UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales

Departamento de Matemática

Tesis de Licenciatura

COMPLEJIDAD DE ALGORITMOS PARA LA INTERPOLACIÓN POLINOMIAL EN VARIAS VARIABLES

Nardo Giménez

Director: Guillermo Matera.

Fecha de Presentación: 26 de Julio de 2007.

Agradecimientos

Deseo expresar mi agradecimiento a Guillermo Matera y Pablo Solernó, por su paciencia y dedicación a lo largo de este trabajo, que no hubiera sido posible sin ellos. Quiero agradecer además a Joos Heintz, cuya influencia es manifiesta en el carácter de esta tesina.

A Cecilia, el Amor de mi vida, que estuvo a mi lado en todas las circunstancias, y que fue y será mi musa inspiradora.

A mi querida familia, mis padres Guillermo y Alfreda y mi hermano Julián, que siempre me acompañaron y alentaron a continuar en el camino elegido, aun en momentos de incertidumbre y dificultad.

A todos ellos agradezco por haber considerado mis estudios como parte de su propio proyecto.

Quiero agradecer por último a mis amigos incondicionales que de distintos modos estuvieron presentes en estos años, Sebastián Borrachia, Alberto Penas, Jorge Flolasco y Andrés Racket.

Resumen

El tema principal de esta tesina es la interpolación polinomial multivariada considerada desde el punto de vista algorítmico.

En la primera mitad del trabajo se estudia el problema de la interpolación polinomial multivariada cuando el conjunto de nodos es una $\mathbb{Q}$–variedad algebraica afín 0–dimensional V de $\mathbb{C}^n$, que se supone dada en forma implícita por un sistema de ecuaciones polinomiales $F_1 = 0, \ldots, F_n = 0$ con coeficientes en $\mathbb{Q}$. A partir de estos polinomios se construye un subespacio de interpolantes Π_V de "bajo grado". Finalmente se considera una versión algorítmica de este problema, basada en el modelo de computación de los straight–line programs.

En la segunda mitad del trabajo se obtienen cotas inferiores de complejidad para ciertos problemas de interpolación. Para tal fin se fija un modelo para procesos de interpolación, que permite modelizar además de los problemas de interpolación clásicos, otros problemas de interpolación que presentan "singularidades". Además, se consideran fenómenos de coalescencia, a través de la noción de *robustez* para algoritmos que resuelven problemas de interpolación. En este contexto, básicamente obtenemos cotas inferiores en términos del número de nodos involucrados, y cotas inferiores en términos del costo de la "longitud" de la representación de los interpolantes.

Índice general

Capítulo 1

Introducción

En esta tesina estudiamos el aspecto algorítmico de la interpolación polinomial multivariada. Fíjese $n \in \mathbb{N}$ y denotemos con $\Pi := \mathbb{C}[X_1, \ldots, X_n]$ al anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en $\mathbb{C}$. En la Parte I partimos de la consideración del siguiente problema de interpolación de Lagrange:

Problema 1 *El* problema de interpolación de Lagrange (lineal y genérico) en los nodos $x^{(1)}, \ldots, x^{(\delta)} \in \mathbb{C}^n$ definido en un subespacio $\mathcal{O} \subset \Pi$*, consiste en hallar para cada conjunto ordenado de valores* $y_1, \ldots, y_\delta \in \mathbb{C}$ *un polinomio* P *(un interpolante) "simple" en* $\mathcal{O}$*, que verifique las condiciones de interpolación* $P(x^{(j)}) = y_j$ $(1 \leq j \leq \delta)$.

Al contrario que en el caso univariado, donde el subespacio de interpolantes canónico $\mathcal{O}$ es el conjunto de polinomios de grado a lo sumo $\delta - 1$, en el caso multivariado la elección del subespacio $\mathcal{O}$, depende fuertemente de las propiedades impuestas a los interpolantes [9, Introduction]. La noción de simplicidad del interpolante P se precisa según el contexto, pero en términos generales significa que P posee buenas propiedades con respecto a posibles aplicaciones. Por ejemplo, para que la interpolación polinomial sea útil como método de aproximación es necesario evitar que el interpolante tenga grandes oscilaciones. Siendo el *grado* del polinomio lo que causa dichas oscilaciones, un requerimiento generalmente adoptado es que P tenga grado "bajo"([9, Introduction], [16, 3.2, 3.1].) así pues, vamos a preocuparnos de controlar el grado del interpolante.

Usualmente los nodos y los valores que definen el problema de interpolación son dados explícitamente. Por otra parte ya en 1865 Kronecker [26] investigó la interpolación cuando el conjunto de nodos es el conjunto de ceros de un sistema de ecuaciones polinomiales y de hecho empleó dichas ecuaciones para construir el polinomio interpolante, aunque todavía suponiendo el conocimiento de los nodos. Inspirados en la idea de Kronecker nosotros consideramos un problema de interpolación implícita, en donde únicamente se supone el conocimiento de las ecuaciones que definen los nodos. Más precisamente, vamos a considerar la siguiente reformulación del Problema 1:

Problema 2 *Sean dados polinomios $F_1, \ldots, F_n$ en $\mathbb{Q}[X_1, \ldots, X_n]$ tales que el conjunto de ceros del sistema de ecuaciones $F_1(x) = 0, \ldots, F_n(x) = 0$ es el conjunto de nodos $V = \{x^{(1)}, \ldots, x^{(\delta)}\} \subset \mathbb{C}^n$. Asimismo supongamos dado un polinomio $F \in \mathbb{Q}[X_1, \ldots, X_n]$. El* problema de la interpolación de Lagrange (implícita) *consiste en hallar un polinomio $P \in \mathbb{Q}[X_1, \ldots, X_n]$ "simple" tal que $P(x^{(i)}) = F(x^{(i)})$ para $1 \leq i \leq \delta$.*

Ahora los datos de entrada, esto es, los polinomios $F_1, \ldots, F_n$ y F, se pueden representar a partir de parámetros racionales de los cuales obtenemos el polinomio interpolante P de F mediante un número finito de operaciones racionales. En efecto, a partir de estos polinomios construimos una base $(G_1, \ldots, G_\delta)$ de polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ de grados a lo sumo $n(d-1)$, donde d es una cota a priori para los grados de los polinomios $F_1, \ldots, F_n$, y tales que generan un subespacio de interpolantes $\mathcal{O} := \Pi_V$ para el problema en consideración. Luego se calculan las coordenadas del interpolante $P \in \Pi_V$ en dicha base, por medio de un algoritmo probabilístico cuyo costo depende linealmente del costo de evaluar los polinomios de entrada y cuadráticamente de un invariante geométrico asociado al sistema de entrada, que denominamos el *grado del sistema* (Teorema 5.18). Este grado está siempre acotado por el número de Bézout del sistema de entrada (el producto de los grados de los polinomios $F_1, \ldots, F_n$) y en ciertos casos de interés práctico resulta considerablemente menor que éste. En este sentido, nuestro algoritmo mejora significativamente el costo de los algoritmos que utilizan bases de Gröbner.

En la Parte II estudiamos la complejidad de resolver familias de problemas de interpolación. Para tal fin fijamos un modelo para los procesos de interpolación. En éste, la familia de problemas de interpolación está codificada por un subconjunto construible $\mathcal{D}$ de un cierto espacio ambiente afín. Aquí, las coordenadas de un código $d \in \mathcal{D}$ se interpretan como la lista de nodos/valores que definen un problema de interpolación particular. Un algoritmo de interpolación que resuelve la familia de problemas está dado por una codificación del espacio de interpolantes, mediante un constructible $\mathcal{D}^*$ y por una aplicación racional Ψ de $\mathcal{D}$ en la estructura de datos $\mathcal{D}^*$. La complejidad del algoritmo Ψ se define entonces como la dimensión del espacio ambiente donde está incluida la estructura de datos $\mathcal{D}^*$ que codifica las salidas del algoritmo. Así pues, nuestro objetivo es obtener cotas inferiores de complejidad para la representación de las salidas (es decir, los interpolantes) de algoritmos de interpolación que resuelven (genéricamente) familias de problemas de interpolación.

Considérese, por ejemplo, la clásica familia de problemas de interpolación de Lagrange con N nodos. Esta familia de problemas está representada por la estructura de datos $\mathcal{D} := \{(\xi_1, y_1, \ldots, \xi_N, y_1) \in \mathbb{C}^{(n+1)N} : \ \xi_i \in \mathbb{C}^n, \ y_i \in \mathbb{C} \text{ para } 1 \leq i \leq N, \ \xi_i \neq \xi_j, \text{para } 1 \leq \mathrm{i} < \mathrm{j} \leq \mathrm{N}\} \subset \mathbb{C}^{(n+1)N}$, de modo que cada punto $d := ((\xi_1, y_1, \ldots, \xi_N, y_1) \in \mathcal{D}$ determina un problema de interpolación de Lagrange que consiste en hallar un polinomio interpolante $P \in \mathbb{C}[X_1, \ldots, X_n]$ que verifique $P(\xi_i) = y_i$ para $1 \leq i \leq N$. Obsérvese que en este caso la estructura de datos $\mathcal{D}$ es un subconjunto denso Zaris-

ki del espacio afín $\mathbb{C}^{(n+1)N}$. Esta es la situación típica de muchas otras familias de problemas de interpolación clásicas.

Ahora bien, es un hecho que, fijando una complejidad de representación para el aproximante de una función dada, los espacios no lineales proveen aproximantes con mejores calidades aproximativas que las obtenidas con aproximantes tomados de espacios lineales (véase [38, 5.8 y 5.9]). Por otra parte, la interpolación polinomial constituye uno de los métodos más simples de aproximación. Por tales motivos, nosotros consideramos, más generalmente, familias de problemas de interpolación cuyas estructuras de datos son subconjuntos construibles $\mathcal{D}$ de dimensión estrictamente menor que la dimensión del espacio afín donde están incluidos, y aun con presencia de puntos singulares, pues típicamente las familias de problemas de interpolación no lineales están representadas por estructuras de datos de este tipo (Ejemplo 6.2.4).

El primer resultado que obtenemos demuestra que toda familia de problemas de interpolación de Lagrange con un número fijo de nodos codificada por un conjunto abierto Zariski tiene esencialmente la complejidad del método usual de interpolación lineal univariado, es decir, el número de nodos (Teorema 8.1).

Con el fin de obtener cotas inferiores de complejidad para las familias de problemas de interpolación no lineales introducidas en los Ejemplos 8.1.2 y 6.2.4, suponemos que los algoritmos de interpolación son *robustos*. Esencialmente Ψ es un algoritmo robusto de interpolación, si admite una única extensión a toda instancia de la familia de problemas donde Ψ no está definida. Nosotros formalizamos la noción de robustez mediante la teoría de places de la geometría algebraica y el álgebra conmutativa. El resultado más importante que obtenemos en este contexto es la cota inferior para la familia de problemas del Ejemplo 6.2.4. En este ejemplo el espacio de interpolantes es el conjunto $\mathcal{O}_{n,L}$ de polinomios n-variados que se pueden evaluar mediante un straight-line program de longitud no escalar a lo sumo L. Consideramos la familia de problemas de interpolación que consiste en reconstruir un polinomio $f \in \mathcal{O}_{n,L}$ a partir de sus valores en suficientes nodos (un sucesión de identificación). En este caso obtenemos una cota inferior que depende exponencialmente del número de nodos (Teorema 8.3).

Capítulo 2

Preliminares

2.1. Geometría algebraica

Uno de los aspectos del método de interpolación que desarrollamos en la Parte I de este trabajo es el uso de las propiedades geométricas del conjunto de nodos en consideración. Por esta razón, comenzamos repasando algunas nociones básicas de la geometría algebraica.

2.1.1. Variedades algebraicas

Sea $k := \mathbb{Q}$ o $\mathbb{C}$. Un subconjunto $V \subseteq \mathbb{C}^n$ se llama una *k–variedad* (*algebraica*) *afín* de $\mathbb{C}^n$ (brevemente una *k–variedad*) si existen polinomios $F_1, \ldots, F_s$ en $k[X_1, \ldots, X_n]$ tales que

$$V = \{x \in \mathbb{C}^n : F_1(x) = 0, \ldots, F_s(x) = 0\}.$$

Denotamos esto brevemente con $V = V(F_1, \ldots, F_s)$. Una k–variedad $V := V(F)$ definida por un solo polinomio F no constante se llama una *hipersuperficie*.

Las k–variedades afínes de $\mathbb{C}^n$ son los conjuntos cerrados de la topología de $\mathbb{C}^n$ llamada la *topología de Zariski sobre k*. Cada k–variedad $V \subseteq \mathbb{C}^n$ se considera equipada con la topología inducida por la topología de Zariski de $\mathbb{C}^n$. Una k–variedad $V \subseteq \mathbb{C}^n$ se dice *irreducible* si es un espacio topológico irreducible con esta topología. Es decir, V es irreducible si no se puede expresar como una descomposición irredundante $V = V_1 \cup V_2$, donde V_1, V_2 son k–variedades. Toda k–variedad tiene una única (salvo reordenamientos) descomposición irredundante como unión finita de k–variedades irreducibles $V = C_1 \cup \cdots \cup C_h$. Las k–variedades $C_1, \ldots, C_h$ se denominan las *componentes irreducibles* de V.

Dada una k–variedad $V \subseteq \mathbb{C}^n$, su *ideal asociado* $I(V)$ es el ideal de $k[X_1, \ldots, X_n]$ formado por todos los polinomios que se anulan idénticamente sobre V. El *anillo de coordenadas* $k[V]$ de V se define como el anillo cociente $k[X_1, \ldots, X_n]/I(V)$. Se tiene que V es irreducible si y solo si $k[V]$ es íntegro. En tal caso el cuerpo de fracciones $k(V)$

de $k[V]$ se denomina el *cuerpo de funciones racionales* de V. Si V es una k–variedad irreducible, la *dimensión* de V se define como el máximo $m \geq 0$ tal que existe una cadena $V_0 \subset \ldots \subset V_m = V$ donde V_i es una k–variedad irreducible para todo $0 \leq i \leq m$. Equivalentemente, la dimensión de V puede definirse como el grado de trascendencia de la extensión de cuerpos $k \hookrightarrow k(V)$. La dimensión de una k–variedad arbitraria $V \subseteq \mathbb{C}^n$ se define como el máximo de las dimensiones de sus componentes irreducibles. Una k–variedad se dice *equidimensional* si todas sus componentes irreducibles tienen la misma dimensión. En particular una, k–variedad V es de *dimensión cero*, o 0*–dimensional*, si y solo si V es un conjunto finito. Los conjuntos de nodos que vamos a considerar para los problemas de interpolación en la Parte I son $\mathbb{Q}$–variedades 0–dimensionales.

Si V es irreducible, definimos su *grado* $\mathrm{gr}\,(V)$ como el máximo número de puntos en la intersección de V con un subespacio lineal afín L de $\mathbb{A}^n$ de codimensión $\dim V$, para el cual se verifica $\#(V \cap L) < \infty$. Más generalmente, si $V = C_1 \cup \cdots \cup C_N$ es la descomposición de una variedad afín arbitraria V en componentes irreducibles sobre $\mathbb{C}$, definimos el grado de V como $\mathrm{gr}\,(V) := \sum_{i=1}^{N} \mathrm{gr}\,(C_i)$ (véase [22]). En lo que sigue usaremos la siguiente *desigualdad de Bézout* ([22]; véase también [15], [37]): si V y W son subvariedades de $\mathbb{A}^n$, entonces vale la siguiente desigualdad:

$$\mathrm{gr}\,(V \cap W) \leq \mathrm{gr}\,(V)\,\mathrm{gr}\,(W). \tag{2.1}$$

2.1.2. Conjuntos y aplicaciones construibles

Una k–variedad algebraica afín $V \subseteq \mathbb{C}^n$ también se llama una variedad k*–definible* o k*–construible*. Más generalmente, un subconjunto $X \subseteq \mathbb{C}^n$ es k*–construible* si es una combinación Booleana ($finita$) de k–variedades algebraicas afines de $\mathbb{C}^n$. Equivalentemente, X es una unión disjunta $V_1 \cup \cdots \cup V_k$, donde V_i es de la forma $V_i = V_i' \setminus V_i''$, siendo V_i', V_i'' k–variedades de $\mathbb{C}^n$ con $V_i'' \subseteq V_i'$.

Asimismo, una aplicación $\varphi : X \to Y$ entre conjuntos construibles se dice k*–construible* si su gráfico es un subconjunto k–construible de $\mathbb{C}^n \times \mathbb{C}^m$.

2.1.3. Morfismos

Sean $V \subseteq \mathbb{C}^n$ y $W \subseteq \mathbb{C}^m$ dos k–variedades. Una aplicación $f : V \to W$ se llama un *morfismo regular* (k*–definible*) si existen m polinomios $f_1, \ldots, f_m$ en $k[X_1, \ldots, X_n]$ tales que $f(x) = (f_1(x), \ldots, f_m(x))$ para todo $x \in V$. Un morfismo regular $f : V \to W$ es un *isomorfismo* si tiene inversa, es decir, si existe un morfismo regular $g : W \to V$ tal que $f \circ g = Id_V$ y $g \circ f = Id_W$.

Ahora sea $V \subseteq \mathbb{C}^n$ una k–variedad irreducible, y sea $f \in k(V)$ una función racional. Se dice que f está definida en un punto $x \in V$ si existe una representación $f = h/g$, con h, g en $k[V]$, tal que $g(x) \neq 0$. El conjunto de todos los puntos $x \in V$ tales

que f está definida en x se denomina el *dominio de definición* de f y es un abierto denso de V. Un *morfismo racional* $f : V \dashrightarrow \mathbb{C}^m$ está definido por una sucesión de funciones racionales $f_1, \ldots, f_m$ en $k(V)$. El dominio de definición de f se define como la intersección de los dominios de definición de todas las f_i, se nota $\mathrm{dom} f$ y es un abierto denso de V. Así, el morfismo f es una aplicación parcialmente definida tal que $f(x) := (f_1(x), \ldots, f_m(x))$ para todo x en el dominio de definición de f. Un morfismo racional $f : V \dashrightarrow \mathbb{C}^m$ se llama *regular* si $\mathrm{dom} f = V$. La *imagen* de f se define como el conjunto de los valores $f(x)$ con x en el dominio de definición de f y se nota $\mathrm{im}\, f$.

Sean $V \subseteq \mathbb{C}^n$ y $W \subseteq \mathbb{C}^m$ dos k–variedades irreducibles. Un *morfismo racional* $f : V \dashrightarrow W$ es un morfismo racional $f : V \to \mathbb{C}^m$ tal que $f(x) \in W$ para todo x en el dominio de definición de f.

Sean $f : V \dashrightarrow W$ un morfismo racional. Supóngase que f está dada por funciones racionales $f_1, \ldots, f_m \in k(V)$. Entonces f induce un homomorfismo de anillos

$$f^* : k[W] \to k(V)$$

definido por $f^*(\bar{F}) := F(f_1, \ldots, f_m)$ (obsérvese que f^* está bien definida pues $\mathrm{im} f \subseteq W$). Puesto que $\mathrm{im}\, f$ es la imagen del conjunto irreducible $\mathrm{dom}\, f$, se sigue que la clausura $\overline{\mathrm{im}\, f}$ es un subconjunto cerrado irreducible de W. En consecuencia el ideal $\mathfrak{P}$ de $k[W]$ asociado a $\overline{\mathrm{im}\, f}$ es un ideal primo. Por otra parte es claro que el núcleo de f^* es precisamente el ideal $\mathfrak{P}$. Sea $k[W]_{\mathfrak{P}}$ el anillo local asociado al ideal $\mathfrak{P}$. Entonces f^* admite una única extensión

$$f^* : k[W]_{\mathfrak{P}} \to k(V).$$

Sea $g : W \dashrightarrow \mathbb{C}^l$ otro morfismo racionale tal que $\mathrm{im}\, f \cap \mathrm{dom}\, g \neq \emptyset$. Sean $g_1, \ldots, g_l \in k(W)$ las funciones racionales que definen a g. La hipótesis $\mathrm{im}\, f \cap \mathrm{dom}\, g \neq \emptyset$ es quivalente a $g_i \in k[W]_{\mathfrak{P}}$ para todo i. Las funciones racionales $f^*(g_1), \ldots, f^*(g_l) \in k(V)$ definen entonces un morfismo racional $g \circ f : V \dashrightarrow \mathbb{C}^l$ que se llama la *composición* de f con g. Obsérvese que por construcción $f^{-1}(\mathrm{dom}\, g) \subseteq \mathrm{dom}\, (g \circ f)$ y que para todo $x \in f^{-1}(\mathrm{dom}\, g)$ vale $(g \circ f)(x) = g(f(x))$.

En particular, si la imagen de f es un subconjunto denso de W, la aplicación racional $f : V \dashrightarrow W$ se llama *dominante*, y f se puede componer con *toda* otra aplicación racional $g : W \dashrightarrow \mathbb{C}^l$. Un morfismo racional dominante $f : V \to W$ se denomina un morfismo *biracional* si es inversible, esto es, si existe un morfismo racional dominante $g : W \to V$ tal que se verifican las identidades $g \circ f = Id_{\mathcal{U}_1}$ y $f \circ g = Id_{\mathcal{U}_2}$ en abiertos Zariski $\mathcal{U}_1$ de V y $\mathcal{U}_2$ de W respectivamente.

2.2. Resolución geométrica de una variedad de dimensión 0

En esta sección, sea $k := \mathbb{Q}$ el cuerpo base de la topología Zariski. Nuestro principal objetivo en esta sección es mostrar que toda $\mathbb{Q}$–variedad 0–dimensional V de un espacio afín $\mathbb{C}^n$ para n arbitrario se puede parametrizar por los ceros de un polinomio univariado con coeficientes racionales. Es sabido que toda $\mathbb{Q}$–variedad equidimensional de dimensión r es biracionalmente equivalente a una $\mathbb{Q}$–hipersuperficie [35, Chapter I, § 3, Theorem 6] de $\mathbb{C}^{r+1}$. Más aun, una $\mathbb{Q}$–variedad 0–dimensional es isomorfa a una $\mathbb{Q}$–hipersuperficie de $\mathbb{C}^1$, es decir, el conjunto de ceros de un polinomio con coeficientes racionales, hecho que demostraremos a continuación. En estos términos, tenemos la siguiente definición preliminar:

Definición 2.1 Resolver geométricamente *una $\mathbb{Q}$–variedad 0–dimensional V significa hallar un polinomio en $\mathbb{Q}[T]$ que define una hipersuperficie de $\mathbb{C}^1$ birracionalmente equivalente a V y los polinomios que determinan el isomorfismo entre V y el conjunto de ceros de ese polinomio.*

El concepto central aquí es el de *elemento primitivo*, que es una herramienta comúnmente usada en el ámbito del Cálculo formal para la resolución simbólica de sistemas de ecuaciones polinomiales 0-dimensionales, pues reduce la resolución de los mismos a cómputos en una sola variable.

Sea entonces $V \subseteq \mathbb{C}^n$ una $\mathbb{Q}$–variedad afín de dimensión cero e $I := I(V)$ su ideal asociado. De ahora en adelante, sea B el anillo de coordenadas de V, es decir, la $\mathbb{Q}$–álgebra $\mathbb{Q}[X_1, \ldots, X_n]/I$. Es sabido que cuando la variedad V es 0–dimensional, B resulta un $\mathbb{Q}$–espacio vectorial de dimensión finita [7, Theorem 2.10]. Más aun, la dimensión $\dim_{\mathbb{Q}} B$ coincide con la cardinalidad δ de la variedad V.

Un polinomio $G \in \mathbb{Q}[X_1, \ldots, X_n]$ se dice *separante* de un conjunto finito $V := \{x^{(1)}, \ldots, x^{(\delta)}\} \subseteq \mathbb{C}^n$, o que *separa los puntos de V*, si se verifica $G(x^{(i)}) \neq G(x^{(j)})$ para todo par de puntos $x^{(i)}$ y $x^{(j)}$ distintos de V. En el siguiente lema se afirma que siempre existe una forma lineal separante de cualquier conjunto finito.

Lema 2.2 *Sea $V := \{x^{(1)}, \ldots, x^{(\delta)}\} \subseteq \mathbb{C}^n$ un conjunto finito de puntos. Entonces existe una forma lineal $U = \lambda_1 X_1 + \cdots + \lambda_n X_n \in \mathbb{Q}[X_1, \ldots, X_n]$ separante de V.*

Demostración: Sean $U_1, \ldots, U_n$ nuevas indeterminadas sobre $\mathbb{C}$ y sea $f \in \mathbb{Q}[U_1, \ldots, U_n, X_1, \ldots, X_n]$ el polinomio $f := U_1 X_1 + \cdots + U_n X_n$. Para cada $1 \leq i \leq \delta$ consideramos la forma lineal $f_i := U_1 x_1^{(i)} + \cdots + U_n x_n^{(i)} \in \mathbb{C}[U_1, \ldots, U_n]$ en las variables $U_1, \ldots, U_n$, que se obtiene al especializar las variables $X_1, \ldots, X_n$ del polinomio f en las coordenadas del punto $x^{(i)} = (x_1^{(i)}, \ldots, x_n^{(i)})$ de V. Para todo $i \neq j$ es $x^{(i)} \neq x^{(j)}$, con lo cual $f_i - f_j$ es una forma lineal no nula en $\mathbb{C}[U_1, \ldots, U_n]$. Luego $\Delta := \prod_{i<j}(f_i - f_j)$ es un polinomio no nulo

en $\mathbb{C}[U_1, \ldots, U_n]$. Ahora bien, siendo $\mathbb{Q}$ un subconjunto infinito de $\mathbb{C}$, existe una n-tupla $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Q}^n$ tal que $\Delta(\lambda_1, \ldots, \lambda_n) \neq 0$. Sea $U \in \mathbb{Q}[X_1, \ldots, X_n]$ la forma lineal $U := \lambda_1 X_1 + \cdots + \lambda_n X_n$. Se concluye que $\Delta(\lambda_1, \ldots, \lambda_n) = \prod_{i<j}(U(x^{(i)}) - U(x^{(j)})) \neq 0$, o equivalentemente, $U(x^{(i)}) \neq U(x^{(j)})$ para todo $i \neq j$. ∎

Cabe mencionar que la construcción de una forma lineal separante se puede hacer en forma efectiva mediante un algoritmo probabilístico conocido como el test de Schwartz–Zippel. Más precisamente, dada una probabilidad admisible μ, existe un subconjunto finito de $\mathbb{C}^n$, tal que la probabilidad de que un elemento seleccionado al azar de ese conjunto con distribución uniforme, sea la n–tupla de coeficientes de una forma lineal separante, es mayor que μ (para más detalles ver [34], [40], [38, Lemma 6.44]).

En consecuencia, podemos dar la siguiente definición:

Definición 2.3 *Sea $V \subseteq \mathbb{C}^n$ una $\mathbb{Q}$–variedad 0-dimensional. Un elemento primitivo de V es la imagen u en B de una forma lineal $U = \lambda_1 X_1 + \cdots + \lambda_n X_n \in \mathbb{Q}[X_1, \ldots, X_n]$ separante de V.*

Sea ahora $\mathrm{End}_{\mathbb{Q}}(B)$ el conjunto de endomorfismos $\mathbb{Q}$–lineales de B dotado con la estructura de $\mathbb{Q}$–álgebra mediante las operaciones usuales de multiplicación por escalares, suma y composición de funciones. A cada elemento $g \in B$ asociamos la homotecia $\eta_g : B \to B$ definida por la multiplicación por g, es decir, $\eta_g(f) := gf$ para todo $f \in B$. Así pues, η_g es un elemento de $\mathrm{End}_{\mathbb{Q}}(B)$, y como B es de dimensión finita δ, está definido el polinomio minimal de η_g en $\mathbb{Q}[T]$, notado q_g, mónico y con grado $gr(q_g) \leq \delta$. Llamamos a q_g simplemente el *polinomio minimal* de g. De este modo, se tiene definida una aplicación $\eta : B \to \mathrm{End}_{\mathbb{Q}}(B)$, $g \mapsto \eta_g$, que claramente es un morfismo inyectivo de $\mathbb{Q}$–álgebras. De aquí deducimos que el polinomio minimal q_g de g es el polinomio mónico $q \in \mathbb{Q}[T]$ de menor grado que anula a g en B, es decir, tal que $q(g) = 0$ en B. De este modo obtenemos la siguiente caracterización del polinomio minimal:

Lema 2.4 *Sea $V \subseteq \mathbb{C}^n$ una $\mathbb{Q}$–variedad 0–dimensional. Entonces el polinomio minimal $q_u \in \mathbb{Q}[T]$ de un elemento primitivo u de V inducido por una forma lineal $U \in \mathbb{Q}[X_1, \ldots, X_n]$ tiene grado $\delta = \#(V)$ y tiene todas sus raíces simples. En forma explícita se tiene:*

$$q_u(T) = \prod_{j=1}^{\delta}(T - U(x^{(j)})).$$

Demostración: Sabemos que $q_u(u) = 0$ en B, con lo cual se verifica $q_u(U(x^{(j)})) = 0$ para todo punto $x^{(j)} \in V$. Es decir que el conjunto $\{U(x^{(j)}) : x^{(j)} \in V\}$ está incluído en el conjunto de raíces de q_u. Por otro lado, como U separa los puntos de V, obtenemos la igualdad de cardinales:

$$\#\{U(x^{(j)}) : x^{(j)} \in V\} = \#V = \delta.$$

Por lo tanto, como en principio $gr(q_u) \leq \delta$, el conjunto de raíces de q_u debe ser exactamente $\{U(x^{(j)}) : x^{(j)} \in V\}$ y la conclusión del lema es inmediata. ∎

Consideremos ahora el subconjunto algebraico H_u de $\mathbb{C}$ determinado por el conjunto de ceros del polinomio minimal de u, es decir, $H_u := \{\xi \in \mathbb{C} : q_u(\xi) = 0\}$. Siendo q_u libre de cuadrados, el anillo de coordenadas de H_u es el anillo cociente $A_u := \mathbb{Q}[T]/(q_u)$. Ahora bien A_u es una $\mathbb{Q}$–álgebra monógena generada por la imagen t en A_u de la indeterminada T, lo que denotamos escribiendo $A_u = \mathbb{Q}[t]$. Se tiene el siguiente corolario:

Corolario 2.5 *Los anillos de coordenadas B y A_u son $\mathbb{Q}$–álgebras isomorfas por medio de un isomorfismo que aplica u en t.*

Demostración: Afirmamos que B es una $\mathbb{Q}$–álgebra monógena con generador u. En efecto, como $gr(q_u) = \delta$, el conjunto $\{1, u, \ldots, u^{\delta-1}\}$ es linealmente independiente sobre $\mathbb{Q}$ y por lo tanto una $\mathbb{Q}$–base de B. Así pues, $B = \mathbb{Q}[u]$ y $A_u = \mathbb{Q}[t]$ son $\mathbb{Q}$–álgebras monógenas cuyos generadores respectivos, u y t, poseen el mismo polinomio minimal $q_u \in \mathbb{Q}[T]$. Esto implica el enunciado del corolario. ∎

El Corolario 2.5 admite una interpretación geométrica en los siguientes términos. Tomemos una forma $\mathbb{Q}$–lineal $U = \lambda_1 X_1 + \cdots + \lambda_n X_n$ cuya imagen u en B es un elemento primitivo de V. Como $\{1, t, \ldots, t^{\delta-1}\}$ es una base del $\mathbb{Q}$–espacio vectorial A_u, entonces para todo i con $1 \leq i \leq n$ existe un único polinomio $v_i(T) \in \mathbb{Q}[T]$ de grado a lo sumo $\delta - 1$ tal que el elemento $v_i(t)$ de A_u se aplica en el elemento $\bar{X}_i$ de B (donde $\bar{X}_i$ denota la clase residual de la indeterminada X_i), o equivalentemente, tal que $X_i - v_i(U)$ se halla en el ideal I. Entonces U induce el morfismo regular

$$\begin{aligned} U : \mathbb{C}^n &\to \mathbb{C}, \\ (x_1, \ldots, x_n) &\mapsto (\lambda_1 x_1 + \cdots + \lambda_n x_n), \end{aligned}$$

que define un isomorfismo entre V y H_u. Es claro que el morfismo inverso de U viene dado por $U^{-1}(T) = (v_1(T), \ldots, v_n(T))$. En tal caso se dice que los polinomios $v_1, \ldots, v_n$ *parametrizan* la variedad V, por los ceros de H_u.

Ahora estamos en condiciones de definir en forma precisa la noción de *resolución geométrica* de una variedad 0–dimensional (Compárese con [20], [31], [18], [19]).

Definición 2.6 *Sea $V \subseteq \mathbb{C}^n$ una $\mathbb{Q}$–variedad 0–dimensional e I su ideal asociado. Los siguientes ítems definen una resolución geométrica de la variedad V:*

- *Una forma $\mathbb{Q}$–lineal $U = \lambda_1 X_1 + \cdots + \lambda_n X_n$ cuya imagen u en $B := \mathbb{Q}[X_1, \ldots, X_n]/I$ es un elemento primitivo de V.*
- *El polinomio minimal mónico $q_u \in \mathbb{Q}[T]$ de u.*
- *La parametrización de V dada por polinomios $v_1, \ldots, v_n$ en $\mathbb{Q}[T]$ tales que $X_j - v_j(U) \in I$ y $gr(v_i) < gr(q_u)$ para todo $1 \leq j \leq n$.*

Parte I

Interpolación implícita

Capítulo 3

Bezoutianos e interpolación multivariada

Nuestro algoritmo se deriva esencialmente de un método de interpolación multivariada expuesto por Kronecker en [26] (véase también [17]), que explicaremos a continuación.

Como es sabido, el método de Lagrange consiste en construir para un conjunto dado de nodos $t^{(1)}, \ldots, t^{(\delta)} \in \mathbb{C}$ una "base de Lagrange"

$$P_j(T) = \frac{\prod_{k=1,k\neq j}^{\delta}(T - t^{(k)})}{\prod_{k=1,k\neq j}^{\delta}(t^{(j)} - t^{(k)})}, \qquad 1 \leq j \leq \delta,$$

del espacio de polinomios $\Pi_{\delta-1}$. Estos polinomios verifican $P_j(t^{(k)}) = 0$ si $j \neq k$ y $P_j(t^{(k)}) = 1$ si $j = k$, de modo que el polinomio P que interpola los valores $f(t^{(1)}), \ldots, f(t^{(\delta)}) \in \mathbb{C}$ se escribe $P = \sum_{j=1}^{\delta} f(t^{(j)})P_j$.

El método de interpolación de Kronecker generaliza esta construcción al caso multivariado de modo que para cada conjunto de nodos $x^{(1)}, \ldots, x^{(\delta)} \in \mathbb{C}^n$ se hallan polinomios $P_1, \ldots, P_\delta$ en $\mathbb{C}[X_1, \ldots, X_n]$ que forman una base de un espacio de interpolantes tal que, como en el caso univariado, el polinomio que interpola los valores $F(x^{(1)}), \ldots, F(x^{(\delta)})$ se escribe $\sum_{j=1}^{\delta} F(x^{(j)})P_j$.

Por otro lado, a diferencia del método de Lagrange, que se aplica a un conjunto arbitrario de nodos, el método de Kronecker asume que el conjunto de nodos $V \subseteq \mathbb{C}^n$ viene representado por un conjunto de polinomios $F_1, \ldots, F_n$ en $\mathbb{C}[X_1, \ldots, X_n]$ tales que $V = V(F_1, \ldots, F_n)$, y de hecho hace referencia a las ecuaciones $F_1 = 0, \ldots, F_n = 0$ para construir la antedicha base de polinomios.

Antes de explicar este método vamos a establecer las siguientes hipótesis que serán asumidas de ahora en adelante: Supondremos que la $\mathbb{Q}$–variedad 0-dimensional $V = \{x^{(1)}, \ldots, x^{(\delta)}\} \subseteq \mathbb{C}^n$ viene dada por n polinomios $F_1, \ldots, F_n$ en $\mathbb{Q}[X_1, \ldots, X_n]$ que verifican la siguiente condición:

- El ideal $(F_1, \ldots, F_i)$ es radical para $1 \leq i \leq n$.
- Los polinomios $F_1, \ldots, F_n$ forman una sucesión regular, es decir, la variedad $V(F_1, \ldots, F_i)$ es de dimensión $n - i$ para $1 \leq i \leq n$.

Observamos que la condición de que $(F_1, \ldots, F_n)$ sea un ideal radical 0-dimensional, que fuera también requerida por Kronecker en [26], es esencial para el método. Por otro lado, la condición de radicalidad y $(n-i)$–dimensionalidad para $1 \leq i \leq n-1$ no es realmente restrictiva, ya que es posible recuperar esta situación mediante una combinación lineal genérica de las ecuaciones originales, como se demuestra por ejemplo en [14] y [25].

3.1. Fórmula de interpolación de Kronecker

El método de Kronecker se puede describir en los siguientes términos:

Sea $J := J(F_1, \ldots, F_n)$ el jacobiano de la sucesión de polinomios $F_1, \ldots, F_n$, es decir, J es el polinomio en $\mathbb{Q}[X_1, \ldots, X_n]$ definido mediante el determinante

$$J(F_1, \ldots, F_n) := \det\left(\frac{\partial F_j}{\partial X_k}\right) \tag{3.1}$$

Recordemos que el ideal 0-dimensional $(F_1, \ldots, F_n)$ es radical si y solo si todo punto $x^{(i)}$ de la variedad V es no singular (véase por ejemplo [7, Corollary 2.6]). Por el criterio del jacobiano ([27, VI, Theorem 1.15], [11, Theorem 16.19]), esto a su vez equivale a que $J(x^{(i)}) \neq 0$ para todo punto $x^{(i)}$ de V, o también, a que la clase residual $\overline{J}$ de J es una unidad en el anillo cociente $\mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_n)$.

Para cada i con $1 \leq i \leq \delta$, sea $\mathcal{M}_i \subseteq \mathbb{C}[X_1, \ldots, X_n]$ el ideal de los polinomios que se anulan en $x^{(i)}$. Como $\mathbb{C}$ es un cuerpo algebraicamente cerrado, $\mathcal{M}_i$ es el ideal maximal de $\mathbb{C}[X_1, \ldots, X_n]$ generado por los polinomios $X_1 - x_1^{(i)}, \ldots, X_n - x_n^{(i)}$. Ciertamente todo polinomio F_j $(1 \leq j \leq n)$ está en el ideal $\mathcal{M}_i$. Por lo tanto para cada par de índices i, j con $1 \leq i \leq \delta, 1 \leq j \leq n$ existen n polinomios, no únicos, $\gamma_{j,k}^{(i)}(X)$ $(1 \leq k \leq n)$ en $\mathbb{C}[X_1, \ldots, X_n]$ que satisfacen las identidades

$$F_j(X) = \sum_{k=1}^{n} \gamma_{j,k}^{(i)}(X)(X_k - x_k^{(i)}). \tag{3.2}$$

Fijemos arbitrariamente una elección de los polinomios $\gamma_{j,k}^{(i)}$. Para cada i con $1 \leq i \leq \delta$ se define el polinomio $D_i \in \mathbb{C}[X_1, \ldots, X_n]$ como el determinante de la matriz $(\gamma_{j,k}^{(i)})_{1 \leq j,k \leq n}$, cuya entrada de la fila j y la columna k es el polinomio $\gamma_{j,k}^{(i)}$. En el lema siguiente se enuncia una importante propiedad que satisfacen los polinomios D_i.

Lema 3.1 *Para todo par de índices i, h con $1 \leq i, h \leq \delta$ vale $D_i(x^{(h)}) = 0$ si $i \neq h$ y $D_i(x^{(i)}) = J(x^{(i)}) \neq 0$ si $i = h$.*

Demostración: Sean i, h un par de índices distintos con $1 \leq i, h \leq \delta$. Especializando $X = x^{(h)}$ en la identidad (3.2) para $1 \leq j \leq n$ se obtiene un sistema homogéneo de ecuaciones lineales con matriz de coeficientes $(\gamma_{j,k}^{(i)}(x^{(h)}))_{1 \leq j,k \leq n} \in \mathbb{C}^{n \times n}$, que posee la solución no trivial $x^{(h)} - x^{(i)} \in \mathbb{C}^n$. Por lo tanto el determinante del sistema debe ser cero, es decir, $D_i(x^{(h)}) = \det(\gamma_{j,k}^{(i)}(x^{(h)})) = 0$.

Sea ahora $i = h$. Derivando ambos miembros de la identidad (3.2) respecto de la variable X_k resulta

$$\frac{\partial F_j(X)}{\partial X_k} = \gamma_{j,k}^{(i)}(X) + \sum_{h=1}^{n} \frac{\partial \gamma_{j,h}^{(i)}(X)}{\partial X_k}(X_h - x_h^{(i)}).$$

Especializando X en $x^{(i)}$ se obtiene $\gamma_{j,k}^{(i)}(x^{(i)}) = \partial F_j(x^{(i)})/\partial X_k$. Por lo tanto

$$D_i(x^{(i)}) = \det(\gamma_{j,k}^{(i)}(x^{(i)})) = \det\left(\frac{\partial F_j(x^{(i)})}{\partial X_k}\right) = J(x^{(i)}),$$

lo que concluye la demostración. ∎

En vista de la analogía con la base de Lagrange establecida en el Lema 3.1, nos referimos a la sucesión de polinomios $D_1, \ldots, D_\delta$ como a una *base de Kronecker* asociada al conjunto de nodos $x^{(1)}, \ldots, x^{(\delta)}$.

Sea ahora un polinomio arbitrario F en $\mathbb{Q}[X_1, \ldots, X_n]$. Como consecuencia inmediata del Lema 3.1 se obtiene el siguiente corolario:

Corolario 3.2 *El polinomio en $\mathbb{C}[X_1, \ldots, X_n]$ expresado por la fórmula*

$$\sum_{j=1}^{\delta} F(x^{(j)}) \frac{D_j(X)}{J(x^{(j)})}, \tag{3.3}$$

interpola a F en los puntos $x^{(1)}, \ldots, x^{(\delta)}$ de V.

Llamamos a la expresión (3.3) la *fórmula de interpolación de Kronecker*.

Por último observamos que para calcular el interpolante mediante la fórmula (3.3) es necesario conocer tanto los nodos $x^{(1)}, \ldots, x^{(\delta)}$ como las ecuaciones $F_1 = 0, \ldots, F_n = 0$ que los definen. Por otra parte el método descripto no es completamente constructivo pues solo se afirma la existencia de los polinomios $\gamma_{j,k}^{(i)}$.

3.1.1. Fórmula de interpolación de Kronecker en una variable

Como mencionamos al comienzo de esta sección la fórmula de interpolación de Kronecker (3.3) es una generalización de la fórmula de Lagrange en una variable. De hecho, si $n = 1$ y $q(T) = (T - t^{(1)}) \cdots (T - t^{(\delta)})$ es un polinomio en $\mathbb{Q}[T]$ libre de cuadrados y de grado δ, el jacobiano de q es simplemente la derivada primera de q, que notamos q'. En este caso los polinomios D_j están unívocamente determinados por las identidades $D_j(T) = \prod_{k=1,k\neq j}^{\delta}(T - t^{(k)})$ para todo $1 \leq j \leq \delta$, de modo que con $D_1(T), \ldots, D_\delta(T)$ recuperamos la base de Lagrange. Por consiguiente obtenemos el siguiente corolario:

Corolario 3.3 *Sea $f \in \mathbb{Q}[T]$ un polinomio arbitrario. Con las notaciones anteriores el polinomio interpolante de Lagrange de f en los nodos $t^{(1)}, \ldots, t^{(\delta)}$ se expresa en la forma*

$$\sum_{j=1}^{\delta} f(t^{(j)}) \frac{D_j(T)}{q'(t^{(j)})}. \tag{3.4}$$

En adelante nos referiremos a (3.4) como a la *fórmula de interpolación de Lagrange*.

3.2. Bezoutianos y trazas en álgebras 0-dimensionales

Nuestro objetivo es expresar el polinomio interpolante del Corolario 3.3 sin hacer referencia explícita a los nodos $x^{(1)}, \ldots, x^{(\delta)}$ ni a los valores $F(x^{(1)}), \ldots, F(x^{(\delta)})$, sino solo a los polinomios $F_1, \ldots, F_n$ y F. Esto será llevado a cabo en el Capítulo 4. Como primer paso en esta dirección vamos a introducir en esta sección la noción de *bezoutiano* de la sucesión $F_1, \ldots, F_n$ (véase [14], [25], [32], [12]). Este concepto nos permitirá encontrar un procedimiento constructivo y eficiente para obtener los polinomios $D_1, \ldots, D_\delta$ de una base de Kronecker, cuyos grados estén además convenientemente acotados.

3.2.1. Bezoutianos

Introduzcamos un nuevo conjunto de variables $Y_1, \ldots, Y_n$. La idea del bezoutiano surge naturalmente al realizar la misma contrucción hecha en la Sección 3.1 con los puntos concretos $x^{(i)}$ de V, pero ahora con el punto "genérico" $Y := (Y_1, \ldots, Y_n)$. Para cada $1 \leq j \leq n$ sea $F_j^{(Y)} := F_j(Y_1, \ldots, Y_n)$ el polinomio de $\mathbb{Q}[Y_1, \ldots, Y_n]$ que se obtiene substituyendo en F_j las variables $X_1, \ldots, X_n$ por $Y_1, \ldots, Y_n$. En el siguiente lema se establece una identidad análoga a (3.2):

Lema 3.4 *Sea d una cota para los grados de los polinomios $F_1, \ldots, F_n$. Existen n^2 polinomios $\gamma_{j,k}(X,Y)$ $(1 \leq j,k \leq n)$ en $\mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ de grados totales en las variables $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ acotados por $d-1$ tales que se verifica la relación:*

$$F_j - F_j^{(Y)} = \sum_{k=1}^{n} \gamma_{j,k}(X,Y)(X_k - Y_k). \tag{3.5}$$

Al igual que antes, los polinomios $\gamma_{j,k}$ no están unívocamente determinados por la sucesión $F_1, \ldots, F_n$.

Demostración: Sea $1 \leq j \leq n$ fijo. Para cada $0 \leq k \leq n$ sea $F_j^{(k)}$ el polinomio en $\mathbb{Q}[X,Y]$ que resulta de reemplazar en F_j las variables $(X_1, \ldots, X_k)$ por $(Y_1, \ldots Y_k)$, en particular $F_j^{(0)} = F_j$. Para cada $1 \leq k \leq n$ escribimos a $F_j^{(k-1)}$ como un polinomio en la variable X_k:

$$F_j^{(k-1)} = \sum_{m=0}^{d} A_{j,m}^{(k-1)} X_k^m,$$

donde los $A_{j,m}^{(k-1)}$ son polinomios en $\mathbb{Q}[X,Y]$ que no contienen la variable X_k. Se observa que el grado total de $A_{j,m}^{(k-1)}$ está acotado por $d-m$. Ahora, como $F_j^{(k)}$ se obtiene de $F_j^{(k-1)}$ substituyendo la variable X_k por Y_k, de la expresión anterior se deduce:

$$F_j^{(k)} = \sum_{m=0}^{d} A_{j,m}^{(k-1)} Y_k^m.$$

Para $1 \leq m \leq d$ y $1 \leq k \leq n$, sea B_k^m el polinomio $B_k^m := \sum_{l=0}^{m-1} X_k^l Y_k^{m-1-l}$, que satisface la identidad $B_k^m(X_k - Y_k) = X_k^m - Y_k^m$. Entonces restando $F_j^{(k)}$ de $F_j^{(k-1)}$ se obtiene

$$F_j^{(k-1)} - F_j^{(k)} = \left(\sum_{m=1}^{d} A_{j,m}^{(k-1)} B_k^m \right) (X_k - Y_k), \quad (1 \leq k \leq n).$$

(Obsérvese que el término $A_{j,0}^{(k-1)}$ se cancela).

Por último definimos $\gamma_{j,k} := \sum_{m=1}^{d} A_{j,m}^{(k-1)} B_k^m$. Por construcción es claro que los grados de los polinomios $\gamma_{j,k}$ están acotados por $d-1$ y verifican

$$F_j - F_j^{(Y)} = \sum_{k=1}^{n} F_j^{(k-1)} - F_j^{(k)} = \sum_{k=1}^{n} \gamma_{j,k}(X_k - Y_k).$$

Esto concluye la demostración. ∎

Por supuesto, es posible demostrar el lema anterior considerando el desarrollo de Taylor de los polinomios F_j, sin embargo se optó por la demostración dada ya que se usa en la construcción efectiva en el Lema 5.11.

El lema 3.4 nos permite dar la siguiente definición:

Definición 3.5 *Para una elección arbitraria de polinomios $\gamma_{j,k}$ que verifiquen las identidades* (3.5)*, sea D el polinomio en $\mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ definido como el determinante de la matriz $(\gamma_{j,k})_{1 \leq j,k \leq n}$ cuya entrada de la fila j y la columna k es el polinomio $\gamma_{j,k}(X, Y)$. El polinomio D se llama un bezoutiano de la sucesión de polinomios $F_1, \ldots, F_n$.*

De la demostración del Lema 3.4 dedujimos que es posible construir a partir de los polinomios $F_1, \ldots, F_n$ un bezoutiano D cuyo grado total en las variables $X_1, \ldots, X_n$, $Y_1, \ldots, Y_n$ sea a lo sumo $n(d-1)$. Por otro lado es claro que los polinomios $\gamma_{j,k}^{(i)}$ definidos en la forma $\gamma_{j,k}^{(i)}(X) := \gamma_{j,k}(X, x^{(i)})$ verifican las identidades (3.2). Por lo tanto los polinomios D_i de la fórmula de Kronecker (3.3) pueden tomarse como $D_i := D(X, x^{(i)})$ para un tal bezoutiano D. Este hecho, junto con los resultados sobre trazas en álgebras 0–dimensionales de la próxima sección, permitirán en el Capítulo 4 eliminar completamente los puntos $x^{(i)}$ y los valores $F(x^{(i)})$ de la expresión del polinomio interpolante.

3.2.2. Trazas en álgebras 0-dimensionales

Sea nuevamente $B := \mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_n)$ el anillo de coordenadas de la variedad $V := V(F_1, \ldots, F_n)$ y sea $B^* := \mathrm{Hom}_{\mathbb{Q}}(B, \mathbb{Q})$ el espacio dual del $\mathbb{Q}$–espacio vectorial B. Existe un elemento relevante de B^* que se denota con Tr y se llama la *traza estándar* de B. Se define de la siguiente manera: dado $f \in B$, sea η_f la homotecia de multiplicación por f, como fue definida en la Sección 2.2. La imagen $Tr(f)$ por Tr se define como la traza ordinaria del endomorfismo η_f. En el Capítulo 4 hallaremos una base de un espacio de interpolación para el conjunto de nodos V, de tal modo que las coordenadas del polinomio interpolante en dicha base se pueden expresar en términos de la traza. En la presente sección estudiamos las propiedades de la traza necesarias a tal efecto.

Mediante el empleo del elemento primitivo podemos reducir el estudio de la traza estándar al caso univariado. Sea entonces $u \in B$ un elemento primitivo de V, $q_u \in \mathbb{Q}[T]$ su polinomio minimal y A_u la $\mathbb{Q}$–álgebra $A_u := \mathbb{Q}[T]/(q_u)$. En forma análoga al caso multivariado consideramos el espacio dual $A_u^* = \mathrm{Hom}_{\mathbb{Q}}(A_u, \mathbb{Q})$ y la correspondientemente traza estándar de A_u, que notamos con tr. En vista del próximo lema, hacemos las siguientes observaciones. En primer lugar, como sabemos por el Corolario 2.5 existe un isomorfismo de $\mathbb{Q}$–álgebras $\theta : B \to A_u$, tal que $\theta(u) = t$ (donde t denota la

clase residual de la indeterminada T). Luego es claro que $Tr = tr \circ \theta$. Considérese ahora una forma lineal $U \in \mathbb{Q}[X_1, \ldots, X_n]$ que induce el elemento primitivo u de V. Como vimos en la Sección 2.2, la forma lineal U determina una biyección entre V y el conjunto de raíces de q_u. Luego si para cada punto $x^{(k)} \in V$ definimos $t^{(k)} \in \mathbb{C}$ como $t^{(k)} := U(x^{(k)})$, se tiene que $q_u(T) = (T - t^{(1)}) \cdots (T - t^{(\delta)})$. Sea F un polinomio arbitrario en $\mathbb{Q}[X_1, \ldots, X_n]$ y f su imagen en B. Sea además $P \in \mathbb{Q}[T]$ un representante del elemento de A_u definido por $p := \theta(f)$. Entonces de la identidad $f = \overline{P(U)}$ en B se sigue que para todo $1 \leq k \leq \delta$ vale $F(x^{(k)}) = P(U(x^{(k)})) = P(t^{(k)})$. Con estas observaciones y notaciones en mente enunciamos el siguiente lema:

Lema 3.6 *Sea Tr la traza estándar de B. Entonces para todo $f \in B$ vale $Tr(f) = \sum_{k=1}^{\delta} F(x^{(k)})$.*

Demostración: Como antes sea $f \in B$ arbitrario y $p := \theta(f) \in A_u$. Sea M_t la matriz de la homotecia η_t en la base $\mathcal{A} := \{1, t, \ldots, t^{\delta-1}\}$ de A_u. Puesto que q_u es un polinomio anulador de η_t, M_t es la matriz compañera de q_u. Además, como q_u es libre de cuadrados (Lema 2.4) la matriz M_t es diagonalizable. Es decir, si $q_u(T) = (T - t^{(1)}) \ldots (T - t^{(\delta)})$, entonces se tiene la siguiente semejanza de matrices en $\mathbb{C}^{\delta \times \delta}$:

$$M_t \sim \begin{pmatrix} t^{(1)} & & \\ & \ddots & \\ & & t^{(\delta)} \end{pmatrix}.$$

Como antes, sea $f \in B$ arbitrario y $p := \theta(f) \in A_u$. Luego, si M_p es la matriz de la homotecia η_p, también en la base $\mathcal{A}$, entonces se tiene que

$$M_p = P(M_t) \sim \begin{pmatrix} P(t^{(1)}) & & \\ & \ddots & \\ & & P(t^{(\delta)}) \end{pmatrix}.$$

Finalmente puesto que la traza es invariante por semejanza de matrices, se obtiene

$$Tr(f) = tr(p) = \sum_{k=1}^{\delta} P(t^{(k)}) = \sum_{k=1}^{\delta} F(x^{(k)}).$$

Esto completa la demostración. ∎

Ahora dotamos a B^* con la estructura de B–módulo definida a partir del homomorfismo $B \times B^* \to B^*$ que asocia a cada par (f, σ) en $B \times B^*$ el morfismo $\mathbb{Q}$–lineal $f\sigma : B \to \mathbb{Q}$ definido por $(f\sigma)(g) = \sigma(fg)$ para cada elemento $g \in B$. En particular

A_u^* resulta un A_u–módulo. Además de la traza estándar es conveniente introducir un segundo elemento β_0 de B^* que se define de la siguiente manera: recordando que la clase residual $\overline{J}$ del Jacobiano J es una unidad de B, definimos $\beta_0 := \bar{J}^{-1}Tr$. El elemento σ_0 de A_u^* que corresponde a β_0 es $\sigma_0 := (\bar{q}_u')^{-1}\, tr$ y es conocido como la *traza de Tate*. El siguiente lema es importante para la evaluación efectiva de la traza estándar.

Lema 3.7 *Sea σ_0 en A_u^* la traza de Tate. Supóngase que un elemento p de A_u se escribe en la forma $p = b_{\delta-1}t^{\delta-1} + \cdots + b_0$ en la base $\{1, t, \ldots, t^{\delta-1}\}$ de A_u. Entonces vale $\sigma_0(p) = b_{\delta-1}$.*

Demostración: Sea $P = b_{\delta-1}T^{\delta-1} + \cdots + b_0 \in \mathbb{Q}[T]$ el representante de p con $\deg(P) < \delta$. Sean $D_1, \ldots, D_{\delta-1}$ los polinomios en $\mathbb{C}[T]$ definidos por $D_1 := \prod_{j\neq 1}(T - t^{(j)}), \ldots, D_\delta := \prod_{j\neq\delta}(T - t^{(j)})$. Entonces según la fórmula de Lagrange (3.4), P se puede escribir en la forma $P = \sum_{j=1}^{\delta} P(t^{(j)})D_j/q_u'(t^{(j)})$. Como los polinomios D_j son mónicos y de grado $\delta - 1$, el coeficiente $b_{\delta-1}$ de P debe ser $b_{\delta-1} = \sum_{j=1}^{\delta} P(t^{(j)})/q_u'(t^{(j)})$. Luego aplicando el Lema 3.6 para $B = A_u$ resulta $b_{\delta-1} = tr(\bar{q}_u'^{-1}p) = (\bar{q}_u'^{-1}tr)(p) = \sigma_0(p)$. ∎

Capítulo 4

Construcción del espacio de interpolantes

En este capítulo abordamos el problema de hallar un espacio de interpolantes Π_V para el conjunto de nodos definido por la $\mathbb{Q}$-variedad $V \subseteq \mathbb{C}^n$. Ahora bien, si queremos reducir el grado de los interpolantes lo mejor que se puede esperar del espacio Π_V es que sea un *espacio de interpolantes de grado minimal*. Esto significa que para todo $F \in \mathbb{Q}[X_1, \ldots, X_n]$ el interpolante $P \in \Pi_V$, definido por las condiciones $P(x^{(i)}) = F(x^{(i)})$, $1 \leq i \leq \delta - 1$, satisface $gr(P) \leq gr(F)$. En un contexto diferente al nuestro, a saber, cuando el conjunto de nodos está dado en forma explícita, han habido dos construcciones sistemáticas de espacios de interpolantes con esa propiedad: los "least maps" de de Boor y Ron ([9], [10]) y los espacios obtenidos apartir de las H-bases ([29], [33]).

Notemos con Π_k^n el subespacio de $\mathbb{Q}[X_1, \ldots, X_n]$ formado por los polinomios de grado total a lo sumo k. Sea m la cota óptima para los grados de los polinomios en Π_V, es decir, $m := \text{mín}\{k : k \in \mathbb{N}_0, \Pi_V \subseteq \Pi_k^n\}$. Por comodidad llamamos a m el grado del espacio Π_V. El hecho de que Π_V sea un espacio de grado minimal implica que no existe ningún subespacio de Π_{m-1}^n que sea un espacio de interpolantes para V. Para ver esto, elíjase una base $P_1, \ldots, P_\delta$ de Π_V. Entonces uno de estos polinomios, digamos P_1, debe tener grado m. Sin embargo, del supuesto de que existe un subespacio de Π_{m-1}^n que permite interpolar, se deduce la existencia de un polinomio $Q \in \Pi_{m-1}^n$ que satisface $Q(x^{(i)}) = P_1(x^{(i)})$ para $1 \leq i \leq \delta$. Luego el interpolante con respecto a Q en Π_V es P_1. Pero $gr(P_1) > gr(Q)$, lo que contradice que Π_V es de grado minimal.

Consideremos ahora el caso univariado ($n = 1$). Sea $q_0 \in \mathbb{Q}[T]$ libre de cuadrados y de grado δ y sea $V = \{t^{(1)}, \ldots, t^{(\delta)}\} \subseteq \mathbb{C}$ el conjunto de ceros de q_0. Veamos que $\Pi_{\delta-1}^1$ es un espacio de interpolantes de grado minimal para V. En efecto, sea $f \in \mathbb{Q}[T]$ un polinomio arbitrario. Mediante el algoritmo de división obtenemos polinomios $h \in \mathbb{Q}[T]$ y $r \in \Pi_{\delta-1}^1$ tales que $f = q_0 h + r$. Pero entonces $f(t^{(i)}) = r(t^{(i)})$ para $1 \leq i \leq \delta$, con lo cual r es el único interpolante en $\Pi_{\delta-1}^1$ con respecto a f. Es claro además que $r = 0$

o $gr(f) \geq gr(r)$. Se concluye que en el caso univariado el grado del interpolante debe ser en general del mismo orden que la cardinalidad del conjunto de nodos. Sin embargo en el caso multivariado existen espacios de interpolantes Π_V de grado esencialmente menor a la cardinalidad de V. Primeramente observamos que si U es una forma lineal en $\mathbb{Q}[X_1, \ldots, X_n]$ separante de V podemos obtener un espacio de interpolantes $\mathcal{P}$ de la siguiente forma obvia: $\mathcal{P} :=< 1, U, \ldots, U^{\delta-1} >_{\mathbb{Q}}$.

Por otra parte, en nuestro caso, la variedad V está dada por n polinomios $F_1, \ldots, F_n$ en $\mathbb{Q}[X_1, \ldots, X_n]$, que forman una sucesión regular reducida y que generan un ideal radical $(F_1, \ldots, F_n)$. En esta situación la desigualdad de Bézout ([22], [15], [37]) afirma que si $d := \text{máx}\{gr(F_1), \ldots, gr(F_n)\}$, entonces $\delta = \#V \leq d^n$ y esta es una cota óptima para la cardinalidad δ. No obstante, en el teorema siguiente se demuestra la existencia de un espacio de interpolantes Π_V para V, que, aunque no es de grado minimal, tiene grado a lo sumo $n(d-1)$. De modo que en el peor caso el grado de $\mathcal{P}$ es d^n, mientras que para el grado de Π_V se tiene una cota esencialmente menor.

Teorema 4.1 *Sean $F_1, \ldots, F_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ de grados a lo sumo d que definen una sucesión regular reducida y que generan el ideal radical $(F_1, \ldots, F_n)$. Sea $V := V(F_1, \ldots, F_n)$ la $\mathbb{Q}$-variedad 0-dimensional de cardinalidad δ definida por estos polinomios y B su anillo de coordenadas. Sea U una forma lineal en $\mathbb{Q}[X_1, \ldots, X_n]$ cuya imagen u en B es un elemento primitivo de V y sea Tr la traza estándar de B. Entonces existen δ polinomios $G_0, \ldots, G_{\delta-1}$ en $\mathbb{Q}[X_1, \ldots, X_n]$ de grados a lo sumo $n(d-1)$ tales que sus imagenes $g_0, \ldots, g_{\delta-1}$ en B forman una base del $\mathbb{Q}$-espacio vectorial B y todo $f \in B$ se escribe en la forma:*

$$f = \sum_{i=0}^{\delta-1} Tr(\bar{J}^{-1} f u^i) g_i. \tag{4.1}$$

En particular $\Pi_V :=< G_0, \ldots, G_{\delta-1} >_{\mathbb{Q}}$ es un espacio de interpolantes para V.

Demostración: Sea q_u en $\mathbb{Q}[T]$ el polinomio minimal de u. Sean también $v_1, \ldots, v_n$ los polinomios en $\mathbb{Q}[T]$ de grados acotados por $\delta - 1$ que determinan la parametrización de la variedad V con respecto a u. Se verifican por lo tanto las congruencias:

$$\begin{aligned} Y_k &\equiv v_k(U(Y)) \mod (F_1(Y), \ldots, F_n(Y)) \ (1 \leq k \leq n), \\ q_u(U(Y)) &\equiv 0 \mod (F_1(Y), \ldots, F_n(Y)). \end{aligned} \tag{4.2}$$

Sea $D(X, Y)$ en $\mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ un bezoutiano de la sucesión de polinomios $F_1, \ldots, F_n$, de grado total en las variables $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ acotado por $n(d-1)$ según se construyó en la Subsección 3.2.1. Sea $D_1 := D(X_1, \ldots, X_n, v_1(T), \ldots, v_n(T))$ el polinomio en $\mathbb{Q}[X_1, \ldots, X_n, T]$ que se obtiene al substituir en D las variables $Y_1, \ldots, Y_n$ por los polinomios univariados $v_1(T), \ldots, v_n(T)$ respectivamente. Consideramos a D_1

como un polinomio en la variable T con coeficientes en el anillo $\mathbb{Q}[X_1, \ldots, X_n]$. Puesto que q_u es mónico, podemos realizar la división con resto de D_1 por q_u en el anillo de polinomios $\mathbb{Q}[X_1, \ldots, X_n][T]$. El resto r de D_1 se escribe por lo tanto en la forma:

$$r = \sum_{j=0}^{\delta-1} G_j(X_1, \ldots, X_n) T^j,$$

para ciertos polinomios G_j en $\mathbb{Q}[X_1, \ldots, X_n]$ $(1 \leq j \leq n)$, ya que $\mathbb{Q}[X, T]/(q_u(T))$ es un $\mathbb{Q}[X]$-módulo libre con base $\{1, T, \ldots, T^{\delta-1}\}$. Como D_1 es de grado a lo sumo $n(d-1)$ en las variables $X_1, \ldots, X_n$ y q_u no depende de las variables X_i, los polinomios G_j también tienen sus grados acotados por $n(d-1)$. Ahora la congruencia $D_1 \equiv r \mod (q_u)$ en el anillo $\mathbb{Q}[X_1, \ldots, X_n][T]$ junto con las ecuaciones (4.2) implican la congruencia:

$$D(X, Y) \equiv \sum_{j=0}^{\delta-1} G_j(X_1, \ldots, X_n) U(Y)^j \mod (F_1(Y), \ldots, F_n(Y)), \tag{4.3}$$

en el anillo $\mathbb{Q}[Y_1, \ldots, Y_n]$.

Tomemos un polinomio arbitrario F en $\mathbb{Q}[X_1, \ldots, X_n]$ y sea f su imagen en B. Según la fórmula de interpolación de Kronecker (3.3), el polinomio

$$P := \sum_{k=1}^{\delta} F(x^{(k)}) \frac{D(X, x^{(k)})}{J(x^{(k)})}$$

interpola a F en los puntos $x^{(1)}, \ldots, x^{(\delta)}$ de V. En principio no es claro que este polinomio tenga coeficientes racionales. No obstante, especializando en la congruencia (4.3) la variable Y en el punto $x^{(k)}$ de V para $1 \leq k \leq \delta$, se obtienen las identidades

$$D(X, x^{(k)}) = \sum_{i=0}^{\delta-1} G_i(X_1, \ldots, X_n) U(x^{(k)})^i \ \ (1 \leq k \leq \delta).$$

En consecuencia, podemos reescribir al polinomio interpolante P en la forma:

$$\begin{aligned} P(X) &= \sum_{k=1}^{\delta} \frac{F(x^{(k)})}{J(x^{(k)})} \left(\sum_{i=0}^{\delta-1} G_i(X_1, \ldots, X_n) U(x^{(k)})^i \right) \\ &= \sum_{i=0}^{\delta-1} \left(\sum_{k=1}^{\delta} \frac{F(x^{(k)}) U(x^{(k)})^i}{J(x^{(k)})} \right) G_i(X_1, \ldots, X_n). \end{aligned}$$

Luego aplicando el Lema 3.6 obtenemos la identidad

$$P(X) = \sum_{i=0}^{\delta-1} Tr(\bar{J}^{-1} f u^i) G_i(X).$$

En particular P es un polinomio en $\mathbb{Q}[X_1, \ldots, X_n]$ que interpola a F sobre los puntos de V. Puesto que el ideal $(F_1, \ldots, F_n)$ es radical, se deduce la identidad de clases residuales $\bar{P} = f$ en B. En consecuencia, tomando clases residuales en ambos miembros de la última expresión de P obtenemos la fórmula (4.1).

En particular, puesto que $\dim_{\mathbb{Q}} B = \delta$, deducimos que $\mathcal{B} = \{g_0, \ldots, g_{\delta-1}\}$ es una base del $\mathbb{Q}$-espacio vectorial B. ∎

Como hecho interesante cabe mencionar que la fórmula (4.1) implica, com veremos a continuación, que B^* es un B-módulo libre de rango 1. Cada elemento σ de B^* que genera a B^* como B-módulo se dice una *traza* de B. En estos términos, tenemos el siguiente corolario:

Corolario 4.2 *El elemento $\beta_0 := \bar{J}^{-1}.Tr$ de B^* es una traza de B. En particular, la traza de Tate σ_0 es un traza de A_u.*

Demostración: Si en (4.1) substituimos f por g_j deducimos que $(u^i\beta_0)(g_j) = \delta_{i,j}$ para todo $0 \leq i, j \leq \delta - 1$. Es decir, $\{\beta_0, u\beta_0, \ldots, u^{\delta-1}\beta_0\}$ es la base dual de $\mathcal{B}$. Entonces es inmediato que β_0 genera a B^* como B-módulo. Pues entonces todo β en B^* se escribe en la forma $\beta = \sum_{j=0}^{\delta-1}(\lambda_j u^j)\beta_0$ para ciertos λ_j en $\mathbb{Q}$. Por lo tanto $\beta = \left(\sum_{j=0}^{\delta-1} \lambda_j u^j\right)\beta_0$ con $\sum_{j=0}^{\delta-1} \lambda_j u^j$ en B. Por último β_0 es libre de torsión, dado que si para algún f es $f\beta_0 = 0$, entonces $0 = (f\beta_0)(u^j) = \beta_0(u^j f)$ para todo $0 \leq j \leq \delta - 1$, y por lo tanto de (4.1) se sigue $f = 0$. ∎

Conclusión A partir del Teorema 4.1 podemos concluir que para un polinomio $F \in \mathbb{Q}[X_1, \ldots, X_n]$ de grado arbitrario, el polinomio

$$P := \sum_{i=0}^{\delta-1} Tr(\bar{J}^{-1}\bar{F}u^i)G_i(X), \tag{4.4}$$

interpola a F sobre el conjunto de nodos V y además $gr(P) \leq n(d-1)$. Según se vió en la demostración de este teorema, P no es otra cosa que una reescritura del polinomio interpolante de Kronecker (3.3).

Capítulo 5

Cálculo del polinomio interpolante

En este capítulo vamos exhibir un procedimiento algorítmico para calcular la expresión del polinomio interpolante dada en (4.4). Comenzamos precisando las estructuras de datos que se utilizan.

5.1. Estructuras de datos

Los objetos matemáticos que manipulamos tanto en la entrada y salida como en los pasos intermedios del algoritmo son polinomios con coeficientes racionales. A lo largo de esta sección todos los polinomios univariados y formas lineales se suponen representados en forma densa, i.e, por un vector de coeficientes. Así por ejemplo la forma lineal $U \in \mathbb{Q}[X_1, \ldots, X_n]$, el polinomio minimal $q_u \in \mathbb{Q}[T]$ y los polinomios $v_1(T), \ldots, v_n(T) \in \mathbb{Q}[T]$ que definen la parametrización de la resolución geométrica de una $\mathbb{Q}$-variedad 0-dimensional se suponen dados en forma densa y nos referiremos a los coeficientes de dichos polinomios simplemente como los coeficientes de la resolución geométrica. Por otra parte, como principio general es necesario evitar la representación densa de los polinomios multivariados ya que esto podría implicar un crecimiento exponencial de la complejidad debido a la cantidad de monomios distintos de grado d en n variables. Por esta razón, todos los polinomios multivariados serán siempre representados mediante *straight-line programs*, cuya definición damos a continuación.

Sea R un anillo arbitrario. Denotamos con $R[X_1, \ldots, X_n]$ al anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en R. Sean $F_1, \ldots, F_s$ polinomios en $R[X_1, \ldots, X_n]$.

Definición 5.1 *Un* straight-line program (*libre de divisiones*) *en* $R[X_1, \ldots, X_n]$ *que calcula o evalúa el conjunto de polinomios* $\{F_1, \ldots, F_s\}$ *es una sucesión* $\beta = (Q_1, \ldots, Q_r)$ *de polinomios en* $R[X_1, \ldots, X_n]$ *con las siguientes propiedades:*

1. $\{F_1, \ldots, F_s\} \subseteq \{Q_1, \ldots, Q_r\}$.

2. *Para cada* $1 \leq \rho \leq r$, *el polinomio* Q_ρ *pertenece a* $R \cup \{X_1, \ldots, X_n\}$ *o existen* $1 \leq \rho_1, \rho_2 < \rho$ *y una operación aritmética* op_ρ *en* $\{+, -, \cdot\}$ *tales que vale* $Q_\rho = Q_{\rho_1} op_\rho Q_{\rho_2}$.

Los polinomios $Q_1, \ldots, Q_r$ se llaman los *resultados intermedios* del straight-line program β y los polinomios $F_1, \ldots, F_s$ son los resultados finales o *salidas* de β. Entre los resultados intermedios, las variables $X_1, \ldots, X_n$ se clasifican como las *entradas* y los elementos de R como los *parámetros* de β. Llamamos *longitud* de β al número de "pasos de computación" $Q_\rho = Q_{\rho_1} op_\rho Q_{\rho_2}$ del ítem 2 de la Definición 5.1. También definimos la *longitud no escalar* de β como el número de pasos de computación correspondientes a multiplicaciones "esenciales", es decir, pasos de computación $Q_\rho = Q_{\rho_1} op_\rho Q_{\rho_2}$ tales que $Q_{\rho_i} \notin R$ para $i = 1, 2$, y op_ρ es la operación de multiplicación.

Alternativamente utilizamos también la representación mixta de un polinomio multivariado dado con respecto a una variable distinguida. Sea F un polinomio en $R[X_1, \ldots, X_n]$ de grado total a lo sumo d. Sea $1 \leq k \leq n$ y sea X_k una variable distinguida. Interpretamos a F como un polinomio multivariado en la variable X_k con coeficientes en $R[X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n]$. Entonces F tiene la forma $F = \sum_{0 \leq j \leq d} F_j X_k^j$ donde los coeficientes F_j son polinomios en las variables $X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n$ con coeficientes en R. Una *representación mixta* del polinomio F con respecto a la variable X_k es un straight-line program libre de divisiones con entradas $X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n$, parámetros en R y con $d + 1$ salidas que representan los polinomios $F_0, \ldots, F_d$.

5.2. Algunos resultados básicos de complejidad

5.2.1. Operaciones aritméticas con polinomios univariados

En esta subsección vamos a presentar algunos resultados estándar sobre la complejidad de las operaciones aritméticas con polinomios univariados. (Para más detalles ver [4], [2], [38].) Más precisamente si R es un anillo conmutativo con unidad y $R[T]$ es el anillo de polinomios sobre R en la indeterminada T, vamos a discutir el costo de realizar las operaciones aritméticas de adición, substracción, multiplicación y división con resto en $R[T]$ medido en términos del número de operaciones en el anillo de base R (adición, substracción, multiplicación y división por unidades de R), suponiendo que tanto los polinomios de entrada como los de salida de la operación aritmética en consideración se representan en forma densa.

Antes de pasar a los enunciados vamos a precisar el tipo de algoritmo que consideramos para el cálculo de tales operaciones. Primeramente observamos que si los polinomios están codificados en forma densa, entonces cualquiera de las operaciones mencionadas (con un divisor mónico en el caso de la división) son funciones polinomiales de los datos de entrada. Mas generalmente sea $\alpha : R^m \to R^r$ una función polinomial arbitraria. Diremos que α *se puede calcular usando a lo sumo* L *operaciones en* R si

se da la siguiente situación: Sean $X_1, \ldots, X_m$ nuevas indeterminadas (que conmutan) sobre R y sea R^* el conjunto de unidades de R. Existe un straight-line program *libre de divisiones* β en $R[X_1, \ldots, X_m]$ con entradas $X = \{X_1, \ldots, X_m\}$ y de longitud L, que satisface la siguiente propiedad:

Notemos con $S \subset R^*$ el conjunto de parámetros, con $V = \{P_1, \ldots, P_L\}$ el conjunto de resultados intermedios y con $\{F_1, \ldots, F_r\} \subset V$ las salidas de β. Entonces para toda interpretación $J : S \cup X \to R$ de β (donde se supone que $J(s) = s$ para $s \in S$), su extensión consistente $J : S \cup X \cup V \to R$ verifica $(J(F_1), \ldots, J(F_r)) = \alpha(J(X_1), \ldots, J(X_m))$.

Con esta terminología en mente, procedemos a los enunciados. Dados dos polinomios en $R[T]$ de grados menores que δ, es claro que su suma o su resta se pueden obtener con a lo sumo δ adiciones o substracciones en R. Para la multiplicación se tiene el siguiente resultado, que surge como consecuencia del algoritmo de multiplicación rápida de Schönhage-Strassen ([2], [4], [38]).

Teorema 5.2 *La multiplicación de dos polinomios de grados menores que δ en el anillo $R[T]$ se puede efectuar usando $\mathcal{O}(\delta \log(\delta) \log(\log(\delta)))$ operaciones en R.*

Es usual que en cuestiones de complejidad en álgebra computacional se suela considerar la complejidad de la multiplicación de polinomios univariados como un invariante. En tal sentido, vamos a utilizar frecuentemente la notación $M(\delta) := \delta \log(\delta) \log(\log(\delta))$.

El siguiente resultado, la complejidad del cálculo de la división con resto por un polinomio *mónico* de $R[T]$, es consecuencia del conocido algoritmo de Sieveking-Kung ([2], [38]).

Teorema 5.3 *Sean polinomios P, Q en $R[T]$ arbitrarios tales que Q es mónico con $gr(Q) = \delta$, $gr(P) < \delta + k$ y $\delta \geq k$. Entonces el cociente y el resto de la división de P por Q se pueden calcular usando $4M(\delta) + M(k) + \mathcal{O}(\delta) = \mathcal{O}(M(\delta))$ operaciones aritméticas en R.*

Sea Q en $R[T]$ mónico de grado δ. Los resultados anteriores permiten estimar el costo de la multiplicación en el anillo cociente $R[T]/(Q)$, asumiendo que una clase residual $\bar{P}$ se representa por la forma densa de su representante P de grado menor que δ. Tenemos entonces el siguiente corolario:

Corolario 5.4 *Una multiplicación en el anillo cociente $R[T]/(Q)$ se puede calcular usando $\mathcal{O}(M(\delta))$ operaciones aritméticas en R.*

Máximo común divisor

Por último consideramos el costo del cálculo del máximo común divisor de dos polinomios univariados. Sea $K[T]$ el anillo de polinomios en la indeterminada T con coeficientes en un cuerpo arbitrario K. Como consecuencia del Algoritmo Extendido de Euclides (véase [2], [38]), tenemos el siguiente resultado:

Lema 5.5 *Sean F, G polinomios en $K[T]$ de grados a lo sumo δ. Entonces los siguientes ítems se pueden calcular con $\mathcal{O}(M(\delta)log(\delta))$ operaciones en K:*

- *El máximo común divisor H en $K[T]$ de F y G.*
- *Polinomios R, S en $K[T]$ de grados a lo sumo $\delta - 1$ con $RF + SG = H$.*

5.2.2. Cálculo del determinante

Consideramos ahora el costo del cálculo del determinante de una matriz con coeficientes en R de tamaño $n \times n$ en términos de operaciones aritméticas en R. A partir del algoritmo de Samuelson para el cálculo del polinomio característico, tenemos el siguiente resultado:

Teorema 5.6 [13] *El cálculo del determinante de una matriz arbitraria A en $R^{n\times n}$ se puede realizar usando $\mathcal{O}(n^4)$ operaciones en R.*

5.2.3. La complejidad del cálculo de la resolución geométrica de una $\mathbb{Q}$-variedad 0-dimensional

En el siguiente resultado expresamos la complejidad del cálculo de un elemento primitivo y de la resolución geométrica asociada, medida en términos del número de operaciones en el cuerpo de base $\mathbb{Q}$. (Ver [21], [23], [5].)

Teorema 5.7 *Sean $F_1, \ldots, F_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ de grados a lo sumo d que definen una sucesión regular reducida, codificados por un straight-line program de longitud L. Sea $V \subseteq \mathbb{C}^n$ la variedad algebraica 0-dimensional definida por estos polinomios y $\delta := \#(V)$. Entonces existe un algoritmo probabilístico que calcula la resolución geométrica de V con $\mathcal{O}(n(nL + n^4)(M(d\delta))^2)$ operaciones aritméticas en $\mathbb{Q}$.*

5.3. Cálculo de la base del espacio de interpolantes

Sean nuevamente $F_1, \ldots, F_n$ polinomios de $\mathbb{Q}[X_1, \ldots, X_n]$ que forman una sucesión regular reducida y definen la variedad 0-dimensional $V \subseteq \mathbb{C}^n$. De ahora en adelante vamos a suponer que tal sucesión viene dada por un straight-line program libre de divisiones β con entradas $X_1, \ldots, X_n$ y con n salidas que representan los polinomios $F_1, \ldots, F_n$. En la Sección 4 se demostró la existencia de polinomios $G_0, \ldots, G_{\delta-1}$ en $\mathbb{Q}[X_1, \ldots, X_n]$ de grados a lo sumo $n(d-1)$ que generan un espacio de interpolantes para el conjunto de nodos V. En esta sección vamos a describir un procedimiento algorítmico para calcular estos polinomios. Como siempre, es necesario evitar el cálculo de la representación densa de los polinomios $G_0, \ldots, G_{\delta-1}$ para evitar un crecimiento

exponencial de la complejidad de los correspondientes algoritmos. Por eso los polinomios $G_0, \ldots, G_{\delta-1}$ se van a representar mediante un straight-line program.

Comenzamos con las siguientes consideraciones de carácter general. Sean n, s y N números naturales y $X_1, \ldots, X_n, Y_1, \ldots, Y_s$ un conjunto de $n+s$ indeterminadas sobre $\mathbb{Q}$. Sea F un polinomio en $\mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_s]$ de grado total en las variables $X_1, \ldots, X_n, Y_1, \ldots, Y_s$ a lo sumo N. Supóngase además que F está representado por un straight-line program libre de divisiones β con entradas $X_1, \ldots, X_n, Y_1, \ldots, Y_s$. Introduzcamos ahora otra indeterminada T sobre $\mathbb{Q}$ y supóngase que son dados polinomios $v_1, \ldots, v_s$ de grados a lo sumo $\delta - 1$ y un polinomio q mónico y de grado δ en $\mathbb{Q}[T]$ (estos polinomios no necesariamente representan la parametrización y el polinomio minimal de una resolución geométrica de V). A continuación consideramos el anillo cociente $\mathbb{Q}[X_1, \ldots, X_n, T]/(q)$, que es un $\mathbb{Q}[X_1, \ldots, X_n]$-módulo libre con base $\mathcal{B} = \{1, \bar{T}, \ldots, \bar{T}^{\delta-1}\}$. Definimos a G como el polinomio en $\mathbb{Q}[X_1, \ldots, X_n, T]$ que se obtiene de F al substituir la variable Y_j por el polinomio v_j para todo $1 \leq j \leq s$, es decir:

$$G(X_1, \ldots, X_n, T) := F(X_1, \ldots, X_n, v_1(T), \ldots, v_s(T)). \tag{5.1}$$

Notemos con $\overline{G}$ a la imagen de G en el cociente $\mathbb{Q}[X_1, \ldots, X_n, T]/(q)$. Sean G_j $(0 \leq j \leq \delta - 1)$ los (únicos) polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ que representan los coordenadas de $\bar{G}$ en la base $\mathcal{B}$. Estos polinomios G_j $(0 \leq j \leq \delta - 1)$ se pueden obtener del siguiente modo: Interpretamos a G como un polinomio univariado en la variable T con coeficientes en $\mathbb{Q}[X_1, \ldots, X_n]$. Puesto que q es mónico podemos realizar la división con resto de G por q en $\mathbb{Q}[X_1, \ldots, X_n][T]$. Luego el resto R de esta división es de la forma

$$R = \sum_{0 \leq j \leq \delta - 1} G_j(X) T^j, \tag{5.2}$$

donde los polinomios G_j $(0 \leq j \leq \delta - 1)$ en $\mathbb{Q}[X_1, \ldots, X_n]$ son precisamente las coordenadas de $\bar{G}$ en la base $\mathcal{B}$. Obsérvese que como G tiene grado a lo sumo N en las variables $X_1, \ldots, X_n$ y q no depende de las variables X_k, los polinomios G_j también tienen sus grados menores o iguales a N. En el siguiente teorema se plantea el problema de hallar un straight-line program que evalúe los polinomios $G_0, \ldots, G_{\delta-1}$, es decir, una representación mixta del polinomio R con respecto a la variable T.

Teorema 5.8 *Sea F un polinomio en $\mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_s]$ de grado acotado por N en las variables $X_1, \ldots, X_n, Y_1, \ldots, Y_s$. Supóngase entonces que son dados los siguientes ítems como entrada:*

- *Un straight-line program β libre de divisiones, de longitud L con entradas $X_1, \ldots, X_n, Y_1, \ldots, Y_s$ que evalúa el polinomio F.*
- *Un polinomio q mónico de grado δ y s polinomios $v_1, \ldots, v_s$ de grados a lo sumo $\delta - 1$ en $\mathbb{Q}[T]$.*

Entonces existe un straight-line program libre de divisiones β' de longitud $\mathcal{O}(LM(\delta))$ que representa los polinomios G_j $(0 \leq j \leq \delta - 1)$ arriba definidos.

Demostración: Recordemos (Definición 5.1) que el straight-line program β es una sucesión $\beta = (Q_1, \ldots, Q_r)$ de polinomios en $\mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_s]$ que verifica:

1. $Q_r = F$.
2. Para cada ρ con $1 \leq \rho \leq r$, el polinomio Q_ρ pertenece a $\mathbb{Q} \cup \{X_1, \ldots, X_n, Y_1, \ldots, Y_s\}$ o existen índices ρ_1, ρ_2 con $1 \leq \rho_1, \rho_2 < \rho$ y una operación aritmética $op_\rho \in \{+, -, \cdot\}$ tales que:

$$Q_\rho = Q_{\rho_1} op_\rho Q_{\rho_2}. \tag{5.3}$$

Para cada índice ρ con $1 \leq \rho \leq r$ sea P_ρ el polinomio en $\mathbb{Q}[X_1, \ldots, X_n, T]$ definido como

$$P_\rho := Q_\rho(X_1, \ldots, X_n, v_1(T), \ldots, v_s(T)),$$

y sea R_ρ el resto de la división de P_ρ por q. En particular, según (5.1) y (5.2) es $P_r = G$ y $R_r = R$. A continuación calculamos en forma sucesiva los coeficientes de todos los polinomios R_ρ $(1 \leq \rho \leq r)$, considerados como polinomios en la variable T con coeficientes en $\mathbb{Q}[X_1, \ldots, X_n]$. Procedemos por inducción en el subíndice ρ.

Si $\rho = 1$ se presentan tres posibilidades:

1. Q_ρ es un parámetro de β en $\mathbb{Q}$ y en tal caso $R_\rho = Q_\rho$.
2. Q_ρ es alguna entrada X_i de β, con lo cual $R_\rho = P_\rho = X_i$.
3. Q_ρ es alguna entrada Y_i de β, con lo cual $R_\rho = P_\rho = v_i(T)$.

En cualquier caso, R_ρ es dato.

Supongamos ahora que $1 < \rho$ y que ya han sido calculados los coeficientes de los polinomios R_μ para todos los índices $1 \leq \mu < \rho$. De la identidad (5.3) deducimos la siguiente congruencia en el anillo $\mathbb{Q}[X_1, \ldots, X_n][T]$:

$$R_\rho \equiv R_{\rho_1} op_\rho R_{\rho_2} \mod(q).$$

Por hipótesis inductiva conocemos los coeficientes de R_{ρ_1} y R_{ρ_2}. Como estos polinomios tienen grado menor que δ en la variable T sabemos por el Corolario 5.4 que los coeficientes de R_ρ se pueden calcular a partir de los coeficientes de R_{ρ_1}, R_{ρ_2} y de q usando $\mathcal{O}(M(\delta))$ operaciones aritméticas en $\mathbb{Q}[X_1, \ldots, X_n]$ (aplicamos el corolario cuando el anillo de coeficientes es $R := \mathbb{Q}[X_1, \ldots, X_n]$). Continuando de este modo vemos que es posible calcular los coeficientes de todos los polinomios R_ρ $(1 \leq \rho \leq r)$ y en particular los polinomios G_j $(0 \leq j \leq \delta - 1)$. Por otro lado, puesto que en β

tenemos L operaciones aritméticas se deduce que los cálculos anteriores requieren a lo sumo $\mathcal{O}(LM(\delta))$ operaciones aritméticas en $\mathbb{Q}[X_1, \ldots, X_n]$. En otras palabras, hemos descripto un straight-line program libre de divisiones β' con entradas $X_1, \ldots, X_n$ de longitud $\mathcal{O}(LM(\delta))$, que es una representación mixta del polinomio R con respecto a la variable T. Con esto queda demostrado el teorema. ∎

Sea nuevamente B la $\mathbb{Q}$-álgebra $B = \mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_n)$. Sea U cualquier forma lineal en $\mathbb{Q}[X_1, \ldots, X_n]$ cuya imagen u en B es un elemento primitivo de V. Como sabemos, $\mathcal{B} = \{1, u, \ldots, u^{\delta-1}\}$ es una base de B. Sea dado un polinomio F en $\mathbb{Q}[X_1, \ldots, X_n]$ y notemos con f a su imagen en B. Consideramos ahora el problema de hallar los coeficientes de f en la base $\mathcal{B}$ o equivalentemente el polinomio P en $\mathbb{Q}[T]$ de grado a lo sumo $\delta - 1$ que verifica $P(u) = f$. La solución de este problema es un caso especial del Teorema 5.8 que enunciamos separadamente:

Corolario 5.9 *Sea F un polinomio arbitrario en $\mathbb{Q}[X_1, \ldots, X_n]$ y f su imagen en B. Supóngase que son dados los siguientes ítems:*

- *Un straight-line program libre de divisiones β de longitud L con entradas $X_1, \ldots, X_n$ que evalúa el polinomio F.*
- *El polinomio minimal q_u y la parametrización dada por los polinomios $v_1, \ldots, v_n$ de la resolución geométrica de V asociada al elemento primitivo u.*

Entonces el polinomio P en $\mathbb{Q}[T]$ de grado a lo sumo $\delta - 1$ tal que $P(u) = f$ se puede calcular con $\mathcal{O}(LM(\delta))$ operaciones en $\mathbb{Q}$.

Una segunda aplicación del Teorema 5.8 es la siguiente: Sea F un polinomio en $\mathbb{Q}[X_1, \ldots, X_n]$ de grado total acotado por d representado mediante un straigh-line program libre de divisiones β con entradas $X_1, \ldots, X_n$ de longitud L. Sea $1 \leq k \leq n$ fijo. Ahora el problema es hallar una representación mixta de F con respecto a la variable distinguida X_k.

Corolario 5.10 *Bajo las hipótesis anteriores existe una representación mixta del polinomio F con respecto a una variable cualquiera de longitud $\mathcal{O}(LM(d))$.*

Demostración: Supongamos en efecto que X_n es la variable distiguida de F y tomemos el monomio $q(X_n) := X_n^{d+1}$. Según el Teorema 5.8 existe un straight-line program β' de longitud $\mathcal{O}(LM(d))$ que evalúa $d+1$ polinomios $F_0, \ldots, F_d$ en $\mathbb{Q}[X_1, \ldots, X_{n-1}]$ tales que se verifica la siguiente congruencia en el anillo $\mathbb{Q}[X_1, \ldots, X_n]$:

$$F(X_1, \ldots, X_n) \equiv \sum_{k=0}^{d} F_k(X_1, \ldots, X_{n-1}) X_n^k \mod(X_n^{d+1}).$$

Como $gr_{X_n}(F) \leq d$, se deduce la igualdad

$$F = \sum_{k=0}^{d} F_k(X_1, \ldots, X_{n-1}) X_n^k,$$

de modo que β' es la representación mixta de F anunciada en el corolario. ∎

Sean nuevamente $F_1, \ldots, F_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ cuyos grados están acotados por d y supóngase que vienen representados mediante un straight-line program libre de divisiones β con entradas $X_1, \ldots, X_n$ de longitud L. Tomemos el Bezoutiano $D(X, Y)$ en $\mathbb{Q}[X, Y]$ asociado a la sucesión $F_1, \ldots, F_n$ conforme fue construído en la Sección 3.2.1.

En el siguiente lema se afirma que es posible transformar el straight-line program β en un straight-line program que evalúa el Bezoutiano D.

Lema 5.11 *Sean $F_1, \ldots, F_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ de grados acotados por d dados mediante un straight-line program libre de divisiones β' con entradas $X_1, \ldots, X_n$ de longitud L. Entonces existe un straight-line program libre de divisiones de longitud $\mathcal{O}(Ln^2M(d) + n^2(d^2 + n^2))$ con entradas $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ que evalúa un Bezoutiano $D(X, Y)$ para la sucesión $F_1, \ldots, F_n$ tal que el grado total de D en las variables $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ es a lo sumo $n(d-1)$.*

Demostración: Sean $F_j^{(k)}$ $(1 \leq j \leq n, 0 \leq k \leq n)$, B_k^m $(1 \leq m \leq d, 1 \leq k \leq n)$, $A_{j,m}^{(k)}$ $(0 \leq k \leq n-1, 1 \leq j \leq n, 0 \leq m \leq d)$ y $\gamma_{j,k}$ $(1 \leq j, k \leq n)$ los polinomios definidos en la demostración del Lema 3.4 de la Sección 3.2.1.

Primeramente vamos calcular los polinomios $\gamma_{j,k}$. Procedemos como sigue: Para cada j, k con $1 \leq j \leq n$ y $0 \leq k \leq n-1$, substituímos en el straight-line program β las variables $(X_1, \ldots, X_k)$ por $(Y_1, \ldots, Y_k)$, obteniendo un straight-line program $\beta_j^{(k)}$ que evalúa el polinomio $F_j^{(k)}$ con longitud L. Por lo tanto cada polinomio $F_j^{(k)}$ se evalúa con L operaciones aritméticas en $\mathbb{Q}[X, Y]$ y tiene grado menor o igual a d. Por el Corolario 5.10 existe una representación mixta de $F_j^{(k)}$ con respecto a la variable X_{k+1}, cuyas salidas representan los polinomios $A_{j,0}^{(k)}, \ldots, A_{j,d}^{(k)}$, con longitud $\mathcal{O}(LM(d))$. En conclusión, como se tienen n^2 pares (j, k) con $1 \leq j \leq n$, $0 \leq k \leq n-1$, el conjunto de polinomios $A_{j,m}^{(k)}$ $(0 \leq k \leq n-1, 1 \leq j \leq n, 1 \leq m \leq d)$, se puede evaluar con $\mathcal{O}(Ln^2M(d))$ operaciones aritméticas en $\mathbb{Q}[X, Y]$. Por otra parte es claro que los polinomios B_k^m $(1 \leq m \leq d, 1 \leq k \leq n)$, se evalúan con $\mathcal{O}(nd^2)$ operaciones. A continuación, para obtener los polinomios $\gamma_{j,k} := \sum_{m=1}^{d} A_{j,m}^{(k-1)} B_k^m$ $(1 \leq j, k \leq n)$, se requieren $\mathcal{O}(n^2 d)$ operaciones adicionales. Por lo tanto el conjunto de polinomios $\gamma_{j,k}$ $(1 \leq j, k \leq n)$ se puede evaluar por un straight-line program de longitud $\mathcal{O}(Ln^2M(d)+n^2d^2)$. Finalmente recordemos que el Bezoutiano $D(X, Y)$ está definido como el determinante $D := \det(\gamma_{j,k})$. Luego aplicando el Lema

5.6 sobre el cálculo del determinante, concluímos que existe un straight-line program β' de longitud $\mathcal{O}(Ln^2M(d) + n^2(d^2 + n^2))$ que evalúa el Bezoutiano D. ∎

Ahora estamos en condiciones de calcular los polinomios $G_0, \ldots, G_{\delta-1}$ que forman una base de un espacio de interpolación tal como se describen en el Teorema 4.1.

Teorema 5.12 *Sean $F_1, \ldots, F_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ de grados a lo sumo d que definen una sucesión regular reducida y que generan el ideal radical $(F_1, \ldots, F_n)$. Sea $V := V(F_1, \ldots, F_n)$ la $\mathbb{Q}$-variedad 0-dimensional de cardinalidad δ definida por estos polinomios y B su anillo de coordenadas. Supóngase que como entrada son dados los siguientes ítems*

- *Un straight-line program libre de divisiones β con entradas $X_1, \ldots, X_n$ de longitud L que evalúa los polinomios $F_1, \ldots, F_n$.*
- *El polinomio minimal q_u y la parametrización dada por los polinomios $v_1, \ldots, v_n$ de la resolución geométrica de V asociada a un elemento primitivo u.*

Entonces existe un straight-line program libre de divisiones β' con entradas $X_1, \ldots, X_n$ de longitud $\mathcal{O}(n(nL+n^4)M(d^2\delta))$ y con δ salidas que representan polinomios $G_0, \ldots, G_{\delta-1}$ en $\mathbb{Q}[X_1, \ldots, X_n]$ de grados a lo sumo $n(d-1)$ que verifican la siguiente propiedad: Denotemos con $g_0, \ldots, g_{\delta-1}$ las imágenes en B de los polinomios $G_0, \ldots, G_{\delta-1}$. Entonces para todo elemento f en B vale la fórmula de la traza*:*

$$f = \sum_{k=0}^{\delta-1} Tr(\bar{J}^{-1} f u^k) g_k. \tag{5.4}$$

En particular $\{g_0, \ldots, g_{\delta-1}\}$ es una base de B y los polinomios $G_0, \ldots, G_{\delta-1}$ generan un espacio de interpolación para el conjunto de nodos V.

Demostración: Por hipótesis tenemos un straight-line program libre de divisiones β de longitud a lo sumo L que evalúa el conjunto de polinomios $F_1, \ldots, F_n$. Por el Lema 5.11 se puede transformar a β en un straight-line program libre de divisiones β_1 de longitud a lo sumo $\mathcal{O}(Ln^2M(d) + n^2(d^2 + n^2))$ con entradas $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ que evalúa un Bezoutiano D de la sucesión $F_1, \ldots, F_n$ de grado acotado por $n(d-1)$. Sea D_1 el polinomio en $\mathbb{Q}[X_1, \ldots, X_n, T]$ que se obtiene al substituir en D las variables $Y_1, \ldots, Y_n$ por los polinomios univariados $v_1(T), \ldots, v_n(T)$ respectivamente, es decir

$$D_1 := D(X_1, \ldots, X_n, v_1(T), \ldots, v_n(T)).$$

Como sabemos el anillo cociente $\mathbb{Q}[X_1, \ldots, X_n, T]/(q_u)$ es un $\mathbb{Q}[X_1, \ldots, X_n]$-módulo libre con base $\mathcal{B} = \{1, \bar{T}, \ldots, \bar{T}^{\delta-1}\}$. Denotemos con $\bar{D}_1$ a la imagen de D_1 en

el cociente $\mathbb{Q}[X,T]/(q_u)$. Sean $G_0,\ldots,G_{\delta-1}$ los polinomios en $\mathbb{Q}[X_1,\ldots,X_n]$ que representan las coordenadas de $\bar{D}_1$ en la base $\mathcal{B}$. Según la demostración del Teorema 4.1, los polinomios $G_0,\ldots,G_{\delta-1}$ verifican todas las propiedades del enunciado del presente teorema. Ahora bien, de acuerdo con el Teorema 5.9 es posible obtener a partir de β_1 y de la resolución geométrica de V un straight-line program β' de longitud $\mathcal{O}((Ln^2M(d)+n^2(d^2+n^2))M(\delta)) = \mathcal{O}(n(nL+n^4)M(d^2\delta))$ que evalúa los polinomios G_j $(1\leq j\leq \delta-1)$, lo que concluye la demostración. ∎

5.4. Cálculo de los coeficientes

En la sección anterior hemos calculado polinomios $G_0,\ldots,G_{\delta-1}$ que forman una base para un espacio de interpolación. Además esta base posee la propiedad que dado un polinomio arbitrario F en $\mathbb{Q}[X_1,\ldots,X_n]$ su interpolante en dicho espacio se escribe en la forma $\sum_{0\leq j\leq\delta-1} Tr(\bar{J}^{-1}fu^j)G_j$. En esta sección nos ocupamos del cálculo de los coeficientes $Tr(\bar{J}^{-1}fu^j)$ $(0\leq j\leq\delta-1)$, suponiendo que los polinomios $F_1,\ldots,F_n$ y F vienen dados por un straight-line program de longitud L.

5.4.1. Cálculo del jacobiano

En primer término consideramos el problema de calcular las derivadas parciales primeras $\partial F/\partial X_1,\ldots,\partial F/\partial X_n$ de un polinomio F en $\mathbb{Q}[X_1,\ldots,X_n]$ arbitrario. Tenemos el siguiente lema:

Lema 5.13 *Sea F un polinomio en $\mathbb{Q}[X_1,\ldots,X_n]$ dado mediante un straight-line program β de longitud L. Entonces, existe un straight-line program β' que evalúa el conjunto de polinomios $\{\partial F/\partial X_1,\ldots,\partial F/\partial X_n\}$ con longitud $\mathcal{O}(nL)$.*

Demostración: La idea es calcular "paso a paso" cada derivada primera de F siguiendo el esquema de computación β que calcula F. Procedemos de la siguiente manera: Por cada paso de computación ρ de β se calculan las n derivadas primeras de la función calculada en ρ. A fin de calcular esas derivadas basta tener en cuenta que en pasos de computación anteriores se tienen calculadas las derivadas primeras de los resultados intermedios predecesores de ρ, por lo que el esquema de cálculo de las derivadas de la función calulada en ρ es una consecuencia directa de las reglas de derivación para funciones de tipo $P\,op\,Q$ con $op\in\{+,-,\cdot\}$. ∎

Combinando el Lema 5.13 con el Teorema 5.6 sobre el cálculo del determinante, se obtiene el corolario:

Corolario 5.14 *Sean $F_1,\ldots,F_n$ polinomios en $\mathbb{Q}[X_1,\ldots,X_n]$ dados mediante un straight-line program β de longitud L. Entonces existe un straight-line program β' que evalúa el Jacobiano $J(F_1,\ldots,F_n)$ con longitud $\mathcal{O}(nL+n^4)$.*

5.4.2. Inversión del jacobiano

Sea $\bar{J}$ la imagen en B del polinomio jacobiano $J(F_1, \ldots, F_n)$. Consideramos ahora el problema de calcular su inverso $\bar{J}^{-1}$ en B. Sea u el elemento primitivo previamente fijado en B. Para nuestro propósito es suficiente hallar el polinomio H en $\mathbb{Q}[T]$ de grado a lo sumo $\delta - 1$ que verifica $H(u) = \bar{J}^{-1}$. Tenemos el siguiente resultado:

Teorema 5.15 *Sean $F_1, \ldots, F_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ que definen una sucesión regular reducida y que generan un ideal radical $(F_1, \ldots, F_n)$. Sea $V = V(F_1, \ldots, F_n)$ la $\mathbb{Q}$-variedad 0-dimensional de cardinalidad δ definida por estos polinomios y B su anillo de coordenadas. Supóngase que los siguientes ítems son dados como entrada:*

- *Un straight-line program β de longitud L que evalúa los polinomios $F_1, \ldots, F_n$.*
- *Una resolución geométrica de V.*

Entonces el polinomio H en $\mathbb{Q}[T]$ de grado a lo sumo $\delta - 1$ que verifica la identidad $H(u) = \bar{J}^{-1}$ en B se puede calcular con $\mathcal{O}((nL + n^4)M(\delta)\log(\delta))$ operaciones en $\mathbb{Q}$.

Demostración: Por el Corolario 5.14 existe un straight-line program β' que evalúa el jacobiano J con longitud $\mathcal{O}(nL+n^4)$. Luego, por el Corolario 5.9 el polinomio G en $\mathbb{Q}[T]$ de grado a lo sumo $\delta - 1$ tal que $G(u) = \bar{J}$ se puede calcular usando $\mathcal{O}((nL+n^4)M(\delta))$ operaciones en $\mathbb{Q}$. Sea ahora H el polinomio en $\mathbb{Q}[T]$ de grado $gr(H) \leq \delta - 1$ tal que $HG \equiv 1 \bmod(q_u)$. Es claro que H verifica la identidad $H(u) = \bar{J}^{-1}$. Aplicando el Lema 5.5 (cálculo del máximo común divisor) el polinomio H se puede calcular a partir de q_u y G con $\mathcal{O}(M(\delta)\log(\delta))$ operaciones en $\mathbb{Q}$. En conclusión es necesario realizar $\mathcal{O}((nL + n^4)M(\delta)\log(\delta))$ operaciones en $\mathbb{Q}$. ∎

5.4.3. Cálculo de las trazas

Dado un elemento primitivo u en B consideramos nuevamente la $\mathbb{Q}$-álgebra $A_u = \mathbb{Q}[T]/(q_u)$ de clases residuales en $\mathbb{Q}[T]$ módulo el polinomio minimal q_u de u. En el siguiente lema se establece el costo de evaluar la traza estándar tr de A_u.

Lema 5.16 *Sea p una clase residual dada en A_u. Supóngase que son dados los siguientes ítems:*

- *El representante P en $\mathbb{Q}[T]$ de grado a lo sumo $\delta - 1$ de la clase residual p.*
- *El polinomio minimal q_u.*

Entonces la traza estándar $tr(p)$ de p se puede calcular con $\mathcal{O}(M(\delta))$ operaciones aritméticas en $\mathbb{Q}$.

Demostración: Sea q'_u la derivada de q_u. Por el Lema 3.7 sabemos que si $R = b_{\delta-1}T^{\delta-1}+\cdots+b_0$ es el resto de la división del producto $q'_u P$ por q_u entonces $tr(p) = b_{\delta-1}$. A fin de demostrar el enunciado basta observar que por el Corolario 5.4 podemos calcular R a partir de P y q'_u con $\mathcal{O}(M(\delta))$ operaciones aritméticas en $\mathbb{Q}$. ∎

En consecuencia, podemos determinar el costo de calcular las trazas que necesitamos a fin de calcular un polinomio interpolante.

Teorema 5.17 *Sean $F_1, \ldots, F_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ de grados acotados por d que definen una sucesión regular reducida y que generan un ideal radical $(F_1, \ldots, F_n)$. Sea $V = V(F_1, \ldots, F_n)$ la $\mathbb{Q}$-variedad 0-dimensional de cardinalidad δ definida por estos polinomios y B su anillo de coordenadas. Sea además F un polinomio en $\mathbb{Q}[X_1, \ldots, X_n]$ de grado arbitrario, y denótese con f su imagen en B . Supóngase que los siguientes ítems son dados como entrada:*

- *Un straight-line program libre de divisiones β de longitud L que evalúa los polinomios $F_1, \ldots, F_n$ y F.*
- *Una resolución geométrica de V.*

Entonces todas las trazas $Tr(\bar{J}^{-1} f u^j)$ $(0 \leq j \leq \delta - 1)$ se pueden calcular a partir de los coeficientes de la resolución geométrica y de los parámetros de β usando $\mathcal{O}((nL + n^4)M(\delta)^2)$ operaciones en $\mathbb{Q}$.

Demostración: Sea u el elemento primitivo de la resolución geométrica dada. Sean P y H los polinomios en $\mathbb{Q}[T]$ de grados a lo sumo $\delta - 1$ tales que valen las igualdades $P(u) = f$ y $H(u) = \bar{J}^{-1}$ en B. Por el Teorema 5.15 y el Corolario 5.9 los polinomios P y H se pueden calcular a partir de los coeficientes de la resolución geométrica y de los parámetros de β con $\mathcal{O}((nL + n^4)M(\delta)\log(\delta))$ operaciones en $\mathbb{Q}$. A continuación hallamos para todo $0 \leq j \leq \delta - 1$ el polinomio K_j en $\mathbb{Q}[T]$ de grado a lo sumo $\delta - 1$ representante de la clase residual $\bar{K}_j = \bar{H}\bar{P}\bar{T}^j$ del cociente $A_u = \mathbb{Q}[T]/(q_u)$. Este cálculo requiere $\mathcal{O}(\delta)$ multiplicaciones en A_u y por lo tanto, según el Corolario 5.4, el cálculo de la representación densa de las clases $\bar{K}_0, \ldots, \bar{K}_{\delta-1}$ requiere $\mathcal{O}(\delta M(\delta))$ operaciones aritméticas en $\mathbb{Q}$. En virtud del isomorfismo de $\mathbb{Q}$-álgebras $\theta : B \to A_u$ dado por $\theta(u) = \bar{T}$ tenemos que $Tr = tr \circ \theta$. Por lo tanto $Tr(\bar{J}^{-1} f u^j) = tr(\bar{K}_j)$ para todo $0 \leq j \leq \delta - 1$. Por el Lema 5.16 una traza estándar $tr(\bar{K}_j)$ se puede calcular a partir de los polinomios q_u y K_j con $\mathcal{O}(M(\delta))$ operaciones en $\mathbb{Q}$. En consecuencia el costo total es de $\mathcal{O}((nL + n^4)M(\delta)\log(\delta) + \delta M(\delta)) = \mathcal{O}((nL + n^4)M(\delta)^2)$. ∎

5.5. Estimación de complejidad del algoritmo completo

En conclusión podemos decir que la eficiencia del método de interpolación expuesto en las páginas precedentes reside en el cálculo del interpolante, es decir, de las trazas, junto con el costo del cálculo de los polinomios $G_0, \ldots, G_{\delta-1}$ de la base del espacio de interpolantes.

Finalmente resumimos los resultados anteriores en el siguiente teorema:

Teorema 5.18 *Sean $F_1, \ldots, F_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ de grados acotados por d que definen una sucesión regular reducida y que generan un ideal radical $(F_1, \ldots, F_n)$. Sea $V = V(F_1, \ldots, F_n)$ la $\mathbb{Q}$-variedad 0-dimensional de cardinalidad δ definida por estos polinomios y B su anillo de coordenadas. Sea además F un polinomio en $\mathbb{Q}[X_1, \ldots, X_n]$ de grado arbitrario, y denótese con f a su imagen en B. Supóngase que es dado como entrada un straight-line program libre de divisiones β de longitud L que evalúa los polinomios $F_1, \ldots, F_n$ y F. Entonces:*

- *Probabilísticamente puede construirse un straight-line program libre de divisiones β' de longitud $\mathcal{O}(n(nL + n^4)M(d\delta)^2)$ que evalúa δ polinomios $G_0, \ldots, G_{\delta-1}$ en $\mathbb{Q}[X_1, \ldots, X_n]$ cuyos grados están acotados por $n(d-1)$ y tales que sus imágenes $\mathcal{B} = \{g_0, \ldots, g_{\delta-1}\}$ forman una $\mathbb{Q}$-base de B.*
- *Las coordenadas $(\alpha_0, \ldots, \alpha_{\delta-1})$ en la base $\mathcal{B}$ del elemento f de B se pueden calcular a partir de los parámetros de β con $\mathcal{O}((nL + n^4)M(\delta))^2)$ operaciones aritméticas en $\mathbb{Q}$.*

En particular, el polinomio $P := \sum_{j=0}^{\delta-1} \alpha_j G_j$ es un interpolante de F en los puntos de la variedad V, tiene grado acotado por $n(d-1)$ y se evalúa mediante un straight-line program de longitud $\mathcal{O}(n(nL + n^4)M(d\delta)^2)$.

Demostración: Dado que el cálculo de la resolución geométrica de V requiere $\mathcal{O}(n(nL+n^4)M(d\delta)^2)$ operaciones aritméticas en $\mathbb{Q}$, y según el Teorema 5.12 los polinomios $G_0, \ldots, G_{\delta-1}$ se evalúan a partir de β y de la resolución geométrica de V con $\mathcal{O}(n(nL+n^4)M(d^2\delta))$ operaciones aritméticas en $\mathbb{Q}[X_1, \ldots, X_n]$, fácilmente se deduce la estimación de complejidad del enunciado. ∎

Parte II

Cotas inferiores

Capítulo 6

Un modelo para procesos de interpolación

6.1. Algoritmos para familias de problemas de interpolación

En lo que sigue vamos a ocuparnos de familias de problemas de interpolación. Una familia de problemas de interpolación está representada por una *estructura de datos*, que es un subconjunto construible $\mathcal{D}$ de un espacio ambiente afín $\mathbb{C}^N$ dado. Cada instancia admisible $d \in \mathcal{D}$, o *código de entrada*, determina o *codifica* un problema de interpolación, interpretando las coordenadas de d como la lista de nodos y valores que definen el problema. Así, por ejemplo, cada punto $(x^{(1)}, y_1, \ldots, x^{(\delta)}, y_\delta) \in \mathbb{C}^{(n+1)K}$, donde $x^{(i)} \in \mathbb{C}^n$, $y_i \in \mathbb{C}$ para todo $1 \leq i \leq \delta$ y $x^{(i)} \neq x^{(j)}$ para $i \neq j$, determina de forma natural un problema de interpolación de Lagrange con nodos $x^{(1)}, \ldots, x^{(\delta)}$ y valores $y_1, \ldots, y_\delta$. En forma análoga se puede representar una amplia variedad de familias de problemas de interpolación, como quedará claro en los ejemplos que se darán en la Sección 6.2. Recalcamos que para toda familia de problemas interpolación considerada aquí, existen $n, D \in \mathbb{N}$, tales que todas las instancias de la familia tienen una solución (no necesariamente única) en el espacio Π_D de los polinomios n–variados con coeficientes en $\mathbb{C}$ de grado a lo sumo D. En otras palabras, tenemos una aplicación $\Phi : \mathcal{D} \to \Pi_D$ tal que para cada $d \in \mathcal{D}$ el polinomio $\Phi(d)$ resuelve el problema de interpolación determinado por d. Más aun, vamos a restringirnos a los casos en que esta aplicación Φ es un morfismo racional regular sobre un subconjunto abierto Zariski de $\mathcal{D}$ y además es continua (en la topología fuerte) en todo su dominio $\mathcal{D}$.

En suma, una *familia de problemas de interpolación de grado D* consiste de:

- un subconjunto construible $\mathcal{D}$ de un espacio afín $\mathbb{C}^N$, donde cada $d \in \mathcal{D}$ codifica un problema de interpolación con una solución en el espacio Π_D.

- un morfismo racional $\Phi : \mathcal{D} \to \Pi_D$ que se extiende con continuidad (en la topología fuerte) a todo $\mathcal{D}$ y tal que $\Phi(d)$ resuelve el problema de interpolación definido por d para todo $d \in \mathcal{D}$.

Definimos ahora la noción de algoritmo que resuelve (genéricamente) una familia dada de problemas de interpolación.

Definición 6.1 *Un* algoritmo de interpolación *para la familia de problemas de interpolación $\mathcal{D}$, $\Phi : \mathcal{D} \to \Pi_D$ está dado por un conjunto construible $\mathcal{D}^* \subset \mathbb{C}^M$, llamado la* estructura de datos de salida*, junto con una aplicación (polinomial) $\omega^* : \mathcal{D}^* \to \Pi_D$, y una aplicación racional $\Psi : \mathcal{D} \dashrightarrow \mathcal{D}^*$, tal que $\Psi(d)$ resuelve el problema de interpolación codificado por cada $d \in \mathcal{D}$ donde Ψ está definida. En otras palabras $\Psi(d)$ representa el código del interpolante $\Phi(d) \in \Pi_D$. En suma, el siguiente diagrama conmuta:*

$$\begin{array}{ccc} \mathcal{D} & \overset{\Psi}{\dashrightarrow} & \mathcal{D}^* \\ & \searrow^{\Phi} & \downarrow{\scriptstyle \omega^*} \\ & & \Pi_D \end{array} \tag{6.1}$$

Denotamos con $\overline{\mathcal{D}}$ la clausura Zariski de $\mathcal{D}$ en su espacio ambiente $\mathbb{C}^N$. En adelante, vamos a suponer que $\overline{\mathcal{D}}$ es un conjunto algebraico irreducible.

Como Ψ se supone una aplicación racional, existe un conjunto denso y abierto Zariski $\mathcal{U} \subseteq \overline{\mathcal{D}}$, tal que Ψ es una función regular en $\mathcal{U}$, i.e, Ψ es una M–tupla de funciones racionales $\Psi_j \in \mathbb{C}(\overline{\mathcal{D}})$, $1 \leq j \leq M$, bien definidas en $\mathcal{U}$.

6.2. Tres ejemplos críticos

El propósito de esta sección es ilustrar las nociones de la sección anterior, las cuales se discuten en tres significativas familias de problemas de interpolación. Estas familias de problemas de interpolación constituyen nuestros ejemplos prototípicos, y serán retomados en las Secciones 7.3 y 8.

La primera familia que consideramos es la interpolación de Lagrange univariada clásica, que está parametrizada por una estructura de datos *suave*. Luego consideramos un caso de interpolación de Lagrange multivariada sobre una curva *singular*. Nuestro último ejemplo es el de una familia *no lineal* de problemas de interpolación, esto es, el conjunto de interpolantes no es un subespacio lineal, sino un conjunto construible del correspondiente espacio ambiente afín.

6.2.1. Interpolación de Lagrange univariada

Fíjese $N \in \mathbb{N}$ y $\gamma := (\gamma_1, \ldots, \gamma_N) \in \mathbb{C}^N$ con $\gamma_i \neq \gamma_j$ para $i \neq j$. El problema de interpolación de Lagrange univariado (genérico) en nodos fijos $\gamma_1, \ldots, \gamma_N$ consiste en hallar, para cada $d := (d_1, \ldots, d_N) \in \mathbb{C}^N$, el único polinomio $p_d \in \Pi_{N-1}$ que satisface $p_d(\gamma_j) = d_j$ para $1 \leq j \leq d$.

Con el fin de representar estos problemas de interpolación en nuestros términos sea $D := N - 1$, $\mathcal{D} := \mathbb{C}^N$ y la aplicación $\Phi : \mathcal{D} \to \Pi_{N-1}$ definida por $\Phi(d) := p_d$. Ahora bien, como para todo $d := (d_1, \ldots, d_N) \in \mathcal{D}$, la representación densa de $p_d \in \Pi_{N-1}$ está dada por el vector $V^{-1}d$, donde $V := (\gamma_i^{j-1})_{1 \leq i,j \leq N} \in \mathbb{C}^{N \times N}$ es la matriz de Vandermonde asociada a $\gamma_1, \ldots, \gamma_N$, es claro que Φ es un morfismo regular y continuo en todo $\mathcal{D}$. Luego, la familia de problemas de interpolación de Lagrange univariados en nodos fijos $\gamma_1, \ldots, \gamma_N$ está representada por todo el espacio afín $\mathcal{D} := \mathbb{C}^N$, y la aplicación $\Phi : \mathcal{D} \to \Pi_{N-1}$ en el sentido de la Sección 6.1.

Sea $\mathcal{D}^* := \mathbb{C}^N$ y $\omega^* : \mathcal{D}^* \to \Pi_{N-1}$ la codificación de los elementos de Π_{N-1} determinada por su representación densa, i.e, $\omega^*(a_0, \ldots, a_{n-1}) := \sum_{j=0}^{N-1} a_j X^j$. Por lo tanto, la aplicación regular $\Psi : \mathcal{D} \to \mathcal{D}^*$ definida por $\Psi(d) := V^{-1}(d)$ es un algoritmo de interpolación en el sentido de arriba que está definido en todo $\mathcal{D}$.

Esta construcción se puede modificar fácilmente para modelar también la clásica interpolación de Lagrange univariada con nodos genéricos: sea $\mathcal{U} \subset \mathbb{C}^N$ el conjunto abierto $\mathcal{U} := \{ (\gamma_1, \ldots, \gamma_N) \mid \gamma_i \neq \gamma_j,\ 1 \leq i < j \leq N\}$ y sea $\mathcal{D} := \mathcal{U} \times \mathbb{C}^N \subset \mathbb{C}^N \times \mathbb{C}^N$.

Cada $(\gamma, d) \in \mathcal{D}$ define un problema de interpolación de Lagrange como antes *mutatis mutandis* en los nodos $\gamma_1, \ldots, \gamma_N$ con valores $d_1, \ldots, d_N$. Luego el *problema de interpolación de Lagrange genérico* está representado por la estructura de datos $\mathcal{D}$ y el morfismo $\Phi : \mathcal{D} \to \Pi_{N-1}$ que aplica cada $d \in \mathcal{D}$ en el único $p_{(\gamma,d)} \in \Pi_{N-1}$ que satisface $p_{(\gamma,d)}(\gamma_i) = d_i$ para $1 \leq i \leq N$. Puesto que la representación densa de $p_{(\gamma,d)}$ está dada por el vector $V(\gamma)^{-1}d$, vemos que para $\mathcal{D}^* := \mathbb{C}^N$, la aplicación $\omega^* : \mathcal{D}^* \to \Pi_{N-1}$, $\omega^*(p_0, \ldots, p_{N-1}) := \sum_{j=0}^{N-1} p_j X^j$, y el morfismo $\Psi : \mathcal{D} \to \mathcal{D}^*$, $\Psi(\gamma, d) := V(\gamma)^{-1}d$, constituyen un algoritmo que resuelve esta familia de problemas de interpolación.

6.2.2. Interpolación univariada de Lagrange-Hermite de un polinomio fijo

Fíjese $N \in \mathbb{N}$ y un polinomio univariado $f \in \Pi := \mathbb{C}[X]$ con $\mathrm{gr}(f) \gg N$, y sea $\mathcal{D} := \mathbb{C}^N$. Para cada $d \in \mathbb{C}^N$ consideramos el problema de interpolación de Lagrange-Hermite que consiste en hallar el único polinomio $p_d \in \Pi_{N-1}$ que satisface

$$D^j p_d(z) = D^j f(z) \qquad \text{para } \ 0 \leq j < u_z, \tag{6.2}$$

donde $u_z := \#\{j \in \{1, \ldots, N\} : z = d_j\}$, $z \in \mathbb{C}$.

Sea $\mathcal{D}^* := \mathbb{C}^N$ y $\omega^* : \mathcal{D}^* \to \Pi_{N-1}$ la codificación densa de los elementos de Π_{N-1}. El conocido método de interpolación de Newton o de diferencias divididas permite expresar

el único polinomio de Π_{N-1} que satisface las condiciones de interpolación (6.2) en la forma:

$$\sum_{j=1}^{N} f[d_1, \ldots, d_j](X - d_1) \ldots (X - d_j), \tag{6.3}$$

donde $f[d_1, \ldots, d_j]$ denota la j-ésima diferencia dividida. Afirmamos que las diferencias divididas $f[d_1, \ldots, d_j]$ son polinomiales en d. En efecto, sean nuevas indeterminadas $X_1, \ldots, X_N$ y definamos los polinomios $P_j \in \mathbb{C}[X_1, \ldots, X_j]$, $1 \leq j \leq N$, inductivamente como:

$$\begin{aligned} P_1 &:= f(X_1), \\ P_j &:= \frac{P_{j-1}(X_2, \ldots, X_j) - P_{j-1}(X_1, \ldots, X_{j-1})}{X_j - X_1}, \quad 2 \leq j \leq N. \end{aligned}$$

Sabemos que para todo $d := (d_1, \ldots, d_N) \in \mathbb{C}^N$ con $d_i \neq d_j$ para $i \neq j$, valen las identidades:

$$P_j(d_1, \ldots, d_j) = f[d_1, \ldots, d_j], \quad 1 \leq j \leq N. \tag{6.4}$$

Puesto que además las diferencias divididas $f[d_1, \ldots, d_j]$ son funciones continuas de d en la topología fuerte de $\mathbb{C}^N$ (véase [8]), concluimos que la identidad (6.4) vale para todo $d \in \mathbb{C}^N$, lo que demuestra nuestra afirmación.

Ahora, definimos $\Psi : \mathcal{D} \to \mathcal{D}^*$ como la aplicación tal que los valores $\Psi_1(d), \ldots, \Psi_N(d)$ son los coeficientes del polinomio de (6.3) considerado como un polinomio en $\mathbb{C}[d][X]$ para cada $d \in \mathcal{D}$. En consecuencia con $\omega^* : \mathcal{D}^* \to \Pi_{N-1}$ y $\Psi : \mathcal{D} \to \mathcal{D}^*$ así definidas, obtenemos un algoritmo de interpolación regular, esto es, definido en todo $\mathcal{D}$, para la familia de problemas de interpolación de Lagrange-Hermite definida por $\mathcal{D}$.

Por otra parte, es claro que el subconjunto $\mathcal{D}_0 := \{(d_1, \ldots, d_N) \in \mathbb{C}^N : d_i \neq d_j, \text{ para } i \neq j\}$ de $\mathcal{D}$ se puede interpretar como una estructura de datos que codifica la subfamilia de problemas de interpolación de Lagrange del polinomio fijo f en nodos genéricos.

Si $V(d) := (d_i^{j-1})_{1 \leq i,j \leq N} \in \mathbb{C}^{N \times N}$ representa la matriz de Vandermonde asociada a $d_1, \ldots, d_N$, la representación densa del único interpolante $p_d \in \Pi_{N-1}$ para el problema de interpolación de Lagrange definido por d está dado por $V(d)^{-1} f(d)$, donde $f(d) := (f(d_1), \ldots, f(d_N))$. Por lo tanto el morfismo racional $\psi : \mathcal{D}_0 \to \mathbb{C}^N$ definido por $\psi(d) := V(d)^{-1} f(d)$ es un algoritmo de interpolación para la familia de problemas de Lagrange $\mathcal{D}_0$.

A primera vista podría pensarse que este algoritmo ψ es una aplicación racional bien definida sobre $\mathcal{D}_0$, que no se extiende a $\overline{\mathcal{D}}_0 \setminus \mathcal{D}_0 = \mathbb{C}^N \setminus \mathcal{D}_0$. Sin embargo como ψ y Ψ son idénticas sobre el conjunto denso $\mathcal{D}_0$, se deduce que $\psi \equiv \Psi$ y por lo tanto ψ es polinomial.

6.2.3. Interpolación de Lagrange-Hermite bivariada sobre la curva $X^3 - Y^2 = 0$

Sea $\mathcal{D} := \mathcal{C} \setminus \{(-1, \pm i)\}$, donde $\mathcal{C} \subset \mathbb{C}^2$ es la curva algebraica definida por la ecuación $X^3 - Y^2 = 0$. Para cada $(u, v) \in \mathcal{D}$ distinto de $(0, 0)$ consideramos la interpolación de una función polinomial dada $f : \mathbb{C}^2 \to \mathbb{C}$ en los puntos (u, v) y $(0, 0)$.

Más precisamente, cada $(u, v) \in \mathcal{D} \setminus \{(0, 0)\}$, define un problema de interpolación de Lagrange en los nodos $(0, 0)$ y (u, v) con valores asociados $f(0, 0)$ y $f(u, v)$ respectivamente. Por otro lado, para el punto $(0, 0)$ consideramos el problema de interpolación de Hermite en el nodo $(0, 0)$ con valores $f(0, 0)$ y $\frac{\partial f}{\partial X}(0, 0)$, donde este último representa la evaluación en $(0, 0)$ de la derivada parcial con respecto a la variable X, y que consiste en hallar un polinomio $I_{(0,0)} \in \Pi_1$ tal que verifique $I_{(0,0)}(0, 0) = f(0, 0)$, $\frac{\partial I_{(0,0)}}{\partial X}(0, 0) = \frac{\partial f}{\partial X}(0, 0)$.

Es fácil ver que para cada $(u, v) \in \mathcal{D} \setminus \{(0, 0)\}$ existe un *único* polinomio interpolante $I_{(u,v)}$ que se halla en el espacio lineal $\mathbb{C} \oplus \mathbb{C} \cdot (uX + vY) \subset \Pi_1$ (este espacio de interpolantes corresponde al *"least solution space"* introducido en [10], véase también [9]):

$$I_{(u,v)} := f(0, 0) + \frac{(f(u, v) - f(0, 0))uX}{u^2 + v^2} + \frac{(f(u, v) - f(0, 0))vY}{u^2 + v^2}.$$

Para $(u, v) = (0, 0)$, tomamos

$$I_{(0,0)} := f(0, 0) + \frac{\partial f}{\partial X}(0, 0)X,$$

que de hecho es el único interpolante que se halla en el espacio lineal $\mathbb{C} \oplus \mathbb{C} \cdot X \subset \Pi_1$ para el problema de interpolación definido por el punto $(0, 0)$.

La aplicación $\Phi : \mathcal{D} \to \Pi_1$ definida por $\Phi(u, v) := I_{(u,v)}$, es claramante un morfismo racional sobre el abierto $\mathcal{D} \setminus \{(0, 0)\}$ y es fácil ver que también es continua (en la topología fuerte) en el punto $(0, 0)$. Por lo tanto tenemos una familia de problemas de interpolación de grado 1 codificada por $\mathcal{D}$ y $\Phi : \mathcal{D} \to \Pi_1$ en el sentido de la Sección 6.1.

Ahora, definiendo $\mathcal{D}^* := \mathbb{C}^3$ y $\omega^* : \mathcal{D}^* \to \Pi_1$ como $\omega^*(a, b, c) := a + bX + cY$ (la representación canónica densa de los polinomios bivariados de grado a lo sumo 1), tenemos que la aplicación racional $\Psi : \mathcal{D} \dashrightarrow \mathcal{D}^*$ definida como:

$$\Psi(u, v) := \big(f(0, 0), \frac{(f(u, v) - f(0, 0))u}{u^2 + v^2}, \frac{(f(u, v) - f(0, 0))v}{u^2 + v^2}\big), \tag{6.5}$$

junto con ω^* constituyen un algoritmo que resuelve la familia de problemas de interpolación $\mathcal{D}$, $\Phi : \mathcal{D} \to \Pi_1$ sobre el conjunto abierto Zariski $\mathcal{D} \setminus \{(0, 0)\}$.

6.2.4. Un ejemplo no lineal: sucesiones de identificación e interpolación

Sean $n, L \in \mathbb{N}$ que satisfacen $2^L \geq n$, y sea $\mathcal{O}_{L,n} \subset \Pi := \mathbb{C}[X_1, \ldots, X_n]$ el conjunto de los polinomios que se pueden evaluar mediante un straight-line program de longitud no escalar a lo sumo L. Observamos que todo polinomio $f \in \mathcal{O}_{L,n}$ tiene grado acotado por 2^L (véase [4, Exercise 9.18] o [24, Theorem 3.2]). En consecuencia $\mathcal{O}_{L,n} \subset \Pi_{2^L}$ puede considerarse como un subconjunto construible de $\mathbb{C}^{N_L}$, donde $N_L := \binom{2^L+n}{n}$.

Denotemos con $\overline{\mathcal{O}}_{L,n}$ a la clausura Zariski de $\mathcal{O}_{L,n}$ en su espacio ambiente $\mathbb{C}^{N_L}$. Se tiene que $\overline{\mathcal{O}}_{L,n}$ es una variedad absolutamente irreducible. Los elementos de este conjunto algebraico se corresponden con los polinomios n-variados que tienen *complejidad aproximativa* acotada por L (véase [1, Lemma 2 y Satz 4]).

Sea $n_L := 4(L + n + 1)^2 + 2$. De acuerdo con [6, Corollary 2] existen vectores $\gamma_1, \ldots, \gamma_{n_L} \in \mathbb{C}^n$ tales que para $f, g \in \overline{\mathcal{O}}^*_{L,n}$ las igualdades $f(\gamma_i) = g(\gamma_i)$ para $i = 1, \ldots, n_L$ implican $f = g$. Tal conjunto de vectores $\{\gamma_1, \ldots, \gamma_{n_L}\}$ se denomina una *sucesión de identificación* para la clase de polinomios $\overline{\mathcal{O}}_{L,n}$.

Sea $\Xi : \overline{\mathcal{O}}_{L,n} \to \mathbb{C}^{n_L}$ la aplicación polinomial (lineal) definida por

$$\Xi(f) := (f(\gamma_1), \ldots, f(\gamma_{n_L})).$$

Sea $\mathcal{D}_{L,n} := \Xi(\mathcal{O}_{L,n}) \subset \mathbb{C}^{n_L}$. Entonces [6, Theorem 2] muestra que $\overline{\mathcal{D}}_{L,n}$ es un cono irreducible afín de $\mathbb{C}^{n_L}$ y $\Xi : \overline{\mathcal{O}}_{L,n} \to \overline{\mathcal{D}}_{L,n}$ es un morfismo bijectivo, birracional, finito de variedades algebraicas y un homeomorfismo en la topología fuerte. Vamos a considerar a $\mathcal{D}_{L,n}$ como una estructura de datos que representa en forma natural una familia de problemas de interpolación.

Más precisamente, obsérvese que la elección $\gamma_1, \ldots, \gamma_{n_L}$ como una sucesión de identificación implica que para cada $d \in \mathcal{D}_{L,n}$, existe un *único* elemento $f \in \mathcal{O}_{L,n}$ que satisface $f(\gamma_j) = d_j$ para $1 \leq j \leq n_L$, a saber, el elemento $f = \Xi^{-1}(d)$. Así pues, si definimos $\Phi : \mathcal{D}_{L,n} \to \Pi_{2^L}$ como $\Phi(d) = \Xi^{-1}(d)$ obtenemos una familia de problemas de interpolación parametrizada por $\mathcal{D}_{L,n}$ en el sentido de la Sección 6.1. Obsérvese además que esta familia de problemas de interpolación es *no lineal* en el sentido que el espacio de interpolantes $\mathcal{O}_{L,n}$ es no lineal (no es cerrado para la adición).

La Sección 8.2 será dedicada al estudio de la complejidad algorítmica de resolver esta familia particular de problemas de interpolación, o equivalentemente, la complejidad de reconstruir los polinomios de $\mathcal{O}_{L,n}$ a partir de sus valores en una sucesión de identificación.

6.3. Complejidad de una familia de problemas de interpolación

Sea una familia de problemas de interpolación de grado D dada por una estructura de datos $\mathcal{D}$ y una aplicación $\Phi : \mathcal{D} \to \Pi_D$. Para todo algoritmo de interpolación $\omega^* : \mathcal{D}^* \to \Pi_D$, $\Psi : \mathcal{D} \dashrightarrow \mathcal{D}^*$, la dimensión del espacio ambiente de $\mathcal{D}^*$ se llama la *complejidad del algoritmo de interpolación* (ω^*, Ψ). Asimismo, la *La complejidad de una familia dada de problemas de interpolación* se define como la complejidad mínima de todos los algoritmos de interpolación que resuelven la familia de problemas de interpolación $\mathcal{D}$, $\Phi : \mathcal{D} \to \Pi_D$.

Por ejemplo, la complejidad de la interpolación de Lagrange univariada (genérica) en N nodos fijos (Ejemplo 6.2.1) es a lo sumo N.

Recalcamos que esta noción de complejidad es una generalización adecuada de tres medidas usuales de complejidad en teoría de eliminación efectiva: el tamaño de la representación densa o rala y la longitud (no escalar) de la representación por straight–line programs. En efecto, es claro que el tamaño mínimo de la representación densa o rala (el número total de monomios o de monomios no nulos en consideración) de una familia "continua" dada $\mathcal{F} := \{Q_j; j \in \mathcal{J}\} \subset \mathbb{C}[X_1, \ldots, X_n]$ de polinomios de grado acotado es una cota inferior para la complejidad de calcular un miembro genérico de $\mathcal{F}$. En otras palabras, podemos estimar inferiormente tal complejidad mediante la dimensión del menor espacio ambiente $\mathbb{A}^M$ que contiene $\mathcal{F}$. Por otro lado, para un polinomio dado $F \in \mathbb{C}[X_1, \ldots, X_n]$ podemos considerar la longitud no escalar mínima $L(F)$ de un straight–line program que evalúa F. Sea $L \in \mathbb{N}$ y defínase $W_L := \{F \in \mathbb{C}[X_1, \ldots, X_n]; L(F) \leq L\}$. De [4, Exercise 9.18] (véase también [24, Theorem 3.2]) deducimos que W_L es un subconjunto construible de $\mathbb{A}^{(L+n+1)^2}$ y por lo tanto la dimensión $(L + n + 1)^2$ del espacio ambiente de W_L refleja la longitud (no escalar) del straight–line program de un polinomio genérico $F \in W_L$.

Capítulo 7

Algoritmos robustos de interpolación

Con el fin de incluir fenómenos de coalescencia en nuestro modelo (véase, e.g., [3], [10], [30]), vamos a considerar resoluciones de problemas de interpolación límites mediante la noción de *algoritmo robusto*.

7.1. Hechos básicos de la teoría de places

Comenzamos recordando algunos hechos básicos de la teoría de places en el álgebra conmutativa y la geometría algebraica que necesitaremos después (seguimos los libros clásicos [39] y [28]) con el fin de dar un marco teórico adecuado a nuestra noción de robustez.

Un *place* (o un place Δ–valuado) de un cuerpo K es un homomorfismo de anillos $\vartheta : R_\vartheta \to \Delta$ donde Δ es otro cuerpo y $R_\vartheta \subset K$ es un subanillo que verifica que si $x \in K \setminus R_\vartheta$ entonces $1/x \in R_\vartheta$ y $\vartheta(1/x) = 0$. Para $x \notin R_\vartheta$ escribimos $\vartheta(x) = \infty$. El anillo R_ϑ se llama el *anillo de valuación* asociado a ϑ. Si el cuerpo K es una k–álgebra para otro cuerpo k y ϑ es un morfismo de k–espacios vectoriales, decimos que ϑ es un k–place.

Recordamos los siguientes resultados básicos y bien conocidos:

Teorema I (Extensión de places) ([39, Theorem 5', Ch.VI, §4] y [28, Ch. VII, §3, Corollary 3.3]) *Sea A un dominio íntegro contenido en un cuerpo K y sea $\epsilon : A \to L$ una especialización (i.e., un homomorfismo de anillos) de A sobre otro anillo L. Entonces ϵ se puede extender a un place ϑ de K. Si L es algebraicamente cerrado, el place ϑ puede elegirse L–valuado.*

Obsérvese que si K, L y A son k–álgebras para cierto cuerpo k y ϵ es un k–homomorfismo, el place ϑ resulta un k–place.

Teorema II (Places y clausura entera) ([39, Theorem 6, Ch.VII, §5]) *Sea A un dominio íntegro contenido en un cuerpo K. Entonces la intersección $\bigcap_\vartheta R_\vartheta$, donde ϑ recorre todos los places de K tales que $A \subset R_\vartheta$, es la clausura entera de A en K.*

Si A es la localización de una $\mathbb{C}$–álgebra finitamente generada, la clausura entera de A en su cuerpo de fracciones es la intersección de los anillos de valuación asociados a los $\mathbb{C}$–places $\mathbb{C}$–valuados que contienen A.

7.2. La noción de robustez

Ahora procedemos a introducir la noción de *robustez* para algoritmos de interpolación.

Con la terminología de la Sección 6.1, sea $\omega^* : \mathcal{D}^* \to \Pi_D$, $\Psi : \mathcal{D} \dashrightarrow \mathcal{D}^* \subseteq \mathbb{C}^M$ un algoritmo que resuelve un familia dada $\mathcal{D}$, $\Phi : \mathcal{D} \to \Pi_D$ de problemas de interpolación. En lo que sigue, denotamos con $\mathfrak{M}_d$ al ideal maximal asociado a un punto dado $d \in \overline{\mathcal{D}}$ en el anillo de coordenadas $\mathbb{C}[\overline{\mathcal{D}}]$.

Informalmente hablando, un algoritmo robusto de interpolación para una familia dada de problemas de interpolación es un algoritmo que admite una única extensión a los problemas límites bien definidos, esto es, los problemas correspondientes a puntos de $\mathcal{D}$ donde Ψ no está definido, y que los resuelve. Formalizamos esta idea mediante la teoría de places.

Definición 7.1 *Con las notaciones anteriores, decimos que el algoritmo $\omega^* : \mathcal{D}^* \to \Pi_D$, $\Psi : \mathcal{D} \dashrightarrow \mathcal{D}^*$ es* robusto *si y solo si la siguiente condición se satisface en* todo *punto $d \in \mathcal{D}$: para todo $\mathbb{C}$–place $\vartheta : \mathbb{C}(\overline{\mathcal{D}}) \to \mathbb{C} \cup \{\infty\}$ que es finito sobre el anillo local $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d}$, el valor $\vartheta(\Psi_j)$ es finito y depende solo del punto d y del índice j, pero no depende del place ϑ. Denotaremos este valor con $\Psi_j(d)$, aun si Ψ_j no está definida en d.*

En la próxima sección exhibiremos algoritmos robustos que resuelven las familias de problemas de las Subsecciones 6.2.1 y 6.2.3 con el objeto de ilustrar esta noción.

Ahora establecemos algunos comentarios y consecuencias concernientes a esta definición que necesitaremos más tarde.

Sea $d \in \mathcal{D}$ y sea ϑ un place $\mathbb{C}$–valuado del cuerpo $\mathbb{C}(\overline{\mathcal{D}})$ cuyo anillo de valuación asociado R_ϑ contiene el anillo local $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d}$. El place ϑ induce por restricción un $\mathbb{C}$-homomorfismo $\epsilon : \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d} \to \mathbb{C}$, que es necesariamente la evaluación en el punto d. Si la función racional Ψ_j está definida en d (i.e., $\Psi_j \in \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d}$ para $1 \leq j \leq M$), el valor $\vartheta(\Psi_j)$ no depende del place ϑ y coincide con $\Psi_j(d)$. Por lo tanto, la condición de robustez se satisface trivialmente en todo punto del dominio de Ψ y tenemos la siguiente observación:

Observación 7.2 *Un algoritmo definido por una aplicación regular* $\Psi : \mathcal{D} \to \mathcal{D}^*$ *es necesariamente robusto.*

Sin embargo, la condición de la Definición 7.1 tiene un sentido no trivial (en el espíritu de la regla de L'Hôpital) si d anula tanto el numerador como el denominador de Ψ_j. Esta analogía sugiere nuestra notación extendida $\Psi(d)$ para puntos d de $\mathcal{D}$ donde Ψ no está definida.

Del Teorema II inferimos que si Ψ es robusto, el morfismo natural $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d}$ $\hookrightarrow \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d}[\Psi_1, \ldots, \Psi_M]$ es una extensión entera para todo punto $d \in \mathcal{D}$, i.e., las funciones racionales Ψ_j son enteras sobre $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d}$. En particular, si d es un punto suave de $\mathcal{D}$ esto implica que la aplicación Ψ puede ser realmente evaluada en d, puesto que el anillo local $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d}$ es integralmente cerrado y entonces contiene a las funciones Ψ_j. Esto justifica la siguiente observación:

Observación 7.3 *Si el conjunto construible* $\mathcal{D}$ *es suave y el algoritmo es robusto, la aplicación racional* $\Psi : \mathcal{D} \to \mathcal{D}^*$ *está definida en todas partes, i.e, es una aplicación regular sobre todo el espacio* $\mathcal{D}$*.*

Este es el caso para la clásica interpolación univariada de Lagrange-Hermite (véase las Secciones 6.2.1 y 6.2.2). Para la robustez en puntos singulares, véase el ejemplo considerado en las Subsecciones 6.2.3 y 7.3.2.

Nuestra definición de robustez afirma que la aplicación Ψ se puede extender a todo el conjunto $\mathcal{D}$, produciendo puntos bien definidos en $\mathbb{C}^M$. Las imágenes correspondientes a *puntos límites*, esto es, a puntos de $\mathcal{D}$ donde Ψ no está definida, no necesariamente pertenecen al conjunto construible $\mathcal{D}^*$, sino a su clausura Zariski en $\mathbb{C}^M$. En efecto, para todo polinomio g que se anula sobre $\mathcal{D}^*$, la composición $g \circ \Psi$ es una función racional en $\mathbb{C}(\overline{\mathcal{D}})$ que se anula en un conjunto $\mathcal{U} \subset \mathcal{D}$ (a saber, la intersección de $\mathcal{D}$ con el dominio de Ψ) denso en $\overline{\mathcal{D}}$ y por lo tanto, es la función racional cero. En consecuencia, para todo place ϑ de $\mathbb{C}(\overline{\mathcal{D}})$ tenemos $0 = \vartheta(g \circ \Psi) = g(\vartheta(\Psi))$, lo que prueba nuestra afirmación.

Las imágenes por la extensión de Ψ de los puntos límites representan de hecho el código de polinomios en Π_D, que son recuperados mediante la aplicación polinomial ω^*. Por otro lado, el algoritmo Ψ resuelve el problema de interpolación definido por cada punto de su dominio. En consecuencia es natural preguntarse si la extensión de Ψ a los puntos límites por medio de los places produce códigos en $\mathcal{D}^*$ correspondientes a polinomios que resuelven los respectivos problemas de interpolación particulares. En otras palabras, nos preguntamos si la identidad $\Phi(d) = \omega^*(\Psi(d))$ es válida aun para puntos fuera del dominio de Ψ. No intentaremos establecer las condiciones necesarias y suficientes en las que esto se verifica en general, pero podremos constatarlo en los ejemplos particulares de la Sección 7.3.

7.2.1. Robustez bajo restricción

Como dijimos antes, la condición de robustez asegura que el algoritmo Ψ se puede especializar en todo punto (cerrado) de $\mathcal{D}$. De hecho podemos mostrar algo más fuerte y muy natural: aun si las funciones racionales Ψ_j no están definidas en todo punto de $\mathcal{D}$, para toda subvariedad cerrada $\mathcal{Z} \subset \overline{\mathcal{D}}$ tal que $\mathcal{D} \cap \mathcal{Z}$ es un subconjunto denso en $\mathcal{Z}$, las funciones Ψ_j inducen "funciones restricción" ψ_j que son racionales sobre $\mathcal{Z}$. Más precisamente:

Proposición 7.4 *Sea $\omega^* : \mathcal{D}^* \to \Pi_D$, $\Psi : \mathcal{D} \dashrightarrow \mathcal{D}^* \subset \mathbb{C}^M$ un algoritmo robusto que resuelve una familia de problemas de interpolación $\mathcal{D}$, $\Psi : \mathcal{D} \to \Pi_D$, y sea $\mathcal{Z} \subset \overline{\mathcal{D}}$ un cerrado irreducible Zariski tal que $\mathcal{D} \cap \mathcal{Z}$ es un subconjunto Zariski denso en $\mathcal{Z}$. Entonces, existen funciones racionales $\psi_1, \ldots, \psi_M \in \mathbb{C}(\mathcal{Z})$ tales que para todo punto $d \in \mathcal{D} \cap \mathcal{Z}$ y para todo par de $\mathbb{C}$-places ϑ, ϑ' de los cuerpos $\mathbb{C}(\overline{\mathcal{D}})$ y $\mathbb{C}(\mathcal{Z})$ respectivamente, que son finitos sobre los anillos locales $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d}$ y $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_d}$, la identidad $\vartheta(\Psi_j) = \vartheta'(\psi_j)$ vale para todo $j = 1, \ldots, M$.*

Demostración: Considérese el morfismo surjectivo canónico $\pi : \mathbb{C}[\overline{\mathcal{D}}] \to \mathbb{C}[\mathcal{Z}]$ inducido por la inclusión $\mathcal{Z} \subset \overline{\mathcal{D}}$. Por la propiedad de extensión de places (Teorema I) se sigue que existe un $\mathbb{C}$–place $\wp$ de $\mathbb{C}(\overline{\mathcal{D}})$ que extiende π. Denotamos con Ω el cuerpo residual asociado. En consecuencia, tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathbb{C}[\overline{\mathcal{D}}] & \xrightarrow{\pi} & \mathbb{C}[\mathcal{Z}] \\ \big\downarrow & & \big\downarrow{\scriptstyle \sigma} \\ R_\wp & \xrightarrow[\wp]{} & \Omega \end{array}$$

donde el anillo local $R_\wp \subset \mathbb{C}(\overline{\mathcal{D}})$ asociado a $\wp$ contiene $\mathbb{C}[\overline{\mathcal{D}}]$ y σ es un monomorfismo.

Sea $d_0 \in \mathcal{D} \cap \mathcal{Z}$. Por la condición de robustez, la función racional Ψ_j pertenece a la clausura entera del anillo $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}}$ y por lo tanto existe un polinomio $P := T^N + a_{N-1}T^{N-1} + \cdots + a_0 \in \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}}[T]$ que anula a Ψ_j. Sea $\mathcal{V} \subset \overline{\mathcal{D}}$ un conjunto abierto Zariski, que contiene a d_0, donde todos los coeficientes a_i están bien definidos. Por lo tanto $P = 0$ también es una ecuación de dependencia entera para Ψ_j sobre el anillo local de todo punto que se halla en $\mathcal{D} \cap \mathcal{V}$. Como $d_0 \in \mathcal{V} \cap \mathcal{Z}$, concluímos que $\mathcal{V} \cap \mathcal{Z}$ también es un subconjunto abierto Zariski denso de $\mathcal{Z}$.

Puesto que el morfismo π también está bien definido en el anillo local del punto d_0, por el Teorema II se sigue que el anillo $R_\wp$ contiene al anillo $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}}$ y al elemento entero Ψ_j. En consecuencia, el elemento $\xi := \wp(\Psi_j)$ se halla en el cuerpo Ω y es entero sobre $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_{d_0}}$. En particular, ξ es algebraico sobre $\mathbb{C}(\mathcal{Z})$ y $\pi(P) = 0$ es una ecuación de dependencia algebraica (no necesariamente minimal) para ξ sobre $\mathbb{C}(\mathcal{Z})$. Para evitar notaciones innecesarias consideramos $\mathbb{C}(\mathcal{Z})$ como un subcuerpo de Ω.

Sea $m_\xi \in \mathbb{C}(\mathcal{Z})[T]$ el polinomio unitario minimal de ξ sobre $\mathbb{C}(\mathcal{Z})$. Tenemos que m_ξ es libre de cuadrados y su discriminante Δ es no nulo. En consecuencia, existe un conjunto abierto Zariski no vacío $\mathcal{V}' \subseteq \mathcal{Z}$ tal que, para todo $d \in \mathcal{V}'$, el polinomio $m_\xi(d, T)$ está bien definido y resulta $\Delta(d) \neq 0$, en otras palabras, el polinomio $m_\xi(d, T)$ es libre de cuadrados para todo d en este subconjunto abierto de $\mathcal{Z}$. Sin pérdida de generalidad podemos suponer $\mathcal{V}' \subset \mathcal{V} \cap \mathcal{Z}$ y $d_0 \in \mathcal{V}'$ (recuérdese que $\mathcal{D} \cap \mathcal{Z}$ se supone denso en $\mathcal{Z}$).

Sea $I \subset \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}}[T]$ el ideal generado por los polinomios univariados que se anulan en Ψ_j (en particular, $P \in I$). Tenemos un isomorfismo natural

$$\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}}[\Psi_j] \simeq \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}}[T]/I.$$

Por otro lado, el morfismo π induce una aplicación $\varphi : \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}}[T] \to \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_{d_0}}[T]/m_\xi$, cuyo núcleo contiene al ideal I: si $Q(\Psi_j) = 0$, aplicando el place $\wp$ tenemos $\pi(Q)(\xi) = 0$, por lo tanto $\pi(Q)$ es divisible por el polinomio minimal m_ξ in $\mathbb{C}(\mathcal{Z})[T]$; puesto que $\pi(Q)$ y m_ξ pertenecen a $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_{d_0}}[T]$ y m_ξ es unitario, la división ocurre en este anillo, y por lo tanto $\pi(Q)$ es un múltiplo de m_ξ en $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_{d_0}}[T]$. Resumiendo, tenemos el siguiente diagrama:

$$\begin{array}{ccc} \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}} & \xrightarrow{\quad\pi\quad} & \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_{d_0}} \\ \downarrow & & \downarrow \\ \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}}[\Psi_j] & \xrightarrow[\varphi]{} & \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_{d_0}}[T]/m_\xi \end{array}$$

Sea ahora $\omega \in \mathbb{C}$ una raíz de $m_\xi(d_0, T)$. Tenemos que

$$\begin{array}{ccc} \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}} & \xrightarrow{\mathrm{ev}_{d_0}} & \mathbb{C} \\ \downarrow & \nearrow_{\mathrm{ev}_\omega} & \\ \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_{d_0}}[T]/m_\xi & & \end{array}$$

conmuta, donde ev_ω es la aplicación obtenida mediante la evaluación de toda función racional de $\mathbb{C}[\overline{\mathcal{Z}}]_{\mathfrak{M}_{d_0}}$ en d_0 y T en ω. Siguiendo el Teorema I, la aplicación $\mathrm{ev}_\omega \circ \varphi : \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}}[\Psi_j] \to \mathbb{C}$ se puede extender a un $\mathbb{C}$–place ϑ_ω del cuerpo de fracciones $\mathbb{C}(\overline{\mathcal{D}})$ con valores en $\mathbb{C} \cup \{\infty\}$. Este place también extiende la evaluación in d_0, su anillo local asociado R_{ϑ_ω} contiene $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{d_0}}$ y verifica $\vartheta_\omega(\Psi_j) = \omega$.

Por la hipótesis de robustez, el valor $\vartheta_\omega(\Psi_j)$ no depende del place ϑ_ω, lo que en particular implica que es independiente de la elección de la raíz ω. Por lo tanto el polinomio $m_\xi(d_0, T)$ es de grado uno y por ende lo es m_ξ. En consecuencia el elemento ξ es una función racional de $\mathbb{C}(\mathcal{Z})$.

Escribamos $\psi_j := \xi$. Afirmamos que con esta definición, las funciones racionales ψ_j para $1 \leq j \leq M$ verifican el enunciado de la proposición.

Sea $d \in \mathcal{D} \cap \mathcal{Z}$ y sea $\vartheta' : \mathbb{C}(\mathcal{Z}) \to \mathbb{C} \cup \{\infty\}$ un $\mathbb{C}$–place que es finito sobre el anillo local $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_d}$. En particular, ϑ' extiende la evaluación $\mathrm{ev}_d : \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_d} \to \mathbb{C}$. Claramente $\vartheta'(\psi_j)$ es finito pues ψ_j es entero sobre $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_d}$. Si $R_{\vartheta'} \subset \mathbb{C}(\mathcal{Z}) \subset \Omega$ denota su anillo de valuación asociado, existe un place $\theta : \Omega \to \mathbb{C} \cup \{\infty\}$ que extiende $\vartheta' : R_{\vartheta'} \to \mathbb{C}$ y, en particular, es finito sobre $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_d} \subset R_{\vartheta'}$.

Finalmente, considérese el homomorfismo $\theta \circ \wp : \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d}[\Psi_j] \to \mathbb{C}$. Este morfismo se puede extender a un $\mathbb{C}$–place $\vartheta : \mathbb{C}(\overline{\mathcal{D}}) \to \mathbb{C} \cup \{\infty\}$ finito sobre $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_d}$, y por lo tanto vale $\vartheta'(\psi_j) = \theta(\psi_j) = \theta \circ \wp(\Psi_j) = \vartheta(\Psi_j)$. Esto concluye la demostración de la proposición. ∎

7.3. Ejemplos de algoritmos robustos

En esta sección analizamos si los algoritmos que resuelven las familias de problemas de interpolación introducidas en la Sección 6.2 son robustos.

7.3.1. Interpolación de Lagrange y de Lagrange–Hermite univariada clásica: ejemplos 6.2.1 y 6.2.2

Los algoritmos que resuelven las familias de problemas de interpolación univariados de Lagrange y de Lagrange–Hermite de las Subsecciones 6.2.1 y 6.2.2 respectivamente, son ambos regulares, y por lo tanto, de acuerdo a la Observación 7.2, son trivialmente robustos. Más interesante es el caso de la familia de problemas de interpolación de Lagrange bivariada de la Subsección 6.2.3 que discutimos a continuación.

7.3.2. Robustez en puntos singulares: ejemplo 6.2.3

Ahora analizamos el algoritmo para la familia de problemas de interpolación discutida en la Subsección 6.2.3: la interpolación de Lagrange bivariado de una función polinomial arbitraria $f : \mathbb{C}^2 \to \mathbb{C}$ en los nodos $(0,0)$ y (u,v), donde (u,v) recorre la curva abierta $\mathcal{D} := \{X^3 - Y^2 = 0\} \setminus \{(-1, \pm i)\}$. Este ejemplo difiere de los anteriores en que la estructura de datos $\mathcal{D}$ de la familia de problemas de interpolación en consideración no es suave en el punto $(0,0)$.

Procedemos a mostrar la robustez en $(0,0)$ del algoritmo $\omega^* : \mathcal{D}^* \to \Pi_1$, $\Psi : \mathcal{D} \dashrightarrow \mathcal{D}^*$ definido en la Subsección 6.2.3, donde $\mathcal{D}^* := \mathbb{C}^3$, la codificación $\omega^* : \mathcal{D}^* \to \Pi_1$ corresponde a la representación densa, y Ψ está definida por:

$$\Psi(u,v) := \big(f(0,0), \frac{(f(u,v) - f(0,0))u}{u^2 + v^2}, \frac{(f(u,v) - f(0,0))v}{u^2 + v^2}\big).$$

Puesto que $X^2+Y^2 = X^2(1+X)$ sobre la curva, tenemos las siguientes expresiones equivalentes para las funciones racionales $\Psi_2, \Psi_3 \in \mathbb{C}(\mathcal{D})$:

$$\Psi_2(X,Y) = \frac{(f(X,Y)-f(0,0))}{X(1+X)},\ \Psi_3(X,Y) = \frac{(f(X,Y)-f(0,0))X}{Y(1+X)}.$$

Primeramente analizamos si es posible definir el valor de Ψ_2 en $(0,0)$ en el sentido de la Definición 7.1. Claramente, el elemento $1/1+X$ es una unidad en el anillo local $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{(0,0)}}$ y $\vartheta(1/1+X) = 1$ para todo $\mathbb{C}$–place ϑ cuyo anillo de valuación contiene $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{(0,0)}}$. Además, tenemos la siguiente identidad en $\mathbb{C}(\overline{\mathcal{D}})$:

$$\frac{f(X,Y)-f(0,0)}{X} = \frac{\partial f}{\partial X}(0,0) + \frac{Y}{X}\,\frac{\partial f}{\partial Y}(0,0) + X\,Q_1(X,Y) +$$

$$\frac{Y^2}{X}\,Q_2(X,Y) + Y\,Q_3(X,Y)$$

para polinomios Q_1, Q_2 y Q_3 adecuados. De la igualdad

$$\left(\frac{Y}{X}\right)^2 - X = \frac{Y^2}{X^2} - Y = \frac{X^3}{X^2} - X = 0 \tag{7.1}$$

en $\mathbb{C}(\overline{\mathcal{D}})$, concluimos que Y/X pertenece a la clausura entera de $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{(0,0)}}$ y por lo tanto, para todo $\mathbb{C}$–place ϑ finito sobre $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{(0,0)}}$ tenemos $\vartheta(Y/X) \neq \infty$. Además, de (7.1) concluimos que $(Y/X)^2$ pertenece a $\mathfrak{M}_{(0,0)}R_\vartheta$ y por lo tanto Y/X pertenece al ideal maximal de R_ϑ. En consecuencia, tenemos $\vartheta(Y/X) = 0$, lo que implica que $\vartheta(\Psi_2) = \frac{\partial f}{\partial X}(0,0)$. Esto muestra que el valor $\Psi_2(0,0)$ puede definirse como $\Psi_2(0,0) := \frac{\partial f}{\partial X}(0,0)$.

Con un análisis similar se infiere que $\vartheta(\Psi_3) = 0$ para todo $\mathbb{C}$–place ϑ finito sobre $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{(0,0)}}$ y por lo tanto, podemos definir $\Psi_3(0,0) := 0$. Se sigue que el algoritmo $\omega^* : \mathcal{D}^* \to \Pi_1$, $\Psi : \mathcal{D} \dashrightarrow \mathcal{D}^*$ de la Subsección 6.2.3 es robusto en $(0,0)$ y que vale $\Psi(0,0) = (f(0,0), \frac{\partial f}{\partial X}(0,0), 0)$.

Cabe mencionar que mediante las mismas relaciones entre las variables X, Y establecidas en la discusión anterior es posible deducir que el algoritmo Ψ se extiende con continuidad (en la topología fuerte) al punto $(0,0)$, y que el valor límite en este sentido coincide con el hallado mediante places.

7.3.3. Robustez de algoritmos para interpolar polinomios codificados por sus valores: ejemplo 6.2.4

Retomamos aquí el análisis de la familia de problemas de interpolación de la Subsección 6.2.4: la reconstrucción de los polinomios n–variados con coeficientes complejos

que se evalúan por un straight–line program de longitud no escalar a lo sumo L, a partir de sus valores en una sucesión de identificación. Siguiendo las notaciones de aquella subsección, esta familia de problemas está representada por la estructura de datos $\mathcal{D}_{L,n}$ y la aplicación $\Phi : \mathcal{D}_{L,n} \to \mathcal{O}_{L,n} \subset \Pi_{2^L}$, que es la inversa de la aplicación polinomial $\Xi : \mathcal{O}_{L,n} \to \mathcal{D}_{L,n}$ dada por la evaluación en una sucesión de identificación del conjunto $\overline{\mathcal{O}}^*_{L,n}$.

Considérese un algoritmo robusto $\omega^* : \mathcal{D}^* \to \mathcal{O}_{L,n}$, $\Psi : \mathcal{D}_{L,n} \dashrightarrow \mathcal{D}^*$ para esta familia de problemas de interpolación. Como se mencionó en los comentarios a la Definición 7.1, de la hipótesis de robustez se sigue que para cada $d \in \mathcal{D}_{L,n}$ tenemos un vector bien definido $\Psi(d)$ de la clausura $\overline{\mathcal{D}}^*$. En el siguiente lema se confirma que este vector $\Psi(d)$ resulta un código de la solución $\Phi(d) \in \mathcal{O}_{L,n}$ del problema de interpolación correspondiente al punto d.

Lema 7.5 *Sea $\omega^* : \mathcal{D}^* \to \mathcal{O}_{L,n}$, $\Psi : \mathcal{D}_{L,n} \dashrightarrow \mathcal{D}^*$ un algoritmo robusto que resuelve la familia de problemas de interpolación $\mathcal{D}_{L,n}$, $\Phi : \mathcal{D}_{L,n} \to \mathcal{O}_{L,n}$. Entonces se verifica $\omega^*(\Psi(d)) = \Phi(d)$ para todo $d \in \mathcal{D}_{L,n}$.*

Demostración: Sea $\mathcal{U}$ el abierto Zariski de la clausura $\overline{\mathcal{D}}_{L,n}$ donde está definida la aplicación racional Ψ y sea $\mathcal{V} := \mathcal{D}_{L,n} \cap \mathcal{U}$. De la Definición 6.1 de algoritmo de interpolación, es inmediato que $\omega^*(\Psi(d)) = \Phi(d)$ para todo $d \in \mathcal{V}$. Equivalentemente, la aplicación racional $\Xi \circ \omega^* \circ \Psi$ coincide con la identidad en el conjunto $\mathcal{V}$. Puesto que $\mathcal{V}$ es un subconjunto denso de $\overline{\mathcal{D}}_{L,n}$ deducimos que $\Xi \circ \omega^* \circ \Psi$ es la aplicación racional identidad. Por lo tanto, recordando que Ξ y ω^* son polinomiales, tenemos que para todo $d \in \mathcal{D}_{L,n}$ y todo $\mathbb{C}$–place $\vartheta : \mathbb{C}(\overline{\mathcal{D}}_{L,n}) \to \mathbb{C} \cup \{\infty\}$ finito sobre el anillo local $\mathbb{C}[\overline{\mathcal{D}}_{L,n}]_{\mathfrak{m}_d}$, vale la igualdad $(\Xi \circ \omega^*)(\vartheta(\Psi)) = d$. En otras palabras, $\omega^*(\vartheta(\Psi)) = \Phi(d)$ como se quería demostrar. ∎

Capítulo 8

Cotas inferiores de complejidad para algoritmos robustos

En esta sección obtenemos los resultados principales de la Parte II, a saber, cotas inferiores de complejidad (en el sentido de la Sección 6.3) de ciertas familias de problemas de interpolación. Nuestros resultados pueden clasificarse en dos grupos: cotas inferiores en términos del número de nodos involucrados, que se presentan en la Sección 8.1, y cotas inferiores en términos del costo de la "longitud" de la representación de los interpolantes, que son consideradas en la Sección 8.2.

8.1. Problemas de interpolación de Lagrange

En esta sección exhibimos cotas inferiores de complejidad de problemas de interpolación de Lagrange. Primeramente, en la Sección 8.1.1 mostramos que la complejidad de una familia de problemas de interpolación de Lagrange con N nodos, codificada por un subconjunto abierto Zariski no vacío de todo el espacio afín $\mathbb{C}^N$, es lineal en el número N de nodos, mostrando por lo tanto que los conocidos métodos de interpolación son esencialmente óptimos. Reforzamos significativamente esta conclusión en la Sección 8.1.2 para algoritmos *robustos*, demostrando que la conclusión anterior también vale para una familia de problemas de interpolación con N nodos que tienen interpolantes "fáciles" de evaluar.

8.1.1. Familias codificadas por un abierto de Zariski no vacío en el espacio afín

Sea $\mathcal{D} \subset \mathbb{C}^{(n+1)N}$ un conjunto abierto Zariski no vacío que codifica una familia de problemas de interpolación de Lagrange n–variados de grado D con N nodos. Más precisamente, supóngase que para cada $d := (\xi_1, y_1, \ldots, \xi_N, y_N) \in \mathcal{D}$ con $\xi_i \in \mathbb{C}^n$ y

$y_i \in \mathbb{C}$, se tiene el problema de interpolación, que consiste en hallar un polinomio n–variado p de grado a lo sumo D tal que $p(\xi_i) = y_i$, $1 \leq i \leq N$. Supóngase además que el problema está bien definido para todo $d \in \mathcal{D}$, esto es, que para cada $d \in \mathcal{D}$, existe el correspondiente interpolante de manera que existe una aplicación $\Phi : \mathcal{D} \to \Pi_D$ que asocia cada $d \in \mathcal{D}$ con un interpolante.

Tenemos el siguiente resultado:

Teorema 8.1 *Sea $\mathcal{D}^* \subseteq \mathbb{C}^M$ un conjunto construible para el cual existe un algoritmo $\omega^* : \mathcal{D}^* \to \Pi_D$, $\Psi : \mathcal{D} \dashrightarrow \mathcal{D}^*$ que resuelve la familia de problemas de interpolación de Lagrange $\mathcal{D}$, $\Phi : \mathcal{D} \to \Pi_D$. Entonces $M \geq N$.*

En otras palabras, todo *algoritmo que resuelve* toda *familia de problemas de interpolación de Lagrange codificada por un conjunto abierto Zariski con un número fijo de nodos N tiene complejidad al menos lineal en N.*

Demostración: Sea $\mathcal{U}$ un subconjunto abierto Zariski no vacío de $\mathcal{D} \subset \mathbb{C}^{(n+1)N}$ donde la función racional Ψ es regular. Fíjese un elemento $a := (a_1, \ldots, a_N) \in \mathbb{C}^{nN}$ tal que el conjunto

$$A := \{(y_1, \ldots, y_N) \in \mathbb{C}^N | (a_1, y_1, \ldots, a_N, y_N) \in \mathcal{U}\}$$

contenga un conjunto abierto Zariski no vacío en $\mathbb{C}^N$. Un tal elemento $a \in \mathbb{C}^{nN}$ debe existir ya que $\mathcal{U}$ es un subconjunto abierto Zariski no vacío de $\mathbb{C}^{(n+1)N}$ y la projección es una aplicación abierta.

Considérese la aplicación de A a $\mathbb{C}^N$ definida por la siguiente regla:

$$y \mapsto (\Phi(a, y)(a_1), \ldots, \Phi(a, y)(a_N)),$$

donde $a := (a_1, \ldots, a_N)$, $y := (y_1, \ldots, y_N)$ y $(a, y) := (a_1, y_1, \ldots, a_N, y_N)$. De esta definición se sigue que esta aplicación es simplemente la aplicación identidad sobre el conjunto A. Por otro lado, por la definición de un algoritmo de interpolación tenemos la identidad $\Phi = \omega^* \circ \Psi$ en $\mathcal{U}$. Por lo tanto, la aplicación identidad sobre $\mathcal{U}$ también se puede escribir como la composición $\mathrm{id}_{\mathcal{U}} = \varphi_2 \circ \varphi_1$, donde $\varphi_1 : \mathcal{U} \to \mathcal{D}^*$ está definida por $y \mapsto \Psi(a, y)$ y $\varphi_2 : \mathcal{D}^* \to \mathbb{C}^N$ por $d^* \mapsto (\omega^*(d^*)(a_1), \ldots, \omega^*(d^*)(a_N))$. Obviamente las aplicaciones φ_1 y φ_2 son ambas regulares sobre sus dominios.

Puesto que la dimensión nunca aumenta bajo aplicaciones regulares y $\dim \mathcal{U} = N$, concluimos que $M \geq \dim \mathcal{D}^* \geq \dim \mathrm{im}(\varphi_1) \geq \dim \mathrm{im}(\varphi_2 \circ \varphi_1) = \dim \mathcal{U} = N$. ∎

8.1.2. Una familia codificada por el gráfico de una aplicación polinomial

Sea $N \in \mathbb{N}$, sean T, X dos indeterminadas sobre $\mathbb{C}$ y sea

$$F(X, T) := (T^N - 1) \sum_{i=0}^{N-1} T^i X^i.$$

Considérese el conjunto construible $\mathcal{D} \subset \mathbb{C}^{2N}$ definido como:

$$\mathcal{D} := \{(x_1, y_1, \ldots, x_N, y_N) | \ \exists\ t \in \mathbb{C} \text{ tal que } y_i = F(x_i, t) \text{ para } i = 1, \ldots, N \\ \text{y } x_i \neq x_j \text{ para } 1 \leq i < j \leq N\}.$$

Sea $\mathcal{U} := \{(x_1, \ldots, x_N) \in \mathbb{C}^N | x_i \neq x_j \text{ para } 1 \leq i < j \leq N\}$ y sea $\sigma : \mathcal{U} \times \mathbb{C} \to \mathbb{C}^{2N}$ la siguiente aplicación polinomial:

$$\sigma(x_1, \ldots, x_N, t) := (x_1, F(x_1, t), \ldots, x_N, F(x_N, t)).$$

Claramente $\mathcal{D} = \mathrm{Im}(\sigma)$, lo que en particular implica que la clausura Zariski $\overline{\mathcal{D}}$ es irreducible. Para todo $z := (x_1, y_1, \ldots, x_N, y_N) \in \mathcal{D}$, la fibra σ^{-1} es un conjunto finito y por lo tanto, por el Teorema de la dimensión de las fibras [36], concluímos que $\dim \mathcal{D} = \dim \mathrm{Im}(\sigma) = N+1$. [§I.6.3, Theorem] El conjunto $\mathcal{D}$ codifica una familia de problemas de interpolación de Lagrange univariados con N nodos, donde el morfismo $\Phi : \mathcal{D} \to \Pi_{N-1}$ asigna a cada $z := (x_1, y_1, \ldots, x_N, y_N) \in \mathcal{D}$ el único polinomio de la forma $F(X, t)$ $(t \in \mathbb{C})$ que satisface las condiciones de interpolación definidas por z.

Obsérvese que en este caso la estructura de datos $\mathcal{D}$ que codifica la familia de problemas de interpolación de Lagrange $\mathcal{D}$, $\Phi : \mathcal{D} \to \Pi_{N-1}$ no es un subconjunto denso Zariski del espacio de nodos/valores $\mathbb{C}^{2N}$, como en la subsección anterior, sino un subconjunto de dimensión $N + 1$ en un espacio ambiente $2N$–dimensional.

Proposición 8.2 *Con las notaciones de arriba, supóngase que existe un conjunto construible $\mathcal{D}^* \subseteq \mathbb{C}^M$ para el cual existe un algoritmo* robusto *$\omega^* : \mathcal{D}^* \to \Pi_{N-1}$, $\Psi : \mathcal{D} \dashrightarrow \mathcal{D}^*$ que resuelve la familia de problemas de interpolación $\mathcal{D}$, $\Phi : \mathcal{D} \to \Pi_{N-1}$. Entonces $M \geq N$.*

Demostración: De la definición de algoritmo de interpolación (Definición 6.1), tenemos que para cada $z := (x_1, y_1, \ldots, x_N, y_N)$ en el dominio de Ψ, el polinomio $(\omega^* \circ \Psi)(z)$ es un polinomio univariado asume el valor y_i en cada x_i para $i = 1, \ldots, N$. Sea $\mathcal{U}$ un subconjunto abierto de $\mathcal{D}$ incluído en el dominio de Ψ, y fíjese un elemento $(a_1, b_1, \ldots, a_N, b_N) \in \mathcal{U}$. Escríbase $a := (a_1, \ldots, a_N)$.

Considérese la aplicación polinomial $\varepsilon : \mathbb{C} \to \mathcal{D}$ definida por:

$$\varepsilon(t) := (a_1, F(a_1, t), \ldots, a_N, F(a_N, t)).$$

Entonces $\psi := \Psi \circ \varepsilon$ es una aplicación racional sobre la recta $\mathbb{C}$. Escríbase $\psi := (\psi_1, \ldots, \psi_M)$, con $\psi_j \in \mathbb{C}(T)$, para $j = 1, \ldots, M$. Afirmamos que cada ψ_j es regular en un entorno de $T = \eta$ para cada elemento $\eta \in \mathcal{G}_N$, donde $\mathcal{G}_N \subset \mathbb{C}$ es el conjunto de todas las raíces N–ésimas de la unidad.

Para probar esta afirmación, obsérvese que la hipótesis de robustez implica que Ψ_j es entera sobre el anillo local $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}}$, donde $\mathfrak{M}$ denota el ideal maximal asociado al punto

$(a_1, 0, \ldots, a_N, 0)$. Por lo tanto existe $s \in \mathbb{N}$ y polinomios $P_i, Q_i \in \mathbb{C}[X_1, Y_1, \ldots, X_N, Y_N]$ con $Q_i(a_1, 0, \ldots, a_N, 0) \neq 0$ para $1 \leq i \leq s$ tales que

$$\Psi_j^s + \frac{P_{s-1}}{Q_{s-1}}\Psi_j^{s-1} + \cdots + \frac{P_0}{Q_0} = 0$$

en $\mathbb{C}(\overline{\mathcal{D}})$.

Si escribimos $p_i := P_i \circ \varepsilon$ y $q_i := Q_i \circ \varepsilon$ para $1 \leq i \leq s$, de la identidad anterior obtenemos la siguiente identidad en $\mathbb{C}(T)$:

$$\psi_j^s + \frac{p_{s-1}}{q_{s-1}}\Psi_j^{s-1} + \cdots + \frac{p_0}{q_0} = 0,$$

y ahora las funciones racionales $\frac{p_i}{q_i}$ pertenecen al anillo local $\mathbb{C}[T]_{\mathfrak{N}}$ donde $\mathfrak{N} \subset \mathbb{C}[T]$ es el ideal principal generado por $T - \eta$. Puesto que el anillo $\mathbb{C}[T]_{\mathfrak{N}}$ es integralmente cerrado en su cuerpo de fracciones, tenemos que $\psi_j \in \mathbb{C}[T]_{\mathfrak{N}}$ para todo $j = 1, \ldots, M$. Esto muestra que la aplicación ψ_j es regular en un entorno de η para todo $\eta \in \mathcal{G}_N$ y concluye la demostración de nuestra afirmación.

Ahora considérese la aplicación polinomial $\varphi : \mathcal{D}^* \to \mathbb{C}^N$ definida por

$$\varphi(u) := (\omega^*(u)(a_1), \ldots, \omega^*(u)(a_N)).$$

La composición $\theta := \varphi \circ \Psi \circ \varepsilon : \mathbb{C} \to \mathbb{C}^N$ está definida simplemente por

$$\theta(t) = (F(a_1, t), \ldots, F(a_N, t)),$$

y por lo tanto es regular en un entorno de todo $\eta \in \mathcal{G}_N$. Si $\mathcal{G}_N := \{\eta_1, \ldots, \eta_N\}$, aplicando la Regla de la cadena para cada $\eta_j \in \mathcal{G}_N$, tenemos:

$$\begin{aligned} N\eta_j^{N-1} \begin{pmatrix} \sum_{i=0}^{N-1} \eta_j^i a_1^i \\ \sum_{i=0}^{N-1} \eta_j^i a_2^i \\ \vdots \\ \vdots \\ \sum_{i=0}^{N-1} \eta_j^i a_N^i \end{pmatrix} &= D\theta(\eta_j) \\ &= D\varphi((\Psi \circ \varepsilon)(\eta_j))\ D(\Psi \circ \varepsilon)(\eta_j) \\ &= D\varphi(\Psi(a_1, 0, \ldots, a_N, 0))\ D(\Psi \circ \varepsilon)(\eta_j). \end{aligned} \tag{8.1}$$

Sea $v_j := \frac{1}{N\eta_j^{N-1}} D\theta(\eta_j) \in \mathbb{C}^N$ para cada $j = 1, \ldots, N$. La relación (8.1) implica que todos los vectores v_j pertenecen a la imagen de la matriz Jacobiana $D\varphi(\Psi(a_1, 0, \ldots, a_N, 0))$.

Afirmamos que estos vectores son linealmente independientes. Para probar esta afirmación, denótese por $\mathcal{M}$ la matriz $N \times N$ que tiene los vectores v_j como sus columnas. Tenemos la siguiente descomposición:

$$\mathcal{M} = V(\eta_1, \ldots, \eta_N)^t V(a_1, \ldots, a_N),$$

donde $V(\eta_1,\ldots,\eta_N) := (\eta_i^{j-1})_{1\le i,i\le N}$ es la matriz de Vandermonde asociada al conjunto $\mathcal{G}_N$ de todas las raíces N-ésimas de la unidad, $V(a_1,\ldots,a_N) := (a_i^{j-1})_{1\le i,i\le N}$ es la matriz de Vandermonde asociada a los números complejos $a_1,\ldots,a_N$ (que son distintos de a pares) y ^{t} denota la trasposición. Puesto que ambas matrices del miembro derecho de la última expresión son no singulares, también lo es $\mathcal{M}$.

Como consecuencia de nuestra afirmación, el rango de la matriz $D\varphi(\Psi(a_1,0,\ldots,a_N,0)) \in \mathbb{C}^{N\times M}$ es al menos N y por lo tanto $M \ge N$. Esto concluye la demostración de la proposición. ∎

8.2. Polinomios codificados por sus valores: la reconstrucción es difícil

Con las nociones y notaciones de la Subsección 6.2.4, aquí mostramos que la complejidad de *todo* algoritmo *robusto* de interpolación que reconstruye todos los polinomios multivariados de una complejidad dada mediante una sucesión de identificación es intrínsecamente exponencial.

Teorema 8.3 *Sea $\mathcal{D}^* \subseteq \mathbb{C}^M$ un conjunto construible para el cual existe un algoritmo* robusto *$\omega^* : \mathcal{D}^* \to \mathcal{O}_{L,n}$, $\Psi : \mathcal{D}_{L,n} \dashrightarrow \mathcal{D}^*$ que resuelve la familia de problemas de interpolación $\mathcal{D}_{L,n}$, $\Phi : \mathcal{D}_{L,n} \to \mathcal{O}_{L,n}$ de la Subsección 6.2.4. Entonces se verifica la siguiente desigualdad:*

$$M \ge \binom{2^{\lfloor \frac{L}{2}+1\rfloor} - 1 + n}{n} = 2^{O(Ln)}.$$

Demostración: Sea $\ell := \lfloor \frac{L}{2} + 1\rfloor$ y sea $\mathcal{Y}$ el siguiente subconjunto de Π_{2^L}:

$$\mathcal{Y} := \{t \sum_{i=0}^{2^\ell - 1} (\lambda_1 X_1 + \cdots + \lambda_n X_n)^i ; (t,\lambda_1,\ldots,\lambda_n) \in \mathbb{C}^{n+1}\}.$$

Teniendo en cuenta que la longitud no escalar de cualquier $g \in \mathcal{Y}$ está acotada por $2(\ell-1)$, concluímos que $\mathcal{Y} \subseteq \mathcal{O}_{L,n}$. Denotemos con $\overline{\mathcal{Y}}$ su clausura Zariski en $\mathbb{C}^{N_L}$. Vemos que $\overline{\mathcal{Y}}$ es una subvariedad irreducible de $\overline{\mathcal{O}}_{L,n}$, pues es la clausura Zariski de la imagen bajo un morfismo regular de la variedad irreducible $\mathbb{C}^{n+1}$.

Sea $\mathcal{Z}$ la subvariedad irreducible afín de $\overline{\mathcal{D}}_{L,n}$ definida por $\mathcal{Z} := \Xi(\overline{\mathcal{Y}})$ (nótese que $\mathcal{Z}$ es cerrado Zariski pues $\Xi : \overline{\mathcal{O}}_{L,n} \to \overline{\mathcal{D}}_{L,n}$ es una aplicación polinomial finita). Obsérvese que el punto 0 pertenece a $\mathcal{Z}$.

Sea $\mathcal{U} \subset \mathcal{D}_{L,n}$ un conjunto abierto Zariski no vacío donde las funciones racionales Ψ_j de la aplicación racional Ψ están definidas. Si bien algunas de estas funciones pueden

no estar definidas en $\mathcal{Z}$, la Proposición 7.4 asegura la existencia de funciones racionales $\psi_j \in \mathbb{C}(\mathcal{Z})$ que juegan el rol de restricciones de las Ψ_j a la subvariedad $\mathcal{Z}$.

No asumimos que el punto 0 se halla en el abierto $\mathcal{U}$. Sin embargo, la hipótesis de robustez implica que estas funciones racionales ψ_j verifican ecuaciones de dependencia entera sobre el anillo local $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}}$, donde $\mathfrak{M}$ denota el ideal maximal asociado al punto 0.

Sean $T, U_1, \ldots, U_n$ nuevas indeterminadas, $U := (U_1, \ldots, U_n)$ y sea

$$g_{T,U}(X) := T \sum_{i=0}^{2^\ell - 1} (U_1 X_1 + \cdots + U_n X_n)^i.$$

Los polinomios $f_i := g_{T,U}(\gamma_i) \in \mathbb{C}[T, U]$, $1 \leq i \leq n_L$ inducen las funciones coordenadas de una aplicación polinomial dominante $f : \mathbb{C}^{n+1} \to \mathcal{Z} \subseteq \mathbb{C}^{n_L}$. Sea $f^* : \mathbb{C}(\mathcal{Z}) \to \mathbb{C}(T, U)$ el homomorfismo de cuerpos de funciones racionales inducido por f y para cada índice j sea $\widetilde{\psi}_j$ la función racional en $\mathbb{C}(T, U)$ definida como $\widetilde{\psi}_j := f^*(\psi_j)$ (es decir, $\widetilde{\psi}_j$ es la composición $\psi_j \circ f : \mathbb{C}^{n+1} \dashrightarrow \mathbb{C}$).

Ahora bien, mediante el morfismo f^* podemos identificar:

- el anillo de coordenadas $\mathbb{C}[\mathcal{Z}]$ con $\mathbb{C}[f_1, \ldots, f_{n_L}]$,
- el ideal maximal $\mathfrak{M}$ asociado al punto 0 con el ideal $(f_1, \ldots, f_{n_L})$,
- el cuerpo de fracciones $\mathbb{C}(\mathcal{Z})$ con $\mathbb{C}(f_1, \ldots, f_{n_L})$,
- el anillo local $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}}$ con el anillo $S^{-1}\mathbb{C}[f_1, \ldots, f_{n_L}]$, donde S es el subconjunto multiplicativo de $\mathbb{C}[f_1, \ldots, f_{n_L}]$ definido por

$$S := \{P(f_1, \ldots, f_{n_L}) | P \in \mathbb{C}[Y_1, \ldots, Y_{n_L}], P(0, \ldots, 0) \neq 0\} \subset \mathbb{C}[T, U].$$

De esta manera, podemos considerar a $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}}$ como un subanillo de $S^{-1}\mathbb{C}[T, U]$ y $\mathbb{C}(\mathcal{Z})$ como un subcuerpo de $\mathbb{C}(T, U)$.

En consecuencia, como en particular las funciones racionales ψ_j ($1 \leq j \leq M$) son enteras sobre $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}}$, deducimos que las funciones racionales $\widetilde{\psi}_j$ pertenecen a $S^{-1}\mathbb{C}[T, U]$, que es un anillo integralmente cerrado.

Para cada $u \in \mathbb{C}$ denotemos con $\mathfrak{M}_{(0,u)}$ al ideal maximal asociado al punto $(0, u) \in \mathbb{C}^{n+1}$ en el anillo $\mathbb{C}[T, U]$. De la identidad $f_i(0, U) = g_{0,U}(\gamma_i) = 0$ para $1 \leq k \leq n_L$ y de la definición del conjunto S, deducimos que $S^{-1}\mathbb{C}[T, U]$ es un subanillo del anillo local $\mathbb{C}[T, U]_{\mathfrak{M}_{(0,u)}}$ para todo $u \in \mathbb{C}$. En particular las funciones racionales $\widetilde{\psi}_j$ pertenecen al anillo local $\mathbb{C}[T, U]_{\mathfrak{M}_{(0,u)}}$ para todo $u \in \mathbb{C}$. En otras palabras el punto $(0, u)$ pertenece al dominio de definición de la función racional $\widetilde{\psi}_j$ para todo $u \in \mathbb{C}$.

Sea una ecuación de dependencia entera de $\widetilde{\psi}_j$ sobre $S^{-1}\mathbb{C}[f_1, \ldots, f_{n_L}]$:

$$(\widetilde{\psi}_j)^m + \frac{p_{m-1}}{q_{m-1}}(\widetilde{\psi}_j)^{m-1} + \cdots + \frac{p_0}{q_0} = 0,$$

donde $p_i, q_i \in \mathbb{C}[f_1, \ldots, f_{n_L}]$ y $q_i \in S$. Especializando $T = 0$ los polinomios p_i, q_i resultan números complejos $\widetilde{p}_i$ y $\widetilde{q}_i$ con $\widetilde{q}_i \neq 0$. En consecuencia, de la anterior ecuación de dependencia entera deducimos que la función racional $\widetilde{\psi}_j(0, U)$ satisface una ecuación mónica cuyos coeficientes son números complejos, y por lo tanto

$$\widetilde{\psi}_j(0, U) \in \mathbb{C} \quad \text{para} \;\; 1 \leq j \leq M, \tag{8.2}$$

en otras palabras, las funciones racionales $\widetilde{\psi}_j(0, U)$ no dependen de las variables U.

Sea $\Sigma := \{\alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n; |\alpha| := \alpha_1 + \cdots + \alpha_n \leq 2^L\}$. Obsérvese que Σ consiste de $N_L := \binom{2^L+n}{n}$ elementos. Puesto que todo polinomio de $\mathcal{O}_{L,n}$ tiene grado acotado por 2^L, para cada $\alpha \in \Sigma$ consideraremos la función coordenada θ_α de $\mathbb{C}[\mathcal{O}_{L,n}]$ que, aplicada a $f \in \mathcal{O}_{L,n}$, da el α-ésimo coeficiente de f.

En particular, para cada $g_{t,u} \in \mathcal{Y}$ tenemos

$$\begin{aligned} g_{t,u} &= t \sum_{i=0}^{2^\ell - 1} \sum_{\substack{\alpha \in \mathbb{N}_0^n \\ |\alpha| = i}} \frac{i!}{\alpha_1! \alpha_2! \ldots \alpha_n!} u_1^{\alpha_1} x_1^{\alpha_1} \ldots u_n^{\alpha_n} x_n^{\alpha_n} \\ &= t \sum_{\substack{\alpha \in \mathbb{N}_0^n \\ 0 \leq |\alpha| \leq 2^\ell - 1}} \frac{|\alpha|!}{\alpha_1! \alpha_2! \ldots \alpha_n!} u_1^{\alpha_1} x_1^{\alpha_1} \ldots u_n^{\alpha_n} x_n^{\alpha_n}, \end{aligned}$$

y por lo tanto, $\theta_\alpha(g_{t,u}) = \frac{t|\alpha|!}{\alpha_1! \ldots \alpha_n!} u^\alpha$ para todo $\alpha \in \Sigma$.

Para $\rho \in \mathbb{C}$ fijo definimos la aplicación $\beta_\rho : \mathbb{C} \to \mathbb{C}^{n+1}$ como

$$\beta_\rho(t) := (t, \rho, \rho^{2^\ell}, \rho^{2^{2\ell}}, \ldots, \rho^{2^{(n-1)\ell}}).$$

De los argumentos anteriores se infiere que las $\widetilde{\psi}_j$ son regulares en un entorno de $\beta_\rho(0)$ y por lo tanto la aplicación

$$\sigma_\rho := \omega^* \circ \widetilde{\psi} \circ \beta_\rho,$$

donde $\widetilde{\psi} := (\widetilde{\psi}_1, \ldots, \widetilde{\psi}_M)$, está bien definida y es regular en un entorno de $t = 0$ (recuérdese que ω^* se supone siempre una función polinomial definida en todo el espacio).

Más aun, podemos dar una descripción explícita de σ_ρ en un entorno de $t = 0$ como sigue: sea Δ_ρ un disco en torno de $t = 0$ tal que todas las $\widetilde{\psi}_j$ son regulares en $\beta_\rho(t)$. Para cada $t \in \Delta_\rho$, el punto $f(\beta_\rho(t)) = (g_{t,\rho}(\gamma_1), \ldots, g_{t,\rho}(\gamma_{n_L}))$, siendo $g_{t,\rho} := g_{t,\rho,\rho^{2^\ell},\rho^{2^{2\ell}},\ldots,\rho^{2^{(n-1)\ell}}}$, se halla en $\mathcal{D}_{L,n} \cap \mathcal{Z}$. Combinando la hipótesis de robustez con el Lema 7.5, tenemos la identidad:

$$\omega^* \circ \Psi(f(\beta_\rho(t))) = \Phi \circ \omega(f(\beta_\rho(t))) \tag{8.3}$$

Ahora, para cada $\mathbb{C}$–place $\varphi : \mathbb{C}(T,U) \to \mathbb{C}\cup\{\infty\}$ finito sobre el anillo local $\mathbb{C}[T,U]_{\mathfrak{M}_{\beta_\rho(t)}}$, la composición $\vartheta' := \varphi \circ f^* : \mathbb{C}(\mathcal{Z}) \to \mathbb{C}\cup\{\infty\}$ es un $\mathbb{C}$–place finito sobre el anillo local $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}_{f(\beta_\rho(t))}}$. Como $\widetilde{\psi}_j$ está definida en $\beta_\rho(t)$ deducimos que

$$\vartheta'(\psi_j) = \varphi(f^*(\psi_j)) = \varphi(\widetilde{\psi}_j) = \widetilde{\psi}_j(\beta_\rho(t)). \tag{8.4}$$

Por la Proposición 7.4, para cada j el valor $\Psi_j(f(\beta_\rho(t)))$ es igual a $\vartheta'(\psi_j)$, con lo cual a partir de (8.3) y (8.4) deducimos la identidad:

$$\sigma_\rho(t) = \Phi \circ \omega(f(\beta_\rho(t))), \tag{8.5}$$

y esta última expresión es exactamente la tupla de coeficientes de $g_{t,\rho}$. En suma, tenemos:

$$\sigma_\rho(t) = \left(t\frac{|\alpha|!}{\alpha_1!\ldots\alpha_n!}\rho^{\alpha_1+\cdots+\alpha_n 2^{(n-1)\ell}}; \alpha \in \Sigma \right).$$

Luego, podemos calcular explícitamente la diferencial:

$$d\sigma_\rho(0) = \left(\frac{|\alpha|!}{\alpha_1!\ldots\alpha_n!}\rho^{\alpha_1+\cdots+\alpha_n 2^{(n-1)\ell}}; \alpha \in \Sigma \right) \in \mathbb{C}^{N_L}.$$

Nótese que todos los exponentes de ρ en las coordenadas de $d\sigma_\rho(0)$ son números naturales distintos pues las coordenadas α_i que aparecen en la expresión de arriba son menores o iguales que $2^\ell - 1$. Por otro lado, aplicando la regla de la cadena en el punto $t = 0$, obtenemos:

$$D\sigma_\rho(0) = D\omega^*(\widetilde{\psi} \circ \beta_\rho(0))D(\widetilde{\psi} \circ \beta_\rho)(0).$$

De (8.2) tenemos que $\widetilde{\psi} \circ \beta_\rho(0)$ es un vector complejo independiente de ρ. Por lo tanto concluímos que la matriz $C := D\omega^*(\widetilde{\psi} \circ \beta_\rho(0))$ es una matriz constante (i.e., independiente de ρ) en $\mathbb{C}^{N_L\times M}$. Por lo tanto, puesto que $D\sigma_\rho(0) = CD(\widetilde{\psi} \circ \beta_\rho(0))(0)$ vale para todo $\rho \in \mathbb{C}$, concluímos que el vector $D\sigma_\rho(0)$ pertenece al rango de C para todo $\rho \in \mathbb{C}$.

Por el Lema 8.4 siguiente, deducimos que, para valores $\rho_1, \ldots, \rho_{N_L} \in \mathbb{C}$ adecuados, los vectores $D\sigma_{\rho_i}(0)$ son linealmente independientes y pertenecen al rango de C, lo que implica $M \geq N_L = \binom{2^\ell - 1+n}{n} = \binom{2^{\lfloor \frac{L}{2}+1\rfloor}-1+n}{n}$. Esto concluye la demostración del teorema. ∎

Lema 8.4 *Sean $m \in \mathbb{N}$, $n_1 < n_2 < \cdots < n_m \in \mathbb{N}_0$ y sean $a_1, \ldots, a_m \in \mathbb{C}$ elementos no nulos. Sean $Z_1, \ldots, Z_m$ indeterminadas sobre $\mathbb{C}$ y sea $M := (M_{i,j})_{1\leq i,j\leq m} \in \mathbb{C}[Z_1, \ldots, Z_m]^{m\times m}$ la matriz definida por $M_{i,j} := a_j Z_i^{n_j}$. Entonces* $\det(M) \neq 0$.

En particular, existen elementos $\rho_1, \ldots, \rho_m \in \mathbb{C}$ de norma arbitrariamente pequeña para los cuales la matriz $(a_j\rho_i^{n_j})_{1\leq i,j\leq m}$ es no singular.

Demostración: Argumentamos por inducción en m. Puesto que el enunciado es obvio para $m = 1$, suponemos $m > 1$. Desarrollando el determinante por la última columna de M, vemos que $\det M = a_m Z_1^{n_m} \det Q_1 + \cdots + a_m Z_m^{n_m} \det Q_m$, donde todas las matrices Q_i tienen determinante no nulo, y por su forma particular concluimos que $gr_{Z_j}(Q_i) \leq n_{m-1}$ para $1 \leq i, j \leq m$. En particular, $a_m \det Q_1$ es el coeficiente de la mayor potencia de Z_1 que aparece en $\det M$ y es no nulo. Por lo tanto $\det M$ es no nulo. ∎

Bibliografía

[1] A. Alder, *Grenzrang und Grenzkomplexität aus algebraischer und topologischer sicht*, Ph.D. thesis, Universität Zürich, Philosophische Fakultät II, 1984.

[2] D. Bini and V. Pan, *Polynomial and matrix computations*, Progress in Theoretical Computer Science, Birkhäuser, Boston, 1994.

[3] T. Bloom and J.-P. Calvi, *A continuity property of multivariate Lagrange interpolation*, Math. Comp. **66** (1997), no. 220, 1561–1577.

[4] P. Bürgisser, M. Clausen, and M.A. Shokrollahi, *Algebraic complexity theory*, Grundlehren Math. Wiss., vol. 315, Springer, Berlin, 1997.

[5] A. Cafure and G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. **12** (2006), no. 2, 155–185.

[6] D. Castro, M. Giusti, J. Heintz, G. Matera, and L.M. Pardo, *The hardness of polynomial equation solving*, Found. Comput. Math. **3** (2003), no. 4, 347–420.

[7] D. Cox, J. Little, and D. O'Shea, *Using algebraic geometry*, Grad. Texts in Math., vol. 185, Springer, New York, 1998.

[8] C. de Boor, *On multivariate polynomial interpolation*, Surv. Approx. Theory **1** (2005), 46–69.

[9] C. de Boor and A. Ron, *On multivariate polynomial interpolation*, Constr. Approx. **6** (1990), no. 3, 287–302.

[10] ———, *The least solution for the polynomial interpolation problem*, Math. Z. **210** (1992), no. 3, 347–378.

[11] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Grad. Texts in Math., vol. 150, Springer, New York, 1995.

[12] I. Emiris and B. Mourrain, *Computer algebra methods for studying and computing molecular conformations*, Algorithmica **25** (1999), no. 2-3, 372–402, Special Issue on Algorithms for Computational Biology.

[13] D.K. Faddeev and V.N. Faddeeva, *Computational methods of linear algebra*, Freeman, San Francisco, 1963.

[14] N. Fitchas, M. Giusti, and 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, pp. 247–329.

[15] W. Fulton, *Intersection theory*, Springer, Berlin Heidelberg New York, 1984.

[16] M. Gasca and T. Sauer, *Polynomial interpolation in several variables*, Adv. Comput. Math. **12** (2000), no. 4, 377–410.

[17] M. Gasca and T. Sauer, *On the history of polynomial interpolation*, J. Comput. Appl. Math. **122** (2000), no. 1–2, 23–35.

[18] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, and L.M. Pardo, *Lower bounds for Diophantine approximation*, J. Pure Appl. Algebra **117,118** (1997), 277–317.

[19] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, and L.M. Pardo, *Straight–line programs in geometric elimination theory*, J. Pure Appl. Algebra **124** (1998), 101–146.

[20] M. Giusti, J. Heintz, J.E. Morais, and L.M. Pardo, *When polynomial equation systems can be solved fast?*, Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings AAECC-11 (Berlin) (G. Cohen, M. Giusti, and T. Mora, eds.), Lecture Notes in Comput. Sci., vol. 948, Springer, 1995, pp. 205–231.

[21] M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity **17** (2001), no. 1, 154–211.

[22] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci. **24** (1983), no. 3, 239–277.

[23] J. Heintz, G. Matera, and A. Waissbein, *On the time–space complexity of geometric elimination procedures*, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 4, 239–296.

[24] J. Heintz and C. P. Schnorr, *Testing polynomials which are easy to compute*, International Symposium on Logic and Algorithmic, Zurich 1980, Monogr. Enseig. Math., vol. 30, 1982, pp. 237–254.

[25] T. Krick and L.M. Pardo, *A computational method for Diophantine approximation*, Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94 (Boston) (L. González-Vega and T. Recio, eds.), Progr. Math., vol. 143, Birkhäuser Boston, 1996, pp. 193–254.

[26] L. Kronecker, *Über Einige Interpolationsformeln für Ganze Functionen Mehrer Variabeln*, Monatsberichte der Königlich Preussischen Akademie der Wissenschafften zu Berlin vom Jahre 1865, 686–691.

[27] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser, Boston, 1985.

[28] S. Lang, *Algebra*, third ed., Addison–Wesley, Reading, Massachusetts, 1993.

[29] H.M. Möller and T. Sauer, *H-bases for polynomial interpolation and system solving*, Adv. Comput. Math. **12** (2000), no. 4, 335–362.

[30] P. Olver, *On multivariate interpolation*, Stud. Appl. Math. **116** (2006), no. 2, 201–240.

[31] L.M. Pardo, *How lower and upper complexity bounds meet in elimination theory*, Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC–11 (Berlin) (G. Cohen, M. Giusti, and T. Mora, eds.), Lecture Notes in Comput. Sci., vol. 948, Springer, 1995, pp. 33–69.

[32] J. Sabia and P. Solernó, *Bounds for traces in complete intersections and degrees in the Nullstellensatz*, Appl. Algebra Engrg. Comm. Comput. **6** (1996), no. 6, 353–376.

[33] T. Sauer, *Gröbner basis, h–bases and interpolation*, Trans. Amer. Math. Soc. **353** (2001), no. 6, 2293–2308.

[34] J.T. Schwartz, *Probabilistic algorithms for verification of polynomial identities*, EUROSAM '79: Proceedings of International Symposium on Symbolic and Algebraic Computation, Marseille 1979 (Berlin), Lecture Notes in Comput. Sci., vol. 72, Springer, 1979, pp. 200–215.

[35] I.R. Shafarevich, *Basic algebraic geometry*, Springer, Berlin Heidelberg, 1974.

[36] I.R. Shafarevich. *Basic Algebraic Geometry: Varieties in Projective Space*, Springer, Berlin Heidelberg New York, 1994.

[37] W. Vogel, *Results on Bézout's theorem*, Tata Inst. Fundam. Res. Lect. Math., vol. 74, Tata Inst. Fund. Res., Bombay, 1984.

[38] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge Univ. Press, Cambridge, 1999.

[39] O. Zariski and P. Samuel, *Commutative algebra II*, Grad. Texts in Math., vol. 39, Springer, New York, 1960.

[40] R. Zippel, *Probabilistic algorithms for sparse polynomials*, EUROSAM '79: Proceedings of International Symposium on Symbolic and Algebraic Computation, Marseille 1979 (Berlin), Lecture Notes in Comput. Sci., vol. 72, Springer, 1979, pp. 216–226.