorname{codim}(P) \leq r$.

El Teorema de los ideales principales tiene la siguiente consecuencia geométrica.

Teorema 2.1.18. *Sea $V \subset \mathbb{A}^n$ una $\mathbb{K}$–subvariedad afín de dimensión pura r y sea $F \in \mathbb{K}[X_1, \ldots, X_n]$. Sea $W := V \cap \{F = 0\}$ y $f \in \mathbb{K}[V]$ la imagen de F. Vale una y sólo una de las siguientes afirmaciones:*

- $W = \emptyset$ *(esto sucede cuando f es una unidad de $\mathbb{K}[V]$);*
- W *tiene dimensión r (esto sucede cuando f es divisor de cero en $\mathbb{K}[V]$).*
- W *tiene dimensión pura $r-1$ (esto sucede cuando f no es divisor de cero ni unidad en $\mathbb{K}[V]$).*

En particular, si $F_1, \ldots, F_s$ son polinomios en $\mathbb{K}[X_1, \ldots, X_n]$ y $W := \mathcal{V}(F_1, \ldots, F_s) \subset \mathbb{A}^n$, entonces o bien $W = \emptyset$ o bien $\dim W \geq n - s$.

En el caso proyectivo tenemos el siguiente resultado.

Teorema 2.1.19 ([Sha94, Chapter 1, Section §2.6, Corollary 2])**.** *Sea $V \subset \mathbb{P}^n$ una variedad proyectiva de dimensión r y sea $W := \mathcal{V}(G_1, \ldots, G_s)$ una subvariedad de V. Entonces toda componente no vacía irreducible de W tiene dimensión por lo menos $r - s$.*

Un ideal propio I de un anillo Noetheriano R se dice **no mezclado** si sus primos asociados tienen todos la misma codimensión.

Definición 2.1.20. *Se dice que un anillo Noetheriano R satisface la condición de* pureza (*unmixedness*) *si todo ideal de codimensión r de R generado por r elementos es no mezclado para todo $r \geq 0$.*

Sea R un anillo Noetheriano e I un ideal de codimensión r de R generado por r elementos. Puesto que por el Teorema 2.1.17 todo ideal primo minimal de I tiene codimensión menor o igual que r, decir que I es no mezclado en la definición anterior equivale a decir que I no tiene primos asociados inmersos.

Un anillo Noetheriano que satisface la condición de pureza se dice que es **Cohen–Macaulay**. Un resultado clásico dice que los anillos de polinomios con coeficientes en un cuerpo son anillos Cohen–Macaulay (ver, por ejemplo, [Mat86, Theorems 17.6 and 17.7]).

A continuación consideramos una familia particular de $\mathbb{K}$–variedades definidas por ideales no mezclados, llamadas intersecciones completas.

Definición 2.1.21. *Sea V una $\mathbb{K}$–subvariedad afín de $\mathbb{A}^n$ de dimensión $n - r$.*

(i) Decimos que V es una intersección completa conjuntista *si V es la intersección de r $\mathbb{K}$–hipersuperficies.*

(ii) Decimos que V es una intersección completa *si $\mathcal{I}(V)$ puede ser generado por r polinomios en $\mathbb{K}[X_1, \ldots, X_n]$.*

Por la condición de pureza, una $\mathbb{K}$–subvariedad afín intersección completa conjuntista de $\mathbb{A}^n$ es necesariamente equidimensional.

Definición 2.1.22. *Sean $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$. Decimos que $F_1, \ldots, F_r$ forman una* sucesión regular *si F_1 no es el polinomio cero, ningún F_i es divisor de cero en el anillo $\mathbb{K}[X_1, \ldots, X_n]/(F_1, \ldots, F_{i-1})$ para $2 \leq i \leq r$ y $\mathcal{V}(F_1, \ldots, F_r) \neq \emptyset$.*

Si $F_1, \ldots, F_r$ forman una sucesión regular en $\mathbb{K}[X_1, \ldots, X_n]$ o $\mathbb{K}[X_0, \ldots, X_n]$, entonces la $\mathbb{K}$–variedad afín o proyectiva que ellos definen es una intersección completa conjuntista y es de dimensión pura $n - r$. Más aún, si el ideal $(F_1, \ldots, F_r)$ es radical entonces dicha variedad es una intersección completa.

2.1.2. Un criterio de radicalidad

Por último, enunciamos el siguiente criterio para decidir la radicalidad de un ideal. Por falta de una referencia adecuada ofrecemos aquí una demostración de este resultado, probablemente bien conocido.

Lema 2.1.23. *Sea $\mathbb{K}$ un cuerpo perfecto, $I := (F_1, \ldots, F_s) \subset \mathbb{K}[X_1, \ldots, X_n]$ un ideal de dimensión $n-s$, y J el ideal de $\mathbb{K}[X_1, \ldots, X_n]$ generado por I y los $(s \times s)$–menores de la matriz Jacobiana $(\partial F_i/\partial X_j)_{1 \leq i \leq s, 1 \leq j \leq n}$. Entonces, las siguientes condiciones son equivalentes:*

- *I es radical;*
- *J no está contenido en ningún primo minimal de I.*

Demostración. Sea $B := \mathbb{K}[X_1, \ldots, X_n]/I$. Por [Eis95, Exercise 11.10], basta probar que la segunda condición es equivalente a las siguientes:

1. la localización de B en cada primo de codimensión 0 es regular;
2. todos los primos asociados a cero en B tienen codimensión 0.

Para probar esta equivalencia, nótese que el homomorfismo canónico $\mathbb{K}[X_1, \ldots, X_n] \to B$ induce una biyección entre el conjunto de primos asociados a I y el conjunto de primos asociados a 0 en B. Esta biyección aplica los primos minimales sobre I en los primos minimales sobre 0 en B, que son precisamente los primos de codimensión 0 en B. Ahora, puesto que $\mathbb{K}[X_1, \ldots, X_n]$ satisface la condición de pureza, el ideal I es no mezclado, y por lo tanto el conjunto de primos asociados a I coincide con el conjunto de los primos minimales sobre I, lo que implica que se satisface (2). A continuación, la segunda condición del lema se puede expresar diciendo que la imagen $\overline{J}$ de J en B no está contenida en ningún primo de B de codimensión 0. Por [Eis95, Corollary 16.20], esto es equivalente a (1), lo que termina la demostración. □

2.1.3. Normalización de Noether

Sea $V \subset \mathbb{A}^n$ una intersección completa conjuntista de dimensión $n - s$ definida sobre $\mathbb{K}$. Sean $F_1, \ldots, F_s \in \mathbb{K}[X_1, \ldots, X_n]$ polinomios tales que $V = \mathcal{V}(F_1, \ldots, F_s)$. Puesto que $\mathbb{K}[X_1, \ldots, X_n]$ es Cohen–Macaulay, el ideal $I := (F_1, \ldots, F_s)$ es no mezclado y en particular V es equidimensional. Sean $Y_1, \ldots, Y_n \in \mathbb{K}[X_1, \ldots, X_n]$ formas lineales linealmente independientes tales que la aplicación $\pi : V \to \mathbb{A}^{n-s}$ definida por $Y_1, \ldots, Y_{n-s}$ es un morfismo finito. En tal caso, se dice que el cambio de variables $(X_1, \ldots, X_n) \to (Y_1, \ldots, Y_n)$ es una **normalización de Noether** de V (o I) y que las variables $Y_1, \ldots, Y_n$ están en **posición de Noether** con respecto a V (o I), siendo $Y_1, \ldots, Y_{n-s}$ las variables **libres**. Sea $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$ y denotemos con R' el cuerpo de fracciones de R. Escribamos $B := \mathbb{K}[X_1, \ldots, X_n]/I$ y sea $B' := R' \otimes_{\mathbb{K}} B := R'[Y_{n-s+1}, \ldots, Y_n]/I^e$, donde I^e es la extensión de I a $R'[Y_{n-s+1}, \ldots, Y_n]$. Consideramos a B como un R–módulo y a B' como un R'–espacio vectorial respectivamente. Puesto que B es finitamente generado, B' es un R'–espacio

vectorial de dimensión finita, cuya dimensión denotamos con $\dim_{R'} B'$. En particular, para todo $f \in \mathbb{K}[X_1, \ldots, X_n]$ podemos considerar el polinomio característico $\chi \in R'[T]$ (respectivamente el polinomio minimal de $\mu \in R'[T]$) de la homotecia de multiplicación por f en B'. Llamaremos a χ y a μ respectivamente el polinomio **característico** y el polinomio **minimal** de f módulo I. Sean χ_0 y μ_0 los coeficientes constantes de χ y μ respectivamente. Tenemos el siguiente resultado (ver, por ejemplo, [DL08]).

Lema 2.1.24. *Con las hipótesis y notaciones anteriores valen las siguientes condiciones:*

(*i*) χ *y* μ *pertenecen a* $R[T]$ *y* $\chi(f)$ *y* $\mu(f)$ *pertenecen a* I.

(*ii*) χ_0 *y* μ_0 *pertenecen a* $I + (f)$, *e* $\big(I + (f)\big) \cap R \subseteq \sqrt{(\mu_0)} = \sqrt{\chi_0}$.

(*iii*) f *es divisor de cero en* B *si y solo si* $\chi_0 = 0$ *(o equivalentemente* $\mu_0 = 0$*), si y solo si* $Y_1 \ldots Y_{n-s}$ *son algebraicamente independientes módulo* $I + (f)$.

(*iv*) $I + (f) = (1)$ *si y solo si* $\chi_0 \in \mathbb{K} \setminus \{0\}$ *(o equivalentemente* $\mu_0 \in \mathbb{K} \setminus \{0\}$*).*

Recordamos el siguiente resultado bien conocido (ver, por ejemplo, [GHS93, Lemma 3.3.1]).

Teorema 2.1.25. *Sea* $\mathbb{K}$ *un cuerpo perfecto, infinito y* $F_1, \ldots, F_s \in \mathbb{K}[X_1, \ldots, X_n]$ *polinomios que generan un ideal* $(F_1, \ldots, F_s)$ *de codimensión* s. *Supóngase que las variables* $X_1, \ldots, X_n$ *están en posición de Noether con respecto a* $(F_1, \ldots, F_s)$. *Entonces* $\mathbb{K}[X_1, \ldots, X_n]/(F_1, \ldots, F_s)$ *es un* $\mathbb{K}[X_1, \ldots, X_{n-s}]$*-módulo libre de rango finito.*

2.1.4. Representación de Kronecker de una variedad equidimensional

Sea $\mathbb{K}$ un cuerpo perfecto, infinito. Siguiendo con las notaciones anteriores, por el Teorema 2.1.25, B es un R–módulo libre de rango finito que denotamos con $\operatorname{rank}_R B$. Puesto que toda base de B como R–módulo induce una base de B' como R'–espacio vectorial, tenemos que $\operatorname{rank}_R B = \dim_{R'} B'$. En este caso decimos que $G \in \mathbb{K}[X_1, \ldots, X_n]$ induce un **elemento primitivo** para I si las potencias de la imagen g de G en B' generan el R'–espacio vectorial B'. En tal caso diremos también que G induce un elemento primitivo de la extensión de anillos $R \hookrightarrow B$.

Sea $V \subset \mathbb{A}^n$ una $\mathbb{K}$–variedad equidimensional de dimensión $n - s$ y sea $I \subset \mathbb{K}[X_1, \ldots, X_n]$ su ideal anulador. Para un cambio de variables $(X_1, \ldots, X_n) \to (Y_1, \ldots, Y_n)$, denótese $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$, $B := \mathbb{K}[V]$ y $R' := \mathbb{K}(Y_1, \ldots, Y_{n-s})$. Considérese $B' := R'[Y_{n-s+1}, \ldots, Y_n]/I^e$ como un R'–espacio vectorial, donde I^e denota el ideal extendido $IR'[Y_{n-s+1}, \ldots, Y_n]$, y sea $\delta := \dim_{R'} B'$.

Definición 2.1.26. *Una* representación de Kronecker *de* I *(o* V*) consiste de los siguientes elementos:*

- *una normalización de Noether de I, definida por un cambio lineal de variables $(X_1,\dots,X_n) \to (Y_1,\dots,Y_n)$ tal que Y_{n-s+1} induce un elemento primitivo para I;*
- *el polinomio (mónico) minimal $Q \in R'[T]$ de Y_{n-s+1} módulo I;*
- *los (únicos) polinomios $W_{n-s+2},\dots,W_n \in R'[T]$ de grado a lo sumo $\delta-1$ tales que la siguiente identidad de ideales vale en $R'[Y_{n-s+1},\dots,Y_n]$:*

$$I^e = \big(Q(Y_{n-s+1}), Q'(Y_{n-s+1})Y_{n-s+2} - W_{n-s+2}(Y_{n-s+1}),\dots, Q'(Y_{n-s+1})Y_n - Q_n(Y_{n-s+1})\big), \tag{2.1}$$

donde Q' denota la primera derivada de Q con respecto a T.

Si en cambio se consideran polinomios $V_{n-s+2},\dots,V_n \in R'[T]$ de grado a lo sumo $\delta-1$ tales que

$$I^e = \big(Q(Y_{n-s+1}), Y_{n-s+2} - V_{n-s+2}(Y_{n-s+1}),\dots, Y_n - V_n(Y_{n-s+1})\big), \tag{2.2}$$

se tiene una representación univariada *de I (o V).*

Observación 2.1.27. *Por el ítem (i) del Lema 2.1.24 el polinomio minimal Q de la definición anterior pertenece a $R[T]$.*

Si $Q' \neq 0$, la identidad (2.1) se puede interpretar en términos geométricos como se explica a continuación. Sea $\ell : \mathbb{A}^n \to \mathbb{A}^n$ la aplicación lineal definida por $Y_1,\dots,Y_n$ y $W := \ell(V)$. Interprétese a $Y_1,\dots,Y_n$ como nuevas indeterminadas y considérese la aplicación $\Pi : W \to \mathbb{A}^{n-s+1}$ definida por la proyección en las $n-s+1$ primeras coordenadas. Considerando a Q como un elemento de $\mathbb{K}[Y_1,\dots,Y_{n-s+1}]$ (Observación 2.1.27), resulta que Π define un isomorfismo birracional entre W y la hipersuperficie $\{Q=0\}$ de $\mathbb{A}^{n-s+1}$, cuya inversa es la aplicación racional $\Phi : \{Q=0\} \to W$ definida por

$$\Phi(\boldsymbol{y}) := \left(\boldsymbol{y}, \frac{W_{n-s+2}(\boldsymbol{y})}{Q'(\boldsymbol{y})},\dots,\frac{W_n(\boldsymbol{y})}{Q'(\boldsymbol{y})}\right).$$

Lema 2.1.28. *Con las hipótesis y notaciones previas a la Definición 2.1.26, sea $Q \in R[T]$ un polinomio libre de cuadrados de grado δ y $W_{n-s+2},\dots,W_n \in R[T]$ polinomios de grado a lo sumo $\delta-1$ tales que*

$$Q(Y_{n-s+1}) \in I, \quad Q'(Y_{n-s+1})Y_j - W_j(Y_{n-s+1}) \in I \quad (n-s+2 \le j \le n). \tag{2.3}$$

Entonces $Q, W_{n-s+2},\dots,W_n$ forman la representación de Kronecker de I con elemento primitivo Y_{n-s+1}. Además, sea $F := {Q'}^{-1} \mod (Q) \in R'[T]$ y $V_j \in R'[T]$ el polinomio con $\deg V_j \le \delta-1$ tal que $FW_j \equiv V_j \mod (Q)$ para $n-s+2 \le j \le n$. Entonces los polinomios $Q, V_{n-s+2},\dots,V_n$ forman la representación univariada de I con elemento primitivo Y_{n-s+1}.

Demostración. Puesto que Q es libre de cuadrados, Q' es inversible módulo Q. En particular $Q'(Y_{n-s+1})$ es inversible en $B' := R'[Y_{n-s+1},\dots,Y_n]/I^e$, y (2.3) muestra que el homomorfismo de R'–álgebras $R'[T]/(Q) \to B'$, que aplica $T \mod Q$ en

Y_{n-s+1} mód I^e, es suryectivo. Esto significa que Y_{n-s+1} es un elemento primitivo para I. Por otro lado, puesto que $\dim_{R'} B' = \delta$, el homomorfismo anterior es un isomorfismo. Concluimos que Q es el polinomio minimal de Y_{n-s+1} sobre R' módulo I^e.

Para probar (2.2) denotemos con $K \subseteq R'[Y_{n-s+1}, \ldots, Y_n]$ el ideal del lado derecho de esta identidad. Por (2.3) y la definición de $V_{n-s+2}, \ldots, V_n$ es claro que $K \subseteq I^e$. Para probar la otra inclusión sea $f \in R'[Y_{n-s+1}, \ldots, Y_n]$ un elemento de I^e. Desarrollando por Taylor a f en torno del punto $\big(Y_{n-s+1}, V_{n-s+2}(Y_{n-s+1}), \ldots, V_n(Y_{n-s+1})\big)$ deducimos que existe $h \in R'[T]$ tal que se satisface la siguiente congruencia en $R'[Y_{n-s+1}, \ldots, Y_n]$:

$$f \equiv h(Y_{n-s+1}) \mod \big(Y_{n-s+2} - V_{n-s+2}(Y_{n-s+1}), \ldots, Y_n - V_n(Y_{n-s+1})\big).$$

Esto implica que $h(Y_{n-s+1}) = 0$ en B' y por lo tanto que h es múltiplo del polinomio minimal Q. Concluimos que $f \in K$. Esto prueba que $I^e = K$, demostrando así la segunda afirmación del lema.

La primera afirmación se sigue de la igualdad de ideales

$$K = \big(Q(Y_{n-s+2}), Q'(Y_{n-s+1})Y_{n-s+2} - W_{n-s+2}(Y_{n-s+1}), \ldots, Q'(Y_{n-s+1})Y_n - W_n(Y_{n-s+1})\big),$$

la cual es una consecuencia inmediata de la definición $V_{n-s+2}, \ldots, V_n$ y de (2.3). □

2.1.5. Grado de una variedad

Sea V una $\mathbb{K}$–variedad irreducible. Se define el **grado** $\deg V$ de V como el número máximo de puntos en la intersección de V con una variedad lineal L de codimensión $\dim V$ para la cual dicha intersección es finita. Más generalmente, si $V = C_1 \cup C_2 \cup \cdots \cup C_r$ es la descomposición de V en componentes $\mathbb{K}$–irreducibles, definimos el grado de V como $\deg V := \sum_{i=1}^r \deg C_i$ (ver [Hei83]). El grado de una $\mathbb{K}$–hipersuperficie H es el grado de un polinomio de grado mínimo que define a H. El grado de un abierto denso contenido en una $\mathbb{K}$–variedad V es igual al grado de V. A continuación enunciamos una desigualdad de Bézout que usaremos para obtener las estimaciones (ver [Hei83, Ful84, Vog84]).

Teorema 2.1.29. *Si V y W son $\mathbb{K}$–variedades, entonces*

$$\deg(V \cap W) \leq \deg V \cdot \deg W. \tag{2.4}$$

Damos a continuación propiedades relacionadas con la noción de grado de $\mathbb{K}$–variedades.

(*i*) Sean $V \subset \mathbb{A}^n$, $\overline{V} \subset \mathbb{P}^n$ su clausura proyectiva y $\widehat{V} \subset \mathbb{A}^{n+1}$ el cono afín de $\overline{V}$. Se satisface (ver, por ejemplo, [CGH91, Proposition 1.11]):

$$\deg V = \deg \overline{V} = \deg \widehat{V}.$$

(*ii*) Sea $\phi : V \to W$ un morfismo lineal de $\mathbb{K}$–variedades. Entonces [Hei83, Lemma 2],

$$\deg \overline{\phi(V)} \leq \deg V \tag{2.5}$$

donde $\overline{\phi(V)}$ es la clausura de Zariski de $\phi(V)$ con respecto a la topología Zariski de W.

Sea $V \subset \mathbb{P}^n$ una $\mathbb{K}$–variedad intersección completa de grado δ y dimensión $n-r$, y sea $F_1, \ldots, F_r$ un conjunto de generadores de $\mathcal{I}(V)$ de grados $d_1, \ldots, d_r$ respectivamente. Los grados $d_1, \ldots, d_r$ dependen de V y no del sistema de generadores de $\mathcal{I}(V)$. Sin pérdida de generalidad, podemos suponer que $d_1 \geq \cdots \geq d_r$. Definimos entonces el **multigrado** de V como $\boldsymbol{d} := (d_1, \ldots, d_r)$. Un resultado fundamental sobre intersecciones completas es el **Teorema de Bézout**, que enunciamos a continuación (ver, por ejemplo, [Har92, Theorem 18.3]).

Teorema 2.1.30. *Sea $V \subset \mathbb{P}^n$ una intersección completa de grado δ, dimensión $n-r$ y sean $F_1, \ldots, F_r$ generadores de $\mathcal{I}(V)$ de grados $d_1 \geq \ldots \geq d_r$ respectivamente. Entonces*

$$\delta = \prod_{i=1}^{r} d_i.$$

2.1.6. Alturas

Decimos que un número racional $r/t \in \mathbb{Q}$, con $r, t \in \mathbb{Z}$ está en **forma canónica** si r/t es reducida y $t > 0$. Sea $q = r/t \in \mathbb{Q} \setminus \{0\}$ un número racional en forma canónica. La **altura** de q se define como la cantidad $h(q) := \max\{\log|r|, \log t\}$, donde log denota el logaritmo en base 2. Por lo tanto, la altura de q controla la longitud bit tanto del numerador como del denominador mínimos de q. Más generalmente, sea $\mathcal{A} \subset \mathbb{Q}$ un conjunto finito, y sea $a \in \mathbb{N}$ un denominador común mínimo para todos los elementos de $\mathcal{A}$. Entonces la altura de $\mathcal{A}$ se define como $h(\mathcal{A}) := \max\{\log|a\mathcal{A}|, \log a\}$. Finalmente, la altura $h(F)$ de un polinomio F con coeficientes en $\mathbb{Q}$ se define como la altura de su conjunto de coeficientes.

El siguiente resultado vincula la altura de polinomios con las operaciones aritméticas básicas y la composición ([DKS13, Lemma 2.37]).

Lema 2.1.31. *Sean $F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$. Entonces*

1. *$h(\sum_i F_i) \leq \max_i h(F_i) + \log(s)$;*
2. *$h(\prod_i F_i) \leq \sum_i h(F_i) + \log(n+1) \sum_{i=2}^{s} \deg(F_i)$;*
3. *sea $G \in \mathbb{Z}[Y_1, \ldots, Y_s]$ y nótese $d := \max_i \deg(F_i)$ y $h := \max_i h(F_i)$. Entonces $h\big(G(F_1, \ldots, F_s)\big) \leq h(G) + \deg(G)\big(h + \log(s+1) + d\log(n+1)\big)$.*

Altura de variedades

Recordamos aquí brevemente la noción de altura de variedades equidimensionales definidas sobre $\mathbb{Q}$. Para más detalles ver [KPS01] y [DKS13]. Sea $V \subset \mathbb{A}^n(\overline{\mathbb{Q}})$ una $\mathbb{Q}$–variedad equidimensional de dimensión $n-s$, con $1 \leq s \leq n$, y sea $h(V)$ la altura de Faltings de su clausura proyectiva $\overline{V} \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ (ver [Fal91]). Tenemos la siguiente identidad:

$$h(V) = m(F_V; S_{n+1}^{n-s+1}) + \sum_p \log |F_V|_p + (n-s+1)\left(\sum_{i=1}^{n} \frac{1}{2i}\right) \deg V, \tag{2.6}$$

donde F_V es una forma de Chow de V, $m(F_V; S_{n+1}^{n-s+1})$ es la S_{n+1}^{n-s+1}–**medida de Mahler** de F_V y $|F_V|_p$ es el valor absoluto p–ádico sobre $\mathbb{Q}$ para todos los primos p (ver, por ejemplo, [KPS01, Section 1.2.4]). Puesto que F_V está unívocamente determinada salvo multiplicación por elementos no nulos de $\mathbb{Q}$, podemos suponer que F_V es un polinomio primitivo en $\mathbb{Z}[\mathbf{\Lambda}_1^h, \ldots, \mathbf{\Lambda}_{n-s+1}^h]$, en cuyo caso $\log |F_V|_p = 0$ para todo primo p y la suma $\sum_p \log |F_V|_p$ en (2.6) desaparece. Por otra parte, por [KPS01, Lemma 1.1] tenemos que

$$|m(F_V) - h(F_V)| \leq (n-s+1)\log(n+2)\deg V, \tag{2.7}$$

donde $m(F_V)$ denota la **medida de Mahler** de F_V. La medida de Mahler y la S_{n+1}^{n-s+1}–medida de Mahler de F_V están relacionadas por las desigualdades

$$0 \leq m(F_V) - m(F_V; S_{n+1}^{n-s+1}) \leq (n-s+1)\deg(V) \sum_{i=1}^{n} \frac{1}{2i} \tag{2.8}$$

(ver, por ejemplo, [KPS01, (1.2)]). Combinando (2.6), (2.7) y (2.8) resulta

$$h(F_V) \leq h(V) + (n-s+1)\log(n+2)\deg V.$$

Además, la **altura canónica** $\widehat{h}(V)$ de V se define por $\widehat{h}(V) := \widehat{h}(\overline{V})$, donde $\widehat{h}(V)$ es la altura canónica de $\overline{V} \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ definida como en [DKS13]. Las alturas de Faltings y canónica de V están relacionadas por la desigualdad

$$|\widehat{h}(V) - h(V)| \leq \frac{7}{2}\log(n+1)\deg V \tag{2.9}$$

(ver, por ejemplo, [DKS13, Proposition 2.39 (5)]). En consecuencia, tenemos que

$$h(F_V) \leq \widehat{h}(V) + \frac{9}{2}(n-s+1)\log(n+2)\deg V. \tag{2.10}$$

Finalmente, sean $F_1, \ldots, F_s \in \mathbb{Q}[\boldsymbol{X}]$ polinomios que forman una sucesión regular. Sea $d_j := \deg(F_j)$ y $h_j := h(F_j)$ para $1 \leq j \leq s$. Por [DKS13, Corollary 2.62], teniendo en cuenta [DKS13, Lemma 2.30 (1)], obtenemos la siguiente **desigualdad de Bézout aritmética**:

$$\widehat{h}\big(V(F_1, \ldots, F_s)\big) \leq \sum_{\ell=1}^{s} h_\ell \left(\prod_{j=1, j\neq\ell}^{s} d_j\right) + s\left(\prod_{j=1}^{s} d_j\right)\log(n+2). \tag{2.11}$$

2.2. Estructuras de datos y algoritmos básicos

Para expresar el costo de los algoritmos, además de la notación Big–Oh $\mathcal{O}$, también utilizamos la notación estándar Soft–Oh $\mathcal{O}^{\sim}$ que omite términos logaritmicos (ver, por ejemplo, [vzGG99, Appendix]).

2.2.1. Straight–line programs

Los algoritmos en geometría algebraica computacional se describen usualmente usando el modelo de complejidad denso estándar (o ralo), es decir, codificando los polinomios multivariados por medio del vector de todos los coeficientes (o de todos los coeficientes no nulos). Teniendo en cuenta que un polinomio n–variado genérico de grado $d \geq 2$ tiene $\binom{d+n}{n} = O(d^n)$ coeficientes no nulos, vemos que la representación densa de polinomios multivariados requiere un tamaño exponencial, y su manipulación usualmente requiere un número exponencial de operaciones aritméticas con respecto a los parámetros d y n. Para evitar este comportamiento, vamos a usar codificaciones alternativas de las entradas y de los resultados intermedios de nuestros cálculos por medio de straight–line programs (ver [BCS97]). Sea $\mathbb{K}$ un cuerpo arbitrario y $\boldsymbol{X} := (X_1, \ldots, X_n)$ una tupla de indeterminadas sobre $\mathbb{K}$. Un **straight–line program** β sobre $\mathbb{K}(\boldsymbol{X})$ es una sucesión finita de funciones racionales $(F_1, \ldots, F_k) \in \mathbb{K}(\boldsymbol{X})^k$ tales que para $1 \leq i \leq k$, la función F_i es un elemento del conjunto $\{X_1, \ldots, X_n\}$ (una **entrada**), o un elemento de $\mathbb{K}$ (un **parámetro**), o existen $1 \leq i_1, i_2 < i$ tales que $F_i = F_{i_1} \circ_i F_{i_2}$, donde $\circ_i$ es una de las operaciones aritméticas $+, -, \times, \div$. Las entradas y los parámetros se consideran de libre acceso (modelo de acceso aleatorio). Los elementos del conjunto $\{F_1, \ldots, F_k\}$ se llaman **resultados intermedios** de β. El straight–line program β se llama (esencialmente) **sin divisiones**, si las divisiones se restringen a parámetros no nulos, es decir, si para $1 \leq i \leq k$, o bien $\circ_i \in \{+, -, \times\}$ o bien $\circ_i = \div$ y $f_{i_2} \in \mathbb{K} \setminus \{0\}$. Obsérvese que, si β es sin divisiones, los resultados intermedios de β pertenecen al anillo de polinomios $\mathbb{K}[\boldsymbol{X}]$.

Una medida natural de la complejidad de β es su **longitud**, es decir, el número total de operaciones aritméticas realizadas durante el proceso de evaluación definido por β. Otra medida relevante de complejidad es la **longitud no escalar** de β, que se define como el número de operaciones $\circ_i \in \{\times, \div\}$ con $f_{i_1}, f_{i_2} \notin \mathbb{K}$ para $\circ_i = \times$ y $f_{i_2} \notin \mathbb{K}$ para $\circ_i = \div$. La longitud (no escalar) de β modeliza el tiempo de ejecución secuencial del programa.

Decimos que el straight–line program β **calcula**, **evalúa**, **representa**, o **codifica** un subconjunto S de $\mathbb{K}(\boldsymbol{X})$ si S está contenido en la lista de resultados intermedios $\{F_1, \ldots, F_k\}$ de β. En este caso llamamos a los elementos de S **salidas** de β.

También utilizamos la representación mixta de un polinomio multivariado con respecto a una variable distinguida. Sea $F \in \mathbb{K}[\boldsymbol{X}]$ un polinomio de grado a lo sumo d. Fijamos $1 \leq k \leq n$ y consideramos a F como un polinomio en X_k con coeficientes en el anillo de polinomios $\mathbb{K}[X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n]$. Sean $F_0, \ldots, F_d$ los polinomios en $\mathbb{K}[X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n]$ definidos por $F = \sum_{0 \leq j \leq d} F_j X_k^j$. Una **representación mixta** de F con respecto a la **variable distinguida** X_k es

un straight–line program β sobre $\mathbb{K}[X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n]$ que representa los polinomios $F_0, \ldots, F_d$.

2.2.2. Tests de Zippel Schwartz

Los algoritmos de resolución de sistemas polinomiales y de interpolación implícita que consideramos en esta tesis son probabilísticos, de tipo *Monte Carlo* (ver, por ejemplo, [vzGG99]). Uno de los aspectos probabilísticos de estos algoritmos está relacionado con la elección aleatoria de puntos fuera de ciertos conjuntos cerrados Zariski. Una herramienta básica para estimar la probabilidad de éxito de estas elecciones es el siguiente resultado (ver, por ejemplo, [vzGG99, Lemma 6.44]).

Lema 2.2.1. *Sea R un dominio íntegro, $U_1, \ldots, U_k$ indeterminadas sobre R, $S \subseteq R$ un conjunto finito con $s := \#S$ elementos y $F \in R[U_1, \ldots, U_k]$ un polinomio no nulo de grado a lo sumo d. Entonces F tiene a lo sumo ds^{k-1} ceros en S^k.*

Interpretamos el Lema 2.2.1 en términos de probabilidades de la siguiente manera: para un elemento $\boldsymbol{u}$ elegido uniformemente al azar en S^k, $F(\boldsymbol{u}) \neq 0$ con probabilidad mayor a $1 - d/s$.

El segundo aspecto probabilístico se relaciona con la elección de un primo "lucky" p. A este respecto tenemos el siguiente resultado (ver, por ejemplo, [vzGG99, Section 18.4]).

Lema 2.2.2. *Sean B y m enteros positivos y M un entero no nulo tal que $\log |M| \leq \frac{B}{m}$. Existe un algoritmo probabilístico que, a partir de B y un entero positivo k, calcula un primo p con $B < p \leq 2B$ tal que p no divide a M. El algoritmo realiza $\mathcal{O}^{\sim}(k \log^2 B)$ operaciones bit y entrega un resultado correcto con probabilidad al menos*

$$\Big(1 - \frac{\log B}{2^{k-1}}\Big)\Big(1 - \frac{2}{m}\Big).$$

Demostración. De acuerdo con, por ejemplo, [vzGG99, Theorem 18.8], existe un algoritmo probabilístico que calcula un primo aleatorio p tal que $B < p \leq 2B$ con $\mathcal{O}^{\sim}(k \log^2 B)$ operaciones bit y probabilidad de éxito al menos $1 - \log B/2^{k-1}$. Por otra parte, si p es un primo aleatorio con $B < p \leq 2B$, entonces p no divide a M con probabilidad al menos $1 - 2/m$. Combinando ambas afirmaciones se deduce el lema. □

2.2.3. Costo de los algoritmos básicos

A continuación discutimos el costo de los algoritmos básicos que vamos a utilizar. El costo de los mismos se expresará en términos de las cantidades

$$\mathcal{M}(\delta) := \delta \log(\delta) \log\log(\delta), \quad \mathcal{U}(\delta) := \mathcal{M}(\delta) \log \delta.$$

Sea R un anillo conmutativo con unidad. El número de operaciones aritméticas (adición, multiplicación y división) en R requerido para multiplicar dos polinomios univariados en $R[T]$ de grado menor que D es $\mathcal{O}\big(\mathcal{M}(D)\big)$. Sea $q \in R[T]$ un polinomio

mónico de grado D. Representamos los elementos del anillo cociente $R[T]/(q)$ de forma natural como polinomios univariados de grados menores que D. Entonces una multiplicación en $R[T]/(q)$ se puede realizar con $\mathcal{O}\big(\mathcal{M}(D)\big)$ operaciones aritméticas en R (ver, por ejemplo, [BP94], [vzGG99]).

También utilizamos algoritmos para la multiplicación transpuesta en $R[T]/(q)$ sobre R: dado $f \in R[T]/(q)$ y un vector $\boldsymbol{v} \in R^D$, la **multiplicación transpuesta** de f y v es el el único vector $\boldsymbol{w} \in R^D$ que satisface $\langle \boldsymbol{w}, g\rangle = \langle \boldsymbol{v}, fg\rangle$ para todo $g \in R[T]/(q)$. Aquí, $\langle \cdot, \cdot \rangle$ denota el producto interno, que se define por $\langle \boldsymbol{x}, \boldsymbol{y}\rangle = \sum_{j=1}^{D} x_j y_j$ para $\boldsymbol{x}, \boldsymbol{y} \in R^D$. Consecuentemente, identificamos todo elemento de $R[T]/(q)$ con el vector de coeficientes de su representante. Por medio del algoritmo descripto en [Sho99], el vector $\boldsymbol{w}$ se puede calcular, a partir de f y $\boldsymbol{v}$, con $\mathcal{O}(\mathcal{M}(D))$ operaciones aritméticas en R.

El determinante de una matriz de tamaño $n \times n$ con coeficientes en R se puede calcular sin usar divisiones con $\mathcal{O}(n^4)$ operaciones en R (ver [FF63]).

Si R es un cuerpo, utilizamos algoritmos basados en el Algoritmo de Euclides extendido para calcular el máximo común divisor de dos polinomios univariados en $R[T]$ de grado menor que D con $\mathcal{O}\big(\mathcal{U}(D)\big)$ operaciones aritméticas en R (ver, por ejemplo, [BP94], [vzGG99]).

La complejidad bit de una operación aritmética (adición, multiplicación, cociente, resto y máximo común divisor) de dos enteros de altura a lo sumo n es $\mathcal{O}\big(\mathcal{U}(n)\big)$. Además, dado un entero positivo m de altura n, una operación aritmética (adición, multiplicación e inversión o división) en el anillo cociente $\mathbb{Z}/m\mathbb{Z}$ de los enteros módulo m se puede realizar con $\mathcal{O}\big(\mathcal{U}(n)\big)$ operaciones bit.

También usamos el siguiente algoritmo de reconstrucción racional (ver [Knu81], [Dix82], [vzGG99]).

Proposición 2.2.3. *Sea $r/t \in \mathbb{Q}$ la forma canónica de un número racional y $g, m \in \mathbb{Z}$ con $0 \leq g < m$ tales que se satisfacen las siguientes condiciones:*

- $m \geq 2\,\mathrm{máx}\{|r|, t\}^2$.
- *t y m son coprimos y $rt^{-1} \equiv g \mod (m)$, donde t^{-1} es la inversa de t módulo m.*

Entonces, por medio del Algoritmo de Euclides extendido aplicado a m y g, podemos calcular la forma canónica r/t con $\mathcal{O}\big(\mathcal{U}(\log m)\big)$ operaciones bit.

Capítulo 3

La forma de Chow de una variedad equidimensional

Sea $\mathbb{K}$ un cuerpo perfecto y $V \subset \mathbb{A}^n$ una $\mathbb{K}$–variedad equidimensional de dimensión $n-s$ y grado δ. En este capítulo recordamos la noción de forma de Chow de V y sus propiedades básicas.

Sea $\mathbf{\Lambda}^h := (\Lambda_{ij})_{1\leq i\leq n-s+1, 0\leq j\leq n}$ una matriz de indeterminadas sobre $\mathbb{K}[V]$; escribamos $\mathbf{\Lambda}_i^h := (\Lambda_{i0}, \ldots, \Lambda_{in})$ y $\mathbf{\Lambda}_i := (\Lambda_{i1}, \ldots, \Lambda_{in})$ para $1 \leq i \leq n-s+1$. Denotemos con $\boldsymbol{X} := (X_1, \ldots, X_n)$ un conjunto de indeterminadas sobre $\mathbb{K}$. Una **forma de Chow** de V es un polinomio libre de cuadrados F_V de $\mathbb{K}[\mathbf{\Lambda}^h]$ tal que $F_V(\boldsymbol{\lambda}^h) = 0$ si y solo si $\overline{V} \cap \{\lambda_{i0} + \sum_{j=1}^n \lambda_{ij} X_j = 0 \ (1 \leq i \leq n-s+1)\}$ es no vacío, donde $\overline{V} \subset \mathbb{P}^n$ es la clausura proyectiva de V con respecto a la inclusión canónica $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$ (ver [HP68b, Chapter X, Section 6]). Observamos que F_V es multihomogéneo de grado δ en cada grupo de variables $\mathbf{\Lambda}_i^h$ para $1 \leq i \leq n-s+1$, y que este polinomio está unívocamente determinado salvo múltiplos no nulos en $\mathbb{K}$. Escribamos $\mathbf{\Lambda} := (\Lambda_{ij})_{1\leq i\leq n-s+1, 1\leq j\leq n}$ y sean $Z_1, \ldots, Z_{n-s+1}$ nuevas indeterminadas. Sea $P_V \in \mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s+1}]$ el único polinomio tal que

$$P_V(\mathbf{\Lambda}, \Lambda_{10}, \ldots, \Lambda_{n-s+1,0}) = F_V(\mathbf{\Lambda}_1^h, \ldots, \mathbf{\Lambda}_{n-s+1}^h).$$

Por abuso de lenguaje también llamaremos a P_V una forma de Chow de V.

Sean $\xi_1, \ldots, \xi_n$ las funciones coordenadas de V inducidas por $X_1, \ldots, X_n$. Escribamos $\boldsymbol{\xi} := (\xi_1, \ldots, \xi_n)$ y sea $\mathbf{\Lambda}_i \cdot \boldsymbol{\xi} \in \mathbb{K}[V][\mathbf{\Lambda}]$ definida por

$$\mathbf{\Lambda}_i \cdot \boldsymbol{\xi} := \sum_{j=1}^n \Lambda_{ij} \xi_j \quad (1 \leq i \leq n-s+1).$$

Una propiedad fundamental de la forma de Chow P_V es que está unívocamente determinada, salvo multiplicación por elementos no nulos de $\mathbb{K}$, por las siguientes dos condiciones:

- Si $\mathbf{\Lambda}\boldsymbol{\xi} := (\mathbf{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \mathbf{\Lambda}_{n-s+1} \cdot \boldsymbol{\xi})$, se satisface la siguiente identidad en $\mathbb{K}[V][\mathbf{\Lambda}]$:

$$P_V(\mathbf{\Lambda}, \mathbf{\Lambda}\boldsymbol{\xi}) = 0. \tag{3.1}$$

Equivalentemente, sea $\mathbf{\Lambda}_i \cdot \boldsymbol{X} := \sum_{j=1}^{n} \Lambda_{ij} X_j$ para $1 \leq i \leq n-s+1$ y $\mathbf{\Lambda}\boldsymbol{X} := (\mathbf{\Lambda}_1 \cdot \boldsymbol{X}, \ldots, \mathbf{\Lambda}_{n-s+1} \cdot \boldsymbol{X})$. Entonces el polinomio $P_V(\mathbf{\Lambda}, \mathbf{\Lambda}\boldsymbol{X}) \in \mathbb{K}[\mathbf{\Lambda}, \boldsymbol{X}]$ se anula sobre la variedad $\mathbb{A}^{(n-s+1)n} \times V$.

- Si $G \in \mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s+1}]$ es un polinomio tal que $G(\mathbf{\Lambda}, \mathbf{\Lambda}\boldsymbol{\xi}) = 0$, entonces P_V divide a G en $\mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s+1}]$.

Además, F_V satisface las siguientes propiedades (ver [HP68b, Chapter X, Sections 7 y 9]):

1. F_V es homogéneo de grado δ en los $(n-s+1) \times (n-s+1)$–menores de $\mathbf{\Lambda}^h$;
2. $\deg_{(\Lambda_{10}, \ldots, \Lambda_{n-s+1,0})} F_V = \deg_{\Lambda_{n-s+1,0}} F_V = \delta$;
3. Si V es una $\mathbb{K}$–variedad irreducible, entonces F_V es un polinomio irreducible de $\mathbb{K}[\mathbf{\Lambda}^h]$. Más generalmente, si $V = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_N$ es la descomposición de V en componentes $\mathbb{K}$–irreducibles y $F_{\mathcal{C}_i}$ es una forma de Chow de $\mathcal{C}_i$ para $1 \leq i \leq N$, entonces $\prod_{1 \leq i \leq N} F_{\mathcal{C}_i}$ es una forma de Chow de V.

Observación 3.0.1. *Sea $A_V \in \mathbb{K}[\mathbf{\Lambda}_1^h, \ldots, \mathbf{\Lambda}_{n-s}^h]$ el polinomio (no nulo) que aparece como el coeficiente del monomio $\Lambda_{n-s+1,0}^{\delta}$ en F_V, considerando a F_V como un elemento de $\mathbb{K}[\mathbf{\Lambda}][\Lambda_{10}, \ldots, \Lambda_{n-s+1,0}]$. Entonces la propiedad (2) arriba indicada implica que A_V es independiente de $\Lambda_{10}, \ldots, \Lambda_{n-s\,0}$, es decir, $A_V \in \mathbb{K}[\mathbf{\Lambda}_1, \ldots, \mathbf{\Lambda}_{n-s}]$. En particular, A_V es homogéneo de grado δ en los $(n-s) \times (n-s)$–menores de la matriz $\mathbf{\Lambda}^* = (\Lambda_{ij})_{1 \leq i \leq n-s, 1 \leq j \leq n}$.*

Sea $\rho_V \in \mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s}]$ el discriminante de P_V con respecto a Z_{n-s+1}, a saber

$$\rho_V := \mathrm{Res}_{Z_{n-s+1}} \left(P_V, \frac{\partial P_V}{\partial Z_{n-s+1}} \right).$$

Lema 3.0.2. *ρ_V y $\partial P_V / \partial Z_{n-s+1}$ son ambos no nulos.*

Demostración. Notemos que $A := \mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s+1}]/(P_V)$ es una $\mathbb{K}$–álgebra reducida. Como $\mathbb{K}$ es perfecto, por [Mat80, Corollary, página 194] se deduce que A es una $\mathbb{K}$–álgebra separable. Sea $\mathbb{K}'$ la clausura algebraica de $\mathbb{K}(\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s})$. Por [Mat80, 27.G] se deduce que la $\mathbb{K}'$–álgebra $A \otimes_{\mathbb{K}} \mathbb{K}' = \mathbb{K}'[Z_{n-s+1}]/(P_V)$ es reducida. Como $\mathbb{K}'$ es un cuerpo perfecto, esto implica que $\partial P_V / \partial Z_{n-s+1} \neq 0$. Ahora, por las propiedades (2) y (3) arriba indicadas, cada factor irreducible de P_V es una forma de Chow de una componente irreducible $\mathcal{C}_i$ de V, de grado $\deg \mathcal{C}_i$ en Z_{n-s+1}. Entonces el argumento previo muestra que la derivada parcial con respecto a Z_{n-s+1} de cada factor irreducible de P_V no se anula, lo que a su vez implica que P_V y $\partial P_V / \partial Z_{n-s+1}$ son polinomios coprimos de $\mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s+1}]$. Como $\mathbb{K}[\mathbf{\Lambda}, Z_1, \ldots, Z_{n-s}]$ es un anillo factorial, esto implica que la resultante ρ_V de estos polinomios no se anula. □

Además, ρ_V satisface las siguientes estimaciones de grado:

$$\deg_{(Z_1, \ldots, Z_{n-s})} \rho_V \leq (2\delta - 1)\delta, \quad \deg_{\mathbf{\Lambda}_i} \rho_V \leq (2\delta - 1)\delta \quad (1 \leq i \leq n-s+1).$$

En particular, se tiene $\deg \rho_V \leq (n-s+2)(2\delta^2-\delta)$.

Sea $\boldsymbol{Z} := (Z_1, \ldots, Z_{n-s+1})$. Para cada $\boldsymbol{\lambda} := (\lambda_{ij})_{1\leq i\leq n-s+1, 1\leq j\leq n} \in \mathbb{A}^{(n-s+1)n}$, escribimos $\boldsymbol{\lambda}_i := (\lambda_{i1}, \ldots, \lambda_{in})$ y $\boldsymbol{\lambda}_i \cdot \boldsymbol{\xi} := \sum_{j=1}^{n} \lambda_{ij}\xi_j$ para $1 \leq i \leq n-s+1$. Consideramos a $\mathbb{K}[V][\boldsymbol{\Lambda}]$ como una $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$–álgebra por medio del homomorfismo de anillos $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}] \to \mathbb{K}[V][\boldsymbol{\Lambda}]$ que aplica cada $F \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ en $F(\boldsymbol{\Lambda}, \boldsymbol{\Lambda\xi})$. En estos términos, tenemos el siguiente resultado.

Lema 3.0.3. *$\partial P_V/\partial Z_{n-s+1}$ no es un divisor de cero de la $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$–álgebra $\mathbb{K}[V][\boldsymbol{\Lambda}]$.*

Demostración. Sea $G \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{X}]$ un polinomio arbitrario tal que

$$\frac{\partial P_V}{\partial Z_{n-s+1}}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda\xi}) \cdot G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) = 0 \tag{3.2}$$

en $\mathbb{K}[V][\boldsymbol{\Lambda}]$. Puesto que $\rho_V \in (P_V, \partial P_V/\partial Z_{n-s+1})\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$, de la identidad $P_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda\xi}) = 0$ deducimos que $\rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi})$ es un múltiplo de $\partial P_V/\partial Z_{n-s+1}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda\xi})$ en $\mathbb{K}[V][\boldsymbol{\Lambda}]$. Combinando esto con (3.2) deducimos que

$$\rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi}) \cdot G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) = 0$$

en $\mathbb{K}[V][\boldsymbol{\Lambda}]$. Supongamos que existe una componente $\mathbb{K}$–irreducible $\mathcal{C}$ de V tal que $G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) \neq 0$ en $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$. En $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$ tenemos la identidad:

$$\rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi}) \cdot G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) = 0.$$

Puesto que $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$ es un dominio íntegro concluimos que $\rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi}) = 0$ en $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$. Esto implica que

$$\rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi}) = 0 \tag{3.3}$$

en $\overline{\mathbb{K}}[\mathcal{C}][\boldsymbol{\Lambda}]$, donde $\overline{\mathbb{K}}$ denota la clausura algebraica de $\mathbb{K}$. Por otra parte, por el Lemma 3.0.2 el polinomio ρ_V es no nulo. Luego, para una elección genérica de $\boldsymbol{\lambda} \in \mathbb{A}^{(n-s+1)n}$, la extensión de anillos $\overline{\mathbb{K}}[\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}] \hookrightarrow \overline{\mathbb{K}}[V]$ es entera y $\rho_V(\boldsymbol{\lambda}, Z_1, \ldots, Z_{n-s})$ es un polinomio no nulo en $\overline{\mathbb{K}}[Z_1, \ldots, Z_{n-s}]$. Por (3.3) deducimos que $\rho_V(\boldsymbol{\lambda}, \boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}) = 0$ en $\overline{\mathbb{K}}[\mathcal{C}]$, lo que muestra que $\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}$ son algebraicamente dependientes sobre $\overline{\mathbb{K}}$. Puesto que la extensión de anillos $\overline{\mathbb{K}}[\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}] \hookrightarrow \overline{\mathbb{K}}[\mathcal{C}]$ también es entera, se sigue que $\dim \mathcal{C} \leq n-s-1$, lo que es una contradicción. Por lo tanto $G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) = 0$ en $\mathbb{K}[\mathcal{C}][\boldsymbol{\Lambda}]$ para cada componente irreducible $\mathcal{C}$ de V. Concluimos que $G(\boldsymbol{\Lambda}, \boldsymbol{\xi}) = 0$ en $\mathbb{K}[V][\boldsymbol{\Lambda}]$, lo que concluye la demostración. □

3.1. Una condición genérica para una normalización de Noether

En lo que sigue, para $\boldsymbol{\lambda} := (\lambda_{ij})_{1\leq i\leq n-s+1, 1\leq j\leq n} \in \mathbb{K}^{(n-s+1)n}$ escribimos $\boldsymbol{\lambda}^* := (\lambda_{ij})_{1\leq i\leq n-s, 1\leq j\leq n}$.

Proposición 3.1.1. *Con las hipótesis y notaciones anteriores, sea* $\boldsymbol{\lambda} \in \mathbb{K}^{(n-s+1)n}$ *tal que* $A_V(\boldsymbol{\lambda}^*) \neq 0$. *Sea* $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ *para* $1 \leq i \leq n-s+1$, $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$, $B := \mathbb{K}[V]$, $R' := \mathbb{K}(Y_1, \ldots, Y_{n-s})$ *y* $B' := R' \otimes_{\mathbb{K}} B$. *Entonces la aplicación* $\pi : V \to \mathbb{A}^{n-s}$ *definida por* $Y_1, \ldots, Y_{n-s}$ *es un morfismo finito. Si además* $\rho_V(\boldsymbol{\lambda}, Z_1, \ldots, Z_{n-s}) \neq 0$, *entonces* Y_{n-s+1} *induce un elemento primitivo de la extensión de anillos* $R \hookrightarrow \mathbb{K}[V]$ *y* $\dim_{R'} B' \leq \delta$.

Demostración. Sea $\boldsymbol{\Lambda}^* = (\Lambda_{ij})_{1 \leq i \leq n-s, 1 \leq j \leq n}$. Recordemos que A_V es homogéneo de grado δ en los $(n-s)\times(n-s)$–menores de $\boldsymbol{\Lambda}^*$. Puesto que $A_V(\boldsymbol{\lambda}^*) \neq 0$, al menos uno de los $(n-s)\times(n-s)$–menores de la matriz $\boldsymbol{\lambda}^*$ es no nulo. Deducimos que las formas lineales $Y_1, \ldots, Y_{n-s}$ son linealmente independientes. Por lo tanto existen formas lineales $Y_{n-s+1}, \ldots, Y_n \in \mathbb{K}[\boldsymbol{X}]$ tales que $Y_1, \ldots, Y_{n-s}, Y_{n-s+1}, \ldots, Y_n$ son linealmente independientes. Sea $\boldsymbol{w}_k := (w_{k1}, \ldots, w_{kn}) \in \mathbb{K}^n$ tal que $Y_{n-s+k} = \boldsymbol{w}_k \cdot \boldsymbol{X}$ para $1 \leq k \leq s$. Sea $Q_k \in \mathbb{K}[Z_1, \ldots, Z_{n-s+1}]$ el polinomio que se obtiene al sustituir en P_V la matriz $\boldsymbol{\Lambda}$ por $(\boldsymbol{\lambda}^*, \boldsymbol{w}_k)$. A partir de (3.1) deducimos que

$$Q_k(Y_1, \ldots, Y_{n-s}, \boldsymbol{w}_k \cdot \boldsymbol{\xi}) = 0 \tag{3.4}$$

en la R–álgebra B para $1 \leq k \leq s$, donde $\boldsymbol{\xi} := (\xi_1, \ldots, \xi_n)$ denota la n–tupla de funciones coordenadas en B inducidas por $X_1, \ldots, X_n$. Obsérvese que $\deg_{Z_{n-s+1}} Q_k \leq \delta$ y que $A_V(\boldsymbol{\lambda}^*)$ es el coeficiente de Z_{n-s+1}^{δ} en Q_k. Puesto que $A_V(\boldsymbol{\lambda}^*) \neq 0$, resulta $\deg_{Z_{n-s+1}} Q_k = \delta$ y (3.4) puede ser interpretado como una relación de dependencia entera para la imagen $\boldsymbol{w}_k \cdot \boldsymbol{\xi}$ de Y_{n-s+k} en B sobre R para $1 \leq k \leq s$. Más aun, $\mathbb{K}[Y_1, \ldots, Y_n] = \mathbb{K}[\boldsymbol{X}]$ puesto que las formas lineales $Y_1, \ldots, Y_n$ son linealmente independientes. Esto implica que $R \to B$ es una extensión entera de anillos.

Para probar que π es finita, sea $\mathcal{C}$ una componente $\mathbb{K}$–irreducible de V y $\pi_{\mathcal{C}}$ la restricción de π a $\mathcal{C}$. Es suficiente probar que $\pi_{\mathcal{C}}$ es dominante o, equivalentemente, que su homomorfismo de anillos dual $\pi_{\mathcal{C}}^* : \mathbb{K}[\mathbb{A}^{n-s}] \to \mathbb{K}[\mathcal{C}]$ es inyectivo. Denotemos con t_i a la i–ésima función coordenada de $\mathbb{A}^{n-s}$ para $1 \leq i \leq n-s$. Con un ligero abuso de notación denotemos también con $\boldsymbol{\xi}$ a la n–tupla de funciones coordenadas de $\mathbb{K}[\mathcal{C}]$ inducidas por $X_1, \ldots, X_n$. Así, $\pi_{\mathcal{C}}^*(t_i) = \boldsymbol{\lambda}_i \cdot \boldsymbol{\xi}$ para $1 \leq i \leq n-s$. Puesto que $\mathbb{K}[\mathcal{C}]$ es entero sobre $\mathbb{K}[\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}]$ y $\dim \mathcal{C} = n-s$, deducimos que $\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}$ son algebraicamente independientes sobre $\mathbb{K}$. Esto implica la inyectividad de $\pi_{\mathcal{C}}^*$, lo que concluye la demostración de la primera afirmación de la proposición.

A continuación, tomando derivadas parciales con respecto a las variables $\Lambda_{n-s+1,k}$ en ambos miembros de (3.1), obtenemos la siguiente identidad en $\mathbb{K}[V][\boldsymbol{\Lambda}]$ para $1 \leq k \leq n$:

$$\frac{\partial P_V}{\partial Z_{n-s+1}}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi})\, \xi_k + \frac{\partial P_V}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi}) = 0. \tag{3.5}$$

A partir (3.1) y (3.5) deducimos que existe $R_k \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ tal que

$$\rho_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{\xi})\, \xi_k = R_k(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi}) \tag{3.6}$$

en $\mathbb{K}[V][\boldsymbol{\Lambda}]$ para $1 \leq k \leq n$. Sustituyendo $\boldsymbol{\Lambda}$ por $\boldsymbol{\lambda}$ en (3.6) deducimos que

$$\rho_V(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s})\xi_k = R_k(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s}, \boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi})$$

en $\mathbb{K}[V]$ para $1 \leq k \leq n$. Por la elección de $\boldsymbol{\lambda}$, el polinomio $\rho_V(\boldsymbol{\lambda}, Z_1, \ldots, Z_{n-s})$ es no nulo. Puesto que $\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}$ son algebraicamente independientes sobre $\mathbb{K}$, deducimos que $\rho_V(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s})$ es un elemento no nulo de R. Luego las identidades anteriores muestran que las potencias de $\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi}$ generan el R'–espacio vectorial B'. En otras palabras, Y_{n-s+1} induce un elemento primitivo de la extensión de anillos $R \hookrightarrow \mathbb{K}[V]$.

Sea ahora $Q \in R[Z_{n-s+1}]$ el polinomio que se obtiene al sustituir $\boldsymbol{\Lambda}$ por $\boldsymbol{\lambda}$ y $Z_1, \ldots, Z_{n-s}$ por $Y_1, \ldots, Y_{n-s}$ en P_V. A partir de (3.1) deducimos que $Q(\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi}) = 0$ en B'. Teniendo en cuenta que $\deg_{Z_{n-s+1}} Q = \delta$ concluimos que $\dim_{R'} B' \leq \delta$. $\square$

Capítulo 4

Puntos y fibras de levantamiento

Supongamos, como en el Capítulo 3, que $\mathbb{K}$ es un cuerpo perfecto y que $V \subset \mathbb{A}^n$ es una $\mathbb{K}$–variedad equidimensional de dimensión $n-s$ y grado δ. Sean $F_1, \ldots, F_s \in \mathbb{K}[\boldsymbol{X}]$ polinomios que generan el ideal anulador $\mathcal{I}$ de V. Sean además $Y_1, \ldots, Y_{n-s} \in \mathbb{K}[\boldsymbol{X}]$ formas lineales que definen un morfismo finito $\pi : V \to \mathbb{A}^{n-s}$ y denotemos con $J \in \mathbb{K}[\boldsymbol{X}]$ al determinante Jacobiano de $Y_1, \ldots, Y_{n-s}, F_1, \ldots, F_s$ con respecto a las variables $X_1, \ldots, X_n$. Un punto $\boldsymbol{p} \in \mathbb{K}^{n-s}$ es un **punto de levantamiento** de π con respecto al sistema $F_1 = 0, \ldots, F_s = 0$ si $J(\boldsymbol{x}) \neq 0$ para todo $\boldsymbol{x} \in \pi^{-1}(\boldsymbol{p})$. Llamamos a la variedad cero–dimensional $\pi^{-1}(\boldsymbol{p})$ la **fibra de levantamiento** de $\boldsymbol{p}$. De acuerdo con la Proposición 4.2.1 más abajo, las nociones de punto de levantamiento y de fibra de levantamiento son independientes de la elección de los polinomios $F_1, \ldots, F_s$ que generan $\mathcal{I}$. Consecuentemente, en lo que sigue diremos simplemente que $\boldsymbol{p}$ es un punto de levantamiento de π y que $\pi^{-1}(\boldsymbol{p})$ es una fibra de levantamiento sin referencia a $F_1, \ldots, F_s$.

4.1. Propiedades de los puntos de levantamiento

Sea $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$. Luego $\pi^{-1}(\boldsymbol{p}) = V \cap \{Y_1 - p_1 = 0, \ldots, Y_{n-s} - p_{n-s} = 0\}$. A continuación probaremos que $\boldsymbol{p}$ es un punto de levantamiento de π si y solo si el ideal

$$\mathcal{J} := (F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}) \subset \mathbb{K}[\boldsymbol{X}] \tag{4.1}$$

es radical. A tal fin comenzamos con un resultado técnico.

Lema 4.1.1. *Con las hipótesis y notaciones anteriores, supongamos además que $\mathbb{K}[V]$ es un R–módulo libre de rango D, donde $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$. Fijemos j con $0 \leq j \leq n-s$ y sea $\mathcal{J}_j \subseteq \mathbb{K}[\boldsymbol{X}]$ el ideal $\mathcal{J}_j := (F_1, \ldots, F_s) + (Y_1 - p_1, \ldots, Y_j - p_j)$. Entonces $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ es un $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$–módulo libre de rango igual a D. Además, si las funciones coordenadas de V definidas por $G_1, \ldots, G_D \in \mathbb{K}[\boldsymbol{X}]$ forman una base de $\mathbb{K}[V]$ como R–módulo, $G_1, \ldots, G_D$ inducen una base de $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ como $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$–módulo.*

Demostración. Basta probar la última afirmación. Sea $F \in \mathbb{K}[\boldsymbol{X}]$. Existen $A_1, \ldots, A_D \in R$ tales que $F = A_1G_1 + \cdots + A_DG_D$ in $\mathbb{K}[V]$. Notemos que

$$A_i \equiv A_i(p_1, \ldots, p_j, Y_{j+1}, \ldots, Y_{n-s}) \qquad \text{mód } (Y_1 - p_1, \ldots, Y_j - p_j)$$

para $1 \leq i \leq D$. Por lo tanto, si $B_i := A_i(p_1, \ldots, p_j, Y_{j+1}, \ldots, Y_{n-s})$ para $1 \leq i \leq D$, resulta que $F = B_1G_1 + \cdots + B_DG_D$ en $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$. Esto prueba que $G_1, \ldots, G_D$ generan $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ como $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$–módulo. A continuación, supongamos que $B_1G_1 + \cdots + B_DG_D = 0$ en $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ para ciertos $B_1, \ldots, B_D \in \mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$. Se sigue que existen $H_1, \ldots, H_j \in \mathbb{K}[\boldsymbol{X}]$ tales que $B_1G_1 + \cdots + B_DG_D = H_1(Y_1 - p_1) + \cdots + H_j(Y_j - p_j)$ en $\mathbb{K}[V]$. Podemos escribir $H_i = \sum_{k=1}^{D} C_{ik}G_k$ en $\mathbb{K}[V]$ con $C_{ik} \in R$ para $1 \leq i \leq j$ y $1 \leq k \leq D$. En consecuencia, obtenemos la siguiente identidad en $\mathbb{K}[V]$:

$$\left(B_1 - \sum_{k=1}^{j} C_{k1}(Y_k - p_k)\right)G_1 + \cdots + \left(B_D - \sum_{k=1}^{j} C_{kD}(Y_k - p_k)\right)G_D = 0.$$

Puesto que $G_1, \ldots, G_D$ inducen una base de $\mathbb{K}[V]$ como R–módulo, deducimos que $B_i = \sum_{k=1}^{j} C_{ki}(Y_k - p_k)$ para $1 \leq i \leq D$. Sustituyendo Y_k por p_k en estas identidades para $1 \leq k \leq j$, concluimos que $B_i = 0$ para $1 \leq i \leq D$. Esto muestra que $G_1, \ldots, G_D$ definen elementos $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$–linealmente independentes de $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$, lo que concluye la demostración del lema. □

Ahora estamos en condiciones de probar que, si $\boldsymbol{p}$ es un punto de levantamiento de π, el ideal $\mathcal{J}$ es radical.

Lema 4.1.2. *Con las hipótesis y notaciones del Lema 4.1.1, supongamos además que $\boldsymbol{p}$ es un punto de levantamiento de π. Entonces $\mathcal{J}_j$ es un ideal radical, equidimensional de dimensión $n - s - j$. Además, si $W_j \subseteq \mathbb{A}^n$ es la $\mathbb{K}$–variedad definida por $\mathcal{J}_j$, entonces la aplicación $\pi_j : W_j \to \mathbb{A}^{n-s-j}$ definida por $Y_{j+1}, \ldots, Y_{n-s}$ es un morfismo finito.*

Demostración. Puesto que, por el Lemma 4.1.1, $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ es un $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$–módulo finito, deducimos que $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}_j$ es entero sobre $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}]$. Esto implica que $\dim W_j \leq n - s - j$. Por otra parte, el Teorema de los Ideales Principales (ver, por ejemplo, [Eis95, Theorem 10.2]) muestra que $\dim W_j \geq n - s - j$, de donde concluimos que $\dim W_j = n - s - j$. Por la condición de pureza, se sigue que $\mathcal{J}_j$ es no mezclado. A continuación, considérese una componente $\mathbb{K}$–irreducible $\mathcal{C}$ de W_j. Afirmamos que la restricción $\pi_{\mathcal{C}} : \mathcal{C} \to \mathbb{A}^{n-s-j}$ de π_j a $\mathcal{C}$ es un morfismo finito. En efecto, puesto que $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}] \hookrightarrow \mathbb{K}[W]$ es una extensión entera de anillos, también lo es la extensión $\mathbb{K}[Y_{j+1}, \ldots, Y_{n-s}] \to \mathbb{K}[\mathcal{C}]$ inducida por el homomorfismo de anillos dual $\pi_{\mathcal{C}}^*$. Además, puesto que $\dim \mathcal{C} = n - s - j$, se sigue que $\pi_{\mathcal{C}}^*$ es inyectiva y por lo tanto que $\pi_{\mathcal{C}}$ es dominante. Esto prueba la afirmación, lo que implica que π_j es un morfismo finito.

Resta probar que $\mathcal{J}_j$ es radical. Sea $\mathcal{C}$ una componente $\mathbb{K}$–irreducible de W_j. Puesto que la restriction $\pi_{\mathcal{C}}$ de π_j a $\mathcal{C}$ is un morfismo finito, es suryectiva, y existe

$\boldsymbol{x} \in \pi_{\mathcal{C}}^{-1}(p_{j+1}, \ldots, p_{n-s}) = \mathcal{C} \cap \{Y_{j+1} - p_{j+1} = 0, \ldots, Y_{n-s} - p_{n-s} = 0\}$. Sea J el determinante Jacobiano de $F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}$ con respecto a $X_1, \ldots, X_n$ y M_j la matriz Jacobiana de $F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_j - p_j$ con respecto a $X_1, \ldots, X_n$. Puesto que $\boldsymbol{p}$ es un punto de levantamiento de π y $\boldsymbol{x} \in \pi^{-1}(\boldsymbol{p})$, tenemos que $J(\boldsymbol{x}) \neq 0$, lo que implica que $M_j(\boldsymbol{x})$ tiene rango $s+j$. En consecuencia, existe un $(s+j) \times (s+j)$–menor m de M_j tal que $m(\boldsymbol{x}) \neq 0$. Se sigue que el ideal generado por $\mathcal{J}_j$ y todos los $(s+j) \times (s+j)$–menores de M_j no está contenido en $\mathcal{I}(\mathcal{C})$. Luego, el Lemma 2.1.23 muestra que $\mathcal{J}_j$ es radical. □

Sea $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$ un punto de levantamiento de π. En lo que sigue interpretaremos a $Y_1, \ldots, Y_{n-s}$ ya sea como formas lineales en $X_1, \ldots, X_n$ o bien como indeterminadas sobre $\mathbb{K}$, estando claro por el contexto cuál es la interpretación adoptada. Por el Lema 4.1.2, el ideal cero–dimensional $\mathcal{J} := (F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}) \subset \mathbb{K}[\boldsymbol{X}]$ es radical y por lo tanto es el ideal anulador de la fibra de levantamiento $V_{\boldsymbol{p}} := \pi^{-1}(\boldsymbol{p})$. Para el algoritmo principal que se discutirá en el Capítulo 7 consideraremos ciertas curvas asociadas a $\boldsymbol{p}$ y V, que introducimos a continuación. Sea $\boldsymbol{p}^* := (p_1, \ldots, p_{n-s-1})$ y sea $W_{\boldsymbol{p}^*} \subset \mathbb{A}^n$ la $\mathbb{K}$–variedad definida por el ideal

$$\mathcal{K} := (F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s-1} - p_{n-s-1}) \subseteq \mathbb{K}[\boldsymbol{X}].$$

De acuerdo con el Lemma 4.1.2, $\mathcal{K}$ es un ideal radical, equidimensional de dimensión 1 y la aplicación $\pi_1 : W_{\boldsymbol{p}^*} \to \mathbb{A}^1$ definida por Y_{n-s} es un morfismo finito. Llamamos a $W_{\boldsymbol{p}^*}$ la **curva de levantamiento** definida por $\boldsymbol{p}^*$.

En lo que sigue identificaremos a $V_{\boldsymbol{p}}$ con una subvariedad cero–dimensional de $\mathbb{A}^s$ y a $W_{\boldsymbol{p}^*}$ con una curva de $\mathbb{A}^{s+1}$ del modo siguiente. Por simplicidad de notación, denotaremos con $F_i(Y_1, \ldots, Y_n)$ o $F_i(\boldsymbol{Y})$ al elemento de $\mathbb{K}[Y_1, \ldots, Y_n]$ que se obtiene reescribiendo $F_i(X_1, \ldots, X_n)$ en las variables $Y_1, \ldots, Y_n$.

Lema 4.1.3. *Con las hipótesis del Lemma 4.1.2, valen las siguientes afirmaciones:*

- *los polinomios* $F_1(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n), \ldots, F_s(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n)$ *generan un ideal radical, cero–dimensional* $\overline{\mathcal{J}}$ *de* $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$ *y la* $\mathbb{K}$*–variedad* $\mathcal{V}(\overline{\mathcal{J}}) \subset \mathbb{A}^s$ *es isomorfa a* $V_{\boldsymbol{p}}$*. Además,* $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}}$ *es un* $\mathbb{K}$*–espacio vectorial de dimensión* $\operatorname{rank}_R \mathbb{K}[V]$*;*

- *los polinomios* $F_1(\boldsymbol{p}^*, Y_{n-s}, \ldots, Y_n), \ldots, F_s(\boldsymbol{p}^*, Y_{n-s}, \ldots, Y_n)$ *generan un ideal radical, equidimensional* $\overline{\mathcal{K}}$ *de* $\mathbb{K}[Y_{n-s}, \ldots, Y_n]$ *de dimensión* 1*, y la* $\mathbb{K}$*–variedad* $\mathcal{V}(\overline{\mathcal{K}}) \subset \mathbb{A}^{s+1}$ *es isomorfa a* $W_{\boldsymbol{p}^*}$*. Además,* $Y_{n-s}, \ldots, Y_n$ *están en posición de Noether con respecto a* $\overline{\mathcal{K}}$ *y* $\mathbb{K}[Y_{n-s}, \ldots, Y_n]/\overline{\mathcal{K}}$ *es un* $\mathbb{K}[Y_{n-s}]$*–módulo libre de rango igual a* $\operatorname{rank}_R \mathbb{K}[V]$*.*

Demostración. Claramente, tenemos un isomorfismo de $\mathbb{K}$–álgebras

$$\mathbb{K}[Y_1, \ldots, Y_n]/\mathcal{J} \cong \mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}},$$

que aplica $F(Y_1, \ldots, Y_n) \mod \mathcal{J}$ en $F(\boldsymbol{p}, Y_{n-s+1}, \ldots, Y_n) \mod \overline{\mathcal{J}}$. Se sigue que $\overline{\mathcal{J}}$ es radical y cero–dimensional, puesto que lo es $\mathcal{J}$. Por lo tanto, éste es un isomorfismo

entre los anillos de coordenadas de $V_{\boldsymbol{p}}$ y $\mathcal{V}(\overline{\mathcal{J}})$, lo que prueba que $V_{\boldsymbol{p}}$ y $\mathcal{V}(\overline{\mathcal{J}})$ son isomorfas. Similarmente, tenemos un isomorfismo de $\mathbb{K}$–álgebras

$$\mathbb{K}[Y_1,\ldots,Y_n]/\mathcal{K} \cong \mathbb{K}[Y_{n-s},\ldots,Y_n]/\overline{\mathcal{K}},$$

que aplica $F(Y_1,\ldots,Y_n) \mod \mathcal{K}$ en $F(\boldsymbol{p}^*,Y_{n-s},\ldots,Y_n) \mod \overline{\mathcal{K}}$. Argumentando como antes concluimos que $\overline{\mathcal{K}}$ es radical y que $W_{\boldsymbol{p}^*}$ y $\mathcal{V}(\overline{\mathcal{K}})$ son isomorfas. Además, Y_j es entera sobre $\mathbb{K}[Y_{n-s}]$ módulo $\overline{\mathcal{K}}$ para $n-s+1 \leq j \leqq n$, lo que prueba que $Y_{n-s},\ldots,Y_n$ están en posición de Noether con respecto a $\overline{\mathcal{K}}$. Finalmente, las afirmaciones concernientes a los rangos se siguen del Lema 4.1.1, lo que completa la demostración. □

Un paso crítico en el algoritmo resolvente de Kronecker es obtener una representación de Kronecker de una curva de levantamiento $W_{\boldsymbol{p}^*}$ a partir de una tal representación de una fibra de levantamiento $V_{\boldsymbol{p}}$. Esto se llevará a cabo mediante una versión simbólica del método de Newton, que requiere que los polinomios $F_1(\boldsymbol{p},Y_{n-s+1},\ldots,Y_n),\ldots,F_s(\boldsymbol{p},Y_{n-s+1},\ldots,Y_n)$ definan todos los puntos de $V_{\boldsymbol{p}}$ por cortes transversales. Además, en la Sección 7.2 levantaremos una representación de Kronecker de la fibra de levantamiento de la salida módulo un número primo p, lo que también requiere tal condición de transversalidad. Como muestra el siguiente resultado, esta condición está garantizada si $\boldsymbol{p}$ es un punto de levantamiento de π.

Lema 4.1.4. *Con las hipótesis del Lema 4.1.2, el determinante Jacobiano $\overline{J}$ de $F_1(\boldsymbol{p},Y_{n-s+1},\ldots,Y_n),\ldots,F_s(\boldsymbol{p},Y_{n-s+1},\ldots,Y_n)$ con respecto a $Y_{n-s+1},\ldots,Y_n$ es inversible en $\mathbb{K}[Y_{n-s+1},\ldots,Y_n]/\overline{\mathcal{J}}$.*

Demostración. Sean $\mathcal{P}_1,\ldots,\mathcal{P}_N$ los ideales primos minimales de $\overline{\mathcal{J}}$. Puesto que $\overline{\mathcal{J}}$ es radical, por el Lema 2.1.23 deducimos que $\overline{J} \notin \mathcal{P}_i$ para $1 \leq i \leq N$. Como $\overline{\mathcal{J}}$ es de dimensión cero, cada $\mathcal{P}_i$ es un ideal maximal de $\mathbb{K}[Y_{n-s+1},\ldots,Y_n]$, lo que implica que $\overline{J}$ es una unidad en $\mathbb{K}[Y_{n-s+1},\ldots,Y_n]/\mathcal{P}_i$ para $1 \leq i \leq N$. Por el Teorema chino del resto concluimos que $\overline{J}$ es una unidad en $\mathbb{K}[Y_{n-s+1},\ldots,Y_n]/\overline{\mathcal{J}}$, lo que finaliza la demostración del lema. □

Finalmente, suponiendo que $F_1,\ldots,F_s$ forma una sucesión regular, se requerirá que esta condición se preserve al especializar las variables $(Y_1,\ldots,Y_{n-s})$ en un punto de levantamiento $\boldsymbol{p}$. Tenemos el siguiente resultado.

Lema 4.1.5. *Supóngase que $F_1,\ldots,F_s$ forman una sucesión regular de $\mathbb{K}[\boldsymbol{X}]$ y que $Y_1,\ldots,Y_n$ son formas lineales de $\mathbb{K}[\boldsymbol{X}]$ en posición de Noether con respecto a $V_i := \{F_1 = 0,\ldots,F_i = 0\}$ para $1 \leq i \leq s$. Entonces, para todo $\boldsymbol{p} \in \mathbb{K}^{n-s}$, los polinomios $F_1(\boldsymbol{p},Y_{n-s+1},\ldots,Y_n),\ldots,F_s(\boldsymbol{p},Y_{n-s+1},\ldots,Y_n)$ forman una sucesión regular de $\mathbb{K}[Y_{n-s+1},\ldots,Y_n]$.*

Demostración. Basta mostrar que $F_1(\boldsymbol{p},Y_{n-s+1},\ldots,Y_n),\ldots,F_i(\boldsymbol{p},Y_{n-s+1},\ldots,Y_n)$ definen una subvariedad de $\mathbb{A}^s$ de dimensión $s-i$ para $1 \leq i \leq s$. Sea $L_s := \{Y_1 = p_1,\ldots,Y_{n-s} = p_{n-s}\} \subset \mathbb{A}^n$ y $\pi_i : V_i \to \mathbb{A}^{n-i}$ la aplicación definida por $Y_1,\ldots,Y_{n-i}$. Entonces $V_i \cap L_s = \pi_i^{-1}\big(\{Y_1 = p_1,\ldots,Y_{n-s} = p_{n-s}\}\big)$. Puesto que π_i es un morfismo finito, tenemos que $\dim V_i \cap L_s = \dim_{\mathbb{A}^{n-i}}\{Y_1 = p_1,\ldots,t_{n-s} = Y_{n-s}\} = s-i$, y la conclusión del lema se obtiene observando que $\big\{F_1(\boldsymbol{p},Y_{n-s+1},\ldots,Y_n) = 0,\ldots,F_i(\boldsymbol{p},Y_{n-s+1},\ldots,Y_n) = 0\big\}$ y $V_i \cap L_s$ son variedades isomorfas. □

4.2. Una condición para puntos de levantamiento

En esta sección obtenemos una condición sobre las coordenadas de un punto $\boldsymbol{p} \in \mathbb{K}^{n-s}$ que implica que éste es un punto de levantamiento de π. Como primer paso en esta dirección, tenemos la siguiente caracterización de la noción de punto de levantamiento, que también prueba que el concepto es independente de los polinomios $F_1, \ldots, F_s$ que generan el ideal anulador de la variedad V.

Proposición 4.2.1. *Supóngase que $\mathbb{K}[V]$ es un R–módulo libre de rango finito $D := \operatorname{rank}_R \mathbb{K}[V]$. Entonces $\#\pi^{-1}(\boldsymbol{p}) \leq D$ para todo $\boldsymbol{p} \in \mathbb{K}^{n-s}$, y vale la igualdad si y sólo si $\boldsymbol{p}$ es un punto de levantamiento de π.*

Demostración. Sea $\boldsymbol{p} := (p_1, \ldots, p_{n-s})$ y sea $\mathcal{J} \subset \mathbb{K}[\boldsymbol{X}]$ el ideal cero–dimensional de (4.1). Por el Lema 4.1.1 es $\dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{X}]/\mathcal{J} = D$. Puesto que $\#\pi^{-1}(\boldsymbol{p}) = \dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{X}]/\sqrt{\mathcal{J}}$, se deduce la desigualdad del enunciado.

A continuación probamos la caracterización de los puntos de levantamiento. Sea $\chi_J \in R[T]$ el polinomio característico de J módulo $\mathcal{I}$. Puesto que, por el Lema 4.1.1, una base de $\mathbb{K}[V]$ como R–módulo induce una base de $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}$ como $\mathbb{K}$–espacio vectorial, es fácil ver que $\chi_J(\boldsymbol{p}, T)$ es el polinomio característico de J módulo $\mathcal{J}$. Sea $\mu := \chi_J(0)$ el término constante de χ_J, de modo que $\mu(\boldsymbol{p})$ es el término constante de $\chi_J(\boldsymbol{p}, T)$. Por el Teorema de los ceros de Hilbert, $\boldsymbol{p}$ es un punto de levantamiento de π si y sólo si se satisface la igualdad de ideales $\mathcal{J} + (J) = (1)$ en $\mathbb{K}[\boldsymbol{X}]$. Nótese que, puesto que la condición de pureza se satisface en $\mathbb{K}[\boldsymbol{X}]$, $\mathcal{J}$ es no mezclado. Entonces, por el ítem (iv) del Lema 2.1.24, $\mathcal{J} + (J) = (1)$ si y sólo si $\mu(\boldsymbol{p}) \neq 0$. Además, por el ítem (iii) del Lema 2.1.24 $\mu(\boldsymbol{p}) \neq 0$ si y sólo si J no es un divisor de cero en $\mathbb{K}[\boldsymbol{X}]/\mathcal{J}$, lo que a su vez vale si y sólo si J no está contenido en ningún primo asociado de $\mathcal{J}$ (ver, por ejemplo, [Mat86, Theorem 6.1(ii)]). Finalmente, por el Lema 2.1.23, esto último equivale a la radicalidad de $\mathcal{J}$. En resumen, $\boldsymbol{p}$ es un punto de levantamiento de π si y sólo si $\mathcal{J}$ es un ideal radical. Por otro lado, $\mathcal{J}$ es radical si y sólo si $\dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{X}]/\mathcal{J} = \#\pi^{-1}(\boldsymbol{p})$. Puesto que $\dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{X}]/\mathcal{J} = D$, se concluye la proposición. □

Sea $\boldsymbol{\Lambda} := (\Lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n}$, $\boldsymbol{Z} := (Z_1, \ldots, Z_{n-s+1})$ y sea $P_V \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ una forma de Chow de V. Denótese como antes por $A_V \in \mathbb{K}[\boldsymbol{\Lambda}_1, \ldots, \boldsymbol{\Lambda}_{n-s}]$ al coeficiente (no nulo) del monomio Z_{n-s+1}^{δ} en P_V, y por $\rho_V \in \mathbb{K}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}]$ al discriminante de P_V con respecto a Z_{n-s+1}. Considérese el anillo cociente $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]/(P_V)$ como una $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$–álgebra a través del homomorfismo de anillos canónico $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}] \to \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]/(P_V)$. Además, considérese como antes $\mathbb{K}[V][\boldsymbol{\Lambda}]$ como una $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$–álgebra a través del homomorfismo $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}] \to \mathbb{K}[V][\boldsymbol{\Lambda}]$ que aplica todo $F \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ en $F(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{\xi})$. Por el Lema 3.0.2, el polinomio $\partial P_V / \partial Z_{n-s+1}$ es no nulo y por lo tanto

$$S := \left\{ (\partial P_V / \partial Z_{n-s+1})^{\eta} : \eta \geq 0 \right\}$$

es un subconjunto multiplicativamente cerrado de $\mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$. Consideramos las loca-

lizaciones

$$\begin{aligned}\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]_{\partial P_V/\partial Z_{n-s+1}} &:= S^{-1}\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}],\\ \big(\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]/(P_V)\big)_{\partial P_V/\partial Z_{n-s+1}} &:= S^{-1}\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]/(P_V),\\ \mathbb{K}[V][\boldsymbol{\Lambda}]_{\partial P_V/\partial Z_{n-s+1}} &:= S^{-1}\mathbb{K}[V][\boldsymbol{\Lambda}].\end{aligned}$$

Sea $\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]/(P_V)\to\mathbb{K}[V][\boldsymbol{\Lambda}]$ el homomorfismo de $\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]$–álgebras que aplica $[Z_i]_{\mathrm{mod}P_V}$ en $\boldsymbol{\Lambda}_i\cdot\boldsymbol{\xi}$ para $1\le i\le n-s+1$ y considérese el homomorfismo de $\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]_{\partial P_V/\partial Z_{n-s+1}}$–álgebras

$$\Phi : \big(\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]/(P_V)\big)_{\partial P_V/\partial Z_{n-s+1}} \to \mathbb{K}[V][\boldsymbol{\Lambda}]_{\partial P_V/\partial Z_{n-s+1}}. \tag{4.2}$$

que extiende esta aplicación. El siguiente resultado afirma que Φ es un isomorfismo.

Lema 4.2.2. *Φ es un isomorfismo de $\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]_{\partial P_V/\partial Z_{n-s+1}}$–álgebras.*

Demostración. Por la minimalidad de P_V el homomorfismo $\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]/(P_V)\to\mathbb{K}[V][\boldsymbol{\Lambda}]$ es inyectivo, y por lo tanto también lo es Φ. Para probar la suryectividad, nótese que por (3.5) es $\xi_k = -\frac{\partial P_V/\partial\Lambda_{n-s+1,k}(\boldsymbol{\Lambda},\boldsymbol{\Lambda\xi})}{\partial P_V/\partial Z_{n-s+1}}$ en $\mathbb{K}[V][\boldsymbol{\Lambda}]_{\partial P_V/\partial Z_{n-s+1}}$ para $1\le k\le n$. Se sigue que

$$\xi_k = \Phi\left(-\frac{[\partial P_V/\partial\Lambda_{n-s+1,k}]_{\mathrm{mod}P_V}}{\partial P_V/\partial Z_{n-s+1}}\right) \tag{4.3}$$

para $1\le k\le n$. Puesto que $\xi_1,\dots,\xi_n$ generan $\mathbb{K}[V][\boldsymbol{\Lambda}]_{\partial P_V/\partial Z_{n-s+1}}$ como $\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]_{\partial P_V/\partial Z_{n-s+1}}$–álgebra, se deduce el lema. □

También necesitaremos el siguiente resultado técnico.

Lema 4.2.3. *Para todo $F\in\mathbb{K}[\boldsymbol{X}]$, sea $F_\Lambda\in\mathbb{K}[\boldsymbol{\Lambda},\boldsymbol{Z}]$ un polinomio tal que*

$$F\left(-\frac{\partial P_V/\partial\Lambda_{n-s+1,1}}{\partial P_V/\partial Z_{n-s+1}},\dots,-\frac{\partial P_V/\partial\Lambda_{n-s+1,n}}{\partial P_V/\partial Z_{n-s+1}}\right) = \frac{F_\Lambda}{(\partial P_V/\partial Z_{n-s+1})^\eta} \tag{4.4}$$

para algún $\eta\in\mathbb{N}$. Si F se anula idénticamente en V, entonces F_Λ es un múltiplo de P_V. Además, para $1\le i\le n-s+1$, el siguiente polinomio $H_i\in\mathbb{Z}[\boldsymbol{\Lambda},\boldsymbol{Z}]$ es un múltiplo de P_V:

$$H_i := \frac{\partial P_V}{\partial Z_{n-s+1}}\,Z_i + \sum_{j=1}^{n}\Lambda_{ij}\frac{\partial P_V}{\partial\Lambda_{n-s+1,j}}. \tag{4.5}$$

Demostración. Considerando (4.4) módulo P_V y aplicando Φ en ambos miembros, por (4.3) vemos que

$$F(\boldsymbol{\xi}) = \frac{F_\Lambda(\boldsymbol{\Lambda},\boldsymbol{\Lambda\xi})}{(\partial P_V/\partial Z_{n-s+1})^\eta}.$$

Puesto que $F(\boldsymbol{\xi})=0$ y $\partial P_V/\partial Z_{n-s+1}$ no es un divisor de cero de $\mathbb{K}[V][\boldsymbol{\Lambda}]$ (Lema 3.0.3), concluimos que $F_\Lambda(\boldsymbol{\Lambda},\boldsymbol{\Lambda\xi})=0$. Por la minimalidad de P_V se sigue la primera afirmación.

Para probar la segunda afirmación, observamos que

$$[Z_i]_{\mathrm{mod}P_V} = \Phi^{-1}(\boldsymbol{\Lambda}_i\cdot\boldsymbol{\xi}) = \sum_{j=1}^{n}\Lambda_{ij}\,\Phi^{-1}(\xi_j) \tag{4.6}$$

para $1 \leq i \leq n-s+1$. A partir de esto y de (4.3) se sigue que

$$[Z_i]_{\mathrm{mod}P_V} = -\sum_{j=1}^{n} \Lambda_{ij} \frac{[\partial P_V/\partial \Lambda_{n-s+1,j}]_{\mathrm{mod}P_V}}{\partial P_V/\partial Z_{n-s+1}}$$

para $1 \leq i \leq n-s+1$, lo que fácilmente implica la segunda afirmación del lema. □

El siguiente resultado, combinado con la Proposición 4.2.1, proporcionará la condición que estamos buscando que caracteriza a los puntos de levantamiento.

Proposición 4.2.4. *Sea $\boldsymbol{\lambda} \in \mathbb{K}^{(n-s+1)n}$ y $\boldsymbol{p} \in \mathbb{K}^{n-s}$ tales que $A_V(\boldsymbol{\lambda}^*)\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$, sea $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ para $1 \leq i \leq n-s$ y $\pi : V \to \mathbb{A}^{n-s}$ la aplicación definida por $Y_1, \ldots, Y_{n-s}$. Entonces $\#\pi^{-1}(\boldsymbol{p}) = \delta$.*

Demostración. Por la elección de $\boldsymbol{\lambda}$, el polinomio $P_V(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ tiene grado δ. Puesto que

$$\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) = \mathrm{Res}_{Z_{n-s+1}}\left(P_V(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1}), \frac{\partial P_V}{\partial Z_{n-s+1}}(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})\right)$$

y $\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$, el polinomio $P_V(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ es separable. Sean $z_1, \ldots, z_\delta \in \overline{\mathbb{K}}$ las δ raíces distintas de $P_V(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ y sea $\boldsymbol{y}^k := (\boldsymbol{p}, z_k)$ para $1 \leq k \leq \delta$. Tenemos que $\partial P_V/\partial Z_{n-s+1}(\boldsymbol{\lambda}, \boldsymbol{y}^k) \neq 0$ para $1 \leq k \leq \delta$, y por lo tanto el punto

$$\boldsymbol{x}^k := \left(-\frac{\partial P_V/\partial \Lambda_{n-s+1,1}(\boldsymbol{\lambda}, \boldsymbol{y}^k)}{\partial P_V/\partial Z_{n-s+1}(\boldsymbol{\lambda}, \boldsymbol{y}^k)}, \ldots, -\frac{\partial P_V/\partial \Lambda_{n-s+1,n}(\boldsymbol{\lambda}, \boldsymbol{y}^k)}{\partial P_V/\partial Z_{n-s+1}(\boldsymbol{\lambda}, \boldsymbol{y}^k)}\right) \in \mathbb{A}^n$$

está bien definido para $1 \leq k \leq \delta$.

Afirmamos que $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^\delta$ son distintos dos a dos y que $\pi^{-1}(\boldsymbol{p}) = \{\boldsymbol{x}^1, \ldots, \boldsymbol{x}^\delta\}$. En efecto, sea $F \in \mathbb{K}[\boldsymbol{X}]$ un polinomio cualquiera que se anula idénticamente en V y $F_\Lambda \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ un polinomio correspondiente de acuerdo a (4.4). Por el Lema 4.2.3 se tiene que $F_\Lambda(\boldsymbol{\lambda}, \boldsymbol{y}^k) = 0$ y por lo tanto $F(\boldsymbol{x}^k) = 0$ para $1 \leq k \leq \delta$. Esto prueba que $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^\delta$ pertenecen a V. Además, el Lema 4.2.3 también muestra que

$$H_i(\boldsymbol{\lambda}, \boldsymbol{y}^k) = \frac{\partial P_V}{\partial Z_{n-s+1}}(\boldsymbol{\lambda}, \boldsymbol{y}^k) y_i^k + \sum_{j=1}^{n} \lambda_{ij} \frac{\partial P_V}{\partial \Lambda_{n-s+1,j}}(\boldsymbol{\lambda}, \boldsymbol{y}^k) = 0$$

para $1 \leq i \leq n-s+1$ y $1 \leq k \leq \delta$. Por la definición de $\boldsymbol{x}^k$ se sigue que

$$y_i^k = \boldsymbol{\lambda}_i \cdot \boldsymbol{x}^k \quad (1 \leq i \leq n-s+1). \tag{4.7}$$

Puesto que $y_i^k = p_i$ para $1 \leq i \leq n-s$, (4.7) implica que $\pi(\boldsymbol{x}^k) = \boldsymbol{p}$ y $z_k = \boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{x}^k$ para $1 \leq k \leq \delta$. Puesto que los z_k son distintos dos a dos, deducimos que también lo son los $\boldsymbol{x}^k$. Esto prueba que $\#\pi^{-1}(\boldsymbol{p}) \geq \delta$. Por otro lado, puesto que π es un morfismo finito (Proposición 3.1.1), la fibra $\pi^{-1}(\boldsymbol{p})$ es finita, y por (2.4) tenemos que

$$\#\pi^{-1}(\boldsymbol{p}) = \deg\big(V \cap \{Y_1 - p_1 = 0, \ldots, Y_{n-s} - p_{n-s} = 0\}\big) \leq \deg V = \delta,$$

lo que concluye la demostración de la afirmación y de la proposición. □

Ahora estamos en condiciones de establecer el resultado principal de esta sección.

Teorema 4.2.5. *Sean* $\boldsymbol{\lambda} \in \mathbb{K}^{(n-s+1)n}$ *y* $\boldsymbol{p} \in \mathbb{K}^{n-s}$ *tales que* $A_V(\boldsymbol{\lambda}^*)\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$. *Sea* $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ *para* $1 \leq i \leq n-s+1$ *y* $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$. *Entonces:*

- *la aplicación* $\pi : V \to \mathbb{A}^{n-s}$ *definida por* $Y_1, \ldots, Y_{n-s}$ *es un morfismo finito e* Y_{n-s+1} *induce un elemento primitivo de la extensión de anillos* $R \hookrightarrow \mathbb{K}[V]$*;*
- *si* $\mathbb{K}[V]$ *es un* R*–módulo libre, entonces* $\operatorname{rank}_R \mathbb{K}[V] = \delta$*;*
- $\boldsymbol{p}$ *es un punto de levantamiento de* π *e* Y_{n-s+1} *induce un elemento primitivo de* $\pi^{-1}(\boldsymbol{p})$.

Demostración. La Proposición 3.1.1 prueba la primera afirmación. Combinando las Proposiciones 3.1.1, 4.2.1 y 4.2.4 deducimos que $\delta = \#\pi^{-1}(\boldsymbol{p}) \leq \operatorname{rank}_R \mathbb{K}[V] \leq \delta$. Se sigue que $\#\pi^{-1}(\boldsymbol{p}) = \delta$ y que $\boldsymbol{p}$ es un punto de levantamiento de π. Sea $\boldsymbol{p} := (p_1, \ldots, p_{n-s})$. Sustituyendo $\boldsymbol{\Lambda}$ por $\boldsymbol{\lambda}$ y $\boldsymbol{\lambda}_1 \cdot \boldsymbol{\xi}, \ldots, \boldsymbol{\lambda}_{n-s} \cdot \boldsymbol{\xi}$ por $p_1, \ldots, p_{n-s}$ en (3.6), deducimos que

$$\rho_V(\boldsymbol{\lambda}, \boldsymbol{p})\xi_k = R_k(\boldsymbol{\lambda}, \boldsymbol{p}, \boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi})$$

en $\pi^{-1}(\boldsymbol{p})$ para $1 \leq k \leq n$. Puesto que $\rho_V(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$, concluimos que $\mathbb{K}\big[\pi^{-1}(\boldsymbol{p})\big] = \mathbb{K}[\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{\xi}]$, lo que prueba que Y_{n-s+1} induce un elemento primitivo de $\pi^{-1}(\boldsymbol{p})$. □

4.3. Representaciones de Kronecker a partir de especializaciones de la forma de Chow

Sean $\boldsymbol{\lambda} := (\lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n} \in \mathbb{K}^{(n-s+1)n}$ y $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$ que satisfacen las hipótesis de la Proposición 4.2.1 y el Teorema 4.2.5. Defínase $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ para $1 \leq i \leq n-s+1$, y sean $R := \mathbb{K}[Y_1, \ldots, Y_{n-s}]$ y $B := \mathbb{K}[V]$. Supóngase también que $Y_j := \lambda_{j1}X_1 + \cdots + \lambda_{jn}X_n \in \mathbb{K}[\boldsymbol{X}]$ $(n-s+2 \leq j \leq n)$ son formas lineales tales que $Y_1, \ldots, Y_n$ son linealmente independientes. Entonces

- $Y_1, \ldots, Y_n$ están en posición de Noether con respecto a $\mathcal{I}$;
- $\boldsymbol{p}$ es un punto de levantamiento del morfismo finito $\pi : V \to \mathbb{A}^{n-s}$ definido por $Y_1, \ldots, Y_{n-s}$;
- B es un R–módulo libre de rango finito igual a δ.

En lo que sigue mostraremos que es posible obtener representaciones de Kronecker de V, la fibra de levantamiento $V_{\boldsymbol{p}}$ y la curva de levantamiento $W_{\boldsymbol{p}^*}$ especializando una forma de Chow de V. Esto proporcionará un criterio para chequear que las reducciones modulares consideradas durante el algoritmo resolvente de Kronecker se comportan apropiadamente.

Sea $P_V \in \mathbb{K}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ una forma de Chow de V, y sean $A_V \in \mathbb{K}[\boldsymbol{\Lambda}_1, \ldots, \boldsymbol{\Lambda}_{n-s}]$ y $\rho_V \in \mathbb{K}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}]$ definidas como en la Sección 4.2. Por (3.1) y (3.5), es

$$P_V(\boldsymbol{\Lambda}, \boldsymbol{\Lambda\xi}) = 0, \quad \frac{\partial P_V}{\partial Z_{n-s+1}}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda\xi})\xi_k + \frac{\partial P_V}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda\xi}) = 0 \quad (1 \leq k \leq n), \tag{4.8}$$

en $\mathbb{K}[V][\mathbf{\Lambda}]$. Sea T una nueva indeterminada y defínanse $Q, W_{n-s+2}, \ldots, W_n \in R[T]$ por

$$Q := \frac{P_V(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s}, T)}{A_V(\boldsymbol{\lambda}^*)}, \quad W_j := -\sum_{k=1}^{n} \frac{\lambda_{jk}}{A_V(\boldsymbol{\lambda}^*)} \frac{\partial P_V}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s}, T)$$

para $n - s + 2 \leq j \leq n$.

Por construcción, Q es un polinomio mónico con $\deg_T Q = \delta = \dim_{R'} B'$ y $\deg_T W_j < \delta$ para $n - s + 2 \leq j \leq n$. Además, por la elección de $\boldsymbol{\lambda}$ el discriminante $\rho_V(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s})/A_V(\boldsymbol{\lambda}^*)^{2\delta-1}$ de Q es un elemento no nulo de R. Esto implica que Q es libre de cuadrados. Por otra parte, sustituyendo $\mathbf{\Lambda}$ por $\boldsymbol{\lambda}$ en (4.8) deducimos que

$$Q(Y_{n-s+1}) \in \mathcal{I}, \quad Q'(Y_{n-s+1})Y_j - W_j(Y_{n-s+1}) \in \mathcal{I} \quad (n - s + 2 \leq j \leq n), \tag{4.9}$$

donde Q' denota la derivada de Q con respecto a T. Por el Lema 2.1.28, las observaciones anteriores implican el siguiente resultado.

Proposición 4.3.1. *Los polinomios $Q, W_{n-s+2}, \ldots, W_n$ forman la representación de Kronecker de $\mathcal{I}$ con elemento primitivo Y_{n-s+1}.*

Observación 4.3.2. *Puesto que $\deg_{(Z_1,\ldots,Z_{n-s+1})} P_V = \deg_{Z_{n-s+1}} P_V = \delta$ (ver el Capítulo 3), resulta $\deg_{(Y_1,\ldots,Y_{n-s},T)} Q = \delta$ y $\deg_{(Y_1,\ldots,Y_{n-s},T)} W_j \leq \delta$ para $n - s + 2 \leq j \leq n$.*

Sea $\mathcal{J} := \mathcal{I} + (Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s})$. Denótese, como en el Lema 4.1.3, por $\overline{\mathcal{J}}$ a la imagen de $\mathcal{J}$ en $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$.

El polinomio $Q(\boldsymbol{p}, T)$ es mónico de grado δ y $\deg W_j(\boldsymbol{p}, T) < \delta$ para $n - s + 2 \leq j \leq n$. Notemos además que $\mathbb{K}[V_{\boldsymbol{p}}] \cong \mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}}$ es un $\mathbb{K}$–espacio vectorial de dimensión igual a $\operatorname{rank}_R \mathbb{K}[V]$, con lo cual $\deg Q(\boldsymbol{p}, T) = \dim_{\mathbb{K}} \mathbb{K}[Y_{n-s+1}, \ldots, Y_n]/\overline{\mathcal{J}}$. Por la elección de $\boldsymbol{\lambda}$ y $\boldsymbol{p}$ el discriminante $\rho_V(\boldsymbol{\lambda}, \boldsymbol{p})/A_V(\boldsymbol{\lambda}^*)^{2\delta-1}$ de $Q(\boldsymbol{p}, T)$ es no nulo, de donde se sigue que $Q(\boldsymbol{p}, T)$ es libre de cuadrados. Por otra parte, sustituyendo $Y_1, \ldots, Y_{n-s}$ por $p_1, \ldots, p_{n-s}$ en (4.9) obtenemos

$$Q(\boldsymbol{p}, Y_{n-s+1}) \in \overline{\mathcal{J}}, \;\; Q'(\boldsymbol{p}, Y_{n-s+1})Y_j - W_j(\boldsymbol{p}, Y_{n-s+1}) \in \overline{\mathcal{J}} \;\; (n - s + 2 \leq j \leq n).$$

Por el Lema 2.1.28, identificando $\mathcal{J}$ con su imagen en $\mathbb{K}[Y_{n-s+1}, \ldots, Y_n]$, obtenemos el siguiente resultado.

Proposición 4.3.3. *Los polinomios $Q(\boldsymbol{p}, T), W_{n-s+2}(\boldsymbol{p}, T), \ldots, W_n(\boldsymbol{p}, T)$ forman la representación de Kronecker de $\mathcal{J}$ con elemento primitivo Y_{n-s+1}.*

Finalmente, discutimos la representación de Kronecker de $\mathcal{K} := \mathcal{I} + (Y_1 - p_1, \ldots, Y_{n-s-1} - p_{n-s-1})$. Sea $\boldsymbol{p}^* := (p_1, \ldots, p_{n-s-1})$ y sea $\overline{\mathcal{K}}$ la imagen de $\mathcal{K}$ en $\mathbb{K}[Y_{n-s}, \ldots, Y_n]$ como en el Lema 4.1.3. Entonces $Y_{n-s}, \ldots, Y_n$ están en posición de Noether con respecto a $\overline{\mathcal{K}}$ y $\mathbb{K}[W_{\boldsymbol{p}^*}] \cong \mathbb{K}[Y_{n-s}, \ldots, Y_n]/\overline{\mathcal{K}}$ es un $\mathbb{K}[Y_{n-s}]$–módulo libre de rango igual a $\delta = \operatorname{rank}_R \mathbb{K}[V]$. Obsérvese que $Q(\boldsymbol{p}^*, Y_{n-s}, T)$ es mónico de grado δ y que $\deg W_j(\boldsymbol{p}^*, Y_{n-s}, T) < \delta$ para $n - s + 2 \leq j \leq n$. Por la elección de

$\boldsymbol{\lambda}$ y $\boldsymbol{p}$, el discriminante $\rho_V(\lambda, \boldsymbol{p}^*, Y_{n-s})/A_V(\boldsymbol{\lambda}^*)^{2\delta-1}$ de $Q(\boldsymbol{p}^*, Y_{n-s}, T)$ es un elemento no nulo de $\mathbb{K}[Y_{n-s}]$. Por lo tanto, $Q(\boldsymbol{p}^*, Y_{n-s}, T)$ es libre de cuadrados. Por último, sustituyendo $Y_1, \ldots, Y_{n-s-1}$ por $p_1, \ldots, p_{n-s-1}$ en (4.9) obtenemos

$$\begin{gathered} Q(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1}) \in \overline{\mathcal{K}}, \\ Q'(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1})Y_j - W_j(\boldsymbol{p}^*, Y_{n-s}, Y_{n-s+1}) \in \overline{\mathcal{K}} \quad (n-s+2 \leq j \leq n). \end{gathered}$$

Por el Lema 2.1.28, identificando $\mathcal{K}$ con su imagen en $\mathbb{K}[Y_{n-s}, \ldots, Y_n]$, obtenemos el siguiente resultado.

Proposición 4.3.4. *$Q(\boldsymbol{p}^*, Y_{n-s}, T), W_{n-s+2}(\boldsymbol{p}^*, Y_{n-s}, T), \ldots, W_n(\boldsymbol{p}^*, Y_{n-s}, T)$ forman la representación de Kronecker de $\mathcal{K}$ con elemento primitivo Y_{n-s+1}.*

Capítulo 5

Condiciones para una buena reducción modular

De ahora en adelante consideramos polinomios $F_1, \ldots, F_r \in \mathbb{Z}[\boldsymbol{X}]$ de grados a lo sumo d que forman una sucesión regular reducida, y notamos $\mathcal{V}_s := \mathcal{V}(F_1, \ldots, F_s)$ y $\delta_s := \deg \mathcal{V}_s$ para $1 \leq s \leq r$. Como se explicó en la introducción, nuestro objetivo es describir un algoritmo que resuelve el sistema $F_1 = 0, \ldots, F_r = 0$ y analizar su complejidad bit. Este algoritmo entrega en la salida una representación de Kronecker de una fibra de levantamiento de $\mathcal{V}_r$ y se basa en métodos modulares. Por esta razón, un punto crucial es la elección de un número primo "lucky", es decir, un primo que proporciona una buena reducción modular, de "baja" longitud bit. En esta sección exhibimos un entero no nulo $\mathfrak{N}$ que es un múltiplo de todos los primos "unlucky". Más precisamente, mostramos que, para una elección adecuada de $\boldsymbol{\lambda} \in \mathbb{Z}^{n^2}$ y $\boldsymbol{p} \in \mathbb{Z}^{n-1}$, existe un entero no nulo $\mathfrak{N}$ con la siguiente propiedad: si p es un número primo que no divide $\mathfrak{N}$, entonces todas las condiciones en el Teorema 1.2.2 se satisfacen módulo p. Además, nuestra descripción de $\mathfrak{N}$ es lo suficientemente explícita como para permitirnos estimar su longitud bit (Teorema 6.3.5). A partir de esta estimación y de métodos bien conocidos para determinar primos pequeños que no dividen un entero dado podremos calcular en el Capítulo 7 un primo "lucky" de baja longitud bit con alta probabilidad de éxito.

Para la determinación del entero $\mathfrak{N}$ procedemos en varias etapas. En la Sección 5.1 consideramos las condiciones (1)–(2) del Teorema 1.2.2, y los correspondientes resultados se reúnen en el Teorema 5.1.5. Luego en la Sección 5.2 discutimos el cumplimiento de la más difícil condición (3) del Teorema 1.2.2.

En lo que sigue, si p es un número primo y G un polinomio con coeficientes enteros, denotamos por G_p su reducción módulo p. Además, si $G_1, \ldots, G_t \in \mathbb{Z}[X_1, \ldots, X_m]$ definen una variedad $\mathcal{W} := \mathcal{V}(G_1, \ldots, G_t) \subset \mathbb{A}^m := \mathbb{A}^m(\overline{\mathbb{Q}})$, denotamos con $\mathcal{W}_p := \mathcal{V}(G_{1,p}, \ldots, G_{t,p}) \subseteq \mathbb{A}^m_{\overline{\mathbb{F}}_p} := \mathbb{A}^m(\overline{\mathbb{F}}_p)$ la correspondiente reducción módulo p.

5.1. Primeras condiciones

Fíjese s con $1 \leq s \leq r$ y sea $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n}$ tal que se satisfacen las hipótesis de la Proposición 3.1.1. En esta sección establecemos una condición sobre un número primo p que implica que los polinomios $F_{1,p}, \ldots, F_{s,p}$ generan un ideal radical y definen una variedad $\mathcal{V}_{s,p}$ equidimensional de dimensión $n-s$ y grado δ_s, y que las formas lineales $(Y_{1,p}, \ldots, Y_{n-s,p}) := \boldsymbol{\lambda}_p \boldsymbol{X}$ son las variables libres de una normalización de Noether de $\mathcal{V}_{s,p}$.

A lo largo de esta sección y la siguiente, $\boldsymbol{\Lambda} := (\Lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n}$ y $\boldsymbol{Z} := (Z_1, \ldots, Z_{n-s+1})$ denotan una matriz y un vector de indeterminadas sobre $\mathbb{Q}[\mathcal{V}_s]$. Sea $\boldsymbol{\Lambda}_i := (\Lambda_{i1}, \ldots, \Lambda_{in})$ y $\boldsymbol{\Lambda}_i \cdot \boldsymbol{X} := \sum_{j=1}^{n} \Lambda_{ij} X_j$ para $1 \leq i \leq n-s+1$. Además, notamos $\boldsymbol{\Lambda X} := (\boldsymbol{\Lambda}_1 \cdot \boldsymbol{X}, \ldots, \boldsymbol{\Lambda}_{n-s+1} \cdot \boldsymbol{X})$, $\boldsymbol{\Lambda}^* := (\Lambda_{ij})_{1 \leq i \leq n-s, 1 \leq j \leq n}$ y $\boldsymbol{\Lambda}^* \boldsymbol{X} := (\boldsymbol{\Lambda}_1 \cdot \boldsymbol{X}, \ldots, \boldsymbol{\Lambda}_{n-s} \cdot \boldsymbol{X})$. Finalmente, dado $\boldsymbol{\lambda} := (\lambda_{ij})_{1 \leq i \leq n-s+1, 1 \leq j \leq n} \in \mathbb{Z}^{(n-s+1)n}$, adoptamos las notaciones $\boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ $(1 \leq i \leq n-s+1)$, $\boldsymbol{\lambda X}$, $\boldsymbol{\lambda}^*$ y $\boldsymbol{\lambda}^* \boldsymbol{X}$ correspondientemente. Denótese con $P_s \in \mathbb{Q}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ una forma de Chow de $\mathcal{V}_s$. Puesto que P_s está unívocamente determinada salvo múltiplicación por elementos no nulos de $\mathbb{Q}$, podemos suponer que P_s es un polinomio primitivo de $\mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$. Sea como antes $A_s \in \mathbb{Z}[\boldsymbol{\Lambda}_1, \ldots, \boldsymbol{\Lambda}_{n-s}]$ el coeficiente del monomio $Z_{n-s+1}^{\delta_s}$ en P_s y $\rho_s \in \mathbb{Z}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}]$ el discriminante de P_s con respecto a Z_{n-s+1}, es decir,

$$\rho_s := \mathrm{Res}_{Z_{n-s+1}} \left(P_s, \frac{\partial P_s}{\partial Z_{n-s+1}} \right).$$

De acuerdo con el Lema 3.0.2, los polinomios $\partial P_s / \partial Z_{n-s+1}$ y ρ_s son ambos no nulos.

Como primer paso, damos una condición de consistencia del sistema $F_{1,p} = 0, \ldots, F_{s,p} = 0$.

Lema 5.1.1. *Sea p un número primo tal que $A_{s,p}(\boldsymbol{\lambda}_p^*) \rho_{s,p}(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s})$ es no nulo. Sea $Y_{i,p} := \boldsymbol{\lambda}_{i,p} \cdot \boldsymbol{X}$ para $1 \leq i \leq n-s$. Si $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ es la aplicación definida por $Y_{1,p}, \ldots, Y_{n-s,p}$, entonces todo $\boldsymbol{q} \in \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ con $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) \neq 0$ satisface $\# \pi_{s,p}^{-1}(\boldsymbol{q}) \geq \delta_s$.*

Demostración. Nótese que $P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1})$ tiene grado δ_s, puesto que $A_{s,p}(\boldsymbol{\lambda}_p^*) \neq 0$. Se sigue que

$$\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) = \mathrm{Res}_{Z_{n-s+1}} \left(P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1}), \frac{\partial P_{s,p}}{\partial Z_{n-s+1}}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1}) \right),$$

y por lo tanto el polinomio $P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1})$ es separable. Sean $z_1, \ldots, z_{\delta_s} \in \overline{\mathbb{F}}_p$ las raíces de $P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}, Z_{n-s+1})$ e $\boldsymbol{y}^k := (\boldsymbol{q}, z_k)$ para $1 \leq k \leq \delta_s$. Como $\partial P_{s,p} / \partial Z_{n-s+1}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) \neq 0$ para $1 \leq k \leq \delta_s$, el punto

$$\boldsymbol{x}^k := \left(-\frac{\partial P_{s,p} / \partial \Lambda_{n-s+1,1}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k)}{\partial P_{s,p} / \partial Z_{n-s+1}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k)}, \ldots, -\frac{\partial P_{s,p} / \partial \Lambda_{n-s+1,n}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k)}{\partial P_{s,p} / \partial Z_{n-s+1}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k)} \right) \in \mathbb{A}^n_{\overline{\mathbb{F}}_p}$$

está bien definido para $1 \leq k \leq \delta_s$.

Afirmamos que $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}$ son distintos dos a dos y que $\{\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}\} \subseteq \pi_{s,p}^{-1}(\boldsymbol{q})$. En efecto, sean $F_{\Lambda,j} \in \mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ y $\eta_j \in \mathbb{N}$ tales que

$$F_j\left(-\frac{\partial P_s/\partial \Lambda_{n-s+1,1}}{\partial P_s/\partial Z_{n-s+1}}, \ldots, -\frac{\partial P_s/\partial \Lambda_{n-s+1,n}}{\partial P_s/\partial Z_{n-s+1}}\right) = \frac{F_{\Lambda,j}}{(\partial P_s/\partial Z_{n-s+1})^{\eta_j}} \tag{5.1}$$

para $1 \leq j \leq s$. Sea también

$$H_i := \frac{\partial P_s}{\partial Z_{n-s+1}}\, Z_i + \sum_{j=1}^{n} \Lambda_{ij} \frac{\partial P_s}{\partial \Lambda_{n-s+1,j}}.$$

para $1 \leq i \leq n-s+1$. El Lema 4.2.3 muestra que $F_{\Lambda,j}$ $(1 \leq j \leq s)$ y H_i $(1 \leq i \leq n-s+1)$ son múltiplos de P_s en $\mathbb{Q}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$. Además, puesto que P_s es un polinomio primitivo, concluimos que estos polinomios son múltiplos de P_s en $\mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{Z}]$, y por lo tanto que $F_{\Lambda,j,p}$ $(1 \leq j \leq s)$ y $H_{i,p}$ $(1 \leq i \leq n-s+1)$ son múltiplos de $P_{s,p}$. Como, por construcción, es $P_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) = 0$, vemos que $F_{\Lambda,j,p}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) = 0$ y $H_{i,p}(\boldsymbol{\lambda}_p, \boldsymbol{y}^k) = 0$ para $1 \leq k \leq \delta_s$, y reduciendo (5.1) módulo p deducimos que $F_{j,p}(\boldsymbol{x}^k) = 0$ para $1 \leq k \leq \delta_s$. Entonces siguiendo la demostración de la Proposición 4.2.4 *mutatis mutandis* concluimos que $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}$ son puntos de $\pi_{s,p}^{-1}(\boldsymbol{q})$ distintos dos a dos. □

Por definición, $P_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X}) \in \mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{X}]$ se anula idénticamente sobre el conjunto $\mathbb{A}^{(n-s+1)n} \times \mathcal{V}_s$ de ceros comunes de $F_1, \ldots, F_s$ en $\mathbb{A}^{(n-s+1)n} \times \mathbb{A}^n$. Por el Teorema de los ceros de Hilbert, existen enteros $\alpha_s \in \mathbb{Z} \setminus \{0\}$ y $\mu_s \in \mathbb{N}$ tales que

$$\alpha_s P_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X})^{\mu_s} \in (F_1, \ldots, F_s)\mathbb{Z}[\boldsymbol{\Lambda}, \boldsymbol{X}]. \tag{5.2}$$

Nuestro próximo resultado proporciona una condición que implica que la reducción modular preserva la dimensión y una normalización de Noether.

Proposición 5.1.2. *Sea p un número primo tal que $\alpha_{s,p} A_{s,p}(\boldsymbol{\lambda}_p^*) \rho_{s,p}(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s})$ es no nulo. Sea $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ para $1 \leq i \leq n-s$. Entonces:*

1. *$F_{1,p}, \ldots, F_{s,p}$ generan un ideal no mezclado en $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ de dimensión $n-s$;*
2. *la aplicación $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ definida por $Y_{1,p}, \ldots, Y_{n-s,p}$ es un morfismo finito.*

Demostración. Recuérdese que A_s es homogéneo de grado δ_s en los $(n-s)\times(n-s)$–menores de $\boldsymbol{\Lambda}^*$. Puesto que $p \nmid A_s(\boldsymbol{\lambda}^*)$, al menos uno de los $(n-s)\times(n-s)$–menores de $\boldsymbol{\lambda}^*$ es no nulo módulo p. Deducimos que las formas lineales $Y_{1,p}, \ldots, Y_{n-s,p}$ son linealmente independientes, y que existen formas lineales $Y_{n-s+1}, \ldots, Y_n \in \mathbb{Z}[\boldsymbol{X}]$ tales que $Y_{1,p}, \ldots, Y_{n,p}$ son linealmente independientes en $\mathbb{F}_p[\boldsymbol{X}]$. Sea $\boldsymbol{w}_k \in \mathbb{Z}^n$ tal que $Y_{n-s+k} = \boldsymbol{w}_k \cdot \boldsymbol{X}$ para $1 \leq k \leq s$ y

$$Q_k := P_s(\boldsymbol{\lambda}^*, \boldsymbol{w}_k, Y_1, \ldots, Y_{n-s}, Y_{n-s+k}) \in \mathbb{Z}[Z_1, \ldots, Z_{n-s+1}].$$

Teniendo en cuenta (5.2) vemos que $\alpha_s Q_k(Y_1, \ldots, Y_{n-s}, Y_{n-s+k})^{\mu_s} \in (F_1, \ldots, F_s)\mathbb{Z}[\boldsymbol{X}]$ para $1 \leq k \leq s$, y reduciendo módulo p obtenemos

$$\alpha_{s,p} Q_{k,p}(Y_{1,p}, \ldots, Y_{n-s,p}, Y_{n-s+k,p})^{\mu_s} \in (F_{1,p} \ldots, F_{s,p})\mathbb{F}_p[\boldsymbol{X}] \tag{5.3}$$

para $1 \leq k \leq s$. Obsérvese que $\deg_{Z_{n-s+1}} Q_k = \delta_s$ y que $A_s(\boldsymbol{\lambda}^*)$ es el coeficiente de $Z_{n-s+1}^{\delta_s}$ en Q_k. Puesto que $p \nmid \alpha_s A_s(\boldsymbol{\lambda}^*)$, la identidad (5.3) puede interpretarse como una relación de dependencia entera para $Y_{n-s+k,p}$ sobre $\overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n-s,p}]$ módulo $(F_{1,p} \ldots, F_{s,p})$. Además, puesto que $\overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n,p}] = \overline{\mathbb{F}}_p[\boldsymbol{X}]$, concluimos que $\overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n-s,p}] \to \overline{\mathbb{F}}_p[\mathcal{V}_{s,p}]$ es una extensión entera de anillos. En particular, se sigue que $\dim \mathcal{V}_{s,p} \leq n-s$. Además, puesto que $A_{s,p}(\boldsymbol{\lambda}_p^*)\rho_{s,p}(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s}) \neq 0$, por el Lema 5.1.1 la variedad $\mathcal{V}_{s,p} = \mathcal{V}(F_{1,p}, \ldots, F_{s,p})$ es no vacía. En consecuencia, $(F_{1,p}, \ldots, F_{s,p})$ es un ideal propio de $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ de dimensión a lo sumo $n-s$, en tanto que el Teorema de los ideales principales implica que $\dim(F_{1,p}, \ldots, F_{s,p}) \geq n-s$. Concluimos que $\dim(F_{1,p}, \ldots, F_{s,p}) = n-s$, lo que por la condición de pureza implica que $(F_{1,p}, \ldots, F_{s,p})$ es no mezclado. Esto prueba la primera afirmación. Como la extensión de anillos $\overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n-s,p}] \to \overline{\mathbb{F}}_p[\mathcal{V}_{s,p}]$ es entera y $\dim \mathcal{V}_{s,p} = n-s$, se sigue que $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ es un morfismo finito, lo que termina la demostración. □

A continuación mostramos que las hipótesis de la Proposición 5.1.2 también garantizan que el grado se preserva por reducción modular, y que la forma de Chow modular se obtiene reduciendo módulo p la forma de Chow de $\mathcal{V}_s$.

Corolario 5.1.3. *Con las notaciones y las hipótesis de la Proposición 5.1.2,* $\deg \mathcal{V}_{s,p} = \delta_s$ *y* $P_{s,p}$ *es una forma de Chow de* $\mathcal{V}_{s,p}$.

Demostración. Puesto que $p \nmid \alpha_s$, a partir de (5.2) deducimos que $P_{s,p}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X})^{\mu_s} \in (F_{1,p}, \ldots, F_{s,p})\mathbb{F}_p[\boldsymbol{\Lambda}, \boldsymbol{X}]$. Se sigue que $P_{s,p}(\boldsymbol{\Lambda}, \boldsymbol{\Lambda X})$ se anula identicamente en $\mathbb{A}^{(n-s+1)n}_{\overline{\mathbb{F}}_p} \times \mathcal{V}_{s,p}$. En consecuencia, si $Q_s \in \mathbb{F}_p[\boldsymbol{\Lambda}, \boldsymbol{Z}]$ es una forma de Chow de $\mathcal{V}_{s,p}$, entonces Q_s divide a $P_{s,p}$ en $\mathbb{F}_p[\boldsymbol{\Lambda}, \boldsymbol{Z}]$. Puesto que P_s es primitivo, $P_{s,p}$ es no nulo y concluimos que

$$\deg \mathcal{V}_{s,p} = \deg_{Z_{n-s+1}} Q_s \leq \deg_{Z_{n-s+1}} P_{s,p} \leq \delta_s.$$

Por otra parte, la Proposición 5.1.2 muestra que $\pi_{s,p}$ es un morfismo finito, y que la fibra (finita) $\pi_{s,p}^{-1}(\boldsymbol{p}_p)$ satisface $\#\pi_{s,p}^{-1}(\boldsymbol{p}_p) \geq \delta_s$ por el Lema 5.1.1. La desigualdad de Bézout (2.4) implica que

$$\#\pi_{s,p}^{-1}(\boldsymbol{p}_p) = \deg\big(\mathcal{V}_{s,p} \cap \{Y_{1,p} - p_{1,p} = 0, \ldots, Y_{n-s,p} - p_{n-s} = 0\}\big) \leq \deg \mathcal{V}_{s,p}.$$

Esto prueba que $\deg \mathcal{V}_{s,p} = \delta_s$. Puesto que Q_s es homogéneo de grado δ_s y $P_{s,p}$ tiene grado a lo sumo δ_s en cada grupo de variables $(Z_i, \Lambda_{i1}, \ldots, \Lambda_{in})$ para $1 \leq i \leq n-s+1$, deducimos que $P_{s,p} = \epsilon Q_s$ para algún $\epsilon \in \mathbb{F}_p \setminus \{0\}$, mostrando así que $P_{s,p}$ es una forma de Chow de $\mathcal{V}_{s,p}$. □

Finalmente, obtenemos una condición que implica que la reducción modular preserva la suavidad genérica, es decir, la radicalidad. Sea $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{Z}^{n-s}$ tal que $A_s(\boldsymbol{\lambda}^*)\rho_s(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$. A partir del Teorema 4.2.5 se sigue que $\boldsymbol{p}$ es un punto de levantamiento de la aplicación $\pi_s : \mathcal{V}_s \to \mathbb{A}^{n-s}$ definida por $Y_1, \ldots, Y_{n-s}$. Luego, los polinomios $F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}$, y el determinante Jacobiano J_s de $F_1, \ldots, F_s, Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s}$ con respecto a $X_1, \ldots, X_n$, no poseen ceros comunes en $\mathbb{A}^n$. Por el Teorema de los ceros de Hilbert, existen un entero $\gamma_s \in \mathbb{Z} \setminus \{0\}$ y polinomios $G_1, \ldots, G_{n+1} \in \mathbb{Z}[\boldsymbol{X}]$ tales que

$$\gamma_s = G_1 F_1 + \cdots + G_s F_s + G_{s+1}(Y_1 - p_1) + \cdots + G_n(Y_{n-s} - p_{n-s}) + G_{n+1} J_s. \quad (5.4)$$

La no anulación de γ_s módulo p provee la condición adicional que estamos buscando.

Lema 5.1.4. *Con las hipótesis y las notaciones anteriores, sea p un número primo tal que $p \nmid \alpha_s\gamma_s A_s(\boldsymbol{\lambda}^*)\rho_s(\boldsymbol{\lambda}, \boldsymbol{p})$. Entonces $F_{1,p}, \ldots, F_{s,p}$ generan un ideal radical en $\overline{\mathbb{F}}_p[\boldsymbol{X}]$.*

Demostración. Puesto que por hipótesis $\alpha_{s,p}A_{s,p}(\boldsymbol{\lambda}_p^*)\rho_{s,p}(\boldsymbol{\lambda}_p, Z_1, \ldots, Z_{n-s})$ es no nulo, de la Proposición 5.1.2 se sigue que $\mathcal{V}_{s,p}$ es equidimensional de dimensión $n-s$ y que la aplicación $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ definida por $Y_{1,p}, \ldots, Y_{n-s,p}$ es un morfismo finito. Por otra parte, reduciendo (5.4) módulo p vemos que se satisface

$$\gamma_{s,p} = G_{1,p}F_{1,p}+\cdots+G_{s,p}F_{s,p}+G_{s+1,p}(Y_{1,p}-p_{1,p})+\cdots+G_{n,p}(Y_{n-s,p}-p_{n-s,p})+G_{n+1,p}J_{s,p}$$

en $\mathbb{F}_p[\boldsymbol{X}]$. Deducimos que $J_{s,p}(\boldsymbol{x}) \neq 0$ para todo $\boldsymbol{x} \in \pi_{s,p}^{-1}(\boldsymbol{p})$. Sean $\mathcal{C}_1, \ldots, \mathcal{C}_h$ las componentes irreducibles de $\mathcal{V}_{s,p}$ y denótese con $\pi_{\mathcal{C}_i,p}$ la restricción de $\pi_{s,p}$ a $\mathcal{C}_i$ para $1 \leq i \leq h$. Puesto que $\mathcal{V}_{s,p}$ es equidimensional, $\pi_{\mathcal{C}_i}$ es un morfismo finito. En particular, $\pi_{\mathcal{C}_i}$ es suryectivo y $\mathcal{C}_i \cap \pi_{s,p}^{-1}(\boldsymbol{p}_p) \neq \emptyset$ para $1 \leq i \leq h$. Se sigue que $J_{s,p}$ no se anula idénticalmente en $\mathcal{C}_i$, lo que implica que existe un menor $M_i \in \mathbb{F}_p[\boldsymbol{X}]$, de tamaño $s \times s$, de la matriz Jacobiana $(\partial F_{i,p}/\partial X_j)_{1\leq i\leq s, 1\leq j\leq n}$ que no se anula idénticalmente en $\mathcal{C}_i$ para $1 \leq i \leq h$. Sea $\mathcal{J} \subseteq \overline{\mathbb{F}}_p[\boldsymbol{X}]$ el ideal generado por $F_{1,p}, \ldots, F_{s,p}$ y los menores $s \times s$ de la matriz Jacobiana $(\partial F_{i,p}/\partial X_j)_{1\leq i\leq s, 1\leq j\leq n}$. Si $\mathcal{P}_i \subseteq \overline{\mathbb{F}}_p[\boldsymbol{X}]$ es el ideal anulador de $\mathcal{C}_i$ para $1 \leq i \leq h$, entonces $\mathcal{P}_1, \ldots, \mathcal{P}_h$ son los ideales primos minimales de $(F_{1,p}, \ldots, F_{s,p})$. Puesto que $M_i \notin \mathcal{P}_i$, tenemos que $\mathcal{J} \nsubseteq \mathcal{P}_i$ para $1 \leq i \leq h$, y el Lema 2.1.23 prueba que el ideal $(F_{1,p}, \ldots, F_{s,p})$ es radical. □

Reunimos los resultados anteriores en el siguiente teorema.

Teorema 5.1.5. *Sean $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n}$ y $\boldsymbol{p} \in \mathbb{Z}^{n-s}$ tales que $A_s(\boldsymbol{\lambda}^*)\rho_s(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$ y p un número primo tal que $p \nmid \alpha_s\gamma_s A_s(\boldsymbol{\lambda}^*)\rho_s(\boldsymbol{\lambda}, \boldsymbol{p})$, donde α_s y γ_s son los enteros de (5.2) y (5.4) respectivamente. Sea $Y_{i,p} := \boldsymbol{\lambda}_{i,p} \cdot \boldsymbol{X}$ para $1 \leq i \leq n-s+1$ y $R_{s,p} := \overline{\mathbb{F}}_p[Y_{1,p}, \ldots, Y_{n-s,p}]$. Entonces se satisfacen las siguientes condiciones:*

- *$F_{1,p}, \ldots, F_{s,p}$ generan un ideal radical en $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ y definen una variedad equidimensional $\mathcal{V}_{s,p} \subset \mathbb{A}^n_{\overline{\mathbb{F}}_p}$ de dimensión $n-s$ y grado δ_s;*
- *la aplicación $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ definida por $Y_{1,p}, \ldots, Y_{n-s,p}$ es un morfismo finito e $Y_{n-s+1,p}$ induce un elemento primitivo de la extensión de anillos $R_{s,p} \hookrightarrow \overline{\mathbb{F}}_p[\mathcal{V}_{s,p}]$;*
- *$\operatorname{rank}_{R_{s,p}}\overline{\mathbb{F}}_p[\mathcal{V}_{s,p}] = \delta_s$;*
- *todo $\boldsymbol{q} \in \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ con $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) \neq 0$ es un punto de levantamiento de $\pi_{s,p}$ e $Y_{n-s+1,p}$ induce un elemento primitivo de $\pi_{s,p}^{-1}(\boldsymbol{q})$.*

Demostración. La primera afirmación se sigue por la Proposición 5.1.2, el Corolario 5.1.3 y el Lema 5.1.4. Puesto que, por el Corolario 5.1.3, $P_{s,p}$ es una forma de Chow de $\mathcal{V}_{s,p}$, las últimas tres afirmaciones son consecuencia del Teorema 4.2.5 aplicado a $\mathbb{K} = \overline{\mathbb{F}}_p$. □

5.2. Fibras de levantamiento que no intersecan un discriminante

En esta sección suponemos que $s \leq r-1$. El algoritmo de resolución de Kronecker es recursivo, y en su s–ésimo paso calcula una representación de Kronecker de la fibra $\pi_{s+1}^{-1}(\boldsymbol{p}^*)$ a partir de una representación de Kronecker de la curva de levantamiento $W_{\boldsymbol{p}^*}$. Puesto que la representación de Kronecker de $W_{\boldsymbol{p}^*}$ constituye una "buena" representación de $W_{\boldsymbol{p}^*}$ fuera del lugar geométrico discriminante $\{\rho_s(\boldsymbol{\lambda}, Y_1, \ldots, Y_{n-s}) = 0\}$, es crucial que $\pi_{s+1}^{-1}(\boldsymbol{p}^*)$ no interseque esta hipersuperficie. En esta sección mostramos que para una elección genérica de las coordenadas de $\boldsymbol{\lambda}$ y $\boldsymbol{p}$ esta condición se satisface y discutimos cuando la misma se preserva bajo reducción modular.

Con este propósito, utilizamos la siguiente terminología: para dos subvariedades V y W de $\mathbb{A}^n$, decimos que W corta a V **propiamente** si W no contiene ninguna componente $\overline{\mathbb{Q}}$–irreducible de V. Tenemos el siguiente resultado.

Lema 5.2.1. *Existe un polinomio* $\mathsf{R}_s \in \overline{\mathbb{Q}}[\boldsymbol{\Lambda}] \setminus \{0\}$ *de grado a lo sumo* $2(n-s+2)\delta_s^2\delta_{s+1}$ *con la siguiente propiedad: para cada* $\boldsymbol{\lambda} \in \mathbb{A}^{(n-s+1)n}$ *con* $\mathsf{R}_s(\boldsymbol{\lambda}) \neq 0$*, la hipersuperficie* $\{\rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{X}) = 0\} \subset \mathbb{A}^n$ *corta a* $\mathcal{V}_{s+1}$ *propiamente.*

Demostración. Sean $\mathcal{C}_1, \ldots, \mathcal{C}_h$ las componentes $\overline{\mathbb{Q}}$–irreducibles de $\mathcal{V}_{s+1}$, y sea $\boldsymbol{z}_i \in \mathcal{C}_i$ un punto no singular de $\mathcal{V}_{s+1}$ para $1 \leq i \leq h$. Defínase

$$\mathsf{R}_s := \prod_{i=1}^{h} \rho_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}^* \boldsymbol{z}_i).$$

Afirmamos que R_s satisface las condiciones del lema. En efecto, fíjese $1 \leq i \leq h$. Puesto que $\boldsymbol{z}_i$ es un punto no singular de $\mathcal{V}_{s+1}$ e $\mathcal{I}(\mathcal{V}_{s+1}) = \mathcal{I}(\mathcal{V}_s) + (F_{s+1})$, entonces $\boldsymbol{z}_i$ también es un punto no singular de $\mathcal{V}_s$. Por lo tanto, para una elección genérica de $\boldsymbol{\lambda} \in \mathbb{A}^{(n-s+1)n}$, denotando con $\pi_s : \mathcal{V}_s \to \mathbb{A}^{n-s}$ a la aplicación $\pi_s(\boldsymbol{x}) := \boldsymbol{\lambda}^* \boldsymbol{x}$ y escribiendo $\boldsymbol{p} := \pi_s(\boldsymbol{z}_i)$, se satisfacen las siguientes condiciones:

- $\#\pi_s^{-1}(\boldsymbol{p}) = \delta_s$;
- la forma lineal $\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{X}$ separa los puntos de $\pi_s^{-1}(\boldsymbol{p})$;
- el discriminante del polinomio $P_s(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ es $\rho_s(\boldsymbol{\lambda}, \boldsymbol{p})$.

En efecto, puesto que $\boldsymbol{z}_i$ es un punto no singular de $\mathcal{V}_s$, $\mathcal{V}_s$ tiene multiplicidad 1 en $\boldsymbol{z}_i$ (ver, por ejemplo, [Mum95, §5A, Corollary 5.15]). Esto significa que un espacio lineal genérico de dimensión s que pasa por $\boldsymbol{z}_i$ interseca a $\mathcal{V}_s$ en exactamente $\delta_s - 1$ puntos distintos de $\boldsymbol{z}_i$, lo que prueba la primera condición. Las condiciones restantes se satisfacen evidentemente.

Sean $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_s}$ los δ_s puntos de $\pi_s^{-1}(\boldsymbol{p})$. Puesto que $\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{X}$ separa estos puntos, el polinomio $P_s(\boldsymbol{\lambda}, \boldsymbol{p}, Z_{n-s+1})$ tiene δ_s raíces distintas, a saber: $\boldsymbol{\lambda}_{n-s+1} \cdot \boldsymbol{x}^i$ para $1 \leq i \leq \delta_s$. Concluimos que $\rho_s(\boldsymbol{\lambda}, \boldsymbol{p}) \neq 0$. Se sigue que $\rho_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}^* \boldsymbol{z}_i)$ es un polinomio no nulo en $\overline{\mathbb{Q}}[\boldsymbol{\Lambda}]$ para $1 \leq i \leq h$ y por lo tanto $\mathsf{R}_s \in \overline{\mathbb{Q}}[\boldsymbol{\Lambda}] \setminus \{0\}$. Puesto

que $\deg \rho_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}^* \boldsymbol{z}_i) \leq (n-s+2)(2\delta_s - 1)\delta_s$ y $h \leq \delta_{s+1}$, se deduce la estimación para el grado de R_s. Finalmente, sea $\boldsymbol{\lambda} \in \mathbb{A}^{(n-s+1)n}$ tal que $\mathsf{R}_s(\boldsymbol{\lambda}) \neq 0$. Entonces $\rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{z}_i) \neq 0$ para $1 \leq i \leq h$, lo que muestra que $\mathcal{C}_i$ no está contenida en la hipersuperficie $\{\rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{X}) = 0\}$ de $\mathbb{A}^n$ para $1 \leq i \leq h$. □

Sea $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n} \setminus \{0\}$ tal que $\mathsf{R}_s(\boldsymbol{\lambda}) \neq 0$ y sea $\mathcal{W}_{\boldsymbol{\lambda}^s} \subset \mathbb{A}^n$ la variedad

$$\mathcal{W}_{\boldsymbol{\lambda}^s} := \mathcal{V}_{s+1} \cap \{\rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{X}) = 0\}. \tag{5.5}$$

Por el Lema 5.2.1, $\mathcal{W}_{\boldsymbol{\lambda}^s}$ es, o bien vacía, o bien equidimensional de dimensión $n-s-2$.

Supóngase que $\mathcal{W}_{\boldsymbol{\lambda}^s} = \emptyset$ y sea $\rho_{\boldsymbol{\lambda}^s} := \rho_s(\boldsymbol{\lambda}, \boldsymbol{\lambda}^* \boldsymbol{X}) \in \mathbb{Z}[\boldsymbol{X}]$. Por el Teorema de los ceros de Hilbert existe un entero $\mu_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ que satisface

$$\mu_{\boldsymbol{\lambda}^s} \in (F_1, \ldots, F_{s+1}, \rho_{\boldsymbol{\lambda}^s})\mathbb{Z}[\boldsymbol{X}]. \tag{5.6}$$

Por otra parte, supóngase que $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$ y sea $Y_j := \boldsymbol{\lambda}_j \cdot \boldsymbol{X}$ para $1 \leq j \leq n-s-1$. Por [Jel05, Theorem 3.3] (ver también [DKS13, Theorem 3.1]) existe un polinomio no nulo $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1, \ldots, Z_{n-s-1}]$ con $\deg B_{\boldsymbol{\lambda}^s} \leq \deg \mathcal{W}_{\boldsymbol{\lambda}^s}$ tal que

$$B_{\boldsymbol{\lambda}^s}\big(Y_1(\boldsymbol{x}), \ldots, Y_{n-s-1}(\boldsymbol{x})\big) = 0 \tag{5.7}$$

para todo $\boldsymbol{x} \in \mathcal{W}_{\boldsymbol{\lambda}^s}$. Puesto que $\deg \mathcal{W}_{\boldsymbol{\lambda}^s} \leq \deg \mathcal{V}_{s+1} \deg \rho_{\boldsymbol{\lambda}^s}$, es

$$\deg B_{\boldsymbol{\lambda}^s} \leq 2(n-s+2)\delta_s^2 \delta_{s+1}. \tag{5.8}$$

Puesto que $B_{\boldsymbol{\lambda}^s}(Y_1, \ldots, Y_{n-s-1})$ se anula idénticamente sobre la variedad $\mathcal{W}_{\boldsymbol{\lambda}^s} \subset \mathbb{A}^n$ definida por $F_1, \ldots, F_{s+1}$ y $\rho_{\boldsymbol{\lambda}^s}$, por el Teorema de los ceros de Hilbert existen enteros $\beta_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ y $\ell_{\boldsymbol{\lambda}^s} \in \mathbb{N}$ tales que

$$\beta_{\boldsymbol{\lambda}^s} B_{\boldsymbol{\lambda}^s}(Y_1, \ldots, Y_{n-s-1})^{\ell_{\boldsymbol{\lambda}^s}} \in (F_1, \ldots, F_{s+1}, \rho_{\boldsymbol{\lambda}^s})\mathbb{Z}[\boldsymbol{X}]. \tag{5.9}$$

Ahora estamos en condiciones de establecer nuestra condición para una buena reducción modular en el s–ésimo paso. Sea $\mathsf{M}_s \in \mathbb{Z}[\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}] \setminus \{0\}$ el polinomio definido por

$$\mathsf{M}_s := \alpha_s \gamma_s A_s(\boldsymbol{\Lambda}^*) \rho_s(\boldsymbol{\Lambda}, Z_1, \ldots, Z_{n-s}), \tag{5.10}$$

donde α_s y γ_s son los enteros de (5.2) y (5.4) respectivamente. Obsérvese que

$$\deg \mathsf{M}_s \leq 2(n-s+2)\delta_s^2. \tag{5.11}$$

Además, sea $\mathsf{C}_s \in \mathbb{Z}[\boldsymbol{\Lambda}]$ un coeficiente no nulo de $\mathsf{M}_s \mathsf{M}_{s+1} \in \mathbb{Z}[\boldsymbol{\Lambda}][Z_1, \ldots, Z_{n-s}]$. Para $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n} \setminus \{0\}$ con $\mathsf{C}_s(\boldsymbol{\lambda})\mathsf{R}_s(\boldsymbol{\lambda}) \neq 0$, defínase $\mathsf{L}_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1, \ldots, Z_{n-s}] \setminus \{0\}$ como

$$\mathsf{L}_{\boldsymbol{\lambda}^s} := \begin{cases} \mu_{\boldsymbol{\lambda}^s} & \text{if } \mathcal{W}_{\boldsymbol{\lambda}^s} = \emptyset, \\ \beta_{\boldsymbol{\lambda}^s} B_{\boldsymbol{\lambda}^s} & \text{if } \mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset, \end{cases} \tag{5.12}$$

donde $\mu_{\boldsymbol{\lambda}^s}$, $B_{\boldsymbol{\lambda}^s}$ y $\beta_{\boldsymbol{\lambda}^s}$ están definidos como en (5.6), (5.9) y (5.7). Finalmente, defínase

$$\mathsf{N}_{\boldsymbol{\lambda}^s} := \mathsf{M}_s(\boldsymbol{\lambda}, Z_1, \ldots, Z_{n-s})\mathsf{M}_{s+1}(\boldsymbol{\lambda}^*, Z_1, \ldots, Z_{n-s-1})\mathsf{L}_{\boldsymbol{\lambda}^s}(Z_1, \ldots, Z_{n-s-1}).$$

Teorema 5.2.2. *Sea $1 \leq s \leq r-1$. Sean $\boldsymbol{\lambda} \in \mathbb{Z}^{(n-s+1)n}$ y $\boldsymbol{p} := (p_1, \ldots, p_{n-s}) \in \mathbb{Z}^{n-s}$ tales que $\mathsf{C}_s(\boldsymbol{\lambda})\mathsf{R}_s(\boldsymbol{\lambda}) \neq 0$ y $\mathsf{N}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}) \neq 0$, y sea p be un número primo con $p \nmid \mathsf{N}_{\boldsymbol{\lambda}^s}(\boldsymbol{p})$. Si $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ para $1 \leq i \leq n-s+1$, entonces se satisfacen las siguientes condiciones:*

1. *$F_{1,p}, \ldots, F_{s,p}$ generan un ideal radical en $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ y definen una variedad equidimensional $\mathcal{V}_{s,p} \subset \mathbb{A}^n_{\overline{\mathbb{F}}_p}$ de dimensión $n-s$ y grado δ_s. Lo mismo vale para $F_{1,p}, \ldots, F_{s+1,p}$ y $\mathcal{V}_{s+1,p}$;*
2. *la aplicación $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ definida por $Y_{1,p}, \ldots, Y_{n-s,p}$ es un morfismo finito, $\boldsymbol{p}_p \in \mathbb{F}_p^{n-s}$ es un punto de levantamiento de $\pi_{s,p}$, e $Y_{n-s+1,p}$ induce un elemento primitivo de $\pi_{s,p}^{-1}(\boldsymbol{p}_p)$;*
3. *la aplicación $\pi_{s+1,p} : \mathcal{V}_{s+1,p} \to \mathbb{A}^{n-s-1}_{\overline{\mathbb{F}}_p}$ definida por $Y_{1,p}, \ldots, Y_{n-s-1,p}$ es un morfismo finito. Además, si $\boldsymbol{p}^* := (p_1, \ldots, p_{n-s-1})$, entonces $\boldsymbol{p}_p^*$ es un punto de levantamiento de $\pi_{s+1,p}$ e $Y_{n-s,p}$ induce un elemento primitivo de $\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)$;*
4. *todo $\boldsymbol{q} \in \pi_{s,p}\big(\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)\big)$ satisface $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) \neq 0$. En particular, un tal $\boldsymbol{q}$ es un punto de levantamiento de $\pi_{s,p}$ e $Y_{n-s+1,p}$ induce un elemento primitivo de $\pi_{s,p}^{-1}(\boldsymbol{q})$.*

Demostración. Puesto que $p \nmid \mathsf{M}_s(\boldsymbol{\lambda}, \boldsymbol{p})\mathsf{M}_{s+1}(\boldsymbol{\lambda}^*, \boldsymbol{p}^*)$, las primeras tres afirmaciones se siguen del Teorema 5.1.5.

Para probar la última afirmación, sea $\boldsymbol{q} \in \pi_{s,p}\big(\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)\big)$. Luego existe $\boldsymbol{x} \in \pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)$ tal que $\boldsymbol{q} = \big(\boldsymbol{p}_p^*, Y_{n-s,p}(\boldsymbol{x})\big)$. Supóngase que la variedad $\mathcal{W}_{\boldsymbol{\lambda}^s}$ de (5.5) es vacía. Considerando (5.6) módulo p, teniendo en cuenta que $p \nmid \mu_{\boldsymbol{\lambda}^s}$, deducimos que $F_{1,p}, \ldots, F_{s+1,p}$ y que $\rho_{\boldsymbol{\lambda}^s,p}$ genera el ideal unidad de $\overline{\mathbb{F}}_p[\boldsymbol{X}]$. Puesto que $\boldsymbol{x} \in \mathcal{V}_{s+1,p}$, se sigue que $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) = \rho_{\boldsymbol{\lambda}^s,p}(\boldsymbol{x}) \neq 0$. Puesto que $p \nmid \mathsf{M}_s(\boldsymbol{\lambda}, \boldsymbol{p})$, por el Teorema 5.1.5 concluimos que $\boldsymbol{q}$ es un punto de levantamiento de $\pi_{s,p}$ y que $Y_{n-s+1,p}$ induce un elemento primitivo de $\pi_{s,p}^{-1}(\boldsymbol{q})$. Por otra parte, si $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$, considerando (5.9) módulo p y teniendo en cuenta que $p \nmid \beta_{\boldsymbol{\lambda}^s}$ vemos que

$$B_{\boldsymbol{\lambda}^s,p}(Y_{1,p}, \ldots, Y_{n-s-1,p})^{\ell_{\boldsymbol{\lambda}^s}} \in (F_{1,p}, \ldots, F_{s+1,p}, \rho_{\boldsymbol{\lambda}^s,p})\overline{\mathbb{F}}_p[\boldsymbol{X}].$$

Esto implica que $B_{\boldsymbol{\lambda}^s,p}$ se anula idénticamente sobre $\mathcal{V}_{s+1,p} \cap \{\rho_{\boldsymbol{\lambda}^s,p} = 0\}$. Además, el hecho que $p \nmid B_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^*)$ implica que $B_{\boldsymbol{\lambda}^s,p}(\boldsymbol{x}) = B_{\boldsymbol{\lambda}^s,p}(\boldsymbol{p}_p^*) \neq 0$, y por lo tanto que $\rho_{s,p}(\boldsymbol{\lambda}_p, \boldsymbol{q}) = \rho_{\boldsymbol{\lambda}^s,p}(\boldsymbol{x}) \neq 0$. Argumentando como antes deducimos que $\boldsymbol{q}$ es un punto de levantamiento de $\pi_{s,p}$ y que $Y_{n-s+1,p}$ induce un elemento primitivo de $\pi_{s,p}^{-1}(\boldsymbol{q})$. □

Observación 5.2.3. *Con las hipótesis del Teorema 5.2.2, sea $\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*) = \{\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_{s+1}}\}$. Puesto que $Y_{n-s,p}$ induce un elemento primitivo de $\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)$, esta forma lineal separa los puntos $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^{\delta_{s+1}}$. Por lo tanto, si $q \in \overline{\mathbb{F}}_p[T]$ es el polinomio minimal de $Y_{n-s,p}$ sobre $\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)$, sus raíces en $\overline{\mathbb{F}}_p$ son $Y_{n-s,p}(\boldsymbol{x}^1), \ldots, Y_{n-s,p}(\boldsymbol{x}^{\delta_{s+1}})$. Puesto que*

$$\pi_{s,p}\big(\pi_{s+1,p}^{-1}(\boldsymbol{p}_p^*)\big) = \Big\{\big(\boldsymbol{p}_p^*, Y_{n-s,p}(\boldsymbol{x}^1)\big), \ldots, \big(\boldsymbol{p}_p^*, Y_{n-s,p}(\boldsymbol{x}^{\delta_{s+1}})\big)\Big\},$$

podemos parafrasear el ítem (4) del Teorema 5.2.2 de la siguiente manera: $\rho_{s,p}\big(\boldsymbol{\lambda}_p, (\boldsymbol{p}_p^*, a)\big) \neq 0$ para toda raíz $a \in \overline{\mathbb{F}}_p$ de q. Por lo tanto, $(\boldsymbol{p}_p^*, a)$ es un punto de levantamiento de $\pi_{s,p}$ e $Y_{n-s+1,p}$ induce un elemento primitivo de $\pi_{s,p}^{-1}(\boldsymbol{p}_p^*, a)$.

5.3. Normalización de Noether simultánea y fibras de levantamiento

De ahora en adelante, $\mathbf{\Lambda} := (\Lambda_{ij})_{1\leq i\leq n, 1\leq j\leq n}$ denota un conjunto de n^2 indeterminadas sobre $\mathbb{Q}$. Para $1 \leq s \leq r$, escribimos $\mathbf{\Lambda}^s := (\Lambda_{ij})_{1\leq i\leq n, 1\leq j\leq n-s+1}$. Además, para $\boldsymbol{\lambda} := (\lambda_{ij})_{1\leq i\leq n, 1\leq j\leq n} \in \mathbb{Z}^{n^2}$, notamos $\boldsymbol{\lambda}^s := (\lambda_{ij})_{1\leq i\leq n-s+1, 1\leq j\leq n}$. Sea $\mathsf{R} \in \overline{\mathbb{Q}}[\mathbf{\Lambda}] \setminus \{0\}$ el polinomio definido por

$$\mathsf{R} := \prod_{s=1}^{r-1} \mathsf{C}_s \mathsf{R}_s. \tag{5.13}$$

Puesto que $\deg \mathsf{C}_s \leq \deg \mathsf{M}_s + \deg \mathsf{M}_{s+1}$, teniendo en cuenta (5.11) y la estimación para el grado de R_s del Lema 5.2.1, fácilmente deducimos que

$$\deg \mathsf{R} \leq D := (2n - r + 4)r(\delta^3 + 2\delta^2). \tag{5.14}$$

Sea $\boldsymbol{\lambda} \in \mathbb{Z}^{n^2} \setminus \{0\}$ tal que $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ y defínase $\mathsf{N}_{\boldsymbol{\lambda}} \in \mathbb{Z}[Z_1, \ldots, Z_{n-1}] \setminus \{0\}$ como

$$\mathsf{N}_{\boldsymbol{\lambda}} := \mathsf{M}_r(\boldsymbol{\lambda}^r, Z_1, \ldots, Z_{n-r}) \prod_{s=1}^{r-1} \mathsf{M}_s(\boldsymbol{\lambda}^s, Z_1, \ldots, Z_{n-s}) \mathsf{L}_{\boldsymbol{\lambda}^s}(Z_1, \ldots, Z_{n-s-1}). \tag{5.15}$$

Obsérvese que

$$\deg \mathsf{N}_{\boldsymbol{\lambda}} \leq \sum_{s=1}^{r} \deg \mathsf{M}_s + \sum_{s=1}^{r} \deg \mathsf{L}_{\boldsymbol{\lambda}^s} \leq 2(\delta^3 + \delta^2) \sum_{s=1}^{r-1} (n - s + 2) + 2(n - r + 2)\delta^2 \leq D.$$

Sea $\boldsymbol{p} := (p_1, \ldots, p_{n-1}) \in \mathbb{Z}^{n-1}$ tal que $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$ nótese $\boldsymbol{p}^s := (p_1, \ldots, p_{n-s})$ para $1 \leq s \leq r$. Con las hipótesis anteriores fácilmente obtenemos el siguiente resultado.

Teorema 5.3.1. *Sean $\boldsymbol{\lambda} \in \mathbb{Z}^{n^2} \setminus \{0\}$ y $\boldsymbol{p} \in \mathbb{Z}^{n-1}$ tales que $\det(\boldsymbol{\lambda})\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ y $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$. Sea $\mathfrak{N} := \det(\boldsymbol{\lambda})\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p})$ e $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ para $1 \leq i \leq n$. Si p es un número primo tal que $p \nmid \mathfrak{N}$, entonces $Y_{1,p}, \ldots, Y_{n,p}$ definen un nuevo conjunto de variables para $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ y las condiciones (1)–(4) del Teorema 5.2.2 se satisfacen para $1 \leq s \leq r-1$ con $\boldsymbol{p} := \boldsymbol{p}^s$ y $\boldsymbol{p}^* := \boldsymbol{p}^{s+1}$. En particular, $F_{1,p}, \ldots, F_{r,p}$ definen una sucesión regular reducida en $\overline{\mathbb{F}}_p[\boldsymbol{X}]$.*

En lo que sigue, un primo p como en el Teorema 5.3.1 será llamado "lucky" y se dirá que la reducción módulo tal primo p es "buena".

Concluimos esta sección discutiendo representaciones de Kronecker para una buena reducción modular. Dados $\boldsymbol{\lambda} := (\lambda_{ij})_{1\leq i,j\leq n} \in \mathbb{Z}^{n^2}$ y $\boldsymbol{p} := (p_1, \ldots, p_{n-1}) \in \mathbb{Z}^{n-1}$ que satisfacen las hipótesis del Teorema 5.3.1, defínase $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ para $1 \leq i \leq n$, y sea $R_s := \mathbb{Q}[Y_1, \ldots, Y_{n-s}]$ y $B_s := \mathbb{Q}[\mathcal{V}_s]$ para $1 \leq s \leq r$. Puesto que $A_s(\boldsymbol{\lambda}^{s+1})\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s) \neq 0$ para $1 \leq s \leq r$, por el Teorema 4.2.5 se satisfacen las siguientes condiciones:

- $Y_1, \ldots, Y_n$ están en posición de Noether con respecto a $\mathcal{I}_s$;
- $\boldsymbol{p}^s$ es un punto de levantamiento del morfismo finito $\pi_s : \mathcal{V}_s \to \mathbb{A}^{n-s}$ definido por $Y_1, \ldots, Y_{n-s}$;

- B_s es un R_s–módulo libre de rango igual a δ_s.

Sea $\mathcal{I}_s := (F_1, \ldots, F_s)$ y $\mathcal{J}_s := \mathcal{I}_s + (Y_1 - p_1, \ldots, Y_{n-s} - p_{n-s})$ para $1 \leq s \leq r$ y $\mathcal{K}_s := \mathcal{I}_s + (Y_1 - p_1, \ldots, Y_{n-s-1} - p_{n-s-1})$ para $1 \leq s \leq r-1$. De acuerdo con el Lema 4.1.2, $\mathcal{J}_s$ y $\mathcal{K}_s$ son los ideales anuladores de la fibra de levantamiento $\mathcal{V}_{\boldsymbol{p}^s}$ y la curva de levantamiento $\mathcal{W}_{\boldsymbol{p}^s}$ respectivamente. Además, identificando $\mathcal{I}_s$ con su imagen en $\mathbb{Q}[Y_{n-s+1}, \ldots, Y_n]$ y $\mathcal{K}_s$ con su imagen en $\mathbb{Q}[Y_{n-s}, \ldots, Y_n]$ como en el Lema 4.1.3, valen las siguientes condiciones para $1 \leq s \leq r$:

- $\mathbb{Q}[Y_{n-s+1}, \ldots, Y_n]/\mathcal{J}_s$ es un $\mathbb{Q}$–espacio vectorial de dimensión δ_s;
- $Y_{n-s}, \ldots, Y_n$ están en posición de Noether con respecto a $\mathcal{K}_s$;
- $\mathbb{Q}[Y_{n-s}, \ldots, Y_n]/\mathcal{K}_s$ es un $\mathbb{Q}[Y_{n-s}]$–módulo libre de rango igual a $\operatorname{rank}_{R_s} \mathbb{Q}[\mathcal{V}_s]$.

Podemos obtener representaciones de Kronecker de $\mathcal{I}_s$, $\mathcal{J}_s$, y $\mathcal{K}_s$ como en la Sección 4.3, a saber, sea T una nueva indeterminada y defínanse $Q^s, W^s_{n-s+2}, \ldots, W^s_n \in R_s[T]$ por

$$Q^s := \frac{P_s(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s}, T)}{A_s(\boldsymbol{\lambda}^{s+1})}, \quad W^s_j := -\sum_{k=1}^{n} \frac{\lambda_{jk}}{A_s(\boldsymbol{\lambda}^{s+1})} \frac{\partial P_s}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s}, T) \tag{5.16}$$

para $n - s + 2 \leq j \leq n$, donde $P_s \in \mathbb{Z}[\boldsymbol{\Lambda}^s, Z_1, \ldots, Z_{n-s+1}]$ es una forma de Chow primitiva de $\mathcal{V}_s$. Así, las Proposiciones 4.3.1, 4.3.3 y 4.3.4 se leen como sigue.

Proposición 5.3.2. *Valen las siguientes afirmaciones:*

- *los polinomios $Q^s, W^s_{n-s+2}, \ldots, W^s_n$ forman la representación de Kronecker de $\mathcal{I}_s$ con elemento primitivo Y_{n-s+1};*
- *los polinomios $Q^s(\boldsymbol{p}^s, T), W^s_{n-s+2}(\boldsymbol{p}^s, T), \ldots, W^s_n(\boldsymbol{p}^s, T)$ forman la representación de Kronecker de $\mathcal{J}_s$ con elemento primitivo Y_{n-s+1};*
- *los polinomios $Q^s(\boldsymbol{p}^{s+1}, Y_{n-s}, T), W^s_{n-s+2}(\boldsymbol{p}^{s+1}, Y_{n-s}, T), \ldots, W^s_n(\boldsymbol{p}^{s+1}, Y_{n-s}, T)$ forman la representación de Kronecker de $\mathcal{K}_s$ con elemento primitivo Y_{n-s+1}.*

Sea ahora p un número primo como en el Teorema 5.3.1. Sean $\mathcal{I}_{s,p}$, $\mathcal{J}_{s,p}$ y $\mathcal{K}_{s,p}$ los ideales de $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ definidos por $\mathcal{I}_{s,p} := (F_{1,p}, \ldots, F_{s,p})$ y $\mathcal{J}_{s,p} := \mathcal{I}_{s,p} + (Y_{1,p} - p_{1,p}, \ldots, Y_{n-s,p} - p_{n-s,p})$ para $1 \leq s \leq r$, y $\mathcal{K}_{s,p} := \mathcal{I}_{s,p} + (Y_{1,p} - p_{1,p}, \ldots, Y_{n-s-1,p} - p_{n-s-1,p})$ para $1 \leq s \leq r-1$. Por el Teorema 5.3.1 se satisfacen las siguientes condiciones para $1 \leq s \leq r$:

- $\mathcal{I}_{s,p}$ es un ideal radical, equidimensional de dimensión $n - s$;
- las variables $Y_{1,p}, \ldots, Y_{n,p}$ están en posición de Noether con respecto a $\mathcal{I}_{s,p}$;
- la aplicación $\pi_{s,p} : \mathcal{V}_{s,p} \to \mathbb{A}^{n-s}_{\overline{\mathbb{F}}_p}$ definida por $Y_{1,p}, \ldots, Y_{n-s,p}$ es un morfismo finito y $\boldsymbol{p}_p$ es un punto de levantamiento de $\pi_{s,p}$;
- $P_{s,p}$ es una forma de Chow de $\mathcal{V}_{s,p}$.

Se sigue que $\mathcal{I}_{s,p}$, $\mathcal{J}_{s,p}$ y $\mathcal{K}_{s,p}$ son los ideales anuladores de la variedad $\mathcal{V}_{s,p}$, la fibra de levantamiento $\mathcal{V}_{\boldsymbol{p}_p^s}$ y la curva de levantamiento $\mathcal{W}_{\boldsymbol{p}_p^{s+1}}$ respectivamente. Puesto que $p \nmid A_s(\boldsymbol{\lambda}^{s+1})$, los polinomios $Q_p^s, W_{n-s+2,p}^s, \ldots, W_{n,p}^s \in R_{s,p}[T]$ están bien definidos. Denotemos con $Q^s(\boldsymbol{p}_p^s, T), W_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, W_n^s(\boldsymbol{p}_p^s, T)$, respectivamente con $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), W_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$, los polinomios que se obtienen sustituyendo $(Y_{1,p}, \ldots, Y_{n-s,p})$ por $\boldsymbol{p}_p^s$, respectivamente $(Y_{1,p}, \ldots, Y_{n-s-1,p})$ por $\boldsymbol{p}_p^{s+1}$, en los polinomios anteriores. En estos términos, tenemos el siguiente resultado.

Proposición 5.3.3. *Valen las siguientes afirmaciones:*

- $Q_p^s, W_{n-s+2,p}^s, \ldots, W_{n,p}^s$ *forman la representación de Kronecker de* $\mathcal{I}_{s,p}$ *con elemento primitivo* $Y_{n-s+1,p}$*;*
- $Q^s(\boldsymbol{p}_p^s, T), W_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, W_n^s(\boldsymbol{p}_p^s, T)$ *forman la representación de Kronecker de* $\mathcal{J}_{s,p}$ *con elemento primitivo* $Y_{n-s+1,p}$*;*
- $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), W_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ *forman la representación de Kronecker de* $\mathcal{K}_{s,p}$ *con elemento primitivo* $Y_{n-s+1,p}$*.*

Demostración. Teniendo en cuenta (5.16) deducimos que

$$Q_p^s = \frac{P_{s,p}\big(\boldsymbol{\lambda}_p^s, Y_{1,p}, \ldots, Y_{n-s,p}, T\big)}{A_{s,p}(\boldsymbol{\lambda}_p^{s+1})},$$

$$W_{j,p}^s = -\sum_{k=1}^{n} \frac{\lambda_{jk,p}}{A_{s,p}(\boldsymbol{\lambda}_p^{s+1})} \frac{\partial P_{s,p}}{\partial \Lambda_{n-s+1,k}}(\boldsymbol{\lambda}_p^s, Y_{1,p}, \ldots, Y_{n-s,p}, T) \quad (n-s+2 \leq j \leq n).$$

Puesto que $P_{s,p}$ es una forma de Chow de $\mathcal{V}_{s,p}$, la proposición se sigue teniendo en cuenta la condición $p \nmid A_s(\boldsymbol{\lambda}^{s+1})\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)$ y argumentando como en las Proposiciones 4.3.1, 4.3.3 y 4.3.4. □

Consideramos ahora la representación univariada $Q^s, V_{n-s+2}^s, \ldots, V_n^s$ de $\mathcal{I}_s$ con elemento primitivo Y_{n-s+1}. Como antes, sea p un primo como en el Teorema 5.3.1. Sea $g_s := \rho_s(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s})$ y $g_{s,p} := \rho_s(\boldsymbol{\lambda}_p^s, Y_{1,p}, \ldots, Y_{n-s,p})$. Sea $\mathbb{Z}[Y_1, \ldots, Y_{n-s}]_{A_s(\boldsymbol{\lambda}^{s+1})g_s}$ la localización de $\mathbb{Z}[Y_1, \ldots, Y_{n-s}]$ con respecto al conjunto multiplicativo $\{(A_s(\boldsymbol{\lambda}^{s+1})g_s)^\mu : \mu \in \mathbb{Z}_{\geq 0}\}$ y $\mathbb{F}_p[Y_{1,p}, \ldots, Y_{n-s,p}]_{g_{s,p}}$ la localización de $\mathbb{F}_p[Y_{1,p}, \ldots, Y_{n-s,p}]$ con respecto al conjunto multiplicativo $\{g_{s,p}^\mu : \mu \in \mathbb{Z}_{\geq 0}\}$.

Proposición 5.3.4. *Con las hipótesis y notaciones anteriores,* $Q^s, V_{n-s+2}^s, \ldots, V_n^s$ *pertenecen a* $\mathbb{Z}[Y_1, \ldots, Y_{n-s}]_{A_s(\boldsymbol{\lambda}^{s+1})g_s}[T]$*. Además, las correspondientes reducciones modulares* $Q_p^s, V_{n-s+2,p}^s, \ldots, V_{n,p}^s$ *pertenecen a* $\mathbb{F}_p[Y_{1,p}, \ldots, Y_{n-s,p}]_{g_{s,p}}[T]$ *y satisfacen las siguientes propiedades:*

- $Q_p^s, V_{n-s+2,p}^s, \ldots, V_{n,p}^s$ *forman la representación univariada de* $\mathcal{I}_{s,p}$ *con elemento primitivo* $Y_{n-s+1,p}$*;*
- $Q^s(\boldsymbol{p}_p^s, T), V_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, V_n^s(\boldsymbol{p}_p^s, T)$ *forman la representación univariada de* $\mathcal{J}_{s,p}$ *con elemento primitivo* $Y_{n-s+1,p}$*;*

- $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), V_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, V_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ *forman la representación univariada de* $\mathcal{K}_{s,p}$ *con elemento primitivo* $Y_{n-s+1,p}$.

Demostración. Existen polinomios $A, B \in \mathbb{Z}[\boldsymbol{\Lambda}^s, Z_1, \ldots, Z_{n-s+1}]$ tales que

$$\rho_s = AP_s + B\partial P_s/\partial Z_{n-s+1}.$$

Sustituyendo $\boldsymbol{\Lambda}^s$ por $\boldsymbol{\lambda}^s$, $Z_1, \ldots, Z_{n-s}$ por $Y_1, \ldots, Y_{n-s}$, y Z_{n-s+1} por T en la identidad anterior deducimos que existen $\widetilde{A}, \widetilde{B} \in \mathbb{Z}[Y_1, \ldots, Y_{n-s}, T]$ tales que

$$\rho_s(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s}) = \widetilde{A}P_s(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s}, T) + \widetilde{B}\frac{\partial P_s}{\partial Z_{n-s+1}}(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s}, T),$$

Por lo tanto

$$1 = \frac{A_s(\boldsymbol{\lambda}^{s+1})\widetilde{A}}{g_s}Q^s + \frac{A_s(\boldsymbol{\lambda}^{s+1})\widetilde{B}}{g_s}(Q^s)'. \tag{5.17}$$

Si $F := \frac{A_s(\boldsymbol{\lambda}^{s+1})\widetilde{B}}{\rho_s(\boldsymbol{\lambda}^s, Y_1, \ldots, Y_{n-s})}$, (5.17) muestra que $F = (Q^s)'^{-1} \mod (Q^s)$ en $R_s'[T]/(Q^s)$. Por el Lema 2.1.28 los polinomios $V_{n-s+2}^s, \ldots, V_n$ están unívocamente determinados por las siguientes condiciones:

$$\deg V_j^s \leq \delta_s - 1 \quad \text{y} \quad FW_j^s \equiv V_j^s \mod (Q^s) \quad \text{en} \quad R_s'[T] \quad (n-s+2 \leq j \leq n). \tag{5.18}$$

Puesto que Q^s y FW_j^s son ambos elementos de $\mathbb{Z}[Y_1, \ldots, Y_{n-s}]_{A_s(\boldsymbol{\lambda}^{s+1})g_s}[T]$ y Q^s es mónico en T las condiciones anteriores implican que $V_j^s \in \mathbb{Z}[Y_1, \ldots, Y_{n-s}]_{A_s(\boldsymbol{\lambda}^{s+1})g_s}[T]$ para $n-s+2 \leq j \leq n$ y que las congruencias en (5.18) tienen lugar en el anillo $\mathbb{Z}[Y_1, \ldots, Y_{n-s}]_{A_s(\boldsymbol{\lambda}^{s+1})g_s}[T]$. Esto prueba la primera afirmación de la proposición.

Asimismo, por la elección de p, tenemos que $p \nmid A_s(\boldsymbol{\lambda}^{s+1})g_s$, lo que demuestra la buena definición de los polinomios $Q_p^s, V_{n-s+2,p}^s, \ldots, V_{n,p}^s$ y su pertenencia a $\mathbb{F}_p[Y_{1,p}, \ldots, Y_{n-s,p}]_{g_{s,p}}[T]$. Luego, a partir de (5.18) se deducen las siguientes congruencias en el anillo $\mathbb{F}_p[Y_{1,p}, \ldots, Y_{n-s,p}]_{g_{s,p}}[T]$:

$$F_pW_{j,p}^s \equiv V_{j,p}^s \mod (Q_p^s) \quad (n-s+2 \leq j \leq n).$$

Especializando adecuadamente estas congruencias se deduce fácilmente que

$$F_p(\boldsymbol{p}_p^s, T)W_j(\boldsymbol{p}_p^s, T) \equiv V_j(\boldsymbol{p}_p^s, T) \mod (Q^s(\boldsymbol{p}_p^s, T)),$$
$$F_p(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)W_j(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T) \equiv V_j(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T) \mod (Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T))$$

para $n-s+2 \leq j \leq n$. Por otra parte, reduciendo módulo p y especializando adecuadamente en (5.17) vemos que

$$F_p(\boldsymbol{p}_p^s, T) = \big((Q^s)'(\boldsymbol{p}_p^s, T)\big)^{-1} \mod Q^s(\boldsymbol{p}_p^s, T),$$
$$F_p(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T) = \big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big)^{-1} \mod Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T).$$

Las últimas tres afirmaciones de la proposición se siguen de las identidades y congruencias anteriores y el Lema 2.1.28. □

Capítulo 6

Estimaciones de altura

En este capítulo obtenemos estimaciones para las alturas de los enteros $\mathfrak{N}$ del Teorema 5.3.1 y de los enteros que aparecen en la salida del algoritmo que subyace al Teorema 7.3.1, es decir, los polinomios de la Proposición 5.3.2 que forman la representación de Kronecker de $\mathcal{J}_r$. Para este propósito, nos basaremos en los Teoremas de ceros artiméticos de [DKS13].

Recordemos (ver la Sección 2.1.6) que para $a \in \mathbb{Z} \setminus \{0\}$, $h(a) := \log|a|$ es la altura de a, donde log denota el logaritmo en base 2. Además $h(0) := 0$. La altura $h(F)$ de un polinomio $F \in \mathbb{Z}[\boldsymbol{X}]$ es el máximo de las alturas de sus coeficientes. Más generalmente, si $F \in \mathbb{Q}[\boldsymbol{X}]\setminus\{0\}$ y $a \in \mathbb{N}$ es un denominador común mínimo para los coeficientes de F, entonces la altura de F se define como $h(F) := \max\{h(aF), h(a)\}$.

6.1. Formas de Chow, discriminantes y representaciones de Kronecker

De ahora en adelante, volvemos al contexto del Capítulo 5, a saber, consideramos polinomios $F_1, \ldots, F_r \in \mathbb{Z}[\boldsymbol{X}]$ que forman una sucesión regular, denotamos con $\mathcal{V}_s \subset \mathbb{A}^n$ la subvariedad afín equidimensional definida por $F_1, \ldots, F_s$ y con δ_s su grado para $1 \le s \le r$. Sea $d_j := \deg(F_j)$ y $h_j := h(F_j)$ para $1 \le j \le r$, y nótese

$$\delta := \max_{1\le s\le r} \delta_s, \quad d := \max_{1\le j\le r} d_j, \quad h := \max_{1\le j\le r} h_j.$$

Sea $\widehat{h}_s := \widehat{h}(\mathcal{V}_s)$ para $1 \le s \le r$ y $\widehat{h} := \max_{1\le s\le r} \widehat{h}_s$. Por la desigualdad de Bézout aritmética (2.11) tenemos que

$$\widehat{h}(\mathcal{V}_s) \le \sum_{\ell=1}^{s} h_\ell \left(\prod_{j=1, j\neq\ell}^{s} d_j \right) + s \left(\prod_{j=1}^{s} d_j \right) \log(n+2) \quad (1 \le s \le r). \tag{6.1}$$

Sean μ y ε números reales fijos con $0 < \mu, \varepsilon < 1$. Sea $\mathsf{a} := \lfloor D/(1-\mu) \rfloor$ y $\mathsf{b} := \lfloor D/(1-\varepsilon) \rfloor$, donde D está definido en (5.14). Recuérdese que D es una cota superior para el grado de los polinomios R y $\mathsf{N}_{\boldsymbol{\lambda}}$ de (5.13) y (5.15). Puesto que $D \in \mathcal{O}(rnd^{3r})$ y $h(\mathsf{a}), h(\mathsf{b}) \in \mathcal{O}(\log D)$, obtenemos la siguiente observación.

Observación 6.1.1. $h(\mathsf{a}), h(\mathsf{b}) \in \mathcal{O}^{\sim}(r \log d + \log n)$.

Sea $\mathsf{S} := \{0, \ldots, \mathsf{a}\}$ y $\mathsf{T} := \{0, \ldots, \mathsf{b}\}$. Sean además $\boldsymbol{\lambda} := (\lambda_{ij})_{1 \le i \le n, 1 \le j \le n} \in \mathsf{S}^{n^2}$ y $\boldsymbol{p} := (p_1, \ldots, p_{n-1}) \in \mathsf{T}^{n-1}$ tales que $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ y $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$. Por el Lema 2.2.1, para una elección aleatoria de $\boldsymbol{\lambda}$ y $\boldsymbol{p}$ tal condición se verifica con probabilidad al menos $\mu\varepsilon$.

Escribamos $\boldsymbol{\lambda}^s := (\lambda_{ij})_{1 \le i \le n-s+1, 1 \le j \le n}$ y $\boldsymbol{p}^s := (p_1, \ldots, p_{n-s})$ para $1 \le s \le r$. Notemos $h(\boldsymbol{\lambda}^s) := \max_{1 \le i \le n-s+1, 1 \le j \le n} h(\lambda_{ij})$ y $h(\boldsymbol{p}^s) := \max_{1 \le i \le n-s} h(p_i)$. Finalmente, sea $\boldsymbol{\lambda}_i := (\lambda_{i1}, \ldots, \lambda_{in})$ y $Y_i = \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ para $1 \le i \le n$. En lo que sigue, suponiendo que $n \ge 2$ y $d \ge 2$, nuestro objetivo es estimar la altura del entero

$$\mathfrak{N} := \det(\boldsymbol{\lambda}) \mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) = \det(\boldsymbol{\lambda}) \mathsf{M}_r\big(\boldsymbol{\lambda}^r, \boldsymbol{p}^r\big) \prod_{s=1}^{r-1} \mathsf{M}_s\big(\boldsymbol{\lambda}^s, \boldsymbol{p}^s\big) L_{\boldsymbol{\lambda}^s}\big(\boldsymbol{p}^{s+1}\big). \tag{6.2}$$

Comenzamos con una estimación del grado y la altura de una forma de Chow primitiva de $\mathcal{V}_s$ y polinomios relacionados.

Lema 6.1.2. *Para $1 \le s \le r$, se satisface:*

$$h(P_s) \in \mathcal{O}^{\sim}\big(n d^{s-1}(h+d)\big), \tag{6.3}$$

$$\deg P_s(\boldsymbol{\Lambda}^s, \boldsymbol{\Lambda}^s \boldsymbol{X}) \in \mathcal{O}^{\sim}(n d^s), \quad h\big(P_s(\boldsymbol{\Lambda}^s, \boldsymbol{\Lambda}^s \boldsymbol{X})\big) \in \mathcal{O}^{\sim}\big(n d^{s-1}(h+d)\big). \tag{6.4}$$

Demostración. (2.10) y (6.1), en combinación con la desigualdad de Bézout (2.4), dan como resultado (6.3). La estimación de grado en (6.4) es clara. Luego, obsérvese que P_s es un elemento de $\mathbb{Z}[\boldsymbol{\Lambda}^s, Z_1, \ldots, Z_{n-s+1}]$ de grado total $(n-s+1)\delta_s$ y que Λ_{ij} $(1 \le i \le n-s+1, 1 \le j \le n)$, $\boldsymbol{\Lambda}_i \cdot \boldsymbol{X}$ $(1 \le i \le n-s+1)$ son elementos de $\mathbb{Z}[\boldsymbol{\Lambda}^s, \boldsymbol{X}]$ que tienen grados totales a lo sumo 2 y alturas igual a 0. En consecuencia, por [DKS13, Lemma 2.37(3)] deducimos que

$$h\big(P_s(\boldsymbol{\Lambda}^s, \boldsymbol{\Lambda}^s \boldsymbol{X})\big) \le h(P_s) + (n-s+1)\delta_s \Big(\log\big((n-s+1)(n+1)+1\big) + 2\log\big((n-s+2)n+1\big) \Big).$$

Esto, junto con (6.3), fácilmente implica la estimación de altura en (6.4). □

A continuación estimamos el grado y la altura del discriminante ρ_s y del polinomio $\rho_{\boldsymbol{\lambda}^s}$ de la Sección 5.2. Para este propósito, utilizamos el siguiente resultado.

Lema 6.1.3. *Sean $U_1, \ldots, U_{k+1}$ indeterminadas sobre $\mathbb{Z}$ y $F, G \in \mathbb{Z}[U_1, \ldots, U_{k+1}]$ polinomios no nulos con $l := \deg_{U_{k+1}} F$ y $m := \deg_{U_{k+1}} G$. Entonces*

$$h\big(\mathrm{Res}_{U_{k+1}}(F, G)\big) \le m h(F) + l h(G) + \log(k+1)\big((m-1)\deg F + l \deg G\big) + \log\big((l+m)!\big).$$

Demostración. Escribamos $F = \sum_{i=0}^{l} F_i U_{k+1}^i$ y $G = \sum_{j=0}^{m} G_j U_{k+1}^j$, donde $F_i, G_j \in \mathbb{Z}[U_1, \ldots, U_k]$. El determinante $\mathrm{Res}_{U_{k+1}}(F, G)$ es una suma de $(l+m)!$ términos, cada uno de los cuales es un producto de la forma $\pm F_{i_1} \cdots F_{i_m} G_{j_1} \cdots G_{j_l}$. Por [DKS13, Lemma 2.37(2)], cada término tiene altura a lo sumo $m h(F) + l h(G) + \log(k+1)\big((m-1)\deg F + l \deg G\big)$. Luego, [DKS13, Lemma 2.37(1)] completa la demostración del lema. □

Ahora estamos en condiciones de estimar el grado y la altura de ρ_s y $\rho_{\boldsymbol{\lambda}^s}$.

Lema 6.1.4. *Para $1 \leq s \leq r$, se satisface:*

$$\begin{gathered}\deg \rho_s \in \mathcal{O}(nd^{2s}), \quad h(\rho_s) \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+d)\big),\\ \deg \rho_{\boldsymbol{\lambda}^s} \in \mathcal{O}(nd^{2s}), \quad h(\rho_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+d)\big),\\ h(\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)) \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+d)\big).\end{gathered}$$

Demostración. Puesto que $\rho_{\boldsymbol{\lambda}^s} := \rho_s(\boldsymbol{\lambda}^s, \boldsymbol{\lambda}^{s+1}\boldsymbol{X})$, es $\deg \rho_{\boldsymbol{\lambda}^s} \leq \deg \rho_s \leq (n-s+2)\delta_s^2$, lo que prueba las estimaciones de grado. Luego, como $\rho_s := \operatorname{Res}_{Z_{n-s+1}}\Big(P_s, \frac{\partial P_s}{\partial Z_{n-s+1}}\Big)$, el Lema 6.1.3 implica que

$$h(\rho_s) \leq \delta_s\big(2h(P_s) + \log \delta_s\big) + 2\delta_s^2 \log\big((n-s+1)(n+1)\big) + \log\big((2\delta_s)!\big).$$

Esto y (6.3) prueba la estimación para $h(\rho_s)$. Además, puesto que $h(\boldsymbol{\lambda}^s) \leq h(\mathsf{a})$ para todo s, a partir de [DKS13, Lemma 2.37 (3)] deducimos que

$$\begin{aligned}h(\rho_{\boldsymbol{\lambda}^s}) &\leq h(\rho_s) + \deg \rho_s\Big(h(\mathsf{a}) + \log\big((n-s+1)(n+1)\big) + \log(n+1)\Big),\\ h(\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)) &\leq h(\rho_s) + \deg \rho_s\Big(\max\{h(\mathsf{a}), h(\mathsf{b})\} + \log\big((n-s+1)(n+1)\big)\Big).\end{aligned}$$

Combinando estas desigualdades con la Observación 6.1.1 y la estimación para $h(\rho_s)$ obtenemos las estimaciones para $h(\rho_{\boldsymbol{\lambda}^s})$ y $h(\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s))$. □

Concluimos esta sección con una estimación de la altura de las representaciones de Kronecker y de las representaciones univariadas de las fibras de cada paso recursivo de nuestro algoritmo principal.

La siguiente estimación del tamaño de los coeficientes del cociente y del resto en una pseudodivisión se encuentra en [vzGG99, Exercise 6.44]. Recordemos que la norma infinito $\|f\|_\infty$ de un polinomio $f = \sum_{0\leq i\leq n} a_i T^i \in \mathbb{Z}[T]$ se define por $\|f\|_\infty := \max\{|a_i| : 0 \leq i \leq n\}$.

Lema 6.1.5. *Sean $a, b \in \mathbb{Z}[T]$, con $n = \deg a \geq m = \deg(b)$, $k := n - m$ y $c \in \mathbb{Z}$ el coeficiente principal de b. Además, sean $q = \sum_{0\leq i\leq k} q_i T^i$ y r en $\mathbb{Z}[T]$ tales que $c^{k+1}a = qb + r$ y $\deg r < m$. Entonces $\|q\|_\infty$ y $\|r\|_\infty$ están acotadas por $\|a\|_\infty(\|b\|_\infty + |c|)^{k+1}$.*

Proposición 6.1.6. *Sea η_s el máximo de las alturas de los polinomios $Q^s(\boldsymbol{p}^s, T)$, $W^s_{n-s+2}(\boldsymbol{p}^s, T), \ldots, W^s_n(\boldsymbol{p}^s, T)$ de la Proposición 5.3.2. Entonces $\eta_s \in \mathcal{O}^{\sim}\big(nd^{s-1}(h + rd)\big)$ para $1 \leq s \leq r-1$ y $\eta_r \in \mathcal{O}^{\sim}\big(nd^{r-1}(h+d)\big)$. Si η'_s es el máximo de las alturas de los polinomios $V^s_{n-s+2}(\boldsymbol{p}^s, T), \ldots, V^s_n(\boldsymbol{p}^s, T)$ de la parametrización de la correspondiente representación univariada, entonces $\eta'_s \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+rd)\big)$ para $1 \leq s \leq r-1$ y $\eta'_r \in \mathcal{O}^{\sim}\big(nd^{2r-1}(h+d)\big)$.*

Demostración. Nótese que

$$Q^s(\boldsymbol{p}^s, T) = \frac{P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)}{A_s(\boldsymbol{\lambda}^{s+1})}, \quad W^s_j(\boldsymbol{p}^s, T) = \frac{\widetilde{W}^s_j(\boldsymbol{p}^s, T)}{A_s(\boldsymbol{\lambda}^{s+1})}. \tag{6.5}$$

donde

$$\widetilde{W}_j^s(\boldsymbol{p}^s,T) := -\sum_{k=1}^{n}\lambda_{jk}\frac{\partial P_s\,(\boldsymbol{\lambda}^s,\boldsymbol{p}^s,T)}{\partial\Lambda_{n-s+1,k}}.$$

Puesto que $h(\boldsymbol{\lambda}^s)\le h(\mathsf{a})$ y $h(\boldsymbol{p}^s)\le h(\mathsf{b})$, por [DKS13, Lemma 2.37 (3)] deducimos que

$$\begin{aligned}h\big(P_s(\boldsymbol{\lambda}^s,\boldsymbol{p}^s,T)\big) &\le h(P_s)+(n-s+1)\delta_s\Big(\text{máx}\{h(\mathsf{a}),h(\mathsf{b})\}+\log\big((n-s+1)(n+1)+1\big)+1\Big)\\ &\le h(P_s)+(n-s+1)\delta_s\big(\text{máx}\{h(\mathsf{a}),h(\mathsf{b})\}+\log(4n^2)\big).\end{aligned}$$

Además, como $h\big(\frac{\partial P_s}{\partial\Lambda_{n-s+1,k}}\big)\le h(P_s)+\log\delta_s$, un argumento similar muestra que

$$h\left(\frac{\partial P_s\,(\boldsymbol{\lambda}^s,\boldsymbol{p}^s,T)}{\partial\Lambda_{n-s+1,k}}\right)\le h(P_s)+\log\delta_s+(n-s+1)\delta_s\big(\text{máx}\{h(\mathsf{a}),h(\mathsf{b})\}+\log(4n^2)\big).$$

Por [DKS13, Lemma 2.37(1)] tenemos que

$$\begin{aligned}h\big(\widetilde{W}_j^s(\boldsymbol{p}^s,T)\big) &\le h(P_s)+\log\delta_s+h(\mathsf{a})+\log n\\ &\quad+(n-s+1)\delta_s\big(\text{máx}\{h(\mathsf{a}),h(\mathsf{b})\}+\log(4n^2)\big)\end{aligned}\tag{6.6}$$

para $n-s+2\le j\le n$. Similarmente deducimos que

$$h\big(A_s(\boldsymbol{\lambda}^{s+1})\big)\le h(P_s)+(n-s)\delta_s\Big(h(\mathsf{a})+\log\big((n-s+1)n+1\big)\Big).$$

Por (6.5) y las estimaciones anteriores vemos que η_s está acotada superiormente por el lado derecho de (6.6). Luego, la primera afirmación de la proposición se sigue por (6.3) y la Observación 6.1.1.

Para probar la segunda afirmación, observemos que sustituyendo $(Y_1,\dots,Y_{n-s})$ por $\boldsymbol{p}^s$ en (5.17) obtenemos

$$\rho_s(\boldsymbol{\lambda}^s,\boldsymbol{p}^s)=\widetilde{A}(\boldsymbol{p}^s,T)P_s(\boldsymbol{\lambda}^s,\boldsymbol{p}^s,T)+\widetilde{B}(\boldsymbol{p}^s,T)\frac{\partial P_s}{\partial Z_{n-s+1}}(\boldsymbol{\lambda}^s,\boldsymbol{p}^s,T),$$

donde $\deg\widetilde{A}(\boldsymbol{p}^s,T)<\delta_s-1$, $\deg\widetilde{B}(\boldsymbol{p}^s,T)<\delta_s$. Además, por [vzGG99, Theorem 6.52 y su demostración] tenemos que

$$\|\widetilde{A}(\boldsymbol{p}^s,T)\|_\infty,\|\widetilde{B}(\boldsymbol{p}^s,T)\|_\infty\le(\delta_s+1)^{\delta_s}(\delta_s\|P_s(\boldsymbol{\lambda}^s,\boldsymbol{p}^s,T)\|_\infty)^{2\delta_s-1}.\tag{6.7}$$

Por lo tanto

$$1=\frac{A_s(\boldsymbol{\lambda}^{s+1})\widetilde{A}(\boldsymbol{p}^s,T)}{\rho_s(\boldsymbol{\lambda}^s,\boldsymbol{p}^s)}Q^s(\boldsymbol{p}^s,T)+\frac{A_s(\boldsymbol{\lambda}^{s+1})\widetilde{B}(\boldsymbol{p}^s,T)}{\rho_s(\boldsymbol{\lambda}^s,\boldsymbol{p}^s)}(Q^s)'(\boldsymbol{p}^s,T),$$

donde $(Q^s)'(\boldsymbol{p}^s,T)$ denota la derivada de $Q^s(\boldsymbol{p}^s,T)$. Si $F:=\frac{A_s(\boldsymbol{\lambda}^{s+1})\widetilde{B}(\boldsymbol{p}^s,T)}{\rho_s(\boldsymbol{\lambda}^s,\boldsymbol{p}^s)}$, deducimos que $F=(Q^s)'^{-1}(\boldsymbol{p}^s,T)\ \ \text{mód}\ Q^s(\boldsymbol{p}^s,T)$. Notemos $a:=\widetilde{B}(\boldsymbol{p}^s,T)\widetilde{W}_j^s(\boldsymbol{p}^s,T)$,

$b := P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)$ y $c := A_s(\boldsymbol{\lambda}^{s+1})$, y sean $\widetilde{Q}_j, \widetilde{V}_j^s(\boldsymbol{p}^s, T) \in \mathbb{Z}[T]$ los polinomios con $\deg \widetilde{V}_j^s(\boldsymbol{p}^s, T) \leq \delta_s - 1$ y tales que

$$c^{\deg(a)-\deg(b)+1} a = \widetilde{Q}_j b + \widetilde{V}_j^s(\boldsymbol{p}^s, T)$$

para $n - s + 2 \leq j \leq n$. Por construcción resulta

$$FW_j^s(\boldsymbol{p}^s, T) = \frac{\widetilde{Q}_j}{c^{\deg(a)-\deg(b)}\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)} Q^s(\boldsymbol{p}^s, T) + \frac{\widetilde{V}_j^s(\boldsymbol{p}^s, T)}{c^{\deg(a)-\deg(b)+1}\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)},$$

de donde se deduce que

$$V_j^s(\boldsymbol{p}^s, T) = \frac{\widetilde{V}_j^s(\boldsymbol{p}^s, T)}{c^{\deg(a)-\deg(b)+1}\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)}.$$

Por el Lema 6.1.5, notando que $|c| \leq \|b\|_\infty$ y que $\deg(a) - \deg(b) \leq \delta_s - 2$, resulta

$$\|\widetilde{V}_j^s(\boldsymbol{p}^s, T)\|_\infty \leq \|a\|_\infty (2\|b\|_\infty)^{\delta_s - 2},$$

y por lo tanto

$$h\big(\widetilde{V}_j^s(\boldsymbol{p}^s, T)\big) \leq h(a) + \delta_s\big(h(b) + 1\big). \tag{6.8}$$

Por (6.7) vemos que

$$h\big(\widetilde{B}(\boldsymbol{p}^s, T)\big) \leq h\big(P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)\big) + 3\delta_s \log(\delta_s + 1).$$

Esto, junto con la estimación $h\big(P_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s, T)\big) \in \mathcal{O}^\sim\big(nd^{s-1}(h + rd)\big)$ que acabamos de demostrar, implica $h\big(\widetilde{B}(\boldsymbol{p}^s, T)\big) \in \mathcal{O}^\sim\big(nd^{2s-1}(h + rd)\big)$. Por lo tanto $h(a) = h\big(\widetilde{B}(\boldsymbol{p}^s, T)\big) + h\big(\widetilde{W}_j^s(\boldsymbol{p}^s, T)\big) \in \mathcal{O}^\sim\big(nd^{2s-1}(h + rd)\big)$. Teniendo en cuenta (6.8) concluimos que $h\big(\widetilde{V}_j^s(\boldsymbol{p}^s, T)\big) \in \mathcal{O}^\sim\big(nd^{2s-1}(h + rd)\big)$. Finalmente, teniendo en cuenta la estimación para $h\big(\rho_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)\big)$ del Lema 6.1.4 la segunda afirmación de la proposición queda probada. □

6.2. La condición de pureza y suavidad genérica

En esta sección estimamos la altura de los enteros α_s y γ_s de (5.2) y (5.4), cuya no anulación módulo p implica que la correspondiente reducción modular es no mezclada y genéricamente suave, y proporciona nuevas variables en posición de Noether (Teorema 5.1.5).

Comenzamos con α_s. Teniendo en cuenta que $\widehat{h}\big(\mathbb{A}^{(n-s+2)n}\big) = 0$ y $\deg\big(\mathbb{A}^{(n-s+2)n}\big) = 1$, de [DKS13, Theorem 2] se sigue que existe $\alpha_s \in \mathbb{Z} \setminus \{0\}$ como en (5.2) con

$$h(\alpha_s) \leq 3h\big(P_s(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}\boldsymbol{X})\big) \prod_{j=1}^{s} d_j + 2\deg\big(P_s(\boldsymbol{\Lambda}^s, \boldsymbol{\Lambda}^s\boldsymbol{X})\big) \prod_{j=1}^{s} d_j \left(h \sum_{\ell=1}^{s} \frac{1}{d_\ell} + c(n) \right),$$

donde $c(n) \in \mathcal{O}^\sim(n)$. Combinando esto con (6.4) deducimos el siguiente resultado.

Lema 6.2.1. $h(\alpha_s) \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+nd)\big)$.

A continuación consideramos γ_s. Sea J_s el determinante Jacobiano de $F_1,\dots,F_s$, $Y_1,\dots,Y_{n-s}$ con respecto a las variables $X_1,\dots,X_n$.

Lema 6.2.2. *Valen las siguientes afirmaciones:*

- $\deg J_s \le s(d-1)$;
- $h(J_s) \le s(\log d + h) + (n-s)h(\mathsf{a}) + s\,d\log(n+1) + \log(n!)$.

Demostración. La afirmación sobre el grado de J_s es clara. Para probar la segunda afirmación, observamos que J_s es una suma de $n!$ términos de la forma $\pm\partial F_1/\partial X_{j_1}\cdots\partial F_s/\partial X_{j_s}\lambda_{1,l_1}\cdots\lambda_{n-s,l_{n-s}}$. Puesto que $h(\lambda_{ij}) \le h(\mathsf{a})$ y $h(\partial F_i/\partial X_j) \le h(F_i)+\log(d_i)$, por [DKS13, Lemma 2.37(2)] deducimos que cada término tiene altura a lo sumo $s(h+\log d)+(n-s)h(\mathsf{a})+\log(n+1)\big((s-1)(d-1)\big)$. La estimación para la altura de J_s se sigue por [DKS13, Lemma 2.37(1)]. □

Sea $d_j := 1$ and $h_j := h(Y_{j-s}-p_{j-s})$ para $s+1 \le j \le n$, $d_{n+1} := \deg J_s$ y $h_{n+1} := h(J_s)$. Por [DKS13, Theorem 1], existen $\gamma_s \in \mathbb{Z}\setminus\{0\}$ y $G_1,\dots,G_{n+1} \in \mathbb{Z}[\boldsymbol{X}]$ como en (5.4) con

$$\begin{aligned} h(\gamma_s) &\le \sum_{\ell=1}^{n+1}\left(\prod_{j\ne\ell} d_j\right) h_\ell + (4n+8)\log(n+3)\prod_{j=1}^{n+1} d_j \\ &\le \deg J_s\left(\prod_{j=1}^{s} d_j\right)\left(\sum_{\ell=1}^{s}\frac{h_\ell}{d_\ell} + \sum_{\ell=1}^{n-s} h(Y_\ell - p_\ell) + (4n+8)\log(n+3)\right) + h(J_s)\prod_{j=1}^{s} d_j. \end{aligned}$$

Puesto que $h(Y_\ell) \le h(\mathsf{a})$ y $h(p_\ell) \le h(\mathsf{b})$ para todo ℓ, obtenemos

$$h(\gamma_s) \le \deg J_s\, d^{s-1}sh + \deg J_s\, d^s\big((n-s)\max\{h(\mathsf{a}),h(\mathsf{b})\} + (4n+8)\log(n+3)\big) + h(J_s)d^s.$$

Combinando esto con la Observación 6.1.1 y el Lema 6.2.2, deducimos el siguiente resultado.

Lema 6.2.3. $h(\gamma_s) \in \mathcal{O}^{\sim}\big(d^s(h+rnd)\big)$.

6.3. Fibras de levantamiento

En esta sección estimamos la altura de los enteros de la Sección 5.2, a saber, $\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)$ y $\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})$, donde M_s es el polinomio de (5.10) y $\mathsf{L}_{\boldsymbol{\lambda}^s}$ es el polinomio de (5.12). Combinando estas estimaciones podremos estimar la altura del entero $\mathfrak{N}$ de (6.2), que comprende todos los primos "unlucky" p.

Comenzamos estimando la altura de $\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)$.

Lema 6.3.1. $h\big(\mathsf{M}_s(\boldsymbol{\lambda}^s, \boldsymbol{p}^s)\big) \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+nd)\big)$ *para* $1 \le s \le r$.

Demostración. Por [DKS13, Lemma 2.37 (3)], resulta

$$h\big(\mathsf{M}_s(\boldsymbol{\lambda}^s,\boldsymbol{p}^s)\big) \le h(\mathsf{M}_s)+\deg(\mathsf{M}_s)\Big(\max\{h(\boldsymbol{\lambda}^s),h(\boldsymbol{p}^s)\}+\log\big((n-s+1)(n+1)+1\big)\Big). \tag{6.9}$$

Recuérdese que $\mathsf{M}_s := \alpha_s\gamma_s A_s\rho_s$ y que, por definición, $\deg A_s \le (n-s)\delta_s$ y $h(A_s) \le h(P_s)$. En consecuencia, de [DKS13, Lemma 2.37 (2)] deducimos que

$$h(\mathsf{M}_s) \le h(\alpha_s)+h(\gamma_s)+h(P_s)+h(\rho_s)+(n-s)\delta_s\log\big((n-s+1)(n+1)+1\big).$$

Combinando esto con (6.3) y los Lemas 6.1.4, 6.2.1 y 6.2.3 obtenemos

$$h(\mathsf{M}_s) \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+nd)\big).$$

Teniendo en cuenta que $h(\boldsymbol{\lambda}^s) \le h(\mathsf{a})$ y $h(\boldsymbol{p}^s) \le h(\mathsf{b})$ para todo s, por la Observación 6.1.1 deducimos que $\max\{h(\boldsymbol{\lambda}^s),h(\boldsymbol{p}^s)\} \in \mathcal{O}^{\sim}(r\log d+\log n)$. Además, $\deg \mathsf{M}_s \in \mathcal{O}(nd^{2s})$ por (5.11). Combinando todas estas estimaciones con (6.9), se deduce el lema. □

A continuación estimamos la altura de $\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})$. Como este entero está expresado en términos de los enteros $\mu_{\boldsymbol{\lambda}^s}$ de (5.6) y $\beta_{\boldsymbol{\lambda}^s}$ de (5.9) y el polinomio $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1,\dots,Z_{n-s-1}]\setminus\{0\}$ de (5.7), comenzamos con una estimación para $\mu_{\boldsymbol{\lambda}^s}$ and $B_{\boldsymbol{\lambda}^s}$.

Proposición 6.3.2. *Sea $1 \le s \le r-1$ y supóngase que $\mathcal{W}_{\boldsymbol{\lambda}^s} = \emptyset$. Entonces existe $\mu_{\boldsymbol{\lambda}^s} \in \mathbb{Z}\setminus\{0\}$ como en (5.6) con*

$$h(\mu_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^{\sim}\big(n^2d^{3s}(h+d)\big). \tag{6.10}$$

Por otra parte, si $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$, existe $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1,\dots,Z_{n-s-1}]\setminus\{0\}$ como en (5.7) con

$$\deg B_{\boldsymbol{\lambda}^s} \in \mathcal{O}(nd^{3s+1}), \quad h(B_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^{\sim}\big(nd^{3s}(h+rnd)\big) \tag{6.11}$$

Demostración. Supóngase que $\mathcal{W}_{\boldsymbol{\lambda}^s} := \mathcal{V}_{s+1}\cap\{\rho_s(\boldsymbol{\lambda}^s,\boldsymbol{\lambda}^{s+1}\boldsymbol{X})=0\} = \emptyset$ y sea $\rho_{\boldsymbol{\lambda}^s} := \rho_s(\boldsymbol{\lambda}^s,\boldsymbol{\lambda}^{s+1}\boldsymbol{X})$. Por [DKS13, Theorem 1] existe $\mu_{\boldsymbol{\lambda}^s} \in \mathbb{Z}\setminus\{0\}$ como en (5.6) con

$$\begin{aligned} h(\mu_{\boldsymbol{\lambda}^s}) \le& h(\rho_{\boldsymbol{\lambda}^s})\prod_{j=1}^{s+1}d_j+\deg(\rho_{\boldsymbol{\lambda}^s})\prod_{j=1}^{s+1}d_j\left(\sum_{\ell=1}^{s+1}\frac{h_\ell}{d_\ell}+(4n+8)\log(n+3)\right)\\ \le& d^{s+1}\big(h(\rho_{\boldsymbol{\lambda}^s})+\deg(\rho_{\boldsymbol{\lambda}^s})(4n+8)\log(n+3)\big)+(s+1)\deg(\rho_{\boldsymbol{\lambda}^s})d^s h. \end{aligned}$$

Combinando esto con el Lema 6.1.4 se prueba la primera afirmación del lema.

Por otra parte, supóngase que $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$. Por hipótesis $\mathsf{R}_s(\boldsymbol{\lambda}^s) \neq 0$, y por lo tanto el Lema 5.2.1 prueba que $\mathcal{W}_{\boldsymbol{\lambda}^s}$ es equidimensional de dimensión $n-s-2$. Por [DKS13, Corollary 3.23] existe un polinomio $B_{\boldsymbol{\lambda}^s} \in \mathbb{Z}[Z_1,\dots,Z_{n-s-1}]\setminus\{0\}$ como en (5.7) con

$$\deg(B_{\boldsymbol{\lambda}^s}) \le \deg \mathcal{W}_{\boldsymbol{\lambda}^s}, \tag{6.12}$$

$$h(B_{\boldsymbol{\lambda}^s}) \le \widehat{h}(\mathcal{W}_{\boldsymbol{\lambda}^s})+\deg\mathcal{W}_{\boldsymbol{\lambda}^s}\left(\sum_{\ell=1}^{n-s-1}h(Y_\ell)+(n-s)\log(2n+8)\right). \tag{6.13}$$

A continuación obtenemos estimaciones de $\deg \mathcal{W}_{\boldsymbol{\lambda}^s}$ y $h(\mathcal{W}_{\boldsymbol{\lambda}^s})$ en términos de los grados y alturas de $\mathcal{V}_s$ y $\mathcal{V}_{s+1}$. Para este propósito, denótese con $\overline{\mathcal{V}}_{s+1}$ y $\overline{\mathcal{W}}_{\boldsymbol{\lambda}^s}$ a las clausuras proyectivas de $\mathcal{V}_{s+1}$ y $\mathcal{W}_{\boldsymbol{\lambda}^s}$ respectivamente, vía la inclusión canónica $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$. Sea $\rho^h_{\boldsymbol{\lambda}^s}$ la homogeneización de $\rho_{\boldsymbol{\lambda}^s}$. El Lema 5.2.1 implica que la hipersuperficie $\{\rho^h_{\boldsymbol{\lambda}^s} = 0\}$ de $\mathbb{P}^n$ corta a $\overline{\mathcal{V}}_{s+1}$ propiamente. Por [DKS13, Corollary 2.62] concluimos que

$$\widehat{h}\big(\overline{\mathcal{V}}_{s+1} \cap \{\rho^h_{\boldsymbol{\lambda}^s} = 0\}\big) \le \deg \rho_{\boldsymbol{\lambda}^s}\, \widehat{h}\big(\overline{\mathcal{V}}_{s+1}\big) + \deg \overline{\mathcal{V}}_{s+1}\, h(\rho^h_{\boldsymbol{\lambda}^s}) + \deg \overline{\mathcal{V}}_{s+1} \deg \rho^h_{\boldsymbol{\lambda}^s}\, \log(n+2).$$

Puesto que $\overline{\mathcal{V}}_{s+1} \cap \{\rho^h_{\boldsymbol{\lambda}^s} = 0\}$ es equidimensional de dimensión $n-s-2$ y contiene toda componente de $\overline{\mathcal{W}}_{\boldsymbol{\lambda}^s}$, vemos que $\widehat{h}\big(\overline{\mathcal{W}}_{\boldsymbol{\lambda}^s}\big) \le \widehat{h}\big(\overline{\mathcal{V}}_{s+1} \cap \{\rho^h_{\boldsymbol{\lambda}^s} = 0\}\big)$. Recordando que $\widehat{h}(\mathcal{V}_{s+1}) = \widehat{h}(\overline{\mathcal{V}}_{s+1})$ y $\deg \mathcal{V}_{s+1} = \deg \overline{\mathcal{V}}_{s+1}$, y teniendo en cuenta que $\deg \rho^h_{\boldsymbol{\lambda}^s} = \deg \rho_{\boldsymbol{\lambda}^s}$ y $h(\rho^h_{\boldsymbol{\lambda}^s}) = h(\rho_{\boldsymbol{\lambda}^s})$, obtenemos

$$\deg \mathcal{W}_{\boldsymbol{\lambda}^s} \le \deg \mathcal{V}_{s+1} \deg \rho_{\boldsymbol{\lambda}^s},$$
$$\widehat{h}(\mathcal{W}_{\boldsymbol{\lambda}^s}) \le \deg \rho_{\boldsymbol{\lambda}^s}\, \widehat{h}(\mathcal{V}_{s+1}) + \deg \mathcal{V}_{s+1}\, h(\rho_{\boldsymbol{\lambda}^s}) + \deg \mathcal{V}_{s+1}\, \deg \rho_{\boldsymbol{\lambda}^s}\, \log(n+2).$$

Por (6.1) tenemos que $\widehat{h}(\mathcal{V}_{s+1}) \in \mathcal{O}^{\sim}\big(d^s(h+d)\big)$. Por lo tanto, por el Lema 6.1.4 concluimos que

$$\deg \mathcal{W}_{\boldsymbol{\lambda}^s} \in \mathcal{O}(nd^{3s+1}), \quad \widehat{h}(\mathcal{W}_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^{\sim}\big(nd^{3s}(h+d)\big).$$

Combinando estas estimaciones con (6.12) y (6.13), y teniendo en cuenta que $h(Y_\ell) \in \mathcal{O}^{\sim}(r \log d + \log n)$ para todo ℓ, la segunda afirmación del lema se sigue fácilmente. □

Ahora estimamos la altura de $\beta_{\boldsymbol{\lambda}^s}$.

Lema 6.3.3. *Sea $1 \le s \le r-1$ y supóngase que $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$. Entonces existe $\beta_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ como en (5.9) con $h(\beta_{\boldsymbol{\lambda}^s}) \in \mathcal{O}^{\sim}\big(n^3 d^{8s+1}(h+rd)\big)$.*

Demostración. Sea $d_j = \deg f_j$ and $h_j := h(f_j)$ para $1 \le j \le s+1$, y $d_{s+2} := \deg \rho_{\boldsymbol{\lambda}^s}$ y $h_{s+2} := h(\rho_{\boldsymbol{\lambda}^s})$. Además, defínase $d_0 := \deg B_{\boldsymbol{\lambda}^s}(Y_1, \ldots, Y_{n-s-1})$ y $h_0 := h(B_{\boldsymbol{\lambda}^s}(Y_1, \ldots, Y_{n-s-1}))$. Finalmente, nótese $D := \prod_{j=1}^{s+2} d_j$ y $H := \max_{1 \le j \le s+2} h_j$. Por [DKS13, Theorem 2], teniendo en cuenta que $\deg \mathbb{A}^n = 1$ y $\widehat{h}(\mathbb{A}^n) = 0$, se sigue que existe $\beta_{\boldsymbol{\lambda}^s} \in \mathbb{Z} \setminus \{0\}$ como en (5.9) con

$$h(\beta_{\boldsymbol{\lambda}^s}) \le 2d_0 D \left(\frac{3h_0}{2d_0} + \sum_{\ell=1}^{s+2} \frac{H}{d_\ell} + e(n) \right),$$

donde $e(n) \in \mathcal{O}^{\sim}(n)$. Ahora, por el Lema 6.1.4 tenemos que $h_{s+2} \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+d)\big)$. Puesto que $H = \max\{h, h_{s+2}\}$, deducimos que $H \in \mathcal{O}^{\sim}\big(nd^{2s-1}(h+d)\big)$. Por otra parte, $d_0 \le \deg B_{\boldsymbol{\lambda}^s} \in \mathcal{O}^{\sim}(nd^{3s+1})$ por (6.11) y $D \le d^{s+1} d_{s+2} \in \mathcal{O}^{\sim}(nd^{3s+1})$. Esto implica que

$$d_0 D \left(\sum_{\ell=1}^{s+2} \frac{H}{d_\ell} + e(n) \right) \in \mathcal{O}^{\sim}\big(n^3 d^{8s+1}(h+d)\big). \tag{6.14}$$

Puesto que $h(\boldsymbol{\lambda}^s) \leq h(\mathsf{a})$ para todo s, por [DKS13, Lemma 2.37 (3)] tenemos que

$$h_0 \leq h(B_{\boldsymbol{\lambda}^s}) + \deg B_{\boldsymbol{\lambda}^s}\big(h(\mathsf{a}) + \log(n-s) + \log(n+1)\big).$$

Combinando esto con (6.11) y la Observación 6.1.1 deducimos que $h_0 \in \mathcal{O}^{\sim}\big(nd^{3s}(h+rnd)\big)$. Por lo tanto $Dh_0 \in \mathcal{O}^{\sim}\big(n^2d^{6s+1}(h+rnd)\big)$ lo que, junto con (6.14), prueba el lema. □

Finalmente estamos en condiciones de estimar la altura de $\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})$.

Corolario 6.3.4. $h\big(\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) \in \mathcal{O}^{\sim}\big(n^3d^{8s+1}(h+rd)\big)$ *para* $1 \leq s \leq r-1$.

Demostración. Obsérvese que $h\big(\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) = h(\beta_{\boldsymbol{\lambda}^s}) + h\big(B_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big)$ para $\mathcal{W}_{\boldsymbol{\lambda}^s} \neq \emptyset$, y que $h\big(\mathsf{L}_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) = h(\mu_{\boldsymbol{\lambda}^s})$ para $\mathcal{W}_{\boldsymbol{\lambda}^s} = \emptyset$. Puesto que $h(\boldsymbol{p}^{s+1}) \leq h(\mathsf{b})$, por [DKS13, Lemma 2.37 (3)] tenemos que

$$h\big(B_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) \leq h(B_{\boldsymbol{\lambda}^s}) + \deg B_{\boldsymbol{\lambda}^s}\,\big(h(\mathsf{b}) + \log(n-s)\big).$$

Teniendo en cuenta la Observación 6.1.1 y (6.11), de la desigualdad anterior deducimos $h\big(B_{\boldsymbol{\lambda}^s}(\boldsymbol{p}^{s+1})\big) \in \mathcal{O}^{\sim}\big(nd^{3s}(h+rnd)\big)$. Comparando esto con (6.10) y el Lema 6.3.3 obtenemos la estimación del lema. □

Como consecuencia del Lema 6.3.1 y del Corolario 6.3.4 estamos en condiciones de estimar la altura del múltiplo $\mathfrak{N}$ de todos los primos "unlucky".

Teorema 6.3.5. *El entero* $\mathfrak{N}$ *de* (6.2) *satisface* $h(\mathfrak{N}) \in \mathcal{O}^{\sim}\big(n^3d^{8r-7}(h+rd)\big)$.

Demostración. Nótese que $h(\det \boldsymbol{\lambda}) \leq \log(n!) + nh(\mathsf{a}) \in \mathcal{O}^{\sim}(rn)$. Esto, junto con el Lema 6.3.1 y el Corolario 6.3.4, fácilmente implican el teorema. □

Capítulo 7

Cálculo de una representación de Kronecker

Sean $F_1, \ldots, F_r \in \mathbb{Z}[\boldsymbol{X}]$, como en el Capítulo 5, polinomios que definen una sucesión regular reducida. En esta sección describimos un algoritmo y establecemos una cota superior para la complejidad bit del cálculo de una representación de Kronecker de una fibra cero–dimensional $\pi_r^{-1}(\boldsymbol{p}^r)$ de $\mathcal{V}(F_1, \ldots, F_r)$. Con este propósito, siguiendo la sugerencia de [GLS01], realizamos este cálculo módulo un número primo p y aplicamos levantamiento p–ádico para recuperar los enteros de una representación de Kronecker de $\pi_r^{-1}(\boldsymbol{p}^r)$ sobre $\mathbb{Q}$. Suponiendo dado un primo "lucky" p, la complejidad del cálculo de una representación de Kronecker de una fibra cero–dimensional de $\mathcal{V}(F_{1,p}, \ldots, F_{r,p})$ fue analizada en [CM06]. Por otra parte, la complejidad del paso de levantamiento p–ádico fue analizada en [GLS01]. Consecuentemente, en este capítulo analizamos el costo de calcular un primo "lucky" (Proposición 7.1.2) y obtenemos una cota superior para la complejidad bit del cálculo de una representación de Kronecker de $\pi_r^{-1}(\boldsymbol{p}^r)$ sobre $\mathbb{Q}$ (Teorema 7.3.1).

7.1. Cálculo de una representación de Kronecker módulo p

Sean $\mathsf{S} := \{0, \ldots, \mathsf{a}\}$ y $\mathsf{T} := \{0, \ldots, \mathsf{b}\}$, donde $\mathsf{a} := \lfloor 8\mathsf{D} \rfloor$ y $\mathsf{b} := \lfloor 9\mathsf{D} \rfloor$. Supóngase que hemos elegido $(\boldsymbol{\lambda}, \boldsymbol{p}) \in \mathsf{S}^{n^2} \times \mathsf{T}^{n-1}$ al azar. El siguiente resultado afirma que esta elección satisface $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ y $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$ con alta probabilidad.

Lema 7.1.1. *Sea $(\boldsymbol{\lambda}, \boldsymbol{p})$ un punto elegido uniformemente al azar en $\mathsf{S}^{n^2} \times \mathsf{T}^{n-1}$. Entonces $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ y $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$ con probabilidad mayor que $\frac{7}{9}$.*

Demostración. Puesto que $\deg \mathsf{R} \leq D$, por el Lema 2.2.1 vemos que para una elección al azar de $\boldsymbol{\lambda}$ en S^{n^2} resulta $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ con probabilidad mayor que $\frac{7}{8}$. De forma similar, puesto que $\deg(\mathsf{N}_{\boldsymbol{\lambda}}) \leq D$, para un punto $\boldsymbol{p}$ elegido uniformemente al azar en T^{n-1}, la probabilidad condicional de que $\mathsf{N}_{\boldsymbol{\lambda}}(\boldsymbol{p}) \neq 0$, dado que $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$, es mayor que $\frac{8}{9}$. Esto concluye la demostración del lema. □

Para una tal elección de $\boldsymbol{\lambda}$ y $\boldsymbol{p}$, sea $\mathfrak{N}$ el entero del Teorema 5.3.1. De acuerdo con el Teorema 6.3.5 podemos elegir $\mathfrak{H} \in \mathbb{N}$ tal que

$$h(\mathfrak{N}) \leq \mathfrak{H} \quad \text{y} \quad \log \mathfrak{H} \in \mathcal{O}^{\sim}\big(\log(d^r nh)\big). \tag{7.1}$$

Ahora podemos estimar la complejidad del cálculo de un primo "lucky" p de "baja" longitud bit.

Proposición 7.1.2. *Existe un algoritmo probabilístico que toma $\mathfrak{H}$ como entrada y calcula un primo p con $12\mathfrak{H} + 1 \leq p \leq 24\mathfrak{H}$ tal que $p \nmid \mathfrak{N}$. El algoritmo utiliza $\mathcal{O}^{\sim}\big(\log^2(d^r nh)\big)$ operaciones bit y su resultado es correcto con probabilidad al menos $\frac{3}{4}$.*

Demostración. La proposición se sigue aplicando el Lema 2.2.2 con $B = m\mathfrak{H}$, $M = \mathfrak{N}$, $m = 12$ y $k = 5 + \log\log(12\mathfrak{H})$, y teniendo en cuenta (7.1). □

Supóngase que hemos calculado un primo "lucky" p como en la Proposición 7.1.2. Supóngase además que tenemos un straight–line program de longitud a lo sumo L, sin divisiones y con parámetros enteros, que representa los polinomios $F_1, \ldots, F_r$. Sea $\boldsymbol{Y} := (Y_1, \ldots, Y_n) := \boldsymbol{\lambda X}$. Como sabemos, la matriz $\boldsymbol{\lambda}_p$ es no singular y las formas lineales $\boldsymbol{Y}_p := (Y_{1,p}, \ldots, Y_{n,p})$ forman un nuevo conjunto de variables para $\mathbb{F}_p[\boldsymbol{X}]$. Como en el Capítulo 5 denotamos con $F_j(Y_1, \ldots, Y_n)$ el polinomio que se obtiene expresando a F_j en las variables $Y_1, \ldots, Y_n$ para $1 \leq j \leq r$. Definimos de manera similar $F_{j,p}(Y_{1,p}, \ldots, Y_{n,p})$ $(1 \leq j \leq r)$. Los algoritmos que se describen más abajo suponen que previamente se ha realizado el cambio de variables $(X_1, \ldots, X_n) \to (Y_1, \ldots, Y_n)$, lo que no afecta significativamente el costo de representación de los polinomios de entrada. En efecto, la identidad $\boldsymbol{X} = \boldsymbol{\lambda}_p^{-1} \boldsymbol{Y}_p$ se puede interpretar como un straight–line program σ en $\mathbb{F}_p[Y_{1,p}, \ldots, Y_{n,p}]$ con entradas $Y_{1,p}, \ldots, Y_{n,p}$ cuyo conjunto de parámetros está formado por los parámetros de β y por las entradas de $\boldsymbol{\lambda}_p^{-1}$. Es claro que σ contiene n^2 multiplicaciones por escalares en $\mathbb{F}_p$ y $n(n-s)$ sumas en $\mathbb{F}_p[\boldsymbol{Y}_p]$. Concatenando σ con β obtenemos el siguiente resultado.

Observación 7.1.3. *A partir de β y $\boldsymbol{\lambda}_p^{-1}$ obtenemos un straight–line program β_p en $\mathbb{F}_p[Y_{1,p}, \ldots, Y_{n,p}]$, sin divisiones, de longitud a lo sumo $L + 2n^2 - n$, que representa los polinomios $F_{1,p}(Y_{1,p}, \ldots, Y_{n,p}), \ldots, F_{r,p}(Y_{1,p}, \ldots, Y_{n,p})$.*

En lo que sigue suponemos que el cambio de variables $\boldsymbol{Y} = \boldsymbol{\lambda X}$ ya ha sido realizado y por simplicidad escribimos $F_1, \ldots, F_r$ en lugar de $F_1(\boldsymbol{Y}), \ldots, F_r(\boldsymbol{Y})$.

Puesto que claramente el entero $\mathfrak{H}$ de (7.1) puede elegirse con $\mathfrak{H} \geq 5n^2 d\delta^4$, podemos suponer que $p > 60n^2 d\delta^4$. Por lo tanto podemos aplicar el algoritmo descripto en [CM06] para calcular la representación de Kronecker de la fibra de levantamiento $V_{\boldsymbol{p}_p^r}$.

El algoritmo comienza calculando la representación de Kronecker de la fibra $V_{\boldsymbol{p}_p^1}$ de la hipersuperficie $\{F_{1,p} = 0\}$ con $Y_{n,p}$ como elemento primitivo. Con las notaciones de la Proposición 5.3.3, tal representación consiste solo del polinomio minimal $Q^1\big(\boldsymbol{p}^1, T\big)$ de $Y_{n,p}$ módulo $\mathcal{J}_{1,p}$. Puesto que, con las notaciones del Capítulo 4, es $\mathcal{J}_{1,p} = \big(F_{1,p}(\boldsymbol{p}_p^1, Y_{n,p})\big)$, vemos que $\overline{\mathbb{F}}_p[V_{\boldsymbol{p}_p^1}] = \overline{\mathbb{F}}_p[Y_{n,p}]/\big(F_{1,p}(\boldsymbol{p}_p^1, Y_{n,p})\big)$. Se sigue que $Q^1\big(\boldsymbol{p}_p^1, T\big)$ coincide con el polinomio $F_{1,p}(\boldsymbol{p}_p^1, T)$ dividido por su coeficiente principal.

Luego el algoritmo procede en $r-1$ etapas. Para $s \in \{1, \ldots, r-1\}$, la s–ésima etapa recibe como entrada una representación de Kronecker $Q^s(\boldsymbol{p}_p^s, T), W_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, W_n^s(\boldsymbol{p}_p^s, T)$ de $\mathcal{J}_{s,p}$ y entrega como salida una representación de Kronecker $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T), W_{n-s+1}^{s+1}(\boldsymbol{p}_p^{s+1}, T), \ldots, W_n^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ de $\mathcal{J}_{s+1,p}$. Esta etapa, cuyo costo se analiza más abajo, consiste en dos tareas principales, llamadas el paso de levantamiento y el paso de intersección.

Previamente estimamos el costo del pasaje de una representación a otra.

Lema 7.1.4. *El pasaje de una representación de Kronecker a una representación univariada de $\mathcal{J}_{s,p}$ o viceversa se puede realizar con complejidad bit $\mathcal{O}^{\sim}\big(s\delta_s \log p\big)$.*

Demostración. Por el Lema 2.1.28, un cambio de representación de $\mathcal{J}_{s,p}$ con el mismo elemento primitivo requiere $s-1$ multiplicaciones y a lo sumo una inversión en $\mathbb{F}_p[T]/(Q^s(\boldsymbol{p}_p^s, T))$. El lema se sigue teniendo en cuenta que tanto una multiplicación como una inversión en $\mathbb{F}_p[T]/(Q^s(\boldsymbol{p}_p^s, T))$ se pueden realizar por medio del Algoritmo de Euclides extendido con $\mathcal{O}^{\sim}(\delta_s)$ operaciones aritméticas en $\mathbb{F}_p$. □

Paso de levantamiento

En el paso de levantamiento calculamos la representación de Kronecker $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), W_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ de $\mathcal{K}_{s,p}$ con elemento primitivo $Y_{n-s+1,p}$, a partir de la representación univariada de $\mathcal{J}_{s,p}$ con el mismo elemento primitivo $Y_{n-s+1,p}$. Ahora bien, por la Observación 4.3.2, vemos que es suficiente calcular $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), W_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ con precisión $(Y_{n-s,p} - p_{n-s,p})^{\delta_s+1}$ en $\mathbb{F}_p[Y_{n-s,p}, T]$.

La herramienta básica para realizar este cálculo es el Algoritmo de Newton global de [GLS01] que resumimos en la siguiente proposición. Si h es un entero positivo, denotamos con $\mathsf{a}(h)$ el costo de las operaciones aritméticas en R/I^h.

Proposición 7.1.5. *Sea R un anillo conmutativo íntegro e I un ideal de R. Sea k una potencia de 2. Existe un algoritmo que toma como entrada:*

- *n polinomios $\boldsymbol{F} := (F_1, \ldots, F_n)$ en $R[\boldsymbol{X}]$ dados por un straight–line program β de longitud L;*
- *una forma lineal $U := \lambda_1 X_1 + \cdots + \lambda_n X_n$ en $R[\boldsymbol{X}]$;*
- *un polinomio mónico $q(T)$ de grado δ en $R[T]$;*
- *n polinomios $\boldsymbol{v} := (v_1, \ldots, v_n)$ de grados estrictamente menores que δ en $R[T]$;*

tales que en $(R/I)[T]/(q(T))$ se satisfacen las siguientes condiciones:

- *$\boldsymbol{F}(\boldsymbol{v}) \equiv 0$;*
- *$T \equiv U(\boldsymbol{v})$;*
- *si J es el determinante Jacobiano de $F_1, \ldots, F_n$ con respecto a $X_1, \ldots, X_n$, $J(\boldsymbol{v})$ es inversible;*

y entrega como salida:

- *un polinomio mónico $Q(T)$ de grado δ en $R[T]$ tal que $Q \equiv q \mod R[T]I$;*
- *n polinomios $\boldsymbol{V} := (V_1, \ldots, V_n)$ de grados estrictamente menores que δ tales que $V_i \equiv v_i \mod R[T]I$ para $1 \leq i \leq n$ y que satisfacen*

$$\boldsymbol{F}(\boldsymbol{V}) \equiv 0 \quad y \quad T \equiv U(\boldsymbol{V}) \quad en \quad (R/I^k)[T]/(Q(T)).$$

Los coeficientes de Q y $\boldsymbol{V}$ están únivocamente determinados por las condiciones anteriores módulo I^k. El algoritmo se ejecuta con complejidad

$$\mathcal{O}\big((nL + n^4)\mathcal{M}(\delta) \sum_{j=0}^{\log k} \mathsf{a}(2^j)\big).$$

Sea $Q^s(\boldsymbol{p}_p^s, T), V_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, V_n^s(\boldsymbol{p}_p^s, T)$ la representación univariada de $\mathcal{J}_{s,p}$ con elemento primitivo $Y_{n-s+1,p}$. Observemos que por la Proposición 5.3.4 tal representación es la especialización en $Y_{n-s,p} = p_{n-s,p}$ de la representación univariada $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), V_{n-s+2}^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, V_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ de $\mathcal{K}_{s,p}$ con elemento primitivo $Y_{n-s+1,p}$. Notemos además que, si J es el determinante Jacobiano de $F_{1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}), \ldots, F_{s,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ con respecto a $Y_{n-s+1,p}, \ldots, Y_{n,p}$, entonces la especialización de J en $Y_{n-s,p} = p_{n-s,p}$ coincide con el determinante Jacobiano de $F_{1,p}(\boldsymbol{p}_p^s, Y_{n-s+1,p}, \ldots, Y_{n,p}), \ldots, F_{s,p}(\boldsymbol{p}_p^s, Y_{n-s+1,p}, \ldots, Y_{n,p})$ con respecto a $Y_{n-s+1,p}, \ldots, Y_{n,p}$ y que, por el Lema 4.1.4, este determinante es inversible en $\mathbb{F}_p[Y_{n-s+1,p}, \ldots, Y_{n,p}]/\mathcal{J}_{s,p}$. A partir de estas observaciones es claro que, si $\boldsymbol{X} := (Y_{n-s+1,p}, \ldots, Y_{n,p})$, $R := \mathbb{F}_p[Y_{n-s,p}]$ e $I \subset R$ es el ideal $I := (Y_{n-s,p} - p_{n-s,p})$, las condiciones de la Proposición 7.1.5 se satisfacen para $U := Y_{n-s+1}$, $q(T) := Q^s(\boldsymbol{p}_p^s, T)$, $\boldsymbol{F} := \big(F_{1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}), \ldots, F_{s,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})\big)$ y $\boldsymbol{v} := \big(T, V_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, V_n^s(\boldsymbol{p}_p^s, T)\big)$.

En consecuencia, si $k := 2^{\lfloor \log(\delta_s+1) \rfloor}$, el algoritmo de la Proposición 7.1.5 calcula los polinomios $Q^s(\boldsymbol{p}^{s+1}, Y_{n-s,p}, T)$, $V_{n-s+2}^s(\boldsymbol{p}^{s+1}, Y_{n-s,p}, T), \ldots, V_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ con precisión $(Y_{n-s,p} - p_{n-s})^{\delta_s+1}$. Luego, $W_{n-s+2}^s(\boldsymbol{p}^{s+1}, Y_{n-s,p}, T), \ldots, W_n^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ se pueden obtener a partir de las identidades

$$W_j^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T) \equiv V_j^s(\boldsymbol{p}^{s+1}, Y_{n-s,p}, T) \frac{d}{dT} Q^s(\boldsymbol{p}^{s+1}, Y_{n-s,p}, T) \quad (n-s+2 \leq j \leq n)$$

en el anillo $(R/I^k)[T]/(Q^s(\boldsymbol{p}^{s+1}, Y_{n-s,p}, T))$. En conclusión, obtenemos el siguiente resultado.

Proposición 7.1.6. *Existe un algoritmo determinístico que recibe como entrada:*

- *un straight–line program de longitud L que representa los polinomios $F_{1,p}, \ldots, F_{s,p}$;*
- *la representación densa de los polinomios en $\mathbb{F}_p[T]$ que forman la representación univariada de $\mathcal{J}_{s,p}$ con elemento primitivo $Y_{n-s+1,p}$;*

y entrega como salida la representación densa de los polinomios en $\mathbb{F}_p[Y_{n-s,p}, T]$ que forman la representación de Kronecker de $\mathcal{K}_{s,p}$ con elemento primitivo $Y_{n-s+1,p}$. El algoritmo utiliza $\mathcal{O}^{\sim}\big((nL+n^4)\delta_s^2 \log p\big)$ operaciones bit.

Demostración. En este caso $\mathsf{a}(h)$ es la complejidad bit de las operaciones aritméticas en $\mathbb{F}_p[Y_{n-s,p}]/(Y_{n-s,p}-p_{n-s})^h$, con lo cual $\mathsf{a}(h) \in \mathcal{O}\big(\mathcal{M}(h)\mathcal{U}(\log p)\big)$. Dado que

$$\sum_{j=0}^{\lfloor \log(\delta_s+1)\rfloor} \mathcal{M}(2^j) \leq \mathcal{M}(k) \sum_{j=0}^{\lfloor \log(\delta_s+1)\rfloor} 1/2^j \in \mathcal{O}(\mathcal{M}(\delta_s)),$$

deducimos que el algoritmo de la Proposición 7.1.5 calcula las aproximaciones de $Q^s(\boldsymbol{p}^{s+1}, Y_{n-s,p}, T)$, $V^s_{n-s+2}(\boldsymbol{p}^{s+1}, Y_{n-s,p}, T), \ldots, V^s_n(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}, T)$ con precisión $(Y_{n-s,p}-p_{n-s,p})^{\delta_s+1}$ utilizando $\mathcal{O}\big((nL+n^4)\mathcal{M}(\delta_s)^2\mathcal{U}(\log p)\big)$ operaciones bit. Teniendo en cuenta que una multiplicación en $(R/I^k)[T]/(Q^s(\boldsymbol{p}^{s+1}, Y_{n-s,p}, T))$ requiere $\mathcal{O}(\mathcal{M}(\delta_s))$ operaciones aritméticas en $R/I^k = \mathbb{F}_p[Y_{n-s,p}]/(Y_{n-s,p}-p_{n-s,p})^{\delta_s+1}$, y por lo tanto $\mathcal{O}\big(\mathcal{M}(\delta_s)^2\mathcal{U}(\log p)\big)$ operaciones bit, se deduce que el procedimiento se ejecuta en la complejidad bit anunciada en la proposición. □

Paso de intersección

La entrada del paso de intersección es la salida del algoritmo de la Proposición 7.1.6, a saber, la representación de Kronecker de $\mathcal{K}_{s,p}$ con elemento primitivo $Y_{n-s+1,p}$. Sea $Q^s(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}, T), V^s_{n-s+2}(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}, T), \ldots, V^s_n(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}, T)$ la correspondiente representación univariada. La salida es la representación univariada $Q^{s+1}(\boldsymbol{p}^{s+1}_p, T), V^s_{n-s+1}(\boldsymbol{p}^{s+1}_p, T), \ldots, V^{s+1}_n(\boldsymbol{p}^{s+1}_p, T)$ de $\mathcal{J}_{s+1,p}$ con elemento primitivo $Y_{n-s,p}$. Considérese $F_{s+1,p}$ como un elemento de $\mathbb{F}_p[Y_{1,p}, \ldots, Y_{n,p}]$ y defínase $h \in \mathbb{F}_p(Y_{n-s,p})[T]$ por

$$h(T) := F_{s+1,p}\big(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}, T, V^s_{n-s+2}(\boldsymbol{p}^{s+1}_p, T), \ldots, V^s_n(\boldsymbol{p}^{s+1}_p, T)\big) \\ \text{mód } \big(Q^s(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}, T)\big).$$

El siguiente resultado proporciona una expresión para $Q^{s+1}(\boldsymbol{p}^{s+1}_p, T)$ a partir de la cual podremos calcular este polinomio eficientemente.

Proposición 7.1.7. *Se satisface*

$$Q^{s+1}(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}) = \epsilon \operatorname{Res}_T\big(h(T), Q^s(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}, T)\big),$$

para algún $\epsilon \in \mathbb{F}_p \setminus \{0\}$.

Demostración. Sea M_h la matriz de la homotecia de multiplicación por h en $\overline{\mathbb{F}}_p(Y_{n-s,p})[T]/\big(Q^s(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}, T)\big)$ con respecto a la base $\{1, T, \ldots, T^{\delta_s-1}\}$. Tenemos que (ver, por ejemplo, [EM07, Proposition 5.4]):

$$\det(M_h) = \operatorname{Res}_T\big(h(T), Q^s(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}, T)\big).$$

Considérese el isomorfismo de $\overline{\mathbb{F}}_p(Y_{n-s,p})$–álgebras

$$\Phi : \overline{\mathbb{F}}_p(Y_{n-s,p})[Y_{n-s+1,p}, \ldots, Y_{n,p}]/\overline{\mathcal{K}}^e_{s,p} \to \overline{\mathbb{F}}_p(Y_{n-s,p})[T]/\big(Q^s(\boldsymbol{p}^{s+1}_p, Y_{n-s,p}, T)\big),$$

que aplica $Y_{n-s+1,p}$ mód $\overline{\mathcal{K}}^e_{s,p}$ en T mód $\big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big)$. Sea S una nueva indeterminada y $\chi \in \overline{\mathbb{F}}_p[Y_{n-s,p}][S]$ el polinomio característico de la homotecia de multiplicación por $F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ módulo $\overline{\mathcal{K}}^e_{s,p}$. Sea $\chi_0 \in \mathbb{F}_p[Y_{n-s,p}]$ el término constante de χ. Puesto que Φ aplica $F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})$ mód $\overline{\mathcal{K}}^e_{s,p}$ en h mód $\big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big)$, χ coincide con el polinomio característico de la homotecia de multiplicación por h módulo $\big(Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)\big)$. Por lo tanto $\chi_0 = (-1)^{\delta_s} \det(M_h)$. Por otra parte, como la hipersuperficie $\{F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}) = 0\}$ interseca la curva de levantamiento $\mathcal{W}_{\boldsymbol{p}_p^{s+1}}$ en la fibra finita $V_{\boldsymbol{p}_p^{s+1}}$, el polinomio $F_{s+1,p}\big(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p}\big)$ no es un divisor de cero en $\overline{\mathbb{F}}_p[Y_{n-s,p}, \ldots, Y_{n,p}]/\overline{\mathcal{K}}_{s,p}$. Puesto que $\overline{\mathcal{J}}_{s+1,p} = \overline{\mathcal{K}}_{s,p} + \big(F_{s+1,p}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, \ldots, Y_{n,p})\big)$, por [DL08, Proposition 2.7] deducimos que $\chi_0(T)$ coincide, salvo multiplicación por elementos de $\mathbb{F}_p \setminus \{0\}$, con el polinomio característico de $Y_{n-s,p}$ en $\overline{\mathbb{F}}_p[Y_{n-s,p}, \ldots, Y_{n,p}]/\overline{\mathcal{J}}_{s+1,p}$. Puesto que $Y_{n-s,p}$ induce un elemento primitivo para $\overline{\mathcal{J}}_{s+1,p}$, concluimos que $\chi_0(T) = \epsilon Q^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ para algún $\epsilon \in \overline{\mathbb{F}}_p \setminus \{0\}$. Esto finaliza la demostración de la Proposición. □

Ahora discutimos el cálculo de los polinomios $V^{s+1}_{n-s+1}(\boldsymbol{p}_p^{s+1},T), \ldots, V^{s+1}_n(\boldsymbol{p}_p^{s+1},T)$. Sea $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T) = q_1 \cdots q_\ell$ la factorización en irreducibles de $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ en $\mathbb{F}_p[T]$. A continuación describimos cómo calcular $V_j^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ mód q_k para $n - s + 1 \le j \le n$ y $1 \le k \le \ell$. Luego los polinomios $V_j^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ se pueden recuperar por medio del Teorema chino del resto. Para $1 \le k \le \ell$, sea a la clase residual de T en $\mathbb{F}_p[T]/(q_k)$. Sea $\mathbb{L} = \mathbb{F}_p[T]/(q_k)$. Por lo tanto, $\mathbb{L} := \mathbb{F}_p[a]$ es una extensión finita de $\mathbb{F}_p$ que contiene a la raíz a de $Q^{s+1}(\boldsymbol{p}_p^{s+1}, T)$. Sea $\overline{\mathbb{L}}$ la clausura algebraica de $\mathbb{L}$. Tenemos un isomorfismo de cuerpos $\overline{\mathbb{L}} = \overline{\mathbb{F}}_p$. Por la Observación 5.2.3 sabemos que $\rho_s\big(\boldsymbol{\lambda}_p^s, (\boldsymbol{p}_p^{s+1}, a)\big) \neq 0$. Por lo tanto, $(\boldsymbol{p}_p^{s+1}, a)$ es un punto de levantamiento de $\pi_{s,p}$ e $Y_{n-s+1,p}$ induce un elemento primitivo de la fibra de levantamiento $\pi_{s,p}^{-1}(\boldsymbol{p}_p^{s+1}, a)$. Además, $\mathcal{K}_{s,p} + (Y_{n-s} - a)$ es un ideal radical de $\overline{\mathbb{F}}_p[\boldsymbol{X}]$ por el Lema 4.1.2, y en consecuencia es el ideal anulador de $\pi_{s,p}^{-1}(\boldsymbol{p}_p^{s+1}, a)$. Sea $q_a, w_{a,n-s+2}, \ldots, w_{a,n}$ la representación de Kronecker de $\mathcal{K}_{s,p} + (Y_{n-s} - a)$ con elemento primitivo $Y_{n-s+1,p}$. Sea $Q_p^s, W^s_{n-s+2,p}, \ldots, W^s_{n,p}$ la representación de Kronecker de $\mathcal{I}_{s,p}$ con elemento primitivo $Y_{n-s+1,p}$. Por la Proposición 4.3.3 las especializaciones de $Q_p^s, W^s_{n-s+2,p}, \ldots, W^s_{n,p}$ en $Y_{1,p} = p_{1,p}, \ldots, Y_{n-s-1,p} = p_{n-s-1,p}, Y_{n-s,p} = a$ coinciden con $q_a, w_{a,n-s+2}, \ldots, w_{a,n}$. Puesto que los polinomios de entrada $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$, $W^s_{n-s+2}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W^s_n(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T)$ coinciden con las especializaciones de $Q_p^s, W^s_{n-s+2,p}, \ldots, W^s_{n,p}$ en $Y_{1,p} = p_{1,p}, \ldots, Y_{n-s-1,p} = p_{n-s-1,p}$, vemos que $q_a, w_{a,n-s+2}, \ldots, w_{a,n}$ se pueden obtener sustituyendo $Y_{n-s,p}$ por a en $Q^s(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), W^s_{n-s+2}(\boldsymbol{p}_p^{s+1}, Y_{n-s,p}, T), \ldots, W^s_n(\boldsymbol{p}$
Por lo tanto podemos calcular la correspondiente representación univariada $q_a, v_{a,n-s+2}, \ldots, v_{a,n}$ mediante las identidades $v_{a,j} = (q_a')^{-1} w_{a,j}$ mód q_a para $n - s + 2 \le j \le n$. Sea $g(Y_{n-s+1,p}) := F_{s+1,p}\big(\boldsymbol{p}_p^{s+1}, a, Y_{n-s+1,p}, v_{a,n-s+2}(Y_{n-s+1,p}), \ldots, v_{a,n}(Y_{n-s+1,p})\big)$. Ahora $V^{s+1}_{n-s+1}(\boldsymbol{p}_p^{s+1}, a), \ldots, V^{s+1}_n(\boldsymbol{p}_p^{s+1}, a)$ se puede calcular utilizando las siguientes identidades (ver, por ejemplo, [DL08]):

$$
\begin{aligned}
Y_{n-s+1,p} - V^{s+1}_{n-s+1}(\boldsymbol{p}_p^{s+1}, a) &= \gcd\big(g(Y_{n-s+1,p}), q_a(Y_{n-s+1,p})\big), \\
V_j^{s+1}(\boldsymbol{p}_p^{s+1}, a) &= v_{a,j}\big(V^{s+1}_{n-s+2}(\boldsymbol{p}_p^{s+1}, a)\big) \quad (n - s + 2 \le j \le n).
\end{aligned}
$$

Más precisamente, estas identidades nos permiten calcular $V_j^{s+1}(\boldsymbol{p}_p^{s+1}, T) \mod Q_k$ para $n-s+1 \leq j \leq n$. Habiendo hecho esto para $1 \leq k \leq \ell$, podemos recuperar $V_{n-s+1}^{s+1}(\boldsymbol{p}_p^{s+1}, T), \ldots, V_n^{s+1}(\boldsymbol{p}_p^{s+1}, T)$ por el Teorema chino del resto.

Como se muestra en [CM06, Section 4], los cálculos anteriores pueden transformarse en un procedimiento efectivo a partir del cual obtenemos el siguiente resultado (ver [CM06, Proposition 4.7]).

Proposición 7.1.8. *Existe a algoritmo probabilístico que recibe como entrada*

- *un straight–line program de longitud a lo sumo L que representa el polinomio $F_{s+1,p}$;*
- *la representación densa de los polinomios en $\mathbb{F}_p[Y_{n-s,p}, T]$ que forman la representación de Kronecker de $\mathcal{K}_{s,p}$ con elemento primitivo $Y_{n-s+1,p}$;*

y entrega como salida la representación densa de los polinomios en $\mathbb{F}_p[T]$ que forman la representación univariada de $\mathcal{J}_{s+1,p}$ con elemento primitivo $Y_{n-s,p}$. Este algoritmo utiliza un número esperado de $\mathcal{O}^{\sim}\big((L+n)\delta_s(d\delta_s + \log p)\log p\big)$ operaciones bit y devuelve el resultado correcto con probabilidad al menos $1 - 1/60n$.

Teniendo en cuenta las estimaciones de complejidad y de probabilidad del Lema 7.1.4 y de las Proposiciones 7.1.6 y 7.1.8 para $1 \leq s \leq r-1$, fácilmente deducimos el siguiente resultado.

Teorema 7.1.9. *Existe a algoritmo probabilístico que recibe como entrada*

- *un primo "lucky" p como en la Proposición 7.1.2;*
- *los puntos $\boldsymbol{\lambda}_p \in \mathbb{F}_p^{n^2}$ y $\boldsymbol{p}_p \in \mathbb{F}_p^{n-1}$, que son las imágenes de $\boldsymbol{\lambda}$ y $\boldsymbol{p}$ módulo p;*
- *un straight–line program de longitud a lo sumo L que representa los polinomios $F_{1,p}, \ldots, F_{r,p}$;*

y entrega como salida la representación de Kronecker (la representación univariada) de $\mathcal{J}_{r,p}$ con elemento primitivo $Y_{n-r+1,p}$. Este algoritmo utiliza un número esperado de $\mathcal{O}^{\sim}\big(r(nL+n^5)\delta(d\delta + \log p)\log p\big)$ operaciones bit y devuelve el resultado correcto con probabilidad al menos $1 - 1/12$.

7.2. Levantando los enteros

Sea s con $1 \leq s \leq r$ y sea p un primo "lucky" como en la Proposición 5.3.1. Hemos visto que la representación de Kronecker $Q^s(\boldsymbol{p}_p^s, T), W_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, W_n^s(\boldsymbol{p}_p^s, T) \in \mathbb{F}_p[T]$ de la Proposición 5.3.3 y la correspondiente representación univariada $Q^s(\boldsymbol{p}_p^s, T)$, $V_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, V_n^s(\boldsymbol{p}_p^s, T)$ de la Proposición 5.3.4 se obtienen reduciendo módulo p los enteros de la representación de Kronecker $Q^s(\boldsymbol{p}^s, T), W_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, W_n^s(\boldsymbol{p}^s, T)$ de la Proposición 5.3.2 y de la correspondiente representación univariada $Q^s(\boldsymbol{p}^s, T), V_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, V_n^s(\boldsymbol{p}^s, T)$. Además, por el Lema 4.1.4 el determinante Jacobiano de los polinomios $F_{1,p}(\boldsymbol{p}_p^s, Y_{n-s+1,p}, \ldots, Y_{n,p}), \ldots, F_{s,p}(\boldsymbol{p}_p^s, Y_{n-s+1,p}, \ldots, Y_{n,p})$

con respecto a $Y_{n-s+1,p}, \ldots, Y_{n,p}$ es inversible en $\mathbb{F}_p[Y_{n-s+1,p}, \ldots, Y_{n,p}]/\overline{\mathcal{J}}_{s,p}$. Siguiendo a [GLS01], con estas condiciones podemos aplicar el Algoritmo de Newton global de la Proposición 7.1.5, con $R = \mathbb{Z}$ e $I = p\mathbb{Z}$, y el algoritmo de reconstrucción racional de la Proposición 2.2.3 obteniendo el siguiente resultado (ver [GLS01, Theorem 2 y Lemma 4]).

Proposición 7.2.1. *Supóngase que son dados:*

- *un straight–line program de longitud a lo sumo L que evalúa los polinomios $F_1, \ldots, F_s$;*
- *un número primo "lucky" p como en la Proposición 5.3.1;*
- *los polinomios $Q^s(\boldsymbol{p}_p^s, T), W_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, W_n^s(\boldsymbol{p}_p^s, T)$ (respectivamente $Q^s(\boldsymbol{p}_p^s, T), V_{n-s+2}^s(\boldsymbol{p}_p^s, T), \ldots, V_n^s(\boldsymbol{p}_p^s, T)$).*

Entonces, si k es una potencia de 2, las aproximaciones p–ádicas de orden k de los polinomios $Q^s(\boldsymbol{p}^s, T), W_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, W_n^s(\boldsymbol{p}^s, T)$ se pueden calcular utilizando

$$\mathcal{O}\big((nL + n^4)\mathcal{U}(\delta_s)\mathcal{U}(k \log p)\big)$$

operaciones bit. Además, si η_s es una cota superior para las alturas de los polinomios $Q^s(\boldsymbol{p}^s, T), W_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, W_n^s(\boldsymbol{p}^s, T)$ tal que $\log p < \eta_s$, estos polinomios se pueden reconstruir con $\mathcal{O}^\sim\big((nL + n^4)\delta_s\eta_s\big)$ operaciones bit. Lo mismo vale verbatim sustituyendo $W_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, W_n^s(\boldsymbol{p}^s, T)$ por $V_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, V_n^s(\boldsymbol{p}^s, T)$.

Corolario 7.2.2. *Con las hipótesis y notaciones anteriores, supóngase además que p es un primo como en la Proposición 7.1.2. Entonces $Q^s(\boldsymbol{p}^s, T), W_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, W_n^s(\boldsymbol{p}^s, T)$ se pueden reconstruir con*

$$\mathcal{O}^\sim\big((n^2L + n^5)\delta_s d^{s-1}(h + rd)\big)$$

operaciones bit y los polinomios $Q^s(\boldsymbol{p}^s, T), V_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, V_n^s(\boldsymbol{p}^s, T)$ con $\mathcal{O}^\sim\big((n^2L + n^5)\delta_s d^{2s-1}(h + rd)\big)$ operaciones bit.

Demostración. Basta notar que $\log p \in \mathcal{O}^\sim\big(\log(d^r nh)\big)$. Por la Proposición 6.1.6 deducimos que existe una cota η_s para las alturas de los polinomios $Q^s(\boldsymbol{p}^s, T), W_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, W_n^s(\boldsymbol{p}^s, T)$ con $\eta_s \in \mathcal{O}^\sim\big(nd^{s-1}(h+rd)\big)$ y una cota η_s' para las alturas de los polinomios $Q^s(\boldsymbol{p}^s, T), V_{n-s+2}^s(\boldsymbol{p}^s, T), \ldots, V_n^s(\boldsymbol{p}^s, T)$ con $\eta_s' \in \mathcal{O}^\sim\big(nd^{2s-1}(h + rd)\big)$ y tales que $\log p < \eta_s, \eta_s'$. El corolario se sigue de la última afirmación de la proposición anterior. □

7.3. Una representación de Kronecker sobre los racionales

Combinando el algoritmo subyacente al Teorema 7.1.9 con el procedimiento de levantamiento p–ádico de la Proposición 7.2.1 obtenemos un algoritmo probabilístico

para calcular una representación de Kronecker de una fibra cero–dimensional de la variedad definida por $F_1, \ldots, F_r$.

Más precisamente, supóngase que $F_1, \ldots, F_r$ están dados por un straight–line program β de longitud a lo sumo L con parámetros enteros. Primeramente elegimos al azar un punto $(\boldsymbol{\lambda}, \boldsymbol{p}) \in \mathsf{S}^{n^2} \times \mathsf{T}^{n-1}$ tal que $\mathsf{R}(\boldsymbol{\lambda}) \neq 0$ y $\mathsf{N}_{\boldsymbol{\lambda}} \neq 0$. Luego calculamos un primo "lucky" p como en la Proposición 7.1.2. Por la Observación 7.1.3, obtenemos un straight–line program β_p de longitud a lo sumo $\mathcal{O}(L + n^2)$ que representa los polinomios $F_{1,p}(\boldsymbol{Y}_p), \ldots, F_{r,p}(\boldsymbol{Y}_p)$. Luego, mediante el algoritmo que subyace al Teorema 7.1.9, calculamos la representación de Kronecker $Q_p^r, W_{1,p}^r, \ldots, W_{n,p}^r$ de la fibra de levantamiento $V_{\boldsymbol{p}_p^r}$ con elemento primitivo $Y_{n-r+1,p}$. Finalmente, aplicando el algoritmo que subyace a la Proposición 7.2.1 levantamos estos polinomios a la representación de Kronecker $Q^r, W_1^r, \ldots, W_n^r$ de la fibra de levantamiento $V_{\boldsymbol{p}^r}$ con elemento primitivo Y_{n-r+1}. Tenemos el siguiente resultado.

Teorema 7.3.1. *Existe un algoritmo probabilístico que recibe como entrada un straight–line program β de longitud a lo sumo L que representa los polinomios $F_1, \ldots, F_r$, y entrega como salida una representación de Kronecker de una fibra cero–dimensional de $\mathcal{V}(F_1, \ldots, F_r)$ con probabilidad al menos $\frac{77}{144}$. Si h es una cota superior para la longitud bit de los coeficientes de $F_1, \ldots, F_r$ y los parámetros en β, entonces la complejidad bit del algoritmo es del orden de*

$$\mathcal{O}^{\sim}\big(r(nL + n^5)\delta(d\delta + nd^r h)\big).$$

Demostración. Denótese con $\mathcal{C}_p$ la complejidad bit del cálculo de un primo "lucky" p y con η una cota superior para las alturas de los enteros en la salida. Combinando las estimaciones de complejidad del Teorema 7.1.9 y de la Proposición 7.2.1, el algoritmo descripto se ejecuta en la complejidad bit

$$\mathcal{O}^{\sim}\Big(r(nL + n^5)\delta\big((d\delta + \log p)\log p + \eta\big)\Big) + \mathcal{C}_p.$$

Por la Proposición 6.1.6 podemos tomar $\eta \in \mathcal{O}^{\sim}\big(nd^{r-1}(h + rd)\big)$. Por lo tanto, teniendo en cuenta la estimación para $\mathcal{C}_p$ en la Proposición 7.1.2, obtenemos la estimación de complejidad del teorema.

Finalmente, la afirmación sobre la probabilidad de éxito del algoritmo se deduce del Lema 7.1.1 y las estimaciones para la probabilidad de éxito de la Proposición 7.1.2 y el Teorema 7.1.9. □

El siguiente resultado estima el costo de calcular una representación univariada.

Teorema 7.3.2. *Existe un algoritmo probabilístico que, a partir de la entrada del Teorema 7.3.1, calcula una representación univariada de una fibra cero–dimensional de $\mathcal{V}(F_1, \ldots, F_r)$ con complejidad bit*

$$\mathcal{O}^{\sim}\big(r(nL + n^5)\delta(d\delta + nd^{2r}h)\big).$$

Demostración. El teorema se deduce mediante los mismos argumentos de la demostración del Teorema 7.3.1. Basta tener en cuenta que, en este caso, de acuerdo con la Proposición 6.1.6, la cota η' para las alturas de los enteros en la salida satisface $\eta' \in \mathcal{O}^{\sim}\big(nd^{2r-1}(h + rd)\big)$. □

En el Capítulo 8 necesitaremos recuperar una parametrización de las variables originales $X_1, \ldots, X_n$. En este sentido tenemos el siguiente resultado.

Corolario 7.3.3. *Sean $F_1, \ldots, F_n \in \mathbb{Z}[\boldsymbol{X}]$ polinomios de grados a lo sumo d, que forman una sucesión regular reducida. Existe un algoritmo probabilístico que recibe como entrada un straight–line program β de longitud a lo sumo L que representa los polinomios $F_1, \ldots, F_n$, y entrega como salida una representación univariada $Q, V_1, \ldots, V_n$ de la variedad cero–dimensional $\mathcal{V}(F_1, \ldots, F_n)$ con elemento primitivo U tal que se satisface la siguiente igualdad de ideales:*

$$(F_1, \ldots, F_n) = \big(Q(U), X_1 - V_1(U), \ldots, X_n - V_n(U)\big). \tag{7.2}$$

Sea δ el grado del sistema de entrada y h una cota superior para la longitud bit de los coeficientes de $F_1, \ldots, F_n$ y los parámetros en β. Entonces el algoritmo entrega una respuesta correcta con probabilidad al menos $\frac{77}{144}$ y se ejecuta con complejidad bit

$$\mathcal{O}^{\sim}\big(n(nL + n^5)\delta(d\delta + nd^{2n}h)\big).$$

Demostración. Por la Proposición 7.1.2 y el Teorema 7.1.9 existe un algoritmo probabilístico que calcula una matriz $\boldsymbol{\lambda} \in \mathbb{Z}^{n^2} \setminus \{0\}$ y un primo "lucky" p como en la Proposición 5.3.1 tales que $h(\boldsymbol{\lambda}) \in \mathcal{O}^{\sim}(n \log d)$ y $\log p \in \mathcal{O}^{\sim}\big(\log(d^n h)\big)$, y la representación univariada $Q_p, \widetilde{V}_{2,p}, \ldots, \widetilde{V}_{n,p}$ de la variedad cero–dimensional $\mathcal{V}(F_{1,p}, \ldots, F_{n,p})$ con elemento primitivo $Y_{1,p}$ tal que se satisface la siguiente igualdad de ideales en $\mathbb{F}_p[\boldsymbol{X}]$:

$$(F_{1,p}, \ldots, F_{n,p}) = \big(Q_p(Y_{1,p}), Y_{2,p} - \widetilde{V}_{2,p}(Y_{1,p}), \ldots, Y_{n,p} - \widetilde{V}_{n,p}(Y_{1,p})\big).$$

Aquí $Y_i := \boldsymbol{\lambda}_i \cdot \boldsymbol{X}$ para $1 \leq i \leq n$. Sea $Q, \widetilde{V}_2, \ldots, \widetilde{V}_n$ la correspondiente representación univariada sobre $\mathbb{Q}$ de $\mathcal{V}(F_1, \ldots, F_n)$ con elemento primitivo Y_1. Sea $\boldsymbol{\lambda}^{-1} := (\mu_{jk})_{1 \leq j,k \leq n}$ la inversa de $\boldsymbol{\lambda}$. Definimos $V_j := \sum_{k=1}^{n} \mu_{jk} \widetilde{V}_k$ para $1 \leq j \leq n$, donde $\widetilde{V}_1 := T$. Asimismo, sea $U := Y_1$. Por construcción, los polinomios $Q, V_1, \ldots, V_n$ forman la representación univariada de V con elemento primitivo U tal que se satisface (7.2). Además las reducciones modulares $Q_p, V_{1,p}, \ldots, V_{n,p}$ de los polinomios anteriores forman la representación univariada de $\mathcal{V}(F_{1,p}, \ldots, F_{n,p})$ con elemento primitivo U_p tal que se satisface la igualdad de ideales

$$(F_{1,p}, \ldots, F_{n,p}) = \big(Q_p(U_p), X_1 - V_{1,p}(U_p), \ldots, X_n - V_{n,p}(U_p)\big).$$

Como en la demostración del Teorema 7.3.1 concluimos que el cálculo de los polinomios $Q, V_1, \ldots, V_n$ se puede realizar con complejidad bit

$$\mathcal{O}^{\sim}\Big(n(nL + n^5)\delta\big((d\delta + \log p)\log p + \eta\big)\Big) + \mathcal{C}_p,$$

donde η es una cota superior para las alturas de $Q, V_1, \ldots, V_n$. Para estimar η notemos que $h(\det \boldsymbol{\lambda}), h(M_{ij}) \leq n \log n + nh(\boldsymbol{\lambda})$ para todo menor $(n-1)\times(n-1)$ M_{ij} de $\boldsymbol{\lambda}$. Teniendo en cuenta que $h(\boldsymbol{\lambda}) \in \mathcal{O}^{\sim}(n \log d)$, se concluye que $h(\boldsymbol{\lambda}^{-1}) \in \mathcal{O}^{\sim}(n^2 \log d)$. Además, por la Proposición 6.1.6, sabemos que $h(\widetilde{V}_j) \in \mathcal{O}^{\sim}(nd^{2n-1}(h+d))$ para $2 \leq j \leq n$. A partir de las estimaciones anteriores concluimos que $h(V_j) \in \mathcal{O}^{\sim}\big(nd^{2n-1}(h+d)\big)$ para $1 \leq j \leq n$. Por lo tanto podemos tomar $\eta \in \mathcal{O}^{\sim}\big(nd^{2n-1}(h+d)\big)$, de donde se sigue la estimación de complejidad de la proposición. □

Capítulo 8

Interpolación implícita

En este capítulo $F_1, \ldots, F_n \in \mathbb{Q}[\boldsymbol{X}]$ son polinomios de grado a lo sumo d y altura a lo sumo h, que forman una sucesión regular reducida y definen la variedad cero–dimensional $V \subset \mathbb{A}^n$. Además, $D := \deg V$ es el grado de V y $\delta := \max_{1 \leq i \leq n} \deg \mathcal{V}(F_1, \ldots, F_i)$ el grado del sistema $F_1 = 0, \ldots, F_n = 0$.

Consideramos el siguiente problema de interpolación **implícita**:

Problema 8.0.1. *Con las hipótesis y notaciones anteriores, sean $\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(D)} \in \mathbb{A}^n$ los puntos de V. Se requiere:*

- *Construir un **espacio de interpolantes** Π_V para el conjunto de nodos V, esto es, un subespacio $\Pi_V \subset \mathbb{Q}[\boldsymbol{X}]$ tal que, para todo $F \in \mathbb{Q}[\boldsymbol{X}]$, existe un único interpolante $P_F \in \Pi_V$ que satisface $P_F(\boldsymbol{x}^{(i)}) = F(\boldsymbol{x}^{(i)})$ para $1 \leq i \leq D$.*
- *Dado un polinomio $F \in \mathbb{Q}[\boldsymbol{X}]$, hallar el correspondiente interpolante $P_F \in \Pi_V$.*

El objetivo de este capítulo es exhibir un espacio de interpolantes Π_V para el conjunto de nodos V como en el Problema 8.0.1 y describir un algoritmo que a partir de los polinomios $F_1, \ldots, F_n$ y F calcula una base de Π_V y el correspondiente interpolante $P_F \in \Pi_V$ de F.

Los polinomios $F_1, \ldots, F_n$ y F se suponen representados por un straight–line program β, sin divisiones, de longitud a lo sumo L. En lo que sigue, por simplicidad y sin pérdida de generalidad, suponemos que β tiene parámetros en $\mathbb{Z}$ y que $F \in \mathbb{Z}[T]$. Además denotamos con h una cota superior tanto para las alturas de los parámetros de β como para las alturas de los polinomios $F_1, \ldots, F_n$.

8.1. Traza y dualidad

De fundamental importancia para nuestro propósito son las propiedades de las trazas del anillo de coordenadas $\mathbb{Q}[V]$ de la variedad V. En los párrafos siguientes recordamos las definiciones y hechos básicos de la teoría de trazas. Para las demostraciones nos remitimos a [Kun86, Appendices E and F] (ver también [EM07, Chapters 8 and 9]). Para los aspectos algorítmicos de la teoría de trazas pueden consultarse, por ejemplo, [GH93], [BCRS96], [FGS95], [ABRW96], [GHH+97].

Sea $F \in \mathbb{Q}[\boldsymbol{X}]$ un polinomio arbitrario y denotemos por f su imagen en $\mathbb{Q}[V]$. Denotamos por $\chi_f \in \mathbb{Q}[T]$ el polinomio característico de la aplicación $\mathbb{Q}$–lineal definida por la homotecia $\eta_f : \mathbb{Q}[V] \to \mathbb{Q}[V]$ de multiplicación por f. Sea $\chi_f = T^D + b_{D-1}T^{D-1} + \cdots + b_0 \in \mathbb{Q}[T]$. Entonces la **norma** $N(f)$ y la **traza** $Tr(f)$ de f se definen como

$$N(f) := (-1)^D b_0 \in \mathbb{Q} \quad , \quad Tr(f) := -b_{D-1} \in \mathbb{Q}.$$

Éstas coinciden con el determinante y la traza de η_f respectivamente. Definimos el **adjunto** F^* de F como

$$F^* := (-1)^{D-1}(F^{D-1} + b_{D-1}F^{D-2} + \cdots + b_1) \in \mathbb{Q}[\boldsymbol{X}].$$

También denotamos por f^* la imagen de F^* en $\mathbb{Q}[V]$ y la llamamos la adjunta de f. Puesto que $\chi_f(f) = 0$, tenemos que $f^*f = N(f)$ en $\mathbb{Q}[V]$.

Denotamos por $\mathbb{Q}[V]^*$ el espacio dual $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}[V], \mathbb{Q})$. Definimos en $\mathbb{Q}[V]^*$ una estructura de $\mathbb{Q}[V]$–módulo: Si $(f, \alpha) \in \mathbb{Q}[V] \times \mathbb{Q}[V]^*$, el producto $f \cdot \alpha$ es el elemento de $\mathbb{Q}[V]^*$ definido por $(f \cdot \alpha)(g) = \alpha(fg)$ para cada $g \in \mathbb{Q}[V]$. Bajo nuestras hipótesis sobre $F_1, \ldots, F_n$ tenemos que $\mathbb{Q}[V]^*$ es un $\mathbb{Q}[V]$–módulo libre de rango 1 (ver [Kun86, Example F.19 y Corollary F.10], [EM07, Proposition 8.25]). Todo generador de $\mathbb{Q}[V]^*$ como $\mathbb{Q}[V]$–módulo se denomina una **traza** de $\mathbb{Q}[V]$ sobre $\mathbb{Q}$. Una traza de $\mathbb{Q}[V]$ se puede construir como sigue: Primero definimos la **traza usual** Tr de $\mathbb{Q}[V]$ como el elemento de $\mathbb{Q}[V]^*$ tal que la imagen de todo $f \in \mathbb{Q}[V]$ vía Tr es la traza de f arriba definida. Denotemos por J el Jacobiano de $F_1, \ldots, F_n$ con respecto a $X_1, \ldots, X_n$ y por $\mathcal{J}$ su imagen en $\mathbb{Q}[V]$. Entonces el elemento $\tau \in \mathbb{Q}[V]^*$ definido como $\tau = \mathcal{J}^{-1} \cdot Tr$ es una traza de $\mathbb{Q}[V]$ (ver, por ejemplo, [Kun86, Corollary F.12 y Example F.19], [EM07, Proposition 9.24]). Por lo tanto la forma lineal τ induce una forma bilineal no degenerada $(f, g) \in \mathbb{Q}[V] \times \mathbb{Q}[V] \mapsto \tau(fg) \in \mathbb{Q}$.

Recordemos la noción de Bezoutiano de una sucesión $F_1, \ldots, F_n$. Sea $\boldsymbol{Y} := (Y_1, \ldots, Y_n)$ un vector de indeterminadas. Escribamos $\boldsymbol{X}_{(0)} = \boldsymbol{X}$, $\boldsymbol{X}_{(k)} = (Y_1, \ldots, Y_k, X_{k+1}, \ldots, X_n)$ para $1 \leq k \leq n-1$ y $\boldsymbol{X}_{(n)} = \boldsymbol{Y}$. El **Bezoutiano** $\mathcal{B}$ de $F_1, \ldots, F_n$ se define (ver, por ejemplo, [EM96], [EM07]) como el determinante

$$\mathcal{B} := \det((\gamma_{j,k})_{1 \leq j,k \leq n}), \tag{8.1}$$

donde $\gamma_{j,k}$ es el polinomio de $\mathbb{Q}[\boldsymbol{X}, \boldsymbol{Y}]$ definido por

$$\gamma_{j,k} = \frac{F_j(\boldsymbol{X}_{(k-1)}) - F_j(\boldsymbol{X}_{(k)})}{X_k - Y_k} \quad (1 \leq j, k \leq n). \tag{8.2}$$

Observación 8.1.1. *Si los grados de $F_1, \ldots, F_n$ están acotados por d, el Bezoutiano $\mathcal{B}$ de $F_1, \ldots, F_n$ tiene grado a lo sumo $n(d-1)$.*

Para cada $F \in \mathbb{Q}[\boldsymbol{X}]$ denotamos por $F^{\boldsymbol{Y}}$ el elemento de $\mathbb{Q}[\boldsymbol{Y}]$ definido por $F^{\boldsymbol{Y}} = F(\boldsymbol{Y})$. Sean a_j, b_j $(1 \leq j \leq N)$ polinomios **cualesquiera** en $\mathbb{Q}[\boldsymbol{X}]$ tales que el Bezoutiano $\mathcal{B}$ de $F_1, \ldots, F_n$ se puede escribir de la siguiente manera:

$$\mathcal{B} \equiv \sum_{j=1}^{N} a_j b_j^{\boldsymbol{Y}} \tag{8.3}$$

módulo el ideal $(F_1, \ldots, F_n, F_1^{\boldsymbol{Y}}, \ldots, F_n^{\boldsymbol{Y}})$ de $\mathbb{Q}[\boldsymbol{X}, \boldsymbol{Y}]$. Sean $\bar{a}_j, \bar{b}_j \in \mathbb{Q}[V]$ las imágenes de a_j, b_j para $1 \leq j \leq N$. Con las hipótesis y notaciones anteriores tenemos el siguiente resultado (ver, por ejemplo, [EM07, Proposition 8.7]).

Proposición 8.1.2. *Supóngase que al menos uno de los conjuntos $\bar{a}_j$ $(1 \leq j \leq N)$ o $\bar{b}_j$ $(1 \leq j \leq N)$ es linealmente independiente sobre $\mathbb{Q}$. Entonces $N = D = \dim_{\mathbb{Q}} \mathbb{Q}[V]$ y $\bar{a}_j$ $(1 \leq j \leq D)$, $\bar{b}_j$ $(1 \leq j \leq D)$ son bases duales de $\mathbb{Q}[V]$ con respecto a la forma bilineal inducida por τ.*

Con las hipótesis de la proposición anterior tenemos la siguiente **fórmula de la traza** que vale para todo $f \in \mathbb{Q}[V]$ (ver [Ive73], [Kun86, Example F.19], [EM07, Section 8.1.3]) :

$$f = \sum_{j=1}^{D} \tau(f\bar{b}_j)\bar{a}_j. \tag{8.4}$$

Finalmente recordamos el siguiente resultado (ver, por ejemplo, [EM07, Corollary 4.32]).

Proposición 8.1.3. *Sean $\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(D)} \in \mathbb{C}^n$ los puntos de V. Entonces para todo $f \in \mathbb{Q}[V]$ vale la identidad*

$$Tr(f) = \sum_{j=1}^{D} f(\boldsymbol{x}^{(j)}).$$

8.1.1. Estimaciones para la altura de las trazas

Las siguientes estimaciones para la altura de normas y trazas se encuentran en [KPS01].

Lema 8.1.4. *Sean $F, G \in \mathbb{Q}[\boldsymbol{X}]$, sean f, g sus imágenes en $\mathbb{Q}[V]$, y supongamos que f no es un divisor de cero en $\mathbb{Q}[V]$. Entonces*

- $h\big(N(g)\big) \leq \deg(G)h(V) + h(G)D + \deg(G)D\log(n+1)$,
- $h\big(Tr(f^*g)\big) \leq \max\{\deg F, \deg G\}\big(h(V) + D\log(n+1)\big) + \big(\max\{h(F), h(G)\} + 1\big)D$.

Corolario 8.1.5. *Sean $F_1, \ldots, F_n \in \mathbb{Z}[\boldsymbol{X}]$ polinomios de grado a lo sumo d y altura a lo sumo h que forman una sucesión regular reducida y definen una variedad cero–dimensional $V \subset \mathbb{A}^n$ de grado D. Sea $U \in \mathbb{Z}[\boldsymbol{X}]$ una forma lineal que induce un elemento primitivo u de V tal que $h(U) \in \mathcal{O}^{\sim}(n\log d)$ y sea $F \in \mathbb{Z}[\boldsymbol{X}]$ un polinomio arbitrario. Sea τ la traza de $\mathbb{Q}[V]$ definida anteriormente. Entonces*

$$h\big(\tau(fu^{j-1})\big) \in \mathcal{O}^{\sim}\Big(\big(d^n + \deg(F)\big)h(V) + \big(nh + d^n + \deg(F) + h(F)\big)D\Big)$$

para $1 \leq j \leq D$.

Demostración. Sea $\mathcal{J} \in \mathbb{Q}[V]$ la imagen del Jacobiano J de $F_1, \ldots, F_n$. Puesto que $\mathcal{J}^{-1} = \mathcal{J}^*/N(\mathcal{J})$, es $\tau(fu^{j-1}) = \frac{1}{N(\mathcal{J})} Tr(\mathcal{J}^* fu^{j-1})$ y por lo tanto

$$h\big(\tau(fu^{j-1})\big) \leq h\big(N(\mathcal{J})\big) + h\big(Tr(\mathcal{J}^* fu^{j-1})\big). \tag{8.5}$$

Por el Lema 8.1.4 tenemos que

$$h\big(N(\mathcal{J})\big) \leq \deg(J)h(V) + h(J)D + \log(n+1)\deg(J)D. \tag{8.6}$$

Puesto que $\deg(J) \leq nd$ y $h(J) \in \mathcal{O}^\sim\big(n(h+d)\big)$ (Lema 6.2.2), concluimos que

$$h\big(N(\mathcal{J})\big) \in \mathcal{O}^\sim\big(ndh(V) + n(h+d)D\big). \tag{8.7}$$

De nuevo, por el Lema 8.1.4 tenemos que

$$\begin{aligned} h\big(Tr(\mathcal{J}^* fu^{j-1})\big) \;\leq\; & \max\{\deg(J), \deg(FU^{j-1})\}\big(h(V) + D\log(n+1)\big) + \\ & \big(\max\{h(J), h(FU^{j-1})\} + 1\big)D. \end{aligned} \tag{8.8}$$

Para $1 \leq j \leq D$, por el Lema 2.1.31 (ítem 2), tenemos que

$$h(U^{j-1}) \leq (j-1)h(U) + (j-2)\log(n+1) \leq D\big(h(U) + \log(n+1)\big),$$

y por lo tanto

$$\begin{aligned} h(FU^{j-1}) &\leq h(F) + h(U^{j-1}) + \min\{\deg(F), \deg(U^{j-1})\}\log(n+1) \\ &\leq h(F) + D(h(U) + \log(n+1)) + \deg(U^{j-1})\log(n+1) \\ &\leq h(F) + D\big(h(U) + 2\log(n+1)\big). \end{aligned}$$

Teniendo en cuenta que $h(U) \in \mathcal{O}^\sim(n\log d)$ y $D \leq d^n$, resulta

$$h(FU^{j-1}) \in \mathcal{O}^\sim\big(h(F) + d^n\big) \quad (1 \leq j \leq D).$$

Por otra parte, obtenemos

$$\max\{\deg(J), \deg(FU^{j-1})\} \leq \deg(F) + d^n, \quad \max\{h(J), h(FU^{j-1})\} \in \mathcal{O}^\sim\big(nh + h(F) + d^n\big).$$

Sustituyendo las estimaciones anteriores en (8.8) resulta

$$h\big(Tr(\mathcal{J}^* fu^{j-1})\big) \in \mathcal{O}^\sim\Big(\big(\deg(F) + d^n\big)h(V) + \big(nh + d^n + \deg(F) + h(F)\big)D\Big).$$

Sustituyendo esta estimación junto con (8.7) en (8.5) se obtiene la estimación del corolario. □

8.2. Construcción del espacio de interpolantes

En esta sección describimos un procedimiento simbólico para construir, a partir de $F_1, \ldots, F_n$, una base $\{G_1, \ldots, G_D\}$ de un espacio de interpolantes Π_V para el conjunto de nodos V del Problema 8.0.1 tal que $\deg G_j \leq n(d-1)$ para $1 \leq j \leq D$. Sean $F_1, \ldots, F_n \in \mathbb{Q}[\boldsymbol{X}]$ polinomios de grado a lo sumo d como en la sección anterior que definen el conjunto de nodos $V := \{\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(D)}\}$. Supóngase además que tenemos una representación univariada $Q, V_1, \ldots, V_n$ de V con elemento primitivo U como en el Corolario 7.3.3. Sea $\{1, u, \ldots, u^{D-1}\}$ la base de $\mathbb{Q}[V]$ inducida por U. Denotemos por $\{g_1, \ldots, g_D\}$ la base dual de $\{1, u, \ldots, u^{D-1}\}$ con respecto a la traza τ de la Sección 8.1. Para obtener la base $\{G_1, \ldots, G_D\}$ consideramos el Bezoutiano $\mathcal{B}$ de $F_1, \ldots, F_n$, sustituimos en $\mathcal{B}$ las variables $Y_1, \ldots, Y_n$ por los polinomios $V_1, \ldots, V_n$ y vemos el polinomio obtenido $\mathcal{B}\big(\boldsymbol{X}, V_1(T), \ldots, V_n(T)\big)$ como un polinomio en T con coeficientes en $\mathbb{Q}[\boldsymbol{X}]$. Definimos $G_1, \ldots, G_D \in \mathbb{Q}[\boldsymbol{X}]$ como los coeficientes del resto $\sum_{1 \leq j \leq D} G_j(\boldsymbol{X}) T^{j-1}$ de $\mathcal{B}\big(\boldsymbol{X}, V_1(T), \ldots, V_n(T)\big)$ en la división por $Q(T)$.

Con las hipótesis y notaciones anteriores tenemos el siguiente resultado.

Proposición 8.2.1. *Los polinomios $G_1, \ldots, G_D$ satisfacen las siguientes propiedades:*

- *G_j es un representante de g_j para $1 \leq j \leq D$;*
- *$\deg G_j \leq n(d-1)$ para $1 \leq j \leq D$.*

Demostración. De las ecuaciones $Q(U) \equiv 0$, $X_k \equiv V_k(U)$ $(1 \leq k \leq n)$ módulo $(F_1, \ldots, F_n)$ deducimos que

$$\mathcal{B} \equiv \sum_{j=1}^{D} G_j(\boldsymbol{X})(U^{\boldsymbol{Y}})^{j-1} \quad \text{mód } (F_1^{\boldsymbol{Y}}, \ldots, F_n^{\boldsymbol{Y}}). \tag{8.9}$$

Teniendo en cuenta que u^{j-1} $(1 \leq j \leq D)$ es una base de $\mathbb{Q}[V]$ la primera afirmación de la proposición se sigue de (8.9) y la Proposición 8.1.2. Finalmente, por la Observación 8.1.1, $\deg_{\boldsymbol{X}} \mathcal{B}(\boldsymbol{X}, V_1(T), \ldots, V_n(T)) \leq n(d-1)$. Puesto que Q no depende de los X_j, se sigue la cota de grados. □

Por la fórmula de la traza (8.4) concluimos el siguiente resultado.

Corolario 8.2.2. *Dado $F \in \mathbb{Q}[\boldsymbol{X}]$, el polinomio $P_F \in \mathbb{Q}[\boldsymbol{X}]$ definido por*

$$P_F := \sum_{j=1}^{D} \tau(f u^{j-1}) G_j \tag{8.10}$$

satisface $P_F(\boldsymbol{x}^i) = F(\boldsymbol{x}^{(i)})$ para $1 \leq i \leq D$. En particular, $\{G_1, \ldots, G_D\}$ es una base de un espacio de interpolantes Π_V en el sentido del Problema 8.0.1.

Observación 8.2.3. *El espacio de interpolantes Π_V del Corolario 8.2.2 está unívocamente determinado por la sucesión $F_1, \ldots, F_n$ que define el conjunto de nodos V.*

La observación anterior es una consecuencia inmediata del siguiente lema que dice que el polinomio P_F de (8.10) es el interpolante que determina la clásica fórmula de interpolación de Kronecker (ver [Kro65]; ver también [GS00a] y [EM07, Remark 9.8]).

Lema 8.2.4. *El polinomio P_F definido por* (8.10) *se puede escribir de la siguiente manera:*

$$P_F = \sum_{j=1}^{D} F(\boldsymbol{x}^{(j)})\mathcal{B}(\boldsymbol{X}, \boldsymbol{x}^{(j)})/J(\boldsymbol{x}^{(j)}). \tag{8.11}$$

Demostración. Sea $F \in \mathbb{Q}[\boldsymbol{X}]$ un polinomio arbitrario. De acuerdo con la Proposición 8.1.3, recordando la definición de τ tenemos que

$$\tau(fu^{j-1}) = \sum_{k=1}^{D} \frac{F(\boldsymbol{x}^{(k)})U(\boldsymbol{x}^{(k)})^{j-1}}{J(\boldsymbol{x}^{(k)})} \quad (1 \leq j \leq D).$$

Por lo tanto podemos reescribir (8.10) de la siguiente manera:

$$P_F = \sum_{k=1}^{D} \frac{F(\boldsymbol{x}^{(k)})}{J(\boldsymbol{x}^{(k)})} \left(\sum_{j=1}^{D} G_j(\boldsymbol{X})U(\boldsymbol{x}^{(k)})^{j-1} \right). \tag{8.12}$$

Sustituyendo $\boldsymbol{Y}$ por $\boldsymbol{x}^{(k)}$ en (8.9) para todo $1 \leq k \leq D$ obtenemos

$$\mathcal{B}(\boldsymbol{X}, \boldsymbol{x}^{(k)}) = \sum_{j=1}^{D} G_j(\boldsymbol{X})U(\boldsymbol{x}^{(k)})^{j-1} \quad (1 \leq k \leq D).$$

Combinando esta identidad con (8.12) se obtiene (8.11), lo que termina la demostración. □

Por otra parte, la base $\{G_1, \ldots, G_D\}$ arriba construida claramente depende de la representación univariada $Q, V_1, \ldots, V_n$ de V.

8.3. Cálculo de los interpolantes

En esta sección describimos un procedimiento para calcular los polinomios $G_1, \ldots, G_D$ y P_F del Corolario 8.2.2.

La estructura general de los algoritmos contenidos en esta sección ya ha sido descripta en [GHH+97]. No obstante, una característica básica del enfoque de aquel trabajo es que los algoritmos se basan en la ejecución de straight–line programs en anillos de matrices (ver [GHS93] para los detalles). Por lo tanto, teniendo en cuenta el costo de la aritmética en el anillo de matrices de talla $\delta \times \delta$, este enfoque conduce a una estimación de $\mathcal{O}(\delta^3)$ operaciones aritméticas en $\mathbb{Q}$.

Nuestro enfoque difiere del de [GHH+97] en que obtenemos los algoritmos ejecutando los straight–line programs en anillos cocientes del tipo $\mathbb{Q}[T]/(Q)$, donde Q denota un elemento adecuado de $\mathbb{Q}[T]$. Por medio de este procedimiento mejoramos

la estimación anterior, obteniendo un costo aritmético que depende solo cuadráticamente de δ.

Comenzamos estableciendo algunos resultados técnicos. Sean $X_1, \ldots, X_n, Y_1, \ldots, Y_s$ indeterminadas. Sea $E \in \mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_s]$ un polinomio arbitrario de grado a lo sumo d y supóngase dado un straight–line program σ de longitud L que representa E. Supónganse también dados polinomios $V_1, \ldots, V_s \in \mathbb{Q}[T]$ de grado menor que D y un polinomio **mónico** $Q \in \mathbb{Q}[T]$ de grado D (estos polinomios no son necesariamente los elementos de una representación univariada de V). Sustituimos en E las variables $Y_1, \ldots, Y_s$ por $V_1, \ldots, V_s$ y consideramos el polinomio resultante $E(\boldsymbol{X}, V_1(T), \ldots, V_s(T))$ como un polinomio en T con coeficientes en $\mathbb{Q}[\boldsymbol{X}]$. Sean $\widetilde{G}_1, \ldots, \widetilde{G}_D \in \mathbb{Q}[\boldsymbol{X}]$ los (únicos) polinomios que satisfacen

$$E(\boldsymbol{X}, V_1(T), \ldots, V_s(T)) \equiv \sum_{j=1}^{D} \widetilde{G}_j(\boldsymbol{X}) T^{j-1} \mod Q(T). \tag{8.13}$$

Puesto que $\deg_{\boldsymbol{X}} E\big(\boldsymbol{X}, V_1(T), \ldots, V_s(T)\big) \leq d$ y $Q(T)$ no depende de los X_j, se concluye fácilmente que $\deg \widetilde{G}_j \leq d$ para $1 \leq j \leq D$.

A partir de σ obtenemos un straight–line program σ' que representa los polinomios $\widetilde{G}_1, \ldots, \widetilde{G}_D$ por medio de los cálculos que se describen a continuación.

Denotemos por Q_ρ la función calculada en el paso ρ de σ. Sea $P_\rho \in \mathbb{Q}[\boldsymbol{X}, T]$ el polinomio que se obtiene sustituyendo en Q_ρ las variables $Y_1, \ldots, Y_s$ por los polinomios $V_1(T), \ldots, V_s(T)$. Consideramos P_ρ como un polinomio en T con coeficientes en $\mathbb{Q}[\boldsymbol{X}]$ y denotamos por R_ρ el resto de la división de P_ρ por $Q(T)$. Supóngase que el polinomio E se calcula en el paso r de σ. De acuerdo con (8.13) tenemos que $Q_r = E$ y $R_r = \sum_{j=1}^{D} \widetilde{G}_j(\boldsymbol{X}) T^{j-1}$.

Calculamos los polinomios $\widetilde{G}_1, \ldots, \widetilde{G}_D$, es decir, la representación densa del polinomio R_r (visto como un polinomio en T con coeficientes en $\mathbb{Q}[\boldsymbol{X}]$) paso a paso siguiendo el esquema de computación de σ. Más precisamente, en cada paso ρ de σ calculamos la representación densa de R_ρ. Supóngase que $Q_\rho = Q_{\rho_1} \circ_\rho Q_{\rho_2}$ con $1 \leq \rho_1, \rho_2 < \rho$, donde $\circ_\rho \in \{+, -, \times\}$. Para calcular R_ρ es suficiente observar que en los pasos anteriores ya hemos calculado R_{ρ_1} y R_{ρ_2}. Luego obtenemos R_ρ realizando la operación $R_{\rho_1} \circ_\rho R_{\rho_2}$ y calculando el resto de dividir el resultado de esta operación por Q. En cada paso ρ estos cálculos se pueden realizar con $\mathcal{O}(\mathcal{M}(D))$ operaciones aritméticas en $\mathbb{Q}[\boldsymbol{X}]$. Puesto que el straight–line program σ contiene L pasos de computación concluimos que el procedimiento completo constituye un straight–line program σ' en $\mathbb{Q}[\boldsymbol{X}]$ de longitud $\mathcal{O}(L\mathcal{M}(D))$ que representa los polinomios $\widetilde{G}_1, \ldots, \widetilde{G}_D$.

Resumiendo, tenemos siguiente resultado.

Lema 8.3.1. *Sea $E \in \mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_s]$ un polinomio arbitrario. Dados:*

- *un straight–line program σ de longitud L que representa E;*
- *polinomios $V_1, \ldots, V_s, Q \in \mathbb{Q}[T]$ con $\deg V_j < D$ para $1 \leq j \leq s$ y $\deg Q = D$;*

el procedimiento descripto calcula un straight–line program σ' de longitud $\mathcal{O}\big(L\mathcal{M}(D)\big)$ que representa los polinomios $\widetilde{G}_j$ $(1 \leq j \leq D)$ de (8.13).

En particular, sea $Q, V_1, \ldots, V_n$ una representación univariada de V con elemento primitivo U como en el Corolario 7.3.3. Si sustituimos las variables $X_1, \ldots, X_n$ en un polinomio $F \in \mathbb{Q}[\boldsymbol{X}]$ por los polinomios $V_1(T), \ldots, V_n(T)$ y realizamos el procedimiento que subyace al Lema 8.3.1 obtenemos el siguiente resultado.

Corolario 8.3.2. *Sea $F \in \mathbb{Q}[\boldsymbol{X}]$ un polinomio arbitrario y f su imagen en $\mathbb{Q}[V]$. Dados:*

- *un straight–line program β de longitud L que representa F;*
- *una representación univariada $Q, V_1, \ldots, V_n$ de V con elemento primitivo U como en el Corolario 7.3.3;*

el polinomio $P \in \mathbb{Q}[T]$ con $\deg P < D$ tal que $P(u) = f$ se puede calcular con $\mathcal{O}\big(L\mathcal{M}(D)\big)$ operaciones aritméticas en $\mathbb{Q}$.

También necesitaremos el siguiente resultado técnico.

Corolario 8.3.3. *Sea β un straight–line program de longitud L que representa un polinomio $F \in \mathbb{Q}[\boldsymbol{X}]$ con $\deg F \leq d$. Entonces la representación mixta β' de F con respecto a cualquier variable distinguida X_k $(1 \leq k \leq n)$ se puede evaluar con $\mathcal{O}(L\mathcal{M}(d))$ operaciones aritméticas.*

Demostración. Supóngase sin pérdida de generalidad que X_n es la variable distinguida. Escribimos $F = \sum_{k=0}^{d} F_k X_n^k$ con $F_k \in \mathbb{Q}[X_1, \ldots, X_{n-1}]$ para $0 \leq k \leq d$. Identificamos la indeterminada T del Lema 8.3.1 con X_n y definimos $Q(X_n) := X_n^{d+1}$. De acuerdo con el Lema 8.3.1 existe un straight–line program β' de longitud $\mathcal{O}(L\mathcal{M}(d))$ que representa los polinomios $F_0, \ldots, F_d$. □

8.3.1. Cálculo de la base del espacio de interpolantes

Supóngase dado un straight–line program β que representa los polinomios $F_1, \ldots, F_n$. Recordemos que $\deg F_j \leq d$ para $1 \leq j \leq n$. A continuación describimos un algoritmo que, a partir de β, calcula la base $\{G_1, \ldots, G_D\}$ de la Proposición 8.2.2.

Primeramente, a partir β obtenemos un straight–line program β' que representa el Bezoutiano $\mathcal{B}$ de $F_1, \ldots, F_n$. Con este propósito reexpresamos los polinomios $\gamma_{j,k}$ $(1 \leq j, k \leq n)$ de (8.2) como se describe a continuación.

Con las notaciones de la Sección 8.1, para $1 \leq j, k \leq n$ tenemos una representación

$$F_j(\boldsymbol{X}_{(k-1)}) = \sum_{m=0}^{d} A_{j,m}^{(k-1)} X_k^m, \tag{8.14}$$

donde $A_{j,m}^{(k-1)} \in \mathbb{Q}[\boldsymbol{X}, \boldsymbol{Y}]$ no depende de X_k. Para $1 \leq m \leq d$ y $1 \leq k \leq n$, sea $B_k^{(m)} \in \mathbb{Q}[\boldsymbol{X}, \boldsymbol{Y}]$ el polinomio $B_k^{(m)} := \sum_{l=0}^{m-1} X_k^l Y_k^{m-1-l} = \frac{X_k^m - Y_k^m}{X_k - Y_k}$.

Afirmamos que $\gamma_{j,k} = \sum_{m=1}^{d} A_{j,m}^{(k-1)} B_k^{(m)}$ para $1 \leq j, k \leq n$. En efecto, teniendo en cuenta que $A_{j,m}^{(k-1)}$ no depende de X_k, después de sustituir X_k por Y_k en (8.14)

obtenemos

$$F_j(\boldsymbol{X}_{(k)}) = \sum_{m=0}^{d} A_{j,m}^{(k-1)} Y_k^m \qquad (1 \le j,k \le n). \tag{8.15}$$

Sustrayendo $F_j(\boldsymbol{X}_{(k)})$ de $F_j(\boldsymbol{X}_{(k-1)})$ obtenemos

$$F_j(\boldsymbol{X}_{(k)}) - F_j(\boldsymbol{X}_{(k-1)}) = \left(\sum_{m=1}^{d} A_{j,m}^{(k-1)} B_k^{(m)} \right) (X_k - Y_k) \qquad (1 \le j,k \le n),$$

lo que prueba nuestra afirmación.

Teniendo en cuenta la construcción anterior, a partir del straight–line program β obtenemos un straight–line program β_1 que representa el Bezoutiano $\mathcal{B}$ como se describe a continuación.

Fíjese j,k con $1 \le j,k \le n$. Sustituyendo $X_1,\ldots,X_{k-1}$ por $Y_1,\ldots,Y_{k-1}$ en el straight–line program β obtenemos un straight–line program de longitud L que representa el polinomio $F_j(\boldsymbol{X}_{(k-1)})$. Puesto que $\deg F_j(\boldsymbol{X}_{(k-1)}) \le d$, de acuerdo con el Corolario 8.3.3 obtenemos una representación mixta de $F_j(\boldsymbol{X}_{(k-1)})$ con respecto a la variable distinguida X_k cuya longitud es $\mathcal{O}(L\mathcal{M}(d))$. En otras palabras, obtenemos un straight–line program de longitud $\mathcal{O}(L\mathcal{M}(d))$ que representa los polinomios $A_{j,0}^{(k-1)},\ldots,A_{j,d}^{(k-1)}$ de (8.14). Por lo tanto obtenemos un straight–line program de longitud $\mathcal{O}(Ln^2\mathcal{M}(d))$ que representa el conjunto de polinomios $A_{j,m}^{(k-1)}$ $(1 \le j,k \le n, 0 \le m \le d)$. Además, es fácil ver que el conjunto de polinomios $B_k^{(m)}$ $(1 \le m \le d, 1 \le k \le n)$ se puede evaluar con $\mathcal{O}(nd^2)$ operaciones aritméticas. Finalmente la evaluación del conjunto de polinomios $\gamma_{j,k} := \sum_{m=1}^{d} A_m^{(k-1)} B_k^{(m)}$ $(1 \le j,k \le n)$ requiere $\mathcal{O}(n^2 d)$ operaciones aritméticas adicionales. Estos cálculos equivalen a $\mathcal{O}(n^2 L\mathcal{M}(d) + n^2 d^2)$ operaciones aritméticas en $\mathbb{Q}[\boldsymbol{X}]$. Por último, calculamos el determinante $\mathcal{B} = \det(\gamma_{j,k})_{1\le j,k\le n}$ con $\mathcal{O}(n^4)$ operaciones aritméticas adicionales. En conclusión, los cálculos anteriores constituyen un straight–line program β_1 de longitud $\mathcal{O}((n^2L + n^4)\mathcal{M}(d^2))$ que representa el Bezoutiano $\mathcal{B}$.

Resumiendo, tenemos el siguiente resultado.

Lema 8.3.4. *Supóngase dado un straight–line program β de longitud L que representa polinomios $F_1,\ldots,F_n$ de grado a lo sumo d. Entonces existe un straight–line program β_1 de longitud $\mathcal{O}((n^2L + n^4)\mathcal{M}(d^2))$ que representa el Bezoutiano $\mathcal{B}$ de $F_1,\ldots,F_n$.*

Finalmente, a partir de β obtenemos un straight–line program β' que representa los polinomios $G_1,\ldots,G_D$ del Corolario 8.2.2. Para ello primero calculamos una representación univariada $Q, V_1,\ldots,V_n$ de V como en el Corolario 7.3.3. Luego, a partir de β obtenemos un straight–line program β_1 de longitud $\mathcal{O}((n^2L+n^4)\mathcal{M}(d^2))$ que representa el Bezoutiano $\mathcal{B}$ de $F_1,\ldots,F_n$ (Lema 8.3.4). De acuerdo con el Lema 8.3.1 podemos obtener un straight–line program β' de longitud $\mathcal{O}((n^2L+n^4)\mathcal{M}(d^2\delta))$ que representa los polinomios $G_1,\ldots,G_D$ del Corolario 8.2.2.

Teniendo en cuenta la estimación del Corolario 7.3.3 para el costo del cálculo de una representación univariada, resumimos los cálculos anteriores en el siguiente resultado.

Teorema 8.3.5. *Sean $F_1, \ldots, F_n \in \mathbb{Z}[\boldsymbol{X}]$ polinomios de grado a lo sumo d que forman una sucesión regular reducida y definen una variedad cero–dimensional $V \subset \mathbb{A}^n$. Supóngase dado un straight–line program β de longitud L que representa $F_1, \ldots, F_n$. Entonces existe un algoritmo probabilístico que calcula un straight–line program β' de longitud $\mathcal{O}(n^2L + n^4)\mathcal{M}(d^2\delta))$ que representa una base $\{G_1, \ldots, G_D\}$ de un espacio de interpolantes Π_V tal que $\deg G_j \leq n(d-1)$ para todo $1 \leq j \leq D$. El algoritmo realiza*

$$\mathcal{O}^{\sim}(n(nL + n^5)\delta(d\delta + nd^{2n}h))$$

operaciones bit.

Observación 8.3.6. *Teniendo en cuenta el Teorema 1.1.1, el cálculo del straight–line program β' del Teorema 8.3.5 requiere $\mathcal{O}^{\sim}(n(nL+n^4)(d\delta)^2)$ operaciones aritméticas en $\mathbb{Q}$.*

Comparación con bases de Gröbner y H-bases

A continuación discutimos brevemente el costo aritmético de aplicar técnicas de bases de Gröbner y H-bases a nuestro problema.

Como mencionamos en el Capítulo 1, el análisis de complejidad más fino para bases de Gröbner en el caso cero–dimensional es el de [HL11]. En este trabajo se demuestra que una base de Gröbner de un ideal cero–dimensional puede calcularse con una cantidad de operaciones bit que es esencialmente polinomial en N^n, donde n es el número de variables y N el valor promedio de los grados de los polinomios de entrada (ver [HL11] para un resumen de resultados anteriores). El algoritmo correspondiente calcula una base de Gröbner reducida de un ideal cero–dimensional con respecto al orden lexicográfico graduado inverso, cuyos elementos tienen grado a lo sumo $nN-n+1$. Las bases de Gröbner para otros órdenes se pueden deducir usando [FGLM93]. En lo que sigue estimamos el número de operaciones aritméticas en $\mathbb{Q}$ necesarias para ejecutar el algoritmo de [HL11] en nuestros polinomios de entrada $F_1, \ldots, F_n$. En este caso los pasos principales del algoritmo se pueden describir en los siguientes términos. Primeramente, se obtienen las homogeneizaciones $F_1^{(h)}, \ldots, F_n^{(h)}$ de los polinomios $F_1, \ldots, F_n$ con respecto a una nueva variable X_0. Luego cada $F_i^{(h)}$ se deforma en $G_i = (1-S)F_i^{(h)} + SX_i^{d_i}$ para $1 \leq i \leq n$, donde S es una nueva indeterminada. A continuación se consideran los ideales $J := (G_1, \ldots, G_n)$ de $\mathbb{Q}[S][X_0, \ldots, X_n]$, la saturación $J : S^\infty$ de J con respecto a S, y el ideal $J : S^\infty|_{S=0}$ de $\mathbb{Q}[X_0, \ldots, X_n]$ que se obtiene especializando S en 0. La primera tarea del algoritmo es calcular una matriz de Macaulay de grado $nN - n + 1$ del ideal $J : S^\infty|_{S=0}$. Esta matriz se deduce de la forma normal de Smith de la matriz de Macaulay usual del mismo grado de J. Sea $J' := J : S^\infty|_{S=0}$. El próximo paso consiste en calcular una matriz de Macaulay de grado $nN - n + 1$ de la saturación $J' : X_0^\infty$ de J' con respecto a X_0, que resulta ser también una matriz de Macaulay del mismo grado del ideal $(F_1^{(h)}, \ldots, F_n^{(h)})$. Para obtener una base de Gröbner para el orden lexicográfico inverso del ideal de entrada $(F_1, \ldots, F_n)$, se reduce la matriz de Macaulay anterior a su forma escalonada por columnas. Los elementos de la base de Gröbner se obtienen entonces como las deshomogeneizaciones de los polinomios representados por

las columnas de esta matriz reducida.

El costo aritmético sobre $\mathbb{Q}$ de los cálculos anteriores está dominado por el costo de calcular la matriz de Macaulay del ideal $J' : X_0^\infty$. Esta matriz se obtiene como una sub–matriz de la forma escalonada de la matriz $\Gamma^{(i)}$ de [HL11]. Por [Sto00] sabemos que la forma escalonada de una matriz de tamaño $p \times q$ con coeficientes en $\mathbb{Q}$ se puede calcular con $\mathcal{O}(\ell^{\omega-2}pq)$ operaciones aritméticas en $\mathbb{Q}$, donde ℓ es el rango de la matriz y ω es el exponente de la complejidad de la multiplicación de matrices. La matriz $\Gamma^{(i)}$ tiene a lo sumo $r(rn+1)$ filas y a lo sumo $r(2rn+1)$ columnas, donde $r = \binom{nN+1}{n}$ es el número de monomios de grado $nN-n+1$ en $n+1$ variables. Concluimos que la forma escalonada de $\Gamma^{(i)}$, y por lo tanto una base de Gröbner del ideal de entrada $(F_1, \ldots, F_n)$, puede calcularse con $\mathcal{O}(\binom{nN+1}{n}^{2\omega} n^\omega)$ operaciones aritméticas en $\mathbb{Q}$. Utilizando las estimaciones $\binom{nN+1}{n} = \mathcal{O}((3N)^n)$ y $\omega < 3$, este costo es esencialmente $\mathcal{O}(n^3(3N)^n)$.

Un procedimiento para construir H–bases de ideales cero–dimensionales que no se basa en órdenes monomiales se describe en [MS00b]. Puesto que los autores no proveen un enunciado claro de complejidad, discutimos aquí brevemente el costo de los cálculos involucrados en dicho procedimento. Con este fin, denotemos con $\prod_d^{(H)} \subset \mathbb{Q}[\mathbf{X}]$ el subespacio de todos los polinomios homogéneos de grado d y con $M_H(h)$ la parte homogénea de grado máximo de un polinomio $h \in \mathbb{Q}[\mathbf{X}]$ dado. Suponemos que $F_1, \ldots, F_n$ son los polinomios de entrada. El procedimiento, que procede ejecutando sucesivamente un "ciclo", comienza inicializando $\mathcal{H} := \{F_1, \ldots, F_n\}$ y $d := 0$. Cada vez que el procedimiento entra en el "ciclo" se realizan los siguientes cálculos: Primero se calcula el espacio lineal de todas las tuplas $(g_h)_{h\in\mathcal{H}}$ de polinomios homogéneos en $\mathbb{Q}[\mathbf{X}]$ con $g_h M_H(h) \in \prod_d^{(H)}$ para todo h tal que

$$\sum_{h\in\mathcal{H}} g_h M_H(h) = 0. \tag{8.16}$$

Para cada $\mathcal{H}$ y d, sea

$$V_d(\mathcal{H}) = \left\{ \sum_{h\in\mathcal{H}} g_h M_H(h) | g_h M_H(h) \in \prod_d^{(H)} \right\}.$$

Dada una tupla $(g_h)_{h\in\mathcal{H}}$ que satisface (8.16), el polinomio $\sum_{h\in\mathcal{H}} g_h h$ se reduce módulo $\mathcal{H}$ a un polinomio, digamos p (ver [PS07]) para una descripción del proceso de reducción). Si $p \neq 0$, p se agrega a $\mathcal{H}$ y se verifica si alguno de los espacios lineales precedentes $V_k(\mathcal{H})$ $(0 \leq k \leq d)$ se modifica. En caso de haberse modificado alguno de estos espacios, d se redefine como el menor k tal que $V_k(\mathcal{H})$ se ha modificado y el procedimiento vuelve al "ciclo". Si para ningún elemento $(g_h)_{h\in\mathcal{H}}$ se halla un polinomio reducido p para el cual alguno de los espacios $V_k(\mathcal{H})$ $(0 \leq k \leq d)$ se modifica, d se incrementa en 1. Si ahora $V_d(\mathcal{H}) = \prod_d^{(H)}$, entonces $\mathcal{H}$ es una H–base, de otro modo el procedimiento vuelve al "ciclo".

El número de operaciones en $\mathbb{Q}$ realizadas dentro de un "ciclo" puede estimarse como sigue: Puesto que el número de monomios en $\prod_d^{(H)}$ es $\binom{d+n-1}{n-1}$ y los g_h son homogéneos de grado a lo sumo d, resolver la ecuación (8.16) equivale a resolver

un sistema de $\binom{d+n-1}{n-1}$ ecuaciones lineales en a lo sumo $\binom{d+n-1}{n-1}|\mathcal{H}|$ indeterminadas, donde $|\mathcal{H}|$ denota el cardinal de $\mathcal{H}$. Teniendo en cuenta la complejidad de la eliminación Gaussiana (ver [Sto00]), resolver (8.16) requiere $\mathcal{O}(\binom{d+n-1}{n-1})^{\omega}|\mathcal{H}|)$ operaciones aritméticas in $\mathbb{Q}$. Si estimamos la dimensión del espacio lineal $V_k(\mathcal{H})$ por $\binom{k+n-1}{n-1} = \mathcal{O}(k^n)$ vemos que el cálculo del polinomio reducido p por medio del procedimiento descripto en [PS07] requiere $\mathcal{O}(n^2d^n)$ operaciones aritméticas en $\mathbb{Q}$. Para calcular la dimensión de $V_k(\mathcal{H})$ tenemos que calcular el rango de una matriz de $\binom{k+n-1}{n-1}$ columnas y a lo sumo $\binom{k+n-1}{n-1}|\mathcal{H}|$ filas, lo que requiere $\mathcal{O}(\binom{k+n-1}{n-1}^{\omega}|\mathcal{H}|)$ operaciones aritméticas en $\mathbb{Q}$. Eventualmente tenemos que calcular la dimensión de $V_k(\mathcal{H})$ para todo $0 \leq k \leq d+1$, lo que requiere $\mathcal{O}((d+1)^{\omega n+1}|\mathcal{H}|)$ operaciones aritméticas en $\mathbb{Q}$. Además, en los cálculos anteriores es suficiente considerar elementos $(g_h)_{h\in\mathcal{H}}$ de una base del espacio lineal de soluciones del sistema (8.16). Puesto que la dimensión de este espacio lineal está acotado por $\binom{d+n-1}{n-1}|\mathcal{H}|$ concluimos que el número total de operaciones aritméticas en $\mathbb{Q}$ que se realizan dentro de un "ciclo" es $\binom{d+n-1}{n-1}|\mathcal{H}|(\mathcal{O}(n^2d^n) + \mathcal{O}((d+1)^{\omega n+1}|\mathcal{H}|))$ o, puesto que $\omega < 3$ y $d+1 \geq 2$, $\mathcal{O}((d+1)^{4n+1}|\mathcal{H}|^2)$.

El máximo d_{max} de los grados d que aparecen durante el procedimiento completo puede estimarse como sigue. Para cada $i = 1, \ldots, n$ existe un polinomio q_i en el ideal $(F_1, \ldots, F_n)$ que depende sólo de X_i. Sea $M := \deg(q_1) + \cdots + \deg(q_n) - n + 1$. Entonces tenemos que $V_M(F_1, \ldots, F_n) = \prod_M^{(H)}$ (ver [MS00b]). Sean $p_1, \ldots, p_m$ polinomios en $(F_1, \ldots, F_n)$ tales que $M_H(p_1), \ldots, M_H(p_m)$ es una base de $\prod_M^{(H)}$. Claramente cada p_i tiene una representación $p_i = \sum_{j=1}^n g_{ij}F_j$. Luego d_{max} es a lo sumo el máximo de los grados $\deg(g_{ij}F_j)$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$. Puesto que por hipótesis $F_1, \ldots, F_n$ es una sucesión regular reducida, sabemos por [HMPS00] que los polinomios g_{ij} pueden elegirse de modo que satisfagan la condición

$$\deg(g_{ij}) \leq 3n^2 \operatorname{máx}\{\deg(F_1), \ldots, \deg(F_n), p_i\}D$$

para todo i, donde D es el grado de la variedad $V(F_1, \ldots, F_n)$. Además, por [Jel05] tenemos que $\deg(q_i) \leq \prod_{j=1}^n \deg(F_j)$ para todo $1 \leq j \leq n$, y por lo tanto $M \leq n(\prod_{j=1}^n \deg(F_j) - 1) + 1$. A partir de estas cotas es fácil ver que d_{max} es a lo sumo $7n^3(\prod_{j=1}^n \deg(F_j))D$. Sean $p_1, \ldots, p_N$ los polinomios reducidos que se agregan a $\mathcal{H}_0$ durante el procedimiento, tal que $n+N$ es el número de elementos de la H–base calculada en la salida. Por lo tanto $|\mathcal{H}| \leq n+N$ durante todo el procedimiento. Es fácil ver que el procedimiento entra en el "ciclo" a lo sumo Nd_{max} veces. Además, puesto que claramente $p_1, \ldots, p_N$ son elementos linealmente independientes de $\prod_{d_{max}}$, resulta $N \leq \binom{d_{max}+n}{n} = \mathcal{O}((d_{max})^n)$. Teniendo en cuenta la cota anterior para el número de operaciones dentro de un "ciclo", concluimos que el procedimiento completo requiere $\mathcal{O}((d_{max}+1)^{7n+2})$ operaciones aritméticas en $\mathbb{Q}$ con $d_{max} \leq 7n^3(\prod_{j=1}^n \deg(F_j))D$. Sea d una cota superior para los grados de los polinomios $F_1, \ldots, F_n$. Entonces los cálculos anteriores requieren $d^{\mathcal{O}(n^2)}$ operaciones aritméticas en $\mathbb{Q}$.

Con respecto a la eficiencia de nuestro algoritmo en comparación con la de los algoritmos que usan bases de Gröbner o H–bases como los arriba descriptos, remitimos a los comentarios hechos en el Capítulo 1.

8.3.2. Cálculo de los interpolantes

En esta sección describimos un procedimiento para calcular las coordenadas $\tau(fu^{j-1})$ $(1 \leq j \leq D)$ de P_F en la base previamente calculada $\{G_1, \ldots, G_D\}$ de acuerdo con (8.10). Nuestro procedimiento para calcular las trazas $\tau(fu^{j-1})$ $(1 \leq j \leq D)$ consiste en calcular aproximaciones p–ádicas adecuadas de las trazas, para luego recuperarlas aplicando el algoritmo de reconstrucción racional de la Proposición 2.2.3.

En lo que sigue, β denota un straight–line program de longitud L, sin divisiones, que representa los polinomios $F_1, \ldots, F_n$ y F. A su vez, $Q, V_1, \ldots, V_n$ denotan una representación univariada de V con elemento primitivo U como en el Corolario 7.3.3. Por último, $\mathcal{J} \in \mathbb{Q}[V]$ denota la imagen del Jacobiano J de $F_1, \ldots, F_n$ y $u \in \mathbb{Q}[V]$ la imagen de U.

Observación 8.3.7. *Como se vió en el Capítulo 7, el algoritmo subyacente al Corolario 7.3.3 proporciona un primo "lucky" p como en la Proposición 7.1.2 tal que* $\log p \in \mathcal{O}^{\sim}(\log(d^n h))$. *En particular p satisface las siguientes condiciones:*

- *p no divide ninguno de los denominadores que aparecen en los polinomios $Q, V_1, \ldots, V_n$;*
- *las imágenes $Q_1, Q_1' \in \mathbb{Z}/p\mathbb{Z}[T]$ de Q, Q' son coprimas;*
- *existen (ver la Sección 6.2) $\gamma \in \mathbb{Z} \setminus \{0\}$ y $G_1, \ldots, G_{n+1} \in \mathbb{Z}[\boldsymbol{X}]$ tales que $p \nmid \gamma$ y*

$$\gamma = G_1 F_1 + \cdots + G_n F_n + G_{n+1} J. \tag{8.17}$$

De ahora en adelante p denota un número primo que satisface las condiciones de la Observación 8.3.7.

En lo que sigue, $\mathbb{Z}_{(p)}$ denota la localización de $\mathbb{Z}$ en p, esto es, el anillo formado por las fracciones $m/n \in \mathbb{Q}$ con $m, n \in \mathbb{Z}$ y $(n, p) = 1$. Además, para todo entero positivo $k \in \mathbb{Z}$ denotamos con $\mathbb{Z}/p^k\mathbb{Z}$ el anillo cociente de enteros módulo p^k. Denotamos con $\theta_k : \mathbb{Z}_{(p)} \to \mathbb{Z}/p^k\mathbb{Z}$ el homomorfismo de anillos definido por $\theta_k(m/n) = \overline{m}/\overline{n}$ para todo m/n (en forma reducida) $\in \mathbb{Z}_{(p)}$, donde $\overline{m}, \overline{n} \in \mathbb{Z}/p^k\mathbb{Z}$ denotan las clases de m y n módulo p^k. Por abuso de notación también denotamos con el símbolo θ_k los homomorfismos de anillos $\theta_k : \mathbb{Z}_{(p)}[\boldsymbol{X}] \to \mathbb{Z}/p^k\mathbb{Z}[\boldsymbol{X}]$ y $\theta_k : \mathbb{Z}_{(p)}[T] \to \mathbb{Z}/p^k\mathbb{Z}[T]$ que extienden el homomorfismo anterior en la forma obvia. Dado un número racional $q \in \mathbb{Z}_{(p)}$ y polinomios $F \in \mathbb{Z}_{(p)}[\boldsymbol{X}]$ y $G \in \mathbb{Z}_{(p)}[T]$, denotamos con q_k, F_k y G_k sus correspondientes imágenes vía θ_k. Llamamos a q_k, F_k y G_k las **aproximaciones p-ádicas** de orden k de q, F y G respectivamente.

Lema 8.3.8. *Sea G un polinomio arbitrario en $\mathbb{Z}_{(p)}[\boldsymbol{X}]$. Sea $g \in \mathbb{Q}[V]$ la imagen de G y $P \in \mathbb{Q}[T]$ el (único) polinomio con $\deg P < D$ tal que $P(u) = g$ en $\mathbb{Q}[V]$. Entonces P y el polinomio característico χ_g de g tienen coeficientes en el anillo local $\mathbb{Z}_{(p)}$. En particular, la norma $N(g)$, la traza $Tr(g)$ y el adjunto G^* de G son elementos de los anillos $\mathbb{Z}_{(p)}$ y $\mathbb{Z}_{(p)}[\boldsymbol{X}]$ respectivamente.*

Demostración. El polinomio $G(V_1, \ldots, V_n)$ que se obtiene sustituyendo $X_1, \ldots, X_n$ por $V_1, \ldots, V_n$ en G claramente es un elemento de $\mathbb{Z}_{(p)}[T]$. Puesto que P es el resto de la división de $G(V_1, \ldots, V_n)$ por el polinomio mónico Q, se sigue que $P \in \mathbb{Z}_{(p)}[T]$. Similarmente, sea $(b_{0,j}, \ldots, b_{D-1,j}) \in \mathbb{Z}_{(p)}^D$ la tupla de coeficientes del resto de la división de $G(V_1, \ldots, V_n)T^j$ por Q para $0 \leq j \leq D-1$. Tenemos las identidades

$$gu^j = \sum_{k=0}^{D-1} b_{k,j} u^k, \quad 0 \leq j \leq D-1.$$

Por lo tanto la matriz M_g de la homotecia η_g en la base $\{1, u, \ldots, u^{D-1}\}$ de $\mathbb{Q}[V]$ tiene entradas $b_{i,j} \in \mathbb{Z}_{(p)}$. Se sigue que

$$\chi_g = \det(TI_d - M_g) \in \mathbb{Z}_{(p)}[T],$$

lo que completa la demostración. □

Corolario 8.3.9. *Sea $H \in \mathbb{Q}[T]$ el (único) polinomio con $\deg H < D$ tal que $H(u) = \mathcal{J}^{-1}$. Entonces $H \in \mathbb{Z}_{(p)}[T]$.*

Demostración. De (8.17) deducimos que $\mathcal{J}^{-1} \in \mathbb{Q}[V]$ es la imagen del polinomio G_{n+1}/γ. La condición $p \nmid \gamma$ implica que $G_{n+1}/\gamma \in \mathbb{Z}_{(p)}[\boldsymbol{X}]$. Por el Lema 8.3.8 concluimos que $H \in \mathbb{Z}_{(p)}[T]$. □

Sea $F \in \mathbb{Z}[\boldsymbol{X}]$ un polinomio representado por un straight–line program β y denotemos con f su imagen en $\mathbb{Q}[V]$. Sea $P \in \mathbb{Q}[T]$ el polinomio con $\deg P < D$ tal que $P(u) = f$ en $\mathbb{Q}[V]$. Puesto que β no contiene divisiones, por el Lema 8.3.8 deducimos que $P \in \mathbb{Z}_{(p)}[T]$.

Sea $k \in \mathbb{Z}$ un entero positivo arbitrario y $Q_k, V_{1,k}, \ldots, V_{n,k} \in \mathbb{Z}/p^k\mathbb{Z}[T]$ las aproximaciones p-ádicas de orden k de $Q, V_1, \ldots, V_n$. Calculamos la aproximación p-ádica $P_k \in \mathbb{Z}/p^k\mathbb{Z}[T]$ de orden k de P siguiendo paso a paso el esquema de computación de β. Más precisamente, en primer lugar sustituimos $X_1, \ldots, X_n$ por $V_{1,k}, \ldots, V_{n,k}$ en β y luego, en cada paso ρ de β, realizamos la correspondiente operación $\circ_\rho$ en el anillo $\mathbb{Z}/p^k\mathbb{Z}[T]/(Q_k)$. Teniendo en cuenta que una operación aritmética $\{+, -, \times\}$ en $\mathbb{Z}/p^k\mathbb{Z}[T]/(Q_k)$ se puede realizar con $\mathcal{O}(\mathcal{M}(D))$ operaciones aritméticas en $\mathbb{Z}/p^k\mathbb{Z}$ y que β contiene L pasos de computación, obtenemos el siguiente resultado.

Lema 8.3.10. *Sea $F \in \mathbb{Z}[\boldsymbol{X}]$ un polinomio y denotemos por f su imagen en $\mathbb{Q}[V]$. Sea $P \in \mathbb{Q}[T]$ el polinomio con $\deg P < D$ tal que $P(u) = f$. Sea $k \in \mathbb{Z}$ un entero positivo arbitrario. Dados:*

- *un straight–line program β que representa a F con L operaciones aritméticas en $\mathbb{Z}[\boldsymbol{X}]$;*
- *un primo p como en la Observación 8.3.7;*
- *las aproximaciones p-ádicas de orden k de los parámetros de β y de los polinomios $Q, V_1, \ldots, V_n$;*

la aproximación p-ádica $P_k \in \mathbb{Z}/p^k\mathbb{Z}[T]$ de orden k de P se puede calcular con $\mathcal{O}(L\mathcal{M}(D))$ operaciones aritméticas en $\mathbb{Z}/p^k\mathbb{Z}$.

Cálculo del Jacobiano

Para calcular el Jacobiano J de $F_1, \ldots, F_n$, primero observamos que, por el Teorema de Baur–Strassen [BS83], a partir del straight–line program β de longitud L que representa $F_1, \ldots, F_n$ podemos obtener un straight–line program sin divisiones, con parámetros en $\mathbb{Z}$, de longitud $\mathcal{O}(L)$ que representa las entradas de J. Teniendo en cuenta el costo del cálculo del determinante de una matriz de tamaño $n \times n$ obtenemos el siguiente resultado.

Lema 8.3.11. *A partir del straight–line program β de longitud L que representa los polinomios $F_1, \ldots, F_n$ podemos obtener un straight–line program β' sin divisiones, con parámetros en $\mathbb{Z}$, de longitud $\mathcal{O}(L + n^4)$, que representa el Jacobiano J de $F_1, \ldots, F_n$.*

Inversión del Jacobiano

Sea $\mathcal{J}^{-1} \in \mathbb{Q}[V]$ la imagen del Jacobiano J de $F_1, \ldots, F_n$ y $H \in \mathbb{Q}[T]$ el polinomio del Corolario 8.3.9 tal que $H(u) = \mathcal{J}^{-1}$. A continuación describimos un algoritmo para calcular aproximaciones p-ádicas de H.

Sea $G \in \mathbb{Q}[T]$ el polinomio con $\deg G < D$ tal que $G(u) = \mathcal{J}$. Teniendo en cuenta la complejidad bit del Algoritmo de Euclides extendido (ver [vzGG99, Theorem 6.58]) una aplicación directa de este algoritmo para calcular el polinomio H a partir de G y Q requiere $\mathcal{O}^{\sim}(D^4\mu^2)$ operaciones bit, donde μ es una cota superior para las alturas de G y Q. En lo que sigue, describimos un procedimiento más eficiente para realizar este cálculo, en base al siguiente resultado.

Lema 8.3.12. *Sean $m \in \mathbb{Z}$ un entero positivo y f, g, $q \in \mathbb{Z}/m^2\mathbb{Z}[T]$ polinomios con q mónico de grado positivo D y f y g de grados menores que D, tales que*

$$f_m g_m \equiv 1 \mod (q_m) \quad \text{en} \quad \mathbb{Z}/m\mathbb{Z}[T].$$

Aquí f_m, g_m y q_m denotan las imágenes en $\mathbb{Z}/m\mathbb{Z}[T]$ de f, g y q respectivamente.

Sean r, $s \in \mathbb{Z}/m^2\mathbb{Z}[T]$ tales que $fg = 1 + rq + sm$. Sea $g' \in \mathbb{Z}/m^2\mathbb{Z}[T]$ con $\deg g' < D$ tal que $g' \equiv g(1 - ms) \mod (q)$ en $\mathbb{Z}/m^2\mathbb{Z}[T]$. Entonces g' satisface

$$fg' \equiv 1 \mod (q) \quad \text{en} \quad \mathbb{Z}/m^2\mathbb{Z}[T].$$

Además, g' se puede calcular, a partir de f, g, q y m, con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(\log(m^2)))$ operaciones bit.

Demostración. Un simple cálculo muestra que

$$fg(1 - ms) = (1 + rq + sm)(1 - ms) = 1 - m^2s^2 + r(1 - ms)q,$$

de donde se sigue la primera parte del lema.

Para calcular g' primero calculamos polinomios $r, s \in \mathbb{Z}/m^2\mathbb{Z}[T]$ tales que $fg = 1 + rq + sm$. Con este propósito calculamos el cociente $r_m \in \mathbb{Z}/m\mathbb{Z}[T]$ de la división de $f_m g_m$ por q_m. Escribamos

$$r_m = \sum_{i=0}^{D-2} [a_i]_m T^i, \quad \text{con} \quad a_i \in \{0, \ldots, m-1\},$$

y definamos

$$r := \sum_{i=0}^{D-2} [a_i]_{m^2} T^i.$$

Sea $h = fg - rq - 1$ y denótese con $h_m \in \mathbb{Z}/m\mathbb{Z}[T]$ la imagen de h. Por construcción $f_m g_m = r_m q_m + 1$. Luego $h_m = 0$ y podemos escribir

$$h = \sum_{i=0}^{2D-2} [b_i]_{m^2} T^i, \quad \text{con} \quad b_i \in \{0, \ldots, m^2 - 1\},$$

donde cada b_i es un múltiplo de m para $0 \leq i \leq 2D-2$. Defínase

$$s := \sum_{i=0}^{2D-2} [b_i/m]_{m^2} T^i.$$

Es claro que los polinomios $r, s \in \mathbb{Z}/m^2\mathbb{Z}[T]$ recién construidos satisfacen $fg = 1 + rq + sm$ como se deseaba. Finalmente obtenemos g' como el resto de la división de $g(1 - ms)$ por q en $\mathbb{Z}/m^2\mathbb{Z}[T]$.

A continuación analizamos la complejidad del procedimiento anterior. El cálculo de f_m, g_m y q_m requiere la reducción módulo m de enteros de longitud bit del orden $\mathcal{O}(\log(m^2))$. Esto requiere $\mathcal{O}(D\mathcal{M}(\log(m^2)))$ operaciones bit. El producto $f_m g_m$ y el cociente r_m se pueden calcular, a partir de f_m, g_m, y q_m, con $\mathcal{O}(\mathcal{M}(D))$ operaciones aritméticas en $\mathbb{Z}/m\mathbb{Z}$, lo que equivale a $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(\log m))$ operaciones bit. El cálculo de h requiere dos multiplicaciones de polinomios de grado a lo sumo D en $\mathbb{Z}/m^2\mathbb{Z}[T]$ más dos substracciones. Esto se puede hacer con $\mathcal{O}(\mathcal{M}(D))$ operaciones aritméticas en $\mathbb{Z}/m^2\mathbb{Z}$ y por lo tanto con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(\log(m^2)))$ operaciones bit. El cáclulo de los cocientes b_i/m requiere $\mathcal{O}(D\mathcal{M}(\log(m^2)))$ operaciones bit adicionales. Finalmente, a partir de g y s podemos calcular el producto $g(1 - ms)$ y el resto g' de la división de $g(1 - ms)$ por q con $\mathcal{O}(\mathcal{M}(D))$ operaciones aritméticas en $\mathbb{Z}/m^2\mathbb{Z}$ y por lo tanto con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(\log(m^2)))$ operaciones bit. Resumiendo, obtenemos la complejidad anunciada para el procedimiento completo. □

Corolario 8.3.13. *Sea p un número primo y $k \in \mathbb{Z}$ un entero positivo. Sean f, $q \in \mathbb{Z}/p^{2^k}\mathbb{Z}[T]$ con q mónico, $D := \deg q > 0$, $\deg f < D$, tales que f es una unidad en el anillo cociente $\mathbb{Z}/p^{2^k}\mathbb{Z}[T]/(q)$. Entonces podemos calcular el polinomio $g \in \mathbb{Z}/p^{2^k}\mathbb{Z}[T]$ con $\deg g < D$ tal que*

$$fg \equiv 1 \mod (q) \quad \text{en} \quad \mathbb{Z}/p^{2^k}\mathbb{Z}[T],$$

con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(2^k \log p))$ operaciones bit.

Demostración. Calculamos la sucesión de polinomios $g_i \in \mathbb{Z}[T]$ $(0 \leq i \leq k)$ tal que g_i tiene coeficientes en $\{0, \ldots, p^{2^i} - 1\}$, $\deg g_i < D$, y las aproximaciones p-ádicas f_{2^i}, $g_{i,2^i}$, y q_{2^i} de orden 2^i de los polinomios f, g_i y q satisfacen las ecuaciones

$$f_{2^i} g_{i,2^i} \equiv 1 \mod (q_{2^i}) \quad \text{en} \quad \mathbb{Z}/p^{2^i}\mathbb{Z}[T],$$

para $0 \leq i \leq k$. Por lo tanto $g = g_{k,2^k}$. Con este propósito primero calculamos todos los f_{2^i}, q_{2^i} $(0 \leq i \leq k)$ con $\mathcal{O}(D\mathcal{M}(\log p^{2^k}))$ operaciones bit. Luego aplicamos el Algoritmo de Euclides extendido a f_1 y q_1 para calcular g_0 con $\mathcal{O}(\mathcal{U}(D))$ operaciones aritméticas en $\mathbb{Z}/p\mathbb{Z}$ y por lo tanto con $\mathcal{O}(\mathcal{U}(D)\mathcal{U}(\log p))$ operaciones bit. Supóngase que ya hemos calculado g_{i-1} y sea $g_{i-1,2^i} \in \mathbb{Z}/p^{2^i}\mathbb{Z}[T]$ su aproximación p–ádica de orden 2^i. Por el Lema 8.3.12 podemos calular g_i, a partir de f_{2^i}, q_{2^i}, y $g_{i-1,2^i}$, con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(\log(p^{2^i})))$ operaciones bit. Puesto que $\sum_{i=0}^{k} \mathcal{U}(\log(p^{2^i})) = \mathcal{O}(\mathcal{U}(\log(p^{2^k})))$, el procedimiento completo se puede realizar con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(2^k \log p))$ operaciones bit. □

Sea p un número primo como en la Observación 8.3.7 y $k \in \mathbb{Z}$ un entero positivo arbitrario. A continuación, calculamos la aproximación p-ádica $H_{2^k} \in \mathbb{Z}/p^{2^k}\mathbb{Z}[T]$ de orden 2^k de H. Más precisamente, supóngase que, además de p y el straight–line program β, tenemos las aproximaciones p-ádicas de orden 2^k de los polinomios $Q, V_1, \ldots, V_n$ y de los parámetros de β. Para calcular el polinomio H_{2^k} primero obtenemos a partir de β un straight–line program β' de talla $\mathcal{O}(L+n^4)$ que representa el Jacobiano J (Lema 8.3.11). Luego, a partir de β' calculamos la aproximación p-ádica $G_{2^k} \in \mathbb{Z}/p^{2^k}\mathbb{Z}[T]$ de orden 2^k del polinomio $G \in \mathbb{Z}_{(p)}[T]$ con $\deg G < D$ tal que $G(u) = \mathcal{J}$. Por los Lema 8.3.10 y 8.3.11 este cálculo se puede hacer con $\mathcal{O}((L + n^4)\mathcal{M}(D))$ operaciones aritméticas en $\mathbb{Z}/p^{2^k}\mathbb{Z}$. La congruencia $HG \equiv 1$ mód (Q) claramente vale en el anillo $\mathbb{Z}_{(p)}[T]$. Por lo tanto, deducimos la congruencia $H_{2^k}G_{2^k} \equiv 1 \mod (Q_{2^k})$ en el anillo $\mathbb{Z}/p^{2^k}\mathbb{Z}[T]$. Por el Corolario 8.3.13, el polinomio H_{2^k} se calcula a partir de Q_{2^k} y G_{2^k} con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(2^k \log p))$ operaciones bit.

En resumen, obtenemos el siguiente resultado.

Lema 8.3.14. *Sea $H \in \mathbb{Q}[T]$ el polinomio con $\deg H < D$ tal que $H(u) = \mathcal{J}^{-1}$ y sea $k \in \mathbb{Z}$ un entero positivo arbitrario. Dados:*

- *el straight–line program β de longitud L que representa los polinomios $F_1, \ldots, F_n$;*
- *un primo p como en la Observación 8.3.7;*
- *las aproximaciones p-ádicas de orden 2^k de los parámetros de β y de los polinomios $Q, V_1, \ldots, V_n$;*

la aproximación p-ádica $H_{2^k} \in \mathbb{Z}/p^{2^k}\mathbb{Z}[T]$ de orden 2^k de H se calcula con $\mathcal{O}((L + n^4)\mathcal{M}(D)\mathcal{U}(2^k \log p))$ operaciones bit.

Cálculo de las trazas

En el siguiente lema estimamos el costo de calcular aproximaciones p-ádicas de las trazas $Tr(u^j)$ $(0 \leq j \leq D-1)$.

Lema 8.3.15. *Sea $k \in \mathbb{Z}$ un entero positivo arbitrario. Dados un primo p como en la Observación 8.3.7 y la aproximación p–ádica Q_{2^k} de orden 2^k del polinomio minimal Q, las aproximaciones p-ádicas $Tr(u^j)_{2^k}$ $(0 \leq j \leq D-1)$ de orden 2^k de las trazas $Tr(u^j)$ $(0 \leq j \leq D-1)$ se calculan con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(2^k \log p))$ operaciones bit.*

Demostración. Recordamos la siguiente identidad de series de potencias formales en la variable T (ver [Lan93, Chapter XIV, Exercise 24]):

$$-\frac{d}{dT}\log\det(I-TA)=\sum_{j=0}^{\infty}Tr(A^{j+1})T^j. \tag{8.18}$$

Aquí I es la matriz identidad y A una matriz cuadrada cualquiera con coeficientes en un cuerpo.

Sea $A\in\mathbb{Q}^{D\times D}$ la matriz compañera de $Q=T^D+a_{D-1}T^{D-1}+\cdots+a_0$ y sea $P:=\det(I-TA)$. Es fácil comprobar que $P(T)=1+a_{D-1}T+a_{D-2}T^2+\cdots+a_0T^D$. En este caso $Tr(A^j)=Tr(u^j)$ para $j\geq 0$ y la identidad (8.18) ahora resulta

$$-\frac{P'(T)}{P(T)}=\sum_{j=0}^{\infty}Tr(u^{j+1})T^j.$$

Por lo tanto, tenemos la siguiente identidad de series de potencias formales en $\mathbb{Z}/p^{2^k}\mathbb{Z}[\![T]\!]$:

$$-\frac{P'_{2^k}(T)}{P_{2^k}(T)}=\sum_{j=0}^{\infty}Tr(u^{j+1})_{2^k}T^j. \tag{8.19}$$

Sea $f\in\mathbb{Z}/p^{2^k}\mathbb{Z}[T]$ el polinomio $f:=P_{2^k} \mod (T^D)$. Entonces $\deg f<D$ y f es una unidad en $\mathbb{Z}/p^{2^k}\mathbb{Z}[T]/(T^D)$. Por el Corolario 8.3.13 podemos calcular a partir de f el polinomio $g\in\mathbb{Z}/p^{2^k}\mathbb{Z}[T]$ con $\deg g<D$ tal que $fg\equiv 1 \mod (T^D)$ con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(2^k\log p))$ operaciones bit. A partir de (8.19) deducimos fácilmente la siguiente identidad de polinomios en $\mathbb{Z}/p^{2^k}\mathbb{Z}[T]$:

$$-P'_{2^k}g \mod (T^D)=\sum_{j=0}^{D-1}Tr(u^{j+1})_{2^k}T^j.$$

Por lo tanto, obtenemos todos los coeficientes $Tr(u^j)_{2^k}$ $(1\leq j\leq D-1)$ calculando el producto $-P'_{2^k}g$, lo que se puede hacer con $\mathcal{O}(\mathcal{M}(D))$ operaciones aritméticas en $\mathbb{Z}/p^{2^k}\mathbb{Z}$. El cálculo completo requiere $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(2^k\log p))$ operaciones bit. □

Sean $\boldsymbol{v},\boldsymbol{w}\in\mathbb{Q}^D$ los vectores definidos por $\boldsymbol{v}_j:=Tr(u^{j-1})$ y $\boldsymbol{w}_j:=\tau(fu^{j-1})$ para $1\leq j\leq D$. Sea $k\in\mathbb{Z}$ un entero positivo arbitrario. Sea $\boldsymbol{v}^k\in(\mathbb{Z}/p^k\mathbb{Z})^D$ el vector definido por $\boldsymbol{v}^k_j:=\boldsymbol{v}_{j,k}$ para $1\leq j\leq D$. Aquí $\boldsymbol{v}_{j,k}$ es la aproximación p–ádica de orden k de $\boldsymbol{v}_j$. Defínase $\boldsymbol{w}^k\in(\mathbb{Z}/p^k\mathbb{Z})^D$ de manera similar. Recuérdese que, si R es un anillo, denotamos con $\langle\cdot,\cdot\rangle$ el producto interno, que se define por $\langle\boldsymbol{x},\boldsymbol{y}\rangle:=\sum_{j=1}^{D}x_jy_j$ para $\boldsymbol{x},\boldsymbol{y}\in R^D$. Tenemos el siguiente lema.

Lema 8.3.16. *Con las hipótesis y notaciones anteriores, sea además $P\in\mathbb{Z}_{(p)}[T]$ el polinomio con $\deg P<D$ tal que $\mathcal{J}^{-1}f=P(u)$ en $\mathbb{Q}[V]$. Entonces valen las siguientes afirmaciones:*

- *$\boldsymbol{w}$ es el único vector de $\mathbb{Q}^D$ que satisface $\langle\boldsymbol{w},g\rangle=\langle\boldsymbol{v},\mathcal{J}^{-1}fg\rangle$ para todo $g\in\mathbb{Q}[V]$.*

- $\boldsymbol{w}^k$ *es el único vector de* $(\mathbb{Z}/p^k\mathbb{Z})^D$ *que satisface* $\langle \boldsymbol{w}^k, h\rangle = \langle \boldsymbol{v}^k, P_k h\rangle$ *para todo* $h \in \mathbb{Z}/p^k\mathbb{Z}[T]/(q_{u,k})$.

Demostración. Consideremos un elemento arbitrario $g \in \mathbb{Q}[V]$ y escribamos $g = \sum_{0\le j\le D-1} g_j u^j$, donde $g_j \in \mathbb{Q}$ para $0 \le j \le D-1$. Por linealidad,

$$\langle \boldsymbol{v}, g\rangle = \sum_{j=1}^{D} g_{j-1}\boldsymbol{v}_j = \sum_{j=1}^{D} g_{j-1} Tr(u^{j-1}) = Tr(g).$$

Por lo tanto tenemos que

$$\langle \boldsymbol{v}, \mathcal{J}^{-1} f u^{j-1}\rangle = Tr(\mathcal{J}^{-1} f u^{j-1}) = \tau(f u^{j-1}) = \boldsymbol{w}_j = \langle \boldsymbol{w}, u^{j-1}\rangle,$$

para $1 \le j \le D$. Puesto que $\{1, u, \ldots, u^{D-1}\}$ es una base de $\mathbb{Q}[V]$, la primera afirmación del lema queda probada.

A continuación, considérese un polinomio arbitrario $G = \sum_{0\le j\le D-1} b_j T^j \in \mathbb{Z}[T]$. Escríbase $g := G(u)$ y $\mathcal{J}^{-1} f g = \sum_{0\le j\le D-1} c_j u^j$, donde $c_j \in \mathbb{Q}$ para $0 \le j \le D-1$. Tenemos que

$$\langle \boldsymbol{w}, g\rangle_k = \sum_{j=1}^{D} \boldsymbol{w}_{j,k} b_{j-1,k} = \langle \boldsymbol{w}^k, G_k\rangle,$$

y

$$\langle \boldsymbol{v}, \mathcal{J}^{-1} f g\rangle_k = \sum_{j=1}^{D} \boldsymbol{v}_{j,k} c_{j-1,k} = \langle \boldsymbol{v}^k, P_k G_k\rangle.$$

Esto muestra que $\langle \boldsymbol{w}^k, G_k\rangle = \langle \boldsymbol{v}^k, P_k G_k\rangle$ para todo $G \in \mathbb{Z}[T]$, lo que prueba la segunda afirmación del lema. □

Observación 8.3.17. *Como consecuencia del lema anterior, podemos calcular* $\boldsymbol{w}^k$*, a partir de* $\boldsymbol{v}^k$ *y* P_k*, usando el algoritmo para la multiplicación traspuesta de [Sho99], con* $\mathcal{O}(\mathcal{M}(D))$ *operaciones aritméticas en* $\mathbb{Z}/p^k\mathbb{Z}$.

Finalmente podemos estimar el costo del cálculo de las trazas $\tau(f u^{j-1})$ $(1 \le j \le D)$.

Teorema 8.3.18. *Con las hipótesis y notaciones anteriores, sea* η *una cota superior para las alturas de las trazas* $\tau(f u^{j-1})$ $(1 \le j \le D)$ *y sea* $k := \lceil \log(2\eta+1)\rceil$*. Dados:*

- *el straight–line program* β *de longitud* L *que representa los polinomios* $F_1, \ldots, F_n$*;*
- *un primo* p *como en la Observación 8.3.7;*
- *las aproximaciones* p*-ádicas de orden* 2^k *de los parámetros de* β *y de los polinomios* $Q, V_1, \ldots, V_n$*;*

todas las trazas $\tau(f u^{j-1})$ $(1 \le j \le D)$ *se pueden calcular con* $\mathcal{O}^{\sim}((L+n^4)D\eta \log(d^n h))$ *operaciones bit.*

Demostración. Sea $P \in \mathbb{Z}_{(p)}[T]$ el polinomio tal que $\deg P < D$ y $P(u) = \mathcal{J}^{-1}f$. A partir de β y de las aproximaciones p-ádicas de orden 2^k de los parámetros de β y de los polinomios $Q, V_1, \ldots, V_n$, calculamos la aproximación p–ádica $P_{2^k} \in \mathbb{Z}/p^{2^k}\mathbb{Z}[T]$ de orden 2^k de P. Por los Lemas 8.3.14 y 8.3.10 este cálculo se puede realizar con $\mathcal{O}((L+n^4)\mathcal{M}(D)\mathcal{U}(2^k \log p))$ operaciones bit. Sean $\boldsymbol{v}^{2^k}, \boldsymbol{w}^{2^k} \in (\mathbb{Z}/p^{2^k}\mathbb{Z})^D$ los vectores del Lema 8.3.16. Por el Lema 8.3.15 todas las aproximaciones $Tr(u^{j-1})_{2^k}$ $(1 \leq j \leq D)$, esto es, el vector $\boldsymbol{v}^{2^k}$, se pueden calcular, a partir de Q_{2^k}, con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(2^k \log p))$ operaciones bit. Por el Lema 8.3.17 el vector $\boldsymbol{w}^{2^k}$, esto es, todas las aproximaciones $\tau(fu^{j-1})_{2^k}$ $(1 \leq j \leq D)$ se pueden calcular, a partir de $\boldsymbol{v}^{2^k}$ y P_{2^k}, con $\mathcal{O}(\mathcal{M}(D))$ operaciones aritméticas en $\mathbb{Z}/p^{2^k}\mathbb{Z}$, y por lo tanto con $\mathcal{O}(\mathcal{M}(D)\mathcal{U}(2^k \log p))$ operaciones bit. Puesto que $\sqrt{p^{2^k}/2} \geq 2^\eta$, podemos recuperar cada traza $\tau(fu^{j-1})$ a partir de su aproximación p-ádica $\tau(fu^{j-1})_{2^k}$ con $\mathcal{O}(\mathcal{U}(2^k \log p))$ operaciones bit. Por lo tanto la reconstrucción de todas las trazas $\tau(fu^{j-1}))$ $(1 \leq j \leq D)$ requiere a lo sumo $\mathcal{O}(D\mathcal{U}(2^k \log p))$ operaciones bit. Se ve fácilmente que el cálculo completo se puede realizar con $\mathcal{O}((L+n^4)\mathcal{M}(D)\mathcal{U}(2^k \log p))$ operaciones bit. Las estimaciones de complejidad del teorema se obtienen observando que $2^k \in \mathcal{O}(\eta)$ y $\log p \in \mathcal{O}(\log(d^n h))$. □

Observación 8.3.19. *También se ve fácilmente a partir de los Lemas 8.3.15 y 8.3.16 que las trazas $\tau(fu^{j-1})$ $(1 \leq j \leq D)$ del Teorema 8.3.18 se pueden calcular probabilísticamente con $\mathcal{O}((L+n^4)\mathcal{M}(D))$ operaciones aritméticas en $\mathbb{Q}$.*

8.3.3. Complejidad del procedimiento completo

Finalmente obtenemos la siguiente estimación para el costo total de ejecutar los algoritmos anteriores.

Teorema 8.3.20. *Sean $F_1, \ldots, F_n \in \mathbb{Z}[\boldsymbol{X}]$ polinomios de grado a lo sumo d que forman una sucesión regular reducida y definen una variedad cero–dimensional $V \subset \mathbb{A}^n$. Sea $F \in \mathbb{Z}[\boldsymbol{X}]$ un polinomio adicional arbitrario. Sea β un straight–line program de longitud L sin divisiones, con parámetros enteros, que representa los polinomios $F_1, \ldots, F_n$ y F. Sea $D := \deg(V)$ y δ el grado del sistema $F_1 = 0, \ldots, F_n = 0$. Además, sea h una cota superior para las alturas de los parámetros de β y las alturas de los polinomios $F_1, \ldots, F_n$. Entonces existe un algoritmo probabilístico que calcula los siguientes elementos:*

- *un straight–line program β' de longitud $\mathcal{O}(n^2L + n^4)\mathcal{M}(d^2\delta))$ que representa una base $\{G_1, \ldots, G_D\}$ de un espacio de interpolantes Π_V tal que $\deg(G_j) \leq n(d-1)$ para $1 \leq j \leq D$;*
- *las coordenadas $\tau(fu^{j-1})$ $(1 \leq j \leq D)$ en la base anterior del interpolante $P_F \in \Pi_V$ de F.*

El algoritmo se ejecuta en complejidad bit

$$\mathcal{O}^{\sim}\Big(n(nL+n^5)\delta\big[d\delta + nd^n h\big(d^n + \deg(F) + h(F)\big)\big]\Big).$$

Demostración. Por el Teorema 8.3.5 podemos calcular a partir de β una base $\{G_1, \ldots, G_D\}$ de un espacio de interpolantes Π_V con

$$\mathcal{O}^{\sim}\big(n(nL + n^5)\delta(d\delta + nd^{2n}h)\big) \tag{8.20}$$

operaciones bit. El cálculo anterior proporciona además un primo p como en la Observación 8.3.7 y una representación univariada $Q, V_1, \ldots, V_n$ de V con elemento primitivo U. Sea η una cota superior para las alturas de las trazas $\tau(fu^{j-1})$ $(1 \leq j \leq D)$ y $k := \lceil \log(2\eta + 1) \rceil$. Por medio del algoritmo subyacente al Teorema 7.3.2 podemos calcular las aproximaciones p-ádicas de orden 2^k de $Q, V_1, \ldots, V_n$ (Proposición 7.2.1) con $\mathcal{O}^{\sim}\big((nL+n^4)\delta\eta \log p\big)$ operaciones bit. A continuación, por el Teorema 8.3.18, podemos calcular las coordenadas $\tau(fu^{j-1})$ $(1 \leq j \leq D)$ de P_F en la base $\{G_1, \ldots, G_D\}$ con $\mathcal{O}^{\sim}\big((L+n^4)D\eta \log(d^n h)\big)$ operaciones bit. Puesto que $D \leq \delta$, deducimos que los cálculos anteriores se pueden realizar con $\mathcal{O}^{\sim}\big(n(nL + n^5)\delta(d\delta + nd^{2n}h + \eta)\big)$ operaciones bit. Notando que, de acuerdo con el Lema 8.1.4, podemos tomar $\eta \in \mathcal{O}^{\sim}\Big(\big(d^n + \deg(F) + h(F)\big)d^n h\Big)$ y teniendo en cuenta que $D \leq \delta \leq d^n$, se obtiene la estimación de complejidad del teorema. □

Observación 8.3.21. *Vemos fácilmente a partir de las Observaciones 8.3.6 y 8.3.19 que los ítems del Teorema 8.3.20 se pueden calcular probabilísticamente con* $\mathcal{O}^{\sim}\big(n(nL+n^4)(d\delta)^2\big)$ *operaciones aritméticas en* $\mathbb{Q}$.

Capítulo 9

Un modelo computacional para la interpolación de Hermite–Lagrange

9.1. Definiciones y notaciones básicas

Para todo $n \in \mathbb{N}$, denotamos por $\mathbb{A}^n := \mathbb{A}^n(\mathbb{C})$ el espacio afín n–dimensional $\mathbb{C}^n$, equipado con sus respectivas topologías de Zariski y Euclídea sobre $\mathbb{C}$. En geometría algebraica la topología Euclídea de $\mathbb{A}^n$ también se llama la **topología fuerte**. Utilizaremos esta terminología solo excepcionalmente. En general estará claro por el contexto a cuál de estas dos topologías nos estamos refiriendo.

En lo que sigue utilizaremos la siguiente terminología especial. Una aplicación parcial $\phi : V \dashrightarrow W$, donde V y W son subvariedades afínes cerradas de $\mathbb{A}^n$ y $\mathbb{A}^m$ respectivamente y $\phi_1, \ldots, \phi_m$ son las componentes de ϕ, se llama un **morfismo** de variedades afines (o simplemente una **aplicación polinomial**) si las funciones $\phi_1, \ldots, \phi_m$ pertenecen a $\mathbb{C}[V]$ (por lo tanto, en particular, ϕ es una aplicación total). Si el dominio U de ϕ es un subconjunto abierto y denso Zariski de V y $\phi_1, \ldots, \phi_m$ son las restricciones de funciones racionales adecuadas de V a U, llamamos a ϕ una **aplicación racional** de V en W. Equivalentemente, $\phi : U \to W$ es un morfismo de la variedad abierta U en la variedad W en el sentido de la Definición 2.1.8. Obsérvese que nuestra definición de aplicación racional difiere de la usual en geometría algebraica, es decir, la de la Definición 2.1.9, puesto que no requiere que el dominio U de ϕ sea maximal. Por lo tanto, en el caso $m := 1$, nuestros conceptos de función racional y aplicación racional no coinciden.

9.1.1. Conjuntos construibles y aplicaciones construibles

Sea $\mathcal{M}$ un subconjunto de un espacio afín $\mathbb{A}^n$ y, para un entero no negativo m, sea $\phi : \mathcal{M} \dashrightarrow \mathbb{A}^m$ una aplicación parcial. Llamamos **construible** al conjunto $\mathcal{M}$ si $\mathcal{M}$ es definible por una combinación Booleana de ecuaciones polinomiales. Equivalentemente, $\mathcal{M}$ es construible si es una unión finita (disjunta) de subconjuntos localmente cerrados (en la topología de Zariski) de $\mathbb{A}^n$. Un hecho básico que usaremos

en lo sucesivo es que si $\mathcal{M}$ es construible, entonces su clausura Zariski es igual a su clausura Euclídea (ver, por ejemplo, [Mum88, Chapter I, §10, Corollary 1]).

En la misma línea llamamos **construible** a la aplicación parcial ϕ si el gráfico de ϕ es construible como subconjunto del espacio afín $\mathbb{A}^n \times \mathbb{A}^m$. Decimos que ϕ es **polinomial** si ϕ es la restricción de un morfismo de variedades afines $\mathbb{A}^n \to \mathbb{A}^m$ a un subconjunto construible $\mathcal{M}$ de $\mathbb{A}^n$ (y por lo tanto una aplicación total de $\mathcal{M}$ en $\mathbb{A}^m$). Además, llamamos a ϕ una aplicación **racional** de $\mathcal{M}$ si el dominio U de ϕ es un subconjunto abierto y denso Zariski de $\mathcal{M}$ y ϕ es la restricción a U de una aplicación racional de la clausura Zariski $\overline{\mathcal{M}}$ de $\mathcal{M}$. Obsérvese que, siendo U a su vez construible, U contiene un subconjunto abierto y denso Zariski de $\overline{\mathcal{M}}$ (ver, por ejemplo, [Har77, Exercise 3.18]).

Sea $\phi : \mathcal{M} \to \mathbb{A}^m$ una aplicación construible total. Decimos que ϕ es **regular** en $x \in \mathcal{M}$ si existe una aplicación racional $\psi : \mathcal{M} \dashrightarrow \mathbb{A}^m$ y un subconjunto abierto U de $\mathcal{M}$ con $x \in U$ tal que $\psi = \phi$ en U. Decimos que ϕ es **regular** si es regular en todo punto de $\mathcal{M}$. En otras palabras, ϕ es regular si es una aplicación racional de $\mathcal{M}$ definida en todo punto de $\mathcal{M}$.

Puesto que la teoría elemental (esto es, de primer orden) de cuerpos algebraicamente cerrados con constantes en $\mathbb{C}$ admite eliminación de cuantificadores, constructibilidad significa simplemente definibilidad elemental. En particular, ϕ construible implica que el dominio y la imagen de ϕ son subconjuntos construibles de $\mathbb{A}^n$ y $\mathbb{A}^m$ respectivamente (ver, por ejemplo, [Mar02]). Un hecho útil concerniente a las aplicaciones construibles que vamos a usar en lo sucesivo es el siguiente resultado (ver, por ejemplo, [Mar02, Proposition 3.2.14]).

Lema 9.1.1. *Sea $\mathcal{M}$ un subconjunto construible de $\mathbb{A}^n$ y sea $\phi : \mathcal{M} \dashrightarrow \mathbb{A}^m$ una aplicación parcial. Entonces ϕ es construible si y sólo si existe una partición de su dominio en finitos subconjuntos construibles, digamos $\mathcal{M}_1, \ldots, \mathcal{M}_s$, tales que para $1 \leq k \leq s$ la restricción de ϕ a $\mathcal{M}_k$ es una aplicación racional de $\mathcal{M}_k$ que está definida en todo punto de $\mathcal{M}_k$.*

En particular, si $\phi : \mathcal{M} \to \mathbb{A}^m$ es una aplicación construible total, entonces existe un subconjunto abierto y denso Zariski U de $\mathcal{M}$ tal que la restricción $\phi|_U$ de ϕ a U es una aplicación racional.

Ahora vamos a introducir las nociones de aplicación débilmente continua, fuertemente continua, topológicamente robusta y hereditaria del conjunto construible $\mathcal{M}$. Estas cuatro nociones constituirán una herramienta fundamental para la modelización de los problemas y algoritmos de interpolación de Hermite–Lagrange en la Sección 9.2 y el Capítulo 10.

Definición 9.1.2. *Sea $\mathcal{M}$ un subconjunto construible de $\mathbb{A}^n$ y sea $\phi : \mathcal{M} \to \mathbb{A}^m$ una aplicación construible (total). Consideramos las siguientes cuatro condiciones:*

(i) existe un subconjunto abierto y denso Zariski U de $\mathcal{M}$ tal que la restricción $\phi|_U$ de ϕ a U es una aplicación racional de $\mathcal{M}$ y el gráfico de ϕ está contenido en la clausura Zariski del gráfico de $\phi|_U$ en $\mathcal{M} \times \mathbb{A}^m$;

(ii) ϕ es continua con respecto a la topología Euclídea (esto es, fuerte) de $\mathcal{M}$ y $\mathbb{A}^m$;

(iii) para toda sucesión $(x_k)_{k\in\mathbb{N}}$ de $\mathcal{M}$ que converge en la topología Euclídea a un punto de $\mathcal{M}$, la sucesión $(\phi(x_k))_{k\in\mathbb{N}}$ es acotada;

(iv) para todo subconjunto construible $\mathcal{N}$ de $\mathcal{M}$ la restricción $\phi|_{\mathcal{N}} : \mathcal{N} \to \mathbb{A}^m$ es una extensión de una aplicación racional de $\mathcal{N}$ y el gráfico de $\phi|_{\mathcal{N}}$ está contenido en la clausura Zariski del gráfico de esta aplicación racional en $\mathcal{N} \times \mathbb{A}^m$.

Llamamos a la aplicación ϕ

- ***débilmente continua** si ϕ satisface la condición (i),*
- ***fuertemente continua** si ϕ satisface la condición (ii),*
- ***topológicamente robusta** si ϕ satisface las condiciones (i) y (iii),*
- ***hereditaria** si ϕ satisface la condición (iv).*

Observación 9.1.3. *Sea $\phi : \mathcal{M} \to \mathbb{A}^m$ una aplicación construible total. Entonces ϕ es topológicalmente robusta si y sólo si existe un subconjunto abierto y denso Zariski U de $\mathcal{M}$ para el cual la condición (i) se satisface y, para toda sucesión $(x_k)_{k\in\mathbb{N}}$ de U que converge en la topología Euclídea a un punto de $\mathcal{M}$, la sucesión $(\phi(x_k))_{k\in\mathbb{N}}$ es acotada.*

Demostración. La parte *solo si* es obvia. Vamos a probar la parte *si*: supóngase que la segunda condición en el enunciado de la observación se satisface y sea U el correspondiente subconjunto abierto y denso Zariski de $\mathcal{M}$. Sea $(x_k)_{k\in\mathbb{N}}$ una sucesión arbitraria de $\mathcal{M}$ que converge en la topología Euclídea a un punto $x \in \mathcal{M}$. Entonces de la condición (i) deducimos que existe una sucesión $(y_k)_{k\in\mathbb{N}}$ de puntos de U tal que $||(x_k, \phi(x_k)) - (y_k, \phi(y_k))|| < 1/k$ se satisface para todo $k \in \mathbb{N}$, donde $||\cdot||$ denota la norma Euclídea de $\mathcal{M} \times \mathbb{A}^m$. Esto implica que la sucesión $(y_k)_{k\in\mathbb{N}}$ converge a x y que $||\phi(x_k) - \phi(y_k)|| < 1$ vale para todo $k \in \mathbb{N}$. Por lo tanto la sucesión $(\phi(x_k))_{k\in\mathbb{N}}$ es acotada. Concluimos que la aplicación construible $\phi : \mathcal{M} \to \mathbb{A}^m$ es topológicamente robusta. Esto termina la demostración de la Observación 9.1.3. □

Ahora analicemos la interdependencia de las nociones de aplicación débilmente continua, fuertemente continua, topológicamente robusta y hereditaria.

Lema 9.1.4. *Sea $\phi : \mathcal{M} \to \mathbb{A}^m$ una aplicación construible fuertemente continua. Entonces ϕ es débilmente continua, topológicamente robusta y hereditaria.*

Demostración. Primero probamos que ϕ es débilmente continua. De acuerdo con el Lema 9.1.1, existe un subconjunto abierto y denso Zariski U de $\mathcal{M}$ tal que $\phi|_U$ es una aplicación racional de $\mathcal{M}$. Luego, la continuidad fuerte de ϕ implica que el gráfico de ϕ está contenido en la clausura Euclídea del gráfico de $\phi|_U$. Puesto que las clausuras Euclídea y de Zariski de un conjunto construible coinciden, deducimos que ϕ es débilmente continua.

Puesto que la condición (ii) implica la condición (iii), la aplicación construible ϕ es topológicamente robusta. Ahora es claro que ϕ es hereditaria. □

Por otra parte, una aplicación débilmente continua o topológicamente robusta no necesariamente es fuertemente continua, como muestra el siguiente ejemplo.

Ejemplo 9.1.5. *Sea $\mathcal{M} \subset \mathbb{A}^2$ el conjunto construible $\mathcal{M} := \{(x_1, x_2) \in \mathbb{A}^2 : x_1 \cdot x_2 = 0\}$ y $\phi : \mathcal{M} \to \mathbb{A}^1$ la aplicación total definida por*

$$\phi(x_1, x_2) := \begin{cases} \dfrac{x_1}{x_1 + x_2}, & \text{para } (x_1, x_2) \neq (0, 0); \\ 0, & \text{para } (x_1, x_2) = (0, 0). \end{cases}$$

Sean $\mathbf{0} := (0, 0)$ y $U := \mathcal{M} \setminus \{\mathbf{0}\}$. Es claro que ϕ es una aplicación construible, U es un subconjunto abierto y denso Zariski de $\mathcal{M}$ y la restricción $\phi|_U$ de ϕ a U es una aplicación racional de $\mathcal{M}$. Afirmamos que el gráfico $\mathcal{G}$ de ϕ está contenido en la clausura Zariski del gráfico $\mathcal{G}_U$ de $\phi|_U$. En efecto, puesto que $\mathcal{G}_U$ es un conjunto construible, la clausura Zariski de $\mathcal{G}_U$ es igual a la clausura fuerte de $\mathcal{G}_U$. Por lo tanto, para probar nuestra afirmación es suficiente probar que el gráfico $\mathcal{G}$ de ϕ está contenido en la clausura fuerte de $\mathcal{G}_U$. Por definición, el conjunto construible $\mathcal{G} \setminus \mathcal{G}_U$ consiste sólo del punto $(\mathbf{0}, 0)$. No obstante, $(\mathbf{0}, 0)$ pertenece a la clausura fuerte de $\mathcal{G}_U$, puesto que este punto es el límite de la sucesión $\left(x^{(k)}, \phi|_U(x^{(k)})\right)_{k \in \mathbb{N}}$ de $\mathcal{G}_U$ definida por $x^{(k)} := (0, 1/k)$ para todo $k \in \mathbb{N}$. Esto termina la demostración de nuestra afirmación y prueba que la aplicación ϕ es débilmente continua.

Ahora probamos que ϕ es topológicamente robusta. Con este propósito, observamos que $\phi(x_1, 0) = 1$ para todo $x_1 \in \mathbb{A}^1 \setminus \{0\}$ y $\phi(0, x_2) = 0$ para todo $x_2 \in \mathbb{A}^1$. Esto prueba que la aplicación ϕ es acotada. En consecuencia ϕ satisface la condición (iii) y por lo tanto ϕ es topológicamente robusta.

Finalmente, probamos que ϕ no es fuertemente continua. Sea $(x^{(k)})_{k \in \mathbb{N}}$ la sucesión de $\mathcal{M}$ definida por $x^{(k)} := (1/k, 0)$ para todo $k \in \mathbb{N}$. Entonces es fácil ver que

$$\lim_{k \to \infty} x^{(k)} = \mathbf{0} \in \mathcal{M} \;\; y \;\; \lim_{k \to \infty} \phi(x^{(k)}) = 1 \neq \phi(\mathbf{0}).$$

Esto prueba que ϕ no es fuertemente continua.

Si la aplicación construible $\phi : \mathcal{M} \to \mathbb{A}^m$ es débilmente continua, no hay garantía de que la restricción de ϕ a un subconjunto construible arbitrario de $\mathcal{M}$ sea también débilmente continua, como se muestra en el siguiente ejemplo. En consecuencia es posible que las restricciones de aplicaciones topológicamente robustas a subconjuntos construibles de sus dominios no sean topológicamente robustas. Si la aplicación $\phi : \mathcal{M} \to \mathbb{A}^m$ es polinomial, entonces ϕ es fuertemente continua (y por lo tanto, por el Lema 9.1.4, débilmente continua, topológicamente robusta y hereditaria).

Ejemplo 9.1.6. *Considérese de nuevo el conjunto construible $\mathcal{M} \subset \mathbb{A}^2$ y la aplicación total $\phi : \mathcal{M} \to \mathbb{A}^1$ del Ejemplo 9.1.5, a saber, $\mathcal{M} := \{(x_1, x_2) \in \mathbb{A}^2 : x_1 \cdot x_2 = 0\}$ y*

$$\phi(x_1, x_2) := \begin{cases} \dfrac{x_1}{x_1 + x_2}, & \text{para } (x_1, x_2) \neq (0, 0); \\ 0, & \text{para } (x_1, x_2) = (0, 0). \end{cases}$$

Entonces la restricción $\phi|_{\mathcal{N}} : \mathcal{N} \to \mathbb{A}^1$ al subconjunto construible $\mathcal{N} := \{(x_1, 0) \in \mathbb{A}^2 : x_1 \in \mathbb{A}^1\}$ de $\mathcal{M}$ no es débilmente continua. En particular, ϕ no es hereditaria.

El concepto de hereditariedad suena más bien abstracto y axiomático. Lo necesitaremos en lo que sigue para una formulación matemática correcta y completa de nuestro modelo algorítmico. En el Capítulo 10 estableceremos una condición algorítmicamente significativa que implica la hereditariedad de aplicaciones topológicamente robustas adecuadas (ver la Definición 10.2.7, la Proposición 10.2.9 y el Corolario 10.2.11 más abajo).

9.2. Un modelo computacional para la interpolación de Hermite–Lagrange

Sean n, D, K, L, M y N seis parámetros discretos pertenecientes a $\mathbb{N}$. Sea $\boldsymbol{X} := (X_1, \ldots, X_n)$, donde $X_1, \ldots, X_n$ son indeterminadas sobre $\mathbb{C}$, y denótese por Π (o, más precisamente, por $\Pi^{(n)}$) el anillo de polinomios $\mathbb{C}[\boldsymbol{X}] := \mathbb{C}[X_1, \ldots, X_n]$ y por Π_D (o por $\Pi_D^{(n)}$) el $\mathbb{C}$–espacio vectorial de los polinomios de Π de grado a lo sumo D.

En lo que sigue nos ocuparemos de familias discretas (dependiendo de algunos o de todos los parámetros n, D, K, L, M y N) de problemas y algoritmos de interpolación de Hermite–Lagrange. Antes de introducir un modelo general de computación que contiene estos dos conceptos vamos a discutirlos en el contexto más intuitivo de interpolación de Lagrange.

9.2.1. Revisión de la interpolación de Lagrange

Problemas de interpolación de Lagrange

Informalmente, un problema de interpolación de Lagrange está determinado por una clase $\mathcal{D}$ de **datos de interpolación** y una clase $\mathcal{O}$ de **interpolantes**. En lo que sigue pensaremos que para parámetros fijos n, D y K las clases $\mathcal{D}$, $\mathcal{O}$ y la relación entre ellas se realiza por medio de las siguientes estructuras matemáticas:

- La clase $\mathcal{D}$ es un subconjunto construible del espacio ambiente afín $\mathbb{A}^{(n+1)\times K}$ que consiste de K–tuplas $((x_1, y_1), \ldots, (x_K, y_K))$ de nodos $x_i \in \mathbb{A}^n$ y valores $y_i \in \mathbb{C}$, $1 \leq i \leq K$, tales que $x_i \neq x_j$ para toda elección de índices $1 \leq i < j \leq K$.

- La clase $\mathcal{O}$ es un subconjunto construible del espacio vectorial de dimensión finita Π_D, tal que para todo dato de interpolación $d := ((x_1, y_1), \ldots, (x_K, y_K))$ perteneciente a $\mathcal{D}$ existe exactamente un interpolante $f \in \mathcal{O}$ que resuelve el problema de interpolación de Lagrange para d, i.e., que satisface la condición $f(x_i) = y_i$ para $1 \leq i \leq K$.

- Existe una aplicación construible $\Phi : \mathcal{D} \to \Pi_D$ cuya imagen está contenida en $\mathcal{O}$ y que asocia a cada dato de interpolación $d \in \mathcal{D}$ el interpolante $\Phi(d)$.

En el contexto de la interpolación de Lagrange clásica, la clase de interpolantes $\mathcal{O}$ es siempre un subespacio de dimensión finita del anillo de polinomios Π (y por lo

tanto contenido en Π_D para algún D) y $\mathcal{D}$ es usualmente un subconjunto construible, denso Zariski de $\mathbb{A}^{(n+1)\times K}$. En lo que sigue, la clase $\mathcal{O}$ puede tener una estructura geométrica no lineal; por ejemplo, $\mathcal{O}$ puede ser una subvariedad algebraica de grado más alto del espacio afín Π_D. A su vez, los datos de interpolación pueden ser interdependientes, esto es, $\mathcal{D}$ puede estar contenido en una subvariedad algebraica propia de $\mathbb{A}^{(n+1)\times K}$.

En la teoría clásica de interpolación uno desearía que toda sucesión convergente de interpolantes de Lagrange convergiera a un interpolante de Hermite. Desafortunadamente esto no es cierto en general. En consecuencia requeriremos que la aplicación Φ satisfaga una condición de coalescencia más modesta, aunque muy natural, que puede parafrasearse como un tipo débil de "continuidad" de Φ con respecto a las topologías Euclídeas de $\mathcal{D}$ y $\mathcal{O}$. La aplicación Φ establece una cierta interdependencia entre los datos de interpolación de $\mathcal{D}$ y los interpolantes de $\mathcal{O}$. También requeriremos que las características esenciales (topológicas o geométricas) de esta interdependencia se preserven cuando restringimos la clase $\mathcal{D}$ a un subconjunto construible arbitrario. En términos más técnicos podemos pensar que $\Phi : \mathcal{D} \to \Pi_D$ es una aplicación construible, topológicamente robusta y hereditaria en el sentido de la Sección 9.1. Si este es el caso, Φ seguramente satisface nuestros requerimientos (informales). Está de más decir que en la teoría clásica de interpolación de Lagrange la aplicación que corresponde a Φ es siempre fuertemente continua (y por lo tanto, por el Lema 9.1.4, topológicamete robusta y hereditaria).

Ésta es entonces la manera en que vamos a formalizar la noción de un **problema de interpolación de Lagrange**, a saber, por un subconjunto construible $\mathcal{D}$ de un espacio afín $\mathbb{A}^{(n+1)\times K}$, que representa como arriba los datos de interpolación del problema, y por una aplicación topológicamente robusta y hereditaria $\Phi : \mathcal{D} \to \Pi_D$, que para todo $d := ((x_1, y_1), \ldots, (x_K, y_K))$ perteneciente a $\mathcal{D}$ satisface la condición $\Phi(d)(x_i) = y_i$ para $1 \leq i \leq K$.

Algoritmos de interpolación de Lagrange

Para desarrollar nuestro modelo para el concepto informal de familia de problemas de interpolación de Lagrange, sólo hacemos referencia a estructuras matemáticas "objetivas", como datos de interpolación, interpolantes y la aplicación Φ. Siguiendo la terminología de [CGH$^+$03] los elementos de $\mathcal{D}$, interpretados como datos de interpolación, pueden considerarse como **objetos de entrada** y los elementos de $\mathcal{O}$ como **objetos de salida** los cuales resultan relacionados por la aplicación (matemática) Φ. Sin embargo esto no es suficiente, ya que para la modelización del concepto de algoritmo de interpolación de Lagrange, necesitamos tratar con estructuras de datos que representen los objetos de entrada y salida.

Como se mencionó en la Sección 1.2.3, una característica particular de la interpolación de Lagrange (y también de Hermite) consiste en la identificación del concepto de objeto de entrada y el código que lo representa. Por lo tanto el subconjunto construible $\mathcal{D}$ de $\mathbb{A}^{(n+1)\times K}$ no sólo tiene que ser considerado como un conjunto de datos de interpolación (objetivos), sino también, y simultáneamente, como una **estructura de datos** que contiene los **códigos de entrada** (o **representaciones**)

que codifican los datos de interpolación. Esto no es otra cosa que una interpretación de la ciencia computacional de algo que ya es habitual en teoría de interpolación. Por lo tanto, en el contexto de este trabajo, el dato de interpolación y el código de entrada son nociones que reflejan distintos aspectos del mismo objeto matemático.

Sin embargo nuestro punto de vista difiere del estándar con respecto a los interpolantes y sus representaciones, puesto que nosotros no fijamos de antemano la **estructura de datos de salida**, digamos $\mathcal{D}^*$, que codifica la clase de objetos de salida $\mathcal{O}$ definida por los interpolantes. En el contexto de la interpolación de Lagrange (y de Hermite) clásica, $\mathcal{D}^*$ es siempre la representación densa (o convenientemente rala) de los interpolantes por sus coeficientes. En el presente trabajo deseamos admitir como $\mathcal{D}^*$ estructuras de datos más generales como, por ejemplo, el dominio de instancias de una representación adecuada de los interpolantes por straight–line programs. Para explicar nuestro punto de vista vamos a analizar la relación entre la interpolación de Lagrange y la representación de polinomios por straight–line programs en más detalle.

Ahora fijamos los parámetros n y L. Sea $D := 2^L$, $K := 4(L+n+1)^2+2$, $M := (L+n+1)^2$, y sea $\mathcal{O}$ el subconjunto de los polinomios de $\Pi^{(n)}$ que se pueden representar por un straight–line program sin divisiones de longitud no escalar L. A partir de [BCS97, Exercise 9.18] deducimos que $\mathcal{O}$ es un subconjunto construible del espacio vectorial de dimensión finita $\Pi_D = \Pi_D^{(n)}$. Además, puesto que $M = (L+n+1)^2$, existe un straight–line program sin divisiones fijo β de longitud no escalar L en M parámetros **genéricos** (también llamado un **esquema de computación** de longitud no escalar L) con la siguiente propiedad:
Para todo polinomio $f \in \mathcal{O}$ existe una instancia $z \in \mathbb{A}^M$ tal que la especialización $\beta(z)$ de β en z es un straight–line program de longitud no escalar L (con parámetros complejos z) que codifica el polinomio f. Considerando $\mathcal{O}$ como un subconjunto (construible) del espacio vectorial de dimensión finita Π_D, podemos describir esta codificación por una aplicación **polinomial** (esto es, un morfismo de variedades afines) $\omega^* : \mathbb{A}^M \to \Pi_D$. En particular tenemos que $\omega^*(z) = f$. Obsérvese que la imagen de ω^* es $\mathcal{O}$, por lo tanto $\mathcal{O}$ es irreducible.

Supóngase dados puntos $\gamma_1, \ldots, \gamma_K$ de $\mathbb{A}^n$ distintos dos a dos y un subconjunto construible $\mathcal{D}$ de $\mathbb{A}^K$ tales que para $\gamma := (\gamma_1, \ldots, \gamma_K)$ el conjunto $\mathcal{D}_\gamma := \{((\gamma_1, y_1), \ldots, (\gamma_K, y_K)) : (y_1, \ldots, y_K) \in \mathcal{D}\}$ representa los datos de interpolación de un problema de interpolación de Lagrange para la clase de interpolantes $\mathcal{O}$. De acuerdo con nuestros comentarios en la Sección 9.2.1, este problema de interpolación de Lagrange podría modelizarse por una aplicación topológicamente robusta y hereditaria $\Phi : \mathcal{D} \to \Pi_D$ con imagen $\mathcal{O}$. Por lo tanto $\mathcal{D}$ y Φ describen un problema de interpolación de Lagrange. En la Sección 9.2.3, usando la hipótesis $K = 4(L+n+1)^2+2$, exhibiremos un ejemplo concreto de esta situación.

La tarea algorítmica es ahora **calcular** (de manera uniforme y determinística), para cada código de entrada $d \in \mathcal{D}$, un código de salida, digamos $\Psi(d)$, que pertenece a $\mathbb{A}^M$ y que representa el interpolante $\Phi(d)$ de la siguiente manera: $\Psi(d)$ es una instancia del esquema de computación β que satisface la condición $\omega^*(\Psi(d)) = \Phi(d)$. En consecuencia, modelizamos la noción de algoritmo de interpolación de Lagrange usando una aplicación (total) $\Psi : \mathcal{D} \to \mathbb{A}^M$ que tiene que satisfacer ciertas

condiciones que vamos a explicar a continuación.

Sea $\mathcal{D}^*$ un subconjunto construible de $\mathbb{A}^M$ con $\omega^*(\mathcal{D}^*) = \mathcal{O}$. Para simplificar la notación también escribiremos $\omega^* : \mathcal{D}^* \to \Pi_D$ para la restricción de $\omega^* : \mathbb{A}^M \to \Pi_D$ a $\mathcal{D}^*$. Consideramos $\mathcal{D}^*$ como la estructura de datos de salida y ω^* como la codificación de los objetos de salida del algoritmo de interpolación representado por la aplicación Ψ. Consecuentemente requerimos que Ψ aplique $\mathcal{D}$ en $\mathcal{D}^*$.

Además deseamos que Ψ sea en algún sentido "computable" y que Ψ permanezca "computable" si la restringimos a un subconjunto construible arbitrario de $\mathcal{D}$, de acuerdo con el requerimiento anterior sobre el problema de interpolación Φ. Puesto que una aplicación racional se puede considerar como "computable sólo en entradas genéricas", requerimos que Ψ sea hereditaria.

Esta condición es muy débil, puesto que incluye el caso en que el algoritmo de interpolación de Lagrange detrás de la aplicación Ψ se implementa por un programa de computación que contiene ramificaciones. Un caso típico de un algoritmo libre de ramificaciones podría aparecer si Ψ fuera una aplicación **polinomial**. Sin embargo, a partir del Teorema 11.2.1 más abajo deducimos que no existe una aplicación polinomial $\Psi : \mathcal{D} \to \mathcal{D}^*$ tal que, para $M \leq 2^{c\sqrt{K}}$, donde $c > 0$ es una constante universal, el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathcal{D} & \xrightarrow{\Psi} & \mathcal{D}^* \\ & \searrow^{\Phi} & \downarrow{\scriptstyle \omega^*} \\ & & \Pi_D^{(n)} \end{array} \tag{9.1}$$

De hecho, el Teorema 11.2.1 hace la misma afirmación para una clase de aplicaciones Ψ topológicamente robustas y hereditarias mucho más amplia, a saber para la clase de aplicaciones geométricamente robustas que serán introducidas en la Sección 10.2.

Los datos $\mathcal{D}^*$, ω^* y Ψ determinan ahora un **algoritmo de interpolación** que resuelve el problema de interpolación dado por Φ.

Nuestro interés por la codificación de polinomios por straight–line programs está motivado por el hecho de que existen ejemplos computacionalmente relevantes de polinomios de grado alto como $(1+T)^{2^L}$ o $\sum_{0\leq j\leq 2^L} T^j$ que pueden ser evaluados usando sólo unas pocas operaciones aritméticas, a saber $\mathcal{O}(L)$, mientras que existen otros ejemplos de gran interés, como el polinomio de Pochhammer–Wilkinson $\prod_{0\leq j\leq 2^L}(T-j)$ o el polinomio $\sum_{0\leq j\leq 2^L} T^j/j$, cuyo estatus de complejidad es desconocido (aquí T denota una nueva indeterminada). Por otra parte, los polinomios (multivariados) que aparecen como productos secundarios o finales de procesos de eliminación en geometría algebraica y semialgebraica efectiva pueden codificarse por straight–line programs cuya longitud es **polinomial** en el grado de estos polinomios. Esto implica en casos típicos una mejora exponencial de la estructura de datos con respecto a las estructuras de datos clásicas, a saber la codificación densa (o rala) de polinomios.

Se podría plantear la cuestión de si tales polinomios de eliminación admiten también codificaciones por straight–line program cuya longitud es **polilogarítmica** en el grado del polinomio dado. La respuesta esperada es no, ya que si no, tendríamos

$P = NP$ en el modelo de complejidad BSS sobre los números reales o complejos (ver, por ejemplo, [BSS89], [BCSS96], [BCSS98] y [HM93] para más detalles).

Si el concepto de "eliminación polinomial"se interpreta de una manera más abarcativa, a saber, más allá de los ejemplos clásicos de las resultantes, entonces se puede incluso **probar** que los procedimientos de eliminación generales no siempre son capaces de producir representaciones polilogarítmicas por straight–line programs para sus polinomios de salida, a menos que estos procedimientos introduzcan ramificaciones arbitrarias y no controladas (ver [GH01] y [CGH$^+$03]).

9.2.2. El modelo general

Ahora estamos en condiciones de describir el anunciado modelo de computación que incluye también la interpolación de Hermite. Reemplazando en la discusión anterior sobre la interpolación de Lagrange la cantidad $(n+1)K$ (o K) por el parámetro N, llegamos a la siguiente formulación:

Definición 9.2.1. *Sean n, D, M y N números naturales fijos. Decimos que un* ***problema de interpolación*** *de Hermite–Lagrange está* ***determinado*** *por un subconjunto construible $\mathcal{D}$ del espacio afín $\mathbb{A}^N$, actuando como estructura de datos de entrada, y una aplicación topológicamente robusta y hereditaria $\Phi : \mathcal{D} \to \Pi_D^{(n)}$.*

Además decimos que un ***algoritmo de interpolación*** *de Hermite–Lagrange (que resuelve el problema de interpolación dado) está* ***determinado*** *por un subconjunto construible $\mathcal{D}^*$ del espacio afín $\mathbb{A}^M$, actuando como estructura de datos de salida, una codificación polinomial $\omega^* : \mathcal{D}^* \to \Pi_D^{(n)}$ de los objetos de salida y una aplicación hereditaria $\Psi : \mathcal{D} \to \mathcal{D}^*$, es decir, el algoritmo en un sentido restringido, tal que el diagrama (9.1) conmuta.*

Por supuesto, este modelo captura situaciones mucho más generales que la interpolación de Hermite–Lagrange en el sentido intuitivo usual. No obstante, el modelo representa todo lo que necesitamos para nuestra discusión matemática sobre la complejidad de la interpolación polinomial. En particular no habrá necesidad de modelizar **exactamente** la noción informal de la interpolación de Hermite–Lagrange.

9.2.3. Tres familias críticas de ejemplos

El propósito de esta sección es ilustrar las nociones de las secciones anteriores por medio de tres familias significativas de problemas de interpolación. Estas familias constituyen nuestros ejemplos prototípicos, y serán más extensamente discutidas en la Sección 10.3 y en el Capítulo 11.

Las primeras dos familias proceden de la interpolación de Lagrange univariada estándar. Sus estructuras de datos de entrada son subconjuntos abiertos Zariski (no vacíos) de espacios afines y por lo tanto variedades suaves. Luego analizamos dos casos de interpolación de Hermite–Lagrange multivariada sobre curvas **singulares**. Nuestro último ejemplo es el de un problema de interpolación **no lineal**, es decir, el conjunto de interpolantes no es un subespacio lineal, sino un conjunto construible del correspondiente espacio ambiente afín.

Interpolación de Lagrange univariada

En términos de las notaciones introducidas anteriormente, sea $K \geq 2$ un número natural, $n := 1$, $D := K - 1$, $M := K$, $N := 2K$, $\boldsymbol{X} := X_1$ y $\Pi_D := \Pi_D^{(1)}$.

Interpolación de Lagrange en nodos fijos. Fíjese un punto arbitrario $\boldsymbol{\gamma} := (\gamma_1, \ldots, \gamma_K) \in \mathbb{A}^K$ con $\gamma_i \neq \gamma_j$ para $1 \leq i < j \leq K$. El problema de interpolación de Lagrange univariado (genérico) en los nodos (fijos) $\gamma_1, \ldots, \gamma_K$ consiste en hallar, para todo $\boldsymbol{y} := (y_1, \ldots, y_K) \in \mathbb{A}^K$, el (único) polinomio $f_{\boldsymbol{\gamma},\boldsymbol{y}} \in \Pi_D$ que satisface la condición

$$f_{\boldsymbol{\gamma},\boldsymbol{y}}(\gamma_j) = y_j \quad \text{para } 1 \leq j \leq K. \tag{9.2}$$

Sea $\mathcal{D}_{\boldsymbol{\gamma}}$ el subconjunto construible $\mathcal{D}_{\boldsymbol{\gamma}} := \{\gamma_1\} \times \mathbb{A}^1 \times \cdots \times \{\gamma_K\} \times \mathbb{A}^1$ de $\mathbb{A}^N$. Entonces el **problema de interpolación de Lagrange univariado en nodos fijos** $\gamma_1, \ldots, \gamma_K$ está representado por la aplicación $\Phi_{\boldsymbol{\gamma}} : \mathcal{D}_{\boldsymbol{\gamma}} \to \Pi_D$ que asocia a cada $d := (\gamma_1, y_1, \ldots, \gamma_K, y_K) \in \mathcal{D}_\gamma$ el único polinomio $f_d := f_{\boldsymbol{\gamma},\boldsymbol{y}}$ de Π_D determinado por la condición (9.2). Puesto que $\Phi_{\boldsymbol{\gamma}}$ es una aplicación polinomial, concluimos que $\mathcal{D}_{\boldsymbol{\gamma}}$ y $\Phi_{\boldsymbol{\gamma}}$ determinan un problema de interpolación de Lagrange en el sentido de la Definición 9.2.1.

Sea $\mathcal{D}^* := \mathbb{A}^M$ y sea $\omega^* : \mathcal{D}^* \to \Pi_D$ la codificación de los elementos de Π_D por su representación densa, esto es, $\omega^*(a_0, \ldots, a_{K-1}) := \sum_{j=0}^{K-1} a_j X^j$ para $(a_0, \ldots, a_{K-1}) \in \mathcal{D}^*$. Sabemos que para cada $d := \big((\gamma_1, y_1), \ldots, (\gamma_K, y_K)\big) \in \mathcal{D}_\gamma$ con $\boldsymbol{y} := (y_1, \ldots, y_K)$, la representación densa de $f_d \in \Pi_D$ está dada por $V_\gamma^{-1}\boldsymbol{y}$, donde $V_{\boldsymbol{\gamma}} := (\gamma_i^{j-1})_{1 \leq i,j \leq K} \in \mathbb{A}^{K \times K}$ es la matriz de Vandermonde asociada a $\boldsymbol{\gamma}$. Por lo tanto, la aplicación polinomial $\Psi_\gamma : \mathcal{D}_\gamma \to \mathcal{D}^*$ definida por $\Psi_{\boldsymbol{\gamma}}(d) := V_{\boldsymbol{\gamma}}^{-1}\boldsymbol{y}$ determina un algoritmo en el sentido de la Definición 9.2.1 que resuelve el problema de interpolación de Lagrange dado por $\mathcal{D}_{\boldsymbol{\gamma}}$ y $\Phi_{\boldsymbol{\gamma}}$.

Interpolación de Lagrange en nodos genéricos. La construcción anterior se puede modificar fácilmente para modelizar también la interpolación de Lagrange univariada clásica en nodos genéricos. Con las notaciones anteriores, sea $\mathcal{U}$ el subconjunto abierto Zariski de $\mathbb{A}^K$ definido por $\mathcal{U} := \{(\gamma_1, \ldots, \gamma_K) \in \mathbb{A}^K : \gamma_i \neq \gamma_j \text{ para } 1 \leq i < j \leq K\}$ y sea $\mathcal{D}$ el subconjunto construible de $\mathbb{A}^N$ definido por $\mathcal{D} := \mathcal{U} \times \mathbb{A}^K$. Para todo $d := (\boldsymbol{\gamma}, \boldsymbol{y}) \in \mathcal{D}$ denotamos por f_d el único polinomio de Π_D determinado por la condición (9.2). Entonces el **problema de interpolación de Lagrange univariado genérico** está representado por $\mathcal{D}$ y la aplicación racional regular (esto es, bien definida en todo $\mathcal{D}$) $\Phi : \mathcal{D} \to \Pi_D$ que asocia a cada $d \in \mathcal{D}$ el polinomio $f_d \in \Pi_D$. Esto implica que Φ es fuertemente continua (por lo tanto topológicamente robusta y hereditaria). Concluimos que $\mathcal{D}$ y Φ determinan un problema de interpolación de Lagrange en el sentido de la Definición 9.2.1. Puesto que la representación densa de f_d con $d = (\boldsymbol{\gamma}, \boldsymbol{y}) \in \mathcal{D}$ está dada por el vector $V_{\boldsymbol{\gamma}}^{-1}\boldsymbol{y}$, vemos que para $\mathcal{D}^* := \mathbb{A}^M$, la codificación $\omega^* : \mathcal{D}^* \to \Pi_D$ definida por $\omega^*(a_0, \ldots, a_{K-1}) := \sum_{j=0}^{K-1} a_i X^i$, y la aplicación racional regular $\Psi : \mathcal{D} \to \mathcal{D}^*$ definida por $\Psi(d) := V_{\boldsymbol{\gamma}}^{-1}\boldsymbol{y}$, determinan un algoritmo en el sentido de la Definición

9.2.1 que resuelve el problema de interpolación dado por $\mathcal{D}$ y Φ, puesto que Ψ es hereditaria.

Interpolación de Hermite–Lagrange bivariada sobre curvas singulares

Sean X_1, X_2 indeterminadas sobre $\mathbb{C}$ y sea $\Pi^{(2)} := \mathbb{C}[X_1, X_2]$. En esta sección consideramos dos ejemplos de interpolación de Hermite–Lagrange bivariada definidos sobre un subconjunto abierto Zariski $\mathcal{D}$ de una curva singular $\mathcal{C} \subset \mathbb{A}^2$. En el primer ejemplo el problema de interpolación está determinado por una aplicación fuertemente continua $\Phi : \mathcal{D} \to \Pi_1^{(2)}$, mientras que en el segundo ejemplo el problema está determinado por una aplicación topológicamente robusta y hereditaria $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ que no es fuertemente continua.

Interpolación sobre la curva $X_1^3 - X_2^2 = 0$. Consideramos la curva algebraica irreducible $\mathcal{C}$ de $\mathbb{A}^2$ definida por la ecuación $X_1^3 - X_2^2 = 0$, que contiene el subconjunto abierto Zariski no vacío $\mathcal{D} := \mathcal{C} \setminus \{(-1, \pm i)\}$. Sea $f : \mathbb{A}^2 \to \mathbb{A}^1$ una aplicación polinomial. Es claro que la restricción $f|_{\mathcal{D}}$ de f a $\mathcal{D}$ is topológicamente robusta y hereditaria. Obsérvese que el punto $\mathbf{0} := (0, 0)$ pertenece a $\mathcal{D}$. Consideramos el problema de interpolar f a partir de los valores $f(d)$ $(d \in \mathcal{D})$ y $f(\mathbf{0})$ por medio de polinomios de $\Pi_1^{(2)}$.

Obsérvese que para todo punto $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$ existe un único polinomio g_d del subespacio lineal $E_d := \mathbb{C} + \mathbb{C} \cdot (d_1 X_1 + d_2 X_2)$ de $\Pi_1^{(2)}$ que satisface la condición $g_d(d) = f(d)$ y $g_d(\mathbf{0}) = f(\mathbf{0})$. Teniendo en cuenta que $d_1^2 + d_2^2 \neq 0$, el polinomio g_d se puede escribir como

$$g_d := f(\mathbf{0}) + \frac{\big(f(d) - f(\mathbf{0})\big)d_1}{d_1^2 + d_2^2} X_1 + \frac{\big(f(d) - f(\mathbf{0})\big)d_2}{d_1^2 + d_2^2} X_2.$$

El espacio $\mathbb{C}$–lineal de los interpolantes E_d representa el **espacio solución mínimo** (*"least solution space"*) introducido en [dBR92] (ver también [dBR90]).

Finalmente, definimos $g_{\mathbf{0}}$ como el único polinomio del subespacio $\mathbb{C}$–lineal $\mathbb{C} + \mathbb{C} \cdot X_1$ de $\Pi_1^{(2)}$ que interpola f y su derivada parcial $\partial f / \partial X_1$ en el punto $\mathbf{0} \in \mathbb{A}^2$, a saber,

$$g_{\mathbf{0}} := f(\mathbf{0}) + \frac{\partial f}{\partial X_1}(\mathbf{0}) X_1.$$

Por lo tanto tenemos $g_{\mathbf{0}}(\mathbf{0}) = f(\mathbf{0})$ y $(\partial g_{\mathbf{0}} / \partial X_1)(\mathbf{0}) = (\partial f / \partial X_1)(\mathbf{0})$.

Se ve fácilmente que la aplicación $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ definida por $\Phi(d) := g_d$ es construible y que $\Phi|_{\mathcal{D} \setminus \{\mathbf{0}\}}$ es una aplicación racional de $\mathcal{D}$, regular en $\mathcal{D} \setminus \{\mathbf{0}\}$.

Afirmamos que Φ es fuertemente continua (y por lo tanto, topológicamente robusta y hereditaria). Para verlo, es suficiente mostrar que, para toda sucesión $(d^{(k)})_{k \in \mathbb{N}}$ de $\mathcal{D} \setminus \{\mathbf{0}\}$ que converge a $\mathbf{0}$, la sucesión $(\Phi(d^{(k)}))_{k \in \mathbb{N}}$ converge a $\Phi(\mathbf{0})$.

Fíjese $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$. Luego tenemos $d_1^3 = d_2^2$, $d_1 \neq 0$, $d_1^2 + d_2^2 \neq 0$ y $(d_2/d_1)^2 = d_1$. Esto implica

$$\frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2} = \frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2(1 + d_1)} = \frac{f(d) - f(\mathbf{0})}{d_1} \frac{1}{1 + d_1} \tag{9.3}$$

y

$$\frac{(f(d)-f(\mathbf{0}))d_2}{d_1^2+d_2^2} = \frac{(f(d)-f(\mathbf{0}))d_2}{d_1^2(1+d_1)} = \frac{f(d)-f(\mathbf{0})}{d_1}\frac{d_2}{d_1}\frac{1}{1+d_1}. \tag{9.4}$$

Considerando el desarrollo de Taylor de f en $\mathbf{0}$, concluimos que existen polinomios Q_1, Q_2 de $\Pi^{(2)}$ con $Q_1(\mathbf{0}) = Q_2(\mathbf{0}) = 0$ tales que

$$f(d) - f(\mathbf{0}) = \left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + Q_1(d)\right)d_1 + \left(\frac{\partial f}{\partial X_2}(\mathbf{0}) + Q_2(d)\right)d_2.$$

Sea $(d^{(k)})_{k\in\mathbb{N}}$ una sucesión de $\mathcal{D}\setminus\{\mathbf{0}\}$ que converge a $\mathbf{0}\in\mathcal{D}$. Puesto que $(d_2^{(k)}/d_1^{(k)})^2 = d_1^{(k)}$ vale para todo $k\in\mathbb{N}$, concluimos que

$$\lim_{k\to\infty}\frac{f(d^{(k)})-f(\mathbf{0})}{d_1^{(k)}} = \lim_{k\to\infty}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + Q_1(d^{(k)}) + \left(\frac{\partial f}{\partial X_2}(\mathbf{0}) + Q_2(d^{(k)})\right)\frac{d_2^{(k)}}{d_1^{(k)}}\right) = \frac{\partial f}{\partial X_1}(\mathbf{0}).$$

Combinando esta identidad con (9.3) y (9.4) deducimos que Φ es fuertemente continua.

Por lo tanto $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ determina un problema de interpolación de Hermite–Lagrange en el sentido de la Definición 9.2.1.

Ahora sea $\mathcal{D}^* := \mathbb{A}^3$ y considérese la representación densa canónica ω^* de los polinomios bivariados sobre $\mathbb{C}$ de grados a lo sumo uno como la codificación de la salida. Más precisamente, definimos $\omega^* : \mathcal{D}^* \to \Pi_1^{(2)}$ por $\omega^*(a_0, a_1, a_2) := a_0 + a_1X_1 + a_2X_2$. Además, sea $\Psi : \mathcal{D} \to \mathcal{D}^*$ la aplicación construible definida como

$$\Psi(d) := \begin{cases} \left(f(\mathbf{0}), \dfrac{(f(d)-f(\mathbf{0}))d_1}{d_1^2+d_2^2}, \dfrac{(f(d)-f(\mathbf{0}))d_2}{d_1^2+d_2^2}\right), & \text{para } d := (d_1, d_2) \neq \mathbf{0}; \\ \left(f(\mathbf{0}), \dfrac{\partial f}{\partial X_1}(\mathbf{0}), 0\right), & \text{para } d = \mathbf{0}. \end{cases}$$

Entonces Ψ es una aplicación fuertemente continua que resuelve el problema de Hermite–Lagrange determinado por Φ.

Interpolación sobre la curva $X_2^2 = X_1^2 + X_1^3$. Consideramos ahora la curva algebraica irreducible $\mathcal{C}$ de $\mathbb{A}^2$ definida por la ecuación $X_2^2 = X_1^2 + X_1^3$, que contiene el subconjunto abierto Zariski no vacío $\mathcal{D} := \mathcal{C}\setminus\{(-2, \pm 2i)\}$. Nuevamente sea $f : \mathbb{A}^2 \to \mathbb{A}^1$ una aplicación polinomial. Es claro que la restricción $f|_{\mathcal{D}}$ de f a $\mathcal{D}$ es topológicamente robusta y hereditaria. Obsérvese que $\mathbf{0} := (0, 0)$ pertenece a $\mathcal{D}$.

Consideramos ahora el problema de interpolar f a partir de los valores $f(d)$ $(d\in\mathcal{D})$ y $f(\mathbf{0})$ por medio de polinomios de $\Pi_1^{(2)}$.

Para todo punto $d := (d_1, d_2) \in \mathcal{D}\setminus\{\mathbf{0}\}$ existe un único polinomio g_d en el "espacio solución mínimo" de [dBR90], [dBR92], a saber el subespacio lineal $E_d := \mathbb{C} + \mathbb{C}\cdot(d_1X_1 + d_2X_2)$ de $\Pi_1^{(2)}$, que satisface la condición $g_d(d) = f(d)$ y $g_d(\mathbf{0}) = f(\mathbf{0})$. Puesto que $d_1^2 + d_2^2$ es distinto de cero, el polinomio g_d se puede escribir como

$$g_d := f(\mathbf{0}) + \frac{\big(f(d)-f(\mathbf{0})\big)d_1}{d_1^2+d_2^2}X_1 + \frac{\big(f(d)-f(\mathbf{0})\big)d_2}{d_1^2+d_2^2}X_2.$$

Finalmente, definimos $g_{\mathbf{0}}$ como el único polinomio del subespacio $\mathbb{C}$–lineal $\mathbb{C} + \mathbb{C} \cdot (X_1 + X_2)$ de $\Pi_1^{(2)}$ que interpola f y la suma de sus primeras derivadas parciales en $\mathbf{0}$, es decir

$$g_{\mathbf{0}} := f(\mathbf{0}) + \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right)X_1 + \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right)X_2.$$

Por lo tanto tenemos $g_{\mathbf{0}}(\mathbf{0}) = f(\mathbf{0})$ y $(\partial g_{\mathbf{0}}/\partial X_1 + \partial g_{\mathbf{0}}/\partial X_2)(\mathbf{0}) = (\partial f/\partial X_1 + \partial f/\partial X_2)(\mathbf{0})$.

Se ve fácilmente que la aplicación $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ definida por $\Phi(d) := g_d$ es construible y que $\Phi|_{\mathcal{D}\setminus\{\mathbf{0}\}}$ es una función racional de $\mathcal{D}$, regular en $\mathcal{D} \setminus \{\mathbf{0}\}$.

Afirmamos que Φ también es topológicamente robusta. Para verlo, primeramente mostramos que $\Phi(d)$ permanece acotada cuando $d \in \mathcal{D}$ se aproxima a $\mathbf{0} \in \mathcal{D}$. Sea $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$. Tenemos $d_1^2 + d_2^2 = 2d_1^2 + d_1^3$, $d_1 \neq 0$ y $d_1^2 + d_2^2 \neq 0$. Esto implica

$$\frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2} = \frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2(2 + d_1)} = \frac{f(d) - f(\mathbf{0})}{d_1}\frac{1}{2 + d_1} \tag{9.5}$$

y

$$\frac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2} = \frac{(f(d) - f(\mathbf{0}))d_2}{d_1^2(2 + d_1)} = \frac{f(d) - f(\mathbf{0})}{d_1}\frac{d_2}{d_1}\frac{1}{2 + d_1}. \tag{9.6}$$

Considerando el desarrollo de Taylor de f en $\mathbf{0}$, deducimos que existen polinomios Q_1, Q_2 de $\Pi^{(2)}$ con $Q_1(\mathbf{0}) = Q_2(\mathbf{0}) = 0$ tales que

$$f(d) - f(\mathbf{0}) = \left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + Q_1(d)\right)d_1 + \left(\frac{\partial f}{\partial X_2}(\mathbf{0}) + Q_2(d)\right)d_2. \tag{9.7}$$

Sea $(d^{(k)})_{k\in\mathbb{N}}$ una sucesión de $\mathcal{D} \setminus \{\mathbf{0}\}$ que converge a $\mathbf{0} \in \mathcal{D}$. Para todo $k \in \mathbb{N}$ tenemos

$$\frac{f(d^{(k)}) - f(\mathbf{0})}{d_1^{(k)}} = \frac{\partial f}{\partial X_1}(\mathbf{0}) + Q_1(d^{(k)}) + \left(\frac{\partial f}{\partial X_2}(\mathbf{0}) + Q_2(d^{(k)})\right)\frac{d_2^{(k)}}{d_1^{(k)}}.$$

Teniendo en cuenta que $(d_2^{(k)}/d_1^{(k)})^2 = 1 + d_1^{(k)}$ y el hecho de que Q_1, Q_2 definen funciones fuertemente continuas en un entorno de $\mathbf{0}$ concluimos que la sucesión $\big(\big(f(d^{(k)}) - f(\mathbf{0})\big)/d_1^{(k)}\big)_{k\in\mathbb{N}}$ es acotada. Combinando esta observación con (9.5) y (9.6), vemos que Φ satisface la condición (iii) de la Definición 9.1.2.

Para ver que Φ es topológicamente robusta queda probar que Φ es débilmente continua. Afirmamos que el gráfico de Φ está contenido en la clausura Zariski del gráfico de la restricción $\Phi|_U$ de Φ al subconjunto denso y abierto Zariski $U := \mathcal{D}\setminus\{\mathbf{0}\}$ de $\mathcal{D}$. En efecto, sea $(r_k)_{k\in\mathbb{N}}$ una sucesión de reales positivos que converge a $0 \in \mathbb{R}$ y sea $(s_k)_{k\in\mathbb{N}}$ la sucesión definida por $s_k := r_k\sqrt{1 + r_k}$ para todo $k \in \mathbb{N}$. Es fácil ver que $(r_k, s_k)_{k\in\mathbb{N}}$ es una sucesión de U y que $\lim_{k\to\infty} s_k/r_k = 1$. Combinando esta observación con (9.5), (9.6) y (9.7) concluimos fácilmente que

$$\lim_{k\to\infty} \Phi(r_k, s_k) = g_{\mathbf{0}}.$$

Esto muestra que el punto $(\mathbf{0}, g_{\mathbf{0}})$ pertenece a la clausura Euclídea, y por lo tanto a la clausura Zariski, del gráfico de la restricción $\Phi|_U$ de Φ a $U := \mathcal{D} \setminus \{\mathbf{0}\}$, como habíamos afirmado. Por lo tanto, Φ también satisface la condición (i) de la Definición 9.1.2. Puesto que $\mathcal{D}$ es una curva abierta irreducible, concluimos que $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ también es hereditaria.

En consecuencia Φ determina un problema de interpolación de Hermite–Lagrange en el sentido de la Definición 9.2.1.

Sea ahora $\mathcal{D}^* := \mathbb{A}^3$ y considérese la representación densa canónica $\omega^* : \mathcal{D}^* \to \Pi_1^{(2)}$, $\omega^*(a_0, a_1, a_2) := a_0 + a_1X_1 + a_2X_2$ de los polinomios bivariados sobre $\mathbb{C}$ de grados a lo sumo uno como la codificación de la salida. Además, sea $\Psi : \mathcal{D} \to \mathcal{D}^*$ la aplicación construible definida por

$$\Psi(d) := \begin{cases} \left(f(\mathbf{0}), \dfrac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2}, \dfrac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2}\right), & \text{para } d := (d_1, d_2) \neq \mathbf{0}; \\ \left(f(\mathbf{0}), \dfrac{1}{2}\Big(\dfrac{\partial f}{\partial X_1}(\mathbf{0}) + \dfrac{\partial f}{\partial X_2}(\mathbf{0})\Big), \dfrac{1}{2}\Big(\dfrac{\partial f}{\partial X_1}(\mathbf{0}) + \dfrac{\partial f}{\partial X_2}(\mathbf{0})\Big)\right), & \text{para } d = \mathbf{0}. \end{cases}$$

Entonces Ψ es una aplicación hereditaria (e incluso topológicamente robusta) que resuelve el problema de Hermite–Lagrange determinado por Φ.

Es importante observar que, en general, ni Φ ni Ψ son fuertemente continuas. De hecho, sea $(r_k)_{k\in\mathbb{N}}$ una sucesión de reales positivos que converge a $0 \in \mathbb{R}$ y sea $(s_k)_{k\in\mathbb{N}}$ la sucesión definida por $s_k := -r_k\sqrt{1 + r_k}$ para todo $k \in \mathbb{N}$. Es fácil ver que $(r_k, s_k)_{k\in\mathbb{N}}$ es una sucesión de puntos de $\mathcal{D}$ que converge a $\mathbf{0}$ y que $\lim_{k\to\infty} s_k/r_k = -1$. Combinando esta observación con (9.5), (9.6) y (9.7) concluimos fácilmente que

$$\lim_{k\to\infty} \Phi(r_k, s_k) = f(\mathbf{0}) + \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) - \frac{\partial f}{\partial X_2}(\mathbf{0})\right)X_1 + \frac{1}{2}\left(-\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right)X_2.$$

Para $(\partial f/\partial X_2)(\mathbf{0}) \neq 0$, el lado derecho de la identidad anterior no es igual a $g_{\mathbf{0}}$. Esto muestra que Φ no es fuertemente continua. Un argumento similar prueba que Ψ no es fuertemente continua.

Un ejemplo no lineal: sucesiones de identificación e interpolación

Retomamos aquí el ejemplo de la Sección 9.2.1. Sean $n, L \in \mathbb{N}$ que satisfacen la condición $2^{L/4} \geq n$ y sea $\mathcal{O}$ el subconjunto de los polinomios de $\Pi^{(n)} := \mathbb{C}[\boldsymbol{X}]$ que pueden ser evaluados por un straight–line program sin divisiones de longitud no escalar a lo sumo L.

Observamos que todo polinomio $f \in \mathcal{O}$ tiene grado acotado por 2^L. Además $\mathcal{O} \subset \Pi_{2^L}^{(n)}$, identificando cada elemento de $\mathcal{O}$ con su representación densa, y así puede considerarse como un subconjunto construible de $\mathbb{A}^{n_L}$, donde $n_L := \binom{2^L+n}{n}$ (ver [HS82, Theorem 3.2] o [BCS97, Exercise 9.18]). Obsérvese que $\mathcal{O}$ es un cono de $\mathbb{A}^{n_L}$.

Denotemos con $\overline{\mathcal{O}}$ la clausura de $\mathcal{O}$ con respecto a la topología fuerte o Zariski de $\mathbb{A}^{n_L}$. Sucede que $\overline{\mathcal{O}}$ es una variedad irreducible que forma también un cono en $\mathbb{A}^{n_L}$. Los elementos de $\overline{\mathcal{O}}$ pueden considerarse como polinomios de $\Pi_{2^L}^{(n)}$ de **complejidad aproximada** acotada por L (ver [Ald84, Lemma 2 y Satz 4]).

Sea $K := 4(L+n+1)^2+2$. De acuerdo con [CGH$^+$03, Corollary 2] (ver también [HS82, Theorem 4.4]), existen puntos enteros $\gamma_1, \ldots, \gamma_K \in \mathbb{A}^n$ de longitud bit a lo sumo $4(L+1) \leq 2\sqrt{K}$ tales que para todo $f, g \in \overline{\mathcal{O}}$ las igualdades $f(\gamma_j) = g(\gamma_j)$ para $1 \leq j \leq K$ implican $f = g$. Tal sucesión $\gamma := (\gamma_1, \ldots, \gamma_K)$ de puntos de $\mathbb{A}^n$ se llama una **sucesión de identificación** para la clase de polinomios $\overline{\mathcal{O}}$. Sea $\boldsymbol{\gamma} := (\gamma_1, \ldots, \gamma_K)$ una sucesión de identificación para $\overline{\mathcal{O}}$ y sea $\Xi : \overline{\mathcal{O}} \to \mathbb{A}^K$ la aplicación polinomial definida por

$$\Xi(f) := \big(f(\gamma_1), \ldots, f(\gamma_K)\big).$$

Sea además $N := K$ y $\mathcal{D}$ el subconjunto construible de $\mathbb{A}^N$ definido por $\mathcal{D} := \Xi(\mathcal{O})$. Entonces [CGH$^+$03, Corollary 3] implica que $\overline{\mathcal{D}}$ es un cono afín, cerrado e irreducible de $\mathbb{A}^N$ y $\Xi : \overline{\mathcal{O}} \to \overline{\mathcal{D}}$ es un morfismo finito, birracional de variedades irreducibles que es además un homeomorfismo con respecto a las topologías fuerte y de Zariski. En particular, la aplicación $\Phi := \Xi^{-1} : \mathcal{D} \to \Pi_{2^L}^{(n)}$ es construible. Asimismo, en términos de la Definición 10.2.7 de la Sección 10.2, Φ es geométricamente robusta. Por lo tanto la Proposición 10.2.9 y el Corolario 10.2.11 de la Sección 10.2 implican que Φ es topológicamente robusta y hereditaria. Por lo tanto Φ determina un problema de interpolación de Lagrange en el sentido de la Definición 9.2.1.

Obsérvese que la elección de $\boldsymbol{\gamma} := (\gamma_1, \ldots, \gamma_K)$ como una sucesión de identificación para $\overline{\mathcal{O}}$ implica que para todo punto $\boldsymbol{y} := (y_1, \ldots, y_K) \in \mathcal{D}$ existe un **único** interpolante $f \in \mathcal{O}$ que resuelve el problema de interpolación de Lagrange para el dato de interpolación $\boldsymbol{y}$. Por lo tanto el conjunto construible $\mathcal{O}$ representa la clase de objetos de salida de un problema de interpolación de Lagrange determinado por $\mathcal{D}$ y una aplicación construible bien definida $\Phi : \mathcal{D} \to \Pi_{2^L}^{(n)}$ con imagen $\mathcal{O}$. Obsérvese también que este problema de interpolación de Lagrange es **no lineal** en el sentido que el espacio de interpolantes $\mathcal{O}$ es no lineal (no es cerrado bajo adiciones).

La Sección 11.2 estará dedicada al estudio de la complejidad algorítmica de resolver este problema de interpolación particular, es decir, a la complejidad de reconstruir los polinomios de $\mathcal{O}$ a partir de sus valores en una sucesión de identificación.

9.2.4. Complejidad de problemas y algoritmos de interpolación de Hermite–Lagrange

Sean n, D y N números naturales fijos, sea $\mathcal{D}$ un subconjunto construible del espacio afín $\mathbb{A}^N$ y sea $\Phi : \mathcal{D} \to \Pi_D^{(n)}$ una aplicación topológicamente robusta y hereditaria tales que $\mathcal{D}$ y Φ determinan un problema de interpolación de Hermite–Lagrange. Llamamos a N **el tamaño de la entrada del problema de interpolación dado**.

Sea $\mathcal{D}^*$ un subconjunto construible de un espacio afín $\mathbb{A}^M$ actuando como estructura de datos de salida, $\omega^* : \mathcal{D}^* \to \Pi_D^{(n)}$ una codificación polinomial de los objetos de salida $\Phi(\mathcal{D})$ y $\Psi : \mathcal{D} \to \mathcal{D}^*$ una aplicación hereditaria tales que $\mathcal{D}^*$, ω^* y Ψ representan un algoritmo de interpolación de Hermite–Lagrange que resuelve el problema de interpolación dado. Medimos la complejidad de este algoritmo de interpolación por el tamaño de los objetos de salida, es decir, M.

La complejidad del problema de interpolación de Hermite–Lagrange determinado por $\mathcal{D}$ y Φ es el entero no negativo mínimo M tal que existe un

algoritmo de interpolación con estructura de datos de salida de tamaño M que resuelve el problema.

Por ejemplo, la complejidad del problema de interpolación de Lagrange univariado (genérico) en K nodos fijos introducido en la Sección 9.2.3 es al menos $K = N$ (compárese con la Proposición 11.1.1).

Observamos que esta noción de complejidad es una generalización de tres medidas usuales de complejidad del tamaño de los datos en teoría de eliminación efectiva: el tamaño de la representación densa o rala y la longitud (no escalar) de la representación por straight–line program de polinomios multivariados. Por ejemplo, sea $\mathcal{O}$ la clase de objetos de salida de un problema de eliminación y supóngase que los elementos de $\mathcal{O}$ tienen grados acotados. Entonces los polinomios contenidos en $\mathcal{O}$ generan un espacio ambiente $\mathbb{C}$–lineal de dimensión finita, digamos M. Por lo tanto M es una cota inferior para el tamaño de la representación densa de un elemento del "peor-caso"de $\mathcal{O}$. Esto implica que todo algoritmo que resuelve el problema de eliminación subyacente y devuelve los polinomios de salida de $\mathcal{O}$ en su representación densa, requiere al menos tiempo M.

Por otra parte, para un polinomio dado $F \in \Pi^{(n)}$ podemos considerar la longitud no escalar mínima $L(F)$ de un straight–line program sin divisiones que evalúa F. Sea $L \in \mathbb{N}$ y defínase $W_L := \{F \in \mathbb{C}[X_1, \ldots, X_n] : L(F) \leq L\}$. A partir de [BCS97, Exercise 9.18] (ver también [HS82, Theorem 3.2]) deducimos que W_L es un subconjunto construible de $\Pi^{(n)}_{2^L}$ que es la imagen de una aplicación polinomial $\mathbb{A}^{(L+n+1)^2} \to \Pi^{(n)}_{2^L}$, donde $(L+n+1)^2$ es el número de parámetros necesarios para representar los elementos de W_L como instancias de un straight–line program genérico sin divisiones de longitud no escalar L con n entradas. Por lo tanto la dimensión $(L+n+1)^2$ del espacio de parámetros $\mathbb{A}^{(L+n+1)^2}$ refleja el tamaño de los datos de la representación de los elementos de W_L por medio de straight–line programs sin divisiones. Puesto que un elemento genérico de W_L requiere una tal representación de tamaño al menos $(L+n+1)^2$, concluimos que, en el caso que W_L esté contenido en $\mathcal{O}$, la cantidad $(L+n+1)^2$ es una cota inferior para la complejidad de todo algoritmo que resuelve el problema de eliminación considerado anteriormente y devuelve los polinomios de salida de $\mathcal{O}$ en una representación por straight–line program.

Capítulo 10

Algoritmos de interpolación robustos

Esta sección está dedicada a la modelización geométrica y algebraica de los fenómenos de coalescencia (ver, por ejemplo, [BC97], [dBR92], [Olv06]) en el contexto de interpolación de Hermite–Lagrange.

El tema principal es la noción de aplicación **geométricamente robusta**, que captura simultáneamente los conceptos de robustez topológica y hereditariedad introducidos en la Sección 9.1. Esto nos permite modelizar geométrica y algebraicamente la noción intuitiva de problemas y algoritmos de interpolación límites. La noción de robustez topológica nos servirá como un paso intermedio para una mejor comprensión del concepto más bien técnico de robustez geométrica.

Con este fin comenzaremos con una caracterización algebraica de la noción de aplicación topológicamente robusta (Teorema 10.2.2 y Corolario 10.2.4). Luego introduciremos la noción de aplicación geométricamente robusta y mostraremos que tales aplicaciones son siempre hereditarias (Corolario 10.2.11). Usando el concepto de robustez geométrica de aplicaciones construibles finalmente arribaremos a la noción de problema y algoritmo de interpolación geométricamente robusto, que captura un cierto sentido de coalescencia. Esta noción se discutirá por medio de ejemplos concretos en la Sección 10.3 y el Capítulo 11 bajo los aspectos de interpolación y teoría de complejidad.

10.1. Nociones y hechos básicos de la teoría de places

Comenzamos recordando algunas definiciones y hechos básicos de la teoría de valuaciones y places (ver [ZS60] y [Lan93] para más detalles y demostraciones). Para evitar una generalidad innecesaria, limitamos nuestra exposición al contexto de $\mathbb{C}$–álgebras y cuerpos (llamamos $\mathbb{C}$–cuerpo a un cuerpo que extiende a $\mathbb{C}$).

Sean K y Ω dos $\mathbb{C}$–cuerpos. Un **place Ω–valuado** (o simplemente place) del $\mathbb{C}$–cuerpo K es un homomorfismo de anillos $\vartheta : R_\vartheta \to \Omega$ donde R_ϑ es una $\mathbb{C}$–álgebra contenida en K tal que R_ϑ y ϑ satisfacen siguiente condición:

$$x \in K \setminus R_\vartheta \text{ implica } 1/x \in R_\vartheta \text{ y } \vartheta(1/x) = 0.$$

La $\mathbb{C}$–álgebra R_ϑ con ideal maximal $\ker \vartheta$ es local, y se llama el **anillo de valuación** del place ϑ. Asociando a $x \in K \setminus R_\vartheta$ el valor "infinito" escribiremos $\vartheta(x) := \infty$. Así podemos interpretar el place ϑ como una aplicación (total) $\vartheta : K \to \Omega \cup \{\infty\}$.

Recordamos los siguientes dos resultados básicos y bien conocidos.

Theorem I (Extensión de places)**.** *([ZS60, Ch. VI, §4, Theorem 5'] y [Lan93, Ch. VII, §3, Corollary 3.3]) Sea A una $\mathbb{C}$–álgebra contenida en el cuerpo K y sea $\epsilon : A \to \Omega$ un homomorfismo de $\mathbb{C}$–álgebras de A en el $\mathbb{C}$–cuerpo Ω. Entonces ϵ se puede extender a un place ϑ de K. Si Ω es algebraicamente cerrado, el place ϑ se puede elegir Ω–valuado.*

Theorem II (Places y clausuras enteras)**.** *([Lan93, Ch. VII, §3, proof of Proposition 3.5]) Sea A una $\mathbb{C}$–álgebra contenida en el cuerpo K. Entonces la intersección $\bigcap_\vartheta R_\vartheta$, donde ϑ recorre todos los places de K con $A \subset R_\vartheta$, es la clausura entera de A en K.*

Si A es un dominio íntegro que es una $\mathbb{C}$–álgebra local con cuerpo de clases residuales $\mathbb{C}$ y es esencialmente de tipo finito (esto es, es la localización de un anillo que es finitamente generado sobre $\mathbb{C}$), entonces la clausura entera de A en su anillo de fracciones es la intersección de los anillos de valuación de los places $\mathbb{C}$–valuados que contienen a A.

La noción más bien abstracta de place $\mathbb{C}$–valuado se puede parafrasear en los siguientes términos geométricos.

Sea V una variedad irreducible afín y x un punto de V. Obsérvese que evaluar las funciones coordenadas de V, es decir los elementos de $\mathbb{C}[V]$, en el punto $\boldsymbol{x}$ proporciona un homomorfismo de $\mathbb{C}$–álgebras $ev_x : \mathbb{C}[V] \to \mathbb{C}$ que caracteriza el punto $x \in V$. Sea $A := \mathbb{C}[V]$, $K := \mathbb{C}(V)$, $\Omega := \mathbb{C}$, $\epsilon := ev_x$ y fíjese un place $\mathbb{C}$–valuado $\vartheta : K \to \mathbb{C} \cup \{\infty\}$ tal que ϑ extiende ϵ. Entonces ϑ asocia a cada función racional φ de V un valor $\vartheta(\varphi)$ que puede ser finito o infinito. En el primer caso consideramos a φ bien definida en el punto $x \in V$, con valor $\vartheta(\varphi)$. En el segundo caso consideramos el punto $x \in V$ como un punto de indeterminación o polo de la función racional φ. En vista de [Tei82, 1.3.4, Corollaire 2] podemos decir que el place ϑ imita la evaluación de funciones racionales sobre la normalización de un germen de curva en el punto x de la variedad V.

10.2. La noción de robustez geométrica

Por el momento fijemos un subconjunto construible $\mathcal{M}$ del espacio afín $\mathbb{A}^n$ y una aplicación construible (total) $\phi : \mathcal{M} \to \mathbb{A}^m$ con componentes $\phi_1, \ldots, \phi_m$. Supóngase que ϕ es débilmente continua en el sentido de la Definición 9.1.2, es decir

> *existe un subconjunto abierto y denso Zariski U de $\mathcal{M}$ tal que la restricción $\phi|_U$ es una aplicación racional de $\mathcal{M}$ y el gráfico de ϕ está contenido en la clausura Zariski Γ del gráfico de $\phi|_U$ en $\mathcal{M} \times \mathbb{A}^m$.*

Obsérvese que Γ es un subconjunto construible de $\mathbb{A}^n \times \mathbb{A}^m$ que contiene el gráfico de ϕ. Sea $\pi : \Gamma \to \mathcal{M}$ la primera proyección de Γ definida por $\pi(x, y) := x$. Obsérvese que π es una aplicación polinomial.

Recordemos, de acuerdo con la Definición 9.1.2, que la aplicación construible $\phi : \mathcal{M} \to \mathbb{A}^m$ es topológicamente robusta si y sólo si es débilmente continua y satisface la siguiente condición:

(∗) *para toda sucesión $(x_k)_{k\in\mathbb{N}}$ de $\mathcal{M}$ que converge en la topología Euclídea a un punto de $\mathcal{M}$, la sucesión $(\phi(x_k))_{k\in\mathbb{N}}$ es acotada.*

Esta condición es equivalente a la robustez de la aplicación polinomial suryectiva $\pi : \Gamma \to \mathcal{M}$ en el sentido de [CGH$^+$03, Definition 3]. Más precisamente, tenemos el siguiente hecho.

Observación 10.2.1. *La aplicación construible, débilmente continua, ϕ satisface la condición (∗) si y sólo si para toda sucesión $(x_k, y_k)_{k\in\mathbb{N}}$ de Γ tal que $(x_k)_{k\in\mathbb{N}}$ converge a un punto $x_0 \in \mathcal{M}$, existe un punto de acumulación y_0 de la sucesión $(y_k)_{k\in\mathbb{N}}$ con $(x_0, y_0) \in \Gamma$.*

Demostración. Supóngase que ϕ satisface la condición (∗) de arriba y sea $(x_k, y_k)_{k\in\mathbb{N}}$ una sucesión de Γ tal que $(x_k)_{k\in\mathbb{N}}$ converge a un punto $x_0 \in \mathcal{M}$. Sea $(u_k, v_k)_{k\in\mathbb{N}}$ una sucesión del gráfico de $\phi|_U$ con $\|(x_k, y_k) - (u_k, v_k)\| < 1/k$ para todo $k \in \mathbb{N}$, donde $\|\cdot\|$ denota la norma Euclídea de $\mathbb{A}^n \times \mathbb{A}^m$. Entonces $(u_k)_{k\in\mathbb{N}}$ converge a $x_0 \in \mathcal{M}$ y por lo tanto la condición (∗) implica que la sucesión $(v_k)_{k\in\mathbb{N}} = (\phi(u_k))_{k\in\mathbb{N}}$ es acotada. Concluimos que la sucesión $(y_k)_{k\in\mathbb{N}}$ también es acotada, y contiene en consecuencia una subsucesión convergente. Por lo tanto la sucesión $(x_k, y_k)_{k\in\mathbb{N}}$ tiene una subsucesión convergente, cuyo límite (x_0, y_0) necesariamente pertenece a Γ puesto que Γ es cerrado en $\mathcal{M} \times \mathbb{A}^m$ con respecto a la topología Euclídea y x_0 pertenece a $\mathcal{M}$.

Supóngase ahora que ϕ satisface la segunda condición del enunciado de la observación y sea $(x_k)_{k\in\mathbb{N}}$ una sucesión de $\mathcal{M}$ que converge en la topología Euclídea a $x_0 \in \mathcal{M}$. Entonces existe una sucesión $(u_k)_{k\in\mathbb{N}}$ de U que también converge a x_0. Afirmamos que la sucesión $(\phi(u_k))_{k\in\mathbb{N}}$ es acotada. En otro caso, existe una sucesión $(\phi(u_{k_l}))_{l\in\mathbb{N}}$ tal que $(\|\phi(u_{k_l})\|)_{l\in\mathbb{N}}$ diverge a infinito. Por otra parte, la sucesión $(u_{k_l}, \phi(u_{k_l}))_{l\in\mathbb{N}}$ satisface la hipótesis de la segunda condición del enunciado de la observación, pero la sucesión $(\phi(u_{k_l}))_{l\in\mathbb{N}}$ no tiene ningún punto de acumulación. Esto contradice la hipótesis sobre ϕ y prueba la afirmación. Por lo tanto la sucesión $(\phi(x_k))_{k\in\mathbb{N}}$ es acotada, lo que termina la demostración. □

Consideramos ahora la clausura Zariski $\overline{\mathcal{M}}$ del subconjunto construible $\mathcal{M}$ de $\mathbb{A}^n$. Obsérvese que $\overline{\mathcal{M}}$ es una subvariedad cerrada afín de $\mathbb{A}^n$ y que podemos interpretar la $\mathbb{C}$–álgebra $\mathbb{C}(\overline{\mathcal{M}})$ de funciones racionales de $\overline{\mathcal{M}}$ como un $\mathbb{C}[\overline{\mathcal{M}}]$–módulo (o álgebra). Fíjese ahora un punto arbitrario x de $\overline{\mathcal{M}}$. Por $\mathfrak{M}_x$ denotamos el ideal maximal de las funciones coordenadas de $\mathbb{C}[\overline{\mathcal{M}}]$ que se anulan en el punto x, por $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$ la $\mathbb{C}$–álgebra local de la variedad $\overline{\mathcal{M}}$ en el punto x, esto es, la localización de $\mathbb{C}[\overline{\mathcal{M}}]$ en el ideal maximal $\mathfrak{M}_x$ y por $\mathbb{C}(\overline{\mathcal{M}})_{\mathfrak{M}_x}$ la localización del $\mathbb{C}[\overline{\mathcal{M}}]$–módulo $\mathbb{C}(\overline{\mathcal{M}})$ en $\mathfrak{M}_x$.

Supóngase ahora que la aplicación construible $\phi : \mathcal{M} \to \mathbb{A}^m$ es topológicamente robusta. Entonces, de acuerdo con el Lema 9.1.1, podemos interpretar $\phi_1, \ldots, \phi_m$ como funciones racionales de la variedad afín $\overline{\mathcal{M}}$ y por lo tanto como elementos del anillo de fracciones total $\mathbb{C}(\overline{\mathcal{M}})$ de $\mathbb{C}[\overline{\mathcal{M}}]$. En consecuencia $\mathbb{C}[\overline{\mathcal{M}}][\phi_1, \ldots, \phi_m]$ y $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_x}[\phi_1, \ldots, \phi_m]$ son $\mathbb{C}$–subálgebras de $\mathbb{C}(\overline{\mathcal{M}})$ y $\mathbb{C}(\overline{\mathcal{M}})_{\mathfrak{m}_x}$ que contienen a $\mathbb{C}[\overline{\mathcal{M}}]$ y $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_x}$, respectivamente.

Con estas notaciones podemos formular el siguiente enunciado que establece el puente hacia una comprensión algebraica de la noción de robustez topológica.

Teorema 10.2.2. *Sean las notaciones y las hipótesis como antes. Supóngase que la aplicación construible $\phi : \mathcal{M} \to \mathbb{A}^m$ es topológicamente robusta y sea x un punto arbitrario de $\mathcal{M}$. Entonces $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_x}[\phi_1, \ldots, \phi_m]$ es un $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_x}$–módulo finito.*

El Teorema 10.2.2 es una consecuencia inmediata de la Observación 10.2.1 y de [CGH$^+$03, Lemma 3], que a su vez está basado en el Teorema Principal de Zariski (ver, por ejemplo, [Ive73, §IV.2]).

En lo que sigue, el Teorema 10.2.2 sólo será usado como motivación para la noción más técnica de robustez geométrica que vamos a definir posteriormente en esta sección. Si reeplazamos la condición $(*)$ de arriba por una condición más fuerte, a saber:

$(**)$ *para toda sucesión $(x_k)_{k\in\mathbb{N}}$ de $\mathcal{M}$ que converge en la topología Euclídea a un punto $x \in \overline{\mathcal{M}}$, la sucesión $(\phi(x_k))_{k\in\mathbb{N}}$ permanece acotada,*

la conclusión del Teorema 10.2.2 es más fácil de probar.

En este sentido, en la Observación 10.2.3 más abajo, daremos una demostración *elemental* del Teorema 10.2.2 bajo la hipótesis de que $\mathcal{M}$ es *cerrado*, esto es, en el caso $\overline{\mathcal{M}} = \mathcal{M}$. Por lo tanto, si aceptamos restringir la noción de robustez topológica a los casos en que la condición $(**)$ se satisface, entonces la Observación 10.2.3 nos permite mantener el presente trabajo autocontenido. Observamos que todos los enunciados de este trabajo sobre aplicaciones topológicamente robustas siguen siendo válidos si reeplazamos la condición $(*)$ en la definición de la noción de aplicaciones topológicamente robustas por el requerimiento $(**)$.

Los siguientes argumentos retoman técnicas de las demostraciones de [Tei82, 1.3.4, Corollaire 2] y [Ald84, Satz 2].

Observación 10.2.3. (Demostración del Teorema 10.2.2 en el caso $\overline{\mathcal{M}} = \mathcal{M}$). Supóngase que $\overline{\mathcal{M}} = \mathcal{M}$. Por lo tanto $\mathcal{M}$ es una subvariedad cerrada de $\mathbb{A}^n$.

Primeramente observamos que podemos suponer sin pérdida de generalidad que $\mathcal{M}$ es irreducible. Por lo tanto $\mathbb{C}[\mathcal{M}]$ es una $\mathbb{C}$–álgebra sin divisores de cero, $\mathbb{C}(\mathcal{M})$ es un cuerpo y para todo $x \in \mathcal{M}$ las $\mathbb{C}$–álgebras $\mathbb{C}[\mathcal{M}]_{\mathfrak{m}_x}$ y $\mathbb{C}[\mathcal{M}]_{\mathfrak{m}_x}[\phi_1, \ldots, \phi_m]$ son extensiones de $\mathbb{C}[\mathcal{M}]$ y $\mathbb{C}[\mathcal{M}][\phi_1, \ldots, \phi_m]$ respectivamente.

Bajo estas condiciones, el Teorema 10.2.2 afirma que la $\mathbb{C}$–álgebra $\mathbb{C}[\mathcal{M}]_{\mathfrak{m}_x}[\phi_1, \ldots, \phi_m]$ es una extensión entera de $\mathbb{C}[\mathcal{M}]_{\mathfrak{m}_x}$.

Interpretada como una aplicación racional, ϕ tiene un dominio, digamos U, que es un subconjunto abierto Zariski no vacío de $\mathcal{M}$. Denótese por r la dimensión de $\mathcal{M}$ y supóngase sin pérdida de generalidad que $X_1, \ldots, X_n$ están en posición genérica

con respecto a $\mathcal{M}$. Escribamos $\boldsymbol{X}' := (X_1, \ldots, X_r)$ y $\nu : \mathcal{M} \to \mathbb{A}^r$ para el morfismo suryectivo finito de variedades afines definido por $\mathcal{M}$ por $\nu(z) := (z_1, \ldots, z_r)$.

Supóngase ahora que la conclusión del Teorema 10.2.2 es falsa. Entonces existe un punto $x := (x_1, \ldots, x_n)$ de $\mathcal{M}$ y una componente de ϕ, digamos ϕ_1, que no es entera sobre $\mathbb{C}[\mathcal{M}]_{\mathfrak{M}_x}$.

Escribamos $x' := (x_1, \ldots, x_r)$ y sea $\mathfrak{M}_{x'}$ el ideal maximal de $\mathbb{C}[\boldsymbol{X}']$ generado por $X_1 - x_1, \ldots, X_r - x_r$. Entonces ϕ_1 tampoco es entera sobre $\mathbb{C}[\boldsymbol{X}']_{\mathfrak{M}_{x'}}$.

Sea T una nueva indeterminada y sea $\alpha(\boldsymbol{X}', T) := A_q T^q + \cdots + A_0$ el polinomio primitivo irreducible de ϕ_1 sobre $\mathbb{C}[\boldsymbol{X}']$ con $A_q, \ldots, A_0 \in \mathbb{C}[\boldsymbol{X}']$, $q > 0$ y $\deg A_q \geq 1$. Puesto que ϕ_1 no es entera sobre $\mathbb{C}[\boldsymbol{X}']_{\mathfrak{M}_{x'}}$, existe $0 \leq h < q$ tal que A_h/A_q no pertenece a $\mathbb{C}[\boldsymbol{X}']_{\mathfrak{M}_{x'}}$. Obsérvese que el polinomio $\alpha(\boldsymbol{X}', T)$ describe la clausura Zariski de la imagen de la aplicación $\mu : U \to \mathbb{A}^{r+1}$ definida por $\mu(z) := (\nu(z), \phi_1(z))$. Por lo tanto existe un subconjunto abierto Zariski no vacío $\mathcal{G}$ de $\mathbb{A}^r$ tal que todo $y \in \mathcal{G}$ satisface la condición $A_q(y) \neq 0$ y tal que para todo $t \in \mathbb{C}$ con $\alpha(y, t) = 0$ existe un elemento $z \in U$ con $\mu(z) = (\nu(z), \phi_1(z)) = (y, t)$.

Para simplificar notaciones, supondremos sin pérdida de generalidad que los polinomios no nulos A_h y A_q no contienen divisores primos comunes. A partir de [GF76, Chapter V, Theorem 3.12] deducimos que existe una sucesión $(s_k)_{k\in\mathbb{N}}$ de $\mathcal{G}$ tal que $(s_k)_{k\in\mathbb{N}}$ converge a x' en la topología Euclídea de $\mathbb{A}^r$ y tal que la sucesión $(\frac{A_h}{A_q}(s_k))_{k\in\mathbb{N}}$ converge a infinito.

Por lo tanto existe una sucesión *no acotada* $(t_k)_{k\in\mathbb{N}}$ de números complejos que satisface para todo $k \in \mathbb{N}$ la condición $\alpha(s_k, t_k) = 0$.

Esto implica la existencia de una sucesión $(z_k)_{k\in\mathbb{N}}$ de elementos de U tal que $\mu(z_k) = (\nu(z_k), \phi_1(z_k)) = (s_k, t_k)$ para todo $k \in \mathbb{N}$. Por lo tanto la sucesión $(\phi_1(z_k))_{k\in\mathbb{N}}$ es no acotada, en tanto que la sucesión $\nu(z_k)_{k\in\mathbb{N}}$ tiende a x'. Puesto que $\nu : \mathcal{M} \to \mathbb{A}^r$ es un morfismo finito de variedades afines, concluimos que la sucesión $(z_k)_{k\in\mathbb{N}}$ es acotada. Por lo tanto podemos suponer sin pérdida de generalidad que $(z_k)_{k\in\mathbb{N}}$ converge al punto $z \in \mathbb{A}^n$.

Puesto que por hipótesis $\mathcal{M}$ es cerrada y z_k pertenece a $\mathcal{M}$ para todo $k \in \mathbb{N}$, deducimos que z es un elemento de $\mathcal{M}$. En consecuencia hemos encontrado una sucesión de puntos de $\mathcal{M}$, a saber $(z_k)_{k\in\mathbb{N}}$, que converge a un elemento de $\mathcal{M}$, a saber z, tal que la sucesión $(\phi_1(z_k))_{k\in\mathbb{N}}$ es no acotada. Esto implica la no acotación de la sucesión $(\phi(z_k))_{k\in\mathbb{N}}$, lo que por $(*)$ contradice la hipótesis que ϕ es topológicamente robusta. ■

Corolario 10.2.4. *Sean las notaciones y las hipótesis como antes y supóngase en particular que la aplicación construible $\phi : \mathcal{M} \to \mathbb{A}^m$ es débilmente continua. Entonces ϕ es topológicamente robusta si y sólo si para todo punto x de $\mathcal{M}$ la $\mathbb{C}$–álgebra $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\phi_1, \ldots, \phi_m]$ es un $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$–módulo finito.*

Demostración. La parte *sólo si* de este enunciado es el contenido del Teorema 10.2.2.

A continuación demostramos la parte *si*. Nuestra argumentación es autocontenida y usa ideas de la demostración de [CGH$^+$03, Lemma 3].

Puesto que ϕ es débilmente continua, existe un subconjunto denso, abierto Zariski U de $\mathcal{M}$ que satisface la condición (i) de la Definición 9.1.2. Sea $(x_k)_{k\in\mathbb{N}}$ una sucesión

de U que converge a un punto $x \in \mathcal{M}$. De acuerdo con la Observación 9.1.3, es suficiente mostrar que la sucesión $(\phi(x_k))_{k\in\mathbb{N}}$ es acotada.

Por hipótesis $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\phi_1,\ldots,\phi_m]$ es un $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$–módulo finito. En consecuencia, $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\phi_1,\ldots,\phi_m]$ es una extensión entera de $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$. Por lo tanto existe un elemento g de $\mathbb{C}[\overline{\mathcal{M}}]$ con $g(x) \neq 0$ tal que $\mathbb{C}[\overline{\mathcal{M}}]_g[\phi_1,\ldots,\phi_m]$ es también una extensión entera de $\mathbb{C}[\overline{\mathcal{M}}]_g$.

Existen a lo sumo finitos índices $k \in \mathbb{N}$ con $g(x_k) = 0$, ya que en otro caso la continuidad de g implicaría $g(x) = 0$, una contradicción. Por lo tanto podemos suponer sin pérdida de generalidad que $g(x_k) \neq 0$ para todo $k \in \mathbb{N}$.

Sea T una nueva indeterminada. Existe un polinomio mónico $P_1(T)$ de $\mathbb{C}[\overline{\mathcal{M}}]_g[T]$ con $P_1(\phi_1) = 0$. Obsérvese que $P_1(T)$ puede especializarse para x y x_k, $k \in \mathbb{N}$, en polinomios $P_1(x)(T)$, $P_1(x_k)(T)$ de $\mathbb{C}[T]$ y números complejos $P_1(x_k)(\phi_1(x_k))$ bien definidos. Además tenemos que $\deg P_1(x)(T) = \deg P_1(x_k)(T) = \deg P_1(T)$ y por lo tanto existe una cota superior para las raíces de los polinomios $P_1(x_k)(T)$ que no depende de $k \in \mathbb{N}$. A partir de $P_1(\phi_1) = 0$ deducimos que $P_1(x_k)(\phi_1(x_k)) = 0$ para todo $k \in \mathbb{N}$. Esto implica que la sucesión $(\phi_1(x_k))_{k\in\mathbb{N}}$ es acotada. Repitiendo el mismo argumento para $\phi_2,\ldots,\phi_m$ concluimos que $(\phi(x_k))_{k\in\mathbb{N}}$ es también acotada. □

Corolario 10.2.5. *Sea $\phi : \mathcal{M} \to \mathbb{A}^m$ topológicamente robusta y supóngase que la variedad afín $\overline{\mathcal{M}}$ es normal en todo punto de $\mathcal{M}$. Entonces $\phi : \mathcal{M} \to \mathbb{A}^m$ es una aplicación regular y es por lo tanto fuertemente continua.*

Demostración. Sea x un punto arbitrario de $\mathcal{M}$. Puesto que $\overline{\mathcal{M}}$ es normal en x, se sigue que x pertenece a una única componente irreducible (Proposición 2.1.15), digamos $\mathcal{M}_1$, de $\overline{\mathcal{M}}$. Obsérvese que vale la identidad $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x} = \mathbb{C}[\mathcal{M}_1]_{\mathfrak{M}_x}$. La robustez topológica de ϕ implica que la extensión $\mathbb{C}[\mathcal{M}_1]_{\mathfrak{M}_x} \hookrightarrow \mathbb{C}[\mathcal{M}_1]_{\mathfrak{M}_x}[\phi_1,\ldots,\phi_m]$ de $\mathbb{C}$–álgebras es entera. Teniendo en cuenta que x es un punto normal de $\mathcal{M}_1$, deducimos que $\mathbb{C}[\mathcal{M}_1]_{\mathfrak{M}_x}$ es integralmente cerrada en $\mathbb{C}(\mathcal{M}_1)$. El Teorema 10.2.2 implica que las funciones racionales $\phi_1,\ldots,\phi_m$ están contenidas en $\mathbb{C}[\mathcal{M}_1]_{\mathfrak{M}_x} = \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$. Por lo tanto la aplicación racional ϕ está bien definida en el punto x, lo que concluye la demostración del corolario. □

En el caso que el conjunto construible $\mathcal{M}$ sea irreducible, podemos caracterizar la robustez topológica de la aplicación construible $\phi : \mathcal{M} \to \mathbb{A}^m$ de manera muy natural por medio de places. En el Capítulo 11 el uso de la noción de robustez topológica estará limitado a este caso.

Proposición 10.2.6. *Sean las notaciones y las hipótesis como antes y supóngase que $\mathcal{M}$ es irreducible. Entonces la aplicación construible $\phi : \mathcal{M} \to \mathbb{A}^m$ es topológicamente robusta si y sólo si ϕ es débilmente continua y si para todo punto $x \in \mathcal{M}$ y todo place $\mathbb{C}$–valuado $\vartheta : \mathbb{C}(\overline{\mathcal{M}}) \to \mathbb{C} \cup \{\infty\}$ que extiende el homomorfismo de $\mathbb{C}$–álgebras $ev_x : \mathbb{C}[\overline{\mathcal{M}}] \to \mathbb{C}$, los valores $\vartheta(\phi_1),\ldots,\vartheta(\phi_m)$ son finitos.*

La Proposición 10.2.6 es una consecuencia inmediata del Corolario 10.2.4 y el Teorema II y su demostración será omitida aquí.

De paso, observemos que para $x \in \mathcal{M}$, el place $\mathbb{C}$–valuado ϑ extiende el homomorfismo de $\mathbb{C}$–álgebras ev_x si y sólo si la $\mathbb{C}$–álgebra local $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$ está contenida en el anillo de valuación de ϑ.

La Proposición 10.2.6 motiva la siguiente noción de robustez geométrica.

Definición 10.2.7. *Sea $\phi : \mathcal{M} \to \mathbb{A}^m$ una aplicación construible con componentes $\phi_1, \ldots, \phi_m$ y supóngase que $\mathcal{M}$ es un subconjunto construible irreducible del espacio afín $\mathbb{A}^n$. Entonces ϕ se dice* ***geométricamente robusta*** *si satisface la siguiente condición:*

para todo punto $x \in \mathcal{M}$ y todo place $\mathbb{C}$–valuado $\vartheta : \mathbb{C}(\overline{\mathcal{M}}) \to \mathbb{C} \cup \{\infty\}$ que extiende el homomorfismo de $\mathbb{C}$–álgebras $ev_x : \mathbb{C}[\overline{\mathcal{M}}] \to \mathbb{C}$, los valores $\vartheta(\phi_1), \ldots, \vartheta(\phi_m)$ son finitos y están unívocamente determinados por x (es decir, estos valores no dependen de la extensión particular del homomorfismo de $\mathbb{C}$–álgebras ev_x a un place $\mathbb{C}$–valuado ϑ de $\mathbb{C}(\overline{\mathcal{M}})$). Además, se satisfacen las identidades $\vartheta(\phi_1) = \phi_1(x), \ldots, \vartheta(\phi_m) = \phi_m(x)$.

Observación 10.2.8. *La aplicaciones regulares y las composiciones de aplicaciones geométricamente robustas con aplicaciones polinomiales son geométricamente robustas.*

Proposición 10.2.9. *Sean las notaciones y las hipótesis como en la Definición 10.2.7 y supóngase que la aplicación construible $\phi : \mathcal{M} \to \mathbb{A}^m$ es geométricamente robusta. Entonces ϕ es topológicamente robusta.*

Demostración. Por hipótesis $\mathcal{M}$ es un subconjunto construible irreducible del espacio afín $\mathbb{A}^n$. Por lo tanto $\overline{\mathcal{M}}$ es una subvariedad cerrada irreducible de $\mathbb{A}^n$. Sean $\xi_1, \ldots, \xi_n$ las funciones coordenadas de $\overline{\mathcal{M}}$ inducidas por las indeterminadas $X_1, \ldots, X_n$. Sea $\boldsymbol{X} := (X_1, \ldots, X_n)$ y $\xi := (\xi_1, \ldots, \xi_n)$.

En vista de la Proposición 10.2.6 sólo tenemos que mostrar que ϕ es débilmente continua.

Por el Lema 9.1.1, existe un subconjunto denso y abierto Zariski U de $\mathcal{M}$ tal que $\phi|_U$ es una aplicación racional. Afirmamos que el gráfico de ϕ está contenido en la clausura Zariski del gráfico de $\phi|_U$ en $\mathcal{M} \times \mathbb{A}^m$.

Sea $\boldsymbol{Y} := (Y_1, \ldots, Y_m)$, donde $Y_1, \ldots, Y_m$ son nuevas indeterminadas, y sea $Q \in \mathbb{C}[\boldsymbol{X}, \boldsymbol{Y}]$ un polinomio arbitrario que satisface la condición $Q(x, \phi(x)) = 0$ para todo punto $x \in U$. Entonces Q se anula en todo punto de la clausura Zariski del gráfico de $\phi|_U$ en $\mathcal{M} \times \mathbb{A}^m$. Es suficiente mostrar que $Q(x, \phi(x)) = 0$ para todo punto $x \in \mathcal{M}$.

Obsérvese que la hipótesis sobre Q implica que $Q(\xi, \phi) = Q(\xi, \phi_1, \ldots, \phi_m) = 0$, donde $\phi_1, \ldots, \phi_m$ se interpretan como elementos de $\mathbb{C}(\overline{\mathcal{M}})$. Sea x un punto arbitrario de $\mathcal{M}$ y sea $\vartheta : \mathbb{C}(\overline{\mathcal{M}}) \to \mathbb{C} \cup \{\infty\}$ un place $\mathbb{C}$–valuado que extiende el homomorfismo de $\mathbb{C}$–álgebras $ev_x : \mathbb{C}[\overline{\mathcal{M}}] \to \mathbb{C}$. Luego $Q(\xi, \phi) = 0$ implica $Q(x, \vartheta(\phi_1), \ldots, \vartheta(\phi_m)) = 0$. Por hipótesis tenemos que $\vartheta(\phi_1) = \phi_1(x), \ldots, \vartheta(\phi_m) = \phi_m(x)$ y por lo tanto $Q(x, \phi(x)) = Q(x, \phi_1(x), \ldots, \phi_m(x)) = Q(x, \vartheta(\phi_1), \ldots, \vartheta(\phi_m)) = 0$. □

Ahora vamos a demostrar que una aplicación geométricamente robusta $\phi : \mathcal{M} \to \mathbb{A}^m$ es siempre hereditaria. Con este propósito, probamos el resultado más fuerte

que dice que la restricción de ϕ a un subconjunto construible irreducible de $\mathcal{M}$ es geométricamente robusta.

Teorema 10.2.10. *Sean las notaciones y las hipótesis como en la Definición 10.2.7. Sea $\phi : \mathcal{M} \to \mathbb{A}^m$ una aplicación geométricamente robusta y sea $\mathcal{N}$ un subconjunto construible irreducible de $\mathcal{M}$. Entonces la restricción $\phi|_{\mathcal{N}}$ es una aplicación geométricamente robusta.*

Demostración. Por hipótesis $\mathcal{M}$ es un subconjunto construible irreducible del espacio afín $\mathbb{A}^n$ y por lo tanto $\overline{\mathcal{M}}$ es una subvariedad cerrada irreducible de $\mathbb{A}^n$.

Sea $\mathcal{Z} := \overline{\mathcal{N}}$ la clausura Zariski de $\mathcal{N}$ en el espacio ambiente afín $\mathbb{A}^n$. Entonces $\mathcal{Z}$ es una subvariedad cerrada irreducible de $\overline{\mathcal{M}}$ y $\mathcal{N}$ contiene un subconjunto abierto Zariski no vacío (y por lo tanto denso Zariski) de $\mathcal{Z}$.

Para todo punto $z \in \mathcal{Z}$, sean $ev_z(\overline{\mathcal{M}}) : \mathbb{C}[\overline{\mathcal{M}}] \to \mathbb{C}$ y $ev_z(\mathcal{Z}) : \mathbb{C}[\mathcal{Z}] \to \mathbb{C}$ los homomorfismos de $\mathbb{C}$–álgebras dados por la evaluación de las funciones coordenadas de $\mathbb{C}[\overline{\mathcal{M}}]$ y $\mathbb{C}[\mathcal{Z}]$ en z respectivamente.

Ahora vamos a mostrar que existen funciones racionales $\psi_1, \ldots, \psi_m \in \mathbb{C}(\mathcal{Z})$ tales que para todo punto $z \in \mathcal{N}$ y todo place $\mathbb{C}$–valuado ϑ de $\mathbb{C}(\mathcal{Z})$ que extiende el homomorfismo de $\mathbb{C}$–álgebra $ev_z(\mathcal{Z})$, se satisface la siguiente condición:

$$\text{los valores de } \vartheta \text{ en } \psi_1, \ldots, \psi_m \text{ son finitos y satisfacen } \vartheta(\psi_1) = \phi_1(z), \ldots, \vartheta(\psi_m) = \phi_m(z).$$

Considérese el homomorfismo suryectivo canónico de $\mathbb{C}$–álgebras $\pi : \mathbb{C}[\overline{\mathcal{M}}] \to \mathbb{C}[\mathcal{Z}]$ inducido por la inmersión natural de $\mathcal{Z}$ en $\overline{\mathcal{M}}$. A partir del Teorema I deducimos que existe un cuerpo Ω que contiene a $\mathbb{C}(\mathcal{Z})$ tal que π se puede extender a un place Ω–valuado de $\mathbb{C}(\overline{\mathcal{M}})$, que también denotamos por π. Sea R_π el anillo de valuación del place π. Obsérvese que R_π contiene a $\mathbb{C}[\overline{\mathcal{M}}]$ y asimismo a su localización $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_z}$ en el ideal maximal $\mathfrak{M}_z$ de todo punto z de $\mathcal{Z}$.

Sea $1 \leq j \leq m$ y sea z_0 un elemento arbitrario (pero fijo) de $\mathcal{Z}$. Denotamos por $\mathfrak{M}'_{z_0}$ el ideal maximal de las funciones coordenadas de $\mathbb{C}[\mathcal{Z}]$ que se anulan en el punto z_0. Por hipótesis $\phi : \mathcal{M} \to \mathbb{A}^m$ es geométricamente robusta. Por lo tanto, por el Teorema II, la función racional ϕ_j pertenece a la clausura entera de $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}$ en $\mathbb{C}(\overline{\mathcal{M}})$. Luego existe un polinomio mónico

$$\alpha = \alpha(T) = T^s + a_{s-1}T^{s-1} + \cdots + a_0$$

de $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[T]$ tal que $\alpha(\phi_j) = 0$ se satisface en $\mathbb{C}(\overline{\mathcal{M}})$ (aquí s es un entero positivo y T una nueva indeterminada). Teniendo en cuenta que el anillo de valuación R_π contiene a $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}$, deducimos a partir del Teorema II que ϕ_j pertenece a R_π. Por lo tanto el valor $\psi_j := \pi(\phi_j)$ es finito y entero sobre $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}$. En particular, $\psi_j \in \Omega$ es algebraico sobre $\mathbb{C}(\mathcal{Z})$ y

$$\pi(\alpha) = \pi(\alpha)(T) := T^s + \pi(a_{s-1})T^{s-1} + \cdots + \pi(a_0) \in \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]$$

es una relación de dependencia algebraica para ψ_j sobre $\mathbb{C}(\mathcal{Z})$ (que no necesariamente es de grado of mínimo).

Sea $m_{\psi_j} \in \mathbb{C}(\mathcal{Z})[T]$ el polinomio mínimo (mónico) de ψ_j sobre $\mathbb{C}(\mathcal{Z})$ y sea $\Delta_{\psi_j} \in \mathbb{C}(\mathcal{Z})$ su discriminante. Puesto que m_{ψ_j} es irreducible y $\mathbb{C}(\mathcal{Z})$ es de característica cero, tenemos que $\Delta_{\psi_j} \neq 0$. Por lo tanto existe un subconjunto abierto Zariski no vacío $\mathcal{U}^*$ de $\mathcal{Z}$ tal que para todo $z \in \mathcal{U}^*$ los coeficientes del polinomio m_{ψ_j} (y por lo tanto también Δ_{ψ_j}) están bien definidos en z y tal que se satisface $\Delta_{\psi_j}(z) \neq 0$. Por lo tanto $m_{\psi_j}(z,T)$ es libre de cuadrados. Puesto que $\mathcal{N}$ es denso Zariski en $\mathcal{Z}$ existe un subconjunto abierto Zariski no vacío $\mathcal{U}_j$ de $\mathcal{Z}$ que está contenido en $\mathcal{N} \cap \mathcal{U}^*$ (y por lo tanto en $\mathcal{N}$). Ahora supóngase que $z_0 \in \mathcal{U}_j$. Entonces $m_{\psi_j}(T)$ pertenece a $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]$ y $m_{\psi_j}(z_0,T)$ es libre de cuadrados.

Sea $Q(T)$ un polinomio arbitrario de $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[T]$ con $Q(\phi_j) = 0$ y sea $\pi(Q)(T)$ el polinomio de $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]$ que se obtiene aplicando el place π a los coeficientes de $Q(T)$. Puesto que $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}$ está contenido en R_π, el place π toma sólo finitos valores sobre los coeficientes de $Q(T)$ y $\pi(Q)(T)$ está bien definida. A partir de $Q(\phi_j) = 0$ deducimos $0 = \pi(Q(\phi_j)) = \pi(Q)(\pi(\phi_j)) = \pi(Q)(\psi_j)$. En consecuencia el polinomio $m_{\psi_j}(T)$ divide a $\pi(Q)(T)$ en $\mathbb{C}(\mathcal{Z})[T]$ y por lo tanto, puesto que $m_{\psi_j}(T)$ es mónico, también en $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]$. Esto implica que π induce un homomorfismo suryectivo de $\mathbb{C}$–álgebras

$$\varphi : \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[\phi_j] \to \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]/m_{\psi_j}.$$

Resumiendo, tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}} & \xrightarrow{\pi'} & \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}} \\ \downarrow & & \downarrow \\ \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[\phi_j] & \xrightarrow{\varphi} & \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]/m_{\psi_j} \end{array},$$

donde las flechas verticales son homomorfismos inyectivos, las flechas horizontales homomorfismos suryectivos de $\mathbb{C}$–álgebras y π' es la restricción del place π a $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}$.

Sea $\tau \in \mathbb{C}$ una raíz arbitraria del polinomio mónico $m_{\psi_j}(z_0,T) \in \mathbb{C}[T]$. Entonces la evaluación en z_0 y τ induce un homomorfismo de $\mathbb{C}$–álgebras $ev_\tau : \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]/m_{\psi_j} \to \mathbb{C}$ tal que el diagrama

$$\begin{array}{ccc} \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}} & \xrightarrow{ev_{z_0}(\overline{\mathcal{M}})} & \mathbb{C} \\ \downarrow & \nearrow_{ev_\tau} & \\ \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]/m_{\psi_j} & & \end{array}$$

conmuta y tal que $\varphi(\phi_j)$, es decir la clase de T en $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]/m_{\psi_j}$, se aplica en $\tau \in \mathbb{C}$. A partir del Teorema I deducimos que el homomorfismo de $\mathbb{C}$–álgebras de $ev_\tau \circ \varphi : \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[\phi_j] \to \mathbb{C}$ se puede extender a un place $\mathbb{C}$–valuado ϑ_τ del cuerpo $\mathbb{C}(\overline{\mathcal{M}})$. Obsérvese que $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[\phi_j]$ está contenido en el anillo de valuación de ϑ_τ y que se satisface $\vartheta_\tau(\phi_j) = ev_\tau(\varphi(\phi_j)) = \tau$. Puesto que por hipótesis $\phi : \mathcal{M} \to \mathbb{A}^m$ es geométricamente robusta, el valor $\vartheta_\tau(\phi_j)$ no depende del place ϑ_τ. Por lo tanto el polinomio univariado $m_{\psi_j}(z_0,T)$ tiene un único cero en $\mathbb{C}$, a saber τ. Dado que $z_0 \in \mathcal{U}_j \subset \mathcal{U}^*$ deducimos que $m_{\psi_j}(z_0,T)$ es un polinomio libre de cuadrados de $\mathbb{C}[T]$.

Por lo tanto tenemos que $\deg m_{\psi_j}(T) = \deg m_{\psi_j}(z_0, T) = 1$, lo que implica que ψ_j pertenece a $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}$.

Concluimos que ψ_j está definida en todo punto de $\mathcal{U}_j$ para $1 \leq j \leq m$. De esta manera obtenemos funciones racionales $\psi_1, \ldots, \psi_m$ y subconjuntos abiertos Zariski $\mathcal{U}_1, \ldots, \mathcal{U}_m$ de $\mathcal{Z}$ tales que para $1 \leq j \leq m$ la función racional ψ_j está bien definida en $\mathcal{U}_j$ y tal que $\mathcal{U}_j$ está contenido en $\mathcal{N}$.

En consecuencia $\mathcal{U} := \mathcal{U}_1 \cap \cdots \cap \mathcal{U}_m$ es un subconjunto abierto Zariski de $\mathcal{N}$ donde las funciones racionales $\psi_1, \ldots, \psi_m$ están bien definidas. Además, para todo punto $z \in \mathcal{U}$ tenemos que $\psi_1(z) = \phi_1(z), \ldots, \psi_m(z) = \phi_m(z)$.

Sea $\psi := (\psi_1, \ldots, \psi_m)$. Entonces ψ es una aplicación racional de $\mathcal{Z}$ en $\mathbb{A}^m$ con $\psi|_{\mathcal{U}} = \phi|_{\mathcal{U}}$. Vamos a mostrar que $\phi|_{\mathcal{N}}$ es geométricamente robusta.

Sea z un punto arbitrario de $\mathcal{N}$ y sea ϑ un place $\mathbb{C}$–valuado arbitrario de $\mathbb{C}(\mathcal{Z})$ que extiende el homomorfismo de $\mathbb{C}$–álgebras $ev_z(\mathcal{Z}) : \mathbb{C}[\mathcal{Z}] \to \mathbb{C}$. Levantando, de acuerdo con el Teorema I, el place ϑ a un place $\mathbb{C}$–valuado del cuerpo Ω y componiendo el resultado con el place Ω–valuado π, obtenemos un place $\mathbb{C}$–valuado ϑ' de $\mathbb{C}(\overline{\mathcal{M}})$ que extiende el homomorfismo de $\mathbb{C}$–álgebras $ev_z(\overline{\mathcal{M}})$. Puesto que por hipótesis $\phi : \mathcal{M} \to \mathbb{A}^m$ es geométricamente robusta, concluimos que para $1 \leq j \leq m$ el valor $\vartheta(\psi_j) = \vartheta(\pi(\phi_j)) = \vartheta \circ \pi(\phi_j) = \vartheta'(\phi_j)$ es finito e independiente de la elección de ϑ' y por lo tanto también de la elección de ϑ. Además tenemos que $\vartheta(\psi_j) = \vartheta'(\phi_j) = \phi_j(z)$ para $1 \leq j \leq m$. Concluimos que $\psi|_{\mathcal{N}}$ es geométricamente robusta. □

Ahora podemos probar que una aplicación geométricamente robusta es hereditaria.

Corolario 10.2.11. *Sean las notaciones y las hipótesis como en la Definición 10.2.7. Supóngase que la aplicación construible $\phi : \mathcal{M} \to \mathbb{A}^m$ es geométricamente robusta. Entonces ϕ es hereditaria.*

Demostración. Sea $\mathcal{N}$ un subconjunto construible arbitrario de $\mathcal{M}$. Tenemos que mostrar que $\phi|_{\mathcal{N}} : \mathcal{N} \to \mathbb{A}^m$ es débilmente continua, es decir, $\phi|_{\mathcal{N}}$ es una extensión de una aplicación racional de $\mathcal{N}$ tal que el gráfico de $\phi|_{\mathcal{N}}$ está contenido en la clausura Zariski del gráfico de esta aplicación racional en $\mathcal{N} \times \mathbb{A}^m$.

Sin pérdida de generalidad podemos suponer que $\mathcal{N}$ es irreducible. De acuerdo con el Teorema 10.2.10, la aplicación restricción $\phi|_{\mathcal{N}}$ es geométricamente robusta. Entonces la Proposición 10.2.9 implica que $\phi|_{\mathcal{N}}$ es topológicamente robusta, y en particular débilmente continua. Esto termina la demostración del Corolario. □

Definición 10.2.12. *Sean n y D números naturales y consideremos un problema de interpolación de Hermite–Lagrange determinado por una aplicación topológicamente robusta y hereditaria $\Phi : \mathcal{D} \to \Pi_D^{(n)}$. Además, sean $\omega^* : \mathcal{D}^* \to \Pi_D^{(n)}$ una aplicación polinomial y $\Psi : \mathcal{D} \to \mathcal{D}^*$ una aplicación hereditaria que determinan un algoritmo de interpolación de Hermite–Lagrange, el cual resuelve este problema en el sentido de la Definición 9.2.1. Llamamos a este algoritmo de interpolación* ***geométricamente robusto*** *si Ψ tiene esta propiedad.*

La Observación 10.2.8 implica el siguiente resultado.

Observación 10.2.13. *Si para el problema de interpolación determinado por $\mathcal{D}$ y Φ en la Definición 10.2.12 existe un algoritmo de Hermite–Lagrange geométricamente robusto, entonces la misma aplicación construible Φ es geométricamente robusta.*

10.3. Ejemplos de algoritmos geométricamente robustos

En esta sección analizamos si los algoritmos introducidos en la Sección 9.2.3 para el problema de interpolación de Lagrange genérico y el problema de interpolación de Lagrange bivariado son robustos.

10.3.1. Interpolación de Hermite–Lagrange de un polinomio fijo

Con un punto de vista ligeramente diferente volvemos ahora al segundo ejemplo de la Sección 9.2.3, es decir a la interpolación de Lagrange de polinomios univariados en $K \geq 2$ nodos genéricos. Así, sea $n := 1$, $D := K-1$, $M := K$, $N := K$, $\boldsymbol{X} := X_1$ y $\Pi_D := \Pi_D^{(1)}$. Sea dado un polinomio univariado F de $\Pi := \mathbb{C}[X_1]$ con $\deg F \gg K$ y sea $\mathcal{D} := \{(d_1, \ldots, d_N) \in \mathbb{A}^N : d_i \neq d_j \text{ para } 1 \leq i < j \leq N\}$. Consideramos el problema de interpolación de Lagrange univariado que consiste en hallar para todo punto $d := (d_1, \ldots, d_N) \in \mathcal{D}$ el único polinomio f_d en Π_D que interpola a F en los nodos $d_1, \ldots, d_N$. Por lo tanto f_d está determinado por la condiciones $f_d(d_i) = F(d_i)$, $1 \leq i \leq N$.

Sea, como en la Sección 9.2.3, $\mathcal{D}^* := \mathbb{A}^M$ y denótese por $\omega^* : \mathcal{D}^* \to \Pi_D$ la codificación de los elementos de Π_D por su representación densa. Para todo $d := (d_1, \ldots, d_N) \in \mathcal{D}$ sea $V_d := (d_i^{j-1})_{1 \leq i,j \leq N}$ la matriz de Vandermonde asociada a d y $F(d) := (F(d_1), \ldots, F(d_N))$. Entonces la representación densa de f_d está dada por $V_d^{-1} F(d)$. Obsérvese que las aplicaciones racionales (regulares) $\Psi_F : \mathcal{D} \to \mathcal{D}^*$ y $\Phi_F : \mathcal{D} \to \Pi_D$ definidas por $\Psi_F(d) := V_d^{-1} F(d)$ y $\Phi_F(d) := \omega^*(\Psi_F(d))$ son fuertemente continuas (por lo tanto topológicamente robustas y hereditarias). En consecuencia, $\mathcal{D}$ y Φ_F, y $\mathcal{D}^*$, ω^* y Ψ_F determinan un problema y un algoritmo de interpolación de Lagrange en el sentido de la Definición 9.2.1.

La aplicación racional Ψ_F está bien definida en todo punto de $\mathcal{D}$ pero no es claro *a priori* si Ψ_F tiene una extensión racional (por lo tanto polinomial) a $\overline{\mathcal{D}} = \mathbb{A}^N$. Sin embargo, a partir del conocido método de interpolación de Newton o de diferencias divididas (ver, por ejemplo, [SB93]) podemos deducir que Ψ_F es una aplicación polinomial.

Para ver esto, sean $T_1, \ldots, T_N$ nuevas indeterminadas, $\boldsymbol{T} := (T_1, \ldots, T_N)$ y sean $\Psi_F^{(1)}, \ldots, \Psi_F^{(N)} \in \mathbb{C}(\boldsymbol{T})$ las componentes de Ψ_F. Además, para $1 \leq j \leq N$ sea $F[T_1, \ldots, T_j] \in \mathbb{C}[\boldsymbol{T}]$ la j-ésima diferencia dividida de F. Obsérvese que las funciones racionales $\Psi_F^{(1)}, \ldots, \Psi_F^{(N)}$ aparecen como los coeficientes del polinomio $\sum_{j=1}^{N} F[T_1, \ldots, T_j](X_1 - T_1) \ldots (X_1 - T_{j-1})$ con respecto a la indeterminada X_1.

Esto implica que $\Psi_F : \mathcal{D} \to \mathcal{D}^*$ es una aplicación polinomial y por lo tanto geométricamente robusta. En otras palabras, el algoritmo de interpolación de Hermite–Lagrange determinado por $\mathcal{D}^*$, ω^* y Ψ_F es geométricamente robusto. Por lo tanto $\Phi_F : \mathcal{D} \to \Pi_D$ es también geométricamente robusta.

Sea $\mathcal{D}^+ := \mathbb{A}^N$. Puesto que Ψ_F es una aplicación polinomial y $\mathcal{D}^* = \mathbb{A}^M$ concluimos que Ψ_F se puede extender a una aplicación geométricamente robusta $\Psi_F^+ : \mathcal{D}^+ \to \mathcal{D}^*$. Sea $\Phi_F^+ := \omega^* \circ \Psi_F^+$. Entonces $\Phi_F^+ : \mathcal{D}^+ \to \Pi_D$ es también geométricamente (y por lo tanto topológicamente) robusta y hereditaria. En consecuencia $\mathcal{D}^+$ y Φ_F^+ determinan un problema de interpolación de Hermite–Lagrange, y el algoritmo determinado por $\mathcal{D}^*, \omega^*$ y Ψ_F^+ resuelve este problema en el sentido de la Definición 9.2.1.

Ahora vamos a analizar el problema de interpolación de Hermite–Lagrange determinado por $\mathcal{D}^+$ y Φ_F^+ para un punto arbitrario $d := (d_1, \ldots, d_M) \in \mathcal{D}^+$.

Si d pertenece a $\mathcal{D}$ tenemos el problema de interpolación de Lagrange considerado antes. Por lo tanto sea $d \in \mathcal{D}^+ \setminus \mathcal{D}$. Luego existen repeticiones entre los números complejos $d_1, \ldots, d_N$. Por simplicidad supondremos que $d_1 = d_2$ y que $d_1, d_3, \ldots, d_N$ son todos distintos. Entonces $f_d := \omega^*(\Psi_F^+(d))$ es el (único) polinomio de Π_D que satisface la condición $f_d(d_1) = F(d_1)$, $f_d'(d_1) = F'(d_1)$ y $f_d(d_i) = F(d_i)$ para $3 \leq i \leq N$, donde f_d' y F' denotan las derivadas de los polinomios f_d y F. Por lo tanto $\mathcal{D}^+$ y Φ_F^+ determinan un problema de interpolación de Hermite–Lagrange que no es simplemente del tipo de Lagrange.

Por otra parte, en vista del Corolario 10.2.5, este ejemplo no es muy ilustrativo, puesto que $\mathcal{D}^+ = \mathbb{A}^N$ implica que *todo* algoritmo determinado por $\mathcal{D}^*$, ω^* y una aplicación topológicamente robusta y hereditaria $\Psi : \mathcal{D}^+ \to \mathcal{D}^*$, que resuelve el problema de interpolación de Hermite–Lagrange dado por $\mathcal{D}^+$ y Φ_F^+, es geométricamente robusto. En este caso Ψ es incluso una aplicación polinomial.

10.3.2. Robustez en presencia de puntos singulares: revisión de los ejemplos de la Sección 9.2.3

Sean X_1, X_2 indeterminadas sobre $\mathbb{C}$ y sea $\Pi^{(2)} := \mathbb{C}[X_1, X_2]$. Analizamos ahora los algoritmos de los dos ejemplos para interpolación de Hermite–Lagrange bivariada considerados en la Sección 9.2.3. En ambos ejemplos, tenemos una función polinomial $f : \mathbb{A}^2 \to \mathbb{A}^1$ que deseamos interpolar y, como estructura de datos de entrada, una curva abierta $\mathcal{D} \subset \mathbb{A}^2$ que contiene $\mathbf{0} := (0, 0)$ como punto singular. Estos dos ejemplos difieren del anterior (interpolación de Hermite–Lagrange univariada clásica) en el hecho de que la estructura de datos de entrada $\mathcal{D}$ es singular en $\mathbf{0}$.

Interpolación sobre la curva $X_1^3 - X_2^2 = 0$. Sea $\mathcal{D} := \{X_1^3 - X_2^2 = 0\} \setminus \{(-1, \pm i)\} \subset \mathbb{A}^2$ y sea $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ la aplicación construible definida por

$$\Phi(d) := \begin{cases} f(\mathbf{0}) + \dfrac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2} X_1 + \dfrac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2} X_2, & \text{para } d := (d_1, d_2) \neq \mathbf{0}; \\ f(\mathbf{0}) + \dfrac{\partial f}{\partial X_1}(\mathbf{0}) X_1, & \text{para } d = \mathbf{0}. \end{cases}$$

En la Sección 9.2.3 mostramos que Φ es fuertemente continua. Por lo tanto $\mathcal{D}$ y Φ determinan un problema de interpolación de Hermite–Lagrange.

Como en la Sección 9.2.3, sea $\mathcal{D}^* := \mathbb{A}^3$ y sea $\omega^* : \mathcal{D}^* \to \Pi_1^{(2)}$ la codificación canónica densa de los polinomios bivariados de grado a lo sumo uno sobre $\mathbb{C}$. Además, sea $\Psi : \mathcal{D} \to \mathcal{D}^*$ la aplicación construible definida por

$$\Psi(d) := \begin{cases} \left(f(\mathbf{0}), \dfrac{(f(d)-f(\mathbf{0}))d_1}{d_1^2+d_2^2}, \dfrac{(f(d)-f(\mathbf{0}))d_2}{d_1^2+d_2^2}\right), & \text{para } d := (d_1,d_2) \neq \mathbf{0}; \\ \left(f(\mathbf{0}), \dfrac{\partial f}{\partial X_1}(\mathbf{0}), 0\right), & \text{para } \ d = \mathbf{0}. \end{cases}$$

Entonces Ψ es hereditaria y $\mathcal{D}^*$, ω^* y Ψ determinan un algoritmo que resuelve el problema de interpolación de Hermite–Lagrange definido por $\mathcal{D}$ y Φ.

Ahora vamos a demostrar que Ψ es geométricamente robusta. Sea $\Psi := (\Psi_1, \Psi_2, \Psi_3)$ y para todo punto $d \in \mathcal{D}$ denótese por $\mathfrak{M}_d$ el ideal maximal de las funciones coordenadas de $\mathbb{C}[\mathcal{C}]$ que se anulan en d, donde $\mathcal{C} := \{X_1^3 - X_2^2 = 0\}$ es la clausura Zariski (irreducible) de $\mathcal{D}$ en $\mathbb{A}^2$. Las funciones racionales Ψ_1, Ψ_2, Ψ_3 pertenecen a $\mathbb{C}[\mathcal{C}]_{\mathfrak{M}_d}$ para todo $d \in \mathcal{D} \setminus \{\mathbf{0}\}$ y por lo tanto satisfacen la condición de la Definición 10.2.7 en todo punto $d \in \mathcal{D} \setminus \{\mathbf{0}\}$. Teniendo en cuenta que $\Psi_1 = f|_{\mathcal{D}}$ es una función polinomial, basta mostrar que las funciones racionales Ψ_2 y Ψ_3 satisfacen la condición de la Definición 10.2.7 en el punto $\mathbf{0} \in \mathcal{D}$.

Puesto que la curva plana $\mathcal{C}$ es irreducible, $\mathbb{C}[\overline{\mathcal{D}}] = \mathbb{C}[\mathcal{C}]$ es un dominio íntegro con cuerpo de fracciones $\mathbb{C}(\overline{\mathcal{D}})$. Sean ξ_1 y ξ_2 las funciones coordenadas de $\mathbb{C}[\overline{\mathcal{D}}]$ inducidas por las indeterminadas X_1 y X_2 y sea $\xi := (\xi_1, \xi_2)$. Considérese un place $\mathbb{C}$–valuado arbitrario ϑ de $\mathbb{C}(\overline{\mathcal{D}})$ cuyo anillo de valuación R_ϑ contiene el álgebra local $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_\mathbf{0}}$. Dado que $\xi_1^3 = \xi_2^2$ y $\xi_1 \neq 0$, deducimos que $(\xi_2/\xi_1)^2 - \xi_1 = 0$ se satisface en $\mathbb{C}(\overline{\mathcal{D}})$. Por lo tanto ξ_2/ξ_1 es entera sobre $\mathbb{C}[\overline{\mathcal{D}}]$ y $(\xi_2/\xi_1)^2$ pertenece a $\mathfrak{M}_\mathbf{0} R_\vartheta$. Esto implica que ξ_2/ξ_1 es un elemento de R_ϑ contenido en el ideal maximal de R_ϑ. Por lo tanto $\vartheta(\xi_2/\xi_1) = 0$. Obsérvese que se satisfacen $\vartheta(\xi_1) = \vartheta(\xi_2) = 0$ y $\vartheta(1+\xi_1) = 1$. A partir del desarrollo de Taylor del polinomio f en el punto $\mathbf{0}$ vemos que existen polinomios Q_1, Q_2, Q_3 de $\Pi^{(2)}$ tales que

$$\frac{f(\xi)-f(\mathbf{0})}{\xi_1} = \frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\xi_2}{\xi_1}\frac{\partial f}{\partial X_2}(\mathbf{0}) + \xi_1 Q_1(\xi) + \frac{\xi_2^2}{\xi_1} Q_2(\xi) + \xi_2 Q_3(\xi)$$

se satisface en $\mathbb{C}(\overline{\mathcal{M}})$. Esto implica

$$\vartheta\Big(\frac{f(\xi)-f(\mathbf{0})}{\xi_1(1+\xi_1)}\Big) = \frac{\partial f}{\partial X_1}(\mathbf{0}).$$

Por otra parte tenemos que $\xi_1^2 + \xi_2^2 = \xi_1^2(1+\xi_1)$, y esto implica

$$\Psi_2(\xi) = \frac{f(\xi)-f(\mathbf{0})}{\xi_1(1+\xi_1)}, \quad \Psi_3(\xi) = \frac{f(\xi)-f(\mathbf{0})}{\xi_1(1+\xi_1)}\frac{\xi_2}{\xi_1}.$$

Por lo tanto el place ϑ tiene en $\Psi_2(\xi)$ y $\Psi_3(\xi)$ valores finitos:

$$\vartheta(\Psi_2(\xi)) = \frac{\partial f}{\partial X_1}(\mathbf{0}) = \Psi_2(\mathbf{0}), \ \vartheta(\Psi_3(\xi)) = 0 = \Psi_3(\mathbf{0}).$$

Concluimos que la aplicación construible Ψ es geométricamente robusta. Esto significa que el algoritmo de interpolación de Hermite–Lagrange determinado por $\mathcal{D}^*$, ω^* y Ψ es geométricamente robusto.

Interpolación sobre la curva $X_2^2 - X_1^2 - X_1^3 = 0$. Supóngase ahora que la aplicación polinomial $f : \mathbb{A}^2 \to \mathbb{A}^1$ satisface la condición $\big(\partial f/\partial X_1(\mathbf{0}), \partial f/\partial X_2(\mathbf{0})\big) \neq \mathbf{0}$. Consideramos la curva abierta $\mathcal{D} := \{X_2^2 - X_1^2 - X_1^3 = 0\} \setminus \{(-2, \pm 2i)\} \subset \mathbb{A}^2$ y la aplicación construible $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ definida por

$$\Phi(d) := \begin{cases} f(\mathbf{0}) + \dfrac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2} X_1 + \dfrac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2} X_2, & \text{para } d := (d_1, d_2) \neq \mathbf{0}; \\ f(\mathbf{0}) + \dfrac{1}{2}\Big(\dfrac{\partial f}{\partial X_1}(\mathbf{0}) + \dfrac{\partial f}{\partial X_2}(\mathbf{0})\Big) X_1 + \dfrac{1}{2}\Big(\dfrac{\partial f}{\partial X_1}(\mathbf{0}) + \dfrac{\partial f}{\partial X_2}(\mathbf{0})\Big) X_2, & \text{para } d = \mathbf{0}. \end{cases}$$

En la Sección 9.2.3 mostramos que Φ es topológicalmente robusta y hereditaria. Por lo tanto $\mathcal{D}$ y Φ determinan un problema de interpolación de Hermite–Lagrange.

De nuevo, como en la Sección 9.2.3, sea $\mathcal{D}^* := \mathbb{A}^3$ y sea $\omega^* : \mathcal{D}^* \to \Pi_1^{(2)}$ la codificación canónica densa de los polinomios bivariados de grado a lo sumo uno sobre $\mathbb{C}$. Además, sea $\Psi : \mathcal{D} \to \mathcal{D}^*$ la aplicación construible definida por

$$\Psi(d) := \begin{cases} \left(f(\mathbf{0}), \dfrac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2}, \dfrac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2}\right), & \text{para } d := (d_1, d_2) \neq \mathbf{0}; \\ \left(f(\mathbf{0}), \dfrac{1}{2}\Big(\dfrac{\partial f}{\partial X_1}(\mathbf{0}) + \dfrac{\partial f}{\partial X_2}(\mathbf{0})\Big), \dfrac{1}{2}\Big(\dfrac{\partial f}{\partial X_1}(\mathbf{0}) + \dfrac{\partial f}{\partial X_2}(\mathbf{0})\Big)\right), & \text{para } d = \mathbf{0}. \end{cases}$$

Entonces Ψ es hereditaria y $\mathcal{D}^*$, ω^* y Ψ determinan un algoritmo que resuelve el problema de interpolación de Hermite–Lagrange dado por $\mathcal{D}$ y Φ.

Afirmamos que Ψ no es geométricamente robusta. En efecto, sea $\Psi := (\Psi_1, \Psi_2, \Psi_3)$ y denótese por $\mathfrak{M}_\mathbf{0}$ el ideal maximal de las funciones coordenadas de $\mathbb{C}[\mathcal{C}]$ que se anulan en el punto $\mathbf{0} \in \mathcal{D}$, donde $\mathcal{C} := \{X_2^2 - X_1^2 - X_1^3 = 0\}$ es la clausura Zariski (irreducible) de $\mathcal{D}$ en $\mathbb{A}^2$. Basta mostrar que las funciones racionales Ψ_2 y Ψ_3 no satisfacen la condición de la Definición 10.2.7 en el punto $\mathbf{0} \in \mathcal{D}$.

Puesto que la curva plana $\mathcal{C}$ es irreducible, $\mathbb{C}[\overline{\mathcal{D}}] = \mathbb{C}[\mathcal{C}]$ es un dominio íntegro con cuerpo de fracciones $\mathbb{C}(\overline{\mathcal{D}})$. Sean ξ_1 y ξ_2 las funciones coordenadas de $\mathbb{C}[\overline{\mathcal{D}}]$ inducidas por las indeterminadas X_1 y X_2 y sea $\xi := (\xi_1, \xi_2)$. Considérese un place $\mathbb{C}$–valuado arbitrario ϑ de $\mathbb{C}(\overline{\mathcal{D}})$ cuyo anillo de valuación R_ϑ contiene el álgebra local $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_\mathbf{0}}$. Dado que $\xi_2^2 = \xi_1^2 + \xi_1^3$ y $\xi_1 \neq 0$, deducimos que $(\xi_2/\xi_1)^2 = 1 + \xi_1$ se satisface en $\mathbb{C}(\overline{\mathcal{D}})$. Por lo tanto ξ_2/ξ_1 es entera sobre $\mathbb{C}[\overline{\mathcal{D}}]$ y $(\xi_2/\xi_1)^2 - 1$ pertenece a $\mathfrak{M}_\mathbf{0} R_\vartheta$. Esto implica que ξ_2/ξ_1 es un elemento de R_ϑ y que se satisface la identidad $(\vartheta(\xi_2/\xi_1))^2 = 1$. Obsérvese que $\vartheta(\xi_1) = \vartheta(\xi_2) = 0$ y $\vartheta(2 + \xi_1) = 2$. A partir del desarrollo de Taylor del polinomio f en $\mathbf{0}$ vemos que existen polinomios Q_1, Q_2, Q_3 of $\Pi^{(2)}$ tales que

$$\frac{f(\xi) - f(\mathbf{0})}{\xi_1} = \frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\xi_2}{\xi_1}\frac{\partial f}{\partial X_2}(\mathbf{0}) + \xi_1 Q_1(\xi) + \frac{\xi_2^2}{\xi_1} Q_2(\xi) + \xi_2 Q_3(\xi)$$

se satisface en $\mathbb{C}(\overline{\mathcal{M}})$. Esto implica que

$$\vartheta\Big(\frac{f(\xi) - f(\mathbf{0})}{\xi_1(2 + \xi_1)}\Big) = \frac{1}{2}\Big(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \vartheta\Big(\frac{\xi_2}{\xi_1}\Big)\frac{\partial f}{\partial X_2}(\mathbf{0})\Big).$$

Por otra parte tenemos que $\xi_1^2+\xi_2^2=\xi_1^2(2+\xi_1)$, lo que prueba que

$$\Psi_2(\xi)=\frac{f(\xi)-f(\mathbf{0})}{\xi_1(2+\xi_1)},\ \Psi_3(\xi)=\frac{f(\xi)-f(\mathbf{0})}{\xi_1(2+\xi_1)}\frac{\xi_2}{\xi_1}.$$

Por lo tanto el place ϑ tiene en $\Psi_2(\xi)$ y $\Psi_3(\xi)$ valores finitos:

$$\vartheta(\Psi_2(\xi))=\frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0})+\vartheta\Big(\frac{\xi_2}{\xi_1}\Big)\frac{\partial f}{\partial X_2}(\mathbf{0})\right),\ \vartheta(\Psi_3(\xi))=\frac{1}{2}\left(\vartheta\Big(\frac{\xi_2}{\xi_1}\Big)\frac{\partial f}{\partial X_1}(\mathbf{0})+\frac{\partial f}{\partial X_2}(\mathbf{0})\right).$$

Por hipótesis $\big(\partial f/\partial X_1(\mathbf{0}),\partial f/\partial X_2(\mathbf{0})\big)\neq\mathbf{0}$. Por lo tanto, la condición $\vartheta(\Psi(\xi))=\Psi(\mathbf{0})$ equivale a la condición $\vartheta(\xi_2/\xi_1)=1$.

Sea T una nueva indeterminada sobre $\mathbb{C}$ y sea $\mathbb{C}[\![T]\!]$ el anillo de las series formales de potencias en T con coeficientes en $\mathbb{C}$. Sea $\sigma\in\mathbb{C}[\![T]\!]$ la única serie de potencias formal que satisface la condición $\sigma^2=1+T$ y $\sigma(0)=-1$. Considérese el homomorfismo de $\mathbb{C}$–álgebras $\chi:\mathbb{C}[\mathcal{C}]\to\mathbb{C}[\![T]\!]$ definido por $\chi(\xi_1):=T$ y $\chi(\xi_2):=T\sigma(T)$. Obsérvese que, puesto que la identidad $(T\sigma)^2=T^2+T^3$ se satisface en $\mathbb{C}[\![T]\!]$, χ está bien definido. Además, χ es inyectiva ya que Y^2-1-T es el polinomio minimal de σ sobre $\mathbb{C}(T)$. Concluimos que χ admite una extensión bien definida $\mathbb{C}(\mathcal{C})\to\mathbb{C}(\!(T)\!)$, que también denotamos por χ. Finalmente, sea $\nu:\mathbb{C}(\!(T)\!)\to\mathbb{C}$ el único place que extiende la evaluación en 0 y sea $\epsilon:\mathbb{C}(\mathcal{C})\to\mathbb{C}$ la composición $\epsilon:=\nu\circ\chi$.

Teniendo en cuenta que $\epsilon(\xi_1)=\nu(T)=0$ y $\epsilon(\xi_2)=\nu(T)\cdot\nu(\sigma)=0$, concluimos que $\epsilon:\mathbb{C}(\mathcal{C})\to\mathbb{C}$ es un place que extiende el homomorfismo evaluación de $\mathbb{C}[\mathcal{C}]$ en el punto $\mathbf{0}$. Además, tenemos que

$$\epsilon(\xi_2/\xi_1)=\nu\big(\chi(\xi_2)/\chi(\xi_1)\big)=\nu(\sigma)=\sigma(0)=-1.$$

Como hemos visto anteriormente, $\epsilon(\xi_2/\xi_1)\neq 1$ implica que $\epsilon\big(\Psi(\xi)\big)\neq\Psi(\mathbf{0})$. Por lo tanto, la aplicación Ψ no es geométricamente robusta.

Capítulo 11

Cotas inferiores para problemas de interpolación de Hermite–Lagrange

Esta sección está dedicada a presentar los resultados principales sobre complejidad para problemas de interpolación. Más precisamente, vamos a exhibir cotas inferiores de complejidad (en el sentido de la Sección 9.2.4) para algoritmos (típicamente geométricamente robustos) que resuelven problemas de interpolación de Lagrange particulares. Las cotas inferiores de complejidad están expresadas en términos del número K de nodos involucrados en la interpolación de Lagrange en consideración y pueden ser lineales en K (resultados de incompresibilidad) o exponenciales en K.

11.1. Resultados de incompresibilidad

En esta sección exhibiremos dos problemas de interpolación de Lagrange con K nodos que requieren algoritmos de complejidad al menos K para su solución. Primero consideramos la complejidad de la interpolación de Lagrange *genérica* por polinomios n–variados de grado a lo sumo D. Luego exhibimos un problema de interpolación de Lagrange con K nodos tal que los interpolantes pueden ser evaluados (en principio) usando $\mathcal{O}(\log K)$ operaciones aritméticas. Sin embargo, todo algoritmo *geométricamente robusto* que resuelve este problema requiere una estructura de datos de salida de tamaño al menos K. En particular no es posible recuperar la representación por straight–line programs de longitud $\mathcal{O}(\log K)$ de los interpolantes por medio de un algoritmo de interpolación geométricamente robusto.

11.1.1. Problemas n–variados genéricos de interpolación de Lagrange

Sean n, D, K y M números naturales y sea $\mathcal{D}$ un subconjunto construible denso Zariski de $\mathbb{A}^{(n+1)\times K}$ que servirá como estructura de datos de entrada para los problemas de interpolación que vamos a considerar en esta sección. Obsérvese que el

tamaño N de la estructura de datos de entrada $\mathcal{D}$ es $(n+1)K$.

Un *problema de interpolación de Lagrange n–variado genérico* en $\Pi_D^{(n)}$ está determinado por $\mathcal{D}$ y una aplicación topológicamente robusta y hereditaria $\Phi : \mathcal{D} \to \Pi_D^{(n)}$, tal que para todo dato de entrada $d := (x_1, y_1, \ldots, x_K, y_K) \in \mathcal{D}$ con $x_1, \ldots, x_K \in \mathbb{A}^n$ e $y_1, \ldots, y_K \in \mathbb{A}^1$, el polinomio $\Phi(d)$ satisface las condiciones $\Phi(d)(x_j) = y_j$ para $1 \leq j \leq K$. Para tal problema de interpolación, el conjunto construible $\mathcal{O} := \Phi(\mathcal{D})$ constituye la clase de interpolantes.

Con estas notaciones e hipótesis tenemos el siguiente resultado de incompresibilidad.

Proposición 11.1.1. *Sea $\mathcal{D}^*$ un subconjunto construible de $\mathbb{A}^M$, $\omega^* : \mathcal{D}^* \to \mathcal{O}$ una codificación polinomial de la clase de interpolantes $\mathcal{O}$ y $\Psi : \mathcal{D} \to \mathcal{D}^*$ una aplicación construible hereditaria, tal que $\mathcal{D}^*, \Psi$ y ω^* determinan un algoritmo que resuelve el problema de interpolación de Lagrange genérico n–variado dado por $\mathcal{D}$ y Φ. Entonces $M \geq K$, es decir, la complejidad del algoritmo de interpolación de Lagrange determinado por $\mathcal{D}^*, \omega^*$ y Ψ es al menos $K = N/(n+1)$.*

Demostración. Puesto que $\mathcal{D}$ es construible, existe un subconjunto abierto Zariski no vacío $\mathcal{U}$ de $\mathbb{A}^{(n+1)\times K}$ que está contenido en $\mathcal{D}$. Elegimos ahora un punto $\gamma := (\gamma_1, \ldots, \gamma_K)$ de $\mathbb{A}^{n\times K}$ con $\gamma_j \in \mathbb{A}^n$, $1 \leq j \leq K$, tal que el conjunto

$$\mathcal{D}_\gamma := \{(y_1, \ldots, y_K) \in \mathbb{A}^K \ : \ (\gamma_1, y_1, \ldots, \gamma_K, y_K) \in \mathcal{U}\}$$

es denso Zariski en $\mathbb{A}^K$. Tal punto $\gamma \in \mathbb{A}^{n\times K}$ puede obtenerse como la imagen de un punto de $\mathcal{U}$ por la proyección canónica $\mathbb{A}^{(n+1)\times K} \to \mathbb{A}^{n\times K}$.

Sean $\varphi_1 : \mathcal{D}_\gamma \to \mathcal{D}^*$ y $\varphi_2 : \mathcal{D}^* \to \mathbb{A}^K$ las aplicaciones construibles definidas por $\varphi_1(y) := \Psi(\gamma, y)$ y $\varphi_2(d^*) := (\omega^*(d^*)(\gamma_1), \ldots, \omega^*(d^*)(\gamma_K))$. Puesto que $\mathcal{D}^*$, ω^* y Ψ determinan un algoritmo que resuelve el problema de interpolación de Lagrange dado por $\mathcal{D}$ y Φ, vale que $\omega^* \circ \Psi = \Phi$. Esto implica que para todo $y \in \mathcal{D}_\gamma$ se satisface la identidad

$$\begin{aligned} \varphi_2 \circ \varphi_1(y) = \varphi_2(\Psi(\gamma, y)) &= \big(\omega^*(\Psi(\gamma, y))(\gamma_1), \ldots, \omega^*(\Psi(\gamma, y))(\gamma_K)\big) \\ &= (\Phi(\gamma, y)(\gamma_1), \ldots, \Phi(\gamma, y)(\gamma_K)) \quad = \quad y. \end{aligned}$$

Por lo tanto $\varphi_2 \circ \varphi_1 = \mathrm{id}_{\mathcal{D}_\gamma}$. Obtenemos las siguientes estimaciones:

$$M = \dim \mathbb{A}^M \geq \dim \overline{\mathcal{D}^*} \geq \dim \overline{\varphi_1(\mathcal{D}_\gamma)} \geq \dim \overline{\varphi_2 \circ \varphi_1(\mathcal{D}_\gamma)} = \dim \overline{\mathcal{D}_\gamma} = \dim \mathbb{A}^K = K,$$

que implican la conclusión de la Proposición 11.1.1. □

11.1.2. Un problema de interpolación de Lagrange incompresible con interpolantes "fáciles de evaluar"

El siguiente ejemplo de un problema de interpolación de Lagrange se encuentra en [CGH+03], donde es analizado desde un punto de vista diferente.

Sean K y M números naturales con $K \geq 2$, sea $N := 2K$, $D := K-1$, $\Pi := \Pi^{(1)}$, sean T y X indeterminadas sobre $\mathbb{C}$ y sea

$$F(X,T) := (T^{D+1}-1)\sum_{k=0}^{D} T^k X^k.$$

Nuestra estructura de datos de entrada es el conjunto construible

$$\mathcal{D} := \{(x_1, y_1, \ldots, x_K, y_K) \in \mathbb{A}^N \,:\, \exists\, t \in \mathbb{C} \,\text{con}\, F(x_i,t) = y_i \text{ para } 1 \leq i \leq K \\ \text{y } x_i \neq x_j \text{ para todo } 1 \leq i < j \leq K\}.$$

Observamos que $\mathcal{D}$ es irreducible. Para ver esto, sea $\mathcal{U} := \{(x_1, \ldots, x_K) \in \mathbb{A}^K : x_i \neq x_j \text{ para } 1 \leq i < j \leq K\}$ y sea $\sigma : \mathcal{U} \times \mathbb{A}^1 \to \mathbb{A}^N$ la aplicación polinomial definida por $\sigma(x,t) := (x_1, F(x_1,t), \ldots, x_K, F(x_K,t))$. Claramente $\mathcal{D}$ es la imagen de σ y por lo tanto irreducible.

Además, para todo $d \in \mathcal{D}$ la fibra $\sigma^{-1}(d)$ es un conjunto finito no vacío (i.e., una variedad algebraica cero-dimensional) y por lo tanto el Teorema 2.1.12 implica que

$$\dim \overline{\mathcal{D}} = \dim \overline{\sigma(\mathcal{U} \times \mathbb{A}^1)} = \dim \overline{\mathcal{U} \times \mathbb{A}^1} = \dim \overline{\mathcal{U}} \times \mathbb{A}^1 = \dim \mathbb{A}^K \times \mathbb{A}^1 = K+1.$$

Sea $\Phi : \mathcal{D} \to \Pi_D$ la aplicación construible que asocia a cada dato de interpolación $d := (x_1, y_1, \ldots, x_K, y_K)$ de $\mathcal{D}$ el *único* polinomio $\Phi(d)$ de Π_D que satisface la condición $\Phi(d)(x_j) = y_j$ para $1 \leq j \leq K$. Teniendo en cuenta la definición de $\mathcal{D}$, vemos que existe un punto (no necesariamente único) $t \in \mathbb{A}^1$ tal que $\Phi(d) = F(X,t)$. A partir de la discusión en la Sección 10.3.1 se deduce fácilmente que Φ es una aplicación regular. Por lo tanto Φ es geométricamente robusta y por lo tanto también topológicamente robusta y hereditaria. En consecuencia $\mathcal{D}$ y Φ determinan un problema de interpolación de Lagrange en el sentido de la Definición 9.2.1.

Obsérvese que la estructura de datos de entrada $\mathcal{D}$ de este problema de interpolación no es densa en su espacio ambiente $\mathbb{A}^N$, puesto que $\dim \overline{\mathcal{D}} = K+1 < 2K = N = \dim \mathbb{A}^N$. Por lo tanto nuestro problema de interpolación de Lagrange no es genérico como el de la Sección 11.1.1.

Denotemos por $\mathcal{O} := \{F(X,t) : t \in \mathbb{C}\}$ la clase de interpolantes del problema de interpolación de Lagrange determinado por $\mathcal{D}$ y Φ. A partir de la definición de F se sigue que todo interpolante $f \in \mathcal{O}$ puede ser evaluado por un straight–line program libre de divisiones de longitud $\mathcal{O}(\log D) = \mathcal{O}(\log K)$. Por lo tanto f es un polinomio univariado que es "fácil de evaluar" (para esta noción y el contexto, ver [BCS97]). Ésta es otra característica particular de nuestro problema de interpolación de Lagrange particular.

Proposición 11.1.2. *Sean las notaciones e hipótesis como antes. Sea un subconjunto construible $\mathcal{D}^*$ de $\mathbb{A}^M$, una codificación polinomial $\omega^* : \mathcal{D}^* \to \Pi_D$ del espacio de interpolantes $\mathcal{O}$ y una aplicación geométricamente robusta $\Psi : \mathcal{D} \to \mathcal{D}^*$ tal que $\mathcal{D}^*$, ω^* y Ψ determinan un algoritmo que resuelve el problema de interpolación de Lagrange representado por $\mathcal{D}$ y Φ (tal solución existe para un número natural adecuado M, puesto que Φ es geométricamente robusta). Entonces $M \geq K$, es decir, la complejidad del algoritmo de interpolación de Lagrange determinado por $\mathcal{D}^*, \omega^*$ y Ψ es al menos $K = N/2$.*

Demostración. Denótese por $\mathbb{G}_D$ el subconjunto de $\mathbb{A}^1$ que consiste de las raíces $(D+1)$-ésimas de la unidad y sean $\psi_1, \ldots, \psi_M$ las componentes de $\Psi : \mathcal{D} \to \mathcal{D}^*$. Por el Lema 9.1.1 existe un subconjunto abierto Zariski no vacío $\mathcal{U}$ de $\overline{\mathcal{D}}$ contenido en $\mathcal{D}$ donde $\psi_1, \ldots, \psi_M$ son funciones racionales regulares (esto es, están bien definidas).

Sea T una nueva indeterminada. Fijamos un punto arbitrario $(a_1, b_1, \ldots, a_K, b_K)$ de $\mathcal{U}$ y escribimos $a := (a_1, \ldots, a_K)$. Consideramos la aplicación polinomial $\varepsilon : \mathbb{A}^1 \to \mathcal{D}$ definida por

$$\varepsilon(t) := (a_1, F(a_1, t), \ldots, a_K, F(a_K, t)).$$

Existe $t_0 \in \mathbb{C}$ con $F(a_1, t_0) = b_1, \ldots, F(a_K, t_0) = b_K$; por lo tanto la imagen de ε y $\mathcal{U}$ tienen intersección no vacía. Esto implica que $\lambda_1 := \psi_1 \circ \varepsilon, \ldots, \lambda_M := \psi_M \circ \varepsilon$ son funciones racionales bien definidas que pertenecen a $\mathbb{C}(T)$. Además, para todo $\zeta \in \mathbb{G}_D$ tenemos que $\varepsilon(\zeta) = (a_1, 0, \ldots, a_K, 0)$.

Afirmación *Las funciones racionales $\lambda_1, \ldots, \lambda_M$ están bien definidas en todo punto de $\zeta \in \mathbb{G}_D$ y los valores $\lambda_1(\zeta), \ldots, \lambda_M(\zeta)$ son independientes de la elección de $\zeta \in \mathbb{G}_D$.*

Demostración de la Afirmación Considérese una raíz $(D+1)$-ésima de la unidad arbitraria $\zeta \in \mathbb{G}_D$ y un índice arbitrario $1 \leq j \leq M$.

Sea $\mathfrak{M}$ el ideal maximal de las funciones coordenadas de $\mathbb{C}[\overline{\mathcal{D}}]$ que se anulan en el punto $\alpha := (a_1, 0, \ldots, a_K, 0) = \varepsilon(\zeta)$ de $\overline{\mathcal{D}}$. Puesto que por hipótesis Ψ es geométricamente robusta, existen $s \in \mathbb{N}$ y $p_0, \ldots, p_{s-1} \in \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}}$ tales que la identidad

$$\psi_j^s + p_{s-1}\psi_j^{s-1} + \cdots + p_0 = 0 \tag{11.1}$$

se satisface en $\mathbb{C}(\overline{\mathcal{D}})$. Puesto que las funciones racionales $p_0, \ldots, p_{s-1}$ están bien definidas en el punto α, las composiciones $\pi_0 := p_0 \circ \varepsilon, \ldots, \pi_{s-1} := p_{s-1} \circ \varepsilon$ están bien definidas en ζ. Por lo tanto $\pi_0, \ldots, \pi_{s-1}$ pertenecen al anillo local $\mathbb{C}[T]_{\mathfrak{N}_\zeta}$, donde $\mathfrak{N}_\zeta = \mathbb{C}[T] \cdot (T - \zeta)$ es el ideal maximal generado por $T - \zeta$ en $\mathbb{C}[T]$.

La identidad (11.1) implica que

$$\lambda_j^s + \pi_{s-1}\lambda_j^{s-1} + \cdots + \pi_0 = 0$$

se satisface en $\mathbb{C}[T]_{\mathfrak{N}_\zeta}$. Por lo tanto λ_j es entera sobre $\mathbb{C}[T]_{\mathfrak{N}_\zeta}$. Puesto que λ_j pertenece a $\mathbb{C}(T)$ y $\mathbb{C}[T]_{\mathfrak{N}_\zeta}$ es integralmente cerrada en $\mathbb{C}(T)$, concluimos que $\lambda_j \in \mathbb{C}[T]_{\mathfrak{N}_\zeta}$. Esto significa que la función racional λ_j está bien definida en ζ. Puesto que $\zeta \in \mathbb{G}_D$ fue elegido arbitrariamente concluimos que λ_j está bien definida en *todo* punto $\zeta \in \mathbb{G}_D$. Esto prueba la primera parte de la afirmación para $1 \leq j \leq M$. Ahora vamos a probar la segunda parte.

El morfismo de variedades irreducibles $\varepsilon : \mathbb{A}^1 \to \overline{\mathcal{D}}$ induce un homomorfismo de $\mathbb{C}$–álgebras $\varepsilon^* : \mathbb{C}[\overline{\mathcal{D}}] \to \mathbb{C}[T]$. A partir del Teorema I deducimos que existe un cuerpo Ω que contiene a $\mathbb{C}(T)$ tal que ε^* se puede extender a un place Ω–valuado de $\mathbb{C}(\overline{\mathcal{D}})$ que también denotamos por ε^*. Sea R_{ε^*} el anillo de valuación del place ε^*. Obsérvese que R_{ε^*} contiene a $\mathbb{C}[\overline{\mathcal{D}}]$ y a su localización $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}}$ en el ideal maximal $\mathfrak{M}$. Para ver esto último, nótese que para $h \in \mathbb{C}[\overline{\mathcal{D}}] \setminus \mathfrak{M}$ y $\zeta \in \mathbb{G}_D$ resulta $\varepsilon^*(h)(\zeta) = (h \circ \varepsilon)(\zeta) = h(\alpha) \neq 0$, y por lo tanto $\varepsilon^*(h) \neq 0$. Esto implica que $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}} \subset R_{\varepsilon^*}$. Por lo tanto la identidad (11.1) implica que $\varepsilon^*(\psi_j)$ es finita. Además,

puesto que ψ_j es una función racional de $\mathbb{C}(\overline{\mathcal{D}})$ y la composición $\psi_j \circ \varepsilon$ está bien definida, tenemos que $\varepsilon^*(\psi_j) = \psi_j \circ \varepsilon = \lambda_j$.

Sean ζ y η elementos arbitrarios de $\mathbb{G}_D$. Entonces ζ y η inducen por evaluación dos homomorfismos de $\mathbb{C}$–álgebras $\mu_\zeta : \mathbb{C}[T] \to \mathbb{C}$ y $\mu_\eta : \mathbb{C}[T] \to \mathbb{C}$. A partir del Teorema I concluimos que μ_ζ y μ_η se pueden extender a dos places $\mathbb{C}$–valuados de Ω que también denotamos por μ_ζ y μ_η. Sean R_{μ_ζ} y R_{μ_η} los anillos de valuación de los places μ_ζ y μ_η. Entonces R_{μ_ζ} contiene a $\mathbb{C}[T]_{\mathfrak{N}_\zeta}$ y R_{μ_η} contiene a $\mathbb{C}[T]_{\mathfrak{N}_\eta}$. Componiendo ahora la evaluación ε^* con la valuación μ_ζ, y con la valuación μ_η, obtenemos dos valuaciones $\mathbb{C}$–valuadas ν_ζ y ν_η de $\mathbb{C}(\overline{\mathcal{D}})$ que extienden la evaluación de las funciones coordenadas de $\mathbb{C}[\overline{\mathcal{D}}]$ en el punto $\alpha \in \mathcal{D}$. Puesto que por hipótesis Ψ es geométricamente robusta tenemos que $\nu_\zeta(\psi_j) = \nu_\eta(\psi_j)$. Por otra parte, como $\lambda_j \in \mathbb{C}[T]_{\mathfrak{N}_\zeta}$ deducimos que $\nu_\zeta(\psi_j) = \mu_\zeta(\varepsilon^*(\psi_j)) = \mu_\zeta(\lambda_j) = \lambda_j(\zeta)$ y similarmente $\nu_\eta(\psi_j) = \lambda_j(\eta)$. Esto implica $\lambda_j(\zeta) = \lambda_j(\eta)$. Por lo tanto el valor de $\lambda_j(\zeta)$ no depende de $\zeta \in \mathbb{G}_D$. Puesto que $1 \leq j \leq M$ fue elegido arbitrariamente, queda demostrada la afirmación. ■

Concluimos que $\lambda := (\lambda_1, \ldots, \lambda_M)$ es una aplicación racional de $\mathbb{C}(T)^M$ bien definida en todo punto $\zeta \in \mathbb{G}_D$ cuyo valor $\alpha^* := \lambda(\zeta)$ es independiente de ζ.

Considérese ahora la aplicación polinomial $\varphi : \mathcal{D}^* \to \mathbb{A}^K$ definida por $\varphi(h) := (\omega^*(h)(a_1), \ldots, \omega^*(h)(a_K))$. Obsérvese que $\theta := \varphi \circ \lambda$ es una aplicación racional bien definida (con dominio maximal) de $\mathbb{A}^1$ en $\mathbb{A}^K$. Para todo punto $t \in \mathbb{A}^1$ tal que ψ_j está bien definida en $\varepsilon(t)$ tenemos que

$$\begin{aligned}\theta(t) = \varphi(\lambda(t)) = \varphi(\Psi(\varepsilon(t))) &= (\omega^*(\Psi(\varepsilon(t)))(a_1), \ldots, \omega^*(\Psi(\varepsilon(t)))(a_K)) \\ &= (\Phi(\varepsilon(t))(a_1), \ldots, \Phi(\varepsilon(t))(a_K)) \\ &= (F(a_1, t), \ldots, F(a_K, t)).\end{aligned}$$

Por lo tanto θ es una aplicación polinomial de $\mathbb{A}^1$ en $\mathbb{A}^K$ y está bien definida en todo punto t de $\mathbb{A}^1$.

Dado que

$$\frac{\partial}{\partial T}F(T, X) = (D+1)T^D \sum_{k=0}^{D} T^k X^k + (T^{D+1} - 1)\frac{\partial}{\partial T}\sum_{k=0}^{D} T^k X^k,$$

deducimos que para todo $\zeta \in \mathbb{G}_D$ y todo $x \in \mathbb{A}^1$ se satisface la identidad

$$\frac{\partial F}{\partial T}(\zeta, x) = (D+1)\zeta^D \sum_{k=0}^{D} \zeta^k x^k.$$

Sean $\zeta_1, \ldots, \zeta_{D+1}$ los (distintos) elementos de $\mathbb{G}_D$. La regla de la cadena y la afirmación anterior implican ahora que para $1 \leq \ell \leq D+1$ la identidad

$$\begin{aligned}(D+1)\zeta_\ell^D \begin{pmatrix} \sum_{k=0}^{D} \zeta_\ell^k a_1^k \\ \vdots \\ \sum_{k=0}^{D} \zeta_\ell^k a_K^k \end{pmatrix} &= (d\theta)(\zeta_\ell) \\ &= (d\varphi)(\lambda(\zeta_\ell)) \cdot (d\lambda)(\zeta_\ell) = (d\varphi)(\alpha^*) \cdot (d\lambda)(\zeta_\ell) \quad (11.2)\end{aligned}$$

tiene sentido y es válida (aquí $(d\theta)(\zeta_\ell)$, $(d\varphi)(\lambda(\zeta_\ell))$ y $(d\lambda)(\zeta_\ell)$ denotan las matrices Jacobianas de θ, φ y λ en los puntos ζ_ℓ, $\lambda(\zeta_\ell)$ y ζ_ℓ respectivamente).

Para $1 \leq \ell \leq D+1$ sea $v_\ell := ((D+1)\zeta_\ell^D)^{-1}((d\theta)(\zeta_\ell))$ y sea C la $(K \times M)$–matriz compleja $C := (d\varphi)(\alpha^*)$ (que es independiente del índice ℓ). Obsérvese que $K = D+1$. A partir de (11.2) deducimos que $v_1, \ldots, v_K$ son combinaciones $\mathbb{C}$–lineales de las columnas de C. Afirmamos que $v_1, \ldots, v_K$ son $\mathbb{C}$–linealmente independientes. Para ver esto, sea $\mathcal{V}$ la $(K \times K)$–matriz compleja cuya vectores columna son $v_1, \ldots, v_K$, $V_K := (\zeta_\ell^{k-1})_{1\leq \ell,k\leq K}$ y $W_\alpha := (a_\ell^{k-1})_{1\leq \ell,k\leq K}$. Entonces tenemos que $\mathcal{V} = W_\alpha V_K^t$. Puesto que V_K y W_α son matrices de Vandermonde inversibles concluimos que $\mathcal{V}$ es de rango maximal K. Esto implica que el rango de $C \in \mathbb{C}^{K\times M}$ es al menos K y por lo tanto que $M \geq K = N/2$. Esto demuestra la Proposición 11.1.2. □

11.2. Polinomios codificados por straight–line programs: interpolación de Lagrange es difícil

Sean n, L, M números naturales con $2^{L/4} \geq n$, $K := 4(L+n+1)^2+2$ y $N := K$. En términos de las nociones y notaciones introducidas en las Secciones 9.2.1 y 9.2.3, ahora vamos a mostrar que todo algoritmo de interpolación *geométricamente robusto*, que reconstruye los polinomios n–variados que pueden ser evaluados por un straight–line program sin divisiones de longitud no escalar a lo sumo L a partir de sus valores en una sucesión de identificación de longitud K, tiene complejidad exponencial de orden $2^{\Omega(Ln)} = 2^{\Omega(\sqrt{K})} = 2^{\Omega(\sqrt{N})}$. Esto significa que la interpolación de Lagrange tradicional en $n_L := \binom{2^L+n}{n} = 2^{\mathcal{O}(Ln)}$ nodos es esencialmente óptima para esta muy especial clase de polinomios.

El siguiente resultado, con una cota de complejidad ligeramente menos fina, fue exhibida en [HK04] en el contexto de bases de datos con restricciones.

Teorema 11.2.1. *Con las notaciones y las hipótesis anteriores, sea $\mathcal{D}$ el subconjunto construible irreducible de $\mathbb{A}^N$ y $\Phi : \mathcal{D} \to \Pi_{2^L}^{(n)}$ la aplicación geométricamente robusta introducida en la Sección 9.2.3. Por lo tanto $\mathcal{D}$ y Φ determinan un problema de interpolación de Lagrange en el sentido de la Definición 9.2.1 y los interpolantes $\mathcal{O} := \Phi(\mathcal{D})$ son los polinomios en $\Pi^{(n)}$ que pueden ser evaluados por un straight–line program sin divisiones de longitud no escalar a lo sumo L.*

Sean $\mathcal{D}^*$ un subconjunto construible de $\mathbb{A}^M$, $\omega^* : \mathcal{D}^* \to \mathcal{O}$ una codificación polinomial de la clase de interpolantes $\mathcal{O}$ y $\Psi : \mathcal{D} \to \mathcal{D}^*$ una aplicación geométricamente robusta tales que $\mathcal{D}^*$, ω^* y Ψ determinan un algoritmo que resuelve el problema de interpolación de Lagrange representado por $\mathcal{D}$ y Φ (tal solución existe para un número natural M adecuado, puesto que Φ es geométricamente robusta). Entonces

$$M \geq \binom{2^{\lfloor \frac{L}{2}+1 \rfloor} - 1 + n}{n} = 2^{\Omega(Ln)} = 2^{\Omega(\sqrt{K})} = 2^{\Omega(\sqrt{N})}.$$

En otras palabras, la complejidad del algoritmo de interpolación de Lagrange determinado por $\mathcal{D}^*, \omega^*$ y Ψ es al menos exponencial en L y n o alternativamente en $\sqrt{K} = \sqrt{N}$.

Demostración. Sea $\ell := \lfloor \frac{L}{2} + 1 \rfloor$ y sea $\mathcal{Y}$ el subconjunto de $\Pi_{2^L} := \Pi_{2^L}^{(n)}$ definido por

$$\mathcal{Y} := \left\{ t \sum_{k=0}^{2^\ell - 1} (\lambda_1 X_1 + \cdots + \lambda_n X_n)^k : (t, \lambda_1, \ldots, \lambda_n) \in \mathbb{A}^{n+1} \right\}.$$

Teniendo en cuenta que todo polinomio $h \in \mathcal{Y}$ se puede evaluar por un straight–line program libre de divisiones de longitud no escalar a lo sumo $2(\ell - 1)$, concluimos que $\mathcal{Y}$ está contenido en la clase de interpolantes $\mathcal{O}$. Denotemos con $\overline{\mathcal{Y}}$ la clausura Zariski de $\mathcal{Y}$ en su espacio ambiente $\mathbb{A}^{n_L}$ (aquí identificamos Π_{2^L} con $\mathbb{A}^{n_L}$). Obsérvese que $\overline{\mathcal{Y}}$ es una subvariedad afín irreducible de $\overline{\mathcal{O}}$, puesto que $\overline{\mathcal{Y}}$ es la clausura Zariski de la imagen de un morfismo polinomial que aplica la variedad afín irreducible $\mathbb{A}^{n+1}$ en $\mathbb{A}^{n_L}$.

En la Sección 9.2.3 fijamos puntos $\gamma_1, \ldots, \gamma_K$ de $\mathbb{A}^n$ (más precisamente, puntos enteros de longitud bit a lo sumo $4(L+1) \leq 2\sqrt{K}$) tales que $\gamma := (\gamma_1, \ldots, \gamma_K)$ resulta una sucesión de identificación para la clase de polinomios $\overline{\mathcal{O}}$. Sea $\Xi : \overline{\mathcal{O}} \to \mathbb{A}^N$ la aplicación polinomial definida por $\Xi(f) := (f(\gamma_1), \ldots, f(\gamma_K))$. Recuérdese que $\mathcal{D} := \Xi(\mathcal{O})$.

Entonces $\overline{\mathcal{D}}$ es una subvariedad afín, cerrada e irreducible de $\mathbb{A}^N = \mathbb{A}^K$ y $\Xi : \overline{\mathcal{O}} \to \overline{\mathcal{D}}$ es un morfismo finito, birracional de variedades afines irreducibles, que es un homeomorfismo (con respecto a la topología fuerte). En particular, la aplicación $\Phi := \Xi^{-1} : \mathcal{D} \to \Pi_{2^L}$ es geométricamente robusta y $\mathcal{D}$ y Φ determinan el problema de interpolación de Lagrange en consideración.

Sea $\mathcal{Z}$ el subconjunto construible irreducible de $\overline{\mathcal{D}} \subset \mathbb{A}^N$ definido por $\mathcal{Z} := \Xi(\overline{\mathcal{Y}})$. Obsérvese que $\mathcal{Z}$ es cerrado Zariski puesto que $\Xi : \overline{\mathcal{O}} \to \overline{\mathcal{D}}$ es un morfismo finito de variedades afines. Por lo tanto $\mathcal{Z}$ es una subvariedad afín cerrada e irreducible de $\overline{\mathcal{D}}$ y $\mathbb{A}^N$. Obsérvese que el punto $(0, \ldots, 0) \in \mathbb{A}^N$ pertenece a $\mathcal{Z} \cap \mathcal{D}$. Además, del hecho de que $\Xi : \overline{\mathcal{O}} \to \overline{\mathcal{D}}$ es un homeomorfismo se sigue también fácilmente que $\mathcal{Z}$ es cerrado en la topología fuerte.

Sean $\psi_1, \ldots, \psi_M$ las componentes de la aplicación construible dada $\Psi : \mathcal{D} \to \mathbb{A}^M$. De acuerdo con el Lema 9.1.1, existe una subvariedad afín abierta (no vacía Zariski) $\mathcal{U}$ de $\overline{\mathcal{D}}$ con $\mathcal{U} \subset \mathcal{D}$, donde las funciones racionales $\psi_1, \ldots, \psi_M$ son regulares. Por lo tanto $\psi_1|_{\mathcal{U}}, \ldots, \psi_M|_{\mathcal{U}}$ son funciones coordenadas de la $\mathbb{C}$–álgebra $\mathbb{C}[\mathcal{U}]$ que está contenida en el cuerpo de funciones racionales $\mathbb{C}(\overline{\mathcal{D}})$.

Por el Teorema 10.2.10, existen funciones racionales $\eta_1, \ldots, \eta_M$ de $\mathbb{C}(\mathcal{Z})$ tales que, para todo punto z de la intersección de sus dominios y $\mathcal{D}$, se satisface la condición $\eta_1(z) = \psi_1(z), \ldots, \eta_M(z) = \psi_M(z)$. Además, si $\mathfrak{M}$ denota el ideal anulador (maximal) de $\mathbb{C}[\mathcal{Z}]$ en el punto $(0, \ldots, 0) \in \mathcal{Z} \cap \mathcal{D}$, puesto que por hipótesis Ψ es geométricamente robusta y $\mathcal{Z}$ es una subvariedad cerrada irreducible de $\overline{\mathcal{D}}$, las funciones racionales $\eta_1, \ldots, \eta_M$ son enteras sobre $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}}$ (ver también la Proposición 10.2.9 y el Teorema 10.2.2). Por lo tanto existen $s \in \mathbb{N}$ y funciones racionales $p_{ij} \in \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}}$, $0 \leq i \leq s-1$, $1 \leq j \leq M$, tales que

$$\eta_j^s + p_{s-1j} \eta_j^{s-1} + \cdots + p_{0j} = 0 \tag{11.3}$$

se satisface en $\mathbb{C}(\mathcal{Z})$ para todo $1 \leq j \leq M$.

Sean $T, U_1, \ldots, U_n$ y $Y_1, \ldots, Y_K$ nuevas indeterminadas, sea $\boldsymbol{U} := (U_1, \ldots, U_n)$ y $\boldsymbol{X} := (X_1, \ldots, X_n)$, y sea $G_{T,\boldsymbol{U}}$ el polinomio de $\mathbb{C}[T, \boldsymbol{U}, \boldsymbol{X}]$ definido por

$$G_{T,\boldsymbol{U}}(\boldsymbol{X}) := T \sum_{k=0}^{2^\ell - 1} (U_1 X_1 + \cdots + U_n X_n)^k.$$

Además, sea $g_{T,\boldsymbol{U}} := (G_{T,\boldsymbol{U}}(\gamma_1), \ldots, G_{T,\boldsymbol{U}}(\gamma_K))$. Entonces $g_{T,\boldsymbol{U}}$ induce un morfismo dominante de variedades afines $\mathbb{A}^{n+1} \to \mathcal{Z}$. Este morfismo induce un isomorfismo de $\mathbb{C}$–álgebras entre $\mathbb{C}[\mathcal{Z}]$ y $\mathbb{C}[g_{T,\boldsymbol{U}}]$, donde $\mathbb{C}[g_{T,\boldsymbol{U}}]$ se interpreta como la subálgebra de $\mathbb{C}[T, \boldsymbol{U}]$ generada por $G_{T,\boldsymbol{U}}(\gamma_1), \ldots, G_{T,\boldsymbol{U}}(\gamma_K)$. Este isomorfismo aplica el ideal maximal $\mathfrak{M}$ of $\mathbb{C}[\mathcal{Z}]$ en el ideal maximal $\widetilde{\mathfrak{M}}$ de $\mathbb{C}[g_{T,\boldsymbol{U}}]$ generado por $G_{T,\boldsymbol{U}}(\gamma_1), \ldots, G_{T,\boldsymbol{U}}(\gamma_K)$. Además, este isomorfismo aplica las funciones racionales $p_{ij} \in \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}}$, $1 \le i \le s-1$, $1 \le j \le M$, en las funciones racionales $\widetilde{p}_{ij} \in \mathbb{C}[g_{T,\boldsymbol{U}}]_{\widetilde{\mathfrak{M}}}$ e induce un $\mathbb{C}$-isomorfismo de cuerpos entre $\mathbb{C}(\mathcal{Z})$ y $\mathbb{C}(g_{T,\boldsymbol{U}})$ que aplica $\eta_1, \ldots, \eta_K$ en funciones racionales $\widetilde{\eta}_1, \ldots, \widetilde{\eta}_K \in \mathbb{C}(g_{T,\boldsymbol{U}})$. Más precisamente, tenemos que $\widetilde{\eta}_1 = \eta_1 \circ g_{T,\boldsymbol{U}}, \ldots, \widetilde{\eta}_K = \eta_K \circ g_{T,\boldsymbol{U}}$ con composiciones bien definidas.

Sea $\boldsymbol{Y} := (Y_1, \ldots, Y_K)$ y $S := \{P(g_{T,\boldsymbol{U}}) : P \in \mathbb{C}[\boldsymbol{Y}]\ ,\ P(0, \ldots, 0) \ne 0\ \}$. Entonces S es un subconjunto multiplicativo de $\mathbb{C}[g_{T,\boldsymbol{U}}]$ y por lo tanto de $\mathbb{C}[T, \boldsymbol{U}]$. Obsérvese que $\mathbb{C}[g_{T,\boldsymbol{U}}]_{\widetilde{\mathfrak{M}}} = S^{-1}\mathbb{C}[g_{T,\boldsymbol{U}}]$. La identidad (11.3) implica que

$$\widetilde{\eta}_j^s + \widetilde{p}_{s-1j}\widetilde{\eta}_j^{s-1} + \cdots + \widetilde{p}_{0j} = 0 \tag{11.4}$$

en $\mathbb{C}(T, \boldsymbol{U})$ para todo $1 \le j \le M$. Por lo tanto $\widetilde{\eta}_1, \ldots, \widetilde{\eta}_M$ son enteras sobre $\mathbb{C}[g_{T,\boldsymbol{U}}]_{\widetilde{\mathfrak{M}}} = S^{-1}\mathbb{C}[g_{T,\boldsymbol{U}}]$ y en consecuencia sobre $S^{-1}\mathbb{C}[T, \boldsymbol{U}]$. Puesto que $\mathbb{C}[T, \boldsymbol{U}]$ es integralmente cerrado, la $\mathbb{C}$–álgebra $S^{-1}\mathbb{C}[T, \boldsymbol{U}]$ es también integralmente cerrada (ver, por ejemplo, [Lan93, Ch. VII, §1, Proposition 1.9]). Además, $S^{-1}\mathbb{C}[T, \boldsymbol{U}]$ contiene a $S^{-1}\mathbb{C}[g_{T,\boldsymbol{U}}]$. Concluimos que las funciones racionales $\widetilde{\eta}_1, \ldots, \widetilde{\eta}_M$ de $\mathbb{C}(T, \boldsymbol{U})$ pertenecen a $S^{-1}\mathbb{C}[T, \boldsymbol{U}]$.

Sea $\boldsymbol{u}$ un punto arbitrario de $\mathbb{A}^n$ y P un polinomio arbitrario de $\mathbb{C}[\boldsymbol{Y}]$ con $P(0, \ldots, 0) \ne 0$. Tenemos que $G_{0,\boldsymbol{u}} = 0$ y por lo tanto $g_{0,\boldsymbol{u}} = (0, \ldots, 0)$. Esto implica que $P(g_{0,\boldsymbol{u}}) = P(0, \ldots, 0) \ne 0$. Por lo tanto toda función racional de $S^{-1}\mathbb{C}[T, \boldsymbol{U}]$ está bien definida en el punto $(0, \boldsymbol{u}) \in \mathbb{A}^{n+1}$. En particular las funciones racionales $\widetilde{\eta}_j$ y $\widetilde{p}_{ij}$, $1 \le i \le s-1$, $1 \le j \le M$, están bien definidas en $(0, \boldsymbol{u})$. Además, el valor $\alpha_{ij} := \widetilde{p}_{ij}(0, \boldsymbol{u})$ no depende de $\boldsymbol{u}$, puesto que $\widetilde{p}_{ij}$ pertenece a $\mathbb{C}[g_{T,\boldsymbol{U}}]_{\widetilde{\mathfrak{M}}}$.

En consecuencia, (11.4) implica que

$$\widetilde{\eta}_j(0, \boldsymbol{u})^s + \alpha_{s-1,j}\widetilde{\eta}_j(0, \boldsymbol{u})^{s-1} + \cdots + \alpha_{0,j} = 0$$

se satisface en $\mathbb{C}$. Por lo tanto para $\widetilde{\eta}_j(0, \boldsymbol{u})$, $\boldsymbol{u} \in \mathbb{A}^n$, hay sólo finitos valores posibles. Por otra parte, la aplicación $\mathbb{A}^n \to \mathbb{A}^1$ que asigna a cada punto $\boldsymbol{u} \in \mathbb{A}^n$ el valor $\widetilde{\eta}_j(0, \boldsymbol{u}) \in \mathbb{A}^1$ es una función racional que es regular en todo $\mathbb{A}^n$ y por lo tanto una aplicación polinomial cuya imagen consiste de finitos puntos. Concluimos que los valores $\widetilde{\eta}_1(0, \boldsymbol{u}), \ldots, \widetilde{\eta}_M(0, \boldsymbol{u})$ son independientes del punto $\boldsymbol{u} \in \mathbb{A}^n$.

Sea $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$ y, para $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$, sea $|\boldsymbol{\alpha}| := \alpha_1 + \cdots + \alpha_n$. Para un entero no negativo dado m, sea

$$\Sigma_m := \{\boldsymbol{\alpha} \in \mathbb{N}_0^n : |\boldsymbol{\alpha}| \le m\}.$$

Obsérvese que Σ_m consiste de $\binom{m+n}{n}$ elementos.

Puesto que todo polinomio de $\overline{\mathcal{O}}$ tiene grado a lo sumo 2^L, podemos considerar para todo $\boldsymbol{\alpha} \in \Sigma_{2^L}$ con $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n)$ la función coordenada $\theta_{\boldsymbol{\alpha}}$ de $\mathbb{C}[\overline{\mathcal{O}}]$ que proporciona el coeficiente de cada polinomio $f \in \overline{\mathcal{O}}$ que corresponde al monomio $X^{\boldsymbol{\alpha}} := X_1^{\alpha_1} \ldots X_1^{\alpha_n}$. Además, para todo $t \in \mathbb{A}^1$ y todo $\boldsymbol{u} := (u_1, \ldots, u_n) \in \mathbb{A}^n$ tenemos que

$$\begin{aligned} G_{t,\boldsymbol{u}} &= t \sum_{0 \le k \le 2^\ell - 1} \sum_{\substack{\boldsymbol{\alpha} \in \mathbb{N}_0^n \\ |\boldsymbol{\alpha}| = k}} \frac{k!}{\alpha_1! \alpha_2! \ldots \alpha_n!} u_1^{\alpha_1} X_1^{\alpha_1} \ldots u_n^{\alpha_n} X_n^{\alpha_n} \\ &= t \sum_{\substack{\boldsymbol{\alpha} \in \mathbb{N}_0^n \\ 0 \le |\boldsymbol{\alpha}| \le 2^\ell - 1}} \frac{|\boldsymbol{\alpha}|!}{\alpha_1! \alpha_2! \ldots \alpha_n!} u_1^{\alpha_1} X_1^{\alpha_1} \ldots u_n^{\alpha_n} X_n^{\alpha_n}. \end{aligned}$$

Obsérvese que $\deg G_{t,\boldsymbol{u}} \le 2^\ell - 1 \le 2^L$ y que $G_{t,\boldsymbol{u}}$ se puede evaluar por un straight–line program sin divisiones de longitud no escalar $2(\ell - 1) \le L$. Por lo tanto $G_{t,\boldsymbol{u}}$ pertenece a $\Pi_{2^L}^{(n)}$ y en particular a $\mathcal{O}$. Luego para $\boldsymbol{\alpha} \in \Sigma_{2^L}$ el valor $\theta_\alpha(G_{t,\boldsymbol{u}})$ está bien definido y tenemos que

$$\theta_\alpha(G_{t,\boldsymbol{u}}) = \begin{cases} \dfrac{t|\boldsymbol{\alpha}|!}{\alpha_1! \cdots \alpha_n!}\, \boldsymbol{u}^{\boldsymbol{\alpha}}, & \text{si } \boldsymbol{\alpha} \in \Sigma_{2^\ell - 1}; \\ 0, & \text{si } \boldsymbol{\alpha} \in \Sigma_{2^L} \setminus \Sigma_{2^\ell - 1}. \end{cases}$$

Para todo $\rho \in \mathbb{A}^1$, sea $\overline{\rho} := (\rho, \rho^{2^\ell}, \rho^{2^{2\ell}} \ldots, \rho^{2^{(n-1)\ell}})$ y sea $\beta_\rho : \mathbb{A}^1 \to \mathbb{A}^{n+1}$ la aplicación (polinomial) definida por

$$\beta_\rho(t) := (t, \rho, \rho^{2^\ell}, \rho^{2^{2\ell}} \ldots, \rho^{2^{(n-1)\ell}}).$$

A partir de nuestra argumentación anterior, deducimos que la composición

$$\sigma_\rho := \omega^* \circ \widetilde{\eta} \circ \beta_\rho \tag{11.5}$$

está bien definida y es regular en el punto $t := 0$.

Ahora elegimos un pequeño polidisco abierto Δ de $\mathbb{A}^2 = \mathbb{C}^2$ que contenga al origen, tal que para todo $(t, \rho) \in \Delta$ la aplicación racional $\widetilde{\eta}$ está bien definida en $\beta_\rho(t)$. Sea $\eta := (\eta_1, \ldots, \eta_M)$. Entonces para $(t, \rho) \in \Delta$ tenemos las identidades

$$\widetilde{\eta}(\beta_\rho(t)) = \eta(g_{t,\overline{\rho}}) = \Psi(g_{t,\overline{\rho}})$$

y por lo tanto

$$\sigma_\rho(t) = \omega^*(\widetilde{\eta}(\beta_\rho(t))) = \omega^*(\eta(g_{t,\overline{\rho}})) = \omega^*(\Psi(g_{t,\overline{\rho}})) = \Phi(g_{t,\overline{\rho}}) = G_{t,\overline{\rho}}.$$

Esto implica que para todo $\boldsymbol{\alpha} \in \Sigma_{2^L}$ con $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n)$, tenemos que

$$\theta_{\boldsymbol{\alpha}}(\sigma_\rho(t)) = \frac{t\,|\boldsymbol{\alpha}|!}{\alpha_1! \ldots \alpha_n!}\, \overline{\rho}^{\,\boldsymbol{\alpha}} = \frac{t\,|\boldsymbol{\alpha}|!}{\alpha_1! \ldots \alpha_n!}\, \rho^{\alpha_1 + \alpha_2 2^\ell + \alpha_3 2^{2\ell} + \cdots + \alpha_n 2^{(n-1)\ell}} \tag{11.6}$$

si $\boldsymbol{\alpha} \in \Sigma_{2^\ell - 1}$ y $\theta_{\boldsymbol{\alpha}}(\sigma_\rho(t)) = 0$ si $\boldsymbol{\alpha} \in \Sigma_{2^L} \setminus \Sigma_{2^\ell - 1}$.

Obsérvese que los elementos de la sucesión $\left(\alpha_1+\alpha_2 2^{\ell}+\cdots+\alpha_n 2^{(n-1)\ell}\right)_{(\alpha_1,\ldots,\alpha_n)\in\Sigma_{2^\ell-1}}$ son todos distintos, puesto que $(\alpha_1,\ldots,\alpha_n)\in\Sigma_{2^\ell-1}$ implica que $\alpha_1,\ldots,\alpha_n$ son enteros no negativos acotados por $2^\ell-1$.

Fijemos $\rho\in\mathbb{A}^1$ con $(0,\rho)\in\Delta$. Aplicando la regla de la cadena a la composición $\sigma_\rho(t)=\omega^*\circ\widetilde{\eta}\circ\beta_\rho(t)$ con $(t,\rho)\in\Delta$ obtenemos

$$\frac{d}{dt}\sigma_\rho(0)=(d\omega^*)(\widetilde{\eta}(\beta_\rho(0)))\cdot\frac{d}{dt}(\widetilde{\eta}\circ\beta_\rho)(0),$$

donde $(d\sigma_\rho/dt)(0)$ y $(d(\widetilde{\eta}\circ\beta_\rho)/dt)(0)$ denotan las derivadas de σ_ρ y $\widetilde{\eta}\circ\beta_\rho$ respectivamente en el punto $t:=0$ y $(d\omega^*)(\widetilde{\eta}(\beta_\rho(0)))$ la matriz Jacobiana de ω^* en el punto $\widetilde{\eta}(\beta_\rho(0))$. Como vimos anteriormente, el valor

$$\mu:=\widetilde{\eta}(\beta_\rho(0))=\widetilde{\eta}(0,\overline{\rho})=(\widetilde{\eta}_1(0,\overline{\rho}),\ldots,\widetilde{\eta}_K(0,\overline{\rho}))$$

es independiente de ρ.

Sea C la $(n_L\times M)$–matriz Jacobiana de ω^* en μ, es decir, $C:=(d\omega^*)(\widetilde{\eta}(\beta_\rho(0)))=d\omega^*(\mu)$, que es independiente del valor ρ. Entonces

$$\frac{d}{dt}\sigma_\rho(0)=(d\omega^*)(\widetilde{\eta}(\beta_\rho(0)))\cdot\frac{d}{dt}(\widetilde{\eta}\circ\beta_\rho)(0)=C\cdot\frac{d}{dt}(\widetilde{\eta}\circ\beta_\rho)(0)$$

implica que $(d\sigma_\rho/dt)(0)$ es una combinación $\mathbb{C}$–lineal de las columnas de C. Por el Lema 11.2.2 deducimos que existen valores $\rho_l\in\mathbb{C}\setminus\{0\}$, $1\le l\le\#\Sigma_{2^\ell-1}$, con $(0,\rho_l)\in\Delta$ tales que los vectores columna $(d\sigma_{\rho_l}/dt)(0)\in\mathbb{A}^{n_L}$ son $\mathbb{C}$–linealmente independientes. Esto implica que el rango de la $(n_L\times M)$–matriz C es al menos

$$\#\Sigma_{2^\ell-1}=\binom{2^\ell-1+n}{n}=\binom{2^{\lfloor\frac{L}{2}+1\rfloor}-1+n}{n}.$$

Por lo tanto

$$M\ge\binom{2^{\lfloor\frac{L}{2}+1\rfloor}-1+n}{n}.$$

Por la hipótesis $2^{L/4}\ge n$ deducimos que

$$\binom{2^{\lfloor\frac{L}{2}+1\rfloor}-1+n}{n}\ge\frac{(2^{\frac{L}{2}}-1)^n}{n!}\ge\frac{(2^{\frac{L}{2}}-1)^n}{n^n}=2^{\Omega(\frac{L}{2}-\log n)n}=2^{\Omega(Ln)},$$

y dado que $N=K=(L+n+1)^2+2$, concluimos que

$$Ln=\Omega(\sqrt{K})=\Omega(\sqrt{N}).$$

Por lo tanto obtenemos la cota inferior

$$M\ge\binom{2^{\lfloor\frac{L}{2}+1\rfloor}-1+n}{n}=2^{\Omega(Ln)}=2^{\Omega(\sqrt{K})}=2^{\Omega(\sqrt{N})}.$$

Para terminar la demostración del Teorema 11.2.1, utilizamos el siguiente resultado.

Lema 11.2.2. *Sean $m \in \mathbb{N}$, $n_1 < n_2 < \cdots < n_m \in \mathbb{N}_0$ y $a_1, \ldots, a_m \in \mathbb{A}^1 \setminus \{0\}$. Sean $Z_1, \ldots, Z_m$ indeterminadas sobre $\mathbb{C}$ y sea $P := (P_{i,j})_{1 \le i,j \le m} \in \mathbb{C}[Z_1, \ldots, Z_m]^{m \times m}$ la matriz tal que $P_{i,j} := a_j Z_i^{n_j}$ para $1 \le i, j \le m$. Entonces $\det P \neq 0$. En particular, existen elementos $\rho_1, \ldots, \rho_m \in \mathbb{C}$ con norma arbitrariamente pequeña para los cuales la matriz $P(\rho_1, \ldots, \rho_m) = (a_j \rho_i^{n_j})_{1 \le i,j \le m}$ es no singular.*

Demostración. Argumentamos por inducción en m. Puesto que el caso $m = 1$ es obvio, podemos suponer que $m > 1$. Para $1 \le i \le m$, sea Q_i la $(m-1) \times (m-1)$–submatriz de P que se obtiene eliminando la fila número i y la columna número m. Obsérvese que $\det Q_i$ no contiene la indeterminada Z_i. Entonces tenemos

$$\det P = (-1)^{m+1} a_m Z_1^{n_m} \det Q_1 + (-1)^{m+2} a_m Z_2^{n_m} \det Q_2 + \cdots + a_m Z_m^{n_m} \det Q_m.$$

Para todo $1 \le i, j \le m$, tenemos $\deg_{Z_j}(\det Q_i) \le n_{m-1}$. Puesto que Q_1 tiene la forma requerida por el enunciado del lema para el caso $m-1$, podemos aplicar la hipótesis inductiva a Q_1. Por lo tanto $\det Q_1 \neq 0$. Luego $(-1)^{n+m} a_m \det Q_1 \neq 0$ es el coeficiente de la potencia más alta, a saber n_m, de Z_1 en P. Esto implica $\det P \neq 0$. El resto del enunciado del lema es entonces obvio. □

Aplicamos ahora el Lema 11.2.2 a los vectores columna $(d\sigma_\rho/dt)(0) \in \mathbb{A}^{n_L}$ con $(0, \rho) \in \Delta$ y $\rho \neq 0$.

Fin de la demostración del Teorema 11.2.1. Con las notaciones del Lema 11.2.2 y la demostración del Teorema 11.2.1, sea $m := \#\Sigma_{2^\ell - 1} = \binom{2^\ell - 1 + n}{n} = \binom{2^{\lfloor \frac{\ell}{2} \rfloor + 1} - 1 + n}{n}$ y sean $0 \le n_1 < \ldots < n_m$ los elementos de la sucesión $\left(\alpha_1 + \alpha_2 2^\ell + \cdots + \alpha_n 2^{(n-1)\ell}\right)_{(\alpha_1, \ldots, \alpha_n) \in \Sigma_{2^\ell - 1}}$ en forma ordenada (recuérdese que los elementos de esta sucesión son todos distintos). Para $1 \le j \le m$ y $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n) \in \Sigma_{2^\ell - 1}$ con $n_j = \alpha_1 + \alpha_2 2^\ell + \cdots + \alpha_n 2^{(n-1)\ell}$, sea $a_j := |\boldsymbol{\alpha}|!/(\alpha_1! \ldots \alpha_n!)$ y $P \in \mathbb{C}[Z_1, \ldots, Z_m]^{m \times m}$ la $(m \times m)$–matriz del enunciado del Lema 11.2.2. Entonces existen $\rho_1, \ldots, \rho_m \in \mathbb{C}^m$ con $(0, \rho_1) \in \Delta, \ldots, (0, \rho_m) \in \Delta$ tales que $\det P(\rho_1, \ldots, \rho_m) \neq 0$.

Sea H la $(n_L \times m)$–matriz compleja formada por los vectores columna $(d\sigma_{\rho_1}/dt)(0)$, $\ldots$, $(d\sigma_{\rho_m}/dt)(0)$. Entonces las identidades (11.6) de la demostración del Teorema 11.2.1 implican que la $(m \times m)$–submatriz de H determinada por las filas correspondientes a los elementos de $\Sigma_{2^\ell - 1}$ es la matriz $P(\rho_1, \ldots, \rho_m)$. Como $\det P(\rho_1, \ldots, \rho_m) \neq 0$, concluimos que H es de rango maximal m. Por lo tanto, los $m := \#\Sigma_{2^\ell - 1}$ vectores columna $(d\sigma_{\rho_l}/dt)(0) \in \mathbb{A}^{n_L}$, $1 \le l \le m$, son $\mathbb{C}$–linealmente independientes. Esto completa la demostración del Teorema 11.2.1. □

Bibliografía

[ABRW96] M. Alonso, E. Becker, M. F. Roy y T. Wörmann, *Zeroes, multiplicities and idempotents for zerodimensional systems*, Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94 (Boston), Progr. Math., vol. 143, Birkhäuser Boston, 1996, 1–15.

[AL94] W. Adams y P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, AMS, 1994.

[Ald84] A. Alder, *Grenzrang und Grenzkomplexität aus algebraischer und topologischer sicht*, Ph.D. thesis, Universität Zürich, Philosophische Fakultät II, 1984.

[BC97] T. Bloom y J. P. Calvi, *A continuity property of multivariate lagrange interpolation*, Math. Comp. **66** (1997), no. 220, 1561–1577.

[BCRS96] E. Becker, J. P. Cardinal, M. F. Roy y Z. Szafraniec, *Multivariate Bezoutians, Kronecker symbol and Eisenbud-Levine formula*, Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94 (Boston), Progr. Math., vol. 142, Birkhäuser Boston, 1996, 79–104.

[BCS97] P. Bürgisser, M. Clausen y M. Shokrollahi, *Algebraic complexity theory*, Grundlehren Math. Wiss., vol. 315, Springer, Berlin, 1997.

[BCSS96] L. Blum, F. Cucker, M. Shub y S. Smale, *Algebraic settings for the problem "P≠NP¿*, The Mathematics of Numerical Analysis: 1995 AMS–SIAM Summer Seminar in Applied Mathematics, July 17–August 11, 1995, Park City, Utah (Providence, RI) (J. Renegar, M. Shub y S. Smale, eds.), Lecture in Applied Mathematics, vol. 32, Amer. Math. Soc., 1996, 125–144.

[BCSS98] ———, *Complexity and real computation*, Springer, New York Berlin Heidelberg, 1998.

[BHM+16] B. Bank, J. Heintz, G. Matera, J. Montaña, L. Pardo y A. R. Paredes, *Quiz games as a model for information hiding*, J. Complexity **34** (2016), 1–29.

[BP94] D. Bini y V. Pan, *Polynomial and matrix computations*, Progress in Theoretical Computer Science, Birkhäuser, Boston, 1994.

[Bro89] M. Brodman, *Algebraische Geometrie*, Basler Lehrbücher: A Series of Advanced Textbooks in Mathematics, vol. 1, Birkhäuser, Basel, Boston, Berlin, 1989, Eine Einfhürung.

[BS83] W. Baur y V. Strassen, *The complexity of partial derivatives*, Theoret. Comput. Sci. **22** (1983), 317–330.

[BSS89] L. Blum, M. Shub y S. Smale, *On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines*, Bull. Amer. Math. Soc. **21** (1989), no. 1, 1–46.

[Buc85] B. Buchberger, *Gröbner bases: An algoritmic method in polynomial ideal theory*, Multidimensional System Theory (N. K. Bose et al, ed.), Reidel, Dordrecht, 1985, 374–383.

[CGH91] L. Caniglia, A. Galligo y J. Heintz, *Equations for the projective closure and effective Nullstellensatz*, Discrete Appl. Math. **33** (1991), no. 1-3, 11–23, Applied algebra, algebraic algorithms, and error-correcting codes (Toulouse, 1989).

[CGH+03] D. Castro, M. Giusti, J. Heintz, G. Matera y L. Pardo, *The hardness of polynomial equation solving*, Found. Comput. Math. **3** (2003), no. 4, 347–420.

[CM06] A. Cafure y G. Matera, *Fast computation of a rational point of a variety over a finite field*, Math. Comput. **75** (2006), no. 256, 2049–2085.

[Dan94] V. I. Danilov, *Algebraic varieties and schemes*, Algebraic geometry, I, Encyclopaedia Math. Sci., vol. 23, Springer, Berlin, 1994, 167–297.

[dBR90] C. de Boor y A. Ron, *On multivariate polynomial interpolation problem*, Constr. Approx. **6** (1990), no. 3, 287–302.

[dBR92] ———, *The least solution for the polynomial interpolation problem*, Math. Z. **210** (1992), no. 3, 347–378.

[DFGS91] A. Dickenstein, N. Fitchas, M. Giusti y C. Sessa, *The membership problem for unmixed polynomial ideals is solvable in single exponential time*, Discrete Appl. Math. **33** (1991), 73–94.

[Dix82] J. Dixon, *Exact solution of linear equations using p-adic expansions*, Numer. Math. **40** (1982), 137–141.

[DKS13] C. D'Andrea, T. Krick y M. Sombra, *Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze*, Ann. Sci. Éc. Norm. Supér. **46** (2013), no. 4, 571–649.

[DL08] C. Durvye y G. Lecerf, *A concise proof of the Kronecker polynomial system solver from scratch*, Expo. Math. **26** (2008), no. 2, 101–139.

[DOSS15] C. D'Andrea, A. Ostafe, I. Shparlinski y M. Sombra, *Modular reduction of systems of polynomial equations and algebraic dynamical systems*, Preprint `arXiv:1505.05814 [math.NT]` (2015).

[Eis95] D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.

[EM96] M. Elkadi y B. Mourrain, *Approche effective des résidus algébriques*, Rapport de Recherche 2884, INRIA, Sophia Antipolis, 1996.

[EM07] ———, *Introduction à la résolution des systèmes polynomiaux*, Springer, 2007.

[Fal91] G. Faltings, *Diophantine approximation on abelian varieties*, Ann. of Math. **133** (1991), 549–576.

[FF63] D. Faddeev y V. Faddeeva, *Computational methods of linear algebra*, Freeman, San Francisco, 1963.

[FGLM93] J. C. Faugère, P. Gianni, D. Lazard y T. Mora, *Efficient computation of zero–dimensional Gröbner bases by change of ordering*, J. Symbolic Comput. **16** (1993), no. 4, 329–344.

[FGS95] N. Fitchas, M. Giusti y F. Smietanski, *Sur la complexité du théorème des zéros*, Approximation and Optimization in the Caribbean II, Proceedings 2nd International Conference on Non–Linear Optimization and Approximation (J. Guddat et al, ed.), Approximation and Optimization, vol. 8, Peter Lange Verlag, Frankfurt am Main, 1995, 247–329.

[Ful84] W. Fulton, *Intersection theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 2, Springer-Verlag, Berlin, 1984.

[GF76] H. Grauert y K. Fritzsche, *Several complex variables*, Grad. Texts in Math., vol. 38, Springer, New York Heidelberg Berlin, 1976.

[GH93] M. Giusti y J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, Computational Algebraic Geometry and Commutative Algebra (Cambridge) (D. Eisenbud y L. Robbiano, eds.), Sympos. Math., vol. XXXIV, Cambridge Univ. Press, 1993, 216–256.

[GH01] ———, *Kronecker's smart, little black–boxes*, Proceedings of Foundations of Computational Mathematics, FoCM'99, Oxford 1999 (Cambridge) (A. I. R. Devore y E. Süli, eds.), London Math. Soc. Lecture Note Ser., vol. 284, Cambridge Univ. Press, 2001, 69–104.

[GHH+97] M. Giusti, K. Hägele, J. Heintz, J. Morais, J. Montaña y L. Pardo, *Lower bounds for Diophantine approximation*, J. Pure Appl. Algebra **117,118** (1997), 277–317.

[GHM+98] M. Giusti, J. Heintz, J. Morais, J. Morgenstern y L. Pardo, *Straight–line programs in geometric elimination theory*, J. Pure Appl. Algebra **124** (1998), 101–146.

[GHMS11] N. Giménez, J. Heintz, G. Matera y P. Solernó, *Lower complexity bounds for interpolation algorithms*, J. Complexity **27** (2011), no. 2, 151–187.

[GHS93] M. Giusti, J. Heintz y J. Sabia, *On the efficiency of effective Nullstellensätze*, Comput. Complexity **3** (1993), 56–95.

[Gim14] N. Giménez, *An algorithm for implicit interpolation*, Appl. Algebra Engng. Comm. Comput. **25** (2014), 119–157.

[Giu89] M. Giusti, *Complexity of standard bases in projective dimension zero*, Proceedings of the European Conference on Computer Algebra (Berlin) (J. Davenport, ed.), Lecture Notes in Comput. Sci., vol. 378, Springer, 1989, 333–335.

[GLS01] M. Giusti, G. Lecerf y B. Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity **17** (2001), no. 1, 154–211.

[GM16] N. Giménez y G. Matera, *On the bit complexity of polynomial system solving*, Preprint `arXiv:1612.07786 [math.AG]` (2016).

[GS00a] M. Gasca y T. Sauer, *On the history of polinomial interpolation*, J. Comput. Appl. Math **122** (2000), no. 1–2, 23–35.

[GS00b] ———, *Polynomial interpolation in several variables*, Adv. Comput. Math. **12** (2000), no. 4, 377–410.

[Har77] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math., vol. 52, Springer, New York, 1977.

[Har92] J. Harris, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 133, Springer-Verlag, New York, 1992, A first course.

[Hei83] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci. **24** (1983), no. 3, 239–277.

[HK04] J. Heintz y B. Kuijpers, *Constraint databases, data structures and efficient query evaluation*, Constraint databases. First international symposium, CDB 2004, Paris, France, (B. Kuijpers, ed.), Lecture Notes in Comput. Sci., vol. 3074, Springer, Berlin, June 12–13 2004, 1–24.

[HKP+00] J. Heintz, T. Krick, S. Puddu, J. Sabia y A. Waissbein, *Deformation techniques for efficient polynomial equation solving*, J. Complexity **16** (2000), no. 1, 70–109.

[HL11] A. Hashemi y D. Lazard, *Sharper complexity bounds for zero–dimensional Gröbner bases and polynomial system solving*, Internat. J. Algebra Comput. **21** (2011), no. 5, 703–713.

[HM93] J. Heintz y J. Morgenstern, *On the intrinsic complexity of elimination theory*, J. Complexity **9** (1993), 471–498.

[HMPS00] K. Hägele, J. Morais, L. Pardo y M. Sombra, *On the intrinsic complexity of the arithmetic Nullstellensatz*, J. Pure Appl. Algebra **146** (2000), no. 2, 103–183.

[HP68a] W. Hodge y D. Pedoe, *Methods of algebraic geometry. Vol. I*, Cambridge Math. Lib., Cambridge Univ. Press, Cambridge, 1968.

[HP68b] ———, *Methods of algebraic geometry. Vol. II*, Cambridge Math. Lib., Cambridge Univ. Press, Cambridge, 1968.

[HS82] J. Heintz y C. P. Schnorr, *Testing polynomials which are easy to compute*, International Symposium on Logic and Algorithmic, Zurich 1980, Monogr. Enseig. Math., vol. 30, 1982, 237–254.

[Ive73] B. Iversen, *Generic local structure of the morphisms in commutative algebra*, Lecture Notes in Math., vol. 310, Springer, New York, 1973.

[Jel05] Z. Jelonek, *On the effective Nullstellensatz*, Invent. Math. **162** (2005), no. 1, 1–17.

[Knu81] D. Knuth, *The art of computer programming: Semi–numerical algorithms*, vol. 2, Addison-Wesley, 1981.

[Kön03] J. König, *Einleitung in die allgemeine Theorie der algebraischen Grözen*, Druck und Verlag von B.G. Teubner, Leipzig, 1903.

[KP94] T. Krick y L. Pardo, *Une approche informatique pour l' approximation diophantienne*, C. R. Math. Acad. Sci. Paris **318** (1994), no. 1, 407–412.

[KPS01] T. Krick, L. Pardo y M. Sombra, *Sharp estimates for the Arithmetic Nullstellensatz*, Duke Math. J. **109** (2001), no. 3, 521–598.

[Kro65] L. Kronecker, *Über Einige Interpolationsformeln für Ganze Functionen Mehrer Variabeln*, Monatsberichte der Königlich Preussischen Akademie der Wissenschafften zu Berlin (1865), 686–691.

[Kro82] ———, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, J. Reine Angew. Math. **92** (1882), 1–122.

[Kun85] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser Boston, Inc., Boston, MA, 1985, Translated from the German by Michael Ackerman, With a preface by David Mumford.

[Kun86] E. Kunz, *Kähler differentials*, Advanced Lectures in Mathematics, Vieweg, Braunschweig, 1986.

[Lan93] S. Lang, *Algebra*, third ed., Addison–Wesley, Reading, Massachusetts, 1993.

[Laz81] D. Lazard, *Résolution des systèmes d'équations algébriques*, Theoret. Comput. Sci. **15** (1981), 77–110.

[Lec03] G. Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, J. Complexity **19** (2003), no. 4, 564–596.

[Mar02] O. Marker, *Model theory: An introduction*, Grad. Texts in Math., vol. 217, Springer, New York, 2002.

[Mat80] H. Matsumura, *Commutative algebra*, Benjamin, 1980.

[Mat86] ———, *Commutative ring theory*, Cambridge Univ. Press, Cambridge, 1986.

[MMM91] M. Marinari, H. Möller y T. Mora, *Gröbner bases of ideals given by dual bases*, Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, ISSAC'91 (Bonn, West Germany), ACM Press, 1991, 267–276.

[MMM93] ———, *Gröbner bases of ideals defined by functionals with an application to ideals of projective points*, Appl. Algebra Engrg. Comm. Comput. **4** (1993), 103–145.

[Mor05] T. Mora, *Solving polynomial equation systems. Vol. II. Macaulay's paradigm and Gröbner technology*, Encyclopedia Math. Appl., vol. 99, Cambridge Univ. Press, Cambridge, 2005.

[Mor15] ———, *Solving polynomial equation systems. Vol. III: Algebraic solving*, Encyclopedia Math. Appl., vol. 157, Cambridge Univ. Press, Cambridge, 2015.

[MS00a] H. M. Möller y T. Sauer, *H-bases for polinomial interpolation and system solving*, Adv. Comput. Math. **12** (2000), 335–362.

[MS00b] ———, *H-Bases I: The Foundation*, Curve and Surface fitting: Saint–Malo 1999 (A. Cohen, C. Rabut y L. Schumaker, eds.), Vanderbildt University Press, 2000, 325–332.

[MS16] S. Melczer y B. Salvy, *Symbolic–numeric tools for analytic combinatorics in several variables*, Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, Algebraic Algorithms and Error-Correcting Codes, Waterloo, ON, Canada, July 2016 (New York), ACM press, 2016.

[Mum88] D. Mumford, *The red book of varieties and schemes*, 1st ed., Lecture Notes in Math., vol. 1358, Springer, New York, 1988.

[Mum95] ———, *Algebraic geometry I. Complex projective varieties*, 2nd ed., Classics Math., Springer, Berlin, 1995.

[Olv06] P. Olver, *On multivariate interpolation*, Stud. Appl. Math. **116** (2006), no. 2, 201–240.

[PS07] J. M. Peña y T. Sauer, *Efficient polynomial reduction*, Adv. Comput. Math. **26** (2007), no. 1–3, 323–336.

[Sau01] T. Sauer, *Gröbner bases, H-bases and interpolation*, Trans. Amer. Math. Soc. **353** (2001), 2293–2308.

[SB93] J. Stoer y R. Bulirsch, *Introduction to numerical analysis*, Springer, 1993.

[Sch00] E. Schost, *Sur la résolution de systèmes à paramètres*, Ph.D. thesis, École Polytechnique, France, 2000.

[Sch03] ———, *Computing parametric geometric resolutions*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), 349–393.

[Sha94] I. R. Shafarevich, *Basic algebraic geometry. 1*, second ed., Springer-Verlag, Berlin, 1994, Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.

[Sho99] V. Shoup, *Efficient computation of minimal polynomials in algebraic extension fields*, ISSAC'99: Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, Canada), ACM New York, USA, 1999, 53–58.

[SS16] M. Safey El Din y E. Schost, *Bit complexity for multi-homogeneous polynomial system solving. Application to polynomial minimization*, Preprint `arXiv:1605.07433 [cs.SC]` (2016).

[Sto00] A. Storjohann, *Algorithms for matrix canonical forms*, Ph.D. thesis, ETH, Zürich, Switzerland, 2000.

[SW05] A. Sommese y C. Wampler, *The numerical solution of systems of polynomials arising in engineering and science*, World Scientific, Singapore, 2005.

[Tei82] B. Teissier, *Variétés polaires. II: Multiplicités polaires, sections planes et conditions de Whitney*, Algebraic geometry, Proc. Int. Conf., La Rábida/Spain 1981 (Berlin Heidelberg New York) (J. Aroca, R. Buchweitz, M. Giusti y M. Merle, eds.), Lect. Notes Math., vol. 961, Springer, 1982, 314–491.

[Vog84] W. Vogel, *Lectures on results on Bezout's theorem*, Tata Institute of Fundamental Research Lectures on Mathematics and Physics, vol. 74, Published for the Tata Institute of Fundamental Research, Bombay; by Springer-Verlag, Berlin, 1984, Notes by D. P. Patil.

[vzGG99] J. von zur Gathen y J. Gerhard, *Modern computer algebra*, Cambridge Univ. Press, Cambridge, 1999.

[ZS60] O. Zariski y P. Samuel, *Commutative algebra II*, Grad. Texts in Math., vol. 39, Springer, New York, 1960.