Tesis de Posgrado

Descomposición equidimensional efectiva de variedades algebraicas

Talí Jerónimo, Gabriela

2002

Tesis presentada para obtener el grado de Doctor en Ciencias Matemáticas de la Universidad de Buenos Aires

UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales

Departamento de Matemática

Descomposición equidimensional efectiva de variedades algebraicas

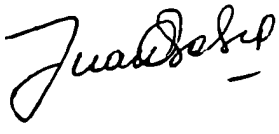
por Gabriela Talí Jeronimo

Director de Tesis: Dr. Juan V. R. Sabia

Lugar de Trabajo: Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, UBA

Trabajo de Tesis para optar por el título de
Doctora en Ciencias Matemáticas

Diciembre de 2001



Descomposición equidimensional efectiva de variedades algebraicas

Resumen

Presentamos algoritmos para el cálculo de la descomposición equidimensional de una variedad algebraica afín a partir de un conjunto finito de polinomios que la define:
En primer lugar, se prueba la existencia de un algoritmo determinístico no uniforme que calcula en tiempo polinomial una descripción de la componente equidimensional de dimensión máxima de una variedad algebraica. Aplicando este algoritmo se obtiene un procedimiento para decidir si una variedad es equidimensional o no. A continuación, se construye un algoritmo probabilístico que da en tiempo polinomial, para cada componente equidimensional de una variedad dada, un conjunto finito de polinomios que la define. Para terminar, se desarrolla otro algoritmo probabilístico, que calcula la forma de Chow de cada una de las componentes equidimensionales de una variedad. La cota para la complejidad de este algoritmo también es –en el peor caso– polinomial en el tamaño del input. Sin embargo, bajo ciertas condiciones genéricas, puede darse una cota para su complejidad secuencial en términos del grado geométrico del sistema de polinomios que define la variedad y, por lo tanto, puede ser de orden muy inferior.

Palabras clave: Sistemas de ecuaciones polinomiales, algoritmos, complejidad, variedades *equidimensionales*, descomposición equidimensional, forma de Chow.

Effective equidimensional decomposition of algebraic varieties

Abstract

We present algorithms for the computation of the equidimensional decomposition of an affine algebraic variety from a finite set of polynomials defining it:
First, we prove the existence of a non-uniform deterministic algorithm which computes a description of the equidimensional component of maximal dimension of an algebraic variety in polynomial time. Applying this algorithm we obtain a procedure to determine whether a variety is equidimensional or not. Then, we construct a probabilistic algorithm which gives a finite set of polynomials defining each equidimensional component of a given variety in polynomial time. Finally, another probabilistic algorithm is developed. It computes the Chow form of each equidimensional component of a variety. The complexity bound for this algorithm –in the worst case– is also polynomial in the input size. However, under certain genericity conditions, a complexity estimate in terms of the geometric degree of the polynomial system defining the variety can be given and, therefore, it may result in a much lower complexity order.

Key words: Polynomial equation systems, algorithms, complexity, equidimensional varieties, equidimensional decomposition, Chow form.

Agradecimientos

A mi director de Tesis, Juan Sabia, por sus enseñanzas, su dedicación y su ayuda permanente, sin las cuales no hubiera sido posible el desarrollo de este trabajo.

A Joos Heintz, por sus valiosos consejos y sugerencias.

A Susana Puddu, por su ayuda en el Capítulo 2, y a Teresa Krick y Martín Sombra, por su colaboración en la obtención de los resultados que se presentan en el Capítulo 4.

A mi familia y a mis amigos que me alentaron y me dieron su apoyo.

Índice

Introducción **5**

1 Preliminares **12**

1.1 Definiciones y notación 12

1.1.1 Nociones básicas 12

1.1.2 Variedades algebraicas 13

1.2 Modelo algorítmico 16

1.2.1 Noción de algoritmo 16

1.2.2 Codificación de polinomios 18

1.3 Manejo de straight-line programs 20

1.3.1 Tests de nulidad 20

1.3.2 Algoritmos básicos con straight-line programs 22

1.4 Algunas herramientas algorítmicas 32

1.4.1 Cálculo de la dimensión de una variedad algebraica 32

1.4.2 Eliminación de cuantificadores 36

1.4.3 Método de Newton 40

2 Forma de Chow. Algoritmos determinísticos **46**

2.1 Forma de Chow de una variedad proyectiva 46

2.2 Resultados conocidos acerca del cálculo de la forma de Chow 50

2.3 Resultados obtenidos 51

2.3.1 Cálculo de una forma de Chow de la componente equidimensional de V de dimensión $\dim V$ 51

2.3.2 Cálculo de la componente equidimensional de V de mayor dimensión 62

2.3.3 El caso afín 64

3 Descomposición equidimensional efectiva **69**

3.1 Descomposición de variedades algebraicas 69

3.2 Resultados obtenidos 70

3.3 Preprocesamiento de los datos 71

3.3.1 Modificación de los polinomios de entrada 71

3.3.2 Posición de Noether de las variables 73

3.4 Descomposición equidimensional 75

3.4.1 Descripción de variedades equidimensionales 75

3.4.2 Cambio del cuerpo de base 77

3.4.3 Resultado principal 78

4 Cálculo de formas de Chow **94**

4.1 Forma de Chow de una variedad afín equidimensional 94

4.1.1 Definición 94

4.1.2 Normalización de formas de Chow 96

4.2 Un caso fundamental 97

4.2.1 Enunciado del resultado 97

4.2.2 Una fórmula multiplicativa para la forma de Chow 99

4.2.3 La forma de Chow como un cociente de dos series 104

4.2.4 La forma de Chow como un cociente de dos polinomios 112

4.2.5 Demostración del resultado principal 119

4.3 Forma de Chow de cada componente equidimensional de una variedad afín 124

4.3.1 Formas de Chow generalizadas y polinomios característicos . . 124

4.3.2 Preparación del input 135

4.3.3 Algunas herramientas 146

4.3.4 El algoritmo 156

4.4 Complejidad y grado geométrico 169

4.4.1 Grado geométrico de un sistema de polinomios 170

4.4.2 Cotas de complejidad que dependen del grado geométrico . . . 174

Referencias **178**

Introducción

Muchos problemas que surgen en diversas ramas de la ciencia y la tecnología están relacionados con sistemas de ecuaciones polinomiales. Algunos de estos problemas pueden resolverse simplemente determinando si el sistema de ecuaciones polinomiales asociado es consistente (es decir, si las ecuaciones tienen una solución en común).

Si $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ son polinomios en n variables con coeficientes en un cuerpo k, el Teorema de los Ceros de Hilbert establece que el sistema de ecuaciones $f_1(x) = 0, \ldots, f_s(x) = 0$ es inconsistente en $\bar{k}^n$ (donde $\bar{k}$ denota una clausura algebraica de k) si y sólo si existen polinomio $g_1, \ldots, g_s \in k[X_1, \ldots, X_n]$ tales que

$$1 = \sum_{i=1}^{s} g_i f_i.$$

Este enunciado establece solamente la *existencia* de polinomios $g_1, \ldots, g_s$ que verifican la igualdad anterior. Más aún, las demostraciones usuales del mismo no dan información sobre los polinomios $g_1, \ldots, g_s$. Desde el punto de vista de la efectividad, surgió entonces la cuestión de dar cotas de grados para los polinomios $g_1, \ldots, g_s$. Un resultado de este tipo permitiría traducir el problema de la consistencia de un sistema de ecuaciones polinomiales arbitrario en un problema de álgebra lineal: la consistencia del sistema lineal obtenido al considerar en la igualdad anterior los coeficientes de los polinomios $g_1, \ldots, g_s$ como incógnitas.

Esta situación fue considerada en primer lugar por G. Hermann [21] quien, utilizando teoría de eliminación, dio una cota -doblemente exponencial en la cantidad de variables- para los grados de los polinomios $g_1, \ldots, g_s$. A partir de ese momento, se han dado distintas versiones efectivas del Teorema de los Ceros de Hilbert, que constituyeron sucesivas mejoras a la cota de Hermann. Entre ellas podemos mencionar los trabajos de J. Kollár [23] y de Noaï Fitchas y A. Galligo [9] en los cuales se prueba una cota simplemente exponencial (esencialmente óptima).

En el caso de problemas que involucran sistemas de ecuaciones polinomiales que son consistentes, puede ser necesario dar una descripción del conjunto de sus soluciones, es decir, de la variedad algebraica definida por los polinomios en cuestión.

Un resultado conocido establece que toda variedad algebraica V sobre un cuerpo algebraicamente cerrado puede descomponerse unívocamente como unión (finita) de variedades algebraicas irreducibles $C_1, \ldots, C_t$ tales que $C_i \not\subset C_j$ para $i \neq j$. Una forma de describir la variedad V es entonces caracterizando cada una de sus componentes irreducibles. Sin embargo, aún en el caso más simple de una variedad en un espacio de dimensión 1, el problema de obtener una descripción de este tipo está íntimamente relacionado con la factorización de polinomios cuya resolución, desde el punto de vista algorítmico, suele ser demasiado costosa.

Uno de los invariantes asociados a una variedad algebraica es su dimensión. Si todas las componentes irreducibles de una variedad algebraica tienen la misma dimensión, la variedad se llama equidimensional. Una variedad algebraica V afín o proyectiva arbitraria puede tener componentes irreducibles de distintas dimensiones, pero siempre puede descomponerse como una unión de variedades equidimensionales: si r es la dimensión de V,

$$V = \bigcup_{\ell=0}^{r} V_\ell$$

donde, para cada $0 \leq \ell \leq r$, V_ℓ es o bien vacía o bien la unión de las componentes irreducibles de V de dimensión ℓ. Esta descomposición se llama la descomposición equidimensional de V y las variedades V_ℓ $(0 \leq \ell \leq r)$ se llaman las componentes equidimensionales de V. Esto provee otra manera posible de describir la variedad V: caracterizando cada una de sus componentes equidimensionales.

El problema es entonces, dados polinomios $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ que definen una variedad algebraica V, obtener una descripción de cada una de las componentes equidimensionales de V.

Entre los primeros algoritmos construidos que calculan la descomposición equidimensional de una variedad podemos mencionar el de A. Chistov y D. Grigor'ev (ver [4]) y el que presentan M. Giusti y J. Heintz en [12]. En ambos casos, si la variedad está dada como el conjunto de los ceros comunes de s polinomios en n variables de grados acotados por d, la complejidad del algoritmo es de orden $s^{O(1)}d^{O(n^2)}$.

El siguiente objetivo era obtener algoritmos que resuelvan el mismo problema con complejidad polinomial en el tamaño del input, es decir, de orden $s^{O(1)}d^{O(n)}$.

Los algoritmos de descomposición equidimensional manipulan principalmente polinomios en varias variables que, en el caso de los algoritmos mencionados, son codificados en forma densa, es decir, como el vector de todos sus coeficientes en un orden preestablecido de los monomios. Esto ocasiona un problema desde el punto de vista de la complejidad, debido a la gran cantidad de coeficientes que posee cada uno de los polinomios que aparecen como resultados intermedios o como output del algoritmo.

Se planteó entonces la posibilidad de cambiar esta forma de codificar a los polinomios por otra estructura de datos: los *straight-line programs*, que son programas que, utilizando solamente las operaciones aritméticas de suma, resta y producto, permiten evaluar al polinomio codificado en cualquier punto.

Esta estructura de datos ya había sido utilizada con éxito en la construcción de algoritmos para resolver diversos problemas de Geometría Algebraica y Álgebra Conmutativa, por ejemplo, para la caracterización de los puntos aislados de una variedad algebraica (ver [13]), para el cálculo de los polinomios que dan la escritura del 1 en el Teorema de los Ceros de Hilbert (ver [15]) y para el problema general de la eliminación de cuantificadores (ver [29]), entre otros.

En este trabajo se construyen algoritmos que, dada una variedad algebraica como el conjunto de los ceros comunes de un sistema finito de polinomios con coeficientes en un cuerpo efectivo k de característica 0, resuelven el problema del cálculo de la descomposición equidimensional de la variedad con cotas de complejidad polinomiales en el tamaño del input.

Hay distintas maneras de describir las componentes equidimensionales de una variedad algebraica. Una de ellas, es por medio de un conjunto finito de polinomios que la define. Otra forma de describir una variedad equidimensional es por medio de su *forma de Chow*. La forma de Chow de una variedad equidimensional V de dimensión r definida sobre un cuerpo k, es un polinomio en varias variables con coeficientes en k que (salvo factores escalares) está unívocamente determinado por la variedad. Este polinomio caracteriza las variedades lineales de codimensión menor o igual que $r+1$ que intersecan a V. Esta propiedad, a su vez, permite caracterizar completamente la variedad equidimensional V a partir de su forma de Chow.

En vista de esto, en la primera parte de este trabajo se considera el problema del cálculo algorítmico de la forma de Chow de una variedad proyectiva equidimensional

y su aplicación para el cálculo de componentes equidimensionales de una variedad afín o proyectiva.

El primero de estos problemas ya había sido estudiado por L. Caniglia que da en [3] un algoritmo que calcula la forma de Chow en el caso equidimensional, por M. Giusti y J. Heintz, que presentan en [12] un algoritmo para el caso general, y por S. Puddu y J. Sabia, quienes dan en [29] un algoritmo que calcula formas de Chow de variedades irreducibles. En todos estos algoritmos las complejidades son de orden mayor o igual que $s^{O(1)}d^{O(n^2)}$.

En el Capítulo 2 de este trabajo se presenta un algoritmo que calcula la forma de Chow de la componente equidimensional de dimensión máxima de una variedad algebraica proyectiva arbitraria a partir de un sistema finito de polinomios que define la variedad. Si la variedad está dada como el conjunto de los ceros comunes de s polinomios homogéneos en $n+1$ variables de grados acotados por $d \geq n$, la complejidad del algoritmo es de orden $s^{O(1)}d^{O(n)}$. El algoritmo se basa en el algoritmo de eliminación de cuantificadores de [29] para fórmulas de primer orden con un solo bloque de cuantificadores existenciales. En particular, el algoritmo resuelve el problema del cálculo de la forma de Chow de una variedad proyectiva equidimensional sin necesidad de información adicional (es decir, sin necesidad de saber de antemano que la variedad es equidimensional) y con complejidades menores que las de los algoritmos conocidos que realizan la misma tarea ([3], [12], [29]).

Utilizando este algoritmo se muestra cómo, dada una variedad V afín o proyectiva como el conjunto de ceros de una familia finita de polinomios, puede obtenerse un conjunto finito de ecuaciones que define la componente equidimensional de V de dimensión máxima con cotas de complejidad de orden $s^{O(1)}d^{O(n)}$. Finalmente, como aplicación de este segundo algoritmo, se muestra un procedimiento que permite decidir en tiempo secuencial del mismo orden, si una variedad dada es equidimensional o no. En todos los casos, las complejidades de los algoritmos construidos son esencialmente mejores que las de los otros algoritmos conocidos para resolver los mismos problemas.

Cabe destacar que los algoritmos presentados en el Capítulo 2 son *determinísticos*, es decir, producen la solución exacta del problema para todas las posibles instancias, y *no uniformes* en el sentido que su construcción depende de cierto preprocesamiento cuyo costo no está considerado en las cotas de complejidad exhibidas.

El Capítulo 3 se centra en el problema del cálculo algorítmico de la descomposición equidimensional de una variedad. Más precisamente: dados polinomios $f_1, \ldots, f_s$ en $k[X_1, \ldots, X_n]$ que definen una variedad algebraica V, se considera el problema de obtener, para cada $0 \leq \ell \leq \dim V$, un conjunto finito de polinomios en $k[X_1, \ldots, X_n]$ cuyo conjunto de ceros comunes sea la componente equidimensional de V de dimensión ℓ.

La iteración del algoritmo exhibido en el Capítulo 2 para el cálculo de las componentes equidimensionales de dimensión no maximal de una variedad algebraica, produce cotas de complejidad que no son polinomiales en el tamaño del input. Teniendo en cuenta esto, el problema de hallar todas las componentes equidimensionales de una variedad ya no fue encarado dentro del contexto de la eliminación de cuantificadores.

Se construye un algoritmo *probabilístico* –funciona bajo ciertas condiciones genéricas que dependen de parámetros que se eligen aleatoriamente– que calcula la descomposición equidimensional de V. Con las hipótesis y notación anteriores, si los grados de los polinomios $f_1, \ldots, f_s$, cuyo conjunto de ceros comunes es la variedad V, están acotados por un entero $d \geq n$, el algoritmo calcula en tiempo polinomial en sd^n (tamaño del conjunto input), para cada $0 \leq \ell \leq \dim V$, un conjunto de $n+1$ polinomios que define la componente equidimensional de dimensión ℓ de V.

Mediante un preprocesamiento de los datos de entrada (que se efectúa aleatoriamente), se suponen buenas condiciones de intersección y posición de Noether de las variables con respecto a ciertas variedades involucradas en el proceso. Esto permite pasar de situaciones de dimensión positiva a problemas cero-dimensionales. El proceso se basa entonces en el algoritmo de [13] aplicado a variedades cero-dimensionales convenientemente elegidas.

El algoritmo diseñado caracteriza *todos* los puntos de cada componente equidimensional de la variedad y las cotas de complejidad del algoritmo son menores que las de los otros algoritmos que resuelven el mismo problema.

Otro algoritmo probabilístico para el cálculo de la descomposición equidimensional de una variedad algebraica fue presentado por G. Lecerf en [27]. La complejidad del algoritmo construido por Lecerf –que fue desarrollado simultánea e independientemente de los que se presentan en esta tesis– también es, en el peor caso, polinomial en el tamaño del input. Sin embargo, este algoritmo no caracteriza todos los puntos de cada componente equidimensional de la variedad, sino que describe de manera paramétrica un abierto denso de cada una de ellas.

Habiéndose obtenido un algoritmo que resuelve el problema del cálculo de la descomposición equidimensional en tiempo polinomial en el tamaño del input, el siguiente paso natural consiste en el diseño de un algoritmo cuya medida de complejidad tenga en cuenta el aspecto geométrico del problema considerado, es decir, que dependa no sólo de parámetros de carácter sintáctico (grado y cantidad de polinomios de entrada, cantidad de variables) sino también de invariantes intrínsecos (geométricos). Esto se debe a que se ha observado que en diversos problemas de Geometría Algebraica hay muchas instancias particulares que, desde el punto de vista algorítmico, pueden resolverse más fácilmente que el caso general. Esta observación motivó la introducción de parámetros asociados al sistema de polinomios que identifiquen estos casos particulares y el diseño de algoritmos que distingan (a nivel complejidad) estas instancias del problema.

En el Capítulo 4 se construye un algoritmo probabilístico que calcula la forma de Chow de cada una de las componentes equidimensionales de una variedad algebraica afín arbitraria a partir de un conjunto finito de polinomios que la define, cuya complejidad puede medirse en términos de la complejidad del input y de un invariante relacionado más intrínsecamente con el problema considerado: el *grado geométrico* del sistema de polinomios de entrada. Teniendo en cuenta que la forma de Chow caracteriza completamente la variedad equidimensional a la que está asociada, este algoritmo provee una forma alternativa de dar la descomposición equidimensional de una variedad algebraica arbitraria.

El algoritmo se basa en un resultado auxiliar que permite calcular la forma de Chow de una variedad afín equidimensional V bajo ciertas hipótesis (que valen genéricamente) a partir de un conjunto finito de polinomios que define la variedad y una resolución geométrica de una fibra cero-dimensional de V por una proyección: Si V es una variedad equidimensional de dimensión r y grado D definida en un espacio n-dimensional por $n-r$ polinomios de grados acotados por d dados por un straight-line program de longitud L, el subalgoritmo produce un straight-line program para la forma de Chow de V con complejidad $(n\,d\,D)^{O(1)}L$. Esta subrutina es determinística. Está basada en una fórmula multiplicativa que permite expresar la forma de Chow como un cociente de dos series de potencias, las cuales son aproximadas por medio de la aplicación simbólica del algoritmo de Newton (ver [11]).

En forma análoga al caso del algoritmo presentado en el Capítulo 3, el algoritmo diseñado para el cálculo de las formas de Chow de todas las componentes equidimensionales de una variedad depende de un preprocesamiento de los datos de entrada que

se realiza aleatoriamente. Este preprocesamiento permite la aplicación recursiva de la subrutina anterior para el cálculo de las formas de Chow de una descomposición equidimensional no minimal de la variedad, de la que finalmente se obtienen las formas de Chow de las componentes equidimensionales.

Si todos los parámetros aleatorios elegidos durante la ejecución del algoritmo satisfacen las condiciones de genericidad apropiadas (lo que sucede con alta probabilidad) el algoritmo finaliza su ejecución produciendo una respuesta correcta en tiempo secuencial acotado por $s(n\,d\,\delta)^{O(1)}L$ donde δ es el grado geométrico del sistema de polinomios $f_1,\ldots,f_s \in k[X_1,\ldots,X_n]$ de entrada (noción que se define generalizando la definición dada en [14]), d es una cota superior para los grados de estos polinomios y L es la longitud del straight-line program dado como representación de los polinomios.

La complejidad del algoritmo construido es, en el peor caso, del mismo orden que la de los algoritmos que no dependen de parámetros intrínsecos, pero en el caso de sistemas polinomiales con ciertas propiedades geométricas particulares el tiempo necesario para la ejecución del algoritmo es sustancialmente menor.

Capítulo 1

Preliminares

1.1 Definiciones y notación

1.1.1 Nociones básicas

Sea k un cuerpo de característica 0. Supondremos que k es efectivo: es decir, que las operaciones aritméticas (adición, sustracción, multiplicación y división) y las comparaciones entre elementos de k son realizables por medio de algoritmos.

Sean $X_1, \ldots, X_n$ indeterminadas sobre k y sea $f \in k[X_1, \ldots, X_n]$ un polinomio. El grado total de f será denotado por $\deg f$. Diremos que f es mónico en la variable X_n si, considerado como polinomio en la variable X_n con coeficientes en $k[X_1, \ldots, X_{n-1}]$, su coeficiente principal es 1; y diremos que es mónico salvo por un factor constante si su coeficiente principal es un elemento de k.

Si $f \in k[X_1, \ldots, X_n]$, $\mathrm{rad}(f)$ denotará un polinomio en $k[X_1, \ldots, X_n]$ libre de cuadrados cuyos ceros son exactamente los ceros de f. En el caso en que $n = 1$, $\mathrm{rad}(f)$ será considerado mónico.

Dados polinomios $g_1, \ldots, g_s \in k[X_1, \ldots, X_n]$, $\gcd(g_1, \ldots, g_s)$ denotará un máximo común divisor de los polinomios $g_1, \ldots, g_s$. En el caso $n = 1$, $\gcd(g_1, \ldots, g_s)$ denotará el máximo común divisor mónico de los polinomios.

Sea $\bar{k}$ una clausura algebraica de k. Denotaremos por $\mathbb{A}^n(\bar{k})$ (o $\mathbb{A}^n$) y $\mathbb{P}^n(\bar{k})$ (o $\mathbb{P}^n$) a los espacios n-dimensionales afín y proyectivo sobre $\bar{k}$ respectivamente. Si K es un subcuerpo de $\bar{k}$, diremos que un subconjunto $V \subseteq \mathbb{A}^n$ es una *variedad algebraica afín definible sobre* K o una *K-variedad* si V es el conjunto de los ceros comunes en $\mathbb{A}^n$ de una familia de polinomios en $K[X_1, \ldots, X_n]$.

Puesto que mediante uniones finitas e intersecciones arbitrarias de K-variedades se obtienen nuevamente K-variedades, se pueden considerar las K-variedades como los conjuntos cerrados de una topología en $\mathbb{A}^n$, que se llama la *topología de Zariski de* $\mathbb{A}^n$ *respecto de* K.

En forma análoga se define una *K-variedad proyectiva* como el conjunto de los ceros comunes en $\mathbb{P}^n$ de una familia de polinomios homogéneos en $K[X_0, \ldots, X_n]$, y el conjunto de las K-variedades en $\mathbb{P}^n$ induce la *topología de Zariski de P^n respecto de K*. Cuando se considere $K = \bar{k}$, diremos simplemente *la* topología de Zariski de $\mathbb{A}^n$ o $\mathbb{P}^n$.

Si $S \subseteq \mathbb{A}^n$ (o $S \subseteq \mathbb{P}^n$), denotaremos por $\overline{S}$ a la clausura de S con respecto a la topología de Zariski de $\mathbb{A}^n$ (o $\mathbb{P}^n$ respectivamente).

Para cada $I \subset k[X_1, \ldots, X_n]$, denotaremos por $V(I)$ a la variedad afín de $\mathbb{A}^n(\bar{k})$ formada por los ceros comunes de los polinomios que pertenecen a I. Dados polinomios $f_1, \ldots, f_s$, la variedad $V(\{f_1, \ldots, f_s\}) \subseteq \mathbb{A}^n$ será llamada la variedad *definida por* $f_1, \ldots, f_s$ y será notada por $V(f_1, \ldots, f_s)$.

Si V es una variedad afín en $\mathbb{A}^n(\bar{k})$, denotaremos por $I(V)$ al ideal de $\bar{k}[X_1, \ldots, X_n]$ formado por todos los polinomios que se anulan sobre V. De la misma manera, si $V \subseteq \mathbb{P}^n$ es una variedad proyectiva, $I(V)$ denotará el ideal homogéneo de todos los polinomios de $\bar{k}[X_0, \ldots, X_n]$ que se anulan sobre V.

Diremos que una propiedad se verifica para $x \in \mathbb{A}^n$ (o $\mathbb{P}^n$) *genérico* o simplemente que se verifica *genéricamente* si existe un abierto de Zariski $U \subseteq \mathbb{A}^n$ no vacío (respectivamente $U \subseteq \mathbb{P}^n$) tal que la propiedad vale para todo $x \in U$.

1.1.2 Variedades algebraicas

Las variedades algebraicas son los objetos básicos involucrados en los distintos problemas que se tratarán en este trabajo. A continuación damos algunas definiciones y propiedades sobre variedades algebraicas que nos serán de utilidad. Para más detalles ver por ejemplo [32], [26] o [16].

Nociones geométricas elementales

Uno de los parámetros más importantes asociados a una variedad algebraica es su dimensión.

Sea $V \subseteq \mathbb{A}^n$ una variedad algebraica afín. Se define la *dimensión de* V, que será denotada por $\dim V$, como la dimensión de Krull de $\bar{k}[V] := \bar{k}[X_1, \ldots, X_n]/I(V)$, el anillo de coordenadas de V: es decir, $\dim V$ es el máximo entero r tal que existe una cadena de ideales primos $\mathcal{P}_0 \subsetneq \mathcal{P}_1 \subsetneq \ldots \subsetneq \mathcal{P}_r$ de $\bar{k}[V]$ de longitud $r+1$. Análogamente, para una variedad proyectiva $V \subseteq \mathbb{P}^n$ puede considerarse el anillo graduado asociado a la variedad definido por $\bar{k}[V] := \bar{k}[X_0, \ldots, X_n]/I(V)$. Entonces la dimensión proyectiva de V puede definirse como $\dim V = \dim_{\text{Krull}} \bar{k}[V] - 1$.

Es un hecho conocido que la dimensión de una variedad algebraica afín o proyectiva V es el entero r tal que una variedad lineal genérica en $\mathbb{A}^n$ (respectivamente en $\mathbb{P}^n$) de codimensión r interseca a V en un número finito de puntos. Observamos que una variedad lineal de codimensión r es la intersección de r hiperplanos y puede representarse entonces por medio de un elemento en $\mathbb{A}^{r\times(n+1)}$ (cada fila representa los coeficientes de una ecuación de uno de los hiperplanos), y en este sentido hablamos de genericidad.

Una K-variedad algebraica V se dice *irreducible* si verifica la siguiente propiedad: si para dos K-variedades V_1 y V_2 vale $V = V_1 \cup V_2$, entonces $V = V_1$ o $V = V_2$.

Para una K-variedad algebraica afín arbitraria $V \subseteq \mathbb{A}^n$, existe una única representación $V = \bigcup_{i=1}^{t} C_i$, donde, para cada $1 \leq i \leq t$, C_i es una K-variedad irreducible de $\mathbb{A}^n$, y $C_i \not\subseteq C_j$ para $i \neq j$. Llamaremos a esta representación, unívocamente determinada por V, la *descomposición irreducible (minimal) de* V y a las variedades C_i $(1 \leq i \leq t)$ las *componentes irreducibles* de V.

Si $r = \dim V$, llamaremos la *descomposición equidimensional de* V a la representación $V = \bigcup_{\ell=0}^{r} V_\ell$ donde, para cada $0 \leq \ell \leq r$, V_ℓ es o bien el conjunto vacío o bien la unión de todas las componentes irreducibles de V de dimensión ℓ.

De la misma manera se definen las componentes irreducibles y equidimensionales en el caso de una variedad proyectiva.

Diremos que las variables $X_1, \ldots, X_n$ están en *posición de Noether con respecto a la variedad* V definida sobre k si el morfismo canónico

$$k[X_1, \ldots, X_r] \to k[X_1, \ldots, X_n]/I(V),$$

donde $r = \dim V$ e $I(V)$ es el ideal de todos los polinomios de $k[X_1, \ldots, X_n]$ que se anulan sobre V, es un monomorfismo entero. En otras palabras, la proyección $\pi : V \to \mathbb{A}^r$ sobre las primeras r coordenadas es un morfismo finito de variedades

afines. Observamos que, si la variedad V es equidimensional (es decir, todas las componentes irreducibles de V tienen la misma dimensión) y las variables están en posición de Noether con respecto a V, entonces están en posición de Noether con respecto a cada componente irreducible de V.

Otro de los parámetros intrínsecos asociados a una variedad algebraica es su *grado*. La noción de grado de una variedad se define en primer lugar para el caso de una variedad afín irreducible y luego se extiende al caso general.
Si $V \subseteq \mathbb{A}^n$ es una variedad algebrica afín irreducible de dimensión r, el *grado* de V es

$$\begin{aligned}\deg V := \sup \{ \#H_1 \cap \ldots \cap H_r \cap V \ ; \ H_1, \ldots, H_r \text{ hiperplanos afines} \\ \text{en } \mathbb{A}^n \text{ tales que } H_1 \cap \ldots \cap H_r \cap V \text{ es un conjunto finito } \}.\end{aligned}$$

Este supremo es finito (ver [17]).

Para una variedad algebraica afín arbitraria $V \subseteq \mathbb{A}^n$, se define $\deg V$ como la suma de los grados de todas las componentes irreducibles de V.

Con esta definición de grado, vale la siguiente propiedad (ver [17]):

Desigualdad de Bézout. *Sean $X, Y \subseteq \mathbb{A}^n$ dos variedades algebraicas. Entonces*

$$\deg(X \cap Y) \leq \deg X . \deg Y$$

El concepto de grado puede extenderse al caso proyectivo: Si $V \subseteq \mathbb{P}^n$ es una variedad proyectiva irreducible, el grado de V es la cantidad de puntos en la intersección de V con una subvariedad lineal genérica de $\mathbb{P}^n$ de codimensión igual a la dimensión de V. Para una variedad proyectiva arbitraria el grado es, nuevamente, la suma de los grados de sus componentes irreducibles. Al igual que en el caso afín, vale la desigualdad de Bézout.

Variedades algebraicas cero-dimensionales

En el caso de variedades algebraicas de dimensión cero, una forma de describir la variedad, muy importante desde el punto de vista algorítmico, está dada por la noción de *resolución geométrica* que introducimos a continuación.

Sea $Z \subseteq \mathbb{A}^n(\overline{k})$ una variedad cero-dimensional de grado D definida sobre k. Una *resolución geométrica de Z* se define como una forma lineal $\ell = u_1 X_1 + \cdots + u_n X_n \in$

$k[X_1, \ldots, X_n]$ junto con $n+1$ polinomios univariados $p, v_1, \ldots, v_n \in k[T]$ que satisfacen las siguientes condiciones:

- La forma lineal ℓ separa los puntos de Z, es decir, si $\xi \neq \xi' \in Z$, entonces $\ell(\xi) \neq \ell(\xi')$.
- El polinomio p es el polinomio minimal (mónico) de ℓ con respecto a Z, es decir,
$$I(Z) \cap k[\ell] = (p(\ell)).$$
- Los polinomios $v_1, \ldots, v_n$ verifican la condición $\deg v_i < D$ $(1 \leq i \leq n)$ y dan la parametrización de los puntos de Z por los ceros de p, más precisamente,
$$Z = \left\{(v_1(\eta), \ldots, v_n(\eta)) : \eta \in \overline{k},\ p(\eta) = 0\right\}.$$

Diremos que la resolución geométrica de Z *está dada* cuando están dados el vector de coeficientes de ℓ y los vectores de coeficientes de los polinomios p y $v_1, \ldots, v_n$.

Los polinomios $p, v_1, \ldots, v_n \in k[T]$ están unívocamente determinados por la variedad Z y la forma lineal ℓ.

1.2 Modelo algorítmico

1.2.1 Noción de algoritmo

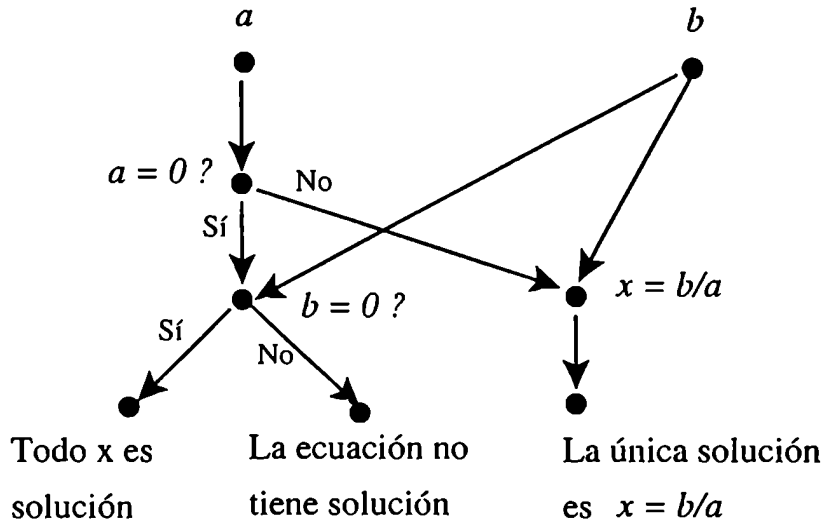
Los algoritmos que se exhiben en este trabajo serán descriptos por medio de familias de redes aritméticas con entradas en el cuerpo de base k. Una red aritmética se representa mediante un grafo orientado acíclico: los nodos externos representan la entrada y la salida de la red; a cada nodo interno le corresponde la ejecución de una operación elemental, y cada rama indica el envío de la salida del resultado de la operación correspondiente al primero de los nodos involucrados para que sirva como entrada para el segundo. Las operaciones elementales a las que corresponden los nodos internos son las siguientes: elección de un elemento fijo de k, operaciones aritméticas entre elementos de k (adición, sustracción, multiplicación y división), comparaciones entre elementos de k seguidas por un selector y operaciones booleanas.

La *complejidad secuencial* de un algoritmo se define como el tamaño de la red, es decir, la cantidad de nodos de su grafo asociado sin tener en cuenta los nodos

de entrada. Esta noción de complejidad, que corresponde a considerar que cada operación o comparación tiene costo unitario, provee una primera estimación del tiempo necesario para la ejecución del algoritmo.

En las estimaciones de la complejidad secuencial de los algoritmos presentados utilizaremos la siguiente notación: si C y $\tilde{C}$ son funciones de $\mathbb{N}$ en $\mathbb{N}$, escribiremos $C(n) = O(\tilde{C}(n))$ si existe una constante $c_0 > 0$ (independiente de n) tal que $C(n) \leq c_0 \tilde{C}(n)$ para todo $n \in \mathbb{N}$.

El siguiente grafo representa un algoritmo que, dados escalares a y b, resuelve la ecuación $a.x = b$:



Esencialmente trabajaremos con dos tipos de algoritmos:

- Algoritmos que producen siempre la solución exacta del problema considerado para todas las posibles instancias, a los que llamaremos algoritmos *determinísticos.*

  El modelo que ya hemos descripto corresponde a esta clase de algoritmos.

- Algoritmos que producen el resultado correcto bajo ciertas condiciones genéricas que dependen de parámetros, los cuales no pueden ser seleccionados determinísticamente sin provocar un aumento demasiado grande de la complejidad. Se supone dado entonces un proceso aleatorio para seleccionar elementos de un subconjunto fijo del cuerpo de base k, el cual se utiliza para elegir los valores

de los parámetros involucrados. Estos valores no necesariamente satisfacen las condiciones requeridas, con lo cual el algoritmo puede producir una respuesta errónea o finalizar su ejecución sin haber obtenido una respuesta para el problema (devuelve "error" porque no puede efectuar la siguiente operación), pero la probabilidad de que esto suceda es baja. En estos casos hablaremos de algoritmos *probabilísticos*.

Este tipo de algoritmos se representan mediante grafos en forma análoga a lo explicado anteriormente: la única modificación al modelo anterior consiste en agregar nodos para representar cada una de las elecciones aleatorias efectuadas durante el algoritmo. Estos nodos no serán tenidos en cuenta para el cálculo de la complejidad.

1.2.2 Codificación de polinomios

Un aspecto importante a tener en cuenta en la construcción de un algoritmo es la estructura de datos utilizada, es decir, la manera de representar los objetos con los que trabaja el algoritmo. En nuestro caso surge la necesidad de codificar los polinomios que aparecen como entrada, salida o resultados intermedios de los algoritmos.

En los algoritmos que se presentan en este trabajo, los polinomios en varias variables serán codificados de alguna de las siguientes maneras:

- *Forma densa*, es decir, representados por el vector de todos sus coeficientes (aún los nulos) en un orden preestablecido de los monomios.

Consideremos por ejemplo, el polinomio $f = (X+1)^{2^d}$ y el orden en los monomios dado por el orden creciente de las potencias de X. Observamos que la codificación de este polinomio en forma densa está dada por el vector de $2^d + 1$ coordenadas

$$\left(1, 2^d, \ldots, \binom{2^d}{k}, \ldots, 2^d, 1\right)$$

Sin embargo, este polinomio puede ser evaluado en sólo $d+1$ pasos: dado x, se calcula la suma $x+1$ y luego se eleva el resultado al cuadrado d veces. Obtenemos así otra manera de codificar el polinomio f: dando un algoritmo que permite calcular $f(x)$ para cada x.

La situación que hemos visto en el ejemplo anterior dio lugar al uso de otra estructura de datos para codificar polinomios: Dado un polinomio $f \in k[X_1, \ldots, X_n]$ se lo

representa por medio de un algoritmo (con ciertas propiedades) que permite calcular $f(x)$ para cada $x \in k^n$. Esto se formaliza con la noción de

- *Straight-line programs*, que son circuitos aritméticos (redes sin ramas), que no contienen ni selectores ni operaciones booleanas.

  Más precisamente: Denotemos por $+, -, \cdot$ a las operaciones de suma, resta y multiplicación en $k[X_1, \ldots, X_n]$. Consideraremos también, para cada $\lambda \in k$, la suma $+_\lambda$ y la multiplicación $\cdot_\lambda$ definidas, para cada $f \in k[X_1, \ldots, X_n]$, como $+_\lambda(f) = f + \lambda$ y $\cdot_\lambda(f) = \lambda \cdot f$.

  Un straight-line program sin divisiones en $k[X_1, \ldots, X_n]$ es una secuencia de instrucciones $\gamma = (\gamma_1, \ldots, \gamma_L)$ de la forma

$$\gamma_i = \begin{cases} (\omega_i; k_1^{(i)}, k_2^{(i)}) & \text{si } \omega_i \in \{+, -, \cdot\} \\ (\omega_i; k^{(i)}) & \text{si } \omega_i \in \{+_\lambda, \cdot_\lambda : \lambda \in k\} \end{cases}$$

  donde, para cada $1 \leq i \leq L$, $k_1^{(i)}$ y $k_2^{(i)}$ (o $k^{(i)}$) son enteros que verifican $-n+1 \leq k_1^{(i)}, k_2^{(i)} \leq i-1$.

  Llamaremos *longitud* del straight-line program γ a la cantidad L de instrucciones de γ.

  Dado un straight-line program $\gamma = (\gamma_1, \ldots, \gamma_L)$ se define la *sucesión de resultados de* γ como

$$f_{-n+1} := X_1, \ldots, f_0 := X_n$$

$$f_i := \begin{cases} \omega_i(f_{k_1^{(i)}}, f_{k_2^{(i)}}) & \text{si } \omega_i \in \{+, -, \cdot\} \\ \omega_i(f_{k^{(i)}}) & \text{si } \omega_i \in \{+_\lambda, \cdot_\lambda : \lambda \in k\} \end{cases}$$

  Diremos que el straight-line program γ calcula (o representa) un polinomio $f \in k[X_1, \ldots, X_n]$ si f es alguno de los polinomios de la sucesión de resultados de γ. (En general será $f = f_L$).

Observamos que un straight-line program representa, en efecto, un procedimiento para evaluar el polinomio que codifica.

Para una definición más precisa y propiedades elementales de la noción de straight-line program ver [18] o [19].

Volviendo al ejemplo, un posible straight-line program para $f = (X+1)^{2^d}$ en $k[X]$, que corresponde a la forma que hemos descripto antes para evaluar f, es $\gamma = (\gamma_1, \ldots, \gamma_{d+1})$ donde

$$\begin{aligned} \gamma_1 &:= (+_1 \,;\, 0) \\ \gamma_i &:= (\cdot \,;\, i-1, i-1) \qquad i = 2, \ldots, d+1 \end{aligned}$$

y la sucesión de resultados de este straight-line program es

$$(X,\, X+1, (X+1)^2, \ldots, (X+1)^{2^i}, \ldots, (X+1)^{2^d}).$$

Observamos que, mientras que para representar este polinomio en forma densa se necesita un vector de 2^d+1 coordenadas, el polinomio puede codificarse por medio de un straight-line program de longitud $d+1$, que está dado por un vector de $O(d+1)$ coordenadas.

Cabe destacar que la codificación de polinomios mediante straight-line programs permite en muchos casos una disminución en la complejidad de los algoritmos, debido a que ciertos polinomios que aparecen en las aplicaciones pueden ser evaluados con una cantidad de operaciones que es de orden considerablemente menor que la cantidad de coeficientes del polinomio (como sucede en el ejemplo que hemos mostrado).

Finalmente, en algunas ocasiones nos será conveniente combinar la representación de polinomios en forma densa y straight-line programs. Utilizaremos entonces la

- *Representación mixta*, es decir, codificando al polinomio en forma densa con respecto a algunas variables distinguidas y dando sus coeficientes, que son polinomios en las restantes, por medio de un straight-line program.

1.3 Manejo de straight-line programs

1.3.1 Tests de nulidad

Un problema que surge al trabajar con polinomios codificados mediante straight-line programs es el de la verificación de identidades polinomiales o, equivalentemente, dado un straight-line program que representa un polinomio $f \in k[X_1, \ldots, X_n]$, determinar si f es el polinomio nulo.

Si bien es posible obtener todos los coeficientes de f a partir del straight-line program que lo representa y determinar si son cero o no, este procedimiento puede dar lugar a un aumento excesivo en la complejidad.

Se busca entonces un método alternativo que permita resolver este problema.

En el caso de polinomios en una variable, si $f \in k[X]$ tiene grado acotado por d, para decidir si f es el polinomio nulo o no, basta evaluarlo en $d+1$ puntos distintos: f es el polinomio nulo si y sólo si el valor obtenido en todos los casos es cero.

En el caso multivariado aplicaremos un método análogo al anterior, que consiste en evaluar el polinomio en una sucesión adecuada de puntos con coordenadas en k. El cardinal de esta sucesión será polinomial en la longitud del straight-line program que evalúa el polinomio y la cantidad de variables, lo cual permite mantener acotada la complejidad del algoritmo. La existencia de tales sucesiones, a las que llamaremos *sucesiones de prueba* (*correct test sequences*), está asegurada por el siguiente resultado:

Lema 1.3.1 *([19, Theorem 4.4]) Sea $W(D,n,L)$ el conjunto de los polinomios de $k[X_1,\ldots,X_n]$ de grado menor o igual que D que pueden ser evaluados por medio de un straight-line program de longitud a lo sumo L. Sea Γ un subconjunto de k de cardinal $2L(1+D)^2$. Entonces existe un subconjunto $Q(D,n,L,\Gamma) = \{\gamma_1,\ldots,\gamma_m\}$ de Γ^n, donde $m = 6(L+n)(L+n+1)$, que verifica: todo polinomio de $W(D,n,L)$ que se anula sobre $\{\gamma_1,\ldots,\gamma_m\}$ es el polinomio nulo.*

Aunque la elección de estas sucesiones de puntos podría hacerse algorítmicamente, el costo de hacer esto excedería la clase de complejidad considerada en este trabajo. Sin embargo, para parámetros de entrada fijos (cantidad de indeterminadas, cantidad y grados de los polinomios involucrados), esta elección es independiente del problema. Por lo tanto, se supondrá que las sucesiones de prueba están dadas por un preprocesamiento cuyo costo no será considerado en las cotas de complejidad obtenidas. En este sentido diremos que los algoritmos son no-uniformes: su construcción depende de un preprocesamiento cuyo costo excede la complejidad de la ejecución del algoritmo en cuestión.

En los algoritmos probabilísticos que se presentarán, será necesario elegir valores de algunos parámetros para que satisfagan ciertas condiciones genéricas que determinan el buen funcionamiento del algoritmo. En cada caso la condición genérica está dada por la no anulación de un polinomio $f \in k[X_1,\ldots,X_n] - \{0\}$ de grado acotado. La

elección de los valores de los parámetros se hará aleatoriamente de un subconjunto fijo de k suficientemente grande, de manera que la probabilidad de que al evaluar f en los valores escogidos el resultado dé cero, sea chica.
Para estimar las probabilidades de éxito de nuestros cálculos se utilizará el siguiente resultado:

Lema 1.3.2 *([31, Lemma 1]) Sea E un dominio íntegro y sea $R \subset E$ un conjunto finito. Sea f un polinomio no nulo en $E[X_1, \ldots, X_n]$. Entonces, para $a_1, \ldots, a_n \in R$ elegidos aleatoriamente, se tiene que*

$$\text{Prob}(f(a_1, \ldots, a_n) = 0) \leq \frac{\deg(f)}{\text{card}(R)}.$$

El resultado anterior se utilizará también para decidir probabilísticamente si un polinomio dado es el polinomio nulo o no.

1.3.2 Algoritmos básicos con straight-line programs

En los algoritmos descriptos en este trabajo se utilizarán como subrutinas distintos algoritmos auxiliares que permiten trabajar con polinomios representados mediante straight-line programs. Estas subrutinas son:

- Cálculo de los coeficientes de un polinomio con respecto a una (o un grupo) de sus variables.
- Cálculo de las componentes homogéneas de un polinomio.
- Cálculo de un straight-line program (sin divisiones) para el cociente exacto entre dos polinomios.
- Cálculo del máximo común divisor entre dos polinomios.
- Cálculo del radical de un polinomio.

Coeficientes de un polinomio con respecto a una variable

El siguiente lema nos permitirá efectuar cambios de codificación en los resultados intermedios de nuestros algoritmos: a partir de un straight-line program que evalúa un polinomio f, calcula un straight-line program para los coeficientes de f con respecto a una variable. Iterando este procedimiento se puede obtener la escritura en forma densa de un polinomio respecto de un subconjunto cualquiera de sus variables.

Lema 1.3.3 *Sea $f \in k[X_1, \ldots, X_n, Y]$ un polinomio dado por medio de un straight-line program de longitud L, y sea d el grado de f con respecto a la variable Y. Entonces existe un straight-line program de longitud $O(d^4 L)$ que calcula todos los coeficientes de f con respecto a la variable Y.*

Demostración. Sea $f = a_d(X_1, \ldots, X_n)\, Y^d + \cdots + a_0(X_1, \ldots, X_n)$. Para calcular los coeficientes $a_d, \ldots, a_0$ de f, se aplica un proceso de interpolación con respecto a la variable Y: se especializa Y en $d+1$ puntos distintos $\alpha_o, \ldots, \alpha_d$ para obtener $\beta_i(X_1, \ldots, X_n) := f(X_1, \ldots, X_n, \alpha_i)$ $(0 \leq i \leq d)$, y se resuelve el sistema lineal

$$\begin{pmatrix} 1 & \alpha_0 & \alpha_0^d \\ & & \vdots \\ 1 & \alpha_d & \alpha_d^d \end{pmatrix} \begin{pmatrix} a_0 \\ \\ a_d \end{pmatrix} = \begin{pmatrix} \beta_0(X_1, \ldots, X_n) \\ \\ \beta_d(X_1, \ldots, X_n) \end{pmatrix}.$$

La solución del sistema es el vector $(a_0(X_1, \ldots, X_n), \ldots, a_d(X_1, \ldots, X_n))$ de los coeficientes de f con respecto a la variable Y.

Desde el punto de vista algorítmico, aplicando por ejemplo el algoritmo descripto en [1], se calcula con $O(d^4)$ operaciones, el vector de coeficientes del polinomio característico de la matriz de Vandermonde que aparece, y luego se calcula su inversa usando el teorema de Cayley-Hamilton.

Finalmente, se obtiene un straight-line program que evalúa los coeficientes de f con respecto a la variable Y, a partir del algoritmo subyacente a la multiplicación de la matriz calculada por el vector de resultados: Si $A = (A_{ij}) \in k^{(d+1)\times(d+1)}$ es la inversa de la matriz de Vandermonde, entonces

$$a_i(X_1, \ldots, X_n) = \sum_{j=0}^{d} A_{ij}\, \beta_j(X_1, \ldots, X_n)$$

y el straight-line program que evalúa a_i $(0 \leq i \leq d)$ se obtiene de la igualdad anterior y los straight-line programs que calculan las entradas A_{ij} de A y los polinomios $\beta_j(X_1, \ldots, X_n)$ $(0 \leq j \leq n)$.

La longitud del straight-line program obtenido es de orden $O(d^4 L)$.

Componentes homogéneas de grados acotados

Otra herramienta que se utilizará en distintas etapas de los algoritmos construidos es el siguiente lema que construye un straight-line program para cada una de las

componentes homogéneas hasta grado prefijado de un polinomio.

Lema 1.3.4 *Sea $f \in k[X_1, \ldots, X_n]$ un polinomio calculable por medio de un straight-line program de longitud L, y sea $d \in \mathbb{N}$. Entonces existe un straight-line program de longitud $O(d^2 L)$ que calcula todas las componentes homogéneas de f de grados acotados por d.*

Demostración. Sean $h_1, \ldots, h_L$ los polinomios que calcula el straight-line program que evalúa f. Modificaremos el straight-line program input de manera que el nuevo straight-line program calcule todas las componentes homogéneas de grados acotados por d de cada uno de los polinomios intermedios $h_1, \ldots, h_L$, en particular del polinomio f.

Denotemos por $h^{(r)}$ la componente homogénea de grado r de un polinomio h dado. Supongamos calculadas todas las componentes homogéneas de grados acotados por d de los polinomios $h_1, \ldots, h_{k-1}$. Se tiene que $h_k = h_i * h_j$ con $* \in \{+, -, \cdot\}$ e $i, j < k$. Entonces si $* = +$ o $* = -$, se tiene que

$$h_k^{(r)} = h_i^{(r)} * h_j^{(r)} \qquad 0 \leq r \leq d$$

con lo cual se calculan todas las componentes homogéneas de h_k de grado acotado por d agregando $d+1$ operaciones al straight-line program obtenido hasta el momento. En el caso en que $* = \cdot$ se tiene, para cada $0 \leq r \leq d$,

$$h_k^{(r)} = \sum_{s+t=r} h_i^{(s)} h_j^{(t)},$$

de donde cada componente homogénea se puede calcular agregando $r+1$ sumas y $r+1$ productos. Por lo tanto, para calcular todas las componentes homogéneas de h_k hasta grado d basta agregar $\sum_{r \leq d+1} 2(r+1) \leq (d+2)^2$ operaciones.

La longitud del straight-line program que se obtiene finalmente para el cálculo de las componentes homogéneas de f de grados acotados por d, está acotada por $(d+2)^2 L$.

□

Elusión de divisiones

El siguiente resultado, debido a Strassen [33] y conocido como *Vermeidung von Divisionen* (elusión de divisiones) muestra cómo reemplazar en un straight-line program una división exacta de polinomios por sumas y productos.

Lema 1.3.5 *Sean $f, g \in k[X_1, \ldots, X_n]$ dos polinomios tales que g divide a f en $k[X_1, \ldots, X_n]$. Supongamos que f y g se pueden calcular por medio de un straight-line program sin divisiones de longitud L, y que se conoce un punto $\xi \in k^n$ tal que $g(\xi) \neq 0$. Entonces, si $\deg(f/g) = d$, existe un straight-line program de longitud $O(d^3\, L)$, sin divisiones en $k[X_1, \ldots, X_n]$, que calcula el polinomio f/g.*

Demostración. Sea $h := f/g$.

Analicemos en primer lugar el caso en que $g(0) = 1$. Consideremos a g como elemento del anillo de series formales $k[[X]] = k[[X_1, \ldots, X_n]]$. Escribimos $g = 1 - g_1$, donde g_1 pertenece al ideal $(X_1, \ldots, X_n) \in k[[X]]$.

Entonces $1/g = \sum\limits_{k \geq 0} g_1^k$ en $k[[X]]$, es decir,

$$h = f \Big(\sum_{k \geq 0} g_1^k \Big).$$

Como $\deg h = d$ y $g_1^k \in (X_1, \ldots, X_n)^k$ para cada $k \in \mathbb{N}_0$, para calcular h basta calcular $\tilde{g} := \sum\limits_{0 \leq k \leq d} g_1^k$, efectuar el producto $\tilde{h} := f\, \tilde{g}$ y truncar el resultado en orden d.

La longitud del nuevo straight-line program se obtiene observando lo siguiente: en primer lugar, se calcula g_1 en longitud $L + 1$, luego se calculan las potencias g_1^k, $2 \leq k \leq d$, lo que agrega $d - 1$ pasos, y se obtiene $\tilde{g}$ sumando todas estas potencias, lo que requiere d pasos adicionales. Finalmente se efectúa el producto de f y $\tilde{g}$. Se tiene entonces un straight-line program que calcula $\tilde{h}$ cuya longitud es $L + 1 + 2\, d$.

A continuación se aplica el Lema 1.3.4 para calcular todas las componentes homogéneas de grado acotado por d del polinomio $\tilde{h}$ en $(d + 2)^2\, (L + 1 + 2\, d)$ pasos, y se las suma con d operaciones más, obteniéndose de este modo el polinomio h.

La longitud final del straight-line program es de orden $O(d^3\, L)$.

Para el caso general en que $g(\xi) \neq 0$, sea $\hat{g} := g(\xi)^{-1}\, g(X + \xi)$, que satisface $\hat{g}(0) = 1$. Aplicando el procedimiento del caso anterior, se calcula un straight-line program sin divisiones que evalúa $f(X + \xi)/\hat{g}(X) = g(\xi)\, h(X + \xi)$. Especializándolo en $(X - \xi)$ y dividiendo el resultado por $g(\xi)$ se obtiene el straight-line program para h. Esto no modifica el orden de la longitud del straight-line program.

Máximo común divisor de polinomios

En primer lugar, mostraremos un algoritmo para el cálculo del máximo común divisor de dos polinomios en una variable basado en subresultantes (ver [5, 2]).

Lema 1.3.6 *Sea $R = k[X_1, \ldots, X_n]$ y sea K el cuerpo de fracciones de R. Sean $f, g \in R[Y]$ dos polinomios de grados acotados por d en la variable Y, dados en forma densa en la variable Y y cuyos coeficientes, que son polinomios en $k[X_1, \ldots, X_n]$, tienen grados acotados por D y están representados por medio de un straight-line program de longitud L. Entonces existe un algoritmo de complejidad secuencial de orden $O(d^{13}(n+L)^3)$ que produce un un straight-line program de longitud $O(d^4 + L)$ que calcula los coeficientes de un máximo común divisor de f y g en $K[Y]$. Estos coeficientes son polinomios en $k[X_1, \ldots, X_n]$ de grados acotados por $2dD$.*

Demostración. El primer paso del algoritmo consiste en la determinación de los grados de f y g: Para esto basta evaluar los coeficientes de f y g en una sucesión de prueba apropiada, que tendrá cardinal $6(L+n)(L+n+1)$ y comparar con cero los resultados obtenidos. Luego, este paso puede realizarse con complejidad secuencial de orden $O((L+n)^2(L+2d+2))$.

Sean $d_1 = \deg_Y f$ y $d_2 = \deg_Y g$. Entonces

$$f = f_{d_1} Y^{d_1} + \cdots + f_0 \quad \text{y} \quad g = g_{d_2} Y^{d_2} + \cdots + g_0$$

y, por hipótesis, $0 \leq d_1, d_2 \leq d$.

Para cada $0 \leq i \leq \max\{d_1, d_2\}$, se considera la submatriz cuadrada S_i (de tamaño $d_1 + d_2 - 2i$) de la matriz de Sylvester de f y g, que consiste de las primeras $d_2 - i$ columnas de coeficientes de f, las primeras $d_1 - i$ columnas de coeficientes de g y las primeras $d_1 + d_2 - 2i$ filas.

A partir de los coeficientes de f y g se obtiene, para cada $0 \leq i \leq \max\{d_1, d_2\}$, un straight-line program de longitud acotada por $O(d^4 + L)$ para $\det(S_i)$ utilizando el algoritmo de Berkowitz. Este paso requiere $O(d^5)$ operaciones adicionales.

El mínimo valor k tal que $\det(S_k) \neq 0$ es el grado del máximo común divisor de f y g en $K[X]$. Este grado puede determinarse especializando, para cada $0 \leq i \leq \max\{d_1, d_2\}$, el straight-line program obtenido para $\det(S_i)$ en una sucesión de prueba, cuyo tamaño será de orden $O((d^4 + L + n)^2)$. Luego, la complejidad secuencial de este paso está acotada por $O(d(d^4 + L)(d^4 + L + n)^2)$.

Luego se calcula la última columna $(a_{d_2-k-1}, \ldots, a_0, b_{d_1-k-1}, \ldots, b_0)$ de la matriz adjunta de la matriz S_k. Esto puede efectuarse a partir del polinomio característico de S_k con complejidad de orden $O(d^4)$. Se obtiene un straight-line program de longitud $O(d^4 + L)$ para las entradas de la última columna de $\mathrm{adj}(S_k)$, que son polinomios de grados acotados por $(2d-1)D$.

El polinomio

$$S := (a_{d_2-k-1}\, Y^{d_2-k-1} + \cdots + a_0)\, f + (b_{d_1-k-1}\, Y^{d_1-k-1} + \cdots + b_0)\, g \in R[Y]$$

es un máximo común divisor de f y g en $K[Y]$. Sus coeficientes son polinomios de grados acotados por $2dD$ que pueden calcularse por medio de un straight-line program de longitud $O(d^4+L)$. Este último paso no modifica el orden de la complejidad del algoritmo.

La complejidad total del algoritmo está acotada por $O(d^{13}(n+L)^3)$.

□

Observación 1.3.7 Con las mismas técnicas utilizadas en la demostración del Lema 1.3.6, se construye un algoritmo que calcula el máximo común divisor de s polinomios de grados acotados por d en una variable con coeficientes en $k[X_1, \ldots, X_n]$, a partir de un straight-line program de longitud L que evalúa sus coeficientes. La complejidad de este algoritmo es de orden $(sdnL)^{O(1)}$ y produce un straight-line program de longitud $O((sd)^5 + L)$ para los coeficientes de un máximo común divisor de los polinomios input.

A continuación enunciamos y demostramos una variante del algoritmo probabilístico de Kaltofen para el cálculo del máximo común divisor de dos polinomios en varias variables dados por straight-line programs (ver [22]), que se obtiene a partir del algoritmo presentado en el lema anterior para el caso de polinomios en una variable.

Lema 1.3.8 *Sean $f, g \in k[X_1, \ldots, X_n]$ polinomios de grados acotados por d calculables por medio de un straight-line program de longitud L. Entonces, existe un algoritmo probabilístico de complejidad $d^{O(1)}\,(n+L)$ que calcula un straight-line program de longitud de orden $d^{O(1)}\,(n+L)$ para un máximo común divisor de f y g. Si los parámetros aleatorios se eligen de un subconjunto de N elementos de k, la probabilidad de éxito del algoritmo (es decir, la probabilidad de que el straight-line program obtenido sea en efecto un máximo común divisor de f y g) es al menos $1 - \frac{2d(d+1)}{N}$.*

Demostración. El primer paso del algoritmo consiste en efectuar un cambio lineal de variables con el objeto de obtener polinomios del mismo grado que los originales, pero que sean mónicos con respecto a alguna variable:

Si F y G denotan las componentes homogéneas de máximo grado de f y g respectivamente, la condición $(FG)(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$ implica que los polinomios

$$\begin{aligned} \tilde{f}(Y_1, \ldots, Y_n) &:= f(Y_1 + \lambda_1 Y_n, \ldots, Y_{n-1} + \lambda_{n-1} Y_n, Y_n) \\ \tilde{g}(Y_1, \ldots, Y_n) &:= g(Y_1 + \lambda_1 Y_n, \ldots, Y_{n-1} + \lambda_{n-1} Y_n, Y_n) \end{aligned}$$

son mónicos (salvo por un factor escalar) con respecto a la variable Y_n y de grados iguales a los grados totales de f y g respectivamente.

Entonces, eligiendo al azar $\lambda_1, \ldots, \lambda_{n-1}$ de un subconjunto de N elementos de k y efectuando el cambio de variables $X_n = Y_n$ y $X_i = Y_i + \lambda_i Y_n$ para $1 \leq i \leq n-1$, los polinomios $\tilde{f}$ y $\tilde{g}$ obtenidos son mónicos en la variable Y_n con probabilidad al menos $1 - \frac{\deg f + \deg g}{N}$. A partir del straight-line program de longitud L que evalúa f y g se obtiene un straight-line program de longitud $2(n-1) + L$ para $\tilde{f}$ and $\tilde{g}$.

Ahora se aplica el Lema 1.3.3 para obtener straight-line programs para los coeficientes de $\tilde{f}$ y $\tilde{g}$ con respecto a la variable Y_n: esto agrega $O(d^4(n+L))$ pasos.

A continuación se determinan los grados d_1 y d_2 de $\tilde{f}$ y $\tilde{g}$ respectivamente, en la variable Y_n: se especializan los straight-line programs para los coeficientes de $\tilde{f}$ y $\tilde{g}$ con respecto a Y_n en cualquier $(n-1)$-upla $\xi = (\xi_1, \ldots, \xi_{n-1})$ y se toma el máximo término no nulo obtenido en cada caso. Observemos que si los polinomios $\tilde{f}$ y $\tilde{g}$ son mónicos, los números hallados son efectivamente los grados de dichos polinomios.

Finalmente, se calcula un máximo común divisor de

$$\tilde{f} = f_{d_1} Y_n^{d_1} + \cdots + f_0 \quad \text{y} \quad \tilde{g} = g_{d_2} Y_n^{d_2} + \cdots + g_0$$

con respecto a la variable Y_n utilizando subresultantes, en forma análoga a lo hecho en el Lema 1.3.6.

Observamos que el grado del máximo común divisor puede calcularse probabilísticamente especializando los straight-line programs obtenidos para los determinantes $\det(S_i)$ $(0 \leq i \leq \max\{d_1, d_2\})$ de las submatrices de la matriz de Sylvester de $\tilde{f}$ y $\tilde{g}$ en un punto elegido al azar $\mu := (\mu_1, \ldots, \mu_{n-1})$. Puesto que para cada $0 \leq i \leq \max\{d_1, d_2\}$, $\deg(\det(S_i)) \leq \deg f\,(\deg g - i) + \deg g\,(\deg f - i) \leq 2 \deg f \deg g$, concluimos que si las coordenadas de μ se eligen al azar de un subconjunto de k con N elementos, la probabilidad de hallar el grado correcto es al menos $1 - \frac{2 \deg f \deg g}{N}$.

El polinomio $S \in k[Y_1, \ldots, Y_{n-1}][Y_n]$ calculado por el algoritmo es un máximo común divisor de $\tilde{f}$ y $\tilde{g}$ en $k[Y_1, \ldots, Y_n]$ multiplicado por $\det(S_k)$.
Se aplica entonces el Lema 1.3.5 a S y $\det(S_k)$ para obtener un straight-line program que calcula $\gcd(\tilde{f}, \tilde{g})$.
La complejidad de estos pasos está acotada por $d^{O(1)}(n + L)$.

Para terminar, se realiza el cambio de variables $Y_n = X_n$ y $Y_i = X_i - \lambda_i X_n$ para $1 \leq i \leq n-1$ con el objeto de obtener el máximo común divisor de f y g buscado.

La complejidad del algoritmo probabilístico y la longitud del straight-line program obtenido para el máximo común divisor de f y g son ambas de orden $d^{O(1)}(n + L)$.
La probabilidad de éxito del algoritmo es al menos

$$\begin{aligned}\Big(1 - \frac{\deg f + \deg g}{N}\Big)\Big(1 - \frac{2 \deg f \deg g}{N}\Big) &\geq 1 - \frac{1}{N}\big(\deg f + \deg g + 2 \deg f \deg g\big) \\ &\geq 1 - \frac{2\,d\,(d+1)}{N}.\end{aligned}$$

□

Observación 1.3.9 El algoritmo probabilístico construido en el Lema anterior puede ser transformado en un algoritmo determinístico de complejidad secuencial de orden $(d(n + L))^{O(1)}$ reemplazando las elecciones aleatorias por la utilización de sucesiones de prueba:

Elección del cambio de variables y determinación del grado de los polinomios f y g: Se calculan todas las componentes homogéneas de f y g de grados acotados por d mediante un straight-line program de longitud $O(d^2 L)$ (ver Lema 1.3.4). Se busca, para cada uno de los polinomios, la componente homogénea no nula de grado más alto evaluando los straight-line programs obtenidos en una sucesión de prueba apropiada. El cardinal de dicha sucesión de prueba es de orden $O(d^4 L^2 + d^2 n L + n^2)$. En consecuencia, se determina las componentes homogéneas F y G de grado máximo de f y g respectivamente con complejidad de orden $O(d^6 L^3 + d^4 n L^2 + n^2 d^2 L)$.
Finalmente se hallan $\lambda_1, \ldots, \lambda_{n-1} \in k$ tales que $(F.G)(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$ evaluando el polinomio no nulo $(F.G)(X_1, \ldots, X_{n-1}, 1)$ en una sucesión de prueba, cuyo tamaño es del mismo orden que el de la sucesión de prueba del paso anterior. Esto no cambia el orden de la complejidad.

Determinación del grado de $\gcd(f, g)$: Procediendo como en la demostración del Lema 1.3.6 se obtiene, para cada $0 \leq i \leq \max\{\deg f, \deg g\}$, un straight-line program de longitud $O(d^4(n + L))$ que calcula $\det(S_i)$. Para determinar el mínimo

k tal que $\det(S_k) \neq 0$, basta evaluar cada uno de estos straight-line programs en una sucesión de prueba apropiada, cuyo tamaño será de orden $O(d^8(n+L)^2)$. La complejidad de este paso es de orden $O(d^{13}(n+L)^3)$.

Radical de un polinomio

Del Lema 1.3.6 se deduce inmediatamente el siguiente resultado sobre el cálculo del radical de un polinomio en una variable:

Lema 1.3.10 *Sea $R = k[X_1, \ldots, X_n]$ y sea $f \in R[Y]$ un polinomio de grado acotado por d en la variable Y y cuyos coeficientes son polinomios de grado acotado por D representados por medio de un straight-line program de longitud L. Entonces existe un algoritmo de complejidad secuencial de orden $O(d^{13}(n+L)^3)$ que produce un straight-line program de longitud $O(d^4 + L)$ que calcula un elemento $\theta \in R$ y los coeficientes de un polinomio $f^* \in R[Y]$ que satisface:*

$$f^* = \theta \cdot \frac{f}{\gcd(f, f')}$$

El elemento θ y los coeficientes del polinomio f^* son polinomios de grados acotados por $2d(d+1)D$.

Demostración. En primer lugar se obtiene un straight-line program que calcula los coeficientes del polinomio derivado f' (con respecto a la variable Y) de f. A continuación se aplica el Lemma 1.3.6 para obtener un straight-line program para los coeficientes de un máximo común divisor de f y f'. Finalmente, se resuelve el sistema lineal que resulta de la relación

$$f = \gcd(f, f') \cdot f^*$$

considerando los coeficientes del polinomio f^* como incógnitas.

Se obtiene así un straight-line program de longitud $O(d^4 + L)$ que representa los coeficientes de f^* y el elemento $\theta \in R$, que es un menor de la matriz de coeficientes del sistema.

La cota para la complejidad del algoritmo se deduce de la dada en el Lema 1.3.6 para el cálculo del máximo común divisor y de la complejidad para la resolución del sistema lineal involucrado.

El algoritmo dado en el Lema 1.3.8 para el cálculo del máximo común divisor nos permite construir un algoritmo que calcula el radical de un polinomio multivariado:

Lema 1.3.11 *Sea $f \in k[X_1, \ldots, X_n]$ un polinomio de grado acotado por d dado por un straight-line program de longitud L. Entonces existe un algoritmo probabilístico que produce un straight-line program para un* $\mathrm{rad}(f)$. *La complejidad secuencial del algoritmo y la longitud del straight-line program obtenido son de orden $d^{O(1)}(n+L)$. Si los parámetros aleatorios son elegidos de un subconjunto de k con N elementos, la probabilidad de éxito del algoritmo es al menos $1 - \frac{2d^2+3d}{N}$.*

Demostración. Observamos que si $f \in k[X_1, \ldots, X_n]$ es mónico en la variable X_n (salvo por un factor constante), entonces

$$\mathrm{rad}(f) = \frac{f}{\gcd(f, \frac{\partial f}{\partial X_n})} \tag{1.1}$$

El algoritmo se desarrolla como sigue:

Paso 1. Efectuar un cambio de variables de la forma $X_n = Y_n$, $X_i = Y_i + \lambda_i X_i$ para cada $1 \leq i \leq n-1$, de manera que el nuevo polinomio $\tilde{f}(Y_1, \ldots, Y_n)$ sea mónico con respecto a la variable Y_n (ver la demostración del Lema 1.3.8).

Paso 2. Calcular $\gcd(\tilde{f}, \frac{\partial \tilde{f}}{\partial Y_n})$ aplicando el Lema 1.3.8. El polinomio $\tilde{f}$ es calculable por medio de un straight-line program de longitud $2n + L$ y, es un hecho conocido que $\frac{\partial \tilde{f}}{\partial Y_n}$ se puede calcular entonces por medio de un straight-line program de longitud acotada por $6(n + L)$.

Paso 3. Elegir aleatoriamente las coordenadas de un punto $\eta := (\eta_1, \ldots, \eta_n)$, con el objeto de que $\gcd(\tilde{f}, \frac{\partial \tilde{f}}{\partial Y_n})(\eta) \neq 0$ y calcular $\mathrm{rad}(\tilde{f})$ según la fórmula (1.1) aplicando el Lema 1.3.5.

Paso 4. Realizar nuevamente un cambio de variables para obtener

$$\mathrm{rad}(f) = \mathrm{rad}(\tilde{f})(X_1 - \lambda_1 X_n, \ldots, X_{n-1} - \lambda_{n-1} X_n, X_n).$$

Las cotas para la complejidad, para la probabilidad de éxito del algoritmo y para la longitud del straight-line program que produce se deducen fácilmente de las correspondientes a los algoritmos usados en los pasos intermedios.

Observación 1.3.12 En forma análoga a lo explicado en la Observación 1.3.9, el algoritmo probabilístico construido en el lema anterior puede transformarse en uno determinístico de complejidad secuencial de orden $(d(n+L))^{O(1)}$.

1.4 Algunas herramientas algorítmicas

Los algoritmos que se construyen en este trabajo están basados en técnicas conocidas de Álgebra Lineal efectiva y en distintos algoritmos existentes para la resolución de problemas de Geometría Algebraica.

En esta sección presentamos las herramientas algorítmicas básicas que se utilizarán.

1.4.1 Cálculo de la dimensión de una variedad algebraica

En los algoritmos presentados en los Capítulos 2 y 3 se necesitará calcular la dimensión de una variedad algebraica proyectiva o afín a partir de un conjunto finito de polinomios que la define. Para hacer esto se aplicará el algoritmo dado en [13].

Por otro lado, las técnicas desarrolladas en [13] y [24] se utilizan también como base del algoritmo para el cálculo de la descomposición equidimensional de una variedad afín que se describe en el Capítulo 3.

Comentamos brevemente estas técnicas.

Descripción de los puntos aislados de una variedad

El algoritmo descripto en [13] calcula la dimensión de una variedad algebraica a partir de un procedimiento que permite caracterizar los puntos aislados de una variedad afín arbitraria V dada por un sistema de ecuaciones polinomiales.

Este procedimiento obtiene una resolución geométrica de una variedad de dimensión cero incluida en V y que contiene a los puntos aislados de V, y se desarrolla como sigue:

(i) Dada una forma lineal ℓ arbitraria determina un polinomio p tal que $p(\ell)$ se anula sobre los puntos aislados de V.

(ii) Determina un elemento primitivo para los puntos aislados de V, es decir, una forma lineal y tal que $y(x) \neq y(x')$ para x, x' puntos aislados de V.

(iii) A partir del elemento primitivo hallado, se obtienen las parametrizaciones que satisfacen las coordenadas de los puntos aislados de V, y una ecuación para y, lo que da la resolución geométrica.

El paso fundamental de este algoritmo es (i), que puede verse como una forma débil de resolución simbólica (y que es equivalente en complejidad al problema general del cálculo de una resolución geométrica).

Se considera una variedad algebraica $V := V(f_1, \ldots, f_s) \subset \mathbb{A}^n$, donde $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$, con $s \geq n$, son polinomios de grados acotados por $d \geq n$ dados en forma densa. En un primer paso, se reemplaza el sistema input por n combinaciones lineales genéricas $\hat{f}_1, \ldots, \hat{f}_n$ de $f_1, \ldots, f_s$. Esta preparación del input conserva todas las componentes irreducibles de V y añade, eventualmente, algunos puntos aislados, pero reduce el problema al caso en que los puntos aislados forman localmente una intersección completa.

A continuación, se reduce el problema al caso proyectivo cero-dimensional mediante técnicas de homotopía: Se considera una sucesión regular de polinomios homogéneos auxiliares $G_1, \ldots, G_n \in k(\varepsilon)[X_0, X_1, \ldots, X_n]$ que define una variedad proyectiva cero-dimensional en $\mathbb{P}^n(\overline{k(\varepsilon)})$ sin puntos en el infinito. Más precisamente, si F_i denota el homogeneizado de $\hat{f}_i$ en la variable X_0, se define

$$G_i := X_0 F_i + \varepsilon X_i^{1+\deg \hat{f}_i} \qquad (1 \leq i \leq n).$$

Se observa que especializando los polinomios $G_1, \ldots, G_n$ en $\varepsilon = 0$, se obtiene una variedad en $\mathbb{P}^n(\bar{k})$ que contiene a los puntos aislados de V como componentes irreducibles.

Finalmente, se hallan ecuaciones de dependencia para formas lineales sobre ideales homogéneos cero-dimensionales sin ceros en el infinito como polinomios característicos de morfismos apropiados, y se muestra cómo calcular a partir de ellas la ecuación p que anula a la forma lineal ℓ sobre los puntos aislados de V.

En cuanto a la elección del elemento primitivo y el cálculo de las parametrizaciones, se considera en primer término la situación para un caso particular en dos variables. En el caso general, se toma una forma lineal genérica $Y = T_1 X_1 + \cdots + T_n X_n$ y se reduce el problema a analizar n situaciones que satisfacen las condiciones del caso particular estudiado de dos variables. Esto permite determinar un polinomio $F \in k[T_1, \ldots, T_n]$ tal que para cada n-upla $(\lambda_1, \ldots, \lambda_n) \in k^n$ con $F(\lambda_1, \ldots, \lambda_n) \neq 0$, la forma lineal inducida separa los puntos aislados de la variedad. Finalmente, se

considera una forma lineal cuyos coeficientes no anulen al polinomio F y se calculan las parametrizaciones a partir de los resultados obtenidos en el caso de dos variables.

El resultado que se prueba es el *lema del elemento primitivo* que enunciamos a continuación en un contexto más general (ver la Sección 3.4.7 de [13] y [24, Proposition 27]):

Lema 1.4.1 *Sea R un anillo de polinomios sobre k y sea K la clausura algebraica del cuerpo de fracciones de R. Sean $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$ polinomios de grados (en $X_1, \ldots, X_n$) acotados por $d \geq n$ dados en forma densa con respecto a $X_1, \ldots, X_n$. Denotemos por $V \subset K^n$ a la variedad definida por estos polinomios. Entonces, existe un algoritmo de complejidad acotada por $s^{O(1)}d^{O(n)}$ que calcula una forma lineal $y = \lambda_1 X_1 + \cdots + \lambda_n X_n \in k[X_1, \ldots, X_n]$, un elemento $\rho \in R$ y polinomios univariados $v_i \in R[Y]$ $(1 \leq i \leq n)$ de grados acotados por $d^{O(n)}$ tales que*

- *La forma lineal y separa los puntos aislados de V.*
- *Las coordenadas $x = (x_1, \ldots, x_n)$ de los puntos aislados de V verifican las ecuaciones $\rho x_i = v_i(y(x))$ $(1 \leq i \leq n)$*

Tanto ρ como los coeficientes de los polinomios v_i $(1 \leq i \leq n)$ son polinomios en los coeficientes de $f_1, \ldots, f_s$ de grados acotados por $d^{O(n)}$ que pueden ser evaluados a partir de dichos coeficientes por medio de un straight-line program de longitud $d^{O(n)}$.

Observamos que, de la demostración del lema (ver [24]), se deduce la existencia de un polinomio $F \in R[T_1, \ldots, T_n]$ de grado acotado por $d^{O(n)}$ que verifica:

- Toda forma lineal $y = \lambda_1 X_1 + \cdots + \lambda_n X_n$ cuyos coeficientes satisfacen la condición $F(\lambda_1, \ldots, \lambda_n) \neq 0$ separa los puntos aislados de V.
- El algoritmo dado para el cálculo de las parametrizaciones puede aplicarse a cualquier forma lineal y cuyos coeficientes no anulen a F.

Sean y una forma lineal, $\rho \in k$ y $v_1, \ldots, v_n \in k[Y]$ los elementos que produce el algoritmo dado por el Lema 1.4.1 aplicado a los polinomios $f_1, \ldots, f_s$ que definen la variedad V.

Consideremos los polinomios

$$F_j := \rho^d f_j\Big(\frac{1}{\rho} \cdot v_1(Y), \ldots, \frac{1}{\rho} \cdot v_n(Y)\Big) \quad 1 \leq j \leq s \tag{1.2}$$

y sea q su máximo común divisor en $k[Y]$.
Se verifica:

- Si la variedad V contiene puntos aislados, entonces $q \neq 1$.
- Si $q \neq 1$, entonces la variedad V es no vacía.

El polinomio q es de grado $d^{O(n)}$ y se pueden calcular los coeficientes de un múltiplo escalar de q por medio de un straight-line program sin divisiones en tiempo secuencial $s^{O(1)}d^{O(n)}$.

La forma lineal y, el polinomio libre de cuadrados cuyos ceros coinciden con los de q, y los polinomios $v_1, \ldots, v_n \in k[Y]$ dan una resolución geométrica de una variedad cero-dimensional incluida en V que contiene a los puntos aislados de V. En particular, si $\dim V = 0$, se obtiene una resolución geométrica de V.

Observación 1.4.2 Con las notaciones anteriores, si V es una variedad que o bien es vacía o bien contiene puntos aislados, se verifica

$$V = \emptyset \iff q \text{ es constante.}$$

Modificando convenientemente la construcción anterior podemos resolver este problema en un caso más general: Sean $f_1, \ldots, f_s, g \in k[X_1, \ldots, X_n]$ polinomios tales que $\deg f_i \leq d_1$ $(1 \leq i \leq s)$ y $\deg g \leq d_2$. Sea $V = V(f_1, \ldots, f_s) \subseteq \mathbb{A}^n$ y sea $U = \{x \in \bar{k}^n : g(x) \neq 0\}$.

Sean y una forma lineal, $\rho \in k$ y $v_1, \ldots, v_n \in k[Y]$ dados por el Lema 1.4.1 aplicado a los polinomios $f_1, \ldots, f_s$ que definen la variedad V. Sean $F_1, \ldots, F_s \in k[Y]$ los polinomios construidos como en la ecuación (1.2) tomando $d = d_1$, y sea $q \in k[Y]$ su máximo común divisor. Sea δ tal que $\deg F_j \leq \delta$ para todo $1 \leq j \leq s$. Consideremos el polinomio

$$G := \left(\rho^{d_2} \cdot g\left(\frac{1}{\rho} \cdot v_1(Y), \ldots, \frac{1}{\rho} \cdot v_n(Y)\right)\right)^{\delta}.$$

Entonces, si $V \cap U$ tiene a lo sumo puntos aislados de V, es fácil ver que

$$V \cap U = \emptyset \iff q \text{ divide a } G.$$

Cálculo de la dimensión

El algoritmo de Giusti y Heintz que calcula la dimensión de una variedad algebraica afín se basa en el lema del elemento primitivo que hemos enunciado y en la siguiente observación: si la variedad V tiene dimensión r, la intersección de V con r hiperplanos genéricos tiene dimensión 0.

En un primer paso se considera, para cada h $(0 \leq h \leq n)$, la variedad V_h que consiste de los ceros comunes de los polinomios que definen a V y h formas lineales genéricas. Se aplica el Lema 1.4.1 para obtener un polinomio q_h de grado $d^{O(n)}$ que verifica:

1. Si la variedad V_h contiene puntos aislados, entonces q_h no es constante.
2. Si q_h no es constante, entonces V_h es no vacía.

A continuación se determina para qué valores de h el polinomio q_h no es constante. El valor $r = \dim V$ es el máximo h tal que el polinomio q_h no es constante, o -1 si todos lo son.

Se deduce entonces el siguiente Teorema (ver la Sección 3.5 de [13]).

Teorema 1.4.3 *Salvo por una preparación previa, se puede calcular la dimensión de una variedad afín V definida por polinomios $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ de grado acotado por $d \geq n$, en tiempo secuencial $s^{O(1)}d^{O(n)}$ mediante un algoritmo bien paralelizable que no contiene divisiones.*

1.4.2 Eliminación de cuantificadores

En los algoritmos que se exhiben en el Capítulo 2 se utiliza de manera fundamental el algoritmo efectivo para eliminación de cuantificadores sobre cuerpos algebraicamente cerrados descripto en [29].

Antes de presentar los resultados que se utilizarán y las ideas en que se basan los algoritmos involucrados, daremos algunas definiciones elementales.

Sea k un cuerpo y sea $\bar{k}$ una clausura algebraica de k. El *lenguaje de primer orden* o *lenguaje elemental* sobre $\bar{k}$ con constantes en k, denotado por $\mathcal{L}$, consta de los siguientes símbolos no lógicos:

i) Para cada $a \in k$, una constante que también llamaremos a.

ii) Los símbolos de funciones: $+$, $-$, $\cdot$.

iii) El símbolo de relación $=$

Las variables de $\mathcal{L}$ serán consideradas como indeterminadas $X_1, \ldots, X_n, \ldots$ sobre $\bar{k}$ (infinitas numerables), y los términos del lenguaje, representados por polinomios en esas indeterminadas con coeficientes en k (notar que cada término involucra finitas variables).

De esta manera, un término típico será un polinomio multivariado F con coeficientes en k y una fórmula atómica típica será $F = 0$. Para la negación de esta fórmula escribiremos $F \neq 0$.

El lenguaje $\mathcal{L}$ se construye a partir de las fórmulas atómicas usando los conectivos lógicos $\wedge, \vee$ y $\neg$, y los cuantificadores de primer orden $\exists$ y $\forall$ aplicados a elementos de $\bar{k}$ (no a conjuntos, relaciones ni predicados de mayor orden de $\bar{k}$).

Se llama *variables ligadas* o *cuantificadas* a aquéllas que aparecen en una fórmula acompañadas por un cuantificador, ya sea existencial o universal. A las restantes variables que aparecen en la fórmula se les dice *variables libres.*

Diremos que dos fórmulas Φ y Ψ del lenguaje $\mathcal{L}$ son *equivalentes con respecto a* $\bar{k}$ si se verifican las dos condiciones siguientes:

i) Φ y Ψ tienen el mismo número de variables libres

ii) Si m es la cantidad de variables libres de Φ (y de Ψ) entonces, para cada m-upla $x = (x_1, \ldots, x_m) \in \bar{k}^m$, $\Phi(x)$ es verdadera si y sólo si $\Psi(x)$ lo es (donde $\Phi(x)$ significa reemplazar las m variables libres de Φ por $x_1, \ldots, x_m$).

La *longitud* de una fórmula Φ, que notaremos $|\Phi|$, es la cantidad de símbolos necesarios para escribir a Φ.

Es un hecho clásico de la teoría de modelos que el lenguaje de primer orden $\mathcal{L}$ sobre $\bar{k}$ admite eliminación de cuantificadores, es decir, para toda fórmula $\Phi \in \mathcal{L}$ existe una fórmula $\Psi \in \mathcal{L}$, sin cuantificadores, equivalente a Φ. Además, esta eliminación puede hacerse en forma algorítmica (ver, por ejemplo [20] y [17]).

Un caso fundamental de eliminación de cuantificadores es el de una fórmula con un solo bloque de cuantificadores que es una conjunción de fórmulas atómicas (y

negaciones de fórmulas atómicas), que corresponde a la proyección de un conjunto cerrado algebraico (resp. localmente cerrado). Nos restringiremos a analizar este caso, que es el tipo de fórmulas con las que trabajaremos más adelante.

Un bloque de cuantificadores existenciales sin desigualdades

Sean $F_1, \ldots, F_s \in k[X_1, \ldots, X_n]$ polinomios de grados acotados por $d \geq m$ en las variables $X_{n-m+1}, \ldots, X_n$ y de grados acotados por d' en las variables $X_1, \ldots, X_{n-m}$, codificados en forma densa en las variables $X_{n-m+1}, \ldots, X_n$ con coeficientes polinomios en $k[X_1, \ldots, X_{n-m}]$ dados por un straight-line program de longitud L.
Sea $\mathcal{P} \subseteq \mathbb{A}^{n-m}$ el conjunto

$$\mathcal{P} = \{(x_1, \ldots, x_{n-m}) \in \bar{k}^{n-m} \,/\, \exists\, (x_{n-m+1}, \ldots, x_n) \in \bar{k}^m : \\ F_1(x_1, \ldots, x_n) = 0 \wedge \ldots \wedge F_s(x_1, \ldots, x_n) = 0\}.$$

Observemos que para cada punto $(\xi_1, \ldots, \xi_{n-m}) \in \bar{k}^{n-m}$ se tiene $(\xi_1, \ldots, \xi_{n-m}) \in \mathcal{P}$ si y sólo si

$$\{(x_{n-m+1}, \ldots, x_n) \in \bar{k}^m : F_1(\xi_1, \ldots, \xi_{n-m}, x_{n-m+1}, \ldots, x_n) = 0 \wedge \\ \wedge \ldots \wedge F_s(\xi_1, \ldots, \xi_{n-m}, x_{n-m+1}, \ldots, x_n) = 0\} \neq \emptyset.$$

Consideremos el anillo $R = k[\xi_1, \ldots, \xi_{n-m}]$. Sean $f_1, \ldots, f_s \in R[X_{n-m+1}, \ldots, X_n]$ los polinomios definidos por

$$f_i(X_{m-m+1}, \ldots, X_n) = F_i(\xi_1, \ldots, \xi_{n-m}, X_{n-m+1}, \ldots, X_n) \quad i = 1, \ldots, s.$$

Sea K una clausura algebraica del cuerpo de fracciones de R y sea V la variedad algebraica definida por los polinomios $f_1, \ldots, f_s$ en K^m. Entonces

$$(\xi_1, \ldots, \xi_{n-m}) \in \mathcal{P} \iff V \neq \emptyset \iff \dim V \geq 0$$

La idea es hallar una condición polinomial equivalente a que la variedad V sea vacía por medio del algoritmo de Giusti y Heintz para el cálculo de la dimensión (ver Teorema 1.4.3). Sin embargo, no es posible aplicar el algoritmo directamente debido a la imposibilidad de decidir si un elemento dado de R es cero o no, puesto que $(\xi_1, \ldots, \xi_{n-m})$ es arbitrario. Se lo modifica entonces convenientemente:

1. Cada vez que se necesita decidir si un elemento β del anillo de base es cero o no, se consideran las dos posibilidades: $\beta = 0$ y $\beta \neq 0$, lo que da lugar a ramificaciones en el algoritmo.

2. Teniendo en cuenta que para cada uno de los polinomios que se obtienen como resultados intermedios del algoritmo se conocen cotas para su grado y para la longitud del straight-line program que lo evalúa, la condición de que un polinomio sea el polinomio nulo se reemplaza por la de que se anule sobre todos los elementos de una sucesión de prueba apropiada.

Así se obtiene el siguiente resultado (ver [29, Theorem 3.2.1]):

Proposición 1.4.4 *Con las notaciones e hipótesis anteriores, salvo por una preparación previa, se puede hallar por medio de un algoritmo bien paralelizable y sin divisiones de complejidad secuencial* $L + s^{O(1)}d^{O(m)}$ *una fórmula* Ψ *libre de cuantificadores que verifica*

$$\mathcal{P} = \{(x_1, \ldots, x_{n-m}) \in \bar{k}^{n-m} \ / \ \Psi(x_1, \ldots, x_{n-m})\}.$$

La longitud de la fórmula Ψ *es de orden* $L + s^{O(1)}d^{O(m)}$ *y en ella aparecen a lo sumo* $s^{O(1)}d^{O(m)}$ *polinomios de grados acotados por* $d'\,d^{O(m)}$*, dados por un straight-line program de longitud* $L + s^{O(1)}d^{O(m)}$.

Un bloque de cuantificadores existenciales con desigualdades

Sean $F_1, \ldots, F_s \in k[X_1, \ldots, X_n]$ polinomios de grados acotados por $d \geq m$ en las variables $X_{n-m+1}, \ldots, X_n$ y de grados acotados por d' en las variables restantes. Sean $G_1, \ldots, G_{s'} \in k[X_1, \ldots, X_n]$ polinomios con grados en las variables $X_{n-m+1}, \ldots, X_n$ acotados por δ y grados acotados por δ' en las variables $X_1, \ldots, X_{n-m}$. Los polinomios $F_1, \ldots, F_s, G_1, \ldots, G_{s'}$ se suponen dados por un straight-line program de longitud L.

Sea $\mathcal{P} \subseteq \mathbb{A}^{n-m}$ el conjunto definido por

$$\mathcal{P} = \{(x_1, \ldots, x_{n-m}) \in \bar{k}^{n-m} \ / \ \exists (x_{n-m+1}, \ldots, x_n) \in \bar{k}^m : F_1(x_1, \ldots, x_n) = 0 \wedge \ldots$$
$$\wedge \ldots \wedge F_s(x_1, \ldots, x_n) = 0 \wedge G_1(x_1, \ldots, x_n) \neq 0 \wedge \ldots \wedge G_{s'}(x_1, \ldots, x_n) \neq 0\}$$

De manera análoga a lo que sucede en el caso sin desigualdades, la idea del algoritmo es ver el problema de la eliminación como el de decidir, para cada punto del espacio de parámetros, si cierto conjunto algebraico (en este caso la intersección de un cerrado con un abierto) es vacío o no. Para resolver este último problema se adaptan los métodos de Giusti y Heintz para el cálculo de la dimensión, teniendo en cuenta la segunda parte de la Observación 1.4.2.

De esta manera, se obtiene el siguiente resultado (ver [29, Theorem 3.4.1]):

Proposición 1.4.5 *Con las notaciones e hipótesis anteriores, salvo por una preparación previa, se puede hallar mediante un algoritmo bien paralelizable y sin divisiones de complejidad secuencial de orden* $L^2(s\,s'\,\delta)^{O(1)}d^{O(m)}$, *una fórmula* Ψ *libre de cuantificadores que verifica*

$$\mathcal{P} = \{(x_1, \ldots, x_{n-m}) \in \bar{k}^{n-m} \,/\, \Psi(x_1, \ldots, x_{n-m})\}$$

La longitud de la fórmula Ψ, *así como también la cantidad de polinomios que aparecen en ella, es de orden* $L^2(s\,s'\,\delta)^{O(1)}d^{O(m)}$. *Además, los polinomios de salida son de grado acotado por* $\delta' d'(s'\,\delta)^{O(1)}d^{O(m)}$ *y están dados por un straight-line program de longitud* $L^2(s\,s'\,\delta)^{O(1)}d^{O(m)}$.

1.4.3 Método de Newton

La tercera de las herramientas algorítmicas principales que se utilizarán es una aplicación simbólica sin divisiones del algoritmo de Newton-Hensel, que representa una versión algorítmica del Teorema de la Función Implícita.

Presentamos en primer lugar el resultado teórico en que se sustenta el algoritmo.

Sean $T_1, \ldots, T_m, X_1, \ldots, X_n$ indeterminadas sobre k. Escribiremos $T := (T_1, \ldots, T_m)$ y $X := (X_1, \ldots, X_n)$. Dado $t \in \bar{k}^n$, notaremos $T - t := (T_1 - t_1, \ldots, T_m - t_m)$.
Sean $f_1, \ldots, f_n \in k[T, X]$ polinomios. Notaremos $f := (f_1, \ldots, f_n)$ y Df a la matriz jacobiana de f con respecto a las variables X, es decir

$$Df := \begin{pmatrix} \frac{\partial f_1}{X_1} & \frac{\partial f_1}{\partial X_n} \\ \vdots & \vdots \\ \frac{\partial f_n}{X_1} & \frac{\partial f_n}{\partial X_n} \end{pmatrix}.$$

Finalmente, Jf denotará al determinante de la matriz Df.

Lema 1.4.6 *Sean* $f_1, \ldots, f_n \in k[T, X]$, *y sea* $(t, \xi) \in \mathbb{A}^m \times \mathbb{A}^n$ *tal que*

$$f_1(t, \xi) = 0, \ldots, f_n(t, \xi) = 0 \quad y \quad Jf(t, \xi) \neq 0.$$

Entonces existe una n-upla $\mathcal{R} = (\mathcal{R}_1, \ldots, \mathcal{R}_n) \in \bar{k}[[T - t]]^n$ *que verifica:*

- $f_1(T, \mathcal{R}) = 0, \ldots, f_n(T, \mathcal{R}) = 0$
- $\mathcal{R}(t) := (\mathcal{R}_1(t), \ldots, \mathcal{R}_n(t)) = \xi$.

Demostración. Sea $f(X) := (f_1(T,X),\ldots,f_n(T,X))$.

Se define el operador de Newton asociado a f como

$$N_f(X)^t := X^t - Df(X)^{-1}.f(X)^t = \frac{Jf(X).X^t - \mathrm{adj}(Df)(X).f(X)^t}{Jf(X)}, \qquad (1.3)$$

donde $\mathrm{adj}(Df)$ denota la matriz adjunta de la matriz Df.

Observamos que $Jf(X) \not\equiv 0$, puesto que considerándolo como polinomio en las variables $T_1,\ldots T_m, X_1,\ldots,X_n$, se tiene que $Jf(t,\xi) \neq 0$.

Se define la siguiente sucesión de vectores de funciones racionales:

$$\begin{cases} R^{(0)} := \xi \\ R^{(k)} := N_f(R^{(k-1)}) = N_f^k(\xi) \quad \text{para } k \in \mathbb{N} \end{cases}$$

Teniendo en cuenta la fórmula (1.3) para el operador de Newton, para ver que la sucesión $(R^{(k)})_{k\in\mathbb{N}_0}$ está bien definida, basta con verificar que $Jf(R^{(k)}) \neq 0$ para cada $k \in \mathbb{N}_0$.

Supongamos que $R^{(k)} \in \bar{k}(T)^n$ y que $R^{(k)}(t) = \xi$ (es claro que esto vale en el caso $k = 0$). Entonces $Jf(R^{(k)}) \not\equiv 0 \in \bar{k}(T)$, puesto que

$$\begin{aligned} Jf(R^{(k)})(t) &= \det \begin{pmatrix} \frac{\partial f_1}{X_1}(t,R^{(k)}(t)) & \frac{\partial f_1}{\partial X_n}(t,R^{(k)}(t)) \\ & \vdots \\ \frac{\partial f_n}{X_1}(t,R^{(k)}(t)) & \frac{\partial f_n}{\partial X_n}(t,R^{(k)}(t)) \end{pmatrix} \\ &= \det \begin{pmatrix} \frac{\partial f_1}{X_1}(t,\xi) & \frac{\partial f_1}{\partial X_n}(t,\xi) \\ \vdots & \vdots \\ \frac{\partial f_n}{X_1}(t,\xi) & \frac{\partial f_n}{\partial X_n}(t,\xi) \end{pmatrix} = Jf(t,\xi) \neq 0 \end{aligned}$$

por hipótesis.

En consecuencia, se puede definir $R^{(k+1)} := N_f(R^{(k)}) \in \bar{k}(T)^n$ y, del hecho que $R^{(k)}(t) = \xi$ y $f(t,\xi) = 0$, se deduce que

$$R^{(k+1)}(t) = N_f(R^{(k)})(t) = \xi^t - Df(t,\xi)^{-1}.f(t,\xi)^t = \xi^t$$

Esto muestra la buena definición de la sucesión $(R^{(k)})_{k\in\mathbb{N}}$.

Por la definición del operador N_f, como $Jf(t,\xi) \neq 0$, resulta que los denominadores de las coordenadas de cada uno de los vectores $R^{(k)}$, $k \in \mathbb{N}$, no se anulan en t. Por lo tanto, considerados como elementos de $\bar{k}[[T-t]]$, son inversibles.

Luego, $R^{(k)} \in \bar{k}[[T-t]]^n$ para cada $k \in \mathbb{N}_0$.

Veamos que para cada $k \in \mathbb{N}_0$ valen las siguientes condiciones:

(i) $f_j(T, R^{(k)}) \in (T-t)^{2^k} \subset \bar{k}[[T-t]]$ para cada $1 \leq j \leq n$.

(ii) $R_i^{(k+1)} - R_i^{(k)} \in (T-t)^{2^k} \subset \bar{k}[[T-t]]$ para cada $1 \leq i \leq n$.

donde $(T-t)$ denota el ideal de $\bar{k}[[T-t]]$ generado por $T_1 - t_1, \ldots, T_m - t_m$.

Para $k = 0$, dado que $f_j(t, \xi) = 0$ para cada $1 \leq j \leq n$,

$$f_j(T, R^{(0)}) = f_j(T, \xi) \in (T-t) \qquad j = 1, \ldots, n$$

y, como $R^{(1)} - \xi^t = -Df(\xi)^{-1}.f(\xi)^t$, vale $R_i^{(1)} - \xi_i \in (T-t)$ para cada $1 \leq i \leq n$.

Supongamos que las condiciones (i) y (ii) valen para $k \in \mathbb{N}_0$.
Para cada $1 \leq j \leq n$, considerando el desarrollo de Taylor centrado en $R^{(k)}$ del polinomio f_j (visto como polinomio en las variables X) se tiene que

$$f_j(T, R^{(k+1)}) - f_j(T, R^{(k)}) - \sum_{i=1}^{n} \frac{\partial f_j}{\partial x_i}(T, R^{(k)}).(R_i^{(k+1)} - R_i^{(k)}) \in (R^{(k+1)} - R^{(k)})^2,$$

donde $(R^{(k+1)} - R^{(k)})$ es el ideal

$$(R^{(k+1)} - R^{(k)}) := (R_i^{(k+1)} - R_i^{(k)} : 1 \leq i \leq n) \subseteq \bar{k}[[T-t]].$$

De la definición de $R^{(k+1)}$ se deduce que

$$Df(R^{(k)}).(R^{(k+1)} - R^{(k)})^t = -f(R^{(k)})$$

y por lo tanto

$$f_j(T, R^{(k+1)}) - f_j(T, R^k) - \sum_{i=1}^{n} \frac{\partial f_j}{\partial x_l}(T, R^{(k)}).(R_i^{(k+1)} - R_i^{(k)}) = f_j(T, R^{(k+1)}).$$

Por hipótesis inductiva, $R_i^{(k+1)} - R_i^{(k)} \in (T-t)^{2^k}$ para todo $1 \leq i \leq n$, de donde se deduce que $(R^{(k+1)} - R^{(k)})^2 \subset (T-t)^{2^{k+1}}$. Luego

$$f_j(T, R^{(k+1)}) \in (T-t)^{2^{k+1}}.$$

Para probar la validez de la condición (ii), basta observar que por definición

$$R^{(k+2)} - R^{(k+1)} = -Df(R^{(k+1)})^{-1}.f(R^{(k+1)})^t$$

y tener en cuenta que vale (i) para $k = 1$.

La condición (ii) implica que para cada $1 \leq i \leq n$ la sucesión $(R_i^{(k)})_{k\in\mathbb{N}}$ converge a un elemento $\mathcal{R}_i \in \bar{k}[[T-t]]$. Sea $\mathcal{R} := (\mathcal{R}_1, \ldots, \mathcal{R}_n)$.
Es claro que $\mathcal{R}(t) = \xi$. Finalmente, la condición (i) implica que $f_j(T, \mathcal{R}) = 0$ para cada $1 \leq j \leq n$.

□

Desde el punto de vista algorítmico, se utilizará el operador de Newton introducido en la demostración del Lema 1.4.6 con el objeto de aproximar soluciones en $\bar{k}[[T-t]]^n$ de sistemas de ecuaciones polinomiales en $k[T][X_1, \ldots, X_n]$.

Se considerará la siguiente noción de aproximación: Dadas φ y $\tilde{\varphi}$ en $\bar{k}[[T-t]]$ y $M \in \mathbb{N}_0$, diremos que $\tilde{\varphi}$ *aproxima a* φ *con precisión* M si $\varphi - \tilde{\varphi} \in (T-t)^M$. Si $\Phi = (\varphi_1, \ldots \varphi_n)$ y $\tilde{\Phi} = (\tilde{\varphi}_1, \ldots \tilde{\varphi}_n)$ son vectores en $\bar{k}[[T-t]]^n$, diremos que $\tilde{\Phi}$ *aproxima a* Φ *con precisión* M si $\tilde{\varphi}_i - \varphi_i \in (T-t)^M$ para cada $1 \leq i \leq n$.

Sean $f_1, \ldots, f_n \in k[T, X]$ polinomios tales que el determinante de la matriz jacobiana Df es un polinomio no nulo. Se considera el operador de Newton asociado a $f := (f_1, \ldots, f_n)$

$$N_f(X) = X^t - Df(X)^{-1}.f(X)^t$$

Como se vio en la demostración del Lema 1.4.6, si $(t, \xi) \in \mathbb{A}^m \times \mathbb{A}^n$ satisface

$$f_1(t, \xi) = 0, \ldots, f_n(t, \xi) = 0 \quad \text{y} \quad Jf(t, \xi) \neq 0$$

para cada $k \in \mathbb{N}_0$, el vector $R^{(k)} := N_f^k(\xi) \in \bar{k}[[T-t]]^n$ aproxima con precisión 2^k a un vector $\mathcal{R} \in \bar{k}[[T-t]]^n$ que es solución del sistema $f_1(X) = 0, \ldots, f_n(X) = 0$.
Observamos que $N_f(X)$ está dado por un vector de n funciones racionales en $k(T, X)$, al igual que N_f^κ, la κ–ésima iteración de N_f. En otras palabras, para cada $\kappa \in \mathbb{N}$ existen numeradores $g_1^{(\kappa)}, \ldots, g_n^{(\kappa)} \in k[T, X]$ y un denominador no nulo $h^{(\kappa)} \in k[T, X]$ tales que

$$N_f^\kappa = \left(\frac{g_1^{(\kappa)}}{h^{(\kappa)}}, \ldots, \frac{g_n^{(\kappa)}}{h^{(\kappa)}}\right) \in k(T, X).$$

En el siguiente lema se describe un straight-line program sin divisiones que evalúa estos polinomios.

Lema 1.4.7 *([11, Lemma 30]) Con las mismas hipótesis y notaciones que en el Lema 1.4.6, supongamos que los polinomios $f_1, \ldots, f_n \in k[T][X]$ tienen grados acotados por d y están dados por un straight-line program de longitud L. Sea $\kappa \in \mathbb{N}$. Entonces existe un straight-line program de longitud $O(\kappa d^2 n^7 L)$ que evalúa polinomios $g_1^{(\kappa)}, \ldots, g_n^{(\kappa)}, h^{(\kappa)}$ en $k[T][X]$ con $h^{(\kappa)}(t, \xi) \neq 0$ que representan los numeradores y un denominador de las funciones racionales que se obtienen en la κ-ésima iteración del operador de Newton.*

Demostración. El operador N_f puede escribirse como

$$N_f(X)^t = \frac{Jf(X).X^t - \mathrm{adj}(Df)(X).f(X)^t}{Jf(X)}$$

Denotemos por a_{ij} $(1 \leq i, j \leq n)$ a las entradas de la matriz $\mathrm{adj}(Df)$. Consideremos los polinomios

$$g_i := Jf.X_i - \sum_{j=1}^{n} a_{ij} f_j \qquad (1 \leq i \leq n).$$

Observamos que las entradas (a_{ij}) de la matriz $\mathrm{adj}(Df)$ son polinomios en $k[T, X]$ de grados acotados por $(n-1)(d-1)$ y que $Jf \in k[T, X]$ tiene grado acotado por $n(d-1)$. Luego, $\nu := nd + 1$ es una cota superior para los grados de los polinomios $g_1, \ldots, g_n \in k[T, X]$.

Para cada $1 \leq i \leq n$, sea $\bar{g}_i(X_0, X_1, \ldots, X_n)$ el polinomio en $k[T][X_0, \ldots, X_n]$ que se obtiene al homogeneizar g_i por una nueva variable X_0. Análogamente, sea $\overline{Jf}(X_0, \ldots, X_n)$ el homogeneizado de Jf. Finalmente, sean

$$\begin{aligned} G_i(X_0, \ldots, X_n) &:= X_0^{\nu - \deg g_i}.\bar{g}_i \qquad (1 \leq i \leq n) \\ H(X_0, \ldots, X_n) &:= X_0^{\nu - \deg Jf}\,\overline{Jf} \end{aligned}$$

Las entradas de la matriz $\mathrm{adj}(Df)$ y el polinomio Jf pueden ser evaluados por medio de un straight-line program de longitud $O(n^5 + nL)$ (calculando un straight-line program para las derivadas parciales de los polinomios $f_1, \ldots, f_n$ y aplicando el algoritmo de Berkowitz a Df). Esto permite obtener un straight-line program de longitud de orden $O(d^2(n^7 + n^3 L))$ para los polinomios $G_1, \ldots, G_n$ y H.

Definimos recursivamente los siguientes polinomios:

$$\begin{aligned} g_i^{(1)} &:= G_i(1, X_1, \ldots, X_n) \quad (1 \leq i \leq n) \\ h^{(1)} &:= H(1, X_1, \ldots, X_n) \end{aligned}$$

$$\text{Para } k \geq 2\colon \quad \begin{aligned} g_i^{(k)} &:= G_i(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)}) \quad (1 \leq i \leq n) \\ h^{(k)} &:= H(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)}) \end{aligned}$$

Es fácil ver que para cada $k \in \mathbb{N}$ los polinomios $g_1^{(k)}, \ldots, g_n^{(k)}$ son numeradores y $h^{(k)}$ es un denominador para la k-ésima iteración del operador de Newton N_f, y teniendo en cuenta que

$$h^{(k)} = (h^{(k)})^{\nu} . Jf(\frac{g_1^{(k-1)}}{h^{(k-1)}}, \ldots, \frac{g_n^{(k-1)}}{h^{(k-1)}})$$

se deduce que $h^{(k)}(t, \xi) \neq 0$ para cada $k \in \mathbb{N}$.

Fijado $\kappa \in \mathbb{N}$, iterando κ veces el straight-line program que calcula $G_1, \ldots, G_n$ y H, se obtiene un straight-line program de longitud $O(\kappa\, d^2 n^7 L)$ que evalúa los polinomios $g_1^{(\kappa)}, \ldots, g_n^{(\kappa)}, h^{(\kappa)}$.

Capítulo 2

Forma de Chow. Algoritmos determinísticos

En este capítulo se muestra la existencia de un algoritmo bien paralelizable que, tomando como entrada un conjunto de s polinomios homogéneos en $n+1$ variables de grados acotados por $d \geq n$ que define una variedad proyectiva V, produce un straight-line program que calcula la forma de Chow de la componente equidimensional de V de mayor dimensión. La complejidad secuencial del algoritmo es de orden $s^{O(1)}d^{O(n)}$.

Aplicando este algoritmo se obtiene otro que, dada una variedad V (afín o proyectiva) produce polinomios que definen su componente equidimensional de mayor dimensión con cotas de complejidad del mismo orden. Como aplicación, se exhibe un algoritmo para decidir si una variedad es equidimensional o no.

2.1 Forma de Chow de una variedad proyectiva

La construcción de la forma de Chow para variedades proyectivas equidimensionales tiene por objeto caracterizar variedades de dimensión y grado dados por medio de coordenadas en cierto espacio proyectivo.

Un caso en el que esto puede hacerse fácilmente es el de las hipersuperficies: cada hipersuperficie de grado D en $\mathbb{P}^n$ tiene asociado unívocamente (salvo por un factor constante) un polinomio homogéneo de grado D en $n+1$ variables: un generador de su ideal de anulación. Los coeficientes de este polinomio pueden considerarse como un punto en un espacio proyectivo.

El problema al intentar parametrizar variedades en $\mathbb{P}^n$ en un caso más general es que una variedad de codimensión mayor que 1 no está definida por un único polinomio, es decir, su ideal de anulación no está generado por un solo polinomio. Además pueden elegirse distintos sistemas de generadores para dicho ideal. La idea para resolver el problema en el caso de una variedad $V \subseteq \mathbb{P}^n$ equidimensional arbitraria es reducirlo al de una hipersuperficie, asociando a cada variedad equidimensional V una hipersuperficie en un espacio proyectivo adecuado.

Comenzaremos por el caso de una variedad proyectiva irreducible (ver [32]):

Sean $X_0, \ldots, X_n$ indeterminadas sobre k. Sea $\mathcal{V} \subseteq \mathbb{P}^n$ una variedad proyectiva irreducible definible por polinomios en $k[X_0, \ldots, X_n]$, y sea r la dimensión proyectiva de $\mathcal{V}$.

Para cada i, $0 \leq i \leq r$, denotamos por U_i a un grupo de $n+1$ nuevas variables $U_i := (U_{i0}, U_{i1}, \ldots, U_{in})$ asociado a una forma lineal genérica

$$L_i(U_i, X) = U_{i0} X_0 + U_{i1} X_1 + \cdots + U_{in} X_n$$

donde $X := (X_1, \ldots, X_n)$.

Sea $\Gamma(\mathcal{V}) \subseteq (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n$ el conjunto

$$\Gamma(\mathcal{V}) = \{(u_0, \ldots, u_r, x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n : x \in \mathcal{V},\ L_0(u_0, x) = 0, \ldots, L_r(u_r, x) = 0\}.$$

Consideremos la proyección canónica $\pi_1 : (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \to (\mathbb{P}^n)^{r+1}$. Se tiene que $\pi_1(\Gamma(\mathcal{V}))$ es un conjunto cerrado en $(\mathbb{P}^n)^{r+1}$.

Veamos que $\pi_1(\Gamma(\mathcal{V}))$ es una hipersuperficie (esta será la hipersuperficie que asociaremos a la variedad $\mathcal{V}$):

Para esto, consideremos la proyección $\pi_2 : \Gamma(\mathcal{V}) \to \mathcal{V}$ sobre las últimas coordenadas.

Es claro que $\pi_2(\Gamma(\mathcal{V})) = \mathcal{V}$.

Dado $\xi \in \mathcal{V}$, el conjunto $\pi_2^{-1}(\xi)$ consta de los sistemas $(u_0, \ldots, u_r, \xi)$ tales que ξ pertenece a cada uno de los hiperplanos de ecuación $u_{i0} X_0 + \cdots + u_{in} X_n = 0$ para $0 \leq i \leq r$. Puesto que el conjunto de los $y \in \mathbb{P}^n$ tales que $\xi \in \{y_0 X_0 + \cdots + y_n X_n = 0\}$ es un hiperplano en $\mathbb{P}^n$, resulta que

$$\pi_2^{-1}(\xi) \simeq (\mathbb{P}^{n-1})^{r+1} \times \{\xi\}$$

Luego, $\pi_2^{-1}(\xi)$ es una variedad irreducible de dimensión $(n-1)(r+1)$.

En consecuencia, $\Gamma(\mathcal{V})$ es irreducible y

$$\dim(\Gamma(\mathcal{V})) = \dim \pi_2^{-1}(\xi) + \dim \mathcal{V} = (n-1)(r+1) + r = n(r+1) - 1$$

Consideremos ahora $\pi_1(\Gamma(\mathcal{V})) \subseteq (\mathbb{P}^n)^{r+1}$, que es por lo tanto un cerrado irreducible. Observamos que este conjunto consta de los puntos $(u_0, \ldots, u_r) \in (\mathbb{P}^n)^{r+1}$ tales que la intersección de los $r+1$ hiperplanos de ecuaciones

$$u_{i0} X_0 + \cdots + u_{in} X_n = 0 \qquad i = 0, \ldots, r$$

con la variedad $\mathcal{V}$ es no vacía.

Puesto que $\dim \mathcal{V} = r$, existen r hiperplanos $H_1, \ldots, H_r \subseteq \mathbb{P}^n$ tales que la variedad $H_1 \cap \cdots \cap H_r \cap \mathcal{V}$ es de dimensión 0.

Sea $p \in H_1 \cap \cdots \cap H_r \cap \mathcal{V}$ y consideremos un hiperplano H_0 que contenga a p. Entonces, si $u_0, \ldots, u_r$ son los vectores de coeficientes de las ecuaciones de $H_0, \ldots, H_r$, se tiene que $\pi_1^{-1}(u_0, \ldots, u_r)$ es de dimensión 0.

Del teorema de dimensión de las fibras, deducimos que

$$\dim(\pi_1(\Gamma(\mathcal{V})) = \dim(\Gamma(\mathcal{V})) = n(r+1) - 1,$$

es decir, que $\pi_1(\Gamma(\mathcal{V}))$ es una hipersuperficie en $(\mathbb{P}^n)^{r+1}$.

Por lo tanto, $\pi_1(\Gamma(\mathcal{V}))$ es el conjunto de los ceros de un único polinomio libre de cuadrados $\mathcal{F}_\mathcal{V} \in k[U_0, \ldots, U_r]$ (unívocamente determinado por $\mathcal{V}$ salvo por un factor constante) irreducible y homogéneo en cada uno de los sistemas de variables $U_0, \ldots, U_r$.

Llamaremos a cualquier polinomio $\mathcal{F}_\mathcal{V}$ que satisfaga lo anterior, una *forma de Chow* de la variedad proyectiva irreducible $\mathcal{V}$.

De la definición de $\mathcal{F}_\mathcal{V}$ se deduce que dados hiperplanos $H_0, \ldots, H_r \subseteq \mathbb{P}^n$, cuyas ecuaciones están determinadas por los vectores de coeficientes $u_0, \ldots, u_r \in \mathbb{P}^n$, se tiene que

$$\mathcal{F}_\mathcal{V}(u_0, \ldots, u_r) = 0 \iff \mathcal{V} \cap H_0 \cap \ldots \cap H_r \neq \emptyset.$$

La variedad $\mathcal{V}$ está unívocamente determinada por su forma de Chow $\mathcal{F}_\mathcal{V}$ en el siguiente sentido: un punto $x \in \mathbb{P}^n$ pertenece a $\mathcal{V}$ si y sólo si dados $r+1$ hiperplanos $H_0, \ldots, H_r$ que contienen a x, cuyas ecuaciones están dadas por $u_0, \ldots, u_r \in \mathbb{P}^n$, se tiene que $\mathcal{F}_\mathcal{V}(u_0, \ldots, u_r) = 0$.

En efecto, de la definición de la forma de Chow se deduce que para cada $x \in \mathcal{V}$, se tiene que $\mathcal{F}_{\mathcal{V}}(u_0, \ldots, u_r) = 0$ para cualesquiera $u_0, \ldots, u_r$ tales que

$$x \in \bigcap_{i=0}^{r} \{u_{i0} X_0 + \cdots + u_{in} X_n = 0\}.$$

Por otro lado, si $x \notin \mathcal{V}$, existen $r+1$ hiperplanos $H_0, \ldots, H_r$ que contienen a x tales que $H_0 \cap \ldots \cap H_r \cap \mathcal{V} = \emptyset$. Luego, si $u_0, \ldots, u_r$ son los coeficientes de estos hiperplanos, será $\mathcal{F}_{\mathcal{V}}(u_0, \ldots, u_r) \neq 0$.

Una forma de Chow $\mathcal{F}_{\mathcal{V}}$ de V es un polinomio homogéneo del mismo grado en cada uno de los grupos de variables $U_0, \ldots, U_n$, puesto que caracteriza un conjunto determinado por una condición que es simétrica con respecto a los grupos de variables. Más aún, este grado coincide con el grado de la variedad $\mathcal{V}$:

Si se consideran r hiperplanos genéricos $H_1, \ldots, H_r$ cuyas ecuaciones están dadas por $u_1, \ldots, u_r$, la intersección de $\mathcal{V}$ con $H_1, \ldots, H_r$ consiste de exactamente $D = \deg \mathcal{V}$ puntos $p^{(1)}, \ldots, p^{(D)}$. Además $(u_0, \ldots, u_r) \in \pi_1(\Gamma(\mathcal{V}))$ si y sólo si el hiperplano H_0 cuya ecuación está determinada por u_0 contiene a alguno de dichos puntos. Luego, si $p^{(j)} := (p_1^{(j)}, \ldots, p_n^{(j)})$ para cada j $(1 \leq j \leq D)$,

$$\mathcal{F}_{\mathcal{V}}(U_0, u_1, \ldots, u_r) = \alpha \prod_{j=1}^{D} (p_0^{(j)} U_{00} + \cdots + p_n^{(j)} U_{0n})^{r_j}$$

para algún $\alpha \in \bar{k}$ y ciertos $r_j \in \mathbb{N}$ $(1 \leq j \leq D)$.

Teniendo en cuenta que $\mathcal{F}_{\mathcal{V}}$ es libre de cuadrados, el polinomio $\mathcal{F}_{\mathcal{V}}(U_0, u_1, \ldots, u_r)$ genéricamente no tiene factores múltiples. Luego $\deg_{U_i} \mathcal{F}_{\mathcal{V}} = D = \deg \mathcal{V}$ para cada $0 \leq i \leq r$.

Para terminar, consideremos el caso de una variedad proyectiva equidimensional:

Sea $V \subseteq \mathbb{P}^n$ una variedad equidimensional definible por polinomios en $k[X_0, \ldots, X_n]$. Sea r la dimensión proyectiva de V y sea $V = \bigcup_{i=1}^{t} C_i$ la descomposición de V en componentes irreducibles.

Con la misma notación utilizada en el caso de variedades irreducibles, se tiene que $\Gamma(V) = \bigcup_{i=1}^{t} \Gamma(C_i)$ y, por lo tanto $\pi_1(\Gamma(V)) = \bigcup_{i=1}^{t} \pi_1(\Gamma(C_i))$.

Por lo demostrado para variedades irreducibles, se tiene que $\pi_1(\Gamma(C_i))$ es una hipersuperficie irreducible en $(\mathbb{P}^n)^{r+1}$. Luego, $\pi_1(\Gamma(V))$ es una hipersuperficie en $(\mathbb{P}^n)^{r+1}$

y por lo tanto está definida por un polinomio $\mathcal{F}_V \in k[U_0, \ldots, U_r]$ libre de cuadrados, unívocamente determinado por V salvo por un factor constante, al que llamaremos una *forma de Chow* de la variedad proyectiva equidimensional V.
Observamos que si $\mathcal{F}_V$ es una forma de Chow de V, entonces $\mathcal{F}_V = \prod_{i=1}^{t} \mathcal{F}_{C_i}$, donde para cada $1 \leq i \leq t$, $\mathcal{F}_{C_i}$ es una forma de Chow de C_i, y $\mathcal{F}_V$ es un polinomio multihomogéneo de grado $\deg V$ en cada uno de los sistemas de variables $U_0, \ldots, U_r$.

Como en el caso de una variedad irreducible, una forma de Chow de una variedad proyectiva equidimensional V de dimensión r contiene toda la información de la variedad. Más aún, más adelante veremos cómo utilizando la equivalencia

$$x \in V \iff \left(u_{i0}x_0 + \cdots + u_{in}x_n = 0 \quad \forall\, 0 \leq i \leq r \Rightarrow \mathcal{F}_V(u_0, \ldots, u_r) = 0\right)$$

se puede recuperar la variedad V a partir de una forma de Chow $\mathcal{F}_V$.

2.2 Resultados conocidos acerca del cálculo de la forma de Chow

El cálculo de la forma de Chow de una variedad proyectiva puede hacerse algorítmicamente. Entre los algoritmos que realizan esta tarea podemos mencionar los exhibidos en [3], [12] y [29].
El algoritmo descripto en [3] calcula la forma de Chow de un ideal homogéneo equidimensional dado por un sistema de generadores, mientras que el algoritmo de Puddu y Sabia ([29]) produce la forma de Chow de una variedad proyectiva irreducible a partir de un conjunto finito de polinomios homogéneos que la define. Un inconveniente que presentan estos dos algoritmos es que uno debe saber *de antemano* que el ideal o la variedad considerados verifican la condición de equidimensionalidad o irreducibilidad necesaria para la aplicación del algoritmo.
Giusti y Heintz construyen en [12] un algoritmo que se desarrolla en dos pasos: En un primer paso, calcula la descomposición equidimensional de una variedad algebraica V a partir de un sistema finito de polinomios que la define. Luego, utilizando las ecuaciones obtenidas para cada una de las componentes equidimensionales de V, calcula la forma de Chow de cada una de dichas componentes equidimensionales.

Las complejidades de los algoritmos mencionados dependen de los siguientes parámetros:

- La cantidad de polinomios homogéneos de entrada s
- El número de variables $n+1$ de estos polinomios
- Una cota superior d para el grado de los polinomios
- La dimensión r del ideal o la variedad considerados

y son de órdenes $s^5 d^{O((n-r)n^2)}$ en el caso de [3], $s^{O(1)} d^{O(nr)}$ para el algoritmo de [29] y $(sd)^{n^{O(1)}}$ en [12].

2.3 Resultados obtenidos

Sean $F_1, \ldots, F_s$ polinomios homogéneos en $k[X_0, \ldots, X_n]$ y sea $V \subseteq \mathbb{P}^n(\overline{k})$ la variedad proyectiva formada por los ceros comunes de estos polinomios, es decir

$$V = \{x \in \mathbb{P}^n(\overline{k}) \ / \ F_1(x) = 0 \wedge \ldots \wedge F_s(x) = 0\}.$$

Sea $r = \dim V$ y sea V_r la componente equidimensional de V de dimensión r.
En un primer paso, se construirá un algoritmo de complejidad secuencial de orden $s^{O(1)} d^{O(n)}$ que produce un straight-line program de longitud del mismo orden para una forma de Chow de V_r. A continuación, utilizando la forma de Chow calculada, se obtendrá un conjunto finito de polinomios que define V_r.
Luego se adaptará convenientemente el algoritmo para calcular la componente equidimensional de mayor dimensión para el caso de una variedad afín, con cotas de complejidad del mismo orden.
Finalmente se describirá un algoritmo que decide si una variedad algebraica es equidimensional o no.
Cabe destacar que el algoritmo para el cálculo de la forma de Chow que exhibiremos realiza la misma tarea que los algoritmos dados en [3] y [29], pero con cotas de complejidad menores a las de dichos algoritmos y sin necesidad de información adicional sobre la variedad considerada.

2.3.1 Cálculo de una forma de Chow de la componente equidimensional de V de dimensión $\dim V$

En esta sección se describe un algoritmo que, a partir de polinomios que definen una variedad proyectiva V de dimensión r, calcula una forma de Chow de su componente equidimensional de dimensión r.

Para comenzar, probaremos un lema que nos permitirá obtener, dada una variedad proyectiva arbitraria V, una relación entre un conjunto finito de polinomios que la define y una forma de Chow de su componente equidimensional de dimensión máxima.

Lema 2.3.1 *Sea $V \subseteq \mathbb{P}^n$ una variedad proyectiva de dimensión r y sea V_r la componente equidimensional de V de dimensión r. Para cada $0 \leq i \leq r$, sea $U_i = (U_{i0}, \ldots, U_{in})$ un grupo de $n+1$ nuevas variables y sea $L_i := U_{i0} X_0 + \cdots + U_{in} X_n$. Consideremos el conjunto $\Gamma(V) \subseteq (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n$ definido por*

$$\Gamma(V) = \{(u, x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \ / x \in V \wedge L_0(u_0, x) = 0 \wedge \ldots \wedge L_r(u_r, x) = 0\}$$

y la proyección $\pi_1 : (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \to (\mathbb{P}^n)^{r+1}$ sobre las primeras coordenadas. Entonces, $\pi_1(\Gamma(V))$ tiene codimensión 1 en $(\mathbb{P}^n)^{r+1}$ y cualquier polinomio libre de cuadrados que define su componente equidimensional de codimensión 1 es una forma de Chow de V_r.

Demostración. Para cada componente irreducible C de V, consideremos el conjunto $\Gamma(C) \subseteq (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n$ definido por

$$\Gamma(C) = \{(u, x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \ / \ x \in C \wedge L_0(u_0, x) = 0 \wedge \ldots \wedge L_r(u_0, x) = 0\}.$$

Observemos que $\Gamma(V) = \bigcup_C \Gamma(C)$, donde la unión recorre todas las componentes irreducibles de V.

Sean $\pi_1 : (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \to (\mathbb{P}^n)^{r+1}$ y $\pi_2 : (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \to \mathbb{P}^n$ las proyecciones canónicas. Se tiene entonces que $\pi_1(\Gamma(V)) = \bigcup_C \pi_1(\Gamma(C))$ (unión sobre todas las componentes irreducibles de V).

Sea C una componente irreducible de V. Analicemos el conjunto $\pi_1(\Gamma(C))$.

Si $\dim C = r$, entonces $\pi_1(\Gamma(C))$ es un conjunto cerrado de codimensión 1 en $(\mathbb{P}^n)^{r+1}$ (ver Sección 2.1).

Consideremos ahora el caso en que $\dim C < r$. Como $\pi_2(\Gamma(C)) = C$ y para cada $x \in C$, $\pi_2^{-1}(x) \cong (\mathbb{P}^{n-1})^{r+1} \times \{x\}$ es un conjunto irreducible de dimensión $(n-1)(r+1)$, entonces $\Gamma(C)$ es irreducible y $\dim \Gamma(C) = \dim \pi_2^{-1}(x) + \dim C < n(r+1) - 1$. Luego, $\dim \pi_1(\Gamma(C)) < n(r+1) - 1$.

Sea

$$\Gamma(V_r) := \{(u, x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \ / \ x \in V_r \wedge L_0(u_0, x) = 0 \wedge \ldots \wedge L_r(u_r, x) = 0\}.$$

Puesto que V_r es la unión de todas las componentes irreducibles de V de dimensión r, resulta que $\pi_1(\Gamma(V_r))$ es la componente equidimensional de $\pi_1(\Gamma(V))$ de codimensión 1.

Teniendo en cuenta que una forma de Chow de V_r es, por definición, un polinomio libre de cuadrados cuyo conjunto de ceros es $\pi_1(\Gamma(V_r))$, resulta que cualquier polinomio libre de cuadrados que defina la componente equidimensional de codimensión 1 de $\pi_1(\Gamma(V))$ es una forma de Chow de V_r.

El principal resultado de este capítulo se enuncia en el siguiente teorema.

Teorema 2.3.2 *Sean $F_1, \ldots, F_s \in k[X_0, \ldots, X_n]$ polinomios homogéneos y sea $d \geq n$ un entero tal que $\deg F_i \leq d$ $(1 \leq i \leq s)$. Sea*

$$V := \{x \in \mathbb{P}^n(\overline{k}) \ / \ F_1(x) = 0 \wedge \ldots \wedge F_s(x) = 0\}.$$

Sea r la dimensión proyectiva de V y sea V_r la componente equidimensional de V de dimensión r.

Entonces existe un algoritmo bien paralelizable de complejidad secuencial acotada por $s^{O(1)}d^{O(n)}$ que, tomando como entrada el conjunto de polinomios $\{F_1, \ldots, F_s\}$ codificados en forma densa produce un straight-line program de longitud $s^{O(1)}d^{O(n)}$ que calcula una forma de Chow $\mathcal{F}_{V_r}$ de V_r.

Demostración. El algoritmo consta de varios pasos.

- Cálculo de la dimensión de V.

El primer paso del algoritmo consiste en calcular $r = \dim V$, lo que puede hacerse por medio del algoritmo bien paralelizable de Giusti y Heintz con complejidad secuencial de orden $s^{O(1)}d^{O(n)}$ (ver [13]).

- Eliminación de cuantificadores.

El segundo paso del algoritmo consiste en la aplicación del algoritmo de eliminación de cuantificadores de [29] (ver Sección 1.4.2) a ciertas fórmulas relacionadas con la definición de la forma de Chow que se obtendrán a partir de la relación dada en el Lema 2.3.1.

Introducimos $r+1$ grupos $U_0, \ldots, U_r$ de $n+1$ nuevas variables, donde para cada $0 \leq i \leq r$, $U_i := (U_{i0}, \ldots, U_{in})$. Para cada i, $0 \leq i \leq r$, sea

$$L_i = U_{i0} X_0 + \cdots + U_{in} X_n.$$

Consideremos el conjunto $\Gamma(V) \subseteq (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n$ definido por

$$\Gamma(V) = \{(u,x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \ / \ F_1(x) = 0 \wedge \ldots \wedge F_s(x) = 0 \wedge \\ \wedge L_0(u_0,x) = 0 \wedge \ldots \wedge L_r(u_r,x) = 0\}.$$

Sea $\pi_1 : (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \to (\mathbb{P}^n)^{r+1}$ la proyección canónica sobre las primeras coordenadas.

Por el Lema 2.3.1, el conjunto $\pi_1(\Gamma(V))$ es un cerrado de codimensión 1 en $(\mathbb{P}^n)^{r+1}$ y una forma de Chow $\mathcal{F}_{V_r}$ de la componente equidimensional V_r de V de dimensión r es un polinomio libre de cuadrados que define la componente equidimensional de codimensión 1 de $\pi_1(\Gamma(V))$.

Con el objeto de aplicar el algoritmo de eliminación de cuantificadores mencionado, consideraremos las coordenadas homogéneas de los puntos en $\pi_1(\Gamma(V))$ como puntos en el espacio afín $\mathbb{A}^{(n+1)(r+1)}$.

Sea φ la fórmula

$$\exists x_0 \ldots \exists x_n : (x_0 \neq 0 \vee \ldots \vee x_n \neq 0) \wedge F_1(x_0,\ldots,x_n) = 0 \wedge \ldots \wedge F_s(x_0,\ldots,x_n) = 0 \\ \wedge L_0(u_{00},\ldots,u_{0n},x_0,\ldots,x_n) = 0 \wedge \ldots \wedge L_r(u_{r0},\ldots,u_{rn},x_0,\ldots,x_n) = 0$$

y sea $W \subseteq \mathbb{A}^{(n+1)(r+1)}$ el conjunto

$$W = \{(u_0,\ldots,u_r) \in \overline{k}^{(n+1)(r+1)} \ / \ \varphi(u_0,\ldots,u_r)\}.$$

Observemos que los polinomios en $k[U_0,\ldots,U_r]$ que definen $\pi_1(\Gamma(V))$ in $(\mathbb{P}^n)^{r+1}$, también definen W en $\mathbb{A}^{(n+1)(r+1)}$ y, por lo tanto, W es un conjunto cerrado. Más aún, la forma de Chow $\mathcal{F}_{V_r}$ que se quiere calcular es el polinomio libre de cuadrados que define la componente equidimensional de codimensión 1 de W en $\mathbb{A}^{(n+1)(r+1)}$.

Dado que los polinomios $F_1,\ldots,F_s,L_0,\ldots,L_r$ son homogéneos, la siguiente fórmula es equivalente a φ:

$$\bigvee_{k=0}^{n} \varphi_k$$

donde φ_k es la fórmula

$$\exists x_0 \ldots \exists x_{k-1} \exists x_{k+1} \ldots \exists x_n : F_1(x_0,\ldots,x_{k-1},1,x_{k+1},\ldots,x_n) = 0 \wedge \ldots \wedge \\ F_s(x_0,\ldots,x_{k-1},1,x_{k+1},\ldots,x_n) = 0 \wedge L_0(u_{00},\ldots,u_{0n},x_0,\ldots,x_{k-1},1,x_{k+1},\ldots,x_n) = 0 \\ \wedge \ldots \wedge L_r(u_{r0},\ldots,u_{rn},x_0,\ldots,x_{k-1},1,x_{k+1},\ldots,x_n) = 0.$$

Para cada k, $0 \leq k \leq n$, sea $W_k \subseteq \mathbb{A}^{(n+1)(r+1)}$ el conjunto definido por φ_k.
Como W es un conjunto cerrado, se tiene que

$$W = \bigcup_{k=0}^{n} W_k = \bigcup_{k=0}^{n} \overline{W_k}.$$

En consecuencia, las componentes irreducibles de W de codimensión 1 son precisamente las componentes irreducibles de codimensión 1 de cada uno de los conjuntos $\overline{W_k}$ $(0 \leq k \leq n)$.
Luego, para hallar el polinomio que define la componente equidimensional de codimensión 1 de W, trabajaremos con los conjuntos $\overline{W_k}$ $(0 \leq k \leq n)$.

Fijemos k, $0 \leq k \leq n$. La fórmula φ_k es una conjunción que involucra sólo fórmulas atómicas del tipo $f = 0$ con un solo bloque de cuantificadores existenciales. Observamos que φ_k involucra $s + r + 1$ polinomios en $(n+1)(r+1) + n$ variables, cuyos grados con respecto a $X_0, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n$ están acotados por $d \geq n$ y cuyos grados con respecto a las variables restantes están acotados por 1.
Aplicando el algoritmo descripto en [29, Theorem 3.2.1.] (ver Proposición 1.4.4) se obtiene una fórmula ψ_k, libre de cuantificadores, equivalente a φ_k, es decir, tal que

$$W_k = \{(u_0, \ldots, u_r) \in \overline{k}^{(n+1)(r+1)} \ / \ \psi_k(u_0, \ldots, u_r)\}$$

que involucra $t \leq s^{O(1)} d^{O(n)}$ polinomios de grados acotados por $d^{O(n)}$ $(1 \leq i \leq t)$ y estos polinomios están dados por un straight-line program de longitud $s^{O(1)} d^{O(n)}$.
La complejidad secuencial de este paso está acotada por $s^{O(1)} d^{O(n)}$.

- *Componente equidimensional de codimensión 1 de* $\overline{W_k}$ $(0 \leq k \leq n)$.
En este paso se calculará, para cada $0 \leq k \leq n$, un polinomio $G_k \in k[U_0, \ldots, U_r]$ que define la componente equidimensional de codimensión 1 del conjunto $\overline{W_k}$.

Sea k con $0 \leq k \leq n$. Para caracterizar las componentes irreducibles de codimensión 1 de $\overline{W_k}$ haremos uso de la existencia de una fórmula escrita en forma normal disyuntiva, equivalente a la fórmula ψ_k que define W_k, obtenida en el paso anterior.
Sean $H_1, \ldots, H_t \in k[U_0, \ldots, U_r]$ los polinomios que aparecen en ψ_k.
Sea $I = \{1, 2, \ldots, t\}$. Para cada $M \subseteq I$ sea

$$\mathcal{Z}_M := \{u \in \overline{k}^{(n+1)(r+1)} \ / \ H_i(u) = 0 \ \forall i \in M \wedge H_j(u) \neq 0 \ \forall j \in I - M\}.$$

Entonces existe un subconjunto S de $\{M \subseteq I \ / \ \mathcal{Z}_M \neq \emptyset\}$ tal que

$$W_k = \bigcup_{M \in S} \mathcal{Z}_M.$$

En consecuencia

$$\overline{W_k} = \bigcup_{M \in S} \overline{\mathcal{Z}_M}$$

y concluimos entonces que las componentes irreducibles de $\overline{W_k}$ de codimensión 1 son las componentes irreducibles de codimensión 1 de los conjuntos $\overline{\mathcal{Z}_M}$ con $M \subseteq S$.

Sea

$$S' := \{M \subseteq I \ / \ \mathcal{Z}_M \subseteq W_k \wedge \operatorname{codim} \overline{\mathcal{Z}_M} = 1\}.$$

Observamos que entonces la componente equidimensional de codimensión 1 de $\overline{W_k}$ es la unión de las componentes de codimensión 1 de todos los conjuntos $\overline{\mathcal{Z}_M}$, $M \in S'$.

Entonces, si para cada $M \in S'$, G_M denota un polinomio libre de cuadrados que define la componente equidimensional de codimensión 1 de $\overline{\mathcal{Z}_M}$, resulta que

$$G_k := \prod_{M \in S'} G_M$$

define la componente equidimensional de codimensión 1 de $\overline{W_k}$. Más aún, teniendo en cuenta que si $M_1 \neq M_2$, los conjuntos de componentes irreducibles de $\overline{\mathcal{Z}_{M_1}}$ y $\overline{\mathcal{Z}_{M_2}}$ son disjuntos, concluimos que G_k es libre de cuadrados.

El siguiente paso del algoritmo consiste en determinar cuáles de los conjuntos $\overline{\mathcal{Z}_M}$, $M \subseteq I$, tienen codimensión 1. El algoritmo que mostraremos encontrará también, para cada uno de estos conjuntos, un polinomio $G_M \in k[U_0, \ldots, U_r]$ cuyo conjunto de ceros sea la componente equidimensional de codimensión 1 de $\overline{\mathcal{Z}_M}$.

En primer lugar se obtendrá una cota superior para la cantidad de conjuntos $M \subseteq \{1, 2, \ldots, t\}$ tales que $\overline{\mathcal{Z}_M}$ tiene codimensión 1, lo que nos permitirá hallar una cota para la cantidad de pasos a realizar en esta etapa del algoritmo.

Sea $M \subseteq I$ uno de tales conjuntos, y sea C una componente irreducible de codimensión 1 de $\overline{\mathcal{Z}_M}$. Entonces, existe i $(1 \leq i \leq t)$ tal que C es una componente irreducible de $V(H_i)$. Teniendo en cuenta que la cantidad de componentes irreducibles de un conjunto cerrado está acotada por su grado, concluimos que hay a lo sumo $\sum_{i=1}^{t} \deg H_i$ componentes irreducibles de codimensión 1 entre todos los conjuntos $\overline{\mathcal{Z}_M}$ con $M \subseteq I$.

Puesto que si $M_1 \neq M_2$ los conjuntos de componentes irreducibles de $\overline{Z_{M_1}}$ y $\overline{Z_{M_2}}$ son disjuntos, la cantidad de conjuntos $M \subseteq I$ tales que $\operatorname{codim}(\overline{Z_M}) = 1$ también está acotada por $\sum_{i=1}^{t} \deg H_i$.

Para simplificar la notación, dados $M, N \subseteq I$, el conjunto

$$\{u \in \overline{k}^{(n+1)(r+1)} \ / \ H_i(u) = 0 \ \forall i \in M \ \wedge \ H_j(u) \neq 0 \ \forall j \in N\}$$

será denotado por

$$\{ \bigwedge_{i \in M} H_i = 0 \wedge \bigwedge_{j \in N} H_j \neq 0\}.$$

Podemos suponer que la cantidad t de polinomios que aparecen en ψ_k es de la forma 2^h para un entero positivo h (considerando $H_i \equiv 0$ para $t+1 \leq i \leq 2^{1+\lfloor \log(t-1) \rfloor}$ en caso de no serlo).

Para determinar los conjuntos M que nos interesan, se adapta un método que aparece en [10]:
En un primer paso se consideran los conjuntos

$$A_i^{(0)} := \{\{H_i = 0\}, \{H_i \neq 0\}\} \qquad (1 \leq i \leq t).$$

Se determina cuáles de los conjuntos $\{H_i = 0\}$ y $\{H_i \neq 0\}$ $(1 \leq i \leq t)$ son no vacíos para obtener

$$B_i^{(0)} := \{\Delta \in A_i^{(0)} \ / \ \Delta \neq \emptyset\} \qquad (1 \leq i \leq t).$$

En el siguiente paso, se consideran los conjuntos

$$A_i^{(1)} := \{\Delta_1 \cap \Delta_2 \ / \ \Delta_1 \in B_{2i-1}^{(0)} \wedge \Delta_2 \in B_{2i}^{(0)}\} \qquad (1 \leq i \leq \frac{t}{2}).$$

Se determina cuáles de los elementos de $A_i^{(1)}$ tienen clausuras de codimensión a lo sumo 1 para obtener

$$B_i^{(1)} := \{\Delta \in A_i^{(1)} \ / \ \operatorname{codim} \overline{\Delta} \leq 1\} \qquad (1 \leq i \leq \frac{t}{2}).$$

Suponiendo hallados los conjuntos $B_i^{(j)}$ $(1 \leq j \leq \log t - 1 \ , \ 1 \leq i \leq \frac{t}{2^j})$, se consideran los conjuntos

$$A_i^{(j+1)} := \{\Delta_1 \cap \Delta_2 \ / \ \Delta_1 \in B_{2i-1}^{(j)} \wedge \Delta_2 \in B_{2i}^{(j)}\} \qquad (1 \leq i \leq \frac{t}{2^{j+1}})$$

y se determina cuáles de los elementos del conjunto $A_i^{(j+1)}$ tienen clausuras de codimensión a lo sumo 1 para obtener

$$B_i^{(j+1)} := \{\Delta \in A_i^{(j+1)} \,/\, \text{codim } \overline{\Delta} \leq 1\} \qquad (1 \leq i \leq \frac{t}{2^{j+1}}).$$

Observemos que de esta manera, en $1 + \log t$ pasos, se obtendrá un único conjunto $B_1^{(\log t)}$ cuyos elementos son los conjuntos $\mathcal{Z}_M$ tales que $\overline{\mathcal{Z}_M}$ tiene codimensión a lo sumo 1.

Queda por ver cómo se determina si la clausura de un conjunto Δ de la forma

$$\Delta = \{ \bigwedge_{i \in M} H_i = 0 \wedge \bigwedge_{j \in N} H_j \neq 0\}$$

donde M, N son subconjuntos disjuntos de I, tiene codimensión a lo sumo 1.

Observemos que $\overline{\Delta} = \mathbb{A}^n$ si y sólo si Δ es un conjunto abierto y no vacío, lo que es equivalente a que

- $M = \emptyset$ o $H_i \equiv 0 \; \forall i \in M$ y
- $H_j \not\equiv 0 \quad \forall j \in N$

Estas condiciones pueden chequearse fácilmente, puesto que en el primer paso se determina cuáles de los polinomios es el polinomio nulo. (Esto puede efectuarse por medio de una sucesión de prueba.)

Supongamos entonces que $M \neq \emptyset$ y que existe $\ell \in M$ tal que $H_\ell \not\equiv 0$.

Sin pérdida de generalidad, se puede suponer que

$$H_i \not\equiv 0 \quad \forall i \in M \qquad \text{y} \qquad H_j \not\equiv 0 \quad \forall j \in N$$

Veamos cómo decidir si $\text{codim}(\overline{\Delta}) = 1$ o no:

Sea $H = \prod_{j \in N} H_j$ y, para cada $i \in M$, sea $H_i = \prod_{l=1}^{n_i} H_{il}^{\alpha_l}$ la factorización irreducible de H_i en $\overline{k}[U_0, \ldots, U_r]$. Supongamos que $M = \{i_1, \ldots, i_m\}$ y sea $\mathcal{P}_M = \{1, \ldots, n_{i_1}\} \times \ldots \times \{1, \ldots, n_{i_m}\}$.

Entonces

$$\overline{\Delta} = \bigcup_{(l_1, \ldots, l_m) \in \mathcal{P}_M} \overline{\{\bigwedge_{j=1}^{m} H_{i_j l_j} = 0 \wedge H \neq 0\}}$$

y, por lo tanto, la componente equidimensional de codimensión 1 de $\overline{\Delta}$ es la unión de las componentes equidimensionales de codimensión 1 de los conjuntos

$$\overline{\{\bigwedge_{j=1}^{m} H_{i_j l_j} = 0 \wedge H \neq 0\}}$$

con $(l_1, \ldots, l_m) \in \mathcal{P}_M$.

Observamos que, como los polinomios $H_{i_j l_j}$ son irreducibles y además

$$\overline{\{\bigwedge_{j=1}^{m} H_{i_j l_j} = 0 \wedge H \neq 0\}} \subseteq \{\bigwedge_{j=1}^{m} H_{i_j l_j} = 0\}, \tag{2.1}$$

si existe una componente de codimensión 1 en $\overline{\{\bigwedge_{j=1}^{m} H_{i_j l_j} = 0 \wedge H \neq 0\}}$, entonces todos los polinomios $H_{i_j l_j}$ que aparecen en (2.1) son el mismo (salvo por un factor constante).

Por otro lado, si existe un polinomio G tal que $H_{i_j l_j} = \lambda_j G$ para cada $1 \leq j \leq m$, entonces G es irreducible y en consecuencia,

$$\overline{\{G = 0 \wedge H \neq 0\}} = \begin{cases} \emptyset & \text{si } G \mid H \\ \{G = 0\} & \text{si no} \end{cases}$$

Por lo tanto, una componente irreducible de $\overline{\Delta}$ de codimensión 1 está definida por un factor común no constante de los polinomios H_i, $i \in M$, que no divide a H.

Luego, para determinar si $\overline{\Delta}$ tiene codimensión 1 sólo se necesita decidir si el polinomio

$$H_\Delta := \frac{\operatorname{rad}(\gcd(H_i,\ i \in M))}{\gcd(\operatorname{rad}(\gcd(H_i,\ i \in M)), H)} \tag{2.2}$$

es una constante no nula o no.

Más aún, en el caso en que H_Δ no sea constante, la componente equidimensional de $\overline{\Delta}$ de codimensión 1 es el conjunto de los ceros en $\bar{k}^{(n+1)(r+1)}$ del polinomio H_Δ.

Desde el punto de vista algorítmico, para calcular el polinomio H_Δ se procede de la siguiente manera:

1. Se consideran dos combinaciones lineales genéricas $\mathcal{H}_1$ y $\mathcal{H}_2$ de los polinomios H_i con $i \in M$

$$\mathcal{H}_1 := \sum_{i \in M} \alpha_i H_i \qquad \mathcal{H}_2 := \sum_{i \in M} \beta_i H_i$$

donde $(\alpha_i)_{i\in M}$ y $(\beta_i)_{i\in M}$ son nuevas indeterminadas. Aplicando la versión determinística del Lema 1.3.8 (ver Observación 1.3.9), se calcula un straight-line program para el máximo común divisor entre $\mathcal{H}_1$ y $\mathcal{H}_2$. Este polinomio coincide con $\gcd(H_i,\, i \in M)$.

2. Aplicando el Lema 1.3.11 según la Observación 1.3.12, se obtiene un straight-line program que calcula $\mathrm{rad}(\gcd(H_i,\, i \in M))$.

3. A partir del straight-line program calculado en 2. y de un straight-line program para H, se obtiene un straight-line program para $\gcd(\mathrm{rad}(\gcd(H_i,\, i \in M)), H)$ por medio del Lema 1.3.8 determinístico.

4. Se aplica el procedimiento de *Vermeidung von Divisionen* (ver Lema 1.3.5) para obtener un straight-line program que calcula un múltiplo escalar de H_Δ.

Finalmente, utilizando una sucesión de prueba apropiada, se determina si H_Δ es una constante no nula.

Para estimar la complejidad de este paso, recordemos que la cantidad de polinomios $H_1, \ldots, H_t$ involucrados en la definición de Δ está acotada por $t \leq s^{O(1)}d^{O(n)}$ y que $\deg H_i \leq d^{O(n)}$ para cada $1 \leq i \leq t$. Estos polinomios están dados por medio de un straight-line program de longitud $s^{O(1)}d^{O(n)}$.

Teniendo en cuenta las cotas de complejidad de los algoritmos utilizados en los pasos intermedios, concluimos que es posible determinar si $\overline{\Delta}$ tiene codimensión a lo sumo 1 en tiempo secuencial $s^{O(1)}d^{O(n)}$.

El algoritmo anterior se utiliza para determinar en cada uno de los pasos $0 \leq j \leq \log t$ y para cada $1 \leq i \leq \frac{t}{2^j}$, cuáles de los elementos de los conjuntos $A_i^{(j)}$ tienen clausuras de codimensión a lo sumo 1.

Como para cada $0 \leq j \leq \log t$ y cada $1 \leq i \leq \frac{t}{2^j}$, la cantidad de elementos de $B_i^{(j)}$ está acotada por la cantidad de conjuntos $M \subseteq I$ tales que $\overline{\mathcal{Z}_M}$ tiene codimensión a lo sumo 1, de la cota obtenida anteriormente para el número de estos conjuntos, resulta que la cantidad de elementos de $B_i^{(j)}$ $(0 \leq j \leq \log t,\ 1 \leq i \leq \frac{t}{2^j})$ está acotada por $\sum_{i=1}^{t} \deg H_i + 1 \leq s^{O(1)}d^{O(n)}$. Luego, para cada uno de los conjuntos $A_i^{(j)}$ el algoritmo para decidir si la clausura de uno de sus elementos Δ tiene codimensión 1 se aplica a lo sumo $s^{O(1)}d^{O(n)}$ veces.

Observemos también que la cantidad de conjuntos $A_i^{(j)}$ $(0 \leq j \leq \log t,\ 1 \leq i \leq \frac{t}{2^j})$ está acotada por $2t \leq s^{O(1)}d^{O(n)}$.
Por lo tanto, el conjunto $B_1^{(\log t)} = \{\mathcal{Z}_M \ / \ M \subseteq I,\ \text{codim}\ \overline{\mathcal{Z}_M} \leq 1\}$ se obtiene en tiempo secuencial $s^{O(1)}d^{O(n)}$.
Además, para cada $M \subseteq I$ tal que codim $\overline{\mathcal{Z}_M} = 1$, el algoritmo produce como resultado intermedio, un straight-line program de longitud $s^{O(1)}d^{O(n)}$ que representa un polinomio $G_M := H_{\mathcal{Z}_M}$ libre de cuadrados que define la componente equidimensional de codimensión 1 de $\overline{\mathcal{Z}_M}$.

Finalmente se determina, para cada uno de los elementos del conjunto $B_1^{(\log t)}$ hallado, cuáles de sus elementos son subconjuntos del conjunto W_k. Esto se hace utilizando la fórmula libre de cuantificadores ψ_k que define W_k, con cotas de complejidad del mismo orden que las de los pasos anteriores.

Recordemos que, si

$$S' = \{M \subseteq I \ / \ \mathcal{Z}_M \subseteq W_k \wedge \text{codim}\ \overline{\mathcal{Z}_M} = 1\},$$

el polinomio

$$G_k := \prod_{M \in S'} G_M$$

es un polinomio libre de cuadrados que define la componente equidimensional de codimensión 1 de $\overline{W_k}$.
Teniendo en cuenta que el cardinal de S' está acotado por $s^{O(1)}d^{O(n)}$ y las longitudes de los straight-line programs obtenidos para los polinomios G_M con $M \in S'$, vemos que G_k puede evaluarse por medio de un straight-line program de longitud $s^{O(1)}d^{O(n)}$.
La complejidad total de este paso es de orden $s^{O(1)}d^{O(n)}$.

- Cálculo de la forma de Chow de V_r.
El último paso del algoritmo consiste en el cálculo de una forma de Chow $\mathcal{F}_{V_r}$ para la componente equidimensional V_r de dimensión r de V, a partir de los polinomios G_k $(0 \leq k \leq n)$.

Recordemos que la forma de Chow $\mathcal{F}_{V_r}$ es un polinomio libre de cuadrados que define la componente equidimensional de codimensión 1 de $W = \bigcup_{k=0}^{n} \overline{W_k}$. Luego, el polinomio

$$\mathcal{F}_{V_r} := \text{rad}\Big(\prod_{k=0}^{n} G_k\Big)$$

es una forma de Chow para V_r.

A partir de los straight-line programs que evalúan los polinomios G_k $(0 \leq k \leq n)$ se calcula un straight-line program para $\prod_{k=0}^{n} G_k$ y finalmente, aplicando el Lema 1.3.11 y la Observación 1.3.12, se obtiene un straight-line program para $\mathcal{F}_{V_r}$.

De las cotas para la longitud de los straight-line programs que representan a los polinomios G_k $(0 \leq k \leq n)$ y del resultado enunciado en el Lema 1.3.11, se deduce que la longitud del del straight-line program que calcula $\mathcal{F}_{V_r}$ y la complejidad de este último paso del algoritmo están acotadas por $s^{O(1)}d^{O(n)}$.

La complejidad secuencial total del algoritmo es de orden $s^{O(1)}d^{O(n)}$.

2.3.2 Cálculo de la componente equidimensional de V de mayor dimensión

En esta sección se mostrará cómo obtener a partir de una forma de Chow de una variedad proyectiva equidimensional, un conjunto finito de polinomios que la define. Este procedimiento, junto con el algoritmo exhibido en la sección anterior nos permitirá, dada una variedad proyectiva arbitraria, encontrar polinomios que definen su componente equidimensional de mayor dimensión.

Lema 2.3.3 *Sea $V \subseteq \mathbb{P}^n$ una variedad proyectiva equidimensional de dimensión r y sea $\mathcal{F}_V \in k[U_0, \ldots, U_r]$ una forma de Chow de V. Supongamos que el polinomio $\mathcal{F}_V$ está dado por un straight-line program de longitud L.*

Entonces existen $N \leq 6(L+2(r+2)\,n\,(n+1))^2$ polinomios $Q_1, \ldots, Q_N$ cuyos grados están acotados por $(r+1)\deg V$, cada uno de los cuales puede ser evaluado mediante un straight-line program de longitud de orden $L + 2(r+1)\,n\,(n+1)$, tales que

$$V = \{x \in \mathbb{P}^n : Q_1(x) = 0 \wedge \ldots \wedge Q_N(x) = 0\}.$$

Demostración. Por la definición de forma de Chow para una variedad proyectiva equidimensional (ver Sección 2.1), vale la siguiente equivalencia en $\mathbb{P}^n$:

$$x \notin V \Longleftrightarrow \exists\, u_0, \ldots, u_r \in \mathbb{P}^n : L_0(u_0, x) = 0 \wedge \ldots \wedge \\ \wedge\, L_r(u_r, x) = 0 \wedge \mathcal{F}_V(u_0, \ldots, u_r) \neq 0$$

A partir de esta equivalencia se obtendrá una fórmula libre de cuantificadores que describe el conjunto $\mathbb{P}^n - V$.

Fijemos $x \in \mathbb{P}^n$ y sea $(x_0 : \ldots : x_n)$ un sistema de coordenadas homogéneas fijo de x. Consideremos el subespacio de $\overline{k}^{n+1}$ definido por la ecuación $x_0Y_0 + \cdots + x_nY_n = 0$. Denotamos por $e_j \in \overline{k}^{n+1}$ a la $(n+1)$-upla cuyas coordenadas son 0 excepto por la j-ésima que es 1. Para cada par (j,l), $0 \leq j < l \leq n$, sea

$$x_{jl} := x_l e_j - x_j e_l.$$

Observamos que $\{x_{jl}\,;\ 0 \leq j < l \leq n\}$ es un sistema de generadores del subespacio considerado. Entonces, para cada $0 \leq i \leq r$, la condición $L_i(u_i, x) = 0$ es equivalente a

$$\exists\, \alpha_{jl}^{(i)},\ 0 \leq j < l \leq n \ /\ u_i = \sum_{j,l} \alpha_{jl}^{(i)} x_{jl}$$

y en consecuencia

$$x \notin V \iff \exists\, \alpha_{jl}^{(i)},\ 0 \leq i \leq r,\ 0 \leq j < l \leq n \ /\ \mathcal{F}_V(\sum_{j,l} \alpha_{jl}^{(0)} x_{jl}, \ldots, \sum_{j,l} \alpha_{jl}^{(r)} x_{jl}) \neq 0.$$

Para cada $0 \leq i \leq r$ sea $A_i := (A_{jl}^{(i)})_{0 \leq j < l \leq n}$ un grupo de nuevas variables.

Sea $Q \in k[A_0, \ldots, A_r, X_0, \ldots, X_n]$ el polinomio

$$Q := \mathcal{F}_V\Big(\sum_{j,l} A_{jl}^{(0)}(X_l e_j - X_j e_l), \ldots, \sum_{j,l} A_{jl}^{(r)}(X_l e_j - X_j e_l)\Big).$$

Este polinomio puede evaluarse por medio de un straight-line program de longitud acotada por $L + 2(r+1)\,n\,(n+1)$.

Sea $\Omega := \{\omega_1, \ldots, \omega_N\}$ una correct test sequence para polinomios en las variables $A_0, \ldots, A_r$, de grado acotado por $(r+1)\deg V$, que pueden ser evaluados por medio de un straight-line program de longitud acotada por $L + 2(r+1)\,n\,(n+1)$. Entonces $N \leq 6(L + 2(r+2)\,n\,(n+1))^2$ y

$$x \notin V \iff \bigvee_{k=1}^{N} Q(\omega_k, x) \neq 0$$

Para cada $1 \leq k \leq N$, sea $Q_k := Q(\omega_k, X)$. Es claro que los polinomios $Q_1, \ldots, Q_N$ verifican las condiciones requeridas.

Estamos ahora en condiciones de deducir el segundo resultado del presente capítulo, que es una consecuencia inmediata del Teorema 2.3.2 y el Lema 2.3.3.

Proposición 2.3.4 *Sean $F_1, \ldots, F_s$ polinomios homogéneos en $k[X_0, \ldots, X_n]$ y sea $d \geq n$ un entero tal que* $\deg F_i \leq d$ $(1 \leq i \leq s)$. *Sea*

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

Sea $r = \dim V$ y sea V_r la componente equidimensional de V de dimensión r.

Entonces existe un algoritmo bien paralelizable de complejidad secuencial acotada por $s^{O(1)}d^{O(n)}$ cuyo input es el conjunto de polinomios $\{F_1, \ldots, F_s\}$ codificados en forma densa y cuyo output es un conjunto de $N \leq s^{O(1)}d^{O(n)}$ polinomios $Q_1, \ldots, Q_N$ de grados acotados por $(r+1)\,deg V_r$, dados por un straight-line program de longitud $s^{O(1)}d^{O(n)}$, tales que

$$V_r = \{x \in \mathbb{P}^n : Q_1(x) = 0 \wedge \ldots \wedge Q_N(x) = 0\}.$$

2.3.3 El caso afín

A continuación se adaptará el algoritmo dado en el Teorema 2.3.2 con el objeto de obtener, en el caso de una variedad algebraica afín, polinomios que definen la componente equidimensional de mayor dimensión de la variedad.

Consideremos la inmersión $\iota : \mathbb{A}^n \to \mathbb{P}^n$ definida por

$$\iota(x_1, \ldots, x_n) = (1 : x_1 : \ldots : x_n)$$

Si $W \subseteq \mathbb{A}^n$ es una variedad afín, llamaremos clausura proyectiva de W, y la denotaremos por $\overline{W}$, a la clausura de $\iota(W)$ en $\mathbb{P}^n$. Se tiene que $\dim W = \dim \overline{W}$ y $\deg W = \deg \overline{W}$.

Sean $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ polinomios de grados acotados por un entero $d \geq n$ y sea

$$V = \{x \in \mathbb{A}^n : f_1(x) = 0 \wedge \ldots \wedge f_s(x) = 0\}.$$

Sea $r = \dim V$ y sea V_r la componente equidimensional de V de dimensión r.

La componente equidimensional V_r de V se obtendrá a partir de la componente equidimensional $\overline{V}_r$ de mayor dimensión de la clausura proyectiva de V.

En una primera etapa, se calculará una forma de Chow para $\overline{V}_r$ a partir de los polinomios $f_1, \ldots, f_s$ que definen la variedad afín V y, utilizando la forma de Chow calculada, se obtendrá un conjunto finito de polinomios que define V_r.

Lema 2.3.5 *Sean $f_1, \ldots, f_s$ polinomios en $k[X_1, \ldots, X_n]$ y sea $d \geq n$ un entero tal que $\deg f_i \leq d$ $(1 \leq i \leq s)$. Sea $V = \{x \in \mathbb{A}^n : f_1(x) = 0 \wedge \ldots \wedge f_s(x) = 0\}$ y sea $r = \dim(V)$.*

Entonces existe un algoritmo bien paralelizable de complejidad secuencial acotada por $s^{O(1)}d^{O(n)}$ que, tomando como entrada el conjunto de polinomios $\{f_1, \ldots, f_s\}$ codificados en forma densa, produce un straight-line program de longitud $s^{O(1)}d^{O(n)}$ que calcula una forma de Chow para la componente equidimensional $\overline{V}_r$ de $\overline{V}$ de dimensión r.

Demostración. Para cada $1 \leq i \leq s$, sea $F_i \in k[X_0, \ldots, X_n]$ el polinomio que resulta de homogeneizar el polinomio $f_i \in k[X_1, \ldots, X_n]$ con respecto a una nueva variable X_0.

Sea U el conjunto

$$U = \{x \in \mathbb{P}^n(\overline{k}) \ / \ F_1(x) = 0 \wedge \ldots \wedge F_s(x) = 0 \wedge x_0 \neq 0\}.$$

Observamos que el conjunto $\overline{U}$ es la clausura proyectiva de V y, en consecuencia, $\dim \overline{U} = \dim V = r$.

Para un conjunto dado $A \subseteq \mathbb{P}^n$ denotaremos por $\Gamma(A)$ al conjunto

$$\Gamma(A) = \{(u, x) \in (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \ / \ x \in A \wedge L_0(u_0, x) = 0 \wedge \ldots \wedge L_r(u_r, x) = 0\}.$$

Sea $\pi : (\mathbb{P}^n)^{r+1} \times \mathbb{P}^n \longrightarrow (\mathbb{P}^n)^{r+1}$ la proyección sobre las primeras coordenadas.

Con esta notación, los argumentos dados en la demostración del Teorema 2.3.2 implican que la forma de Chow de la componente equidimensional $\overline{V}_r$ de $\overline{V}$ de mayor dimensión es un polinomio libre de cuadrados cuyo conjunto de ceros es la componente equidimensional de codimensión 1 de $\pi(\Gamma(\overline{U}))$.

Caracterizaremos entonces el conjunto $\pi(\Gamma(\overline{U}))$.

Afirmación: $\Gamma(\overline{U}) = \overline{\Gamma(U)}$.

Consideremos la variedad proyectiva $V^{(h)} \subseteq \mathbb{P}^n$ definida por

$$V^{(h)} := \{x \in \mathbb{P}^n(\overline{k}) \ / \ F_1(x) = 0 \wedge \ldots \wedge F_s(x) = 0\}$$

Sea $\mathcal{C}$ el conjunto de las componentes irreducibles de $V^{(h)}$, es decir, $V^{(h)} = \bigcup_{C \in \mathcal{C}} C$ la descomposición de $V^{(h)}$ en componentes irreducibles.

Sea $\mathcal{C}' := \{C \in \mathcal{C} : C \subseteq \{X_0 = 0\}\}$. Entonces

$$U = \bigcup_{C \notin \mathcal{C}'} (C \cap \{X_0 \neq 0\}) \qquad \text{y} \qquad \overline{U} = \bigcup_{C \notin \mathcal{C}'} C.$$

Teniendo en cuenta que, para cada conjunto cerrado irreducible C, el conjunto $\Gamma(C)$ es irreducible, se sigue que

$$\overline{\Gamma(U)} = \bigcup_{C \notin \mathcal{C}'} \overline{\Gamma(C \cap \{X_0 \neq 0\})} = \bigcup_{C \notin \mathcal{C}'} \Gamma(C) = \Gamma(\overline{U}).$$

Como la proyección π es una aplicación cerrada, resulta que

$$\pi(\Gamma(\overline{U})) = \pi(\overline{\Gamma(U)}) = \overline{\pi(\Gamma(U))}$$

Luego, para obtener una forma de Chow de $\overline{V}_r$, basta calcular un polinomio libre de cuadrados cuyo conjunto de ceros sea la componente equidimensional de codimensión 1 de $\overline{\pi(\Gamma(U))}$. Para hacer esto, se utilizarán las mismas técnicas que en la demostración del Teorema 2.3.2.

Se tiene que $\pi(\Gamma(U))$ es el conjunto definido en $(\mathbb{P}^n)^{r+1}$ por la fórmula

$$\begin{aligned}\exists x_0 \ldots \exists x_n : F_1(x_0, \ldots, x_n) = 0 \wedge \ldots \wedge F_s(x_0, \ldots, x_n) = 0 \wedge x_0 \neq 0 \wedge \\ \wedge L_0(u_{00}, \ldots, u_{0n}, x_0, \ldots, x_n) = 0 \wedge \ldots \wedge L_r(u_{r0}, \ldots, u_{rn}, x_0, \ldots, x_n) = 0\end{aligned}$$

que es equivalente a

$$\begin{aligned}\exists x_1 \ldots \exists x_n : f_1(x_1, \ldots, x_n) = 0 \wedge \ldots \wedge f_s(x_1, \ldots, x_n) = 0 \wedge \\ \wedge L_0(u_{00}, \ldots, u_{0n}, 1, x_1, \ldots, x_n) = 0 \wedge \ldots \wedge L_r(u_{r0}, \ldots, u_{rn}, 1, x_1, \ldots, x_n) = 0\end{aligned}$$

En un primer paso se aplica a esta fórmula el algoritmo de eliminación de cuantificadores descripto en [29] (ver Proposición 1.4.5) para obtener una fórmula libre de cuantificadores equivalente a la anterior. Luego se procede como en la demostración del Teorema 2.3.2 para calcular un polinomio libre de cuadrados $\mathcal{F}$ cuyo conjunto de ceros es la componente equidimensional de codimensión 1 de $\overline{\pi(\Gamma(U))}$. Este polinomio $\mathcal{F}$ es, por lo tanto, una forma de Chow de $\overline{V}_r$.

La complejidad secuencial del algoritmo está acotada por $s^{O(1)}d^{O(n)}$ y produce un straight-line program de longitud del mismo orden para $\mathcal{F}$.

Con la notación anterior, observamos que, aplicando los Lemas 2.3.5 y 2.3.3, se pueden obtener polinomios $Q_1, \ldots, Q_N$ tales que

$$\overline{V}_r = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n : Q_1(x_0, \ldots, x_n) = 0 \wedge \ldots \wedge Q_N(x_0, \ldots, x_n) = 0\}$$

a partir de los polinomios $f_1, \ldots, f_s$ que definen la variedad V.
Por lo tanto, podemos recuperar la componente equidimensional V_r de V de máxima dimensión como

$$V_r = \overline{V}_r \cap \mathbb{A}^n = \{x \in \mathbb{A}^n : Q_1(1, x_1, \ldots, x_n) = 0 \wedge \ldots \wedge Q_N(1, x_1, \ldots, x_n) = 0\}.$$

En consecuencia, hemos demostrado la siguiente Proposición:

Proposición 2.3.6 *Sean $f_1, \ldots, f_s$ polinomios en $k[X_1, \ldots, X_n]$ y sea $d \geq n$ un entero tal que* $\deg f_i \leq d$ $(1 \leq i \leq s)$. *Sea*

$$V := \{x \in \mathbb{A}^n : f_1(x) = 0 \wedge \ldots \wedge f_s(x) = 0\}.$$

Sea $r = \dim V$ y sea V_r la componente equidimensional de V de dimensión r.
Entonces existe un algoritmo bien paralelizable de complejidad secuencial acotada por $s^{O(1)}d^{O(n)}$ cuyo input es el conjunto de polinomios $\{f_1, \ldots, f_s\}$ codificados en forma densa y cuyo output es un conjunto finito de $N \leq s^{O(1)}d^{O(n)}$ polinomios $q_1, \ldots, q_N$ de grados acotados por $(r+1)\deg(V_r)$ dados por un straight-line program de longitud $s^{O(1)}d^{O(n)}$, tales que

$$V_r = \{x \in \mathbb{A}^n : q_1(x) = 0 \wedge \ldots \wedge q_N(x) = 0\}.$$

Observación 2.3.7 A partir de los resultados anteriores y del algoritmo de eliminación de cuantificadores para conjunciones con un solo bloque de cuantificadores existenciales dado en la Proposición 1.4.5, se deduce la existencia de un algoritmo bien paralelizable que, dados polinomios $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ de grados acotados por $d \geq n$ que definen una variedad algebraica V, decide si V es equidimensional o no. La complejidad secuencial del algoritmo es de orden $s^{O(1)}d^{O(n)}$:

Aplicando el algoritmo descripto en la Proposición 2.3.6, se obtienen $N \leq s^{O(1)}d^{O(n)}$ polinomios $q_1, \ldots, q_N$ que definen V_r, la componente equidimensional de mayor dimensión de V.

Observamos que V es equidimensional si y sólo si $V - V_r = \emptyset$.

Puesto que

$$V - V_r = \{x \in \mathbb{A}^n : f_1(x) = 0 \wedge \ldots \wedge f_s(x) = 0 \wedge (q_1(x) \neq 0 \vee \ldots \vee q_N(x) \neq 0)\}$$

aplicando el algoritmo de eliminación de cuantificadores mencionado a la fórmula

$$\exists x_1 \ldots \exists x_n (\bigvee_{k=1}^{N} f_1 = 0 \wedge \ldots \wedge f_s = 0 \wedge q_k(x) \neq 0)$$

se puede decidir si $V - V_r$ es vacío o no.

Teniendo en cuenta que, para cada $1 \leq k \leq N$, $\deg q_k \leq (r+1)\, d^n$, resulta que la complejidad secuencial del algoritmo está acotada por $s^{O(1)} d^{O(n)}$.

Este procedimiento puede ser aplicado en el caso proyectivo con las mismas cotas de complejidad.

Capítulo 3

Descomposición equidimensional efectiva

3.1 Descomposición de variedades algebraicas

Una manera de describir el conjunto de las soluciones de un sistema de ecuaciones polinomiales consistente, es decir la variedad algebraica V que definen dichos polinomios, es caracterizar cada una de las componentes irreducibles o equidimensionales de la variedad V.

Si V está definida por polinomios con coeficientes en un cuerpo k que no es algebraicamente cerrado, las componentes irreducibles (sobre $\bar{k}$) de V no necesariamente están definidas por polinomios con coeficientes en k. Esto dice que, trabajando en el cuerpo de base k, no es siempre posible obtener algorítmicamente polinomios que definen cada una de las componentes irreducibles sobre $\bar{k}$ de V.

Una posibilidad es entonces describir las componentes de V irreducibles sobre k. Chistov y Grigor'ev exhiben en [4] un algoritmo para el cálculo de la descomposición de una variedad en componentes irreducibles sobre k, que depende de manera fundamental de la existencia de un algoritmo de factorización de polinomios multivariados a coeficientes en k.

Otra forma de describir una variedad es por medio de sus componentes equidimensionales. Cabe destacar que, si V está definida por polinomios con coeficientes en un cuerpo k, cada una de las componentes equidimensionales de V puede definirse también por polinomios a coeficientes en k.

Giusti y Heintz presentan en [12] un algoritmo que obtiene la descomposición equidi-

mensional de una variedad algebraica V a partir de un conjunto finito de polinomios que la define. Si la variedad V está definida por s polinomios en n variables de grados acotados por d, la complejidad de este algoritmo es de orden $s^{O(1)}d^{O(n^2)}$. Cabe destacar que el algoritmo de [4] obtiene la descomposición equidimensional con cotas de complejidad del mismo orden.

Elkadi y Mourrain dan en [7] un algoritmo probabilístico basado en matrices bezoutianas, pero la descomposición que obtienen no es minimal, es decir, las subvariedades equidimensionales de V que caracterizan pueden tener componentes irreducibles que no son componentes irreducibles de V (sino que están contenidas en componentes irreducibles de V de dimensión mayor).

En [27], Lecerf construye un algoritmo, también probabilístico, que produce en tiempo polinomial la descomposición equidimensional de una variedad arbitraria por medio del cálculo de una resolución geométrica de cada una de sus componentes equidimensionales.

Una de las principales diferencias entre los trabajos mencionados es la forma en que se describe cada componente equidimensional de la variedad: en [7] y [27] las variedades se describen en forma paramétrica y esta descripción es genérica (caracteriza todos los puntos que están fuera de cierta hipersuperficie), mientras que en [12] las variedades están dadas como el conjunto de los ceros comunes de un conjunto finito de polinomios lo que caracteriza *todos* los puntos de la variedad. Chistov y Grigor'ev obtienen en [4] descripciones de los dos tipos.

En este capítulo consideraremos el problema de calcular la descomposición equidimensional de una variedad V obteniendo una descripción exacta de cada componente equidimensional, más precisamente:

Dados polinomios $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ que definen una variedad algebraica

$$V = \{x \in \bar{k}^n : f_1(x) = 0, \ldots, f_s(x) = 0\},$$

obtener, para cada $0 \leq \ell \leq \dim V$, un conjunto finito de polinomios cuyo conjunto de ceros comunes sea la componente equidimensional V_ℓ de dimensión ℓ de V.

3.2 Resultados obtenidos

Se construye un algoritmo probabilístico que calcula, a partir de un conjunto finito de polinomios que define una variedad algebraica V, la descomposición de V en componentes equidimensionales.

Si V está definida por s polinomios en n variables de grados acotados por un entero $d \geq n$ y $V = \bigcup_{\ell=0}^{r} V_\ell$ es la descomposición equidimensional de V, el algoritmo obtiene en tiempo secuencial acotado por $s^{O(1)}d^{O(n)}$, para cada $0 \leq \ell \leq r$, un conjunto de $n+1$ polinomios de grados acotados por $\deg(V_\ell)$ que define V_ℓ.
Observamos que la complejidad de este algoritmo es menor que la de los algoritmos conocidos que resuelven este mismo problema.

3.3 Preprocesamiento de los datos

3.3.1 Modificación de los polinomios de entrada

El primer paso del algoritmo consiste en definir la variedad afín cuya descomposición equidimensional se quiere calcular por medio de $n+1$ polinomios. Más aún, pediremos que estos $n+1$ polinomios satisfagan ciertas condiciones adicionales sobre dimensión.
Esto se conseguirá eligiendo combinaciones lineales aleatorias de los polinomios de entrada. En el siguiente lema, que es una adaptación de un lema de [13], se prueba la existencia y genericidad de combinaciones lineales que satisfacen las condiciones requeridas.

Lema 3.3.1 *Sean $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ polinomios y sea V la variedad afín $V = \{x \in \bar{k}^n : f_1(x) = 0 \wedge \ldots \wedge f_s(x) = 0\}$. Entonces existen elementos $t_{ij} \in k$ $(1 \leq i \leq n+1,\ 1 \leq j \leq s)$ tales que los polinomios $\hat{f}_1, \ldots, \hat{f}_{n+1}$ definidos por*

$$\hat{f}_i = t_{i1}f_1 + \cdots + t_{is}f_s \qquad (1 \leq i \leq n+1)$$

satisfacen la siguiente condición para cada h, $1 \leq h \leq n+1$:

(*) La dimensión de toda componente irreducible de

$$V(\hat{f}_1, \ldots, \hat{f}_h) = \{x \in \bar{k}^n : \hat{f}_1(x) = 0 \wedge \ldots \wedge \hat{f}_h(x) = 0\}$$

que no está incluida en V es $n-h$.

Demostración. Probaremos, por inducción en h, la existencia de elementos $t_{ij} \in k$ $(1 \leq i \leq h,\ 1 \leq j \leq s)$ tales que los polinomios $\hat{f}_1, \ldots, \hat{f}_h$ definidos por

$$\hat{f}_i = t_{i1}f_1 + \cdots + t_{is}f_s \qquad (1 \leq i \leq h)$$

satisfacen la condición (*).

Sean T_j $(1 \leq j \leq s)$ nuevas indeterminadas sobre k.

Si $h = 1$, sea $p \in \mathbb{A}^n - V$ y sea $P_1 \in k[T_1, \ldots, T_s]$ el polinomio

$$P_1 = T_1.f_1(p) + \cdots + T_s.f_s(p).$$

Entonces, para cada elección de $t_{11}, \ldots, t_{1s}$ tal que $P_1(t_{11}, \ldots, t_{1s}) \neq 0$, el polinomio $\hat{f}_1$ satisface la condición $(*)$.

Supongamos ahora que existen elementos t_{ij} $(1 \leq i \leq h,\ 1 \leq j \leq s)$ tales que los polinomios $\hat{f}_1, \ldots, \hat{f}_h$ satisfacen la condición $(*)$. Consideremos la variedad

$$V(\hat{f}_1, \ldots, \hat{f}_h) = \{x \in \bar{k}^n : \hat{f}_1(x) = 0 \wedge \ldots \wedge \hat{f}_h(x) = 0\}.$$

Sea C_h el conjunto de las componentes irreducibles de $V(\hat{f}_1, \ldots, \hat{f}_h)$ no contenidas en V.

Si $C_h = \emptyset$, cualquier elección de $t_{h+1\,1}, \ldots, t_{h+1\,s}$ da lugar a un polinomio $\hat{f}_{h+1}$ que satisface la condición requerida.

Si $C_h \neq \emptyset$, para cada $C \in C_h$, consideremos un punto $p_C \in C - V$. Sea $P_{h+1} \in k[T_1, \ldots, T_s]$ el polinomio

$$P_{h+1} = \prod_{C \in C_h} (T_1.f_1(p_C) + \cdots + T_s.f_s(p_C)).$$

Este polinomio no es el polinomio nulo y todo punto $(t_{h+1\,1}, \ldots, t_{h+1\,s})$ en k^n tal que $P_{h+1}(t_{h+1\,1}, \ldots, t_{h+1\,s}) \neq 0$ define un polinomio $\hat{f}_{h+1}$ que no es idénticamente nulo sobre ninguna componente $C \in C_h$. Luego, para cada $C \in C_h$ se tiene que $C \cap V(\hat{f}_{h+1}) = \emptyset$ o $\dim(C \cap V(\hat{f}_{h+1})) = n - h - 1$, de donde se deduce que los polinomios $\hat{f}_1, \ldots, \hat{f}_{h+1}$ satisfacen la condición $(*)$.

Observación 3.3.2 La condición que define los elementos t_{1j} $(1 \leq j \leq s)$ para los cuales $\hat{f}_1$ satisface la condición $(*)$ del Lema 3.3.1 es abierta. Para cada h $(1 \leq h \leq n)$, si se han elegido t_{ij} $(1 \leq i \leq h, 1 \leq j \leq s)$ tales que los polinomios $\hat{f}_1, \ldots, \hat{f}_h$ satisfacen $(*)$, la condición para elegir t_{h+1j} $(1 \leq j \leq s)$ de manera que $\hat{f}_1, \ldots, \hat{f}_h, \hat{f}_{h+1}$ satisfagan $(*)$ también es abierta.

Más aún, si los grados totales de los polinomios $f_1, \ldots, f_s$ están acotados por un entero d, de la desigualdad de Bézout se deduce que, para cada h $(1 \leq h \leq n+1)$, el grado del polinomio P_h que aparece en la demostración del Lema 3.3.1 está acotado

por d^{h-1}. Entonces, por el Lema 1.3.2, si los elementos t_{ij} $(1 \leq i \leq n+1, 1 \leq j \leq s)$ se eligen aleatoriamente de un subconjunto de k con N elementos, la probabilidad de que los polinomios $\hat{f}_1, \ldots, \hat{f}_{n+1}$ satisfagan la condición (*) enunciada en el Lema 3.3.1 para todo $1 \leq h \leq n+1$, es al menos

$$\prod_{h=1}^{n+1} \left(1 - \frac{d^{h-1}}{N}\right) \geq 1 - \sum_{h=1}^{n+1} \frac{d^{h-1}}{N} \geq 1 - \frac{2d^n}{N}.$$

3.3.2 Posición de Noether de las variables

Supongamos dados s polinomios $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ con grados totales acotados por un entero $d \geq n$. Denotamos por V al conjunto de sus ceros comunes en $\mathbb{A}^n$. Aplicando el Lema 3.3.1 podemos suponer, por medio de una elección aleatoria de combinaciones lineales genéricas de los polinomios de entrada, que tenemos $n+1$ polinomios $\hat{f}_1, \ldots, \hat{f}_{n+1} \in k[X_1, \ldots, X_n]$ de grados acotados por d tales que:

(P1) $V(\hat{f}_1, \ldots, \hat{f}_{n+1}) = V$.

(P2) Para cada $0 \leq \ell \leq n-1$, la dimensión de cada componente irreducible de $V(\hat{f}_1, \ldots, \hat{f}_{n-\ell})$ no incluida en V es ℓ.

Sea $r := \dim V$ y sea $V = \bigcup_{i=0}^{r} V_i$ la descomposición equidimensional de V, donde, para cada $0 \leq i \leq r$, o bien $V_i = \emptyset$ o bien V_i es equidimensional con $\dim V_i = i$.

Observamos que, como consecuencia de la condición (P2), la descomposición equidimensional de $V(\hat{f}_1, \ldots, \hat{f}_{n-\ell})$ para $\ell \leq r$ es

$$V(\hat{f}_1, \ldots, \hat{f}_{n-\ell}) = V_r \cup \ldots \cup V_{\ell+1} \cup V'_\ell,$$

donde $V'_\ell = V_\ell \cup Z_\ell$ y Z_ℓ es o bien vacía o bien una variedad equidimensional de dimensión ℓ sin componentes irreducibles en común con V_ℓ.

Elegiremos ahora un cambio lineal de variables de manera que las nuevas variables $\widetilde{X}_1, \ldots, \widetilde{X}_n$ verifiquen simultáneamente:

(V1) La proyección $\pi_r : V_r \cup Z_r \to \mathbb{A}^r$ definida por $\pi_r(x) = (\tilde{x}_1, \ldots, \tilde{x}_r)$ es finita.

(V2) Para cada ℓ $(1 \leq \ell \leq r-1)$, si $Z_{\ell+1} \cap V(\hat{f}_{n-\ell})$ es no vacía, la proyección $\pi_\ell : Z_{\ell+1} \cap V(\hat{f}_{n-\ell}) \to \mathbb{A}^\ell$ definida por $\pi_\ell(x) = (\tilde{x}_1, \ldots, \tilde{x}_\ell)$ es finita.

Esto significa que las nuevas variables $\widetilde{X}_1, \ldots, \widetilde{X}_n$ están en posición de Noether con respecto a las variedades $V_r \cup Z_r$ y $Z_{\ell+1} \cap V(\hat{f}_{n-\ell})$ para cada $1 \leq \ell \leq r-1$, simultáneamente.

El siguiente lema garantiza la existencia de este cambio de variables:

Lema 3.3.3 *Sea $W \subseteq \mathbb{A}^n$ una variedad equidimensional definida sobre k y sea ℓ la dimensión de W. Sean U_{ij} $(1 \leq i \leq n,\ 0 \leq j \leq n)$ indeterminadas sobre $k[X_1, \ldots, X_n]$. Entonces existe un polinomio $G \in k[U_{ij}]_{\substack{1 \leq i \leq \ell \\ 0 \leq j \leq n}} - \{0\}$ con $\deg G \leq 2\,\ell\,(\deg W)^2$ tal que, si $G(u_{ij}) \neq 0$, el morfismo $\pi : W \to \mathbb{A}^\ell$ definido por*

$$\pi(x) = (u_{10} + u_{11}x_1 + \cdots + u_{1n}x_n, \ldots, u_{\ell 0} + u_{\ell 1}x_1 + \cdots + u_{\ell n}x_n)$$

es finito.

Demostración. Es una consecuencia inmediata de [25, Proposition 4.5, Lemma 2.13]. □

El lema anterior provee una condición para obtener un conjunto de variables libres con respecto a una variedad equidimensional dada, que pueda extenderse a un sistema completo de variables que se encuentre en posición de Noether con respecto a la variedad. Para obtener el conjunto completo de nuevas variables, consideraremos también el polinomio $H := \det(U_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$.

Aplicando el Lema 3.3.3 a nuestra situación y la desigualdad de Bézout para acotar los grados de las variedades que aparecen, se deduce la existencia de

- un polinomio G_r con $\deg G_r \leq 2\,r\,(\deg(Z_r \cup V_r))^2 \leq 2\,r\,d^{2(n-r)}$ y,
- para cada ℓ $(1 \leq \ell \leq r-1)$ un polinomio G_ℓ con

$$\deg G_\ell \leq 2\,\ell\,(\deg(Z_{\ell+1} \cap \{\hat{f}_{n-\ell} = 0\}))^2 \leq 2\,\ell\,d^{2(n-\ell)}$$

tales que, si $H(u_{ij}).\prod_{\ell=1}^{r} G_\ell(u_{ij}) \neq 0$, entonces las nuevas variables

$$\widetilde{X}_i = u_{i0} + u_{i1}X_1 + \cdots + u_{in}X_n \qquad (1 \leq i \leq n)$$

verifican las condiciones (V1) y (V2).

Observación 3.3.4 La condición que asegura que un cambio de variables verifica las condiciones de posición de Noether requeridas es abierta. Como $d \geq n$, el grado del polinomio $H.\prod_{\ell=1}^{r} G_\ell \in k[U_{ij}]_{\substack{1\leq i\leq n\\ 0\leq j\leq n}}$ está acotado por d^{2n}. Entonces, si los elementos u_{ij} $(1 \leq i \leq n,\ 0 \leq j \leq n)$ se eligen aleatoriamente de un subconjunto de k con N elementos, la probabilidad de que el cambio de variables que definen satisfaga las condiciones (V1) y (V2) es al menos $1 - \frac{d^{2n}}{N}$.

3.4 Descomposición equidimensional

3.4.1 Descripción de variedades equidimensionales

El algoritmo para la descomposición equidimensional que se presentará se basa esencialmente en la posibilidad de describir una variedad equidimensional arbitraria en $\mathbb{A}^n$ como el conjunto de los ceros comunes de $n+1$ polinomios de grados acotados. En esta sección mostraremos cómo puede obtenerse una descripción de este tipo.

Sea $W \subset \mathbb{A}^n(\bar{k})$ una variedad equidimensional de dimensión $\ell < n$ definible por polinomios en $k[X_1, \ldots, X_n]$. Supongamos que las variables $X_1, \ldots, X_n$ están en posición de Noether con respecto a W (es decir, que la proyección $\pi : W \to \mathbb{A}^\ell$ definida por $\pi(x) = (x_1, \ldots, x_\ell)$ es finita).
Dada una forma lineal $y = \lambda_{\ell+1}X_{\ell+1} + \cdots + \lambda_n X_n$ con $\lambda_{\ell+1}, \ldots, \lambda_n \in k$, consideramos el morfismo $\pi_y : \mathbb{A}^n \to \mathbb{A}^{\ell+1}$ definido por $\pi_y(x) = (x_1, \ldots, x_\ell, y(x))$. La imagen de W por π_y es una hipersuperficie en $\mathbb{A}^{\ell+1}$ y, en consecuencia, está definida por un polinomio libre de cuadrados $m_y \in k[X_1, \ldots, X_\ell, Y]$ unívocamente determinado salvo por un factor constante. Más aún, m_y es mónico en la variable Y y su grado total está acotado por el grado de la variedad W (ver [17, Lemmas 2 y 3] o [30, Proposition 1]). Llamaremos a m_y el *polinomio minimal de y con respecto a W*.

A continuación mostraremos que W puede definirse a partir de los polinomios minimales de $n+1$ formas lineales convenientemente elegidas.

Lema 3.4.1 *Sea $W \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión $\ell < n$. Supongamos que las variables $X_1, \ldots, X_n$ están en posición de Noether con respecto a W. Entonces existen $n+1$ formas lineales*

$$y_i = \lambda_{\ell+1}^{(i)} X_{\ell+1} + \cdots + \lambda_n^{(i)} X_n \qquad (1 \leq i \leq n+1)$$

con $\lambda_j^{(i)} \in k$ $(1 \leq i \leq n+1, \ell+1 \leq j \leq n)$ *tales que* W *es el conjunto de los ceros comunes de los polinomios que resultan, para cada* $1 \leq i \leq n+1$, *de especializar en la forma lineal* y_i, *el polinomio minimal de* y_i *con respecto a* W, *es decir*

$$W = \{x \in \bar{k}^n : m_{y_1}(x_1, \ldots, x_\ell, y_1(x)) = 0, \ldots, m_{y_{n+1}}(x_1, \ldots, x_\ell, y_{n+1}(x)) = 0\}.$$

Demostración. La existencia de las formas lineales se probará inductivamente:

Sea $y_1 = \lambda_{\ell+1}^{(1)} X_{\ell+1} + \cdots + \lambda_n^{(1)} X_n$ una forma lineal no nula, y sea m_{y_1} su polinomio minimal con respecto a W. Entonces $V(m_{y_1}) := V(m_{y_1}(X_1, \ldots, X_\ell, y_1)) \subseteq \mathbb{A}^n$ es una variedad equidimensional de dimensión $n-1$ tal que $W \subseteq V(m_{y_1})$.

Supongamos que se tienen j formas lineales $y_1, \ldots, y_j$ tales que W es un subconjunto de

$$V(m_{y_1}, \ldots, m_{y_j}) := V(m_{y_1}(X_1, \ldots, X_\ell, y_1), \ldots, m_{y_j}(X_1, \ldots, X_\ell, y_j))$$

y cada componente irreducible de $V(m_{y_1}, \ldots, m_{y_j})$ que no está incluida en W tiene dimensión $n-j$.

Sea $\mathcal{C}_j$ el conjunto de las componentes irreducibles de $V(m_{y_1}, \ldots, m_{y_j})$ no incluidas en W.

Si $\mathcal{C}_j = \emptyset$, sea $y_{j+1} = \lambda_{\ell+1}^{(j+1)} X_{\ell+1} + \cdots + \lambda_n^{(j+1)} X_n$ una forma lineal arbitraria.

Si $\mathcal{C}_j \neq \emptyset$, para cada componente $C \in \mathcal{C}_j$, consideremos un punto $x_C \in C - W$.

Sea $\pi : \mathbb{A}^n \to \mathbb{A}^\ell$ la proyección canónica sobre las primeras ℓ-coordenadas. Para cada $C \in \mathcal{C}_j$, consideremos el conjunto finito $M_C = \pi^{-1}(\pi(x_C)) \cap W$.

Tomamos cualquier forma lineal $y_{j+1} = \lambda_{\ell+1}^{(j+1)} X_{\ell+1} + \cdots + \lambda_n^{(j+1)} X_n$ tal que

$$y_{j+1}(x) \neq y_{j+1}(x_C) \qquad \forall\, x \in M_C \ \forall\, C \in \mathcal{C}_j.$$

Observemos que esta condición implica que, para cada x_C $(C \in \mathcal{C}_j)$, el polinomio minimal $m_{y_{j+1}}$ de y_{j+1} con respecto a W, especializado en y_{j+1}, no se anula en x_C.

Luego, cada componente irreducible de

$$V(m_{y_1}, \ldots, m_{y_{j+1}}) := V(m_{y_1}(X_1, \ldots, X_\ell, y_1), \ldots, m_{y_{j+1}}(X_1, \ldots, X_\ell, y_{j+1}))$$

que no está incluida en W tiene dimensión $n-j-1$.

En el paso $n+1$ se tendrá entonces una variedad $V(m_{y_1}, \ldots, m_{y_{n+1}})$ que contiene a W y que no posee componentes irreducibles que no están incluidas en W, de donde $W = V(m_{y_1}, \ldots, m_{y_{n+1}})$.

Observación 3.4.2 Analicemos las condiciones dadas en el Lema anterior para la elección de las formas lineales:

- y_1 puede ser cualquier forma lineal no nula.
- Supongamos elegidas j formas lineales $y_1, \ldots, y_j$ tales que cada componente irreducible de $V(m_{y_1}, \ldots, m_{y_j})$ no incluida en W tiene dimensión $n-j$. Con la notación del Lema, la condición que se pide a y_{j+1} es equivalente a

$$\prod_{C \in C_j} \prod_{x \in M_C} y_{j+1}(x - x_C) \neq 0,$$

que es una expresión polinomial en $\lambda_{\ell+1}^{(j+1)}, \ldots, \lambda_n^{(j+1)}$ de grado acotado por $(\deg W)^{j+1}$.

Entonces, si los coeficientes $\lambda_{\ell+1}^{(i)}, \ldots, \lambda_n^{(i)}$ $(1 \leq i \leq n+1)$ se eligen aleatoriamente de un subconjunto de k con N elementos, la probabilidad de que la variedad W quede definida por los polinomios minimales de las $n+1$ formas lineales asociadas (evaluados en las formas lineales correspondientes) es al menos

$$1 - \frac{2\,(\deg W)^{n+1}}{N}.$$

3.4.2 Cambio del cuerpo de base

En esta sección mostraremos la relación existente entre la descomposición irreducible de una variedad algebraica y la descomposición irreducible de la variedad definida por los mismos polinomios en un espacio afín asociado a una extensión del cuerpo de base.

Como esta situación será considerada en distintas etapas del algoritmo, la estudiaremos en el caso general.

Notación: Sea $\ell < n$ y sea $S = \bar{k}[X_1, \ldots, X_\ell] - \{0\}$. Dada una variedad $W \subset \mathbb{A}^n(\bar{k})$, denotaremos por $\widetilde{W} \subset \mathbb{A}^{n-\ell}(\overline{k(X_1, \ldots, X_\ell)})$ la variedad definida por el ideal $S^{-1}I(W)$.

Notar que si la variedad $W \subset \mathbb{A}^n(\bar{k})$ está definida por un ideal $J \subset \bar{k}[X_1, \ldots, X_n]$, entonces $\widetilde{W} \subset \mathbb{A}^{n-\ell}(\overline{k(X_1, \ldots, X_\ell)})$ está definida por $S^{-1}J$.

Sea I un ideal en $\bar{k}[X_1, \ldots, X_n]$ y sea $V(I)$ la variedad definida por I en $\mathbb{A}^n(\bar{k})$. Sea ℓ un entero tal que, para cada componente irreducible C de $V(I)$, $\dim C \geq \ell$.

Supongamos que las variables $X_1, \ldots, X_\ell$ son libres con respecto a cada componente irreducible de $V(I)$.

Sea $V(I) = \bigcup_{i=1}^{t} C_i$ la descomposición irreducible minimal de $V(I)$ en $\mathbb{A}^n(\bar{k})$. Entonces, considerando los ideales asociados, se tiene que

$$rad(I) = \bigcap_{i=1}^{t} I(C_i) \text{ en } \bar{k}[X_1, \ldots, X_n].$$

Como las variables $X_1, \ldots, X_\ell$ son libres con respecto a cada componente irreducible de $V(I)$, entonces para cada i, $1 \leq i \leq t$, se tiene que $S \cap I(C_i) = \emptyset$. Localizando en S se obtiene

$$S^{-1} rad(I) = \bigcap_{i=1}^{t} S^{-1} I(C_i),$$

que es una descomposición minimal de $S^{-1} rad(I)$ en $\bar{k}(X_1, \ldots, X_\ell)[X_{\ell+1}, \ldots, X_n]$ como intersección de ideales primos.

Entonces, la descomposición irreducible minimal de $\tilde{V}(I)$ en la $\bar{k}(X_1, \ldots, X_\ell)$-topología de Zariski de $\mathbb{A}^{n-\ell}(\overline{k(X_1, \ldots, X_\ell)})$ es

$$\tilde{V}(I) = \bigcup_{i=1}^{t} \tilde{C}_i.$$

Observar que, para cada $1 \leq i \leq t$, $\dim(\tilde{C}_i) = \dim(C_i) - \ell$.

Consideremos ahora la $\overline{k(X_1, \ldots, X_\ell)}$-topología de Zariski de $\mathbb{A}^{n-\ell}(\overline{k(X_1, \ldots, X_\ell)})$. Para cada i $(1 \leq i \leq t)$, todas las componentes irreducibles de $\tilde{C}_i$ tienen la misma dimensión (que es $\dim(\tilde{C}_i)$). Más aún, es fácil ver que, si $i \neq j$, ninguna componente irreducible de $\tilde{C}_i$ está incluida en $\tilde{C}_j$.

En otras palabras, dada la descomposición irreducible de $V(I) = \bigcup_{i=1}^{t} C_i$, la descomposición irreducible *irredundante* de $\tilde{V}(I)$ sobre $\overline{k(X_1, \ldots, X_\ell)}$ está formada por la unión de todas las componentes irreducibles de las variedades $\tilde{C}_i$ $(1 \leq i \leq t)$.

3.4.3 Resultado principal

El resultado principal de este capítulo es el siguiente Teorema:

Teorema 3.4.3 *Sean $f_1, \ldots, f_s$ polinomios en $k[X_1, \ldots, X_n]$, y sea d un entero tal que $d \geq n$ y $\deg f_i \leq d$ para todo $1 \leq i \leq s$. Sea*

$$V = \{x \in \bar{k}^n : f_1(x) = 0 \wedge \ldots \wedge f_s(x) = 0\}$$

y sea $r = \dim V$. *Entonces, existe un algoritmo probabilístico de complejidad secuencial de orden* $s^{O(1)}d^{O(n)}$, *que calcula la descomposición equidimensional de* V: *tomando como entrada a los polinomios* $f_1, \ldots, f_s$ *dados en forma densa produce un straight-line program de longitud* $d^{O(n)}$ *que calcula polinomios* $g_j^{(\ell)}$ $(0 \leq \ell \leq r, 1 \leq j \leq n+1)$ *tales que, para cada* $0 \leq \ell \leq r$, *la componente equidimensional de* V *de dimensión* ℓ *es*

$$V_\ell = \{x \in \bar{k}^n : g_1^{(\ell)}(x) = 0 \wedge \ldots \wedge g_{n+1}^{(\ell)}(x) = 0\}.$$

Para cada $0 \leq \ell \leq r$, *los grados de los polinomios* $g_j^{(\ell)}$ $(1 \leq j \leq n+1)$ *están acotados por* $\deg V_\ell \leq d^{n-\ell}$.

Demostración. La idea general del algoritmo es la siguiente:

Mediante una modificación conveniente de los datos de entrada, se intenta obtener un sistema de ecuaciones para la variedad V que satisfaga ciertas condiciones sobre dimensión de intersecciones.

A continuación, el algoritmo calcula, para cada $0 \leq \ell \leq \dim V$, un conjunto finito de polinomios que define una subvariedad de V de dimensión ℓ que contiene la componente equidimensional de V de dicha dimensión, y un conjunto finito de polinomios que define una variedad equidimensional auxiliar.

Finalmente, a partir de todos los polinomios calculados en la etapa anterior, el algoritmo obtiene, para cada componente equidimensional de V, un sistema finito de polinomios que la define.

– *Cálculo de la dimensión de* V.

El algoritmo comienza calculando r, la dimensión de V. Esto puede hacerse aplicando el algoritmo descripto en [13] en tiempo secuencial $s^{O(1)}d^{O(n)}$.

(Este paso puede evitarse, como explicaremos en la Observación 3.4.5 después de la demostración, pero se incluye aquí para que el desarrollo del algoritmo resulte más claro.)

– *Preparación de los datos de entrada.*

En esta etapa del algoritmo se modifican los datos de entrada en el sentido de la Sección 3.3:

Por medio de una elección aleatoria de $n+1$ combinaciones lineales de los polinomios de entrada, se puede suponer que la variedad V está definida por $n+1$ polinomios

de grados acotados por d que satisfacen las condiciones (P1) y (P2) enunciadas en el Lema 3.3.1. Haciendo un cambio lineal aleatorio de variables, se puede suponer que las nuevas variables satisfacen las condiciones (V1) y (V2) dadas en la Sección 3.3.2. Con el objeto de simplificar la notación, denotaremos a las nuevas variables por $X_1, \ldots, X_n$ y a las combinaciones lineales de los polinomios de entrada en estas nuevas variables por $f_1, \ldots, f_{n+1}$.

Resumiendo, si los coeficientes de las combinaciones lineales de los polinomios y de las combinaciones lineales de las variables se eligen al azar de un subconjunto de k de N elementos, se obtienen $n+1$ polinomios $f_1, \ldots, f_{n+1}$ en las variables $X_1, \ldots, X_n$ que satisfacen con probabilidad

$$\mathcal{P}_* \geq \left(1 - \frac{2d^n}{N}\right)\left(1 - \frac{d^{2n}}{N}\right) \geq 1 - \frac{d^{2n} + 2d^n}{N}$$

(ver Observaciones 3.3.2 y 3.3.4) las siguientes condiciones, que en lo sucesivo llamaremos *condiciones de normalización*:

(P1) $V = V(f_1, \ldots, f_{n+1})$

(P2) Para cada ℓ, $0 \leq \ell \leq n$, la dimensión de cada componente irreducible de $V(f_1, \ldots, f_{n-\ell})$ no incluida en V es ℓ.

(V1) La proyección $\pi_r : V(f_1, \ldots, f_{n-r}) \to \mathbb{A}^r$ (donde $r = \dim V$) definida por $\pi_r(x) = (x_1, \ldots, x_r)$ es finita.

(V2) Para cada j, $0 \leq j \leq r$, sea Z_j la unión de las componentes irreducibles de $V(f_1, \ldots, f_{n-j})$ no incluidas en V. Entonces, para cada $1 \leq \ell \leq r-1$, si $Z_{\ell+1} \cap V(f_{n-\ell}) \neq \emptyset$, la proyección $\pi_\ell : Z_{\ell+1} \cap V(f_{n-\ell}) \to \mathbb{A}^\ell$ definida por $\pi_\ell(x) = (x_1, \ldots, x_\ell)$ es finita.

- *Descomposición auxiliar de V.*

Sea $V = \bigcup_{\ell=0}^{r} V_\ell$ la descomposición equidimensional de V y supongamos que los polinomios $f_1, \ldots, f_{n+1}$ en las variables $X_1, \ldots, X_n$ obtenidos aleatoriamente satisfacen las "condiciones de normalización" (P1), (P2), (V1) y (V2).

En esta etapa el algoritmo calcula, en un primer paso, polinomios que definen V_r y polinomios que definen Z_r. Luego calcula, en pasos intermedios para $\ell = r-1, \ldots, 0$, polinomios que definen Z_ℓ y polinomios que definen una subvariedad $V_\ell \cup \widehat{V}_\ell$ de V, con $\widehat{V}_\ell \subset \bigcup_{h=\ell+1}^{r} V_h$ y $\dim \widehat{V}_\ell \leq \ell$.

PRIMER PASO (dimensión r)

En este paso se calculan polinomios que definen V_r y polinomios que definen Z_r. Más precisamente, V_r y Z_r serán definidas por medio de los polinomios minimales con respecto a V_r y Z_r de $n+1$ formas lineales convenientemente elegidas (ver Lema 3.4.1). Para calcular estos polinomios, se considerarán variedades cero-dimensionales en el sentido de la Sección 3.4.2.

Consideremos $f_1, \ldots, f_{n-r}$ como polinomios en $k(X_1, \ldots, X_r)[X_{r+1}, \ldots, X_n]$. Sea $\overline{k(X_1, \ldots, X_r)}$ una clausura algebraica de $k(X_1, \ldots, X_r)$ y sea $\tilde{V}(f_1, \ldots, f_{n-r})$ el conjunto de los ceros comunes de $f_1, \ldots, f_{n-r}$ en $\overline{k(X_1, \ldots, X_r)}^{n-r}$. Observamos que $\dim \tilde{V}(f_1, \ldots, f_{n-r}) = 0$ y, como $V(f_1, \ldots, f_{n-r}) = V_r \cup Z_r$, entonces

$$\tilde{V}(f_1, \ldots, f_{n-r}) = \tilde{V}_r \cup \tilde{Z}_r$$

donde $\tilde{V}_r$ y $\tilde{Z}_r$ no tienen componentes irreducibles en común.

Adaptando el algoritmo de [24, Proposition 27] (ver también [13, Sections 3.4.7 y 3.4.8]), presentado en la Sección 1.4, calcularemos los polinomios minimales de una forma lineal apropiada con respecto a $\tilde{V}_r$ y $\tilde{Z}_r$ respectivamente. Los polinomios minimales que se obtendrán coinciden con los polinomios minimales de la forma lineal con respecto a V_r y Z_r.

El algoritmo en [24] calcula un polinomio $F_r \in k[X_1, \ldots, X_r][T_{r+1}, \ldots, T_n]$ de grado en las variables $T_{r+1}, \ldots, T_n$ acotado por $d^{c(n-r)}$ (donde c es una constante positiva) tal que, si $F_r(\lambda_{r+1}, \ldots, \lambda_n) \neq 0$, la forma lineal $y = \lambda_{r+1}X_{r+1} + \cdots + \lambda_n X_n$ es un elemento primitivo para $\tilde{V}(f_1, \ldots, f_{n-r})$; es decir, la forma lineal y separa los puntos de $\tilde{V}(f_1, \ldots, f_{n-r})$.

Sea $y = \lambda_{r+1}X_{r+1} + \cdots + \lambda_n X_n$ una forma lineal tal que $F_r(\lambda_{r+1}, \ldots, \lambda_n) \neq 0$.

Paso 1. Aplicando el algoritmo descripto en [24, Proposition 27] se calculan un elemento $\rho \in k[X_1, \ldots, X_r]$ y polinomios

$$v_{r+1}(Y), \ldots, v_n(Y) \in k[X_1, \ldots, X_r][Y]$$

con $\deg_Y v_i \leq d^{O(n-r)}$, tales que las coordenadas $(x_{r+1}, \ldots, x_n)$ de los puntos de $\tilde{V}(f_1, \ldots, f_{n-r})$ verifican las ecuaciones

$$\rho x_i = v_i(y(x)) \qquad i = r+1, \ldots, n \tag{3.1}$$

es decir, se calcula una resolución geométrica de la variedad cero-dimensional $\tilde{V}(f_1, \ldots, f_{n-r})$.

La complejidad secuencial de este paso es $d^{O(n)}$ y ρ y los coeficientes de $v_{r+1}(Y), \ldots, v_n(Y)$ son polinomios de grados acotados por $d^{O(n-r)}$ dados por un straight-line program de longitud $d^{O(n)}$ (ver Lema 1.4.1).

El cálculo del polinomio minimal de y con respecto a V_r se basa en el hecho que $V_r \subseteq V(f_{n-r+1})$ pero ninguna componente irreducible de Z_r está contenida en $V(f_{n-r+1})$. En consecuencia, los puntos de $\tilde{V}_r$ son exactamente los puntos de $\tilde{V}(f_1, \ldots, f_{n-r})$ en los que se anula f_{n-r+1}, de donde $\tilde{V}_r$ es el conjunto de los ceros comunes en $\overline{k(X_1, \ldots, X_r)}^{n-r}$ de los polinomios $f_1, \ldots, f_{n-r}, f_{n-r+1}$. Además estos ceros comunes satisfacen (3.1).

Consideremos los polinomios

$$F_j^{(r)}(Y) := \rho^d f_j(X_1, \ldots, X_r, \frac{v_{r+1}(Y)}{\rho}, \ldots, \frac{v_n(Y)}{\rho}) \qquad j = 1, \ldots, n-r+1.$$

Utilizando estos polinomios, el algoritmo calcula el polinomio minimal de y con respecto a V_r como sigue:

Paso 2. Se calcula, utilizando el algoritmo presentado en el Lema 1.3.3, la representación densa de los polinomios $F_1^{(r)}, \ldots, F_{n-r+1}^{(r)}$ con respecto a la variable Y. El algoritmo produce un straight-line program de longitud $d^{O(n)}$ que calcula dichos coeficientes, que son polinomios en $k[X_1, \ldots, X_r]$.

Paso 3. Se calcula un máximo común divisor en $k[X_1, \ldots, X_r][Y]$ de los polinomios $F_1^{(r)}(Y), \ldots, F_{n-r+1}^{(r)}(Y)$ (considerados como polinomios en la variable Y con coeficientes en el anillo $k[X_1, \ldots, X_r]$). Para esto se aplica el algoritmo del Lema 1.3.6 adaptado convenientemente para el cálculo del máximo común divisor de más de dos polinomios (ver [24, Lemma 11]). Este algoritmo produce un straight-line program de longitud $d^{O(n)}$ para los coeficientes de un máximo común divisor de los polinomios considerados.

Paso 4. Por medio del algoritmo dado en el Lema 1.3.10, se obtiene un straight-line program de longitud $d^{O(n)}$ que calcula los coeficientes de un polinomio $\tilde{p}(Y)$ que es un múltiplo por un polinomio no nulo en $k[X_1, \ldots, X_r]$ de

$$p(Y) = \mathrm{rad}(\gcd(F_1^{(r)}(Y), \ldots, F_{n-r+1}^{(r)}(Y))) \in k[X_1, \ldots, X_r][Y],$$

el polinomio minimal de y con respecto a $\tilde{V}_r$.

Paso 5. Usando el procedimiento *Vermeidung von Divisionen* (ver Lema 1.3.5) se divide el polinomio $\tilde{p}(Y)$ por su coeficiente principal. De esta forma se obtiene un straight-line program de longitud $d^{O(n)}$ que calcula los coeficientes de $p(Y)$ con respecto a la variable Y. Observamos que $\deg p(Y) \leq \deg V_r$.

Para calcular el polinomio minimal de y con respecto a Z_r, basta observar que los puntos de $\tilde{Z}_r$ son exactamente los puntos de $\tilde{V}(f_1, \ldots, f_{n-r})$ en los que no se anula f_{n-r+1}.

Por lo tanto, el polinomio minimal de y con respecto a $\tilde{Z}_r$ es

$$q(Y) = \frac{\operatorname{rad}(\gcd(F_1^{(r)}(Y), \ldots, F_{n-r}^{(r)}(Y))}{\operatorname{rad}(\gcd(F_1^{(r)}(Y), \ldots, F_{n-r}^{(r)}(Y), F_{n-r+1}^{(r)}(Y)))}. \tag{3.2}$$

A partir de esta fórmula se deriva, como antes, un algoritmo que calcula $q(Y)$:

Paso 6. En forma análoga a lo hecho en los pasos 3 y 4, se obtiene un straight-line program que calcula los coeficientes de un múltiplo por un factor en $k[X_1, \ldots, X_r]$ del polinomio

$$\tilde{p}_0(Y) = \operatorname{rad}(\gcd(F_1^{(r)}(Y), \ldots, F_{n-r}^{(r)}(Y))$$

Paso 7. Se calculan los grados con respecto a la variable Y de los polinomios $\tilde{p}(Y)$ y $\tilde{p}_0(Y)$. Para esto se evalúan los straight-line programs que calculan sus coeficientes en sucesiones de prueba apropiadas.

Paso 8. Se obtiene un straight-line program que calcula los coeficientes de un polinomio $\tilde{q}(Y) \in k[X_1, \ldots, X_r][Y]$ que es un múltiplo por un factor no nulo en $k[X_1, \ldots, X_r]$ de $q(Y)$.

El polinomio $\tilde{q}(Y)$ se obtiene como un múltiplo por un factor en $k[X_1, \ldots, X_r]$ del cociente en la división de $\tilde{p}(Y)$ por $\tilde{p}_0(Y)$ en $k(X_1, \ldots, X_r)[Y]$.

La división de $\tilde{p}(Y)$ por $\tilde{p}_0(Y)$ se efectúa considerando los coeficientes del cociente como indeterminadas y resolviendo el sistema lineal que resulta (lo que involucra sólo cálculos de determinantes).

Paso 9. Se divide el polinomio $\tilde{q}(Y)$ por su coeficiente principal utilizando el algoritmo del Lema 1.3.5.

De esta manera, se obtiene un straight-line program de longitud $d^{O(n)}$ que calcula los coeficientes de $q(Y) \in k[X_1, \ldots, X_r][Y]$.

La complejidad secuencial de todo el proceso (pasos 1 a 9) es de orden $d^{O(n)}$.

El algoritmo descripto en los pasos 1 a 9 anteriores se aplica a $n+1$ formas lineales elegidas aleatoriamente. Si los coeficientes de estas formas lineales se eligen de un subconjunto de k de N elementos, las $n+1$ formas lineales lineales $y_1^{(r)}, \ldots, y_{n+1}^{(r)}$ obtenidas satisfacen las siguientes condiciones, a las que en lo sucesivo nos referiremos como *condiciones sobre las formas lineales en el paso* r, con probabilidad

$$\mathcal{P}_r \geq 1 - \frac{1}{N}\left((n+1)d^{c(n-r)} + 2d^{(n-r)(n+1)}\right)$$

(ver Observación 3.4.2):

(L1) Los coeficientes de $y_1^{(r)}, \ldots, y_{n+1}^{(r)}$ no anulan al polinomio F_r (que garantiza la condición de ser un elemento primitivo)

(L2) Z_r es el conjunto de los ceros comunes de los polinomios minimales de $y_1^{(r)}, \ldots, y_{n+1}^{(r)}$ con respecto a Z_r (evaluados en $y_1^{(r)}, \ldots, y_{n+1}^{(r)}$ respectivamente).

(L3) V_r es el conjunto de los ceros comunes de los polinomios minimales de $y_1^{(r)}, \ldots, y_{n+1}^{(r)}$ con respecto a V_r (evaluados en $y_1^{(r)}, \ldots, y_{n+1}^{(r)}$ respectivamente).

Entonces, suponiendo que el cambio de variables y las combinaciones lineales de los polinomios de entrada satisfacen las "condiciones de normalización" (P1), (P2), (V1) y (V2) y que las formas lineales satisfacen las condiciones (L1), (L2) y (L3) para las formas lineales en el paso r, el algoritmo produce polinomios $p_1^{(r)}, \ldots, p_{n+1}^{(r)}$ y $q_1^{(r)}, \ldots, q_{n+1}^{(r)}$ en $k[X_1, \ldots, X_r][Y]$ tales que

$$V_r = \{x \in \bar{k}^n : p_1^{(r)}(x_1, \ldots, x_r, y_1^{(r)}(x)) = 0 \wedge \ldots \wedge p_{n+1}^{(r)}(x_1, \ldots, x_r, y_{n+1}^{(r)}(x)) = 0\}$$
$$Z_r = \{x \in \bar{k}^n : q_1^{(r)}(x_1, \ldots, x_r, y_1^{(r)}(x)) = 0 \wedge \ldots \wedge q_{n+1}^{(r)}(x_1, \ldots, x_r, y_{n+1}^{(r)}(x)) = 0\}$$

(ver Lema 3.4.1).

PASOS INTERMEDIOS (dimensión ℓ, con $0 \leq \ell \leq r-1$)

En estos pasos se calculan, para $\ell = r-1, \ldots, 0$, polinomios que definen ciertas subvariedades de $V(f_1, \ldots, f_{n-\ell})$. Estos polinomios se utilizarán en la última etapa del algoritmo para obtener la descomposición equidimensional de la variedad V.

Recordemos que, para cada $0 \leq \ell \leq r-1$, la descomposición equidimensional de $V(f_1, \ldots, f_{n-\ell})$ es

$$V(f_1, \ldots, f_{n-\ell}) = V_r \cup \ldots \cup V_{\ell+1} \cup V'_\ell$$

donde $V'_\ell = V_\ell \cup Z_\ell$, para cada $\ell \leq h \leq r$, V_h es la componente equidimensional de V de dimensión h (eventualmente $V_h = \emptyset$) y Z_ℓ es o bien vacía o bien una variedad equidimensional de dimensión ℓ sin componentes irreducibles en común con V_ℓ.

Para $\ell = r-1, \ldots, 0$, se calculará, a partir de los polinomios $f_1, \ldots, f_{n-\ell+1}$, un conjunto de $n+1$ polinomios que define Z_ℓ. Simultáneamente se calculará, a partir de los polinomios que definen $Z_{\ell+1}$ y los polinomios $f_1, \ldots, f_{n-\ell+1}$, un conjunto de $n+1$ polinomios que define una variedad $V_\ell \cup \widehat{V}_\ell$ con $\widehat{V}_\ell \subseteq \bigcup_{h=\ell+1}^{r} V_h$ y $\dim \widehat{V}_\ell \leq \ell$. Más aún, los polinomios que se calcularán se obtendrán especializando los polinomios minimales (con respecto a ciertas variedades equidimensionales) de formas lineales convenientemente elegidas, en las correspondientes formas lineales.

Sea ℓ fijo, $0 \leq \ell \leq r-1$.

Consideremos la variedad definida en $\bar{k}^n$ por los polinomios $f_1, \ldots, f_{n-\ell}$. Se tiene que

$$V(f_1, \ldots, f_{n-\ell}) = V_r \cup \ldots \cup V_{\ell+1} \cup V_\ell \cup Z_\ell$$

donde Z_ℓ es o bien vacía o bien una variedad equidimensional de dimensión ℓ.

Sea $\widetilde{V}(f_1, \ldots, f_{n-\ell}) \subseteq \mathbb{A}^{n-\ell}(\overline{k(X_1, \ldots, X_\ell)})$ la variedad afín definida por $f_1, \ldots, f_{n-\ell}$ considerados como polinomios en $k(X_1, \ldots, X_\ell)[X_{\ell+1}, \ldots, X_n]$.

Entonces

$$\widetilde{V}(f_1, \ldots, f_{n-\ell}) = \widetilde{V}_r \cup \ldots \cup \widetilde{V}_{\ell+1} \cup \widetilde{V}_\ell \cup \widetilde{Z}_\ell$$

donde, para cada $\ell \leq j \leq r$, $\widetilde{V}_j = \emptyset$ (si $V_j = \emptyset$) o $\dim \widetilde{V}_j = \dim V_j - \ell$, y $\widetilde{Z}_\ell = \emptyset$ o $\dim \widetilde{Z}_\ell = 0$ (ver Sección 3.4.2).

La información acerca de V_ℓ y Z_ℓ necesaria para nuestros cálculos se obtendrá considerando el conjunto de los puntos aislados de la variedad $\widetilde{V}(f_1, \ldots, f_{n-\ell})$, es decir $\widetilde{V}_\ell \cup \widetilde{Z}_\ell$.

Adaptaremos el algoritmo dado para el cálculo de los polinomios minimales en el primer paso (es decir, el caso en que $\widetilde{V}(f_1, \ldots, f_{n-r})$ es una variedad de dimensión cero) a esta situación más general. Nuevamente, el algoritmo se basa en las técnicas presentadas en la Sección 1.4.

El algoritmo en [24, Proposition 27] trabaja con una forma lineal que es un elemento primitivo para los ceros aislados de $f_1, \ldots, f_{n-\ell}$. Para obtener formas lineales que cumplan esta condición, el algoritmo calcula un polinomio

$$F_\ell \in k[X_1, \ldots, X_\ell][T_{\ell+1}, \ldots, T_n]$$

tal que, si $F_\ell(\lambda_{\ell+1},\ldots,\lambda_n) \neq 0$ entonces la forma lineal $y = \lambda_{\ell+1}X_{\ell+1} + \cdots + \lambda_n X_n$ separa los puntos aislados de $\tilde{V}(f_1,\ldots,f_{n-\ell})$. El grado de F_ℓ está acotado por $d^{c(n-\ell)}$ donde c es una constante positiva.

Sea $y = \lambda_{\ell+1}X_{\ell+1} + \cdots + \lambda_n X_n$ una forma lineal tal que $F_\ell(\lambda_{\ell+1},\ldots,\lambda_n) \neq 0$.

Paso 1. Aplicando el algoritmo dado por el Lema 1.4.1 se calculan un elemento $\rho \in k[X_1,\ldots,X_\ell]$ y polinomios

$$v_{\ell+1}(Y),\ldots,v_n(Y) \in k[X_1,\ldots,X_\ell][Y]$$

con $\deg_Y(v_i) \leq d^{O(n-\ell)}$, tales que las coordenadas de los puntos aislados de $\tilde{V}(f_1,\ldots,f_{n-\ell})$ verifican las ecuaciones

$$\rho x_i = v_i(y(x)) \qquad i = \ell+1,\ldots,n. \tag{3.3}$$

La complejidad secuencial de este paso es $d^{O(n)}$ y ρ y los coeficientes de los polinomios $v_{\ell+1}(Y),\ldots,v_n(Y)$ son polinomios de grados acotados por $d^{O(n-\ell)}$ dados por un straight-line program de longitud $d^{O(n)}$.

El cálculo del polinomio minimal de y con respecto a $\tilde{Z}_\ell$ se realiza como en el primer paso:

Consideremos los polinomios

$$F_j^{(\ell)}(Y) := \rho^d f_j(X_1,\ldots,X_\ell,\frac{v_{\ell+1}(Y)}{\rho},\ldots,\frac{v_n(Y)}{\rho}) \qquad j = 1,\ldots,n-\ell+1. \tag{3.4}$$

Teniendo en cuenta que $\tilde{Z}_\ell$ es el conjunto de los puntos de $\tilde{V}(f_1,\ldots,f_{n-\ell})$ en los cuales $f_{n-\ell+1}$ no se anula, y que todos los puntos de $\tilde{Z}_\ell$ son ceros aislados de $f_1,\ldots,f_{n-\ell}$, concluimos que

$$q(Y) = \frac{\mathrm{rad}(\gcd(F_1^{(\ell)}(Y),\ldots,F_{n-\ell}^{(\ell)}(Y))}{\mathrm{rad}(\gcd(F_1^{(\ell)}(Y),\ldots,F_{n-\ell}^{(\ell)}(Y),F_{n-\ell+1}^{(\ell)}(Y)))} \in k(X_1,\ldots,X_\ell)[Y] \tag{3.5}$$

es el polinomio minimal de y con respecto a $\tilde{Z}_\ell$.

Las "condiciones de normalización" implican que las variables están en posición de Noether con respecto a Z_ℓ, de donde deducimos que $q(Y)$ es el polinomio minimal de y con respecto a Z_ℓ.

El polinomio $q(Y)$ se obtiene algorítmicamente utilizando las mismas técnicas de cálculo de máximo común divisor y radicales aplicadas en el paso correspondiente a dimensión r:

Paso 2. Teniendo en cuenta la fórmula (3.5), se calcula primero un múltiplo de $q(Y)$ por un factor en $k[X_1,\ldots,X_\ell]$, y luego se obtiene $q(Y)$ como el cociente en la división (exacta) de este polinomio por su coeficiente principal.

El resultado de este procedimiento es el polinomio $q(Y)$ dado en forma densa con respecto a Y y sus coeficientes, que son polinomios en $k[X_1,\ldots,X_\ell]$, dados por medio de un straight-line program de longitud $d^{O(n)}$.

Nos gustaría obtener polinomios que definan V_ℓ de la misma manera en que se hizo en el primer paso, pero la aplicación del mismo procedimiento puede llevar a la aparición de componentes irreducibles que no son componentes de V_ℓ.

Para controlar en cierta forma el conjunto en que se anulan los polinomios que serán calculados, tendremos en cuenta que las componentes irreducibles de V que pertenecen a V_ℓ están incluidas en $Z_{\ell+1}$, lo que se sigue de las igualdades

$$V(f_1,\ldots,f_{n-\ell-1}) = V_r \cup \ldots \cup V_{\ell+1} \cup Z_{\ell+1} \tag{3.6}$$

$$V(f_1,\ldots,f_{n-\ell-1},f_{n-\ell}) = V_r \cup \ldots \cup V_{\ell+1} \cup V_\ell \cup Z_\ell. \tag{3.7}$$

Sean $\bar{q}_j^{(\ell+1)}(X_1,\ldots,X_n) = q_j^{(\ell+1)}(X_1,\ldots,X_{\ell+1},y_j^{(\ell+1)})$, $1 \le j \le n+1$, los polinomios que definen $Z_{\ell+1}$ obtenidos por el algoritmo en el paso correspondiente a dimensión $\ell+1$, y sea $\tilde{Z}_{\ell+1}$ la variedad que definen estos polinomios en $\overline{k(X_1,\ldots,X_\ell)}^{n-\ell}$ (considerándolos como polinomios en $k(X_1,\ldots,X_\ell)[X_{\ell+1},\ldots,X_n]$).

Como $V_\ell \subset Z_{\ell+1}$, los puntos de $\tilde{V}_\ell$ son también puntos de $\tilde{Z}_{\ell+1}$. Por otro lado, los puntos en $\tilde{V}_\ell$ son los puntos aislados de $\tilde{V}(f_1,\ldots,f_{n-\ell})$ en los que se anula $f_{n-\ell+1}$. Luego, los puntos aislados que estamos buscando son *algunos* de los ceros comunes de $f_1,\ldots,f_{n-\ell},f_{n-\ell+1}$ en $\tilde{Z}_{\ell+1}$.

Los puntos de $\tilde{V}_\ell$, siendo ceros aislados de $f_1,\ldots,f_{n-\ell}$, satisfacen las ecuaciones (3.3). Consideremos entonces los polinomios

$$Q_j^{(\ell+1)}(Y) = \rho^{\deg \bar{q}_j^{(\ell+1)}} \bar{q}_j^{(\ell+1)}(X_1,\ldots,X_\ell,\frac{v_{\ell+1}(Y)}{\rho},\ldots,\frac{v_n(Y)}{\rho}) \qquad j=1,\ldots,n+1 \tag{3.8}$$

y sea

$$p(Y) = \mathrm{rad}(\gcd(F_1^{(\ell)}(Y),\ldots,F_{n-\ell+1}^{(\ell)}(Y),Q_1^{(\ell+1)}(Y),\ldots,Q_{n+1}^{(\ell+1)}(Y))). \tag{3.9}$$

El polinomio mónico $p(Y) \in k(X_1,\ldots,X_\ell)[Y]$ verifica que $p(y(x)) = 0$ para cada $x \in \tilde{V}_\ell$. Más aún, si $\gamma \in \overline{k(X_1,\ldots,X_\ell)}$ es una raíz de p, entonces $\gamma = y(x)$ para algún x en $\tilde{Z}_{\ell+1} \cap (\tilde{V}_r \cup \ldots \cup \tilde{V}_\ell)$.

Sea $W_\ell \subseteq \mathbb{A}^n$ la variedad formada por la unión de las componentes irreducibles de dimensión ℓ de $Z_{\ell+1} \cap (V_r \cup \ldots \cup V_\ell)$. Entonces W_ℓ es una variedad equidimensional de dimensión ℓ y las igualdades (3.6) y (3.7) implican que todas las componentes irreducibles de W_ℓ son también componentes irreducibles de $Z_{\ell+1} \cap V(f_{n-\ell})$. En consecuencia, las variables están en posición de Noether con respecto a W_ℓ.

Sea $\widetilde{W}_\ell$ la variedad correspondiente a W_ℓ en $\mathbb{A}^{n-\ell}(\overline{k(X_1,\ldots,X_\ell)})$. Como ya hemos observado, el polinomio mónico separable $p(Y) \in k(X_1,\ldots,X_\ell)[Y]$ satisface que, si $\gamma \in \overline{k(X_1,\ldots,X_\ell)}$ es una raíz de p, entonces $\gamma = y(x)$ para algún x en $\widetilde{W}_\ell$. En consecuencia, $p(Y)$ es el polinomio minimal de y con respecto a una variedad incluida en W_ℓ (ver Sección 3.4.2). Sea $m_y \in k[X_1,\ldots,X_\ell][Y]$ el polinomio minimal de y con respecto a W_ℓ. Entonces $p(Y)$ es un polinomio en $k[X_1,\ldots,X_\ell][Y]$ que es un factor de m_y.

Como $p(Y)$ evaluado en y se anula en los puntos aislados de $\widetilde{V}_\ell$, el polinomio minimal de y con respecto a $\widetilde{V}_\ell$ divide a $p(Y)$ y en consecuencia

$$p(X_1,\ldots,X_\ell, y(X_{\ell+1},\ldots,X_n))$$

se anula sobre V_ℓ.

Una vez más, el algoritmo que produce el polinomio $p(Y)$ se basa en cálculos de máximo común divisor y radicales:

Paso 3. Teniendo en cuenta la fórmula (3.9), se calcula primero un múltiplo de $p(Y)$ por un elemento en $k[X_1,\ldots,X_\ell]$ y luego el cociente de este polinomio por su coeficiente principal.

Se obtiene de esta manera, la representación densa de p en la variable Y y sus coeficientes dados por un straight-line program de longitud $d^{O(n)}$.

Resumiendo, dada una forma lineal $y = \lambda_{\ell+1}X_{\ell+1} + \cdots + \lambda_n X_n$ cuyos coeficientes satisfacen $F_\ell(\lambda_{\ell+1},\ldots,\lambda_n) \neq 0$, el algoritmo dado por los pasos 1, 2 y 3 anteriores calcula el polinomio minimal de y con respecto a Z_ℓ y un polinomio $p(Y)$ que es un factor del polinomio minimal de y con respecto a W_ℓ y, evaluado en y, se anula sobre V_ℓ. La complejidad secuencial de este algoritmo es de orden $d^{O(n)}$.

El procedimiento descripto en 1, 2 y 3 se aplica a $n+1$ formas lineales elegidas aleatoriamente. Si los coeficientes de las formas lineales se toman aleatoriamente de un subconjunto de k con N elementos, las formas lineales obtenidas satisfacen las condiciones

(L1') F_ℓ no se anula en los coeficientes de las formas lineales

(L2') Z_ℓ es el conjunto de los ceros comunes en $\mathbb{A}^n$ de los polinomios minimales de las $n+1$ formas lineales con respecto a Z_ℓ (evaluados en las correspondientes formas lineales),

(L3') V_ℓ es el conjunto de los ceros comunes en $\mathbb{A}^n$ de los polinomios minimales de las $n+1$ formas lineales con respecto a V_ℓ (evaluados en las correspondientes formas lineales), y

(L4') W_ℓ es el conjunto de los ceros comunes en $\mathbb{A}^n$ de los polinomios minimales de las $n+1$ formas lineales con respecto a W_ℓ (evaluados en las correspondientes formas lineales)

que en lo sucesivo llamaremos *condiciones sobre las formas lineales en el paso* ℓ, con probabilidad

$$\mathcal{P}_\ell \geq 1 - \frac{1}{N}\left((n+1)d^{c(n-\ell)} + 4d^{(n-\ell)(n+1)}\right)$$

(ver Observación 3.4.2).

La condición (L1') implica que se puede aplicar el algoritmo en [24] a las formas lineales elegidas. La condición (L2') garantiza que los $n+1$ polinomios calculados con respecto a Z_ℓ la definen. Finalmente, las condiciones (L3') y (L4') nos permitirán construir, a partir de los polinomios calculados en las distintas etapas, un conjunto de $n+1$ polinomios que define V_ℓ.

Sean $y_1^{(\ell)}, \ldots, y_{n+1}^{(\ell)}$ las formas lineales elegidas, y sean $p_1^{(\ell)}, \ldots, p_{n+1}^{(\ell)}$ y $q_1^{(\ell)}, \ldots, q_{n+1}^{(\ell)}$ los polinomios en $k[X_1, \ldots, X_\ell][Y]$ calculados por el algoritmo.

Entonces, suponiendo que se satisfacen las "condiciones de normalización" (V1), (V2), (P1) y (P2), y que las formas lineales $y_1^{(\ell)}, \ldots, y_{n+1}^{(\ell)}$ verifican las condiciones (L1') y (L2') anteriores, se tiene que

$$Z_\ell = \{x \in \bar{k}^n : q_1^{(\ell)}(x_1, \ldots, x_\ell, y_1^{(\ell)}(x)) = 0, \ldots, q_{n+1}^{(\ell)}(x_1, \ldots, x_\ell, y_{n+1}^{(\ell)}(x)) = 0\}.$$

Queda por caracterizar el conjunto de los ceros comunes de los polinomios

$$p_1^{(\ell)}(X_1, \ldots, X_\ell, y_1^{(\ell)}(X_{\ell+1}, \ldots, X_n)), \ldots, p_{n+1}^{(\ell)}(X_1, \ldots, X_\ell, y_{n+1}^{(\ell)}(X_{\ell+1}, \ldots, X_n)).$$

Sean $m_1^{(\ell)}, \ldots, m_{n+1}^{(\ell)}$ los polinomios minimales de $y_1^{(\ell)}, \ldots, y_{n+1}^{(\ell)}$ con respecto a W_ℓ. Como ya hemos visto, para cada $1 \leq j \leq n+1$,

$$V_\ell \subseteq \{x \in \bar{k}^n : p_j^{(\ell)}(x_1, \ldots, x_\ell, y_j^{(\ell)}(x)) = 0\} \subseteq \{x \in \bar{k}^n : m_j^{(\ell)}(x_1, \ldots, x_\ell, y_j^{(\ell)}(x)) = 0\}$$

y, en consecuencia,

$$\begin{aligned} V_\ell &\subseteq \{x \in \bar{k}^n : p_1^{(\ell)}(x_1,\ldots,x_\ell,y_1^{(\ell)}(x)) = 0 \wedge \ldots \wedge p_{n+1}^{(\ell)}(x_1,\ldots,x_\ell,y_{n+1}^{(\ell)}(x)) = 0\} \\ &\subseteq \{x \in \bar{k}^n : m_1^{(\ell)}(x_1,\ldots,x_\ell,y_1^{(\ell)}(x)) = 0 \wedge \ldots \wedge m_{n+1}^{(\ell)}(x_1,\ldots,x_\ell,y_{n+1}^{(\ell)}(x)) = 0\} \end{aligned}$$

Por otro lado, si valen las "condiciones de normalización" y las formas lineales $y_1^{(\ell)},\ldots,y_{n+1}^{(\ell)}$ satisfacen la condición (L4') resulta que

$$\{x \in \bar{k}^n : m_1^{(\ell)}(x_1,\ldots,x_\ell,y_1^{(\ell)}(x)) = 0 \wedge \ldots \wedge m_{n+1}^{(\ell)}(x_1,\ldots,x_\ell,y_{n+1}^{(\ell)}(x)) = 0\} = W_\ell.$$

Puesto que V_ℓ y W_ℓ son variedades equidimensionales de dimensión ℓ, y $W_\ell \subseteq \bigcup_{h=\ell}^{r} V_h$, concluimos que el conjunto de los ceros comunes de los polinomios

$$p_1^{(\ell)}(X_1,\ldots,X_\ell,y_1^{(\ell)}(X_{\ell+1},\ldots,X_n)),\ldots,p_{n+1}^{(\ell)}(X_1,\ldots,X_\ell,y_{n+1}^{(\ell)}(X_{\ell+1},\ldots,X_n))$$

es una variedad $V_\ell \cup \widehat{V}_\ell$, donde $\widehat{V}_\ell \subseteq \bigcup_{h=\ell+1}^{r} V_h$ y $\dim \widehat{V}_\ell \leq \ell$.

- Cálculo de la descomposición equidimensional de V.

En esta última etapa del algoritmo se obtendrá, para $\ell = r-1,\ldots,0$, un conjunto finito de polinomios que define la componentes equidimensional V_ℓ de dimensión ℓ de V. Estos polinomios se calcularán a partir de los polinomios obtenidos en la etapa anterior.

Fijemos $\ell < r$.

Sea y una de las formas lineales elegidas en el paso correspondiente a dimensión ℓ de la etapa anterior, es decir $y = y_j^{(\ell)}$ $(1 \leq j \leq n+1)$.

Sea $p(Y) = p_j^{(\ell)}(Y) \in k[X_1,\ldots,X_\ell][Y]$ el polinomio calculado previamente para y, que es el polinomio minimal de la forma lineal y con respecto a una variedad formada por los puntos de $\widetilde{V}_\ell$ y un subconjunto de $\widetilde{V}_{\ell+1} \cup \ldots \cup \widetilde{V}_r$.

Daremos a continuación un algoritmo que calcula el polinomio minimal de y con respecto a V_ℓ a partir de los polinomios calculados en los distintos pasos de la etapa anterior.

En un primer paso, el algoritmo obtiene el factor de $p(Y)$ que no corresponde a los puntos de $\widetilde{V}_\ell$.

Sea $\rho \in k[X_1,\ldots,X_\ell]$ y sean $v_{\ell+1}(Y),\ldots,v_n(Y) \in k[X_1,\ldots,X_\ell][Y]$ tales que valen las ecuaciones (3.3).

Para cada $\ell+1 \leq i \leq r$, sean $\bar{p}_j^{(i)}(X_1,\ldots,X_n) = p_j^{(i)}(X_1,\ldots,X_i,y_j^{(i)})$ $(1 \leq j \leq n+1)$ los polinomio calculados en la etapa anterior que satisfacen

$$\{x \in \bar{k}^n : \bar{p}_1^{(i)}(x) = 0 \wedge \ldots \wedge \bar{p}_{n+1}^{(i)}(x) = 0\} = V_i \cup \widehat{V}_i$$

con $\widehat{V}_i \subseteq \bigcup_{j=i+1}^{r} V_j$.

Consideremos los polinomios

$$P_j^{(i)}(Y) := \rho^{\deg \bar{p}_j^{(i)}} \bar{p}_j^{(i)}(X_1,\ldots,X_\ell,\frac{v_{\ell+1}(Y)}{\rho},\ldots,\frac{v_n(Y)}{\rho}) \qquad j = 1,\ldots,n+1$$

y los polinomios definidos en (3.4) y (3.8).

Paso 1. Aplicando las mismas técnicas utilizadas en la etapa anterior, se calcula, para cada $\ell+1 \leq i \leq r$, un polinomio $h_i(Y)$ que es un múltiplo, por un factor en $k[X_1,\ldots,X_\ell]$, de

$$\mathrm{rad}(\gcd(F_1^{(\ell)}(Y),\ldots,F_{n-\ell+1}^{(\ell)}(Y),Q_1^{(\ell+1)}(Y),\ldots,Q_{n+1}^{(\ell+1)}(Y),P_1^{(i)}(Y),\ldots,P_{n+1}^{(i)}(Y)).$$

Paso 2. A partir de los polinomios h_i $(\ell+1 \leq i \leq r)$ se obtiene un múltiplo, por un factor en $k[X_1,\ldots,X_\ell]$, del polinomio

$$h(Y) = \mathrm{rad}(\prod_{i=\ell+1}^{r} h_i(Y)).$$

Este polinomio $h(Y)$ es el factor de $p(Y)$ que corresponde a los puntos en la variedad $\widetilde{V}_{\ell+1} \cup \ldots \cup \widetilde{V}_r$, es decir, que no pertenecen a $\widetilde{V}_\ell$.

Finalmente se obtiene el polinomio minimal de y con respecto a V_ℓ separando del polinomio $p(Y)$ el factor calculado:

Paso 3. Se calcula un múltiplo del polinomio $\dfrac{p(Y)}{h(Y)}$ por un factor en $k[X_1,\ldots,X_\ell]$ y el polinomio $G(Y)$ que es el cociente en la división de este polinomio por su coeficiente principal.

El polinomio $G(Y)$ obtenido es exactamente el polinomio minimal de y con respecto a V_ℓ, y por lo tanto, su grado total está acotado por $\deg V_\ell$.

Observamos que todo el procedimiento anterior se realiza en tiempo secuencial $d^{O(n)}$.

Aplicando el procedimiento descripto en los pasos 1, 2 y 3 a las $n+1$ formas lineales $y_1^{(\ell)}, \ldots, y_{n+1}^{(\ell)}$ elegidas en la etapa anterior del algoritmo se obtienen los $n+1$ polinomios minimales $G_1^{(\ell)}(Y), \ldots, G_{n+1}^{(\ell)}(Y)$ asociados a ellas. Entonces, si valen las "condiciones de normalización" y las formas lineales $y_1^{(\ell)}, \ldots, y_{n+1}^{(\ell)}$ verifican la condición (L3') para las formas lineales en dimensión ℓ, los polinomios

$$g_j^{(\ell)} = G_j^{(\ell)}(X_1, \ldots, X_\ell, y_j^{(\ell)}(X_{\ell+1}, \ldots, X_n)) \qquad j = 1, \ldots, n+1$$

satisfacen

$$V_\ell = \{x \in \bar{k}^n : g_1^{(\ell)}(x) = 0 \wedge \ldots \wedge g_{n+1}^{(\ell)}(x) = 0\}.$$

Repitiendo el procedimiento anterior para cada ℓ con $0 \leq \ell \leq r-1$ se obtiene la descomposición equidimensional de V.

Teniendo en cuenta las complejidades de cada una de las etapas del algoritmo resulta que la complejidad secuencial total del algoritmo para descomposición equidimensional que hemos descripto es de orden $s^{O(1)}d^{O(n)}$.

Observación 3.4.4 Supongamos dado un proceso aleatorio para seleccionar elementos de un subconjunto fijo de k con N elementos, que se utiliza para elegir los parámetros aleatorios en las distintas etapas del algoritmo: para obtener las combinaciones lineales de los polinomios de entrada, el cambio de variables y los coeficientes de las formas lineales utilizadas en los pasos intermedios. Entonces, teniendo en cuenta las probabilidades de éxito calculadas $\mathcal{P}_*$ para la preparación de los datos de entrada, y $\mathcal{P}_0, \ldots, \mathcal{P}_r$ para los pasos intermedios del algoritmo, resulta que la probabilidad de éxito del algoritmo construido es mayor o igual que

$$1 - \frac{c_1 \cdot d^{n^2+n} + d^{c_2 \cdot (n+1)}}{N}$$

donde c_1 y c_2 son constantes positivas.

Observación 3.4.5 El cálculo de la dimensión de la variedad V realizado al principio del algoritmo no es necesario: dada una variedad $V \neq \mathbb{A}^n$, puede comenzarse el algoritmo en la instancia $n-1$ en lugar de la instancia $r = \dim V$. La complejidad secuencial es, en este caso de orden $(n+1)(2s-1)d^n + d^{O(n)}$.

Por otro lado, si los polinomios de entrada están codificados por medio de un straight-line program de longitud L, la complejidad secuencial del algoritmo puede

estimarse por $(L + (n+1)(2s-1))^{O(1)}d^{O(n)}$. Más aún, si sólo se quiere calcular polinomios que definan V_ℓ, la componente equidimensional de V de dimensión ℓ, la complejidad secuencial es de orden $(L + (n-\ell+1)(2s-1))^{O(1)}d^{O(n-\ell)}$.

Capítulo 4

Cálculo de formas de Chow

En este capítulo se presenta un algoritmo probabilístico que obtiene la descomposición equidimensional de una variedad algebraica afín arbitraria por medio del cálculo de la forma de Chow de cada una de sus componentes equidimensionales. Bajo ciertas condiciones genéricas, la complejidad de este algoritmo depende de un invariante geométrico: el grado geométrico del sistema de polinomios dado que define la variedad, lo que permite obtener estimaciones más precisas sobre la complejidad del cálculo de la descomposición equidimensional de variedades.

4.1 Forma de Chow de una variedad afín equidimensional

4.1.1 Definición

La definición de forma de Chow presentada en la Sección 2.1 para una variedad proyectiva equidimensional puede extenderse al caso de una variedad afín equidimensional: Sea $V \subset \mathbb{A}^n$ una variedad afín equidimensional. Una *forma de Chow* $\mathcal{F}_V$ *de* V se define como una forma de Chow de su clausura proyectiva $\overline{V} \subset \mathbb{P}^n$.

Una forma de Chow $\mathcal{F}_V$ de V está unívocamente determinada por V salvo por un factor constante. Además, como $\dim V = \dim \overline{V}$ y $\deg V = \deg \overline{V}$, resulta que si $r = \dim V$, $\mathcal{F}_V$ es un polinomio en $r+1$ grupos de variables $U_0, \ldots, U_r$, multihomogéneo de grado $\deg V$ en cada grupo de variables.

En el caso en que V es irreducible, $\mathcal{F}_V$ es un polinomio irreducible, y en el caso

general de una variedad equidimensional, es el producto de las formas de Chow de las componentes equidimensionales de V.

A continuación mostramos otras formas equivalentes de definir una forma de Chow de una variedad afín equidimensional V de dimensión r.

Para cada $0 \leq i \leq r$ sea $U_i := (U_{i0}, \ldots, U_{in})$ un grupo de $n+1$ nuevas variables y sea $L_i(U_i, X) := U_{i0} + U_{i1}X_1 + \cdots + U_{in}X_n$. Consideremos la variedad afín

$$\Gamma_{af}(V) := \{(u_0, \ldots, u_r, x) \in (\mathbb{A}^{n+1})^{r+1} \times \mathbb{A}^{n+1} : \\ x \in V,\ L_0(u_0, x) = 0, \ldots, L_r(u_r, x) = 0\}.$$

Sea $\pi : (\mathbb{A}^{n+1})^{r+1} \times \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ la proyección canónica sobre las primeras coordenadas. Entonces la clausura de Zariski $\overline{\pi(\Gamma_{af}(V))}$ de la proyección de $\Gamma_{af}(V)$ es una hipersuperficie en $(\mathbb{A}^{n+1})^{r+1}$ y $\mathcal{F}_V$ es un polinomio libre de cuadrados que la define (ver la demostración del Lema 2.3.5).

Si V es definible sobre k, una forma de Chow de V puede obtenerse también a partir del ideal $I(V) \subset k[X_1, \ldots, X_n]$ formado por los polinomios de $k[X_1, \ldots, X_n]$ que se anulan sobre V:

Lema 4.1.1 *Sea $I \subset k[X_1, \ldots, X_n]$ un ideal radical. Sea $U := (U_0, \ldots, U_n)$ un grupo de $n+1$ nuevas variables y sea $L := U_0 + U_1X_1 + \cdots + U_nX_n$. Entonces el ideal $\mathcal{I} = (I, L) \subset k[U, X]$ es un ideal radical de $k[U, X]$.*

Demostración. Sea $f \in k[U, X]$ un polinomio que se anula sobre $V(\mathcal{I})$.
Consideremos el polinomio $F \in k[U_1, \ldots, U_n, X]$ definido por

$$F(U_1, \ldots, U_n, X) = f(-(U_1X_1 + \cdots + U_nX_n), U_1, \ldots, U_n, X).$$

Puesto que f se anula sobre $V(\mathcal{I})$, el polinomio F se anula sobre $\mathbb{A}^n \times V(I)$, luego $F \in (I) \subset k[U, X]$ (que es un ideal radical).
Sea $F_0 := f - F \in k[U, X]$. Observamos que $V(L) \subset V(F_0)$, de donde $F_0 \in (L)$.
En consecuencia, $f = F + F_0 \in (I) + (L) = \mathcal{I}$.
Luego, $\mathcal{I}$ es un ideal radical de $k[U, X]$.

Observamos que el ideal $(I(V) + (L_0, \ldots, L_r)) \cap k[U_0, \ldots, U_r]$ define la variedad $\overline{\pi(\Gamma_{af}(V))}$.

Por otro lado, aplicando recursivamente el Lema 4.1.1, resulta que el ideal $(I(V) + (L_0, \ldots, L_r))$ es un ideal radical de $k[U_0, \ldots, U_r, X]$. Luego, una forma de Chow $\mathcal{F}_V$ de V puede definirse también como un generador del ideal (principal)

$$(I(V) + (L_0, \ldots, L_r)) \cap k[U_0, \ldots, U_r].$$

4.1.2 Normalización de formas de Chow

Sea $V \subset \mathbb{A}^n$ una variedad afín equidimensional de dimensión r y grado D definida sobre un cuerpo k. Una forma de Chow $\mathcal{F}_V$ de V está unívocamente determinada salvo por un factor constante.

Bajo ciertas hipótesis, esta indeterminación puede evitarse fijando uno de los coeficientes de $\mathcal{F}_V$.

Sea $\overline{V} \subset \mathbb{P}^n$ la clausura proyectiva de V. En el caso en que

$$\overline{V} \cap \{x_0 = 0\} \cap \ldots \cap \{x_r = 0\} = \emptyset,$$

si e_i denota el $(i+1)$-ésimo vector de la base canónica de k^{n+1} (que representa el vector de coeficientes de la forma lineal X_i), se tiene que

$$\mathcal{F}_V(e_0, \ldots, e_r) \neq 0$$

para cualquier forma de Chow $\mathcal{F}_V$ de V. Se define entonces la *forma de Chow normalizada de* V, que denotaremos por Ch_V, como la forma de Chow de V que satisface la condición

$$Ch_V(e_0, \ldots, e_r) = 1.$$

En otras palabras, Ch_V es la forma de Chow de V para la cual el coeficiente del monomio $U_{00}^D \ldots U_{rr}^D$ es 1.

Para una variedad V de dimensión cero, se tiene que la forma de Chow normalizada de V es

$$Ch_V = \prod_{\xi \in V} L_0(U_0, \xi).$$

Observamos también que la forma de Chow normalizada de una variedad afín equidimensional es el producto de las formas de Chow normalizadas de sus componentes irreducibles.

4.2 Un caso fundamental

En esta sección se presenta un algoritmo que, bajo ciertas hipótesis, calcula la forma de Chow de una variedad afín equidimensional V a partir de un sistema finito de polinomios que define la variedad y una resolución geométrica de una fibra cero-dimensional de V por una proyección.

4.2.1 Enunciado del resultado

Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r. Supondremos que la variedad V satisface la siguiente hipótesis:

Hipótesis 4.2.1 *La proyección $\pi_V : V \to \mathbb{A}^r$ definida por $x \mapsto (x_1, \ldots, x_r)$ verifica $\#\pi_V^{-1}(0) = \deg V$ (es decir, $\deg(V \cap V(X_1, \ldots, X_r)) = \deg V$).*

La hipótesis 4.2.1 implica, por el teorema de la dimensión de las fibras, que la proyección $\pi_V : V \to \mathbb{A}^r$ es un morfismo dominante. Más aún, la proyección π_V es finita, es decir, las variables $X_1, \ldots, X_r$ están en posición de Noether con respecto a V (ver [25, Lemma 2.14]), y es un morfismo de grado $D := \deg V$.

Observamos que la condición 4.2.1 puede obtenerse mediante un cambio lineal genérico de variables (ver [25, Proposition 4.5]).

De la condición $\#\pi_V^{-1}(0) = \deg V$ se desprende que, si $\overline{V} \subset \mathbb{P}^n$ es la clausura proyectiva de V, la variedad $\overline{V} \cap \{x_1 = 0\} \cap \ldots \cap \{x_r = 0\}$ es una variedad cero-dimensional sin puntos en el hiperplano $\{x_0 = 0\}$ del infinito, es decir

$$\overline{V} \cap \{x_0 = 0\} \cap \{x_1 = 0\} \ldots \cap \{x_r = 0\} = \emptyset.$$

Tiene sentido entonces hablar de *la* forma de Chow (normalizada) de V.

Para la aplicación de nuestro algoritmo necesitaremos también ciertas condiciones técnicas adicionales sobre la variedad V y sobre los polinomios dados para definirla.

Definición 4.2.2 *Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r. Diremos que V es una* intersección completa reducida *en un abierto $U \subset \mathbb{A}^n$ si existen $n - r$ polinomios $f_1, \ldots, f_{n-r} \in k[X_1, \ldots, X_n]$ tales que*

- $V = \overline{V(f_1, \ldots, f_{n-r}) \cap U}$

- *Si $\mathcal{Q}$ es una componente primaria del ideal $(f_1, \ldots, f_{n-r})$ tal que $V(\mathcal{Q}) \cap U \neq \emptyset$, entonces $\mathcal{Q}$ es un ideal primo de $k[X_1, \ldots, X_n]$.*

Si $f_1, \ldots, f_{n-r} \in k[X_1, \ldots, X_n]$ verifican las condiciones anteriores, diremos también que estos polinomios forman una intersección completa reducida para V en el abierto U.

Observamos que en el caso en que $U = \{g \neq 0\}$ es un abierto básico de $\mathbb{A}^n$, la segunda condición de la definición equivale a que el ideal $(f_1, \ldots, f_{n-r})_g$ sea un ideal radical de $k[X_1, \ldots, X_n]_g$.

Con estas definiciones e hipótesis, podemos enunciar el resultado principal de esta sección:

Proposición 4.2.3 *Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r que satisface la hipótesis 4.2.1. Supongamos que V es intersección completa reducida en un abierto básico $\{g \neq 0\}$ de $\mathbb{A}^n$ que contiene a $V \cap V(X_1, \ldots, X_r)$. Entonces existe un algoritmo que tomando como entrada:*

- *un conjunto de polinomios $\{f_1, \ldots, f_{n-r}\}$, dados por un straight-line program, que forman una intersección completa reducida para V en el abierto $\{g \neq 0\}$ y*
- *una resolución geométrica de $V \cap V(X_1, \ldots, X_r)$*

produce un straight-line program que representa la forma de Chow Ch_V de V.

Si $D := \deg V$, $d := \max\{\deg f_i : 1 \leq i \leq n-r\}$ y L es la longitud del straight-line program que codifica los polinomios $f_1, \ldots, f_{n-r}$, la complejidad del algoritmo y la longitud del straight-line program que produce son de orden $(ndD)^{O(1)}L$.

Antes de dar la demostración de esta proposición, necesitamos probar algunos resultados auxiliares en los que se basa el algoritmo construido:

En la Sección 4.2.2 se probará una fórmula multiplicativa para la forma de Chow. A continuación (Sección 4.2.3) se verá que esta fórmula permite escribir dicha forma de Chow como un cociente de dos series y luego (Sección 4.2.4) se dará un algoritmo que a partir de los desarrollos de las series hasta cierto grado calcula el polinomio cociente. Finalmente, en la Sección 4.2.5 se demostrará la Proposición 4.2.3.

4.2.2 Una fórmula multiplicativa para la forma de Chow

En esta sección se prueba una fórmula multiplicativa para la forma de Chow de una variedad algebraica afín equidimensional que satisface la hipótesis 4.2.1. Esta fórmula es análoga a la fórmula clásica de Poisson para la resultante [6, Ch.3, Theorem 3.4] y es uno de los resultados técnicos básicos para el algoritmo para el cálculo de la forma de Chow que se presentará.

Sea $V \subset \mathbb{A}^n(\bar{k})$ una variedad equidimensional de dimensión r y grado D definible sobre k. Sea $I(V)$ el ideal de $k[X_1, \ldots, X_n]$ formado por los polinomios que se anulan sobre V. Sean $U_0, \ldots, U_r$ grupos de $n+1$ nuevas variables cada uno y consideremos las formas lineales asociadas

$$L_i := U_{i0} + U_{i1}X_1 + \cdots + U_{in}X_n \qquad i = 0, \ldots, r.$$

Consideremos el ideal I^0 definido por

$$I^0 := (I(V), L_0, \ldots, L_{r-1}) \subset k(U_0, \ldots, U_{r-1})[X]$$

y la variedad

$$V^0 = V(I^0) \subset \mathbb{A}^n(\overline{k(U_0, \ldots, U_{r-1})}).$$

Observamos que si $I(V)^e$ denota el ideal extendido de $I(V)$ al anillo de polinomios $k(U_0, \ldots, U_{r-1})[X_1, \ldots, X_n]$, entonces $V^0 = V(I(V)^e) \cap V(L_0, \ldots, L_{r-1})$, de donde se deduce que $\dim(V^0) = \dim(V) - r = 0$ y $\deg V^0 = \deg V = D$.

Lema 4.2.4 *Con las hipótesis y notaciones anteriores, sea $\mathcal{F}_V \in k[U_0, \ldots, U_r]$ una forma de Chow de V y sea $\mathcal{F}_{V^0} \in k(U_0, \ldots, U_{r-1})[\tilde{U}]$ una forma de Chow de V^0 (donde $\tilde{U}$ denota un grupo de $n+1$ nuevas variables).*
Entonces existe un elemento $P \in k(U_0, \ldots, U_{r-1}) - \{0\}$ que satisface:

$$\mathcal{F}_V(U_0, U_1, \ldots, U_r) = P(U_0, \ldots, U_{r-1})\, \mathcal{F}_{V^0}(U_r).$$

Demostración. Denotemos por X al grupo de variables $(X_1, \ldots, X_n)$.
Sea $I := I(V) + (L_0, \ldots, L_r) \subset k[U_0, \ldots, U_r, X]$. De acuerdo a lo visto en la Sección 4.1.1, el ideal I es radical y una forma de Chow $\mathcal{F}_V$ de V es un polinomio en $k[U_0, \ldots, U_r]$ que satisface

$$(\mathcal{F}_V) = I \cap k[U_0, \ldots, U_r].$$

Consideremos el conjunto multiplicativamente cerrado $S := k[U_0, \ldots, U_{r-1}] - \{0\}$. Se tiene que $S^{-1}(I(V) + (L_0, \ldots, L_{r-1}))$ es un ideal radical del anillo de polinomios $k(U_0, \ldots, U_{r-1})[X_1, \ldots, X_n]$ y coincide con el ideal I^0.
Entonces, si $\tilde{U} := (\tilde{U}_0, \tilde{U}_1, \ldots, \tilde{U}_n)$ denota un grupo de $n+1$ indeterminadas sobre $k(U_0, \ldots, U_{r-1})$ y $\tilde{L} := \tilde{U}_0 + \tilde{U}_1 X_1 + \cdots + \tilde{U}_n X_n$ es la forma lineal asociada, una forma de Chow $\mathcal{F}_{V^0}$ de V^0 es un polinomio en $k(U_0, \ldots, U_{r-1})[\tilde{U}]$ que satisface

$$(\mathcal{F}_{V^0}) = (I^0, \tilde{L}) \cap k(U_0, \ldots, U_{r-1})[\tilde{U}].$$

Por otro lado, vemos que

$$(I^0, L_r) = (S^{-1}(I(V) + (L_0, \ldots, L_{r-1})), L_r) = S^{-1}(I(V) + (L_0, \ldots, L_r)) = S^{-1}I$$

de donde, teniendo en cuenta que U_r es un grupo de $n+1$ indeterminadas sobre $k(U_0, \ldots, U_{r-1})$ y que L_r es la forma lineal asociada a U_r, resulta que

$$(\mathcal{F}_{V^0}(U_r)) = (I^0, L_r) \cap k(U_0, \ldots, U_{r-1})[U_r] = S^{-1}(I \cap k[U_0, \ldots, U_r]) = S^{-1}(\mathcal{F}_V).$$

De esta última igualdad concluimos que existe $P \in k(U_0, \ldots, U_{r-1}) - \{0\}$ que satisface

$$\mathcal{F}_V(U_0, \ldots, U_r) = P(U_0, \ldots, U_{r-1})\, \mathcal{F}_{V^0}(U_r).$$

□

El siguiente lema relaciona la forma de Chow de una variedad afín equidimensional V con la forma de Chow de la intersección de V con un hiperplano adecuado.

Lema 4.2.5 *Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado D que satisface la hipótesis 4.2.1. Entonces:*

(1) La variedad $V \cap V(X_r)$ es equidimensional de dimensión $r-1$ y grado D, y satisface la hipótesis 4.2.1.

(2) Si $Ch_V \in k[U_0, \ldots, U_r]$ y $Ch_{V \cap V(X_r)} \in k[U_0, \ldots, U_{r-1}]$ son las formas de Chow normalizadas de V y $V \cap V(X_r)$ respectivamente, y e_r denota el $(r+1)$-ésimo vector de la base canónica de k^{n+1}, se tiene que

$$Ch_V(U_0, \ldots, U_{r-1}, e_r) = Ch_{V \cap V(X_r)}(U_0, \ldots, U_{r-1}).$$

Demostración.

(1) Sea $\pi_V : V \to \mathbb{A}^r$ la proyección sobre las primeras r coordenadas.

Por hipótesis, $\#\pi_V^{-1}(0) = \deg V$. Se tiene que

$$\pi_V^{-1}(0) = \bigcup_C \pi_C^{-1}(0)$$

donde la unión recorre el conjunto de las componentes irreducibles de V.

Cada una de las componentes irreducibles C de V verifica $\dim C = r$. Además $C \cap V(X_1, \ldots, X_r)$ es un conjunto finito con $\#C \cap V(X_1, \ldots, X_r) \leq \deg C$ puntos. Entonces

$$\deg V = \#\pi_V^{-1}(0) \leq \sum_C \#\pi_C^{-1}(0) = \sum_C \#C \cap V(X_1, \ldots, X_r) \leq \sum_C \deg C = \deg V$$

de donde resulta que $\#C \cap V(X_1, \ldots, X_r) = \deg C$ para toda componente irreducible C de V.

En particular, si C es una componente irreducible de V, resulta que $C \cap V(X_r) \neq \emptyset$, y entonces es equidimensional de dimensión $r-1$. Luego $V \cap V(X_r)$ es equidimensional de dimensión $r-1$.

Por otro lado,

$$\deg V \geq \deg(V \cap V(X_r)) \geq \deg(V \cap V(X_r) \cap V(X_1, \ldots, X_{r-1})) = \#\pi_V^{-1}(0) = \deg V$$

lo que implica que $\deg(V \cap V(X_r)) = \deg V$.

(2) Sea Ch_V la forma de Chow normalizada de V y consideremos el polinomio $Ch_V(U_0, \ldots, U_{r-1}, e_r)$ que se obtiene al evaluar el grupo de variables U_r en el $(r+1)$-ésimo vector de la base canónica de k^{n+1}.

Para $i = 0, \ldots, r$, notaremos por $\overline{L_i} := U_{i0}X_0 + U_{i1}X_1 + \cdots + U_{in}X_n$, la homogeneización de L_i con respecto a la variable X_0.

Por la definición de la forma de Chow, se tiene que $Ch_V(u_0, \ldots, u_{r-1}, e_r) = 0$ si y sólo si

$$\overline{V} \cap \{\overline{L_0}(u_0, x) = 0, \ldots, \overline{L_{r-1}}(u_{r-1}, x) = 0\} \cap V(X_r) \neq \emptyset$$

o, equivalentemente, $Ch_{\overline{V} \cap V(X_r)}(u_0, \ldots, u_{r-1}) = 0$.

Puesto que $Ch_{\overline{V} \cap V(X_r)}$ es un polinomio libre de cuadrados, la equivalencia anterior implica que $Ch_{\overline{V} \cap V(X_r)}(U_0, \ldots, U_{r-1})$ divide a $Ch_V(U_0, \ldots, U_{r-1}, e_r)$.

Observamos que las variedades proyectivas $\overline{V} \cap V(X_r)$ y $\overline{V \cap V(X_r)}$ coinciden:

Como $V \cap V(X_r) \subset \overline{V} \cap V(X_r)$, se tiene que $\overline{V \cap V(X_r)} \subset \overline{V} \cap V(X_r)$. Además, de lo demostrado en (1) se deduce que $\overline{V \cap V(X_r)}$ y $\overline{V} \cap V(X_r)$ son equidimensionales de la misma dimensión $(r-1)$ y el mismo grado $(\deg V)$. Luego, $\overline{V} \cap V(X_r) = \overline{V \cap V(X_r)}$.

En consecuencia, $Ch_{\overline{V} \cap V(X_r)}(U_0, \ldots, U_{r-1}) = Ch_{V \cap V(X_r)}(U_0, \ldots, U_{r-1})$.

Teniendo en cuenta que el grado del polinomio $Ch_V(U_0, \ldots, U_{r-1}, e_r)$ en cada grupo de variables está acotado por $D = \deg V$ y que el grado de $Ch_{V \cap V(X_r)}(U_0, \ldots, U_{r-1})$ en cada grupo de variables es $\deg(V \cap V(X_r)) = D$, concluimos que los polinomios coinciden salvo por un factor constante, es decir, existe $c \in k - \{0\}$ tal que

$$Ch_V(U_0, \ldots, U_{r-1}, e_r) = c \cdot Ch_{V \cap V(X_r)}(U_0, \ldots, U_{r-1})$$

Finalmente, las normalizaciones impuestas a Ch_V y $Ch_{V \cap V(X_r)}$, implican que $c = 1$, de donde

$$Ch_V(U_0, \ldots, U_{r-1}, e_r) = Ch_{V \cap V(X_r)}(U_0, \ldots, U_{r-1}).$$

□

Los Lemas 4.2.4 y 4.2.5 se aplicarán recursivamente para obtener una fórmula multiplicativa para la forma de Chow de una variedad equidimensional V.

Comenzamos estableciendo algunas notaciones que utilizaremos en lo que sigue:

Sea $V \subset \mathbb{A}^n(\overline{k})$ una variedad equidimensional de dimensión r y grado D definible sobre k que satisface la hipótesis 4.2.1.

Para cada i con $0 \leq i < r$, definimos

$$V_{(i)} := V \cap V(X_{i+1}, \ldots, X_r) \subset \mathbb{A}^n(\overline{k}).$$

Notaremos también $V_{(r)} := V$.

Denotemos por $I(V_{(i)})$ al ideal de $k[X_1, \ldots, X_n]$ formado por los polinomios que se anulan sobre $V_{(i)}$.

Sea i con $1 \leq i \leq r$. Consideremos el cuerpo $K_i := k(U_0, \ldots, U_{i-1})$. Sea $I(V_{(i)})^e$ la extensión del ideal $I(V_{(i)})$ al anillo de polinomios $K_i[X_1, \ldots, X_n]$. Finalmente, sea

$$V_{(i)}^0 := V(I(V_{(i)})^e) \cap V(L_0, \ldots, L_{i-1}) \subset \mathbb{A}^n(\overline{K}_i).$$

Aplicando el Lema 4.2.5 sucesivamente a las variedades $V_{(r)}, \ldots, V_{(0)}$ se deduce que:

Observación 4.2.6 Para $i = 0, \ldots, r$, $V_{(i)}$ es una variedad equidimensional con $\dim(V_{(i)}) = i$ y $\deg(V_{(i)}) = \deg V = D$, que satisface la hipótesis 4.2.1.

De esta observación se desprende que:

Observación 4.2.7 Para cada $0 \leq i \leq r$, $V^0_{(i)} \subset \mathbb{A}^n(\overline{K_i})$ es una variedad de dimensión $\dim(V^0_{(i)}) = \dim(V_{(i)}) - i = 0$ y grado $\deg(V^0_{(i)}) = \deg(V_{(i)}) = D$, es decir

$$V^0_{(i)} = \{\gamma^{(i)}_1, \ldots, \gamma^{(i)}_D\}.$$

En consecuencia, si $\tilde{U}_i$ denota un grupo de $n+1$ indeterminadas sobre K_i y L la forma lineal asociada a $\tilde{U}_i$, la forma de Chow normalizada de $V^0_{(i)}$ es

$$Ch_{V^0_{(i)}}(\tilde{U}_i) = \prod_{j=1}^{D} L(\tilde{U}_i, \gamma^{(i)}_j).$$

Para cada $1 \leq i \leq r$, notaremos también

$$\Gamma_i := \prod_{j=1}^{D} \gamma^{(i)}_{ji},$$

donde $\gamma^{(i)}_{jk}$ $(1 \leq k \leq n)$ denota la k-ésima coordenada del vector $\gamma^{(i)}_j$ $(1 \leq j \leq D)$. Observamos que, para cada $1 \leq i \leq r$, $\Gamma_i = Ch_{V^{(0)}_{(i)}}(e_i)$ y, por lo tanto, es un elemento de $k(U_0, \ldots, U_{i-1})$.

Proposición 4.2.8 *Sea $V \subset \mathbb{A}^n(\overline{k})$ una variedad equidimensional de dimensión r y grado D, definible sobre k, que satisface la hipótesis 4.2.1. Entonces, con las notaciones anteriores, vale la siguiente igualdad en $k(U_0, \ldots, U_{r-1})[U_r]$:*

$$Ch_V(U_0, \ldots, U_r) = Ch_{V_{(0)}}(U_0) \prod_{1 \leq i \leq r} \frac{Ch_{V^0_{(i)}}(U_i)}{\Gamma_i}$$

Demostración. Sea i con $1 \leq i \leq r$. Por el Lema 4.2.4 aplicado a la variedad $V_{(i)} = V \cap V(X_{i+1}, \ldots, X_r)$ (ver Observación 4.2.6), existe $P_i \in k(U_0, \ldots, U_{i-1}) - \{0\}$ tal que

$$Ch_{V_{(i)}}(U_0, \ldots, U_i) = P_i(U_0, \ldots, U_{i-1})\, Ch_{V^0_{(i)}}(U_i). \tag{4.1}$$

Especializamos en la igualdad anterior $U_i = e_i$, donde e_i denota el $(i+1)$-ésimo vector de la base canónica de k^{n+1}. Teniendo en cuenta la Observación 4.2.7, se obtiene

$$Ch_{V_{(i)}}(U_0, \ldots, U_{i-1}, e_i) = P_i(U_0, \ldots, U_{i-1}) \prod_{j=1}^{D} \gamma^{(i)}_{ji}.$$

Como $V_{(i-1)} = V_{(i)} \cap V(X_i)$, utilizando la relación dada por el Lema 4.2.5 (2) aplicado a $V_{(i)}$ y la definición de Γ_i, esta igualdad puede reescribirse como

$$Ch_{V_{(i-1)}}(U_0, \ldots, U_{i-1}) = P_i(U_0, \ldots, U_{i-1})\, \Gamma_i. \tag{4.2}$$

Finalmente, las ecuaciones (4.1) y (4.2) nos dan la siguiente relación:

$$\frac{Ch_{V_{(i)}}(U_0, \ldots, U_i)}{Ch_{V_{(i-1)}}(U_0, \ldots, U_{i-1})} = \frac{Ch_{V^0_{(i)}}(U_i)}{\Gamma_i}$$

Aplicando la igualdad anterior para $i = 1, \ldots, r$ se obtiene la fórmula

$$\begin{aligned} Ch_V(U_0, \ldots, U_r) &= Ch_{V_{(0)}}(U_0) \cdot \prod_{i=1}^{r} \frac{Ch_{V_{(i)}}(U_0, \ldots, U_i)}{Ch_{V_{(i-1)}}(U_0, \ldots, U_{i-1})} \\ &= Ch_{V_{(0)}}(U_0) \cdot \prod_{i=1}^{r} \frac{Ch_{V^0_{(i)}}(U_i)}{\Gamma_i} \end{aligned}$$

4.2.3 La forma de Chow como un cociente de dos series

En la sección anterior probamos una fórmula multiplicativa que relaciona la forma de Chow de una variedad equidimensional V de dimensión r y grado D que satisface la hipótesis 4.2.1 con las de las variedades definidas, para cada $0 \leq i \leq r$, como:

$$\begin{aligned} V_{(i)} &:= V \cap V(X_{i+1}, \ldots, X_r) \subset \mathbb{A}^n(\overline{k}) \\ V^0_{(i)} &:= V(I(V_{(i)})^e) \cap V(L_0, \ldots, L_{i-1}) \subset \mathbb{A}^n(\overline{k(U_0, \ldots, U_{i-1})}) \end{aligned}$$

Dicha fórmula multiplicativa nos permitirá calcular la forma de Chow de V como un cociente de dos series, las que serán aproximadas utilizando el método de Newton presentado en la Sección 1.4.3.

Para hacer esto, el algoritmo de la Proposición 4.2.3 trabaja con una familia de polinomios $\{f_1, \ldots, f_{n-r}\}$ que es una intersección completa reducida para la variedad V considerada en un abierto $\{g \neq 0\}$.

El siguiente lema prueba que la hipótesis 4.2.1 más la condición adicional $V \cap V(X_1, \ldots, X_r) \subset \{g \neq 0\}$ aseguran que todos los cálculos intermedios pueden llevarse a cabo trabajando en el abierto $\{g \neq 0\}$.

Lema 4.2.9 *Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r que satisface la hipótesis 4.2.1. Sea $g \in k[X_1, \ldots, X_n]$ un polinomio tal que*

$$\overline{V \cap \{g \neq 0\}} = V \qquad y \qquad V \cap V(X_1, \ldots, X_r) \subset \{g \neq 0\}.$$

Finalmente, para cada $0 \leq i \leq r$, sean $V_{(i)} \subset \mathbb{A}^n(\bar{k})$ y $V_{(i)}^0 \subset \mathbb{A}^n(\overline{k(U_0, \ldots, U_{i-1})})$ definidas como antes. Entonces:

(1) $\overline{V_{(i)} \cap \{g \neq 0\}} = V_{(i)}$ para todo i con $0 \leq i \leq r-1$

(2) Para cada $0 \leq i \leq r$, $V_{(i)}^0 \subset \{g \neq 0\}$.

Demostración.

(1) Consideremos en primer lugar el caso $i = 0$. Se tiene que

$$V_{(0)} \cap \{g \neq 0\} = V \cap V(X_1, \ldots, X_r) \cap \{g \neq 0\} = V \cap V(X_1, \ldots, X_r) = V_{(0)}$$

donde la segunda igualdad es consecuencia de que $V \cap V(X_1, \ldots, X_r) \subset \{g \neq 0\}$. Luego, $\overline{V_{(0)} \cap \{g \neq 0\}} = V_{(0)}$.

Pasemos ahora al caso general:

Sea i con $1 \leq i < r$. Es claro que vale la inclusión $\overline{V_{(i)} \cap \{g \neq 0\}} \subset V_{(i)}$.

Como la variedad $V_{(i)}$ es equidimensional de dimensión i (ver Observación 4.2.6), entonces $\overline{V_{(i)} \cap \{g \neq 0\}}$ es o bien vacía o bien equidimensional de dimensión i.

Ahora,

$$V_{(i)} \cap \{g \neq 0\} \cap V(X_1, \ldots, X_i) = V_{(0)} \cap \{g \neq 0\} = V_{(0)} \tag{4.3}$$

de donde se deduce en particular que $V_{(i)} \cap \{g \neq 0\} \neq \emptyset$ y entonces $\overline{V_{(i)} \cap \{g \neq 0\}}$ es equidimensional de dimensión i.

Más aún, la igualdad (4.3) implica que $\deg(\overline{V_{(i)} \cap \{g \neq 0\}}) \geq \deg V_{(0)}$. Teniendo en cuenta que $\deg V_{(i)} = \deg V_{(0)}$ (Observación 4.2.6), la inclusión que ya hemos demostrado y la igualdad de dimensiones, concluimos que $\overline{V_{(i)} \cap \{g \neq 0\}} = V_{(i)}$.

(2) Por lo demostrado en (1) y la Observación 4.2.6, basta considerar el caso de una variedad equidimensional V de dimensión r que satisface la hipótesis 4.2.1 y un abierto $\{g \neq 0\}$ con:

$$\overline{V \cap \{g \neq 0\}} = V \quad \text{y} \quad V \cap V(X_1, \ldots, X_r) \subset \{g \neq 0\}.$$

Sean $U_0, \ldots, U_{r-1}$ grupos de $n+1$ variables y sean $L_0, \ldots, L_{r-1}$ las formas lineales asociadas. Sea

$$V^0 = V(I(V), L_0, \ldots, L_{r-1}) \subset \mathbb{A}^n(\overline{k(U_0, \ldots, U_{r-1})}).$$

Consideremos la variedad

$$\mathcal{V}^0 := \{(u, x) \in \mathbb{A}^{r(n+1)} \times \mathbb{A}^n : x \in V, L_0(u_0, x) = 0, \ldots, L_{r-1}(u_{r-1}, x) = 0\}$$

Observamos que $I(V^0)$ se obtiene localizando en el conjunto multiplicativamente cerrado $k[U_0, \ldots, U_{r-1}] - \{0\}$ el ideal $I(\mathcal{V}^0)$.

La condición $\overline{V \cap \{g \neq 0\}} = V$ equivale a que g no se anula idénticamente sobre ninguna componente irreducible de V, luego, tampoco se anula idénticamente en ninguna componente irreducible de $\mathcal{V}^0$.

En consecuencia, g no se anula en ningún punto de V^0.

A continuación probamos un resultado técnico acerca del ideal de una variedad equidimensional intersección completa reducida que satisface la hipótesis 4.2.1. De este resultado se deduce la validez de las hipótesis que posibilitan la aplicación del algoritmo de Newton (ver 1.4.6) para aproximar los puntos de las variedades cero-dimensionales involucradas en la fórmula multiplicativa dada en la Proposición 4.2.8.

Lema 4.2.10 *Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r que satisface la hipótesis 4.2.1 y es intersección completa reducida en un abierto $\{g \neq 0\}$ que contiene a $V \cap V(X_1, \ldots, X_r)$. Entonces, el ideal $I(V) + (X_1, \ldots, X_r)$ es un ideal radical de $k[X_1, \ldots, X_n]$.*

Demostración. Sean $f_1, \ldots, f_{n-r} \in k[X_1, \ldots, X_n]$ polinomios que forman una intersección completa reducida para V en el abierto $\{g \neq 0\}$, es decir, tales que $I(V)_g = (f_1, \ldots, f_{n-r})_g$.

Para cada $1 \leq i \leq r$ sea $I_i := I(V) + (X_{i+1}, \ldots, X_r) \subset k[X_1, \ldots, X_n]$.

Veremos recursivamente para $i = r, r-1, \ldots, 0$, que el ideal $(I_i)_g \subset k[X_1, \ldots, X_n]_g$ es radical. Más precisamente, si $V_{(i)} := V \cap V(X_{i+1}, \ldots, X_r)$, se probará que $(I_i)_g = I(V_{(i)})_g$.

En primer lugar observamos que $(I_i)_g = (f_1, \ldots, f_{n-r}, X_{i+1}, \ldots, X_r)_g$ es un ideal de codimensión $n-i$ generado por $n-i$ polinomios en el anillo $k[X_1, \ldots, X_n]_g$, que es Cohen-Macaulay. Por lo tanto, todo primo asociado a $(I_i)_g$ es minimal (ver [8, Corollary 18.14]). Entonces, las componentes primarias de $(I_i)_g$ se corresponden biyectivamente con las componentes irreducibles de la variedad $\overline{V(I_i) \cap \{g \neq 0\}} = V_{(i)}$. Por otro lado, puesto que $V_{(i)}$ satisface la hipótesis 4.2.1, para cada componente irreducible C de $V_{(i)}$, se tiene que $I(C) \cap k[X_1, \ldots, X_i] = \{0\}$. Entonces para cada componente primaria $\mathcal{Q}$ del ideal $(I_i)_g$ vale $\mathcal{Q} \cap k[X_1, \ldots, X_i] = \{0\}$, y lo mismo sucede para cada componente de $I(V_{(i)})_g$.

Esto implica que, si $k_i := k(X_1, \ldots, X_i)$ y consideramos las extensiones I_i^e y $I(V_{(i)})^e$ de los ideales $(I_i)_g$ y $I(V_{(i)})_g$ al anillo de polinomios $k_i[X_{i+1}, \ldots, X_n]_g$, vale

$$(I_i)_g = I_i^e \cap k[X_1, \ldots, X_n]_g \quad \text{y} \quad I(V_{(i)})_g = I(V_{(i)})^e \cap k[X_1, \ldots, X_n]_g.$$

En consecuencia

$$(I_i)_g = I(V_{(i)})_g \iff I_i^e = I(V_{(i)})^e. \tag{4.4}$$

Por definición, $I_r = I(V)$ es radical, luego $(I_r)_g$ también lo es.

Sea ahora i con $0 \leq i \leq r-1$ y supongamos que $(I_{i+1})_g = I(V_{(i+1)})_g$.

De acuerdo a (4.4), basta ver que $I_i^e = I(V_{(i)})^e$, lo que es equivalente a la condición

$$\dim_{k_i} k_i[X_{i+1}, \ldots, X_n]_g / I_i^e = \dim_{k_i} k_i[X_{i+1}, \ldots, X_n]_g / I(V_{(i)})^e,$$

puesto que $\operatorname{rad}(I_i^e) = I(V_{(i)})^e$ y son ideales cero-dimensionales de $k_i[X_{i+1}, \ldots, X_n]_g$.

Sean $a_1, \ldots, a_N \in k[X_1, \ldots, X_n]$ tales que $\bar{a}_1, \ldots, \bar{a}_N \in k_i[X_{i+1}, \ldots, X_n]_g / I_i^e$ es un conjunto k_i-linealmente independiente. Veamos que las clases de $a_1, \ldots, a_N$ en $k_{i+1}[X_{i+2}, \ldots, X_n]_g / I_{i+1}^e$ son k_{i+1}-linealmente independientes.

Si no lo fueran, existirían $g_1, \ldots, g_N \in k_{i+1}$ tales que $g_1 a_1 + \ldots + g_N a_N \in I_{i+1}^e$. Multiplicando por un polinomio no nulo en $k[X_1, \ldots, X_{i+1}]$ podemos suponer que

$$g_1 a_1 + \cdots + g_N a_N \in (I_{i+1})_g$$

Por hipótesis inductiva, se tiene que $(I_{i+1})_g = I(V_{(i+1)})_g$ y, como X_{i+1} no se anula idénticamente en $V_{(i+1)}$, resulta que X_{i+1} no es divisor de cero módulo $(I_{i+1})_g$. Podemos suponer entonces que en la suma anterior $g_{j_0}(X_1, \ldots, X_i, 0) \neq 0$ para algún $1 \leq j_0 \leq N$.

Entonces, poniendo $\tilde{g}_j := g_j(X_1, \ldots, X_i, 0) \in k[X_1, \ldots, X_i]$ para cada $1 \leq j \leq N$, se obtiene

$$\tilde{g}_1 a_1 + \cdots + \tilde{g}_N a_N \in (I_{i+1})_g + (X_{i+1}) = (I_i)_g$$

de donde

$$\tilde{g}_1 \bar{a}_1 + \cdots + \tilde{g}_N \bar{a}_N = 0 \quad \text{en} \quad k_i[X_{i+1}, \ldots, X_n]_g / I_i^e$$

con $\tilde{g}_{j_0} \in k_i - \{0\}$, lo que contradice la independencia lineal de $\bar{a}_1, \ldots, \bar{a}_N$.
En consecuencia,

$$\dim_{k_i} k_i[X_{i+1}, \ldots, X_n]_g / I_i^e \leq \dim_{k_{i+1}} k_{i+1}[X_{i+2}, \ldots, X_n]_g / I_{i+1}^e.$$

Por otro lado, como $\operatorname{rad}((I_i)^e) = I(V_{(i)})^e$, se tiene que

$$\dim_{k_i} k_i[X_{i+1}, \ldots, X_n] / I_i^e \geq \dim_{k_i} k_i[X_{i+1}, \ldots, X_n]_g / I(V_{(i)})^e.$$

Finalmente, teniendo en cuenta que, por la hipótesis inductiva, $I_{i+1}^e = I(V_{(i+1)})^e$ y que la hipótesis 4.2.1 implica que, para cada $0 \leq \ell \leq r$,

$$\dim_{k_\ell} k_\ell[X_{\ell+1}, \ldots, X_n] / I(V_{(\ell)})^e = \deg V,$$

concluimos que

$$\dim_{k_i} k_i[X_{i+1}, \ldots, X_n]_g / I_i^e = \dim_{k_i} k_i[X_{i+1}, \ldots, X_n]_g / I(V_{(i)})^e$$

y, por lo tanto, $I_i^e = I(V_{(i)})^e$.

Para terminar, observamos que, como $V \cap V(X_1, \ldots, X_r) \subset \{g \neq 0\}$, se tiene que

$$I(V) + (X_1, \ldots, X_r) = (I_0)_g \cap k[X_1, \ldots, X_n].$$

La radicalidad de $I(V) + (X_1, \ldots, X_r)$ se sigue entonces de la de $(I_0)_g$.

En lo que sigue notaremos $U := (U_0, \ldots, U_r)$ y $U' := (U_0, \ldots, U_{r-1})$, donde para cada $0 \leq i \leq r$, $U_i := (U_{i0}, \ldots, U_{in})$ es un grupo de $n+1$ variables que forma el conjunto de los coeficientes de una forma lineal genérica L_i. Escribiremos también $e' := (e_1, \ldots, e_r)$ donde e_i es el $(i+1)$-ésimo vector de la base canónica de k^{n+1} (asociado a la forma lineal X_i).

Proposición 4.2.11 *Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r que satisface la hipótesis 4.2.1 y es intersección completa reducida en un abierto $\{g \neq 0\}$ que contiene a $V \cap V(X_1, \ldots, X_r)$. Para cada $1 \leq i \leq r$, sea $V_{(i)}^0 = \{\gamma_1^{(i)}, \ldots, \gamma_D^{(i)}\}$ definida como antes, y sea $\Gamma_i = \prod_{j=1}^{D} \gamma_j^{(i)}$.*

Entonces $Ch_V(U)$ puede expresarse como

$$Ch_V(U) = \frac{\Phi(U)}{\Gamma(U')},$$

donde

$$\begin{aligned} \Phi(U) &:= Ch_{V_{(0)}}(U_0) \prod_{1 \leq i \leq r} Ch_{V_{(i)}^0}(U_i) \quad \in \overline{k}[[U' - e']][U_r] \\ \Gamma(U') &:= \prod_{1 \leq i \leq r} \Gamma_i \quad \in \overline{k}[[U' - e']]. \end{aligned}$$

Demostración. Para cada $0 \leq i \leq r$ sea $V_{(i)} := V \cap V(X_{i+1}, \ldots, X_r) \subset \mathbb{A}^n(\overline{k})$. Sea i con $1 \leq i \leq r$ y sean

$$K_i := k(U_0, \ldots, U_{i-1}) \quad \text{y} \quad V_{(i)}^0 := V(I(V_{(i)})^e) \cap V(L_0, \ldots, L_{i-1}) \subset \mathbb{A}^n(\overline{K_i}),$$

donde $I(V_{(i)})^e$ denota la extensión del ideal de la variedad $V_{(i)}$ al anillo de polinomios $K_i[X_1, \ldots, X_n]$.

Por hipótesis, $V_{(0)}$ es una variedad cero-dimensional del mismo grado que V, luego si $\deg V = D$, $V_{(0)} := \{\gamma_1^{(0)}, \ldots, \gamma_D^{(0)}\}$.

Sea $f_1, \ldots, f_{n-r}$ una familia de polinomios en $k[X_1, \ldots, X_n]$ que forman una intersección completa reducida para V en el abierto $\{g \neq 0\}$. Entonces

$$V = \overline{V(f_1, \ldots, f_{n-r}) \cap \{g \neq 0\}}$$

y $(f_1, \ldots, f_{n-r})_g$ es un ideal radical de $k[X_1, \ldots, X_n]_g$.

Más aún, por el Lema 4.2.9, se verifica también

$$\begin{aligned} V_{(i)} &= \overline{V(f_1, \ldots, f_{n-r}, X_{i+1}, \ldots, X_r) \cap \{g \neq 0\}} \subset \mathbb{A}^n(\overline{k}) \\ V_{(i)}^0 &= V(f_1, \ldots, f_{n-r}, L_0, \ldots, L_{i-1}, X_{i+1}, \ldots, X_r) \cap \{g \neq 0\} \subset \mathbb{A}^n(\overline{K_i}) \end{aligned}$$

Fijemos i, $0 \leq i \leq r-1$, y consideremos la aplicación $F_i : \mathbb{A}^{(n+1)i} \times \mathbb{A}^n \to \mathbb{A}^n$ definida por

$$F_i(U_0, \ldots, U_{i-1}, X) = (f_1(X), \ldots, f_{n-r}(X), L_0(U_0, X), \ldots, L_{i-1}(U_r, X), X_{i+1}, \ldots, X_r).$$

Consideremos la matriz $D_X F_i := \left(\frac{\partial F_{ij}}{\partial X_k}\right)_{1\leq j,k\leq n}$ dada por

$$D_X F_i = \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \frac{\partial f_1}{\partial X_i} & \frac{\partial f_1}{\partial X_{i+1}} & \frac{\partial f_1}{\partial X_r} & \frac{\partial f_1}{\partial X_{r+1}} & \frac{\partial f_1}{\partial X_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{\partial f_{n-r}}{\partial X_1} & \frac{\partial f_{n-r}}{\partial X_i} & \frac{\partial f_{n-r}}{\partial X_{i+1}} & \frac{\partial f_{n-r}}{\partial X_r} & \frac{\partial f_{n-r}}{\partial X_{r+1}} & \frac{\partial f_{n-r}}{\partial X_n} \\ U_{01} & U_{0i} & U_{0i+1} & U_{0r} & U_{0r+1} & U_{0n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ U_{i-11} & U_{i-1i} & U_{i-1i+1} & U_{i-1r} & U_{i-1r+1} & U_{i-1n} \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \vdots & \vdots & & & \vdots & \vdots \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Observamos que para cada $\gamma_j^{(0)} \in V_{(0)}$ se verifica

$$F_i(e_1, \ldots, e_i, \gamma_j^{(0)}) = (f_1(\gamma_j^{(0)}), \ldots, f_{n-r}(\gamma_j^{(0)}), \gamma_{j1}^{(0)}, \ldots, \gamma_{ji}^{(0)}, \gamma_{ji+1}^{(0)}, \ldots, \gamma_{jr}^{(0)}) = 0,$$

puesto que $\gamma_j^{(0)} \in V_{(0)} = V(f_1, \ldots, f_{n-r}, X_1, \ldots, X_r) \cap \{g \neq 0\}$.
Además se tiene que

$$\det(D_X F_i(e_1, \ldots, e_i, \gamma_j^{(0)})) = \pm \det \begin{pmatrix} \frac{\partial f_1}{\partial X_{r+1}}(\gamma_j^{(0)}) & \frac{\partial f_1}{\partial X_n}(\gamma_j^{(0)}) \\ \vdots & \vdots \\ \frac{\partial f_{n-r}}{\partial X_{r+1}}(\gamma_j^{(0)}) & \frac{\partial f_{n-r}}{\partial X_n}(\gamma_j^{(0)}) \end{pmatrix}.$$

Por el Lema 4.2.10, $I(V) + (X_1, \ldots, X_r)$ es un ideal radical de $k[X_1, \ldots, X_n]$. Luego, $I(V)_g + (X_1, \ldots, X_r)_g$ es un ideal radical de $k[X_1, \ldots, X_n]_g$. Pero como $f_1, \ldots, f_{n-r}$ forman una intersección completa reducida para V en el abierto $\{g \neq 0\}$, se tiene que $I(V)_g = (f_1, \ldots, f_{n-r})_g$, de donde resulta que $(f_1, \ldots, f_{n-r}, X_1, \ldots, X_r)_g$ es un ideal radical de $k[X_1, \ldots, X_n]_g$. Del criterio del jacobiano (ver [8, Theorem 18.15]), concluimos que

$$\det \begin{pmatrix} \frac{\partial f_1}{\partial X_{r+1}}(\gamma_j^{(0)}) & \frac{\partial f_1}{\partial X_n}(\gamma_j^{(0)}) \\ \vdots & \vdots \\ \frac{\partial f_{n-r}}{\partial X_{r+1}}(\gamma_j^{(0)}) & \frac{\partial f_{n-r}}{\partial X_n}(\gamma_j^{(0)}) \end{pmatrix} \neq 0,$$

es decir,

$$\det(D_X F_i(e_1, \ldots, e_i, \gamma_j^{(0)})) \neq 0.$$

Entonces, del teorema de la función implícita para polinomios demostrado en el Lema 1.4.6, deducimos que para cada $1 \leq i \leq r$ y para cada $1 \leq j \leq D$, existe un vector de series de potencias $\gamma_j^{(i)} \in \overline{k}[[U_0 - e_1, \ldots, U_{i-1} - e_i]]^n$ que verifica simultáneamente

- $f_1(\gamma_j^{(i)}) = 0, \ldots, f_{n-r}(\gamma_j^{(i)}) = 0$, $L_0(U_0, \gamma_j^{(i)}) = 0, \ldots, L_{i-1}(U_{i-1}, \gamma_j^{(i)}) = 0$, $\gamma_{j\,i+1}^{(i)} = 0, \ldots, \gamma_{jr}^{(i)} = 0$
- $\gamma_j^{(i)}(e_1, \ldots, e_i) = \gamma_j^{(0)}$.

En particular, como $g(\gamma_j^{(0)}) \neq 0$, se verifica también $g(\gamma_j^{(i)}) \neq 0$.

Observamos que, para cada i con $1 \leq i \leq r$, los vectores de series de potencias $\gamma_j^{(i)}$, $1 \leq j \leq D$, son todos distintos, puesto que difieren en su término constante. Por lo tanto, como $\deg V_{(i)}^0 = \deg V_{(i)} = D$, si consideramos una clausura algebraica $\overline{K}_i$ de K_i que contenga a $\overline{k}[[U_0 - e_1, \ldots, U_{i-1} - e_i]]$, estos vectores son *todos* los puntos de la variedad cero-dimensional $V_{(i)}^0$. (Por este motivo los hemos denominado $\gamma_j^{(i)}$ como en la Observación 4.2.7.)

Finalmente, por la Proposición 4.2.8, tenemos que

$$Ch_V(U_0, \ldots, U_r) = Ch_{V_{(0)}}(U_0) \prod_{1 \leq i \leq r} \frac{Ch_{V_{(i)}^0}(U_i)}{\Gamma_i}$$

donde, para cada $1 \leq i \leq r$, $\Gamma_i := \prod_{j=1}^{D} \gamma_{ji}^{(i)}$.

Para cada $1 \leq i \leq r$, como $\gamma_{ji}^{(i)} \in \overline{k}[[U_0 - e_1, \ldots, U_{i-1} - e_i]]$, resulta que $\Gamma_i \in \overline{k}[[U_0 - e_1, \ldots, U_{i-1} - e_i]]$.

Por otro lado, para cada $1 \leq i \leq r$, $V_{(i)}^0$ es una variedad cero-dimensional, y en consecuencia

$$Ch_{V_{(i)}^0}(U_i) = \prod_{j=1}^{D} L_i(U_i, \gamma_j^{(i)}),$$

que es un polinomio en U_i con coeficientes en $\overline{k}[[U_0 - e_1, \ldots, U_{i-1} - e_i]]$. En el caso $i = 0$, definimos $V_{(0)}^0 := V_{(0)}$ y vale la fórmula anterior para $Ch_{V_{(0)}^0}(U_0) \in \overline{k}[U_0]$.

Sea entonces i con $0 \leq i \leq r-1$. Como $\gamma_{j\,i+1}^{(i)} = \ldots = \gamma_{jr}^{(i)} = 0$ para cada $1 \leq j \leq D$, cada uno de los factores de $Ch_{V_{(i)}^0}(U_i)$ es de la forma

$$L_i(U_i, \gamma_j^{(i)}) = U_{i0} + \gamma_{j1}^{(i)} U_{i1} + \ldots + \gamma_{ji}^{(i)} U_{ii} + \gamma_{jr+1}^{(i)} U_{ir+1} + \ldots + \gamma_{jn}^{(i)} U_{in},$$

con lo cual, no depende de la variable $U_{i\,i+1}$. Por lo tanto, el desarrollo de $Ch_{V^0_{(i)}}(U_i)$ como polinomio en potencias de $U_i - e_{i+1}$ coincide con su expansión como polinomio en U_i.

En consecuencia, para cada $0 \leq i \leq r-1$, podemos considerar a $Ch_{V^0_{(i)}}(U_i)$ como una serie de potencias en $\overline{k}[[U_0 - e_1, \ldots, U_i - e_{i+1}]]$. En el caso $i = r$, tenemos $Ch_{V^0_{(r)}}(U_r) \in \overline{k}[[U_0 - e_1, \ldots, U_{r-1} - e_r]][U_r]$.

Con la notación $U := (U_0, \ldots, U_r)$, $U' = (U_0, \ldots, U_{r-1})$ y $e' = (e_1, \ldots, e_r)$, concluimos que

$$Ch_V(U) = \frac{\Phi(U)}{\Gamma(U')},$$

donde

$$\begin{aligned} \Phi(U) &:= \prod_{0 \leq i \leq r} Ch_{V^0_{(i)}}(U_i) \in \overline{k}[[U' - e']][U_r] \\ \Gamma(U') &:= \prod_{1 \leq i \leq r} \Gamma_i \in \overline{k}[[U' - e']]. \end{aligned}$$

4.2.4 La forma de Chow como un cociente de dos polinomios

El siguiente paso para la construcción del algoritmo que calcula la forma de Chow de V es expresar Ch_V como un cociente de dos polinomios en lugar de un cociente de dos series de potencias, para efectuar luego la división aplicando el Lema 1.3.5.

Probaremos un resultado general mediante el cual, a partir de los desarrollos de dos series de potencias cuyo cociente es un polinomio, se obtienen (algorítmicamente) dos polinomios cuyo cociente exacto es el polinomio dado.

Sea U un conjunto de N indeterminadas sobre el cuerpo k y sea $u \in k^N$.

Recordamos que, dada una serie de potencias $\Gamma := \sum_{\alpha \in \mathbb{N}_0^N} \Gamma_\alpha (U-u)^\alpha \in k[[U-u]]$, se define el orden de Γ en u como $\mathrm{ord}_u(\Gamma) := \min\{|\alpha| : \Gamma_\alpha \neq 0\}$.

Proposición 4.2.12 *Sea U un conjunto de N variables sobre k, sea $u \in k^N$ y sean*

$$\Phi := \sum_{\alpha \in \mathbb{N}_0^N} \Phi_\alpha (U-u)^\alpha \quad y \quad \Gamma := \sum_{\alpha \in \mathbb{N}_0^N} \Gamma_\alpha (U-u)^\alpha \in k[[U-u]]$$

series de potencias tales que Φ/Γ es un polinomio en $k[U]$ de grado δ.

Sea $m := \mathrm{ord}_u(\Gamma)$. *Supongamos que todas las componentes homogéneas de grado menor o igual que* $m+\delta$ *de las expansiones de* Φ *y* Γ *alrededor de* u *están dadas por medio de un straight-line program de longitud* L.

Sea $G := \Big(\sum_{|\alpha|=m} \Gamma_\alpha (U-u)^\alpha\Big)^{\delta+1}$. *Entonces:*

(1) Existe un straight-line program de longitud $O(\delta^5 L)$ *que calcula un polinomio* $F \in k[U]$ *que satisface*

$$\frac{\Phi}{\Gamma} = \frac{F}{G}.$$

(2) Si se conoce un punto $\tilde{u} \in k^N$ *tal que* $G(\tilde{u}) \neq 0$, *existe un straight-line program de longitud* $O(\delta^8 L)$ *que calcula el polinomio cociente* Φ/Γ.

Demostración.

(1) Sea $Q(U) := \Phi(U)/\Gamma(U) \in k[U]$ el polinomio cociente y sea t una nueva indeterminada. Consideremos el polinomio

$$\tilde{Q}(U,t) := Q(t\,(U-u)+u) \in k[U,t],$$

que verifica $Q(U) = \tilde{Q}(U,1)$.

Sea $\tilde{\Gamma}(U,t) := \Gamma(t\,(U-u)+u)$. Como $\mathrm{ord}_u(\Gamma) = m$ se tiene que

$$\tilde{\Gamma}(U,t) = \sum_\alpha \Gamma_\alpha\,(U-u)^\alpha\, t^{|\alpha|} = t^m \sum_{j\geq 0} A_j(U) t^j$$

donde, para cada $j \geq 0$, $A_j(U) \in k[U-u]$ es la componente homogénea de grado $m+j$ en la expansión de Γ alrededor de u. En particular, tenemos que $G(U) = A_0(U)^{\delta+1}$.

Consideremos los polinomios

$$P(U,t) := A_0(U)^{\delta+1}\,\tilde{Q}(U,t) \quad \text{y} \quad F(U) := P(U,1).$$

Es claro que

$$Q(U) = \tilde{Q}(U,1) = \frac{P(U,1)}{A_0(U)^{\delta+1}} = \frac{F(U)}{G(U)}.$$

Describiremos entonces una forma alternativa de calcular $P(U,t)$ a partir de las componentes homogéneas de grado menor o igual que $m+\delta$ de las expansiones de las series de potencias Φ y Γ alrededor de u.

Sea

$$\Psi(U,t) := -\sum_{j\geq 1} \frac{A_j(U)}{A_0(U)}\, t^j \ \in k(U-u)[[t]].$$

Observamos que

$$\frac{t^m}{\tilde{\Gamma}(U,t)} = \frac{1}{\sum\limits_{j\geq 0} A_j(U)\, t^j} = \frac{1}{A_0(U)\,(1-\Psi(U,t))} = \frac{1}{A_0(U)} \sum_{k\geq 0} \Psi(U,t)^k.$$

Consideremos ahora $\tilde{\Phi}(U,t) := \Phi(t\,(U-u)+u)$. Puesto que $\Phi(U)/\Gamma(U) \in k[U]$, deducimos que $\mathrm{ord}_u(\Phi) \geq \mathrm{ord}_u(\Gamma) = m$. Entonces

$$\tilde{\Phi}(U,t) = \sum_{\alpha} \Phi_\alpha\,(U-u)^\alpha\, t^{|\alpha|} = t^m \sum_{j\geq 0} B_j(U)\, t^j,$$

donde, para cada $j \geq 0$, $B_j(U) \in k[U-u]$ es la componente homogénea de grado $m+j$ en la expansión de Φ alrededor de u.

Finalmente, observemos que valen las siguientes igualdades en $k(U-u)[[t]]$:

$$\begin{aligned} P(U,t) &= A_0(U)^{\delta+1}\, \tilde{Q}(U,t) \\ &= A_0(U)^{\delta+1}\, \frac{\tilde{\Phi}(U,t)}{\tilde{\Gamma}(U,t)} \\ &= A_0(U)^{\delta} \Big(\sum_{j\geq 0} B_j(U)\, t^j\Big)\Big(\sum_{k\geq 0} \Psi(U,t)^k\Big) \\ &= \Big(\sum_{j\geq 0} B_j(U)\, t^j\Big)\Big(\sum_{k\geq 0} A_0(U)^{\delta-k}(A_0(U)\Psi(U,t))^k\Big). \end{aligned}$$

Ahora, teniendo en cuenta que $\deg_t P(U,t) = \deg_t \tilde{Q}(U,t) = \delta$, vemos que para calcular $P(U,t)$ basta obtener los desarrollos hasta grado δ en t de las dos series

$$\sum_{j\geq 0} B_j(U)\, t^j \quad \text{y} \quad \sum_{k\geq 0} A_0(U)^{\delta-k}(A_0(U)\Psi(U,t))^k,$$

efectuar el producto y finalmente truncar el resultado en grado δ con respecto a la variable t.

Como $\Psi(U,t)$ tiene orden mayor o igual que 1 en t, lo que implica que $\Psi(U,t)^k$ tiene orden mayor o igual que k, el polinomio $P(U,t)$ puede obtenerse a partir de

los polinomios

$$\hat{\Phi}(U,t) := \sum_{0\le j\le \delta} B_j(U)\, t^j \tag{4.5}$$

$$\hat{\Psi}(U,t) := -\sum_{1\le j\le \delta} A_j(U)\, t^j \quad \text{y} \tag{4.6}$$

$$\hat{\Theta}(U,t) := \sum_{0\le k\le \delta} A_0(U)^{\delta-k}\hat{\Psi}(U,t)^k, \tag{4.7}$$

calculando el producto $\hat{\Phi}(U,t)\,\hat{\Theta}(U,t)$ y truncando el resultado en grado δ con respecto a t.

Para terminar, se calcula el polinomio F como $F(U) = P(U,1)$.

A continuación se resume el algoritmo que obtiene el straight-line program para F y se calcula su complejidad:

Para cada $0 \le j \le \delta$, sean

$$A_j(U) := \sum_{|\alpha|=m+j} \Gamma_\alpha\,(U-u)^\alpha \quad \text{y} \quad B_j(U) := \sum_{|\alpha|=m+j} \Phi_\alpha\,(U-u)^\alpha.$$

Por hipótesis, estos polinomios están dados por medio de un straight-line program de longitud L.

Algoritmo

Paso 1. Calcular los polinomios $\hat{\Phi}(U,t)$, $\hat{\Psi}(U,t)$, $\hat{\Theta}(U,t)$ dados por las fórmulas (4.5), (4.6) y (4.7) respectivamente, y el producto $\hat{\Phi}(U,t)\,\hat{\Theta}(U,t)$. La longitud del straight-line program que se obtiene es $O(\delta) + L$.

Paso 2. Aplicando el Lema 1.3.3, obtener un straight-line program para todos los coeficientes hasta grado δ del producto $\hat{\Phi}(U,t)\,\hat{\Theta}(U,t)$ considerado como polinomio en la variable t con coeficientes en $k[U]$. Observamos que, si $P_j(U)$ $(0 \le j \le \delta)$, son los coeficientes calculados, entonces $P(U,t) = \sum_{0\le j\le\delta} P_j(U)\, t^j$. La longitud del straight-line program obtenido para los coeficientes de $P(U,t)$ es $O(\delta^5\, L)$.

Paso 3. Calcular $F(U) := P(U,1) = \sum_{0\le j\le\delta} P_j(U)$. La longitud del straight-line program final es $O(\delta^5\, L)$.

(2) Si se conoce un punto $\tilde{u}$ tal que $G(\tilde{u}) \neq 0$, para calcular el cociente F/G se aplica el Lema 1.3.5 a estos polinomios.

Teniendo en cuenta que $\deg(F/G) = \delta$, la longitud del straight-line program obtenido para F en (1), y el hecho que $G(U) := A_0(U)^{\delta+1}$ es calculable por medio de un straight-line program de longitud $\delta + L$, resulta que la longitud del straight-line program final que calcula F/G es de orden $O(\delta^8 L)$.

Recordemos la notación utilizada en la secciones anteriores: Para cada $0 \leq i \leq r$, U_i es un grupo de $n+1$ nuevas indeterminadas sobre k, $U := (U_0, \ldots, U_r)$ y $U' := (U_0, \ldots, U_{r-1})$. Por otro lado, $e' := (e_1, \ldots, e_r)$, donde e_i es el $(i+1)$-ésimo vector de la base canónica de k^{n+1}. Finalmente, notaremos $e := (e', 0)$, donde 0 denota un vector con $n+1$ coordenadas iguales a 0.

La Proposición 4.2.11 asegura la existencia de dos series $\Phi(U) \in \overline{k}[[U' - e']][U_r]$ y $\Gamma(U') \in \overline{k}[[U' - e']]$ cuyo cociente es el polinomio $Ch_V(U)$. Podemos considerar ambas series como elementos de $\overline{k}[[U - e]]$. Finalmente observamos que $\deg \Phi/\Gamma = \deg Ch_V = (r+1)\deg V$ es conocido.

Vemos entonces que, para poder aplicar la proposición anterior a nuestra situación, nos resta calcular $\mathrm{ord}_e(\Gamma)$, que es el orden de $\Gamma \in \overline{k}[[U' - e']]$ en e'.

Proposición 4.2.13 *Bajo las hipótesis y notaciones de la Proposición 4.2.11,*

$$\Gamma(U') = (-1)^{rD} \prod_{0 \leq i \leq r-1} Ch_{V_{(0)}}(U_i) \; + \; O((U' - e')^{rD+1})$$

donde $D := \deg V$. *En particular*

$$\mathrm{ord}_e(\Gamma) = \mathrm{ord}_{e'}(\Gamma) = r\,D.$$

Demostración. Recordemos que, para cada $1 \leq i \leq r$,

$$V^0_{(i)} = V(f_1(X), \ldots, f_{n-r}(X), L_0(U_0, X), \ldots, L_{i-1}(U_{i-1}, X), X_{i+1}, \ldots, X_r) \cap \{g \neq 0\}$$

es la variedad cero-dimensional

$$V^0_{(i)} = \{\gamma_1^{(i)}, \ldots, \gamma_D^{(i)}\} \subset \overline{k}[[U_0 - e_1, \ldots, U_{i-1} - e_i]]^n.$$

Se tiene que $\Gamma = \prod_{1 \leq i \leq r} \Gamma_i$ donde, para cada $1 \leq i \leq r$, $\Gamma_i = \prod_{1 \leq j \leq D} \gamma_{ji}^{(i)}$.

Fijemos i con $1 \leq i \leq r$.

Sea j con $1 \leq j \leq D$. Para simplificar la notación escribiremos $\gamma_j := \gamma_j^{(i)}$.

La i-ésima coordenada $\gamma_{ji} \in \overline{k}[[U_0 - e_1, \ldots, U_{i-1} - e_i]]$ de γ_j puede considerarse como un elemento de $\overline{k}[[U' - e']]$ y entonces es de la forma

$$\gamma_{ji} := \sum_{\alpha} a_\alpha (U' - e')^\alpha \in \overline{k}[[U' - e']].$$

Probaremos que $\mathrm{ord}_{e'}(\gamma_{ji}) = 1$ y calcularemos la parte lineal del desarrollo de esta serie alrededor de e'.

En primer lugar, observamos que $\gamma_j(e_1, \ldots, e_i) = \gamma_j^{(0)}$ (ver la demostración de la Proposición 4.2.11). Entonces $a_0 = \gamma_{ji}(e') = \gamma_{ji}^{(0)} = 0$, puesto que $\gamma_j^{(0)} \in V_{(0)} = V \cap V(X_1, \ldots, X_r)$ y $1 \leq i \leq r$. En particular, $\mathrm{ord}_{e'}(\gamma_{ji}) \geq 1$.

Calcularemos ahora la parte homogénea de grado 1 en la expansión de γ_{ji} centrada en e', es decir, para cada α con $|\alpha| = 1$, el coeficiente $a_\alpha = \frac{\partial \gamma_{ji}}{\partial U'^\alpha}(e')$ (en otras palabras, las derivadas parciales de γ_{ji} con respecto a cada una de las variables $U_{k\ell}$, $0 \leq k < r, 0 \leq \ell \leq n$ especializadas en e').

Como $\gamma_j \in V_{(i)}^0$, se tiene que $L_{i-1}(U_{i-1}, \gamma_j) = 0$, es decir

$$U_{i-1\,0} + U_{i-1\,1}\gamma_{j1} + \cdots + U_{i-1\,n}\gamma_{jn} = 0. \tag{4.8}$$

Derivando esta ecuación respecto de la variable $U_{i-1\,0}$ se obtiene la igualdad

$$1 + U_{i-1\,1}\frac{\partial \gamma_{j1}}{\partial U_{i-1\,0}} + \ldots + U_{i-1\,n}\frac{\partial \gamma_{jn}}{\partial U_{i-1\,0}} = 0.$$

Especializando U' en $e' = (e_1, \ldots, e_r)$ resulta que $\frac{\partial \gamma_{ji}}{\partial U_{i-1\,0}}(e') = -1$. Esto implica que $\mathrm{ord}_{e'}(\gamma_{ji}) = 1$.

Consideremos ahora en (4.8) la derivada con respecto a $U_{i-1\,\ell}$ con $\ell \geq 1$:

$$\gamma_{j\ell} + U_{i-1\,1}\frac{\partial \gamma_{j1}}{\partial U_{i-1\,\ell}} + \cdots + U_{i-1\,n}\frac{\partial \gamma_{jn}}{\partial U_{i-1\,\ell}} = 0$$

de donde obtenemos, especializando U' en e', que $\frac{\partial \gamma_{ji}}{\partial U_{i-1\,\ell}}(e') = -\gamma_\ell(e') = -\gamma_\ell^{(0)}$.

Finalmente, para $0 \leq k < i-1$ y $0 \leq \ell \leq n$, derivando la igualdad (4.8) con respecto a $U_{k\ell}$ resulta

$$U_{i-1\,1}\frac{\partial \gamma_{j1}}{\partial U_{k\ell}} + \cdots + U_{i-1\,n}\frac{\partial \gamma_{jn}}{\partial U_{k\ell}} = 0,$$

lo que implica que $\dfrac{\partial \gamma_{ji}}{\partial U_{k\ell}}(e') = 0$.

Teniendo en cuenta que γ_{ji} no involucra las variables $U_i, \ldots, U_r$, resulta que para todo $k \geq i$ y todo $0 \leq \ell \leq n$ vale $\dfrac{\partial \gamma_{ji}}{\partial U_{k\ell}} \equiv 0$.

En definitiva, para cada $1 \leq i \leq r$ y cada $1 \leq j \leq D$:

$$\frac{\partial \gamma_{ji}^{(i)}}{\partial U_{k\ell}}(e') = \begin{cases} -1 & \text{si } k = i-1, \ell = 0 \\ -\gamma_{ji}^{(0)} & \text{si } k = i-1, 1 \leq \ell \leq n \\ 0 & \text{si } k \neq i-1, 0 \leq \ell \leq n \end{cases}$$

En consecuencia, concluimos que para cada $1 \leq i \leq r$, $1 \leq j \leq D$, la parte lineal de $\gamma_{ji}^{(i)}$ es

$$-(U_{i-1\,0} + U_{i-1\,1}\gamma_{j1}^{(0)} + \cdots + (U_{i-1\,i} - 1)\gamma_{ji}^{(0)} + \cdots + U_{i-1\,n}\gamma_{jn}^{(0)}).$$

Teniendo en cuenta que $\gamma_{j1}^{(0)} = \ldots = \gamma_{jr}^{(0)} = 0$, resulta que la parte lineal de $\gamma_{ji}^{(i)}$ es

$$-(U_{i-1\,0} + U_{i-1\,1}\gamma_{j1}^{(0)} + \cdots + U_{i-1\,r+1}\gamma_{jr+1}^{(0)} + \cdots + U_{i-1\,n}\gamma_{jn}^{(0)}) = -L_{i-1}(U_{i-1}, \gamma_j^{(0)}).$$

Luego

$$\gamma_{ji}^{(i)} = -L_{i-1}(U_{i-1}, \gamma_j^{(0)}) + O((U' - e')^2).$$

Finalmente, como $Ch_{V_{(0)}}(U) = \prod\limits_{1 \leq j \leq D} L(U, \gamma_j^{(0)})$, concluimos que

$$\begin{aligned} \Gamma_i &:= \prod_{1 \leq j \leq D} \gamma_{ji}^{(i)} = \prod_{1 \leq j \leq D} \big(- L_{i-1}(U_{i-1}, \gamma_j^{(0)}) + O((U' - e')^2) \big) \\ &= (-1)^D Ch_{V_{(0)}}(U_{i-1}) + O((U' - e')^{D+1}), \end{aligned}$$

de donde resulta que

$$\begin{aligned} \Gamma(U') &:= \prod_{1 \leq i \leq r} \Gamma_i = (-1)^{rD} \prod_{1 \leq i \leq r} Ch_{V_{(0)}}(U_{i-1}) + O((U' - e')^{rD+1}) \\ &= (-1)^{rD} \prod_{0 \leq i \leq r-1} Ch_{V_{(0)}}(U_i) + O((U' - e')^{rD+1}). \end{aligned}$$

4.2.5 Demostración del resultado principal

Utilizando los resultados y algoritmos presentados en las secciones anteriores, podremos construir el algoritmo para el cálculo de la forma de Chow y demostrar la Proposición 4.2.3.

Hemos visto que la forma de Chow Ch_V que queremos calcular puede expresarse como un cociente de dos polinomios. Estos polinomios se calculan a partir de las series que representan las coordenadas de los puntos de las variedades cero-dimensionales auxiliares $V^0_{(i)} = \{\gamma_1^{(i)}, \ldots, \gamma_D^{(i)}\}$ con $1 \leq i \leq r$.

La aplicación simbólica del algoritmo de Newton (ver Lema 1.4.7) nos permitirá obtener algorítmicamente las componentes homogéneas de las series $\Phi(U)$ y $\Gamma(U')$ involucradas en el cálculo de los polinomios mencionados.

Finalmente, aplicaremos la Proposición 4.2.12 para obtener un straight-line program que evalúa la forma de Chow de V.

Demostración de la Proposición 4.2.3. A lo largo de esta demostración, mantendremos las notaciones utilizadas en las secciones anteriores.

Recordemos que, por las Proposiciones 4.2.11 y 4.2.13, $Ch_V(U) = \Phi(U)/\Gamma(U')$, donde

$$\Phi(U) = \prod_{0\leq i\leq r} Ch_{V^0_{(i)}}(U_i) = \prod_{0\leq i\leq r}\prod_{1\leq j\leq D} L_i(U_i, \gamma_j^{(i)}) \in \overline{k}[[U'-e']][U_r]$$

$$\Gamma(U') = \prod_{1\leq i\leq r} \Gamma_i = \prod_{1\leq i\leq r}\prod_{1\leq j\leq D} \gamma_{ji}^{(i)}$$

$$= (-1)^{rD} \prod_{0\leq i\leq r-1} Ch_{V_{(0)}}(U_i) + O((U'-e')^{rD+1}) \in \overline{k}[[U'-e']].$$

Aplicaremos la Proposición 4.2.12 para calcular Ch_V como el cociente de dos polinomios F y $G \in k[U]$ relacionados con Φ y Γ.

Puesto que $\deg Ch_V = (r+1)\,D$ y, por la Proposición 4.2.13, $\mathrm{ord}_{e'}(\Gamma) = r\,D$, necesitaremos un straight-line program para las componentes homogéneas de grado menor o igual que $(2r+1)\,D$ de los desarrollos de las series de potencias Φ y Γ alrededor de $e := (e', 0)$ (considerando a ambas series como elementos de $\overline{k}[[U-e]]$).

Observamos también que, de la Proposición 4.2.13, se desprende que

$$G(U') = ((-1)^{rD} \prod_{0\leq i\leq r-1} Ch_{V_{(0)}}(U_i))^{(r+1)\,D+1} \tag{4.9}$$

puesto que este polinomio es la $((r+1)D+1)$-ésima potencia de la componente homogénea de grado mínimo del desarrollo de Γ alrededor de e'.

Entonces, conocemos también un punto que no anula a G: si $e_0 := (1,0,\ldots,0) \in k^{n+1}$, se tiene que $G(e_0,\ldots,e_0) = (-1)^{rD} \neq 0$.

Pasamos ahora al cálculo del straight-line program que evalúa las componentes homogéneas de Φ y Γ.

Fijemos i con $1 \leq i \leq r$. Fijemos también una base del espacio vectorial D-dimensional $k[V_{(i)}^0]$. Para cada $0 \leq k \leq n$, sea $M_{X_k}^{(i)}$ la matriz de la multiplicación por X_k en esta base. Entonces valen las siguientes igualdades (ver por ejemplo [6, Proposition 2.7]):

$$\prod_{1\leq j\leq D} L_i(U_i, \gamma_j^{(i)}) = \det(U_{i0}\,\mathrm{Id}_D + U_{i1}\,M_{X_1}^{(i)} + \cdots + U_{in}\,M_{X_n}^{(i)}) \tag{4.10}$$

$$\prod_{1\leq j\leq D} \gamma_{ji}^{(i)} = \det(M_{X_i}^{(i)}). \tag{4.11}$$

Calcularemos las expansiones como series de potencias de (4.10) y (4.11) alrededor de e hasta grado $(2r+1)D$.

Recordemos que, de la demostración del Lema 1.4.6, se desprende que, para cada $1 \leq j \leq D$, el vector de series de potencias $\gamma_j^{(i)}$ puede obtenerse por medio del operador de Newton asociado a la aplicación $F_i : \mathbb{A}^{(n+1)i} \times \mathbb{A}^n \to \mathbb{A}^n$ definida por

$$F_i(U_0,\ldots,U_{i-1},X) = (f_1(X),\ldots,f_{n-r}(X), L_0(U_0,X),\ldots,L_{i-1}(U_{i-1},X), X_{i+1},\ldots,X_r),$$

es decir

$$N_{F_i}(X)^t := X^t - (D_X F_i(U,X))^{-1}(F_i(U,X))^t,$$

como sigue:

Dado $\gamma_j^{(0)} \in V_{(0)}$ se tiene que $F_i(e_1,\ldots,e_i,\gamma_j^{(0)}) = 0$ y $\det(D_X F_i(e_1,\ldots,e_i,\gamma_j^{(0)})) \neq 0$.

Se define recursivamente

$$\begin{aligned} \gamma_j^{(i,0)} &= \gamma_j^{(0)} \\ \gamma_j^{(i,k+1)} &= N_{F_i}(\gamma_j^{(i,k)}) \qquad k \geq 0 \end{aligned}$$

para obtener una sucesión de vectores de funciones racionales

$$\gamma_j^{(i,k)} = (\gamma_{j1}^{(i,k)},\ldots,\gamma_{jn}^{(i,k)}) \in \overline{k}(U_0,\ldots,U_{i-1})^n.$$

Como los denominadores de estas funciones racionales no se anulan en $(e_1, \ldots, e_i)$, pueden invertirse como series de potencias en $\overline{k}[[U_0 - e_1, \ldots, U_{i-1} - e_i]]$.
Ahora, para cada $1 \leq l \leq n$, la sucesión de series de potencias $\left(\gamma_{jl}^{(i,k)}\right)_{k\geq 0}$ converge a la serie de potencias $\gamma_{jl}^{(i)} \in \overline{k}[[U_0 - e_1, \ldots, U_{i-1} - e_i]]$. Más aún, para cada $k \in \mathbb{N}$, la serie de potencias $\gamma_{jl}^{(i,k)}$ aproxima a $\gamma_{jl}^{(i)}$ con precisión 2^k (es decir, los coeficientes de los desarrollos alrededor de $(e_1, \ldots, e_i)$ de $\gamma_{jl}^{(i,k)}$ y $\gamma_{jl}^{(i)}$ coinciden hasta grado $2^k - 1$).

Como no conocemos los puntos $\gamma_1^{(0)}, \ldots, \gamma_D^{(0)}$ de $V_{(0)}$, simularemos este proceso por medio de una aplicación simbólica del operador de Newton tomando como "punto inicial" la resolución geométrica de $V_{(0)}$, que contiene la información de todos los puntos de esta variedad.

Sean $p, v_1, \ldots, v_n \in k[T]$ y $\ell = \lambda_1 X_1 + \cdots + \lambda_n X_n$ los elementos de la resolución geométrica dada de $V_{(0)}$.
Sea M la matriz compañera del polinomio p, que es la matriz de la multiplicación por ℓ en la base $\{1, \ell, \ell^2, \ldots, \ell^{D-1}\}$ del espacio vectorial D-dimensional $k[V_{(0)}]$. Entonces, para cada $1 \leq k \leq n$, $M_{X_k} := v_k(M)$ es la matriz de la multiplicación por X_k con respecto a la misma base.
Observamos que la matriz M es semejante a la matriz diagonal $D(\ell(\gamma_1^{(0)}), \ldots, \ell(\gamma_D^{(0)}))$ y, por lo tanto, para todo $1 \leq k \leq n$, la matriz M_{X_k} es también semejante a una matriz diagonal $D_{X_k} := D(\gamma_{1k}^{(0)}, \ldots, \gamma_{Dk}^{(0)})$.

Sea $\kappa := \lceil \log((2r+1)\,D + 1) \rceil$.

Aplicando el Lema 1.4.7 obtenemos, a partir de un straight-line program que calcula F_i, un straight-line program que evalúa polinomios

$$g_{i1}^{(\kappa)}, \ldots, g_{in}^{(\kappa)} \quad \text{y} \quad h_i^{(\kappa)} \in k[U_0, \ldots, U_{i-1}][X]$$

que representan los numeradores y un denominador de la κ-ésima iteración del operador de Newton N_{F_i}, es decir, tales que

$$N_{F_i}^{(\kappa)}(X) = \left(\frac{g_{i1}^{(\kappa)}}{h_i^{(\kappa)}}(X), \ldots, \frac{g_{in}^{(\kappa)}}{h_i^{(\kappa)}}(X) \right).$$

Consideremos las matrices

$$H_i := h_i^{(\kappa)}(M_{X_1}, \ldots, M_{X_n}) \tag{4.12}$$

$$G_{ik} := g_{ik}^{(\kappa)}(M_{X_1}, \ldots, M_{X_n}) \qquad (1 \leq k \leq n) \tag{4.13}$$

$$N_{ik} := H_i^{-1} G_{ik} \qquad (1 \leq k \leq n). \tag{4.14}$$

Como el polinomio $\det(H_i) \in k[U']$ no se anula en e', $\det(H_i)^{-1}$ es una serie de potencias en $k[[U'-e']]$. Más aún, del hecho que M_{X_k} es semejante a D_{X_k}, deducimos que $\det(N_{ii}) = (\det(H_i))^{-1}\det(G_{ii}) \in k[[U'-e']]$ aproxima (4.11) con precisión $2^\kappa \geq (2r+1)D+1$.

Análogamente

$$\det(U_{i0}I_D + U_{i1}N_{i1} + \cdots + U_{in}N_{in}) = (\det(H_i))^{-1}\det(U_{i0}H_i + U_{i1}G_{i1} + \cdots + U_{in}G_{in})$$

aproxima (4.10) en $k[[U-e]]$ con precisión del mismo orden.

Ahora, la siguiente igualdad vale en $k[[U'-e']]$

$$\det(H_i)^{-1} = \frac{-1}{\det(H_i)(e')}\sum_{j=0}^{\infty}\left(\frac{\det(H_i)(U') - \det(H_i)(e')}{\det(H_i)(e')}\right)^j,$$

y por lo tanto el desarrollo de $\det(H_i)^{-1}$ alrededor de e' puede ser aproximado con precisión $(2r+1)D+1$ mediante el polinomio

$$\widehat{H}_i(U') := \frac{-1}{\det(H_i)(e')}\sum_{j=0}^{(2r+1)D}\left(\frac{\det(H_i)(U') - \det(H_i)(e')}{\det(H_i)(e')}\right)^j \tag{4.15}$$

Concluimos que basta calcular los polinomios

$$\widehat{H}_i\,\det(G_{ii}) \quad \text{y} \quad \widehat{H}_i\,\det(U_{i0}H_i + U_{i1}G_{i1} + \cdots + U_{in}G_{in}),$$

que aproximan (4.11) y (4.10) respectivamente con precisión $(2r+1)D+1$.

La forma de Chow $Ch_{V_{(0)}}(U_0)$ de $V_{(0)}$, que es uno de los factores de $\Phi(U)$, se calcula (exactamente) a partir de la fórmula

$$Ch_{V_{(0)}}(U_0) = \prod_{1\leq j\leq D} L_0(U_0, \gamma_j^{(0)}) = \det(U_{00}\mathrm{Id}_D + U_{01}M_{X_1} + \cdots + U_{0n}M_{X_n}).$$

Finalmente, las componentes homogéneas de los desarrollos de Φ y Γ alrededor de e hasta grado $(2r+1)D$, se calculan considerando los productos

$$\Phi^0(U) := Ch_{V_{(0)}}(U_0)\prod_{1\leq i\leq r}\widehat{H}_i\,\det(U_{i0}H_i + U_{i1}G_{i1} + \cdots + U_{in}G_{in}) \tag{4.16}$$

$$\Gamma^0(U') := \prod_{1\leq i\leq r}\widehat{H}_i\,\det(G_{ii+1}),, \tag{4.17}$$

que aproximan con precisión $(2r+1)D+1$ a Φ y Ψ respectivamente, y extrayendo, por medio del Lema 1.3.4, todas las componentes homogéneas de grado menor o igual que $(2r+1)\,D$ (de los desarrollos alrededor de e) de estos polinomios.

De esta manera obtenemos la aproximación requerida de Φ y Γ y las componentes homogéneas que sirven como input para el algoritmo de la Proposición 4.2.12 (1).

Como dijimos al comienzo de la demostración, el algoritmo de la Proposición 4.2.12 (1) produce entonces un polinomio $F \in k[U]$ tal que $F/G = Ch_V$, donde G es el polinomio definido en (4.9).

Para terminar, teniendo en cuenta que $G(e_0,\ldots,e_0) \neq 0$, la parte (2) de la Proposición 4.2.12, da como output el cociente $\Phi/\Gamma = Ch_V$.

Resumimos el algoritmo y calculamos la longitud del straight-line program obtenido:

Algoritmo

Paso 1. Sea $\kappa := \lceil 1 + \log((2r+1)\,D)\rceil$.

Para cada $1 \leq i \leq r$:

(a) Aplicar el Lema 1.4.7 a F_i para calcular los polinomios $g_{ik}^{(\kappa)}$ $(1 \leq k \leq n)$ y $h_i^{(\kappa)}$ que representan los numeradores y el denominador de $N_{F_i}^{(\kappa)}(X)$. El algoritmo produce un straight-line program cuya longitud es de orden $(n\,d)^{O(1)}\log(D)\,L$.

(b) Dada la resolución geométrica de $V_{(0)}$, calcular un straight-line program para las matrices H_i y G_{ik}, $1 \leq k \leq n$, definidas por (4.12) y (4.13). La longitud de este straight-line program es de orden $(n\,d\,D)^{O(1)}\,L$.

(c) Calcular $\det(H_i)$, $\det(G_{ii})$ y $\det(U_{i0}H_i + U_{i1}G_{i1} + \cdots + U_{in}G_{in})$ por medio del algoritmo descripto en [1]. Esto no modifica el orden de la longitud del straight-line program.

(d) A partir de $\det(H_i)$ calcular $\widehat{H}_i$ según la fórmula (4.15).

Paso 2. Efectuar los productos definidos por Φ^0 y Γ^0 en (4.16) y (4.17). La longitud del straight-line program para Φ^0 y Γ^0 es de orden $(n\,d\,D)^{O(1)}\,L$.

Paso 3. Aplicar el Lema 1.3.4 para calcular todas las componentes homogéneas de grado menor o igual que $(2r+1)\,D$ de los desarrollos de Φ^0 y Γ^0 alrededor de e.

Paso 4. Mediante el algoritmo dado en la Proposición 4.2.12 (1), calcular el polinomio F tal que $F/G = Ch_V$.

Paso 5. Teniendo en cuenta que $G(e_0, \ldots, e_0) \neq 0$, obtener un straight-line program para el cociente Ch_V por medio del Lema 1.3.5. La longitud total del straight-line program es $(n\,d\,D)^{O(1)}\,L$.

Observamos que la complejidad del algoritmo es del mismo orden que la longitud del straight-line program que produce.

4.3 Forma de Chow de cada componente equidimensional de una variedad afín

En esta sección se construye un algoritmo probabilístico para el cálculo de la forma de Chow de cada una de las componentes equidimensionales de una variedad algebraica afín arbitraria $V \subset \mathbb{A}^n$.

El algoritmo toma como entrada un conjunto finito de polinomios dados por medio de un straight-line program cuyo conjunto de ceros es la variedad algebraica V y produce un straight-line program que evalúa las formas de Chow de cada una de las componentes equidimensionales de V. Si la variedad está definida por s polinomios en n variables de grados acotados por d codificados por un straight-line program de longitud L, la complejidad del algoritmo y la longitud del straight-line program que produce son de orden $s\,n^{O(1)}d^{O(n)}L$.

Veremos también que, bajo ciertas condiciones, la complejidad del algoritmo es polinomial en la longitud del straight-line program input y en el denominado *grado geométrico* del sistema de polinomios dado que define la variedad, pudiendo resultar entonces de orden considerablemente menor.

Cabe destacar que este algoritmo provee una forma alternativa de calcular la descomposición equidimensional de una variedad algebraica afín.

4.3.1 Formas de Chow generalizadas y polinomios característicos

Un paso fundamental dentro del algoritmo principal que presentaremos en esta sección es el cálculo de la forma de Chow de la intersección de una variedad equidi-

mensional V con una hipersuperficie que no contiene ninguna componente irreducible de V, a partir de cierta información sobre V y un polinomio f que define la hipersuperficie. La subrutina que realiza esta tarea se basa en una noción teórica que permite estudiar la intersección de la variedad V con una hipersuperficie en la situación mencionada: la *forma de Chow generalizada* de la variedad V.

Otra herramienta teórica en que se sustenta el algoritmo que presentaremos es la noción de *polinomio característico* de una variedad equidimensional.

A continuación se introducen estas nociones y se prueban ciertos resultados auxiliares que se utilizarán para la demostración del resultado principal.

Para un tratamiento más completo de estos temas ver [25, Sections 2.1.1, 2.3.1].

Forma de Chow generalizada

Presentamos a continuación el concepto de forma de Chow generalizada de una variedad equidimensional.

Sea $V \subset \mathbb{A}^n$ una variedad afín equidimensional de dimensión r y grado D definida sobre un cuerpo k.

Como en las secciones anteriores, para cada $0 \leq i \leq r-1$, $U_i = (U_{i0}, \ldots, U_{in})$ denota un grupo de $n+1$ variables asociadas a una forma lineal genérica

$$L_i(U_i, X) := U_{i0} + U_{i1}X_1 + \cdots + U_{in}X_n \qquad (0 \leq i \leq r-1).$$

Para $d \in \mathbb{N}$, denotamos por $U(d)_r$ a un nuevo grupo de $\binom{d+n}{n}$ nuevas variables y por

$$F(U(d)_r, X) := \sum_{|\alpha| \leq d} U(d)_{r\alpha} X^\alpha$$

al polinomio genérico de grado d en n variables asociado a $U(d)_r$.

Sea $N := r(n+1) + \binom{d+n}{n}$ y sea $W \subset \mathbb{A}^N \times V$ la variedad de incidencia de $L_0, \ldots, L_{r-1}, F$ con respecto a V, es decir

$$W := \{(u_0, \ldots, u_{r-1}, u(d)_r; x) \in \mathbb{A}^N \times \mathbb{A}^n;\ x \in V,$$
$$L_0(u_0, x) = 0, \ldots, L_{r-1}(u_{r-1}, x) = 0,\ F(u(d)_r, x) = 0\}.$$

Si $\pi : \mathbb{A}^N \times \mathbb{A}^n \to \mathbb{A}^N$ denota la proyección canónica sobre las primeras coordenadas, se tiene que $\overline{\pi(W)}$ es una hipersuperficie en $\mathbb{A}^N$ (ver [28, Prop. 1.5]).

Una *d-forma de Chow* de V es cualquier polinomio $\mathcal{F}_{d,V} \in k[U_0, \ldots, U_{r-1}, U(d)_r]$ libre de cuadrados que define la hipersuperficie $\overline{\pi(W)} \subseteq \mathbb{A}^N$.

Como en el caso de la forma de Chow usual, una d-forma de Chow está unívocamente determinada salvo por un factor escalar.

Además, si V es una variedad irreducible, $\mathcal{F}_{d,V}$ es un polinomio irreducible y, si la variedad V es equidimensional, su d-forma de Chow coincide con el producto de d-formas de Chow de sus componentes irreducibles.

Sea $I(V)$ el ideal de $k[X_1, \ldots, X_n]$ formado por los polinomios que se anulan sobre V. Se tiene la siguiente igualdad en $k[U_0, \ldots, U_{r-1}, U(d)_r]$

$$(\mathcal{F}_{d,V}) = (I(V) + (L_0, \ldots, L_{r-1}, F)) \cap k[U_0, \ldots, U_{r-1}, U(d)_r]. \tag{4.18}$$

El siguiente resultado, que es una generalización del Lema 4.2.4, relaciona una d-forma de Chow de una variedad V con una d-forma de Chow de una variedad cero-dimensional asociada a V.

Lema 4.3.1 *Sea $V \subseteq \mathbb{A}^n(\overline{k})$ una variedad equidimensional de dimensión r definible sobre k y sea $\mathcal{F}_{d,V} \in k[U_0, \ldots, U_{r-1}, U(d)_r]$ una d-forma de Chow de V.*
Consideremos el ideal I^0 definido por

$$I^0 := (I(V), L_0(U_0, X), \ldots, L_{r-1}(U_{r-1}, X)) \subseteq k(U_0, \ldots, U_{r-1})[X]$$

y la variedad cero-dimensional

$$V^0 = V(I^0) \subseteq \mathbb{A}^n(\overline{k(U_0, \ldots, U_{r-1})}).$$

Finalmente, sea $\mathcal{F}_{d,V^0} \in k(U_0, \ldots, U_{r-1})[U(d)_r]$ una d-forma de Chow de V^0.
Entonces existe un polinomio $Q \in k[U_0, \ldots, U_{r-1}] - \{0\}$ que satisface

$$\mathcal{F}_{d,V}(U_0, \ldots, U_{r-1}, U(d)_r) = Q(U_0, \ldots, U_{r-1})\, \mathcal{F}_{d,V^0}(U(d)_r).$$

Demostración. Se prueba a partir de la igualdad (4.18), localizando en el conjunto multiplicativamente cerrado $S = k[U_0, \ldots, U_{r-1}] - \{0\}$, en forma análoga al Lema 4.2.4.

Una d-forma de Chow $\mathcal{F}_{d,V} \in k[U_0, \ldots, U_{r-1}, U(d)_r]$ de V es un polinomio multihomogéneo de grado D en el grupo de variables $U(d)_r$ y de grado $d\,D$ en cada uno de los grupos de variables U_i $(0 \leq i \leq r-1)$ (ver [28, Lemme 1.8]).

Si $\overline{V} \subset \mathbb{P}^n$ denota la clausura proyectiva de V y, $\overline{L}_i$ $(0 \leq i \leq r-1)$ y $\overline{F}$ son los homogeneizados de los polinomios L_i $(0 \leq i \leq r-1)$ y F con respecto a la variable X_0 respectivamente, el polinomio $\mathcal{F}_{d,V}$ verifica

$$\mathcal{F}_{d,V}(u_0, \ldots, u_{r-1}, u(d)_r) = 0 \iff$$
$$\overline{V} \cap \{\overline{L}_0(u_0, X) = 0\} \cap \cdots \cap \{\overline{L}_{r-1}(u_r, X) = 0\} \cap \{\overline{F}(u(d)_0, X) = 0\} \neq \emptyset$$

para $u_i \in \overline{k}^{n+1}$ $(0 \leq i \leq r-1)$ y $u(d)_r \in \overline{k}^{\binom{d+n}{n}}$.

La d-forma de Chow de una variedad V se relaciona con la forma de Chow usual de la siguiente manera:

Supongamos en primer lugar que V es una variedad irreducible.

Sea U_r un nuevo grupo de $n+1$ variables, y sea $L_r(U_r, X)$ la forma lineal genérica asociada a U_r.

Consideremos el polinomio $\tilde{\mathcal{F}}_{d,V}(U_0, \ldots, U_r) := \mathcal{F}_{d,V}(U_0, \ldots, U_{r-1}, (L_r)^d)$, que resulta de especializar las variables $U(d)_r$ en los coeficientes del polinomio $(L_r)^d$, y sea $\mathcal{F}_V \in k[U_0, \ldots, U_r]$ una forma de Chow de V. Se tiene que

$$\tilde{\mathcal{F}}_{d,V}(u_0, \ldots, u_r) = 0 \iff$$
$$\overline{V} \cap \{\overline{L}_0(u_0, x) = 0, \ldots, \overline{L}_{r-1}(u_{r-1}, x) = 0\} \cap \{\overline{L}_r(u_r, x)^d = 0\} \neq \emptyset$$
$$\iff \mathcal{F}_V(u_0, \ldots, u_r) = 0.$$

Esto dice que los conjuntos de ceros de $\tilde{\mathcal{F}}_{d,V}$ y $\mathcal{F}_V$ coinciden. Entonces, como $\mathcal{F}_V$ es irreducible, existen $c \in k - \{0\}$ y $\alpha \in \mathbb{N}$ tales que

$$\tilde{\mathcal{F}}_{d,V}(U_0, \ldots, U_r) = c \cdot \mathcal{F}_V(U_0, \ldots, U_r)^\alpha.$$

Teniendo en cuenta que $\deg_{U_0} \tilde{\mathcal{F}}_V = dD$ y $\deg_{U_0} \mathcal{F}_V^\alpha = \alpha D$, resulta que $\alpha = d$. Luego

$$\tilde{\mathcal{F}}_{d,V}(U_0, \ldots, U_r) = c \cdot \mathcal{F}_V(U_0, \ldots, U_r)^d. \tag{4.19}$$

Finalmente, del hecho que una forma de Chow de una variedad equidimensional es el producto de formas de Chow de sus componentes irreducibles y que lo mismo vale

para d-formas de Chow, se deduce que la igualdad (4.19) es también válida en el caso de una variedad equidimensional.

Supongamos ahora que la variedad V satisface la hipótesis 4.2.1. Entonces

$$\overline{V} \cap \{x_0 = 0\} \cap \ldots \cap \{x_{r-1} = 0\} \cap \{x_r = 0\} = \emptyset.$$

Esto implica que, si $e(d)_r$ es el vector de $k^{\binom{d+n}{n}}$ con un 1 en el lugar correspondiente al monomio X_r^d y las demás coordenadas 0 y, para cada $0 \leq i \leq r-1$, e_i es el $(i+1)$-ésimo vector de la base canónica de k^{n+1},

$$\mathcal{F}_{d,V}(e_0, \ldots, e_{r-1}, e(d)_r) \neq 0.$$

Definimos entonces la *d-forma de Chow normalizada* $Ch_{d,V}$ de V como la d-forma de Chow de V que satisface $Ch_{d,V}(e_0, \ldots, e_{r-1}, e(d)_r) = 1$.

Bajo estas hipótesis, la forma de Chow normalizada Ch_V y la d-forma de Chow normalizada $Ch_{d,V}$ están relacionadas por la igualdad (4.19) como

$$Ch_{d,V}(U_0, \ldots, U_{r-1}, (L_r)^d) = Ch_V(U_0, \ldots, U_r)^d.$$

De esta igualdad deducimos, como consecuencia del Lema 4.3.1, el siguiente resultado:

Lema 4.3.2 *Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r definible sobre k que satisface la hipótesis 4.2.1 y sea $V^0 \subset \mathbb{A}^n(\overline{k(U_0, \ldots, U_{r-1})})$ la variedad cero-dimensional asociada a V como en el Lema 4.3.1.*

Sean $Ch_V \in k[U_0, \ldots, U_r]$ y $Ch_{d,V} \in k[U_0, \ldots, U_{r-1}, U(d)_r]$ la forma de Chow normalizada y la d-forma de Chow normalizada de V respectivamente, y sean $Ch_{V^0} \in k(U_0, \ldots, U_{r-1})[U_r]$ y $Ch_{d,V^0} \in k(U_0, \ldots, U_{r-1})[U(d)_r]$ la forma de Chow normalizada y la d-forma de Chow normalizada de V^0, respectivamente.

Entonces

$$Ch_{d,V}(U_0, \ldots, U_{r-1}, U(d)_r) = \left(Ch_{V \cap V(X_r)}(U_0, \ldots, U_{r-1})\right)^d \frac{Ch_{d,V^0}(U(d)_r)}{\prod\limits_{\gamma \in V^0} \gamma_r^d}.$$

Demostración. En primer lugar observamos que el Lema 4.3.1 garantiza la existencia de un polinomio $Q \in k[U_0, \ldots, U_{r-1}] - \{0\}$ tal que $Ch_{d,V} = Q\, Ch_{d,V^0}$.

Por otro lado, si $P \in k[U_0, \ldots, U_{r-1}]$ satisface

$$Ch_V(U_0, \ldots, U_r) = P(U_0, \ldots, U_{r-1})\, Ch_{V^0}(U_r),$$

se tiene que

$$P(U_0, \ldots, U_{r-1})^d\, Ch_{V^0}(U_r)^d = Ch_V(U_0, \ldots, U_r)^d = Ch_{d,V}(U_0, \ldots, U_{r-1}, (L_r)^d) =$$
$$= Q(U_0, \ldots, U_{r-1})\, Ch_{d,V^0}((L_r)^d) = Q(U_0, \ldots, U_{r-1})\, Ch_{V^0}(U_r)^d,$$

de donde $Q = P^d$.

Finalmente observamos que de la demostración de la Proposición 4.2.8 se desprende que

$$P(U_0, \ldots, U_{r-1}) = \frac{Ch_{V \cap V(X_r)}(U_0, \ldots, U_{r-1})}{\prod_{\gamma \in V^0} \gamma_r}$$

lo que termina la demostración.

Polinomio característico de una variedad

Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado D definible sobre k. Sean $U_0, \ldots, U_r$ grupos de $n+1$ indeterminadas sobre k, y sean

$$L_i(U_i, X) = U_{i0} + U_{i1}X_1 + \cdots + U_{in}X_n \qquad (0 \leq i \leq r)$$

las formas lineales genéricas asociadas.

Introducimos un nuevo grupo de $r+1$ variables $(T_0, \ldots, T_r)$ que corresponden a las funciones coordenadas de $\mathbb{A}^{r+1}$.

Sea $M := (r+1)(n+1)$. Consideremos la aplicación $\psi : \mathbb{A}^M \times \mathbb{A}^n \to \mathbb{A}^M \times \mathbb{A}^{r+1}$ definida por

$$\psi(u_0, \ldots, u_r, x) = (u_0, \ldots, u_r, L_0(u_0, x), L_1(u_1, x), \ldots, L_r(u_r, x)).$$

La clausura de Zariski $\overline{\psi(\mathbb{A}^M \times V)} \subseteq \mathbb{A}^M \times \mathbb{A}^{r+1}$ es una hipersuperficie. Se llama *polinomio característico* de V a cualquier polinomio $\mathcal{P}_V \in k[U, T_0, \ldots, T_r]$ libre de cuadrados que define $\overline{\psi(\mathbb{A}^M \times V)}$.

Cuando V es irreducible, un polinomio característico de V es irreducible, y si V es equidimensional, un polinomio característico de V coincide con el producto de polinomios característicos de sus componentes irreducibles.

El siguiente lema, extraído de [25, Lemma 2.12], relaciona el polinomio característico de una variedad equidimensional con su forma de Chow.

Lema 4.3.3 *Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado D definible sobre k y sea $\mathcal{F}_V$ una forma de Chow de V. Para $0 \leq i \leq r$, consideremos el cambio de variables $\zeta_i := (U_{i0} - T_i, U_{i1}, \ldots, U_{ir})$. Finalmente, consideremos el polinomio*

$$\mathcal{P} := \mathcal{F}_V(\zeta_0, \ldots, \zeta_r) \in k[U, T_0, \ldots, T_r].$$

Entonces $\mathcal{P}$ es un polinomio característico de V.

Demostración. Basta considerar el caso en que V es una variedad irreducible.

Sea $\mathcal{P}_V \in k[U_0, \ldots, U_r, T_0, \ldots, T_r]$ un polinomio característico de V.

Sea $(u, \xi) := (u_0, \ldots, u_r, \xi) \in \mathbb{A}^M \times V$, y para cada $0 \leq i \leq r$, definamos $t_i := L_i(u_i, \xi)$. Sea $t := (t_0, \ldots, t_r) \in \mathbb{A}^{r+1}$. Entonces $\psi(u, \xi) = (u, t)$, de donde $\mathcal{P}_V(u, t) = 0$.

Ahora, se tiene que

$$\xi \in V \cap \{L_0(u_0, x) = t_0, \ldots, L_r(u_r, x) = t_r\}$$

de donde se deduce inmediatamente que la forma de Chow $\mathcal{F}_V$ de V se anula al especializar, para cada $0 \leq i \leq r$, el grupo de variables U_i en $(u_{i0} - t_0, u_{i1}, \ldots, u_{in})$.

Equivalentemente, el polinomio $\mathcal{P}(U_0, \ldots, U_r, T_0, \ldots, T_r) = \mathcal{F}_V(\zeta_0, \ldots, \zeta_r)$ se anula en el punto (u, t).

Luego, el polinomio $\mathcal{P}$ se anula sobre $\psi(\mathbb{A}^M \times V)$.

Teniendo en cuenta que $\mathcal{P}_V$ es un polinomio libre de cuadrados que define la hipersuperficie $\overline{\psi(\mathbb{A}^M \times V)}$, deducimos que $\mathcal{P}_V \mid \mathcal{P}$.

Por otro lado, como $\mathcal{F}_V$ es irreducible, resulta que $\mathcal{P}$ es también irreducible.

En consecuencia, $\mathcal{P}$ y $\mathcal{P}_V$ coinciden salvo por un factor escalar, de donde $\mathcal{P}$ es un polinomio característico de V.

Observamos que el polinomio característico $\mathcal{P}_V$ de V es multihomogéneo de grado D en cada grupo de variables $U_i \cup \{T_i\}$ $(0 \leq i \leq r)$.

Si la variedad V satisface la hipótesis 4.2.1, se define *el polinomio característico normalizado de V* como

$$\mathcal{P}_V := (-1)^D Ch_V(\zeta_0, \ldots, \zeta_r),$$

donde Ch_V es la forma de Chow normalizada de V.

En este caso, el grado con respecto a T_0 del polinomio característico (normalizado) es $D = \deg V$ y su coeficiente principal a_D con respecto a T_0 coincide con el coeficiente de U_{00}^D en la forma de Chow normalizada Ch_V de V. Luego, $a_D \in k[U_1, \ldots, U_r]$ y verifica $a_D(e_1, \ldots, e_r) = 1$ (ver [25, Section 2.3.1] para más detalles).

Cálculo de resoluciones geométricas a partir de polinomios característicos

En el próximo lema mostramos cómo recuperar, a partir del polinomio característico de una variedad equidimensional V de dimensión r, una resolución geométrica de una fibra genérica de V con respecto a una proyección lineal genérica de V en $\mathbb{A}^r$.

Para esto, observamos en primer término que una resolución geométrica de una variedad cero-dimensional $Z \subset \mathbb{A}^n$ puede darse de la siguiente manera (equivalente a la presentada en la Sección 1.1.2): Además de una forma lineal ℓ que separa los puntos de Z y su polinomio minimal $p \in k[T]$, en lugar de dar polinomios $v_i \in k[T]$, $1 \leq i \leq n$, tales que Z esté descripta por

$$Z = \left\{(v_1(\eta), \ldots, v_n(\eta)) : \eta \in \overline{k},\ p(\eta) = 0\right\},$$

se pueden exhibir polinomios $w_i \in k[T]$, $1 \leq i \leq n$, que verifican

$$Z = \left\{\left(\frac{w_1(\eta)}{p'(\eta)}, \ldots, \frac{w_n(\eta)}{p'(\eta)}\right) : \eta \in \overline{k},\ p(\eta) = 0\right\}.$$

Del hecho que $\gcd(p, p') = 1$, deducimos que a partir de esta última descripción puede recuperarse la primera (es decir, se pueden calcular los polinomios $v_i \in k[T]$, $1 \leq i \leq n$):

Observamos que la condición $\gcd(p, p') = 1$ equivale a que la resultante $\mathrm{Res}(p, p')$ entre p y p' sea no nula.

Sea $D := \deg p$ y sea $S \in k^{(2D-1)\times(2D-1)}$ la matriz de Sylvester de p y p'.

Consideremos el vector $(a_{D-2}, \ldots, a_1, a_0, b_{D-1}, \ldots, b_1, b_0)$ correspondiente a la última columna de la matriz adjunta de S y los polinomios asociados

$$\begin{aligned} q_1 &:= a_{D-2}T^{D-2} + \cdots + a_0 \\ q_2 &:= b_{D-1}T^{D-1} + \cdots + b_1 T + b_0 \end{aligned}$$

Se tiene que

$$\mathrm{Res}(p, p') = q_1 \cdot p + q_2 \cdot p'.$$

Observamos que de esta igualdad se deduce que, para cada $\eta \in \overline{k}$ tal que $p(\eta) = 0$, vale

$$\frac{w_i(\eta)}{p'(\eta)} = \frac{q_2(\eta)w_i(\eta)}{\mathrm{Res}(p,p')} \qquad i = 1,\ldots,n.$$

Para cada $1 \leq i \leq n$ sea $v_i \in k[T]$ el resto de la división de $\frac{1}{\mathrm{Res}(p,p')}q_2 w_i$ por p. Entonces $v_i \in k[T]$ tiene grado acotado por $D-1$ y se verifica

$$v_i(\eta) = \frac{w_i(\eta)}{p'(\eta)} \qquad i = 1,\ldots,n.$$

En consecuencia

$$\left\{\left(\frac{w_1(\eta)}{p'(\eta)},\ldots,\frac{w_n(\eta)}{p'(\eta)}\right) : \eta \in \overline{k},\ p(\eta) = 0\right\} = \left\{(v_1(\eta),\ldots,v_n(\eta)) : \eta \in \overline{k},\ p(\eta) = 0\right\},$$

es decir, $v_1,\ldots,v_n$ completan una resolución geométrica de Z.

Desde el punto de vista algorítmico, se calculan la resultante $\mathrm{Res}(p,p')$ y los coeficientes del polinomio q_2 en tiempo secuencial de orden $O(D^4)$ por medio del algoritmo de Berkowitz para el cálculo de determinantes. A continuación se obtienen los polinomios $\frac{1}{\mathrm{Res}(p,p')}q_2 w_i$ $(1 \leq i \leq n)$ en tiempo $O(n\,D^2)$ y finalmente los restos v_i $(1 \leq i \leq n)$ de las divisiones de estos polinomios por p con $O(n\,D^4)$ pasos adicionales. La complejidad secuencial de todo el proceso es de orden $O(n\,D^4)$.

Lema 4.3.4 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado D definible sobre k que satisface la hipótesis 4.2.1. Sea $\mathcal{P}_V \in k[U,T_0,\ldots,T_r]$ el polinomio característico normalizado de V y denotemos por $\rho \in k[U,T_1,\ldots,T_r]$ su discriminante con respecto a T_0.*

Entonces, para cada $(u,t_1,\ldots,t_r) \in \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^r$ tal que $\rho(u,t_1,\ldots,t_r) \neq 0$, la variedad

$$V \cap V(L_1(u_1,X) - t_1,\ldots,L_r(u_r,X) - t_r)$$

es cero-dimensional de grado D y admite la siguiente resolución geométrica:

- *la forma lineal $\ell(X) := L_0(u_0,X)$,*
- *el polinomio minimal $p(T_0) := \mathcal{P}_V(u,T_0,t_1,\ldots,t_r) \in k[T_0]$ y*
- *para cada $1 \leq i \leq n$, $w_i(T_0) := -\dfrac{\partial \mathcal{P}_V}{\partial U_{0i}}(u,T_0,t_1,\ldots,t_r)$.*

En otras palabras

$$V \cap V(L_1(u_1, X) - t_1, \ldots, L_r(u_r, X) - t_r) = \left\{ \left(\frac{w_1(\eta)}{p'(t_0)}, \ldots, \frac{w_n(t_0)}{p'(t_0)} \right) : t_0 \in \overline{k},\ p(t_0) = 0 \right\}.$$

Demostración. Sea $\overline{V} \subset \mathbb{A}^n$ la clausura proyectiva de V y sea $t' := (t_1, \ldots, t_r) \in \mathbb{A}^r$. De la igualdad $\mathcal{P}_V = (-1)^D Ch_V(\zeta_0, \ldots, \zeta_r)$ deducimos que

$$\mathcal{P}_V(u, t_0, t') = 0 \iff \overline{V} \cap \{\overline{\ell}_0(x) = 0, \ldots, \overline{\ell}_r(x) = 0\} \neq \emptyset$$

donde $\overline{\ell}_i(x) = (u_{i0} - t_i)\, x_0 + u_{i1} x_1 + \cdots + u_{in} x_n$ para cada $0 \leq i \leq n$.

Consideremos ahora un elemento $(u, t') \in \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^r$ tal que $\rho(u, t') \neq 0$, y sea $p(T_0) := \mathcal{P}_V(u, T_0, t')$.

La no anulación del discriminante ρ de $\mathcal{P}_V$ en (u, t') implica que si $a_D \in k[U_1, \ldots, U_r]$ denota el coeficiente principal de $\mathcal{P}_V$ con respecto a la variable T_0, $a_D(u_1, \ldots, u_r) \neq 0$. Entonces, como a_D es el coeficiente de U_{00}^D en Ch_V, deducimos que

$$Ch_V(e_0, (u_{10} - t_1, u_{11}, \ldots, u_{1n}), \ldots, (u_{r0} - t_r, u_{r1}, \ldots, u_{rn})) \neq 0$$

o, equivalentemente,

$$\overline{V} \cap \{x_0 = 0, \overline{\ell}_1(x) = 0, \ldots, \overline{\ell}_r(x) = 0\} = \emptyset.$$

En particular, esto significa que $\overline{V} \cap \{\overline{\ell}_1(x) = 0, \ldots, \overline{\ell}_r(x) = 0\}$ consta de un número finito de puntos incluídos en el abierto afín $\{x_0 \neq 0\}$. Luego

$$V \cap \{L_1(u_1, x) = t_1, \ldots, L_r(u_r, x) = t_r\}$$

es una variedad cero-dimensional, de grado acotado por D, puesto que $\deg V = D$. Por otro lado,

$$p(t_0) = 0 \iff V \cap \{L_0(u_0, x) = t_0, L_1(u_1, x) = t_1, \ldots, L_r(u_r, x) = t_r\} \neq \emptyset, \quad (4.20)$$

lo que implica que para cada $\xi \in V \cap V(L_1(u_1, X) - t_1, \ldots, L_r(u_r, X) - t_r)$, $t_0 := L_0(u_0, \xi)$ es una raíz de $p(T_0)$, y recíprocamente, para cada t_0 raíz de $p(T_0)$, existe al menos un punto $\xi \in V \cap V(L_1(u_1, X) - t_1, \ldots, L_r(u_r, X) - t_r)$ que verifica $L_0(u_0, \xi) = t_0$.

Ahora, la condición sobre el discriminante asegura que $p(T_0)$ es un polinomio libre de cuadrados, es decir, $p(T_0)$ tiene exactamente D raíces distintas. Entonces $V \cap V(L_1(u_1, X) - t_1, \ldots, L_r(u_r, X) - t_r)$ es una variedad cero-dimensional de grado

exactamente D, y para cada t_0 raíz de $p(T_0)$, existe exactamente un punto $\xi \in V \cap V(L_1(u_1, X) - t_1, \ldots, L_r(u_r, X) - t_r)$ que verifica $L_0(u_0, \xi) = t_0$.

Concluimos entonces que la forma lineal $\ell := L_0(u_0, X)$ separa los puntos de la variedad $V \cap V(L_1(u_1, X) - t_1, \ldots, L_r(u_r, X) - t_r)$ y que $p(T_0)$ es, salvo un factor escalar, el polinomio minimal de ℓ con respecto a esta variedad cero-dimensional.

Ahora construiremos los polinomios que caracterizan las coordenadas $(\xi_1, \ldots, \xi_n)$ de cada punto $\xi \in V \cap V(L_1(u_1, X) - t_1, \ldots, L_r(u_r, X) - t_r)$.

Consideremos el polinomio

$$\mathcal{P}(U, X) := \mathcal{P}_V(U, L_0(U_0, X), \ldots, L_r(U_r, X)) \in k[U, X].$$

Observamos que si se escribe $\mathcal{P}(U, X) = \sum_{\alpha} a_\alpha(X) U^\alpha$, los coeficientes $a_\alpha(X) \in k[X_1, \ldots, X_n]$ se anulan sobre V y por lo tanto, para cada α, el polinomio $a_\alpha(X)$ pertenece al ideal $I(V)$.

De lo anterior deducimos que, si $I := k[U] \otimes_k I(V)$, se tiene que $\mathcal{P}(U, X) \in I$ y además, para cada $1 \leq i \leq n$, $\dfrac{\partial \mathcal{P}}{\partial U_{0i}}(U, X) \in I$.

Sea i con $1 \leq i \leq n$.

La derivada parcial $\dfrac{\partial \mathcal{P}}{\partial U_{0i}}(U, X)$ se expresa en términos de derivadas parciales del polinomio característico $\mathcal{P}_V$ como

$$\frac{\partial \mathcal{P}_V}{\partial U_{0i}}(U, L_0(U_0, X), \ldots, L_r(U_r, X)) + \frac{\partial \mathcal{P}_V}{\partial T_0}(U, L_0(U_0, X), \ldots, L_r(U_r, X))\, X_i.$$

Se sigue que

$$\frac{\partial \mathcal{P}_V}{\partial T_0}(U, L_0(U_0, X), \ldots, L_r(U_r, X))\, X_i \equiv -\frac{\partial \mathcal{P}_V}{\partial U_{0i}}(U, L_0(U_0, X), \ldots, L_r(U_r, X)) \pmod{I}.$$

En particular, para cada $\xi \in V \cap V(L_1(u_1, X) - t_1, \ldots, L_r(u_r, X) - t_r)$, tomando $t_0 = L_0(u_0, \xi)$, resulta que $p(t_0) = 0$, $p'(t_0) = \partial \mathcal{P}_V / \partial T_0(u, t_0, t') \neq 0$ y la coordenada ξ_i se escribe en términos de t_0 como

$$\xi_i = \frac{\frac{-\partial \mathcal{P}_V}{\partial U_{0i}}(u, t_0, t')}{p'(t_0)}.$$

Luego, para cada $1 \leq i \leq n$, consideramos

$$w_i(T_0) := -\frac{\partial \mathcal{P}_V}{\partial U_{0i}}(u, T_0, t'),$$

y los polinomios $w_1, \ldots, w_n \in k[T_0]$ completan una resolución geométrica de la variedad cero-dimensional $V \cap V(L_1(u_1, X) - t_1, \ldots, L_r(u_r, X) - t_r)$.

Observación 4.3.5 Bajo las hipótesis y notación del enunciado del Lema 4.3.4, sea $a_D \in k[U_1, \ldots, U_r]$ el coeficiente principal con respecto a la variable T_0 del polinomio característico de V. Entonces, de la primera parte de la demostración de dicho lema, se deduce que, para $u_1, \ldots, u_r \in \mathbb{A}^{n+1}$ tales que $a_D(u_1, \ldots, u_r) \neq 0$, se tiene que

$$V \cap \{L_1(u_1, x) = 0, \ldots, L_r(u_r, x) = 0\}$$

es una variedad cero-dimensional en $\mathbb{A}^n$.

4.3.2 Preparación del input

El primer paso del algoritmo que presentaremos para el cálculo de las formas de Chow de cada una de las componentes equidimensionales de una variedad algebraica V (a partir de un conjunto finito de polinomios que la define) consiste en un preprocesamiento de los datos de entrada con el objeto de obtener condiciones que permitan la aplicación del algoritmo para el cálculo de formas de Chow de variedades equidimensionales presentado en la sección anterior, a ciertas variedades auxiliares.

Modificación de los polinomios que definen la variedad

Consideraremos combinaciones lineales de los polinomios que definen la variedad V, con el objeto de obtener, con alta probabilidad, un conjunto de $n+1$ polinomios que defina la misma variedad V, pero que satisfaga también ciertas condiciones sobre la dimensión de las variedades intermedias que definen (comparar con Sección 3.3.1) y sobre la radicalidad de ciertos ideales involucrados en la construcción del algoritmo.

Sean $f_1, \ldots, f_s$ polinomios en $k[X_1, \ldots, X_n]$. Para cada i, $0 \leq i \leq n$, sea $\mathcal{T}_i := (T_{i1}, \ldots, T_{is})$ un grupo de nuevas variables y sea

$$G_i := T_{i1} f_1 + \cdots + T_{is} f_s \in k[\mathcal{T}_i][X_1, \ldots, X_n]$$

Lema 4.3.6 *Con las hipótesis y notación anteriores, para cada* $0 \leq r \leq n-1$*:*

(1) La variedad

$$\mathcal{Z}_r := \overline{V(G_1, \ldots, G_{n-r}) - V(f_1, \ldots, f_s)} \subset \mathbb{A}^{s(n-r)} \times \mathbb{A}^n$$

es irreducible de dimensión $s(n-r)+r$.

(2) El ideal $I(\mathcal{Z}_r) \subset k[\mathcal{T}_1, \ldots, \mathcal{T}_{n-r}, X_1, \ldots, X_n]$ *es una componente primaria del ideal* $(G_1, \ldots, G_{n-r})$. *Más aún, es la única componente primaria* $\mathcal{Q}$ *de este ideal que satisface* $V(\mathcal{Q}) \not\subset V(f_1, \ldots, f_s)$.

Demostración.

(1) Fijemos r, $0 \leq r \leq n-1$. Consideremos la proyección $\pi : \mathbb{A}^{s(n-r)} \times \mathbb{A}^n \to \mathbb{A}^n$ tal que $(t_1, \ldots, t_{n-r}, x) \mapsto x$.

Sean $U := \mathbb{A}^n - V(f_1, \ldots, f_s)$ y $\mathcal{U} := \mathbb{A}^{s(n-r)} \times U$.

Observamos que para cada $x \in U$ existe un índice i, $1 \leq i \leq s$, tal que $f_i(x) \neq 0$. Resulta entonces que $\pi^{-1}(x) \cap \mathcal{Z}_r \cong \mathbb{A}^{(s-1)(n-r)}$, en particular, es no vacío, de donde deducimos que $\pi : \mathcal{Z}_r \to \mathbb{A}^n$ es dominante. Por el teorema de la dimensión de las fibras,

$$\dim \mathcal{Z}_r = (s-1)(n-r) + n = s(n-r) + r.$$

Por otro lado, el hecho que $\mathcal{Z}_r \subset \mathbb{A}^{s(n-r)} \times \mathbb{A}^n$ es la unión de algunas de las componentes irreducibles de la variedad $V(G_1, \ldots, G_{n-r})$ definida por $n-r$ polinomios, implica que cada componente irreducible de $\mathcal{Z}_r$ tiene dimensión mayor o igual que $s(n-r)+r$.

En consecuencia, $\mathcal{Z}_r$ es equidimensional de dimensión $s(n-r)+r$.

Veamos que, más aún, $\mathcal{Z}_r$ es irreducible:

Supongamos que $\mathcal{Z}_r = C_1 \cup \ldots \cup C_t$ es la descomposición de $\mathcal{Z}_r$ en componentes irreducibles.

Aplicando nuevamente el teorema de la dimensión de las fibras, se obtiene que, para cada componente irreducible C_k de $\mathcal{Z}_r$ vale

$$s(n-r) + r = \dim C_k \leq (s-1)(n-r) + \dim \pi(C_k)$$

y en consecuencia, $\dim \pi(C_k) = n$ o, equivalentemente, $\overline{\pi(C_k)} = \mathbb{A}^n$.

Observamos que $\overline{\pi(C_k)} = \overline{\pi(C_k \cap U)}$, y que la condición $\overline{\pi(C_k \cap U)} = \mathbb{A}^n$ implica la existencia de un abierto U_k con $U_k \subset \pi(C_k \cap U)$ tal que para cada $x \in U_k$

$$\begin{aligned} \dim(\pi^{-1}(x) \cap C_k) &= \dim C_k - \dim \mathbb{A}^n = s(n-r) + r - n \\ &= (s-1)(n-r) = \dim(\pi^{-1}(x) \cap \mathcal{Z}_r), \end{aligned}$$

puesto que $x \in U$. Además $\pi^{-1}(x) \cap C_k \subset \pi^{-1}(x) \cap \mathcal{Z}_r$ y $\pi^{-1}(x) \cap \mathcal{Z}_r \cong \mathbb{A}^{(s-1)(n-r)}$, con lo cual es irreducible, de donde

$$\pi^{-1}(x) \cap C_k = \pi^{-1}(x) \cap \mathcal{Z}_r.$$

En consecuencia

$$\{(t,x) \in C_k : x \in U_k\} = \{(t,x) \in \mathcal{Z}_r : x \in U_k\}.$$

Considerando las clausuras de Zariski de estos conjuntos se obtiene que

$$C_k = \overline{\mathcal{Z}_r \cap (\mathbb{A}^{s(n-r)} \times U_k)}.$$

Análogamente, si C_j es otra componente irreducible de $\mathcal{Z}_r$, existe un abierto $U_j \subset \pi(C_j) \cap U$ tal que $C_j = \overline{\mathcal{Z}_r \cap (\mathbb{A}^{s(n-r)} \times U_j)}$, y entonces

$$\begin{aligned} \overline{\mathcal{Z}_r \cap (\mathbb{A}^{s(n-r)} \times (U_k \cap U_j))} &\subset \overline{\mathcal{Z}_r \cap (\mathbb{A}^{s(n-r)} \times U_k)} = C_k \\ \overline{\mathcal{Z}_r \cap (\mathbb{A}^{s(n-r)} \times (U_k \cap U_j))} &\subset \overline{\mathcal{Z}_r \cap (\mathbb{A}^{s(n-r)} \times U_j)} = C_j \end{aligned}$$

de donde concluimos que

$$\overline{\mathcal{Z}_r \cap (\mathbb{A}^{s(n-r)} \times (U_k \cap U_j))} \subset C_k \cap C_j. \tag{4.21}$$

Pero como $\mathcal{Z}_r \cap (\mathbb{A}^{s(n-r)} \times (U_k \cap U_j))$ es un abierto no vacío de $\mathcal{Z}_r$, su clausura es la unión de algunas componentes irreducibles de $\mathcal{Z}_r$, lo que contradice (4.21).

(2) De lo demostrado en (1) se sigue inducivamente, comenzando con $r = n-1$, que los polinomios $G_1, \ldots, G_{n-r}$ verifican: para toda componente primaria $\mathcal{Q}$ del ideal $(G_1, \ldots, G_{n-r})$ que verifica $V(\mathcal{Q}) \not\subset V(f_1, \ldots, f_s)$ se tiene que $\dim V(\mathcal{Q}) = s(n-r) + r$ (en otras palabras, excepto quizás por componentes primarias cuyos ceros estén incluidos en $V(f_1, \ldots, f_s)$, el ideal $(G_1, \ldots, G_{n-r})$ no tiene componentes inmersas).

El resultado enunciado se sigue entonces de la demostración de [27, Lemma 2].

Del Lema 4.3.6 se desprende la siguiente versión efectiva del Primer Teorema de Bertini, que generaliza la demostrada en [25, Proposition 4.3] y cuya prueba es análoga a la dada en [25]:

Lema 4.3.7 *Sean $f_1, \ldots, f_s$ polinomios en $k[X_1, \ldots, X_n]$ de grados acotados por d, y sea $V := V(f_1, \ldots, f_s) \subset \mathbb{A}^n$. Entonces, para cada $0 \leq r \leq n$ existe un polinomio no nulo $Q_r \in k[T_1, \ldots, T_{n-r}]$ de grado acotado por $2(d+1)^{2(n-r)}$ tal que la condición $Q_r(t_{ij}) \neq 0$ implica que si*

$$\hat{f}_i := t_{i1} f_1 + \cdots + t_{is} f_s, \quad 1 \leq i \leq n-r,$$

la variedad $Z_r := \overline{V(\hat{f}_1, \ldots, \hat{f}_{n-r})} - V \subset \mathbb{A}^n$ es o bien vacía o bien equidimensional de dimensión r y es intersección completa reducida en el abierto $\mathbb{A}^n - V$.

Más aún, si $Z_r \neq \emptyset$, los polinomios $\hat{f}_1, \ldots, \hat{f}_{n-r}$ forman una intersección completa reducida para Z_r en el abierto $\mathbb{A}^n - V$.

Como consecuencia del Lema 4.3.7 se obtiene:

Lema 4.3.8 *Sean $f_1, \ldots, f_s$ polinomios (no todos nulos) en $k[X_1, \ldots, X_n]$ que definen una variedad $V = V(f_1, \ldots, f_s) \subset \mathbb{A}^n$. Sea $V = V_0 \cup \ldots \cup V_{n-1}$ la descomposición equidimensional (minimal) de V, donde para cada $0 \leq r \leq n-1$, $V_r = \emptyset$ o V_r es una variedad equidimensional de dimensión r.*

Entonces, existen elementos $t_{ij} \in k$ $(1 \leq i \leq n+1, 1 \leq j \leq s)$ tales que los polinomios

$$\hat{f}_i := t_{i1} f_1 + \cdots + t_{is} f_s, \quad 1 \leq i \leq n+1,$$

satisfacen las condiciones

(p1) $V = V(\hat{f}_1, \ldots, \hat{f}_{n+1})$.

(p2) Para cada $0 \leq r \leq n-1$, la variedad

$$Z_r := \overline{V(\hat{f}_1, \ldots, \hat{f}_{n-r}) \cap \{\hat{f}_{n-r+1} \neq 0\}}$$

es, o bien vacía, o bien equidimensional de dimensión r y los polinomios $\hat{f}_1, \ldots, \hat{f}_{n-r}$ forman una intersección completa reducida para Z_r en el abierto $\{\hat{f}_{n-r+1} \neq 0\}$.

De la validez de las condiciones (p1) y (p2) se deduce que, para cada $0 \leq r \leq n-1$, se verifican:

(p3) $V(\hat{f}_1,\ldots,\hat{f}_{n-r}) = Z_r \cup V_r \cup \ldots \cup V_{n-1}$.

(p4) $Z_{r+1} \cap V(\hat{f}_{n-r}) = Z_r \cup V_r \cup \widehat{V}_r$, *donde* $\widehat{V}_r$ *es la unión de las componentes irreducibles de* $Z_{r+1} \cap V(\hat{f}_{n-r})$ *incluidas en* $V_{r+1} \cup \ldots \cup V_{n-1}$.

Demostración. Para cada $0 \leq r \leq n-1$, sea $Q_r \in k[\mathcal{T}_1,\ldots,\mathcal{T}_{n-r}] - \{0\}$ el polinomio dado por el Lema 4.3.7, y sea $Q := \coprod_{r=0}^{n-1} Q_r \in k[\mathcal{T}_1,\ldots,\mathcal{T}_n]$.

Sean $t_{ij} \in k$ $(1 \leq i \leq n,\ 1 \leq j \leq s)$ tales que $Q(t_{ij}) \neq 0$. Consideremos los polinomios

$$\hat{f}_i := t_{i1} f_1 + \cdots + t_{is} f_s, \quad 1 \leq i \leq n.$$

Entonces, para cada $0 \leq r \leq n-1$, la variedad

$$Z_r := \overline{V(\hat{f}_1,\ldots,\hat{f}_{n-r}) - V} \tag{4.22}$$

es o bien vacía o bien equidimensional de dimensión r e intersección completa reducida en el abierto $\mathbb{A}^n - V$.

En particular, para $r = 0$, se tiene que Z_0 es o bien vacía o bien un conjunto finito de puntos que no pertenecen a V. Observamos que, por la desigualdad de Bézout, $\#Z_0 \leq d^n$, puesto que Z_0 está formada por algunos de los puntos aislados de la variedad $V(\hat{f}_1,\ldots,\hat{f}_n)$ y $\deg(\hat{f}_i) \leq d$ para todo $1 \leq i \leq n$.

Sea $\mathcal{T}_{n+1} := (T_{n+11},\ldots,T_{n+1s})$ un grupo de nuevas variables y sea

$$Q^* := \prod_{\gamma \in Z_0} \left(T_{n+11} f_1(\gamma) + \cdots + T_{n+1s} f_s(\gamma)\right) \in k[\mathcal{T}_{n+1}],$$

que es un polinomio no nulo, puesto que para cada $\gamma \in Z_0$ se tiene que $\gamma \notin V$ y, en consecuencia, $f_i(\gamma) \neq 0$ para algún $1 \leq i \leq s$.

Entonces, para cualquier s-upla $t_{n+1} := (t_{n+11},\ldots,t_{n+1s})$ que verifica $Q^*(t_{n+1}) \neq 0$, se tiene que el polinomio

$$\hat{f}_{n+1} := t_{n+11} f_1 + \cdots + t_{n+1s} f_s$$

no se anula en ningún punto de Z_0. Luego

$$V(\hat{f}_1,\ldots,\hat{f}_n,\hat{f}_{n+1}) = V,$$

que es la condición (p1).

Veamos que también vale (p2).

Para cada $0 \leq r \leq n-1$, sea $Z_r \subset \mathbb{A}^n$ la variedad definida en (4.22).

Observamos que, como $V \subset V(\hat{f}_1, \ldots, \hat{f}_{n-r})$, vale

$$V(\hat{f}_1, \ldots, \hat{f}_{n-r}) = \overline{V(\hat{f}_1, \ldots, \hat{f}_{n-r}) - V} \cup V = Z_r \cup V. \tag{4.23}$$

Fijemos r con $0 \leq r \leq n-1$. De la igualdad (4.23) y el hecho que $V \subset V(\hat{f}_{n-r+1})$ se deduce que

$$\overline{V(\hat{f}_1, \ldots, \hat{f}_{n-r}) \cap \{\hat{f}_{n-r+1} \neq 0\}} = \overline{Z_r \cap \{\hat{f}_{n-r+1} \neq 0\}}. \tag{4.24}$$

Sea C una componente irreducible de Z_r. Entonces $\dim C = r$ y C está incluida en $V(\hat{f}_1, \ldots, \hat{f}_{n-r})$. Si $C \subset V(\hat{f}_{n-r+1})$, entonces

$$C \subset V(\hat{f}_1, \ldots, \hat{f}_{n-r}, \hat{f}_{n-r+1}) = Z_{r-1} \cup V$$

que es consecuencia de la validez de (4.23) para $r-1$. Como $\dim Z_{r-1} = r-1$, la condición anterior implica que $C \subset V$, lo que contradice el hecho que C es una componente irreducible de $\overline{V(\hat{f}_1, \ldots, \hat{f}_{n-r}) - V}$. Luego, $C \cap \{\hat{f}_{n-r+1} \neq 0\} \neq \emptyset$.

En consecuencia $\overline{Z_r \cap \{\hat{f}_{n-r+1} \neq 0\}} = Z_r$ y entonces de la igualdad (4.24) se sigue que

$$\overline{V(\hat{f}_1, \ldots, \hat{f}_{n-r}) \cap \{\hat{f}_{n-r+1} \neq 0\}} = Z_r.$$

Finalmente observamos que si los polinomios $\hat{f}_1, \ldots, \hat{f}_{n-r}$ forman una intersección completa reducida para Z_r en el abierto $\mathbb{A}^n - V$, lo mismo vale en el abierto $\{\hat{f}_{n-r+1} \neq 0\} \subset \mathbb{A}^n - V$. Esto concluye la prueba de (p2).

La validez de (p3) se sigue por inducción en r:

Para $r = 0$, observamos que

$$\begin{aligned} V(\hat{f}_1, \ldots, \hat{f}_n) &= V(\hat{f}_1, \ldots, \hat{f}_{n+1}) \cup \overline{V(\hat{f}_1, \ldots, \hat{f}_n) \cap \{\hat{f}_{n+1} \neq 0\}} \\ &= V \cup Z_0 \end{aligned}$$

que es la condición (p3) para $r = 0$.

Sea ahora $r \geq 1$ y supongamos que (p3) vale para $r-1$.

En primer lugar, observamos que toda componente irreducible de $V(\hat{f}_1, \ldots, \hat{f}_{n-r})$ tiene dimensión mayor o igual que r.

Por otro lado

$$\begin{aligned} V(\hat{f}_1,\ldots,\hat{f}_{n-r}) &= \overline{V(\hat{f}_1,\ldots,\hat{f}_{n-r})\cap\{\hat{f}_{n-r+1}\neq 0\}}\cup V(\hat{f}_1,\ldots,\hat{f}_{n-r+1}) \\ &= Z_r\cup Z_{r-1}\cup V_{r-1}\cup V_r\cup\ldots\cup V_{n-1}. \end{aligned}$$

Consideremos una componente irreducible C de $V(\hat{f}_1,\ldots,\hat{f}_{n-r})$. Por la igualdad anterior y el hecho que $\dim C\geq r$, resulta que C es una componente irreducible de $Z_r\cup V_r\cup\ldots\cup V_{n-1}$.
Por lo tanto, como también se tiene que $Z_r\cup V_r\cup\ldots\cup V_{n-1}\subset V(\hat{f}_1,\ldots,\hat{f}_{n-r})$, concluimos que vale

$$V(\hat{f}_1,\ldots,\hat{f}_{n-r}) = Z_r\cup V_r\cup\ldots\cup V_{n-1}.$$

Para terminar, veamos que se verifica (p4). Para cada $0\leq r\leq n-1$, de la condición (p3) y del hecho que $V_k\subset V(\hat{f}_{n-r+1})$ para todo k, deducimos que

$$\begin{aligned} Z_r\cup V_r\cup V_{r+1}\cup\ldots\cup V_{n-1} &= V(\hat{f}_1,\ldots,\hat{f}_{n-r}) \\ &= V(\hat{f}_1,\ldots,\hat{f}_{n-r-1})\cap V(f_{n-r}) \\ &= (Z_{r+1}\cup V_{r+1}\cup\ldots\cup V_{n-1})\cap V(\hat{f}_{n-r}) \\ &= (Z_{r+1}\cap V(\hat{f}_{n-r}))\cup V_{r+1}\cup\ldots\cup V_{n-1}. \end{aligned}$$

Puesto que $\hat{f}_{n-r}$ no es divisor de cero módulo $I(Z_{r+1})$, concluimos que

$$Z_{r+1}\cap V(\hat{f}_{n-r}) = Z_r\cup V_r\cup\widehat{V}_r$$

donde $\widehat{V}_r$ es una variedad equidimensional de dimensión r formada por las componentes irreducibles de $Z_{r+1}\cap V(\hat{f}_{n-r})$ que están incluidas en $V_{r+1}\cup\ldots\cup V_{n-1}$.

Observación 4.3.9 Sea $\Omega\subset k$ un conjunto de N elementos. Con las hipótesis y notación del Lema 4.3.8, sea además d una cota superior para los grados de los polinomios $f_1,\ldots,f_s$.
Observamos que entonces, por el Lema 4.3.7, el grado del polinomio Q que determina la condición sobre los elementos t_{ij} $(1\leq i\leq n,\ 1\leq j\leq s)$ está acotado por

$$\deg Q\leq\sum_{r=0}^{n-1}2(d+1)^{2(n-r)}\leq 4(d+1)^{2n}.$$

Una vez elegidos elementos t_{ij} $(1 \leq i \leq n,\ 1 \leq j \leq s)$ tales que $Q(t_{ij}) \neq 0$, la condición para los elementos $t_{n+1\,j}$ $(1 \leq j \leq s)$ está dada por un polinomio de grado acotado por d^n.

Entonces si los elementos t_{ij} $(1 \leq i \leq n+1,\ 1 \leq j \leq s)$ se eligen aleatoriamente de Ω, los polinomios $\hat{f}_1, \ldots, \hat{f}_{n+1}$ satisfacen las condiciones (p1) y (p2) con probabilidad mayor o igual que

$$\Big(1 - \frac{4(d+1)^{2n}}{N}\Big)\Big(1 - \frac{d^n}{N}\Big) \geq 1 - \frac{4(d+1)^{2n} + d^n}{N}.$$

Cambio de variables

Para el desarrollo del algoritmo serán necesarias también algunas condiciones sobre proyecciones, las que se obtendrán con alta probabilidad mediante un cambio lineal de variables.

Lema 4.3.10 *Sean $f_1, \ldots, f_{n+1} \in k[X_1, \ldots, X_n]$ polinomios que satisfacen las condiciones (p1) y (p2) del Lema 4.3.8, y sea $d := \max\{\deg f_i : 1 \leq i \leq s\}$. Para cada $0 \leq r \leq n-1$ sea*

$$Z_r := \overline{V(f_1, \ldots, f_{n-r}) - V(f_1, \ldots, f_{n+1})},$$

y sea $Z_n := \mathbb{A}^n$.

Entonces existe un polinomio no nulo $G \in k[U_{kl};\ 1 \leq k \leq n, 0 \leq l \leq n]$ de grado acotado por $n^2 d^{2(n-1)}$ tal que la condición $G(u_{kl}) \neq 0$ implica que si, para cada $1 \leq k \leq n$, se definen las nuevas variables

$$Y_k := u_{k0} + u_{k1}X_1 + \cdots + u_{kn}X_n,$$

y se consideran las proyecciones

$$\pi_k : \mathbb{A}^n \to \mathbb{A}^k\ ,\ \pi_k(x) = (y_1, \ldots, y_k)$$

entonces, para cada $1 \leq r \leq n-1$, se verifican las condiciones

(v1) $\#(Z_{r+1} \cap V(f_{n-r}) \cap \pi_r^{-1}(0)) = \deg(Z_{r+1} \cap V(f_{n-r}))$

(v2) $\#(Z_r \cap \pi_r^{-1}(0)) = \deg(Z_r)$

(v3) $Z_r \cap \pi_r^{-1}(0) \subseteq \{f_{n-r+1} \neq 0\}$

Demostración. En primer lugar, mostraremos la existencia de un polinomio no nulo $G^0 \in k[U_{kl};\ 1 \leq k \leq n-1, 0 \leq l \leq n]$ tal que la condición $G^0(u_{kl}) \neq 0$ implica que, tomando como nuevas variables $Y_k := u_{k1}X_1 + \cdots + u_{kn}X_n$ $(1 \leq k \leq n-1)$ y considerando las proyecciones $\pi_k : \mathbb{A}^n \to \mathbb{A}^k$ definidas por $\pi_k(x) = (y_1, \ldots, y_k)$, se verifica la condición (v1) para cada $1 \leq r \leq n-1$.

Sea r con $1 \leq r \leq n-1$. De la condición (p2) para Z_{r+1} se deduce que la variedad $Z_{r+1} \cap V(f_{n-r})$ es una variedad equidimensional de dimensión r.
Entonces, por [25, Prop. 4.5], existe un polinomio no nulo $G_r \in k[U_{kl};\ 1 \leq k \leq r, 0 \leq l \leq n]$ con

$$\deg G_r \leq 2\, r\, \deg(Z_{r+1} \cap V(f_{n-r}))^2$$

tal que la condición $G_r(u_{kl}) \neq 0$ implica que para las variables Y_k, $1 \leq k \leq r$, y la proyección π_r definidas en el enunciado se verifica

$$\#(Z_{r+1} \cap V(f_{n-r}) \cap \pi_r^{-1}(0)) = \deg(Z_{r+1} \cap V(f_{n-r})).$$

Teniendo en cuenta que Z_{r+1} es la unión de algunas de las componentes irreducibles de $V(f_1, \ldots, f_{n-r-1})$, deducimos que $\deg Z_{r+1} \leq \deg V(f_1, \ldots, f_{n-r+1})$. Finalmente, aplicando la desigualdad de Bézout, estimamos $\deg(Z_{r+1} \cap V(f_{n-r})) \leq d^{n-r}$, de donde resulta que

$$\deg G_r \leq 2\, r\, d^{2(n-r)}.$$

Definimos $G^0 := \prod_{r=1}^{n-1} G_r \in k[U_{kl}; 1 \leq k \leq n-1, 0 \leq l \leq n]$.
Observamos que la condición $G^0(u_{kl}) \neq 0$ implica que para las proyecciones π_k definidas con las nuevas variables, se verifica (v1) para todo $1 \leq r \leq n-1$. Además se tiene que

$$\deg G^0 \leq \sum_{1 \leq r \leq n-1} 2\, r\, d^{2(n-r)} \leq (n-1)\, n\, d^{2(n-1)}.$$

Veamos que también se verifica la condición (v2) para todo $1 \leq r \leq n-1$:
Para cada r con $1 \leq r \leq n-1$, por la condición (p4) del Lema 4.3.8, se tiene que

$$Z_{r+1} \cap V(f_{n-r}) = Z_r \cup V_r \cup \widehat{V}_r \tag{4.25}$$

donde $\widehat{V}_r$ es la unión de las componentes irreducibles de $Z_{r+1} \cap V(f_{n-r})$ incluidas en $V_{r+1} \cup \ldots \cup V_{n-1}$.
En particular

$$\deg(Z_{r+1} \cap V(f_{n-r})) = \deg Z_r + \deg V_r + \deg \widehat{V}_r \tag{4.26}$$

y

$$\#(Z_{r+1}\cap V(f_{n-r})\cap\pi_r^{-1}(0)) \leq \#(Z_r\cap\pi_r^{-1}(0))+\#(V_r\cap\pi_r^{-1}(0))+\#(\widehat{V}_r\cap\pi_r^{-1}(0)) \quad (4.27)$$

Como por la condición (v1), los miembros izquierdos de las igualdades en (4.26) y (4.27) coinciden y cada sumando del miembro derecho de (4.26) es una cota superior del sumando correspondiente en (4.27), concluimos que la igualdad vale término a término y, en particular, $\deg Z_r = \#(Z_r \cap \pi_r^{-1}(0))$.

A continuación definiremos un polinomio $G^* \in k[U_{kl}; 1 \leq k \leq n-1, 1 \leq l \leq n] - \{0\}$ (independiente de G^0) tal que la condición $G^*(u_{kl}) \neq 0$ implique que, para cada $1 \leq r \leq n-1$, se verifique la condición (v3).

Sea r con $1 \leq r \leq n-1$. Consideremos el morfismo $\phi_r : \mathbb{A}^{rn} \times Z_r \to \mathbb{A}^{rn} \times \mathbb{A}^r$ definido por

$$\phi_r(u'_1,\ldots,u'_r,\xi) := (u'_1,\ldots,u'_r,u_{11}\xi_1+\cdots+u_{1n}\xi_n,\ldots,u_{r1}\xi_1+\cdots+u_{rn}\xi_n)$$

donde $u'_k := (u_{k1},\ldots,u_{kn})$ para cada $1 \leq k \leq n$.

La aplicación ϕ_r es un morfismo dominante y, como $\dim(Z_r \cap V(f_{n-r+1})) = r-1$, resulta que

$$\overline{\phi_r(\mathbb{A}^{rn} \times Z_r \cap V(f_{n-r+1}))} \subseteq \mathbb{A}^{rn} \times \mathbb{A}^r$$

es una hipersuperficie, de grado acotado por $\deg(Z_r \cap V(f_{n-r+1})) \leq d^{n-r+1}$.

Para cada $1 \leq k \leq r$, sea $U'_k := (U_{k1},\ldots,U_{kn})$. Sea $G_r^* \in k[U'_1,\ldots,U'_r,U_{10},\ldots,U_{r0}]$ un polinomio, de grado acotado por $\deg(Z_r\cap V(f_{n-r+1}))$, que define la hipersuperficie $\overline{\phi_r(\mathbb{A}^{rn} \times W_r \cap V(f_{n-r+1}))}$.

Entonces, para $u := (u'_1,\ldots,u'_r,-u_{10},\ldots,-u_{n0})$ tal que $G_r^*(u) \neq 0$, se verifica

$$u \notin \phi_r(\mathbb{A}^{rn} \times Z_r \cap V(f_{n-r+1})).$$

Consideremos las nuevas variables

$$Y_k := u_{k0} + u_{k1}X_1 + \cdots + u_{kn}X_n, \qquad 1 \leq k \leq r$$

asociadas a u, y la proyección $\pi_r : (x_1,\ldots,x_n) \mapsto (y_1,\ldots,y_r)$. Observamos que si $\xi \in Z_r \cap \pi_r^{-1}(0)$, entonces $u_{k1}\xi_1 + \cdots + u_{kn}\xi_n = -u_{k0}$ para cada $1 \leq k \leq r$ y $\xi \in Z_r$, de donde $u = \phi_r(u'_1,\ldots,u'_r,\xi) \in \phi_r(\mathbb{A}^{rn} \times Z_r)$. Teniendo en cuenta que $u \notin \phi_r(\mathbb{A}^{rn} \times Z_r \cap V(f_{n-r+1}))$, deducimos entonces que $\xi \notin V(f_{n-r+1})$.

Esto significa que

$$Z_r \cap \pi_r^{-1}(0) \subseteq \{f_{n-r+1} \neq 0\},$$

que es la condición (v3).

Definimos $G^* := \prod_{r=1}^{n-1} G_r^* \in k[U_{kl}; 1 \leq k \leq n-1, 0 \leq l \leq n]$. De la construcción de G^* se deduce inmediatamente que la condición $G^*(u_{kl}) \neq 0$ implica la validez de (v3) para cada $1 \leq r \leq n-1$. Además, se tiene que

$$\deg G^* \leq \sum_{r=1}^{n-1} d^{n-r+1} \leq (n-1)d^n.$$

Para asegurarnos que las combinaciones lineales $Y_1, \ldots, Y_n$ sean efectivamente un cambio de variables, consideraremos también el polinomio $G_n := \det(U_{kl})_{1 \leq k,l \leq n}$.

Finalmente tomamos $G := G^0 G^* G_n$. Es claro, a partir de las propiedades de los polinomios G^0, G^* y G_n, que $G(u_{kl}) \neq 0$ implica que las combinaciones lineales $Y_1, \ldots, Y_n$ asociadas a $\{u_{kl}; 1 \leq k \leq n, 0 \leq l \leq n\}$ son un cambio de variables y que para las proyecciones π_k, $1 \leq k \leq n$, definidas con estas nuevas variables se verican las condiciones (v1), (v2) y (v3) del enunciado.

A partir de las cotas para los grados de los polinomios G^0, G^* y G_n se obtiene una cota superior para el grado de G:

$$\deg G \leq (n-1)n\, d^{2(n-1)} + (n-1)d^n + n \leq n^2 d^{2(n-1)}.$$

Observación 4.3.11 Con las hipótesis y notación del Lema 4.3.10, si los elementos u_{kl} $(1 \leq k \leq n,\ 0 \leq l \leq n)$ se eligen aleatoriamente de un subconjunto $\Omega \subset k$ de N elementos, la probabilidad de que se verifiquen las condiciones (v1), (v2) y (v3) para cada $1 \leq r \leq n-1$ es al menos $1 - \frac{n^2 d^{2(n-1)}}{N}$.

Preparación de los datos

Como consecuencia de los Lemas 4.3.8 y 4.3.10, y de las Observaciones 4.3.9 y 4.3.11 se obtiene el siguiente resultado que provee una estimación de la probabilidad de éxito de la modificación aleatoria que realizaremos en los polinomios dados como entrada al algoritmo:

Proposición 4.3.12 *Sea $V \subseteq \mathbb{A}^n(\overline{k})$ una variedad algebraica afín definida por polinomios $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ de grados acotados por d. Sea $\Omega \subseteq k$ un conjunto de N elementos. Entonces, si se eligen aleatoriamente elementos $\{t_{ij}, 1 \leq i \leq n+1, 1 \leq j \leq s\}$ y $\{u_{kl}, 1 \leq k \leq n, 0 \leq l \leq n\}$ de Ω, los polinomios*

$$\hat{f}_i := t_{i1} f_1 + \cdots + t_{is} f_s, \quad 1 \leq i \leq n+1,$$

verifican las condiciones (p1) y (p2) del Lema 4.3.8 y para las variables y proyecciones

$$Y_k := u_{k0} + u_{k1} X_1 + \cdots + u_{kn} X_n \quad \text{y} \quad \pi_k(x) = (y_1, \ldots, y_k), \quad 1 \leq k \leq n,$$

se cumplen las condiciones (v1), (v2) y (v3) del Lema 4.3.10, con probabilidad mayor o igual que

$$1 - \frac{4(d+1)^{2n} + d^n + n^2 d^{2(n-1)}}{N}.$$

4.3.3 Algunas herramientas

El algoritmo que presentaremos utiliza varios algoritmos auxiliares en los pasos intermedios. En esta sección describimos dos de estos algoritmos.

Cálculo de intersecciones

Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r y sea $f \in k[X_1, \ldots, X_n]$ un polinomio que no es un divisor de cero módulo el ideal $I(V)$. Entonces, $V \cap V(f)$ es una variedad equidimensional de dimensión $r-1$.

En el próximo lema se construye un algoritmo que bajo ciertas hipótesis técnicas (ver Sección 4.2.1) calcula, a partir de una resolución geométrica de una fibra de V, la forma de Chow de la variedad $V \cap V(f)$.

Lema 4.3.13 *Sea $V \subset \mathbb{A}^n$ una variedad equidimensional de dimensión r que satisface la hipótesis 4.2.1. Supongamos que V es intersección completa reducida en un abierto $\{g \neq 0\}$ de $\mathbb{A}^n$ que contiene a $V \cap V(X_1, \ldots, X_r)$. Sea $f \in k[X_1, \ldots, X_n]$ un polinomio que no es divisor de cero módulo $I(V)$. Entonces existe un algoritmo probabilístico que tomando como entrada:*

- *el polinomio f dado por un straight-line program,*

- *un conjunto de polinomios* $\{f_1, \ldots, f_{n-r}\}$, *dados por un straight-line program, que forman una intersección completa reducida para* V *en el abierto* $\{g \neq 0\}$ *y*
- *una resolución geométrica de* $V \cap V(X_1, \ldots, X_r)$

produce un straight-line program que representa una forma de Chow $\mathcal{F}_{V \cap V(f)}$ *de* $V \cap V(f)$.

Sean $D := \deg V$, $d := \max\{\deg f_i : 1 \leq i \leq n-r\}$ *y* L *la longitud del straight-line program que codifica los polinomios* $f, f_1, \ldots, f_{n-r}$. *Entonces la complejidad del algoritmo y la longitud del straight-line program que produce son de orden* $(n\,d\,D)^{O(1)}L$. *Si los parámetros aleatorios se eligen de un subconjunto de* k *con* N *elementos, la probabilidad de éxito del algoritmo es al menos*

$$1 - \frac{rdD\,(2rdD+3)}{N}.$$

Demostración. Para cada $0 \leq i \leq r$, sea $U_i := (U_{i0}, \ldots, U_{in})$ un grupo de nuevas variables asociado a una forma lineal afín genérica $L_i(U_i, X)$; y sea $U(d)_r$ un grupo de $\binom{d+n}{n}$ variables asociadas a un polinomio genérico F de grado d. Notaremos $U' := (U_0, \ldots, U_{r-1})$.

Sea $Ch_{d,V} \in k[U_0, \ldots, U_{r-1}, U(d)_r]$ la d-forma de Chow normalizada de V.

Denotamos por $Ch_{d,V}(f) \in k[U']$ al polinomio que resulta de especializar las variables $U(d)_r$ de $Ch_{d,V}$ en los coeficientes del polinomio f.

Consideremos la variedad proyectiva $\overline{V} \cap V(\overline{f})$, donde $\overline{V} \subseteq \mathbb{P}^n$ es la clausura proyectiva de V y $\overline{f} \in k[X_0, X_1, \ldots, X_n]$ es la homogeneización de f, con respecto a la variable X_0, hasta grado d.

El hecho que f no es un divisor de cero módulo $I(V)$ implica que $\overline{V} \cap V(\overline{f})$ es una variedad equidimensional de dimensión $r-1$.

Se tiene que

$$Ch_{d,V}(f)(u_0, \ldots, u_{r-1}) = 0 \iff$$
$$\overline{V} \cap \{\overline{L}_0(u_0, x) = 0, \ldots, \overline{L}_{r-1}(u_{r-1}, x) = 0\} \cap \{\overline{f}(x) = 0\} \neq \emptyset,$$

donde $\overline{L}_i$ denota la homogeneización de L_i con respecto a la variable X_0.

La segunda de estas condiciones es equivalente al hecho que

$$\mathcal{F}_{\overline{V} \cap V(\overline{f})}(u_0, \ldots, u_{r-1}) = 0,$$

para una forma de Chow $\mathcal{F}_{\overline{V}\cap V(\overline{f})}$ de $\overline{V}\cap V(\overline{f})$. Se sigue que el polinomio $Ch_{d,V}(f)$ define la misma hipersuperficie en $(\mathbb{P}^n)^r$ que $\mathcal{F}_{\overline{V}\cap V(\overline{f})}$.

Por lo tanto, si $\overline{V}\cap V(\overline{f}) = \bigcup_{C\in\mathcal{C}} C$ es la descomposición irreducible minimal de $\overline{V}\cap V(\overline{f})$ y, para cada componente irreducible C, $\mathcal{F}_C$ denota una forma de Chow de C, existen una constante no nula $a\in k$ y enteros positivos m_C tales que

$$Ch_{d,V}(f)(U') = a\prod_{C\in\mathcal{C}}\mathcal{F}_C(U')^{m_C}.$$

Teniendo en cuenta que las componentes irreducibles de $\overline{V\cap V(f)}$ son las componentes irreducibles C de $\overline{V}\cap V(\overline{f})$ que no están incluidas en el hiperplano $\{x_0=0\}$, concluimos que

$$\mathcal{F}_{V\cap V(f)} := \prod_{C\not\subseteq\{x_0=0\}}\mathcal{F}_C$$

es una forma de Chow de $V\cap V(f)$.

Para calcular esta forma de Chow, se obtendrá en primer lugar el polinomio $Ch_{d,V}(f)$ y luego se eliminarán las multiplicidades y los factores correspondientes a formas de Chow de componentes irreducibles incluidas en el hiperplano del infinito.

- *Cálculo de* $Ch_{d,V}(f)$

Sea $V^0 = \{\gamma_1,\ldots,\gamma_D\}\subset\mathbb{A}^n(\overline{k(U_0,\ldots,U_{r-1})})$ la variedad cero-dimensional definida por el ideal $I^0 := (I(V), L_0,\ldots,L_{r-1})$. Por el Lema 4.3.2, se tiene que

$$Ch_{d,V}(U', U(d)_r) = \left(Ch_{V\cap V(X_r)}(U')\right)^d\ \frac{Ch_{d,V^0}(U(d)_r)}{\prod_{1\le j\le D}\gamma_{jr}^d}.$$

Puesto que V^0 es una variedad cero-dimensional, la d-forma de Chow normalizada de V^0 es

$$Ch_{d,V^0}(U(d)_r) = \prod_{1\le j\le D}F(U(d)_r,\gamma_j),$$

donde $F(U(d)_r, X) := \sum_{|\alpha|\le d}U(d)_{r\alpha}X^\alpha$ es el polinomio genérico de grado d en n variables.

Se obtiene entonces la igualdad

$$Ch_{d,V}(U', U(d)_r) = \left(Ch_{V\cap V(X_r)}(U')\right)^d\prod_{1\le j\le D}F(U(d)_r,\gamma_j)/\prod_{1\le j\le D}\gamma_{jr}^d$$

y especializando las variables $U(d)_r$ en los coeficientes del polinomio f

$$Ch_{d,V}(f)(U') = \left(Ch_{V\cap V(X_r)}(U')\right)^d \prod_{1\le j\le D} f(\gamma_j)/\prod_{1\le j\le D}\gamma_{jr}^d. \tag{4.28}$$

Esta fórmula nos permitirá obtener $Ch_{d,V}(f)(U')$ utilizando las mismas técnicas que en la Sección 4.2.

Observamos que, de los Lemas 4.2.9 y 4.2.10, y de la demostración de la Proposición 4.2.11, se deduce que puede obtenerse un straight-line program para la forma de Chow $Ch_{V\cap V(X_r)}$ por medio del algoritmo dado en la Proposición 4.2.3.

Por otro lado, con las mismas técnicas de aproximación vía el operador de Newton utilizadas en la demostración de dicha Proposición, se pueden obtener las componentes homogéneas de grado prefijado de las series

$$\prod_{1\le j\le D} f(\gamma_j) \quad \text{y} \quad \prod_{1\le j\le D}\gamma_{jr}^d.$$

Finalmente, teniendo en cuenta que de la demostración de la Proposición 4.2.13 se deduce que

$$\prod_{1\le j\le D}\gamma_{jr}^d = (-1)^{dD}Ch_{V_0}^d(U_{r-1}) + O((U'-e')^{dD+1}),$$

donde $V_0 := V\cap V(X_1,\ldots,X_r)$ y $e' = (e_1,\ldots,e_r)$, y que el resultado final de (4.28) es un polinomio de grado conocido, se aplica la Proposición 4.2.12 para obtener un straight-line program que representa el cociente dado en (4.28).

- Eliminación de multiplicidades y componentes en el infinito

El siguiente paso en el cálculo de $\mathcal{F}_{V\cap V(f)}$ consistirá en eliminar los factores múltiples del polinomio $Ch_{d,V}(f)$, así como también los factores correspondientes a las formas de Chow de las componentes incluidas en el hiperplano del infinito.

Afirmación: Para una variedad proyectiva irreducible $C\subset \mathbb{P}^n$ de dimensión ℓ, se tiene que $C\subseteq\{x_0=0\}$ si y sólo si la forma de Chow $\mathcal{F}_C(U_0,\ldots,U_\ell)$ de C no depende de las variables U_{i0}, $0\le i\le \ell$.

En efecto, supongamos que $C\subset\{x_0=0\}$. Entonces podemos considerar la forma de Chow de C como subvariedad de $\mathbb{P}^{n-1}$. Si para cada $0\le i\le\ell$, $\tilde{U}_i := (U_{i1},\ldots,U_{in})$ es un grupo de n variables, se obtiene un polinomio $\tilde{\mathcal{F}}_C\in k[\tilde{U}_0,\ldots,\tilde{U}_\ell]$ que verifica

$$\tilde{\mathcal{F}}_C(\tilde{u}_0,\ldots,\tilde{u}_\ell)=0 \iff C\cap\{\tilde{L}_0(\tilde{u}_0,x)=0,\ldots,\tilde{L}_\ell(\tilde{u}_\ell,x)=0\}\neq\emptyset$$

donde $\tilde{L}_i$ son las formas lineales genéricas asociadas a las variables $\tilde{U}_i$.
Por otro lado, si $u_0, \ldots, u_\ell \in \mathbb{P}^n$, como $C = C \cap \{x_0 = 0\}$, se tiene que

$$C \cap \{L_0(u_0, x) = 0, \ldots, L_\ell(u_\ell, x) = 0\} = C \cap \{\tilde{L}_0(\tilde{u}_0, x) = 0, \ldots, \tilde{L}_\ell(\tilde{u}_\ell, x) = 0\}$$

de donde $\tilde{\mathcal{F}}_C$ es la forma de Chow de C como variedad en $\mathbb{P}^n$ (y en consecuencia esta forma de Chow no depende de las variables U_{i0}).
Recíprocamente, supongamos que $\mathcal{F}_C$ no depende de las variables U_{i0} $(0 \leq i \leq \ell)$.
Sea $x \in \mathbb{P}^n - \{x_0 = 0\}$ y sea $(\tilde{u}_0, \ldots, \tilde{u}_\ell)$ tal que $\mathcal{F}_C(\tilde{u}_0, \ldots, \tilde{u}_\ell) \neq 0$.
Entonces, tomando $u_{i0} := -(u_{i1}\frac{x_1}{x_0} + \cdots + u_{in}\frac{x_n}{x_0})$ se obtienen $u_0, \ldots, u_\ell \in \mathbb{P}^n$ que satisfacen

$$L_i(u_i, x) = 0 \quad \forall\, 0 \leq i \leq \ell \quad \text{y} \quad \mathcal{F}_C(u_0, \ldots, u_r) \neq 0,$$

de donde $x \notin C$.

Sea $\tilde{U} := \{U_{ij} : 0 \leq i \leq r-1,\ 1 \leq j \leq n\}$.
El polinomio $\mathcal{F}(U') := Ch_{d,V}(f)(U')$ admite una descomposición

$$\mathcal{F}(U') = \mathcal{F}_1(U')\mathcal{F}_2(\tilde{U})$$

donde $\mathcal{F}_1(U')$ no tiene ningún factor que dependa sólo de las variables $\tilde{U}$.
La afirmación anterior implica que $\mathrm{rad}(\mathcal{F}_1)$ (es decir, el polinomio libre de cuadrados cuyos ceros coinciden con los de $\mathcal{F}_1$) es una forma de Chow de $V \cap V(f)$.

Daremos ahora una identidad que nos permitirá calcular $\mathrm{rad}(\mathcal{F}_1)$ a partir del polinomio $\mathcal{F}(U')$: observamos que

$$\frac{\partial \mathcal{F}}{\partial U_{00}}(U') = \frac{\partial \mathcal{F}_1}{\partial U_{00}}(U')\,\mathcal{F}_2(\tilde{U})$$

y entonces, teniendo en cuenta que cada factor irreducible de $\mathcal{F}_1$ depende de la variable U_{00}, se obtiene $\mathrm{rad}(\mathcal{F}_1)$ como

$$\mathrm{rad}(\mathcal{F}_1) = \frac{\mathcal{F}_1}{\gcd(\mathcal{F}_1, \frac{\partial \mathcal{F}_1}{\partial U_{00}})} = \frac{\mathcal{F}}{\gcd(\mathcal{F}, \frac{\partial \mathcal{F}}{\partial U_{00}})}. \tag{4.29}$$

A continuación se resume el algoritmo, se calcula su complejidad y se estima la probabilidad de que el polinomio obtenido sea la forma de Chow de $V \cap V(f)$ si los parámetros aleatorios se extraen de un conjunto de N elementos de k.

Algoritmo

Paso 1. Obtener, a partir de la resolución geométrica de $V \cap V(X_1, \ldots, X_r)$ dada, un straight-line program de longitud $(n\,d\,D)^{O(1)}L$ para el polinomio $\mathcal{F}(U') = Ch_{d,V}(f)(U')$ según la igualdad (4.28) como sigue:

(a) Aplicar la Proposición 4.2.3 para obtener un straight-line program para $(Ch_{V\cap V(X_r)})^d$ y calcular las componentes homogéneas de grados acotados por $(r+1)d\,D$ de este polinomio.

(b) Calcular las componentes homogéneas de grados acotados por $(r+1)d\,D$ de $\prod f(\gamma_j)$, $\prod \gamma_{jr}^d$ (aplicando el operador de Newton para aproximar las series) y del producto $Ch^d_{V\cap V(X_r)} \prod f(\gamma_j)$.

(c) Obtener $\mathcal{F}(U')$ aplicando la Proposición 4.2.12, como el cociente de series dado en la igualdad (4.28).

La complejidad secuencial de este paso es de orden $(n\,d\,D)^{O(1)}L$.

Paso 2. Calcular el polinomio $\mathrm{rad}(\mathcal{F}_1)$, que es la forma de Chow de $V \cap V(f)$, de acuerdo al miembro derecho de la igualdad (4.29):

(a) Obtener un straight-line program para $\gcd(\mathcal{F}, \frac{\partial \mathcal{F}}{\partial U_{00}})$ por medio del algoritmo probabilístico dado en el Lema 1.3.8.

Dado que $\deg \mathcal{F} \leq rdD$, la complejidad de este paso es de orden

$$(rdD)^{O(1)}(r(n+1) + (n\,d\,D)^{O(1)}L) = (n\,d\,D)^{O(1)}L$$

y la probabilidad de que el straight-line program obtenido represente al polinomio $\gcd(\mathcal{F}, \frac{\partial \mathcal{F}}{\partial U_{00}})$ es al menos

$$1 - \frac{2rdD\,(rdD+1)}{N},$$

(b) Para cada $0 \leq i \leq r-1$, elegir las coordenadas de $u_i := (u_{i0}, \ldots, u_{in})$ al azar del conjunto de N elementos de k prefijado, y considerar el punto $u' = (u_0, \ldots, u_{r-1}) \in k^{r(n+1)}$. Si $\gcd(\mathcal{F}, \frac{\partial \mathcal{F}}{\partial U_{00}})(u') \neq 0$, efectuar la división de $\mathcal{F}$ por $\gcd(\mathcal{F}, \frac{\partial \mathcal{F}}{\partial U_{00}})$ aplicando el Lema 1.3.5.

La longitud del straight-line program obtenido es de orden $(n\,d\,D)^{O(1)}L$ y, por el Lema 1.3.2, la probabilidad de que el polinomio no se anule en u' es al menos

$$1 - \frac{rdD}{N}.$$

La complejidad total del algoritmo y la longitud del straight-line program que produce son de orden $(n\,d\,D)^{O(1)}$.

La probabilidad de éxito de todo el proceso es al menos

$$\left(1-\frac{2rdD\,(rdD+1)}{N}\right)\left(1-\frac{rdD}{N}\right)\geq 1-\frac{rdD\,(2rd\,D+3)}{N}.$$

Separación de componentes

El algoritmo construido en el siguiente lema calcula, dados la forma de Chow Ch_V de una variedad equidimensional $V\subset \mathbb{A}^n$ y un polinomio $f\in k[X_1,\ldots,X_n]$, el factor de Ch_V que corresponde al producto de las formas de Chow de todas las componentes irreducibles de V incluidas en $V(f)$. Esto permite separar la forma de Chow de V en el producto de dos polinomios: el primero corresponde a la forma de Chow de la unión de las componentes irreducibles de V incluidas en la hipersuperficie prefijada y el segundo, al producto de las formas de Chow de las componentes irreducibles de V que no están incluidas en dicha hipersuperficie.

Este resultado se utilizará en el algoritmo principal para obtener las formas de Chow de las componentes equidimensionales de la variedad dada a partir de las formas de Chow de una descomposición equidimensional no minimal de la variedad.

Lema 4.3.14 *Sea $V\subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado D que satisface la hipótesis 4.2.1, y sea $f\in k[x_1,\ldots,x_n]$ un polinomio de grado acotado por d que define la hipersuperficie $V(f)\subseteq \mathbb{A}^n$. Sea $\widehat{V}$ la unión de las componentes irreducibles de V incluidas en $V(f)$.*

Supongamos que Ch_V y f son calculables por medio de un straight-line program de longitud $\mathcal{L}$.

Entonces existe un algoritmo probabilístico de complejidad secuencial $(n\,d\,D)^{O(1)}\,\mathcal{L}$ que calcula un straight-line program (de longitud del mismo orden) para la forma de Chow $Ch_{\widehat{V}}$ de $\widehat{V}$. Si los parámetros aleatorios se eligen de un subconjunto de N elementos de k, la probabilidad de éxito del algoritmo es al menos

$$1-\frac{2d\,(r+1)^2D^2}{N}.$$

Demostración. Como en las secciones anteriores, sean $U_0, \ldots, U_r$ grupos de $n+1$ variables, $U := (U_0, \ldots, U_r)$, y sea $T := (T_0, \ldots, T_r)$ un grupo de $r+1$ variables. Análogamente, dado $(u,t) \in \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^{r+1}$ notaremos $u := (u_0, \ldots, u_r)$ y $t := (t_0, t')$ donde $t' := (t_1, \ldots, t_r)$.

Sea $\mathcal{P}_V = (-1)^D Ch_V(\zeta_0, \ldots, \zeta_r) \in k[U,T]$ el polinomio característico normalizado de V definido en la Sección 4.3.1.

Definimos los siguientes polinomios en $k[U,T]$:

$$F(U,T) := \left(\frac{\partial \mathcal{P}_V}{\partial T_0}\right)^d f\left(-\frac{\partial \mathcal{P}_V/\partial U_{01}}{\partial \mathcal{P}_V/\partial T_0}, \ldots, -\frac{\partial \mathcal{P}_V/\partial U_{0n}}{\partial \mathcal{P}_V/\partial T_0}\right)$$

$$P(U,T) := \gcd\big(\mathcal{P}_V(U,T), F(U,T)\big)$$

Afirmamos que $P(U,T)$ es un polinomio característico de $\widehat{V}$.

Como en el Lema 4.3.4, sea ρ el discriminante de $\mathcal{P}_V$ con respecto a la variable T_0. Para cada $(u,t) \in \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^{r+1}$ tal que $\mathcal{P}_V(u,t) = 0$ y $\rho(u,t') \neq 0$ se tiene, por el Lema 4.3.4, que

$$\xi := \left(-\frac{\partial \mathcal{P}_V/\partial U_{01}}{\partial \mathcal{P}_V/\partial T_0}(u,t), \ldots, -\frac{\partial \mathcal{P}_V/\partial U_{0n}}{\partial \mathcal{P}_V/\partial T_0}(u,t)\right) \tag{4.30}$$

pertenece a V y verifica $L_0(u_0,\xi) = t_0, \ldots, L_r(u_r,\xi) = t_r$.

En primer lugar, veamos que $\mathcal{P}_{\widehat{V}}$ divide a $P = \gcd(\mathcal{P}_V, F)$.

Como $\widehat{V} \subseteq V$, se sigue inmediatamente de la definición de polinomio característico que $\mathcal{P}_{\widehat{V}}$ divide a $\mathcal{P}_V$.

Sea $(u,t) \in \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^{r+1}$ tal que $\mathcal{P}_{\widehat{V}}(u,t) = 0$ y $\rho(u,t') \neq 0$. En particular, como $\mathcal{P}_{\widehat{V}}$ divide a $\mathcal{P}_V$, resulta que el punto $\xi \in \mathbb{A}^n$ definido en (4.30) pertenece a V. Por otro lado, como el coeficiente principal de $\mathcal{P}_{\widehat{V}}$ con respecto a la variable T_0 no se anula en u (puesto que divide a ρ), de la equivalencia (4.20) de la demostración del Lema 4.3.4 aplicada a $\widehat{V}$, se deduce que, para cada t_0 raíz de $\mathcal{P}_{\widehat{V}}(u, T_0, t')$, existe al menos un punto

$$\zeta \in \widehat{V} \cap V(L_1(u_1,x) - t_1, \ldots, L_r(u_r,x) - t_r) \subseteq V \cap V(L_1(u_1,x) - t_1, \ldots, L_r(u_r,x) - t_r)$$

que verifica $L_0(u_0,\zeta) = t_0$. Pero aplicando el mismo lema a V, resulta que ξ es el único punto en $V \cap \{L_0(u_0,x) = t_0, \ldots, L_r(u_r,x) = t_r\}$, de donde se deduce que $\xi \in \widehat{V}$. Luego $f(\xi) = 0$, y por lo tanto $F(u,t) = 0$.

En consecuencia,

$$V(\mathcal{P}_{\widehat{V}}) \cap \{\rho(u,t') \neq 0\} \subseteq V(F)$$

lo que implica, teniendo en cuenta que $V(\mathcal{P}_{\widehat{V}}) \not\subset V(\rho)$, que $\mathcal{P}_{\widehat{V}}$ divide a F.
Concluimos que $\mathcal{P}_{\widehat{V}}$ divide a $\gcd(\mathcal{P}_V, F) =: P$.

Veamos ahora que P divide a $\mathcal{P}_{\widehat{V}}$.

Sea $\psi : \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^n \to \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^{r+1}$ el morfismo asociado a la definición de polinomio característico, es decir, el morfismo definido por

$$\psi(u,\xi) = (u, L_0(u_0,\xi), L_1(u_1,\xi), \ldots, L_r(u_r,\xi)).$$

En primer lugar mostraremos que

$$V(P) \cap \{\rho \neq 0\} \subseteq \psi(\mathbb{A}^{(r+1)(n+1)} \times (V \cap V(f))).$$

Sea $(u,t) \in \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^{r+1}$ tal que $P(u,t) = 0$ y $\rho(u,t') \neq 0$. Como P divide a $\mathcal{P}_V$, se tiene que $\mathcal{P}_V(u,t) = 0$ y en consecuencia, el punto $\xi \in \mathbb{A}^n$ definido en (4.30) pertenece a V y verifica $L_0(u_0,\xi) = t_0, \ldots, L_r(u_r,\xi) = t_r$.
Además, como P divide a F, también vale $F(u,t) = 0$. Por otro lado, teniendo en cuenta que $\rho(u,t') \neq 0$, deducimos que $\frac{\partial \mathcal{P}_V}{\partial T_0}(u,t) \neq 0$. Concluimos entonces que $f(\xi) = 0$, es decir $\xi \in V(f)$.
Luego, $(u,t) = \psi(u,\xi) \in \psi(\mathbb{A}^{(r+1)(n+1)} \times (V \cap V(f)))$.

Puesto que ρ no depende de la variable T_0, ninguna componente de $V(P)$ está incluida en $V(\rho)$, y por lo tanto $\overline{V(P) \cap \{\rho \neq 0\}} = V(P)$. Luego

$$V(P) \subseteq \overline{\psi(\mathbb{A}^{(r+1)(n+1)} \times (V \cap V(f)))}.$$

Más aún, como $V(P) \subseteq \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^{r+1}$ es una hipersuperficie, se tiene que $V(P)$ está incluida en la componente equidimensional de codimension 1 de la variedad $\overline{\psi(\mathbb{A}^{(r+1)(n+1)} \times (V \cap V(f)))}$, que es

$$\overline{\psi(\mathbb{A}^{(r+1)(n+1)} \times \widehat{V})} = V(\mathcal{P}_{\widehat{V}}).$$

Teniendo en cuenta que P es libre de cuadrados, concluimos entonces que P divide a $\mathcal{P}_{\widehat{V}}$.

Finalmente observamos que para obtener una forma de Chow de $\widehat{V}$ a partir del polinomio $\mathcal{P}_{\widehat{V}} = P(U,T)$, basta especializar las variables $T_0, \ldots, T_r$ en 0. Normalizando la forma de Chow calculada de esta manera, se obtiene $Ch_{\widehat{V}}(U)$.

Para terminar, resumimos el algoritmo que calcula la forma de Chow $Ch_{\widehat{V}}$ a partir de Ch_V, calculamos su complejidad y su probabilidad de éxito al elegir los parámetros al azar de un conjunto dado de N elementos de k.

Algoritmo

Paso 1. A partir de un straight-line program para Ch_V, obtener un straight-line program para $\mathcal{P}_V := Ch_V(\zeta_0, \ldots, \zeta_r)$ y sus derivadas parciales con respecto a las variables T_0 y $U_{01}, \ldots, U_{0n}$. Esto requiere $O(n\,\mathcal{L})$ pasos.

Paso 2. Aplicando el Lema 1.3.4, calcular las componentes homogéneas de grados acotados por d del polinomio f. Esto agrega $d^{O(1)}\mathcal{L}$ pasos.

Notación: Para cada $0 \leq i \leq d$, f_i denotará la componente homogénea de grado i de f.

Paso 3. Obtener un straight-line program para $F(U,T)$ de acuerdo a la siguiente igualdad:

$$F(U,T) = \sum_{i=0}^{d} \left(\frac{\partial \mathcal{P}_V}{\partial T_0}\right)^{d-i} f_i\left(-\frac{\partial \mathcal{P}_V}{\partial U_{01}}, \ldots, -\frac{\partial \mathcal{P}_V}{\partial U_{0n}}\right).$$

La longitud del straight-line program obtenido y la complejidad del algoritmo hasta este paso son de orden $(n\,d)^{O(1)}\mathcal{L}$.

Observamos que $\deg F \leq d\,((r+1)D - 1)$.

Paso 4. Calcular probabilísticamente un straight-line program para el polinomio $\mathcal{P}_{\widehat{V}} := \gcd(\mathcal{P}_V, F)$ aplicando el Lema 1.3.8.

La complejidad es de orden $(n\,d\,D)^{O(1)}\mathcal{L}$ y y la probabilidad de éxito del algoritmo (ver la demostración del Lema 1.3.8) es al menos

$$1 - \frac{2d\,(r+1)^2 D^2}{N}.$$

Paso 5. Especializar las variables $(T_0, \ldots, T_r) \mapsto 0$ en $\mathcal{P}_{\widehat{V}}$ y normalizar la forma de Chow así obtenida dividiéndola por su especialización en $(c_0, \ldots, c_r)$.

La complejidad total del algoritmo y la longitud del straight-line program que produce son de orden $(n\,d\,D)^{O(1)}\mathcal{L}$. La probabilidad de éxito del algoritmo es la estimada en el paso 4.

4.3.4 El algoritmo

En el siguiente Teorema se prueba el resultado principal presentado en este capítulo: la existencia de un algoritmo probabilístico que calcula las formas de Chow de cada una de las componentes equidimensionales de una variedad algebraica afín, a partir de un conjunto finito de polinomios que la define, con complejidad secuencial polinomial en el tamaño del input.

Teorema 4.3.15 *Sean $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ polinomios (no todos nulos) de grados acotados por d dados por medio de un straight-line program de longitud L. Sea $V := V(f_1, \ldots, f_s) \subset \mathbb{A}^n$ la variedad algebraica afín definida por estos polinomios y sea*

$$V = V_0 \cup \ldots \cup V_{n-1}$$

la descomposición equidimensional minimal de V (donde, para cada $0 \leq r \leq n-1$, V_r es o bien vacía o bien una variedad equidimensional de dimensión r).

Entonces, existe un algoritmo probabilístico de complejidad secuencial acotada por $s\, n^{O(1)} d^{O(n)} L$ que produce un straight-line program de longitud $s\, n^{O(1)} d^{O(n)} L$ que representa las formas de Chow de cada una de las componentes equidimensionales V_r de V $(0 \leq r \leq n-1)$.

Demostración. El algoritmo consta de tres etapas:

En la primera etapa, se modifican los polinomios de entrada en el sentido de la Sección 4.3.2 con el objeto de obtener un nuevo sistema de polinomios que defina la variedad V, pero que satisfaga también ciertas condiciones adicionales necesarias para la aplicación de las subrutinas que realizan los cálculos intermedios del algoritmo.

En la segunda etapa, el algoritmo calcula recursivamente las formas de Chow de las componentes equidimensionales de una descomposición equidimensional no minimal de V. El algoritmo presentado en el Lema 4.3.13 es la herramienta principal en que se basa el procedimiento recursivo.

Finalmente, en la tercera etapa, el algoritmo obtiene, a partir de las formas de Chow calculadas en la etapa anterior, las formas de Chow de cada una de las componentes equidimensionales de V por medio del Lema 4.3.14 aplicado a formas de Chow calculadas previamente e hipersuperficies convenientemente elegidas.

- Preparación de los datos.

Sea Ω un subconjunto de k con N elementos. Se eligen al azar del conjunto Ω elementos $\{t_{ij}, 1 \leq i \leq n+1,\ 1 \leq j \leq s\}$ y $\{u_{kl}, 1 \leq k \leq n,\ 0 \leq l \leq n\}$, y se definen los polinomios

$$\hat{f}_i := t_{i1} f_1 + \cdots + t_{is} f_s, \quad 1 \leq i \leq s,$$

y las nuevas variables

$$Y_k := u_{k0} + u_{k1} X_1 + \cdots + u_{kn} X_n, \quad 1 \leq k \leq n.$$

Para simplificar la notación, renombramos a las nuevas variables $Y_1, \ldots, Y_n$ como $X_1, \ldots, X_n$, y a los nuevos polinomios $\hat{f}_1, \ldots, \hat{f}_{n+1}$ en las nuevas variables como $f_1, \ldots, f_{n+1}$.

Por la Proposición 4.3.12, los nuevos polinomios $f_1, \ldots, f_{n+1}$ en las nuevas variables satisfacen, con probabilidad al menos

$$P^{(1)} = 1 - \frac{4(d+1)^{2n} + d^n + n^2 d^{2(n-1)}}{N}$$

las condiciones:

(p1) $V = V(f_1, \ldots, f_{n+1})$,

(p2) Para cada $0 \leq r \leq n-1$, la variedad

$$Z_r := \overline{V(f_1, \ldots, f_{n-r}) \cap \{f_{n-r+1} \neq 0\}}$$

es equidimensional de dimensión r y los polinomios $f_1, \ldots, f_{n-r}$ forman una intersección completa reducida para Z_r en el abierto $\{f_{n-r+1} \neq 0\}$

y, para cada $0 \leq r \leq n-1$,

(v1) $\#(Z_{r+1} \cap V(f_{n-r}) \cap V(X_1, \ldots, X_r)) = \deg(Z_{r+1} \cap V(f_{n-r}))$,

(v2) $\#(Z_r \cap V(X_1, \ldots, X_r)) = \deg(Z_r)$,

(v3) $Z_r \cap V(X_1, \ldots, X_r) \subseteq \{f_{n-r+1} \neq 0\}$.

De ahora en más supondremos que los valores de los parámetros han sido elegidos de manera que valgan las condiciones (p1), (p2), (v1), (v2) y (v3) anteriores.

Observamos que, en particular, las variedades Z_r $(0 \leq r \leq n-1)$ verifican las hipótesis necesarias para la aplicación de los algoritmos dados en la Proposición 4.2.3 y el Lema 4.3.13. Además se verifican las siguientes propiedades derivadas de (p1) y (p2) (ver Lema 4.3.8):

(p3) $V(f_1,\ldots,f_{n-r}) = Z_r \cup V_r \cup \ldots \cup V_{n-1}$

(p4) $Z_{r+1} \cap V(\hat{f}_{n-r}) = Z_r \cup V_r \cup \widehat{V}_r$, donde $\widehat{V}_r$ es la unión de las componentes irreducibles de $Z_{r+1} \cap V(f_{n-r})$ incluidas en $V_{r+1} \cup \ldots \cup V_{n-1}$.

- Formas de Chow de una descomposición equidimensional no minimal de V.

En esta etapa el algoritmo calcula, para cada $0 \leq r \leq n-1$, la forma de Chow de una variedad equidimensional incluida en V y que contiene a la componente equidimensional de dimensión r de V.

Recordemos que, para cada $0 \leq r \leq n-1$, por la propiedad (p4) se tiene que

$$Z_{r+1} \cap V(f_{n-r}) = Z_r \cup V_r \cup \widehat{V}_r$$

donde $\widehat{V}_r$ es una variedad equidimensional de dimensión r incluida en $V_{r+1} \cup \ldots \cup V_{n-1}$. Para cada $0 \leq r \leq n-1$, se calculará la forma de Chow de la variedad equidimensional $V_r \cup \widehat{V}_r$. Este cálculo se hará recursivamente.

PRIMER PASO Se comienza por $r := n-1$.

En este paso se calculan la forma de Chow $Ch_{V_{n-1}}$ de la componente equidimensional V_{n-1} y una resolución geométrica de la variedad cero-dimensional

$$Z_{(n-1,0)} := Z_{n-1} \cap V(X_1,\ldots,X_{n-1}).$$

Se tiene que $V(f_1) = Z_{n-1} \cup V_{n-1}$ donde V_{n-1} es la unión de las componentes irreducibles de $V(f_1)$ incluidas en $V(f_2)$ y Z_{n-1} es la unión de las componentes irreducibles restantes.

Entonces, si consideramos los polinomios libres de cuadrados

$$\tilde{f}_1 := \gcd(\mathrm{rad}(f_1), f_2) \quad \text{y} \quad \tilde{f}_2 := \frac{\mathrm{rad}(f_1)}{\gcd(\mathrm{rad}(f_1), f_2)},$$

(donde $\mathrm{rad}(f_1)$ es un polinomio libre de cuadrados cuyos ceros coinciden con los de f_1), se tiene que

$$V_{n-1} = V(\tilde{f}_1) \quad \text{y} \quad Z_{n-1} = V(\tilde{f}_2)$$

y, más aún, $\tilde{f}_1$ y $\tilde{f}_2$ son generadores de los ideales de V_{n-1} y Z_{n-1} respectivamente.

De la fórmula para la forma de Chow en el caso de una hipersuperficie se sigue que, si $M_0,\ldots,M_n$ denotan los menores maximales de la matriz $(U_{ij})_{0\leq i\leq n-1, 0\leq j\leq n}$

(donde M_j es el menor que se obtiene al suprimir la j-ésima columna de la matriz), y si $d_1 := \deg \tilde{f}_1$, entonces

$$\mathcal{F}_{V_{n-1}} = M_0^{d_1} \tilde{f}_1(-M_1/M_0, M_2/M_0, \ldots, (-1)^n M_n/M_0) \tag{4.31}$$

es una forma de Chow de V_{n-1}. Normalizando esta forma de Chow, es decir, dividiéndola por su especialización en $(e_0, \ldots, e_{n-1})$, se obtiene la forma de Chow $Ch_{V_{n-1}}$ de V_{n-1}.

Para obtener una resolución geométrica de la variedad cero-dimensional $Z_{(n-1,0)} = Z_{n-1} \cap V(X_1, \ldots, X_{n-1})$, basta observar que por hipótesis $\deg Z_{(n-1,0)} = \deg Z_{n-1}$. En consecuencia, la forma lineal X_n separa los puntos de $Z_{(n-1,0)}$ y su polinomio minimal es simplemente $\tilde{f}_2(0, \ldots, 0, X_n)$.

Resumimos el algoritmo que calcula $Ch_{V_{n-1}}$ y una resolución geométrica de $Z_{(n-1,0)}$, calculamos su complejidad $\mathcal{L}_{n-1}$ y su probabilidad de éxito P_{n-1} al elegir los parámetros aleatorios de un subconjunto de N elementos de k.

Algoritmo

Paso 1. Calcular $\mathrm{rad}(f_1)$ aplicando el Lema 1.3.11. Esto puede realizarse con complejidad de orden $d^{O(1)}(n + L)$ y probabilidad de éxito mayor o igual que $1 - \frac{2d^2+3d}{N}$.

Paso 2. Calcular $\tilde{f}_1$ y $\tilde{f}_2$ aplicando los Lemas 1.3.8 y 1.3.5. La complejidad de este paso es de orden $d^{O(1)}(n + L)$ y la probabilidad de calcular $\tilde{f}_1$ y $\tilde{f}_2$ (si en el primer paso el cálculo de $\mathrm{rad}(f_1)$ es correcto) es mayor o igual que

$$\left(1 - \frac{2d(d+1)}{N}\right)\left(1 - \frac{d}{N}\right) \geq 1 - \frac{2d^2 + d}{N}.$$

Observamos que el algoritmo del Lema 1.3.8 calcula también $d_1 := \deg \tilde{f}_1$.

Paso 3. Obtener los menores $M_0, \ldots, M_n$ en $(n+1)n^3$ pasos. Aplicando el Lema 1.3.4 homogeneizar el polinomio $\tilde{f}_1$ y obtener un straight-line program para la forma de Chow $\mathcal{F}_{V_{n-1}}$ según la fórmula (4.31). Finalmente, dividir esta forma de Chow por su especialización en $(e_0, \ldots, e_{n-1})$ para obtener $Ch_{V_{n-1}}$.

Este paso es determinístico y su complejidad es de orden $(n\,d)^{O(1)}L$.

Paso 4. A partir del straight-line program para $\widetilde{f}_2$, obtener un straight-line program para el polinomio univariado $p(X_n) := \widetilde{f}_2(0,\ldots,0,X_n)$ y, por medio de un proceso de interpolación, obtener el vector de sus coeficientes.

Este cálculo agrega $(n\,d)^{O(1)}L$ operaciones.

Por lo tanto, la complejidad total del primer paso de la recursión es de orden $\mathcal{L}_{n-1} = (n\,d)^{O(1)}L$ y la probabilidad de haber calculado los objetos correctos es

$$P_{n-1} \geq \big(1 - \frac{2d^2+3d}{N}\big)\big(1 - \frac{2d^2+d}{N}\big) \geq 1 - \frac{4}{N}(d^2+d).$$

PASOS INTERMEDIOS

Sea ahora $0 \leq r \leq n-2$, y supongamos calculada en el paso anterior, una resolución geométrica de $Z_{(r+1,0)} := Z_{r+1} \cap V(X_1,\ldots,X_{r+1})$.

A partir de esta resolución geométrica se calculará una forma de Chow de la variedad $Z_{r+1} \cap V(f_{n-r})$. Con esta forma de Chow, se obtendrá una resolución geométrica de la variedad $Z_{(r,0)} := Z_r \cap V(X_1,\ldots,X_r)$, necesaria para el próximo paso de la recursión. Finalmente, usando la forma de Chow y la resolución geométrica calculadas se obtendrá la forma de Chow de $V_r \cup \widehat{V}_r$.

Aplicando el Lema 4.3.13 se calcula, a partir de la resolución geométrica de $Z_{(r+1,0)}$, la forma de Chow de la variedad equidimensional $Z_{r+1} \cap V(f_{n-r}) = Z_r \cup V_r \cup \widehat{V}_r$.

Observamos que vale la igualdad

$$Ch_{Z_{r+1}\cap V(f_{n-r})} = Ch_{Z_r} \cdot Ch_{V_r \cup \widehat{V}_r}.$$

La idea del algoritmo consiste en separar la forma de Chow $Ch_{Z_{r+1}\cap V(f_{n-r})}$ calculada en los dos factores del miembro derecho de la igualdad anterior.

Consideremos la variedad

$$Z^{(r)} := Z_{r+1} \cap V(f_{n-r}) \cap V(X_1,\ldots,X_r).$$

Por la condición (v1), $Z^{(r)}$ es una variedad cero-dimensional formada por $\deg(Z_{r+1} \cap V(f_{n-r})) \leq d^{n-r}$ puntos. Esto nos permite calcular la forma de Chow de $Z^{(r)}$ como

$$Ch_{Z^{(r)}} = Ch_{Z_{r+1}\cap V(f_{n-r})}(U_0, e_1, \ldots, e_r).$$

A partir de esta forma de Chow, podemos obtener el polinomio característico de $Z^{(r)}$ por medio de un cambio de variables

$$\mathcal{P}_{Z^{(r)}} := (-1)^{\deg(Z^{(r)})} Ch_{Z^{(r)}}(U_{00} - T_0, U_{01}, \ldots, U_{0n}).$$

Sea $\rho \in k[U_0]$ el discriminante de $\mathcal{P}_{Z^{(r)}}$ con respecto a la variable T_0. Entonces, para cualquier $u = (u_0, u_1, \ldots, u_n) \in k^{n+1}$ tal que $\rho(u) \neq 0$, por el Lema 4.3.4 se puede obtener una resolución geométrica de $Z^{(r)}$. (La elección del punto u se hace aleatoriamente y, si $\rho(u) \neq 0$, se calcula una resolución geométrica de acuerdo al lema mencionado).

Mostraremos ahora cómo obtener una resolución geométrica de

$$Z_{(r,0)} := Z_r \cap V(X_1, \ldots, X_r)$$

a partir de una resolución geométrica de $Z^{(r)}$:

Puesto que por la condición (v3) se tiene que $Z_r \cap V(X_1, \ldots, X_r) \subseteq \{f_{n-r+1} \neq 0\}$ y por otro lado $V_r \cup \widehat{V}_r \subseteq V(f_{n-r})$, valen las siguientes igualdades

$$\begin{aligned} Z_r \cap V(X_1, \ldots, X_r) &= Z^{(r)} \cap \{f_{n-r+1} \neq 0\} \\ (V_r \cup \widehat{V}_r) \cap V(X_1, \ldots, X_r) &= Z^{(r)} \cap V(f_{n-r+1}). \end{aligned}$$

Supongamos que la resolución geométrica de $Z^{(r)}$ está dada por la forma lineal $\ell = u_0 + u_1 X_1 + \cdots + u_n X_n$, su polinomio minimal $p \in k[T]$ y polinomios $v_1, \ldots, v_n \in k[T]$ tales que

$$Z^{(r)} = \{(v_1(\eta), \ldots, v_n(\eta)) : \eta \in \bar{k},\ p(\eta) = 0\}.$$

Es claro que la forma lineal ℓ es también un elemento primitivo con respecto a las variedades $Z_{(r,0)} = Z^{(r)} \cap \{f_{n-r+1} \neq 0\}$ y $Z^{(r)} \cap V(f_{n-r+1})$.

Observamos que el polinomio minimal de ℓ con respecto a $Z^{(r)} \cap V(f_{n-r+1})$ es

$$p_1(T) := \gcd\Big(p(T), f_{n-r+1}(v_1(T), \ldots, v_n(T))\Big),$$

y por lo tanto el polinomio minimal con respecto a $Z_{(r,0)}$ es $p_2 := p/p_1$.

Luego, la forma lineal ℓ, su polinomio minimal p_2 con respecto a $Z_{(r,0)}$, y los polinomios $v_1, \ldots, v_n \in k[T]$ reducidos módulo p_2 dan una resolución geométrica de $Z_{(r,0)}$.

Ahora, el algoritmo dado en la Proposición 4.2.3 obtiene, a partir de la resolución geométrica de $Z_{(r,0)}$ calculada, la forma de Chow Ch_{Z_r} de la variedad Z_r.

Finalmente, se obtiene la forma de Chow $Ch_{V_r \cup \widehat{V}_r}$ como el cociente en la división exacta

$$Ch_{V_r \cup \widehat{V}_r} := \frac{Ch_{Z_{r+1} \cap V(f_{n-r})}}{Ch_{Z_r}},$$

la que puede efectuarse mediante el Lema 1.3.5.

A continuación se resume el algoritmo presentado para el cálculo de la resolución geométrica de la variedad $Z_{(r,0)}$ y la forma de Chow $Ch_{V_r \cup \widehat{V}_r}$ a partir de la resolución geométrica de la variedad $Z_{(r+1,0)} := Z_{r+1} \cap V(X_1, \ldots, X_{r+1})$ obtenida en el paso anterior de la recursión. Se calculan también la complejidad $\mathcal{L}_r$ de este paso y la probabilidad de éxito P_r del cómputo efectuado eligiendo los parámetros aleatorios de un subconjunto $\Omega \subset k$ con N elementos.

Algoritmo

Paso 1. Aplicar el Lema 4.3.13 para calcular, a partir de la resolución geométrica de $Z_{(r+1,0)}$, la forma de Chow $Ch_{Z_{r+1} \cap V(f_{n-r})}$.

Teniendo en cuenta que $\deg(Z_{r+1}) \leq d^{n-r-1}$, la complejidad de este paso resulta de orden $(n\, d^{n-r})^{O(1)} L$ y la probabilidad de éxito es al menos

$$1 - \frac{(r+1)\, d^{n-r}(2(r+1)d^{n-r}+3)}{N}.$$

Paso 2. Con la forma de Chow calculada en el paso 1., obtener un straight-line program para $Ch_{Z^{(r)}} = Ch_{Z_{r+1} \cap V(f_{n-r})}(U_0, e_1, \ldots, e_r)$ y luego uno para el polinomio característico $\mathcal{P}_{Z^{(r)}}$ de $Z^{(r)}$.

Este paso es determinístico y su complejidad es de orden $(n\, d^{n-r})^{O(1)} L$.

Paso 3. Elegir elementos $u_0, \ldots, u_n \in \Omega$ al azar y considerar $u := (u_0, \ldots, u_n) \in k^{n+1}$.

Obtener un straight-line program para el discriminante ρ del polinomio $\mathcal{P}_{Z^{(r)}}$ con respecto a la variable T_0 y evaluar ρ en el punto u. Si $\rho(u) \neq 0$, calcular una resolución geométrica de $Z^{(r)}$ aplicando el Lema 4.3.4.

La complejidad de este paso es de orden $(n\, d^{n-r})^{O(1)} L$ y, teniendo en cuenta que $\deg_{T_0} \rho \leq 2(\deg Z^{(r)})^2 \leq 2d^{2(n-r)}$, la probabilidad de que $\rho(u) \neq 0$ (es decir, la probabilidad de calcular la resolución geométrica de $Z^{(r)}$) es mayor que

$$1 - \frac{2d^{2(n-r)}}{N}.$$

Paso 4. A partir de la resolución geométrica de $Z^{(r)}$ calcular el polinomio $p_1(T) := \gcd(p(T), f_{n-r+1}(v_1(T), \ldots, v_n(T)))$.

Para esto, obtener en primer término el vector de coeficientes del polinomio $f_{n-r+1}(v_1(T), \ldots, v_n(T))$ mediante el Lema 1.3.3 y aplicar luego el Lema 1.3.6 para calcular el máximo común divisor.

Efectuar la división $p_2 := p/p_1$ para obtener el polinomio minimal de ℓ con respecto a la variedad $Z_{(r,0)}$ y calcular los restos de los polinomios $v_1, \ldots, v_n$ en la división por p_2. Estos polinomios, junto con la forma lineal ℓ, dan una resolución geométrica de $Z_{(r,0)}$.

Este paso es determinístico y su complejidad no modifica el orden de las complejidades obtenidas hasta el momento.

Paso 5. Utilizando la resolución geométrica obtenida en el paso anterior, aplicar el algoritmo dado en la Proposición 4.2.3 para obtener un straight-line program para Ch_{Z_r}.

Este paso también es determinístico y su complejidad es de orden $(n\,d^{n-r})^{O(1)}L$.

Paso 6. Aplicar el Lema 1.3.5 para obtener un straight-line program para el cociente

$$Ch_{V_r \cup \widehat{V}_r} = \frac{Ch_{Z_{r+1} \cap V(f_{n-r})}}{Ch_{Z_r}}.$$

Teniendo en cuenta que $Ch_{Z_r}(e_0, \ldots, e_r) = 1$, este proceso, cuya complejidad es de orden $(n\,d^{n-r})^{O(1)}L$, resulta también determinístico.

En consecuencia, el costo total de este paso de la recursión es de orden $\mathcal{L}_r = (n\,d^{n-r})^{O(1)}L$. Observamos que la longitud del straight-line program para $Ch_{V_r \cup \widehat{V}_r}$ que produce el algoritmo es del mismo orden que la complejidad del proceso de cálculo.

La probabilidad de éxito de los cálculos efectuados, suponiendo que los datos provistos por el paso recursivo anterior son correctos, es

$$P_r \geq 1 - \frac{2(r+1)^2 d^{2(n-r)} + 2d^{2(n-r)} + 3(r+1)d^{n-r}}{N}.$$

Concluimos que la complejidad total del algoritmo probabilístico que calcula las formas de Chow de las variedades equidimensionales $V_r \cup \widehat{V}_r$ $(0 \leq r \leq n-1)$ es

$\mathcal{L}_{n-1} + \cdots + \mathcal{L}_0 = (n\,d^n)^{O(1)}L$. Suponiendo que los polinomios y variables satisfacen las condiciones (p1), (p2), (v1), (v2) y (v3), el algoritmo produce, con probabilidad mayor o igual que

$$\begin{aligned} P^{(2)} &= \prod_{r=0}^{n-1} P_r \\ &\geq 1 - \frac{1}{N}\Big(4(d^2+d) + \sum_{r=0}^{n-2} 2(r+1)^2 d^{2(n-r)} + 2d^{2(n-r)} + 3(r+1)d^{n-r}\Big) \\ &\geq 1 - \frac{4\,n^2 d^{2n} + 6\,n\,d^n}{N} \end{aligned}$$

un straight-line program que representa cada una de las formas de Chow $Ch_{V_r \cup \widehat{V}_r}$, $0 \leq r \leq n-1$.

Observamos que, para cada $0 \leq r \leq n-1$, la longitud del straight-line program para $Ch_{V_r \cup \widehat{V}_r}$ es de orden $(n\,d^{n-r})^{O(1)}L$.

- Cálculo de las formas de Chow de las componentes equidimensionales de V.

La última etapa del algoritmo consiste en obtener las formas de Chow de cada una de las componentes equidimensionales V_r $(0 \leq r \leq n-1)$ de la variedad dada V, a partir de las formas de Chow de las componentes de la descomposición no minimal calculadas en la etapa anterior.

Sea r con $0 \leq r \leq n-2$. En la segunda etapa del algoritmo se calculó la forma de Chow

$$Ch_{V_r \cup \widehat{V}_r} = Ch_{V_r}.Ch_{\widehat{V}_r},$$

donde V_r es *la* componente equidimensional de dimensión r de V y $\widehat{V}_r$ es una variedad equidimensional de dimensión r cuyas componentes irreducibles están incluidas en componentes irreducibles de V de dimensión mayor que r.

Para extraer el factor Ch_{V_r} de esta forma de Chow, se construirá un polinomio $G_r \in k[X_1, \ldots, X_n]$ que defina una hipersuperficie $V(G_r)$ que (probabilísticamente) verifique: $\widehat{V}_r$ es exactamente la unión de las componentes irreducibles de $V_r \cup \widehat{V}_r$ incluidas en $V(G_r)$.

Luego, se aplicará el Lema 4.3.14 para calcular $Ch_{\widehat{V}_r}$ y finalmente se efectuará la división de $Ch_{V_r \cup \widehat{V}_r}$ por $Ch_{\widehat{V}_r}$ para obtener la forma de Chow Ch_{V_r} de la componente equidimensional V_r.

Veremos ahora cómo se construye el polinomio G_r.

Recordemos que, para cada $0 \leq k \leq n-2$, se tiene

$$\widehat{V}_k \subset V_{k+1} \cup \ldots \cup V_{n-1}.$$

Se deduce entonces que

$$\widehat{V}_r \subset V_{r+1} \cup \ldots \cup V_{n-1} = (V_{r+1} \cup \widehat{V}_{r+1}) \cup \ldots \cup (V_{n-2} \cup \widehat{V}_{n-2}) \cup (V_{n-1} \cup \widehat{V}_{n-1}),$$

(donde $\widehat{V}_{n-1} = \emptyset$).

Por otro lado, por la minimalidad de la descomposición, ninguna componente irreducible de V_r está incluida en la variedad de la derecha.

Para cada $r+1 \leq k \leq n-1$, se definirá un polinomio $G_{rk} \in k[X_1, \ldots, X_n]$ que cumpla las siguientes hipótesis:

(h1) $V_k \cup \widehat{V}_k \subseteq V(G_{rk})$,

(h2) ninguna componente irreducible de V_r está incluida en $V(G_{rk})$,

y se considerará luego el polinomio $G_r := \prod_{k=r+1}^{n-1} G_{rk}$.

Bajo estas condiciones, la hipersuperficie definida por G_r contiene a la variedad $\widehat{V}_r$, pero no contiene a ninguna de las componentes irreducibles de V_r y, por lo tanto, nos permitirá separar las componentes de dichas variedades.

Fijemos k tal que $r+1 \leq k \leq n-1$.

Puesto que $Z_{k+1} \cap V(f_{n-k}) = Z_k \cup V_k \cup \widehat{V}_k$, las condiciones (v1) y (v2) dadas por la preparación de los datos implican que

$$\deg((V_k \cup \widehat{V}_k) \cap V(X_1, \ldots, X_k)) = \deg(V_k \cup \widehat{V}_k),$$

es decir, que la variedad $V_k \cup \widehat{V}_k$ satisface la hipótesis 4.2.1.

Denotamos por $\mathcal{P}_k \in k[U_0, \ldots, U_k][T_0, \ldots, T_k]$ al polinomio característico normalizado de la variedad $V_k \cup \widehat{V}_k$.

Sea $u := (0, u_1, \ldots, u_n) \in \mathbb{A}^{n+1}$ y sea $\ell := u_1 X_1 + \cdots + u_n X_n$ la forma lineal asociada a u.

Como el coeficiente principal del polinomio $\mathcal{P}_k$ con respecto a la variable T_0 especializado en $(e_1, \ldots, e_k)$ es 1, de la Observación 4.3.5 deducimos que, para cada $(t_1, \ldots, t_k) \in \mathbb{A}^k$,

$$(V_k \cup \widehat{V}_k) \cap V(X_1 - t_1, \ldots, X_k - t_k)$$

es una variedad cero-dimensional (de grado acotado por $\deg(V_k \cup \widehat{V}_k)$). Más aún, la equivalencia (4.20) en la demostración de del Lema 4.3.4 establece que, para cada $(t_1, \ldots, t_k) \in \mathbb{A}^k$, vale

$$\mathcal{P}_k(u, e_1, \ldots, e_k)(t_0, t_1, \ldots, t_k) = 0 \Leftrightarrow (V_k \cup \widehat{V}_k) \cap V(\ell - t_0, X_1 - t_1, \ldots, X_k - t_k) \neq \emptyset.$$

Esto implica, en particular, que el polinomio

$$\mathcal{P}_k(u, e_1, \ldots, e_k)(\ell, X_1, \ldots, X_k) \in k[X_1, \ldots, X_n]$$

se anula sobre $V_k \cup \widehat{V}_k$, es decir que $V_k \cup \widehat{V}_k \subseteq V(\mathcal{P}_k(u, e_1, \ldots, e_k)(\ell, X_1, \ldots, X_k))$.

Por lo tanto, para que valga la condición (h1) podemos definir el polinomio G_{rk} como

$$G_{rk} := \mathcal{P}_k(u, e_1, \ldots, e_k)(\ell, X_1, \ldots, X_k) \cdot$$

para una forma lineal ℓ cualquiera.

Ahora elegiremos la forma lineal ℓ de manera que valga la condición (h2).

Sea C una componente irreducible de V_r. Por la minimalidad de la descomposición equidimensional considerada se tiene que, para cada $r + 1 \leq k \leq n - 1$, C no está incluida en $V_k \cup \widehat{V}_k$.

Existe entonces un punto $\xi^C := (\xi_1^C, \ldots, \xi_n^C) \in C - (V_k \cup \widehat{V}_k)$. Consideremos la variedad cero dimensional

$$(V_k \cup \widehat{V}_k) \cap V(X_1 - \xi_1^C, \ldots, X_k - \xi_k^C).$$

Observamos que, para cada forma lineal $\ell := u_1 X_1 + \cdots + u_n X_n$ que satisface la condición

$$\ell(\xi) \neq \ell(\xi^C) \quad \text{para todo } \xi \in (V_k \cup \widehat{V}_k) \cap V(X_1 - \xi_1^C, \ldots, X_k - \xi_k^C) \tag{4.32}$$

se verifica:

$$\mathcal{P}_k(u, e_1, \ldots, e_k)(\ell(\xi^C), \xi_1^C, \ldots, \xi_k^C) \neq 0.$$

En consecuencia, C no está incluida en $V(\mathcal{P}_k(u, e_1, \ldots, e_k)(\ell, X_1, \ldots, X_k))$, puesto que la condición anterior dice que ξ^C no pertenece a esta hipersuperficie.

Luego, si se elige la forma lineal ℓ de manera que valga la condición (4.32) para un punto ξ^C de cada una de las componentes irreducibles C de V_r (simultáneamente), el polinomio

$$G_{rk} := \mathcal{P}_k(u, e_1, \ldots, e_k)(\ell, X_1, \ldots, X_k)$$

satisface el requisito (h2).

Observamos que para cada componente irreducible C de V_r, fijado $\xi^C \in C$, la condición (4.32) es una condición abierta sobre los coeficientes $u_1, \ldots, u_n$ de ℓ determinada por el polinomio $\prod_\xi(\ell(\xi) - \ell(\xi^C))$ (donde el producto recorre los puntos $\xi \in (V_k \cup \widehat{V}_k) \cap V(X_1 - \xi_1^C, \ldots, X_k - \xi_k^C)$) de grado acotado por $\deg(V_k \cup \widehat{V}_k) \leq d^{n-k}$. Como $\deg(V_r) \leq d^{n-r}$, la condición final sobre los coeficientes de la forma lineal está determinada por un polinomio de grado acotado por $d^{n-r} \cdot d^{n-k}$.

Para terminar, se resume el algoritmo probabilístico que calcula la forma de Chow Ch_{V_r} para r fijo ($0 \leq r \leq n-2$), se calcula su complejidad $\tilde{\mathcal{L}}_r$ en términos de la longitud $\mathcal{L}^{(r)}$ de un straight-line program que evalúa las formas de Chow $Ch_{V_k \cup \widehat{V}_k}$, $r \leq k \leq n-1$, y se estima su probabilidad de éxito $\tilde{P}_r$ al tomar los parámetros aleatorios de un subconjunto $\Omega \subset k$ de N elementos.

Algoritmo

Paso 1. Elegir al azar $\{u_{kj}, r+1 \leq k \leq n-1, 1 \leq j \leq n\}$ en el conjunto Ω, y considerar las formas lineales asociadas $\ell_{r+1}, \ldots, \ell_{n-1}$, definidas por

$$\ell_k := u_{k1}X_1 + \cdots + u_{kn}X_n \qquad k = r+1, \ldots, n-1.$$

La probabilidad de que estas formas lineales satisfagan la condición (4.32) para un punto ξ^C de cada una de las componentes irreducibles C de V_r y para todo $r+1 \leq k \leq n-1$, es al menos

$$\prod_{k=r+1}^{n-1}\left(1 - \frac{d^{n-r} \cdot d^{n-k}}{N}\right) \geq 1 - \frac{d^{n-r}}{N}\Big(\sum_{j=1}^{n-r-1} d^j\Big) \geq 1 - \frac{2d^{2(n-r)-1}}{N}.$$

Paso 2. Para $r+1 \leq k \leq n-1$, obtener un straight-line program que representa al polinomio $G_{rk} := \mathcal{P}_k(u, e_1, \ldots, e_k)(\ell, X_1, \ldots, X_k)$, y luego un straight-line program para $G_r := \prod_{k=r+1}^{n-1} G_{rk}$.

Esto puede hacerse en $O(n^2 + n\mathcal{L}^{(r)})$ pasos.

Paso 3. Aplicar el Lema 4.3.14 a la forma de Chow $Ch_{V_r \cup \widehat{V}_r}$ y el polinomio G_r obtenido en el paso anterior, para obtener un straight-line program que evalúa $Ch_{\widehat{V}_r}$.

Teniendo en cuenta que $\deg(V_r \cup \widehat{V}_r) \leq d^{n-r}$ y que

$$\deg G_r = \sum_{k=r+1}^{n-1} (k+1)d^{n-k} \leq 2n\,d^{n-r-1},$$

resulta que la complejidad de este paso (probabilístico) del algoritmo es de orden $(n\,d^{(n-r)})^{O(1)}\mathcal{L}^{(r)}$ y la probabilidad de calcular la forma de Chow $Ch_{\widehat{V}_r}$ es al menos

$$1 - \frac{4\,n\,(r+1)^2 d^{3(n-r)-1}}{N}.$$

Paso 4. Finalmente, aplicando el Lema 1.3.5, se calcula $Ch_{V_r} := Ch_{V_r \cup \widehat{V}_r}/Ch_{\widehat{V}_r}$.

Como $Ch_{\widehat{V}_r}(e_0, \ldots, e_r) = 1$, este paso es determinístico. La complejidad de este último paso es de orden $(n\,d^{n-r})^{O(1)}\mathcal{L}^{(r)}$.

La complejidad total del algoritmo probabilístico que calcula Ch_{V_r} a partir de las formas de Chow $Ch_{V_k \cup \widehat{V}_k}$, $r \leq k \leq n-1$ es de orden $\tilde{L}_r = (n\,d^{n-r})^{O(1)}\mathcal{L}^{(r)}$.

Teniendo en cuenta las estimaciones dadas para la complejidad de la segunda etapa del algoritmo, concluimos que $\mathcal{L}^{(r)} = (n\,d^{n-r})^{O(1)}L$ y, por lo tanto, la complejidad $\tilde{L}_r$ de este paso es también de orden $(n\,d^{n-r})^{O(1)}L$.

La probabilidad de éxito de este paso del algoritmo es

$$\begin{aligned} \tilde{P}_r &\geq \left(1 - \frac{2\,d^{2(n-r)-1}}{N}\right)\left(1 - \frac{4\,n\,(r+1)^2 d^{3(n-r)-1}}{N}\right) \\ &\geq 1 - \frac{4\,n\,(r+1)^2 d^{3(n-r)-1} + 2\,d^{2(n-r)-1}}{N}. \end{aligned}$$

La complejidad total de esta etapa final del algoritmo es $\tilde{\mathcal{L}} = \tilde{\mathcal{L}}_{n-2} + \cdots \tilde{+} \mathcal{L}_0 = (n\,d^n)^{O(1)}L$. Suponiendo que el input de esta etapa, provisto por la segunda etapa del algoritmo, son las formas de Chow de las variedades $V_r \cup \widehat{V}_r$ $(0 \leq r \leq n-1)$ se obtiene, con probabilidad mayor o igual que

$$\begin{aligned} P^{(3)} &= \prod_{r=0}^{n-2} \tilde{P}_r \geq 1 - \frac{1}{N}\left(\sum_{r=0}^{n-2} 4\,n(r+1)^2 d^{3(n-r)-1} + 2\,d^{2(n-r)-1}\right) \\ &\geq 1 - \frac{8\,n(n-1)^2 d^{3n-1} + 4\,d^{2n-1}}{N}, \end{aligned}$$

un straight-line program que representa las formas de Chow Ch_{V_r} de cada una de las componentes equidimensionales V_r $(0 \leq r \leq n-1)$ de la variedad V.

De las estimaciones hechas para la complejidad de cada una de las etapas del algoritmo, concluimos que la complejidad secuencial total del algoritmo probabilístico descripto es de orden $(n\,d^n)^{O(1)}L$.

Para cada $0 \leq r \leq n-1$, la longitud del straight-line program que (probabilísticamente) produce el algoritmo para representar la forma de Chow Ch_{V_r} de la componente equidimensional V_r de dimensión r de V es de orden $(n\,d^{n-r})^{O(1)}L$.

□

Observación 4.3.16 Supongamos dado un proceso aleatorio para seleccionar elementos de un subconjunto fijo Ω de k con N elementos, que se utiliza para elegir los parámetros aleatorios en las distintas etapas del algoritmo.

Entonces, teniendo en cuenta las probabilidades de éxito estimadas

$$\begin{aligned} P^{(1)} &\geq 1 - \frac{4(d+1)^{2n} + d^n + n^2 d^{2(n-1)}}{N} \\ P^{(2)} &\geq 1 - \frac{4\,n^2 d^{2n} + 6\,n\,d^n}{N} \\ P^{(3)} &\geq 1 - \frac{8\,n(n-1)^2 d^{3n-1} + 4d^{2n-1}}{N} \end{aligned}$$

para la preparación de los datos de entrada, el cálculo de las formas de Chow de una descomposición equidimensional no minimal y la obtención de las formas de Chow de las componentes equidimensionales a partir de las de la descomposición no minimal, respectivamente, resulta que la probabilidad de éxito del algoritmo construido es mayor o igual que

$$P := P^{(1)}\,P^{(2)}\,P^{(3)} \geq 1 - \frac{4(d+1)^{2n} + 8\,n^3 d^{3n-1}}{N}.$$

4.4 Complejidad y grado geométrico

La cota obtenida para la complejidad secuencial del algoritmo presentado en la sección anterior para el cáculo de las formas de Chow de cada una de las componentes equidimensionales de una variedad algebraica afín $V \subset \mathbb{A}^n$, depende de parámetros de carácter sintáctico: la cantidad s de polinomios input que definen la variedad V, el número de variables n, y una cota superior d para los grados de los polinomios input.

Sin embargo, la variedad V puede ser definida por distintos conjuntos de polinomios con distintos grados y propiedades, mientras que las formas de Chow calculadas dependen únicamente de la variedad.

Para evitar en parte esta dependencia de la complejidad del algoritmo en el factor d^n (número de Bézout) asociado a la familia particular de polinomios elegida para definir la variedad input, se considerará un invariante más geométrico: el *grado geométrico del sistema de polinomios*. Este parámetro está relacionado no sólo con la forma sintáctica de los polinomios, sino también con la geometría de ciertos conjuntos algebraicos –involucrados en el desarrollo del algoritmo- que define el sistema de polinomios en cuestión. Por este motivo, el grado geométrico del sistema de polinomios input de un algoritmo permite identificar instancias particulares del problema que, desde el punto de vista algorítmico, pueden resolverse mucho más fácilmente que el caso general.

4.4.1 Grado geométrico de un sistema de polinomios

La siguiente definición de grado geométrico de un sistema polinomial generaliza la presentada en [14]:

Definición 4.4.1 *Sean $f_1, \ldots, f_s$ polinomios en $k[X_1, \ldots, X_n]$. Para cada $1 \leq i \leq n$, sea $\mathcal{T}_i := (T_{i1}, \ldots, T_{is})$ un grupo de nuevas variables, y sean*

$$G_i := \sum_{j=1}^{s} T_{ij} f_j, \qquad 1 \leq i \leq n,$$

las combinaciones lineales genéricas de los polinomios $f_1, \ldots, f_s$ asociadas a los grupos de parámetros $\mathcal{T}_1, \ldots, \mathcal{T}_n$.

Se define el grado geométrico del sistema $f_1, \ldots, f_s$ *como*

$$\delta := \max\{\deg(V(G_1, \ldots, G_\ell)) \quad 1 \leq \ell \leq n\}$$

donde, para cada $1 \leq \ell \leq n$, $V(G_1, \ldots, G_\ell)$ es la variedad definida por los polinomios $G_1, \ldots, G_\ell$ en el espacio afín n-dimensional sobre una clausura algebraica de $k(T_{ij}, 1 \leq i \leq n, 1 \leq j \leq s)$.

De la desigualdad de Bézout se deduce que, si d es una cota superior para los grados de los polinomios $f_1, \ldots, f_s$, para cada $1 \leq \ell \leq n$,

$$\deg V(G_1, \ldots, G_\ell) \leq d^\ell,$$

de donde se obtiene la siguiente cota para el grado geométrico del sistema de polinomios $f_1, \ldots, f_s$:

$$\delta \leq d^n.$$

El próximo lema relaciona el grado geométrico de un sistema de polinomios $f_1, \ldots, f_s$ con los grados de ciertas variedades involucradas en el desarrollo del algoritmo presentado en la sección anterior:

Lema 4.4.2 *Sean $f_1, \ldots, f_s$ polinomios en $k[X_1, \ldots, X_n]$ y sea δ el grado geométrico del sistema $\{f_1, \ldots, f_s\}$.*
Entonces existe un abierto $\mathcal{U} \subset \mathbb{A}^{sn}$ tal que para cada $(t_1, \ldots, t_n) \in k^{sn} \cap \mathcal{U}$, si se consideran los polinomios

$$\hat{f}_i := t_{i1} f_1 + \cdots + t_{is} f_s, \qquad 1 \leq i \leq n,$$

vale

$$\max\{\deg V(\hat{f}_1, \ldots, \hat{f}_\ell) : 1 \leq \ell \leq n\} \leq \delta.$$

Demostración. Para cada $1 \leq i \leq n$, sea $\mathcal{T}_i := (T_{i1}, \ldots, T_{is})$ un grupo de s nuevas variables. Consideremos los polinomios

$$G_i := \sum_{j=1}^{s} T_{ij} f_j, \qquad 1 \leq i \leq n.$$

Por definición, el grado geométrico del sistema $f_1, \ldots, f_s$ es

$$\delta = \max\{\deg(V(G_1, \ldots, G_\ell)) \quad 1 \leq \ell \leq n\}$$

donde, para cada $1 \leq \ell \leq n$, $V(G_1, \ldots, G_\ell)$ es la variedad definida por los polinomios $G_1, \ldots, G_\ell$ en el espacio afín n-dimensional sobre una clausura algebraica de $k(T_{ij}, 1 \leq i \leq n, 1 \leq j \leq s)$.

Para cada $0 \leq r \leq n-1$, sea $Q_r \in k[\mathcal{T}_1, \ldots, \mathcal{T}_{n-r}] - \{0\}$ el polinomio dado por el Lema 4.3.7. Sea $Q := \prod_{r=0}^{n-1} Q_r \in k[\mathcal{T}_1, \ldots, \mathcal{T}_n] - \{0\}$.

Sea $t := (t_1, \ldots, t_n) \in \mathbb{A}^{sn}$ tal que $Q(t) \neq 0$.

Fijemos ℓ con $1 \leq \ell \leq n$. Sea $K = k(\mathcal{T}_1, \ldots, \mathcal{T}_\ell)$ y sea $\overline{K}$ una clausura algebraica de K.

Mostraremos que, para $(t_1, \ldots, t_\ell)$ vale

$$\deg V(G_1(t_1, X), \ldots, G_\ell(t_\ell, X)) \leq \deg V(G_1, \ldots, G_\ell)$$

donde la primera es la variedad definida por los polinomios $G_1(t_1, X), \ldots, G_\ell(t_\ell, X)$ en $\mathbb{A}^n(\bar{k})$ y la segunda, la definida por los polinomios $G_1, \ldots, G_\ell$ en $\mathbb{A}^n(\overline{K})$.

Por el Lema 4.3.6, la variedad

$$\mathcal{Z} := \overline{V(G_1, \ldots, G_\ell) - V(f_1, \ldots, f_s)} \subset \mathbb{A}^{s\ell} \times \mathbb{A}^n$$

es irreducible de dimensión $s\ell + n - \ell$ y el ideal $I(\mathcal{Z}) \subset k[\mathcal{T}_1, \ldots, \mathcal{T}_\ell, X_1, \ldots, X_n]$ es la única componente primaria $\mathcal{Q}$ de $(G_1, \ldots, G_\ell) \subset k[\mathcal{T}_1, \ldots, \mathcal{T}_\ell, X_1, \ldots, X_n]$ que satisface $V(\mathcal{Q}) \not\subset V(f_1, \ldots, f_s)$.

Sea $g \in k[X_1, \ldots, X_n]$ un polinomio tal que $V(f_1, \ldots, f_s) \subset V(g)$. Lo anterior implica que o bien $V(G_1, \ldots, G_\ell) \subset V(g)$ o bien $(G_1, \ldots, G_\ell)_g = I(\mathcal{Z})_g$ es un ideal primo de $k[\mathcal{T}_1, \ldots, \mathcal{T}_\ell, X_1, \ldots, X_n]_g$ (localización del anillo $k[\mathcal{T}_1, \ldots, \mathcal{T}_\ell, X_1, \ldots, X_n]$ en el conjunto multiplicativamente cerrado $\{g^k : k \in \mathbb{N}_0\}$).

Consideraremos $g := t_{\ell+1\,1} f_1 + \cdots + t_{\ell+1\,s} f_s$, que satisface la condición $V(f_1, \ldots, f_s) \subset V(g)$, donde $t_{\ell+1} := (t_{\ell+1\,1}, \ldots, t_{\ell+1\,s}) \in k^s$ es el $(\ell+1)$-ésimo vector en $t = (t_1, \ldots, t_n)$ si $\ell < n$, o $t_{\ell+1} \in k^s$ es tal que el polinomio g no se anula en ningún punto de $\overline{V(G_1(t_1, X), \ldots, G_n(t_n, X)) - V}$ si $\ell = n$.

Sean

$$\begin{aligned} Z^{(T)} &:= \overline{V(G_1, \ldots, G_\ell) \cap \{g \neq 0\}} \subset \mathbb{A}^n(\overline{K}) \\ Z(t) &:= \overline{V(G_1(t_1, X)), \ldots, G_\ell(t_\ell, X)) \cap \{g \neq 0\}} \subset \mathbb{A}^n(\bar{k}). \end{aligned}$$

Observamos que, si consideramos las variedades definidas por $f_1, \ldots, f_s$ en $\mathbb{A}^n(\bar{k})$ y $\mathbb{A}^n(\overline{K})$ respectivamente, y

$$\begin{aligned} V(f_1, \ldots, f_s) &= V_0 \cup V_1 \cup \ldots \cup V_{n-1} \subset \mathbb{A}^n(\bar{k}) \\ V(f_1, \ldots, f_s) &= V_0^{(T)} \cup V_1^{(T)} \cup \ldots \cup V_{n-1}^{(T)} \subset \mathbb{A}^n(\overline{K}) \end{aligned}$$

son las descomposiciones equidimensionales minimales de estas variedades, se tiene que

$$\begin{aligned} V(G_1(t_1, X), \ldots, G_\ell(t_\ell, X)) &= Z(t) \cup V_{n-\ell} \cup \ldots \cup V_{n-1} \\ V(G_1, \ldots, G_\ell) &= Z^{(T)} \cup V_{n-\ell}^{(T)} \cup \ldots \cup V_{n-1}^{(T)}. \end{aligned}$$

Además, para cada $0 \leq r \leq n-1$, vale $\deg V_r = \deg V_r^{(T)}$.

Queda por ver que $\deg Z(t) \leq \deg Z^{(T)}$.

En primer lugar, observamos que $Z^{(T)} = \emptyset$ si y sólo si $I(\mathcal{Z}) \cap k[\mathcal{T}_1, \ldots, \mathcal{T}_\ell] \neq \{0\}$ y, en el caso que $I(\mathcal{Z}) \cap k[\mathcal{T}_1, \ldots, \mathcal{T}_\ell] \neq \{0\}$, el polinomio $Q_{n-\ell}$ dado por el Lema 4.3.7 (que es un factor de Q) es un polinomio no nulo de grado acotado por $\deg \mathcal{Z}$ que pertenece a esta intersección. Por lo tanto, la condición $Q(t) \neq 0$ implica que $Q_{n-\ell}(t_1, \ldots, t_\ell) \neq 0$ y, por lo tanto, $Z(t) = \emptyset$.

Supongamos ahora que $Z^{(T)} \neq \emptyset$. Puesto que $I(\mathcal{Z}) \cap k[\mathcal{T}_1, \ldots, \mathcal{T}_\ell] = \{0\}$ y $\dim \mathcal{Z} = s\,\ell + n - \ell$, resulta que $\dim Z^{(T)} = n - \ell$.

Sean $U_i := (U_{i0}, U_{i1}, \ldots, U_{in})$ $(0 \leq i \leq n-\ell)$ grupos de $n+1$ variables asociados a las formas lineales genéricas

$$L_i := U_{i0} + U_{i1}X_1 + \cdots + U_{in}X_n \qquad 0 \leq i \leq n - \ell.$$

Notaremos $\mathcal{T} = (\mathcal{T}_1, \ldots, \mathcal{T}_\ell)$, $U = (U_0, \ldots, U_{n-\ell})$ y $X = (X_1, \ldots, X_n)$.

Sea $I = (G_1, \ldots, G_\ell, L_0, \ldots, L_{n-\ell})_g \subset k[\mathcal{T}, U, X]_g$, donde $k[\mathcal{T}, U, X]_g$ denota la localización del anillo de polinomios $k[\mathcal{T}, U, X]$ en el conjunto multiplicativamente cerrado $\{g^k : k \in \mathbb{N}_0\}$, y sea $I^{(T)} \subset K[U, X]_g$ el extendido de I.

Por el Lema 4.1.1, I es un ideal radical de $k[\mathcal{T}, U, X]_g$ (más aún, como $(G_1, \ldots, G_\ell)_g$ es primo, I también lo es) y, por lo tanto, $I^{(T)}$ también es radical.

Entonces $\mathcal{F}_{Z^{(T)}} \in K[U]$ es una forma de Chow de $Z^{(T)}$ si y sólo si

$$(\mathcal{F}_{Z^{(T)}}) = I^{(T)} \cap K[U].$$

Multiplicando por un denominador en $k[\mathcal{T}] - \{0\}$, podemos suponer que el polinomio $\mathcal{F}_{Z^{(T)}}$ pertenece a $k[\mathcal{T}, U]$ y no tiene factores en $k[\mathcal{T}]$.

Como $(G_1, \ldots, G_\ell)_g$ es un ideal primo cuya intersección con $k[\mathcal{T}]$ es $\{0\}$, resulta que el ideal primo I verifica $I \cap k[\mathcal{T}] = \{0\}$. Entonces, para $I^{(T)} \cap K[U]$, que es el extendido de $I \cap k[\mathcal{T}, U]$, vale

$$\left(I^{(T)} \cap K[U]\right) \cap k[\mathcal{T}, U] = I \cap k[\mathcal{T}, U].$$

Luego

$$(\mathcal{F}_{Z^{(T)}}) = I \cap k[\mathcal{T}, U]. \tag{4.33}$$

Por los Lemas 4.3.7 y 4.3.8, el ideal $(G_1(t_1, X), \ldots, G_\ell(t_\ell, X))_g \subset k[X]_g$ es radical y define la variedad $Z(t) \subset \mathbb{A}^n(\bar{k})$ equidimensional de dimensión $n - \ell$.

Sea $\mathcal{F}_{Z(t)} \in k[U]$ una forma de Chow de $Z(t)$. Entonces

$$(\mathcal{F}_{Z(t)}) = (G_1(t_1, X), \ldots, G_\ell(t_\ell, X), L_0, \ldots, L_{n-\ell})_g \cap k[U].$$

Ahora, de la igualdad (4.33) se deduce que $\mathcal{F}_{Z(T)} = \mathcal{F}_{Z(T)}(T, U) \in I$, de donde

$$\mathcal{F}_{Z(T)}(t) = \mathcal{F}_{Z(T)}(t, U) \in (G_1(t_1, X), \ldots, G_\ell(t_\ell, X), L_0, \ldots, L_{n-\ell})_g,$$

y por lo tanto $\mathcal{F}_{Z(T)}(t) \in (\mathcal{F}_{Z(t)})$. En consecuencia

$$\deg Z(t) = \deg_{U_i}(\mathcal{F}_{Z(t)}) \leq \deg_{U_i}(\mathcal{F}_{Z(T)}(t)) \leq \deg_{U_i}(\mathcal{F}_{Z(T)}) = \deg Z^{(T)}.$$

Esto concluye la prueba de la desigualdad

$$\deg V(G_1(t_1, X), \ldots, G_\ell(t_\ell, X)) \leq \deg V(G_1, \ldots, G_\ell) \leq \delta \tag{4.34}$$

para los vectores $t_1, \ldots, t_\ell$ que forman las primeras $s\ell$ coordenadas de un punto $t = (t_1, \ldots, t_n) \in k^{sn}$ tal que $Q(t) \neq 0$.

Puesto que la desigualdad (4.34) vale para cada $1 \leq \ell \leq n$, resulta que si $\mathcal{U} \subset \mathbb{A}^{sn}$ es el abierto definido por $\mathcal{U} := \{Q \neq 0\}$ se tiene que: para $(t_1, \ldots, t_n) \in k^{sn} \cap \mathcal{U}$ vale

$$\max\{\deg V(G_1(t_1, X), \ldots, G_\ell(t_\ell, X)) : 1 \leq \ell \leq n\} \leq \delta.$$

Con la notación del enunciado del Lema, los polinomios $\hat{f}_i = G_i(t_i, X)$ $(1 \leq i \leq n)$ verifican

$$\max\{\deg V(\hat{f}_1, \ldots, \hat{f}_\ell) : 1 \leq \ell \leq n\} \leq \delta.$$

4.4.2 Cotas de complejidad que dependen del grado geométrico

Dados $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$, el algoritmo dado en el Teorema 4.3.15 trabaja con un conjunto de $n+1$ combinaciones lineales de $f_1, \ldots, f_s$

$$\hat{f}_i := t_{i1} f_1 + \cdots + t_{is} f_s, \qquad i = 1, \ldots, n+1,$$

donde los elementos t_{ij} $(1 \leq i \leq n+1,\ 1 \leq j \leq s)$ se eligen al azar, y con subvariedades de las variedades

$$V(\hat{f}_1, \ldots, \hat{f}_{n-r}), \qquad r = n-1, \ldots, 0.$$

Las complejidades de las subrutinas utilizadas en los distintos pasos del algoritmo (ver Proposición 4.2.3, Lema 4.3.13 y Lema 4.3.14) dependen polinomialmente de la cantidad de variables n, de la longitud del straight-line program que representa los polinomios input de la subrutina, de una cota superior para el grado de estos polinomios y del grado de las variedades algebraicas involucradas. Más aún, las longitudes de los straight-line programs que producen dependen de los mismos paráinetros.

Más precisamente: Suponiendo que la preparación de los datos de entrada ha sido realizada con éxito, en la segunda etapa del algoritmo (cálculo recursivo de las formas de Chow de una descomposición no minimal) las complejidades dependen esencialmente de los grados de las variedades

$$Z_r = \overline{V(\hat{f}_1, \ldots, \hat{f}_{n-r}) \cap \{\hat{f}_{n-r+1} \neq 0\}}$$

y de los grados de las variedades $V_r \cup \widehat{V}_r$. Por otro lado, en la tercera etapa del algoritmo (cálculo de las formas de Chow de las componentes equidimensionales), las complejidades dependen de los grados de las variedades $V_r \cup \widehat{V}_r$ $(0 \leq r \leq n-2)$. Estas variedades verifican la igualdad

$$Z_{r+1} \cap V(\hat{f}_{n-r}) = Z_r \cup V_r \cup \widehat{V}_r$$

y, más aún, cada una de las variedades Z_r, V_r y $\widehat{V}_r$ es unión de componentes irreducibles de $Z_{r+1} \cap V(f_{n-r})$, de donde, para cada $0 \leq r \leq n-2$, se tiene que $\deg(V_r \cup \widehat{V}_r) \leq \deg(Z_{r+1} \cap V(\hat{f}_{n-r}))$. Finalmente, si d es una cota superior para los grados de los polinomios $f_1, \ldots, f_s$, por la desigualdad de Bézout, concluimos que $\deg(V_r \cup \widehat{V}_r) \leq d \deg(Z_{r+1})$, es decir, que el grado de las variedades $V_r \cup \widehat{V}_r$ $(0 \leq r \leq n-2)$ puede estimarse en términos de d y de los grados de las variedades Z_r $(1 \leq r \leq n-1)$.

Como consecuencia del Lema 4.4.2 deducimos que, para cada $0 \leq r \leq n-1$ vale:

$$\deg Z_r \leq \deg V(\hat{f}_1, \ldots, \hat{f}_{n-r}) \leq \delta$$

y, para cada $0 \leq r \leq n-2$,

$$\deg(V_r \cup \widehat{V}_r) \leq d \deg(Z_{r+1}) \leq d\,\delta.$$

Observamos entonces que, si se conoce de antemano el grado geométrico del sistema de polinomios que define la variedad V (input del algoritmo), el algoritmo

probabilístico dado en el Teorema 4.3.15 puede ser modificado de manera que la complejidad secuencial resulte de orden $s(n\,d\,\delta)^{O(1)}L$.

La modificación consiste esencialmente en reemplazar, para cada $0 \leq r \leq n-1$, en cada etapa en que la complejidad dependa de una cota para el grado de la variedad Z_r, la cota dada por la desigualdad de Bézout $\deg Z_r \leq d^{n-r}$ (utilizada en el caso general en que se desconoce el grado geométrico) por $\deg Z_r \leq \delta$.

Por otro lado, aunque no se conozca el grado geométrico del sistema input, la modificación anterior puede efectuarse estimando (probabilísticamente) los grados de las variedades Z_r $(0 \leq r \leq n-1)$ a partir de las resoluciones geométricas de las variedades cero-dimensionales asociadas a cada una de estas variedades obtenidas en la segunda etapa del algoritmo (para esto basta calcular el grado del polinomio minimal univariado que el algoritmo produce en cada caso). Comparando, para cada $0 \leq r \leq n-1$, el grado de Z_r calculado por el algoritmo con la cota superior d^{n-r} dada por la desigualdad de Bézout, se garantiza que la complejidad secuencial del algoritmo será, en el peor caso, de orden $s(n\,d^n)^{O(1)}L$. (En el caso en que el grado estimado para Z_r supere la cota d^{n-r}, el algoritmo finaliza su ejecución, puesto que alguna de las elecciones aleatorias anteriores debe ser errónea).

De esta manera, se obtiene que, en *cualquier caso*, si todos los parámetros aleatorios elegidos durante la ejecución del algoritmo satisfacen las condiciones de genericidad apropiadas -lo que sucederá con alta probabilidad- el algoritmo finalizará su ejecución produciendo una respuesta correcta en tiempo secuencial acotado por $s(n\,d\,\delta)^{O(1)}L$ donde δ es el grado geométrico del sistema de polinomios $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ input, d es una cota superior para los grados de estos polinomios y L es la longitud del straight-line program dado como representación de los polinomios.

Observamos también que la longitud de los straight-line programs que el algoritmo produce para las formas de Chow de cada una de las componentes equidimensionales de la variedad V será también de orden $s(n\,d\,\delta)^{O(1)}L$.

Teniendo en cuenta la estimación $\delta \leq d^n$ dada por la desigualdad de Bézout, se recuperan las cotas $s(n\,d^n)^{O(1)}L$ enunciadas en el Teorema 4.3.15 para la complejidad del algoritmo y la longitud de los straight-line programs que produce. Sin embargo, cabe destacar que en muchos casos el grado geométrico del sistema es mucho menor que d^n, dando lugar a cotas de complejidad de orden sensiblemente menor.

Una última observación con respecto a la complejidad del algoritmo: Si $G_i := \sum_{j=1}^{s} T_{ij} f_j$ son combinaciones lineales con parámetros T_{ij} $(1 \leq i \leq n,\ 1 \leq j \leq s)$ de los polinomios de entrada $f_1, \ldots, f_s$, de las observaciones anteriores y la demostración del Lema 4.4.2, se desprende que (en el caso en que todas las elecciones aleatorias sean correctas) tanto el tiempo de ejecución total del algoritmo como la longitud del straight-line program para las formas de Chow que produce, en realidad pueden estimarse en términos de los grados de las variedades

$$Z_r^{(T)} := \overline{V(G_1, \ldots, G_{n-r}) - V(f_1, \ldots, f_s)} \subset \mathbb{A}^n(\overline{k(T_{ij})}).$$

Hemos considerado sin embargo el grado geométrico δ (ver Definición 4.4.1) para medir la complejidad, puesto que este parámetro es la generalización natural de una noción que ya ha sido utilizada con éxito en diversos problemas de Geometría Algebraica efectiva.

Referencias

[1] S. J. BERKOWITZ, *On computing the determinant in small parallel time using a small number of processors,* Inform. Process. Lett. **18** (1984), 147-150.

[2] W. S. BROWN Y J. F. TRAUB, *On Euclid's algorithm and the theory of subresultants,* J. ACM **18** (1971), 505-514.

[3] L. CANIGLIA, *How to compute the Chow Form of an unmixed polynomial ideal in single exponential time,* AAECC J. (1990), 25-41.

[4] A. L. CHISTOV Y D. Y. GRIGOR'EV, *Subexponential time solving systems of algebraic equations,* LOMI preprint E-9-83, E-10-83, Steklov Institute, Leningrad (1983).

[5] G. E. COLLINS, *Subresultants and reduced polynomial remainder sequences,* J. ACM **14** (1967) 128-142. Univ. Nice–Sophia Antipolis, 1996.

[6] D. COX, J. LITTLE Y D. O'SHEA, *Using algebraic geometry,* Grad. Texts in Math. **185**, Springer–Verlag (1998).

[7] M. ELKADI Y B. MOURRAIN, *A new algorithm for the geometric decomposition of a variety,* Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (1999).

[8] D. EISENBUD, *Commutative Algebra with a view toward Algebraic Geometry,* Grad. Texts in Math. **150**, Springer–Verlag (1995).

[9] NOAÏ FITCHAS, A. GALLIGO, *Nullstellensatz effectif et conjecture de Serre (Théorème de Quillen-Suslin) pour le calcul formel,* Math. Nachr. **149** (1990), 231-253.

[10] NOAÏ FITCHAS, A. GALLIGO Y J. MORGENSTERN, *Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields,* J. Pure Appl. Algebra **67** (1990), 1-14.

[11] M. GIUSTI, K. HÄGELE, J. HEINTZ, J. L. MONTAÑA, J. E. MORAIS Y L. M. PARDO, *Lower bounds for diophantine approximation,* J. Pure Appl. Algebra **117 & 118** (1997), 277–317.

[12] M. GIUSTI Y J. HEINTZ, *Algorithmes -disons rapides- pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles,* Effective Methods in Algebraic Geometry (T. Mora, C. Traverso, Eds.), Progr. Math. **94**, Birkhäuser (1991), 169-193.

[13] M. GIUSTI Y J. HEINTZ, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial,* Computational Algebraic Geometry and Commutative Algebra, Proceedings of the Cortona Conference on Computational Algebraic Geometry and Commutative Algebra, Sympos. Math., Vol XXXIV (1993), 216-256.

[14] M. GIUSTI, J. HEINTZ, J. E. MORAIS, J. MORGENSTERN Y L. M. PARDO, *Straight line programs in geometric elimination theory,* J. Pure Appl. Algebra **124** (1998), 101-146.

[15] M. GIUSTI, J. HEINTZ Y J. SABIA, *On the efficiency of effective Nullstellensätze,* Comput. Complexity **3** (1993), 56-95.

[16] J. HARRIS, *Algebraic geometry,* Grad. Texts in Math. **133** Springer (1992).

[17] J. HEINTZ, *Definability and fast quantifier elimination in algebraically closed fields,* Theoret. Comput. Sci. **24** (1983), 239-277.

[18] J. HEINTZ, *On the computational complexity of polynomials and bilinear mappings, a survey,* L. Huguet, A. Poli (Eds.), Proc. 5th Internat. Conf. AAECC 5, Menorca, 1987, Lecture Notes in Comput. Sci. **356**, Springer (1989), 269-300.

[19] J. HEINTZ Y C. P. SCHNORR, *Testing polynomials which are easy to compute,* Monographie **30** de l'Enseignement Mathématique (1982), 237-254.

[20] J. HEINTZ Y R. WÜTHRICH, *An efficient quantifier elimination algorithm for algebraically closed fields,* SIGSAM Bull. **9** (1975), 11.

[21] G. HERMANN, *Die Frage der endilch vielen Schritte in der Theorie der Polynomideale,* Math. Ann. **95** (1926), 736-788.

[22] E. KALTOFEN, *Greatest common divisors of polynomials given by straight line programms,* J. ACM **35** No. 1 (1988), 231-264.

[23] J. KOLLÁR, *Sharp effective Nullstellensatz,* J. Amer. Math. Soc. **1** No.1 (1988), 963-975.

[24] T. KRICK Y L. M. PARDO, *A computational method for diophantine aproximation,* Progr. Math. **143** (1996), 193-253.

[25] T. KRICK, L. M. PARDO Y M. SOMBRA, *Sharp estimates for the arithmetic Nullstellensatz,* Duke Math. J. **109** No. 3 (2001), 521-598.

[26] E. KUNZ, *Introduction to commutative algebra and algebraic geometry,* Birkäuser Boston (1985).

[27] G. LECERF, *Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions,* Porceedings of the ISSAC 2000 Conference (ACM) (2000).

[28] P. PHILIPPON, *Critères pour l'indépendance algébrique,* Inst. Hautes Études Sci. Publ. Math. **64** (1986), 5-52.

[29] S. PUDDU Y J. SABIA, *An effective algorithm for quantifier elimination over algebraically closed fields using straight line programs,* J. Pure Appl. Algebra **129** (1998), 173-200.

[30] J. SABIA Y P. SOLERNÓ, *Bounds for traces in complete intersections and degrees in the Nullstellensatz,* AAECC J. **6** (1995), 353-376.

[31] J. T. SCHWARTZ, *Fast probabilistic algorithms for verification of polynomial identities,* J. ACM **27** (1980), 701-717.

[32] I. R. SHAFAREVICH, *Basic Algebraic Geometry,* Springer-Verlag (1974).

[33] V. STRASSEN, *Vermeidung von Divisionen,* Crelle J. Reine Angew. Math. **264** (1973), 184-202.