UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales

Departamento de Matemática

Sistemas de ecuaciones polinomiales ralas: aspectos teóricos y algoritmos

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

María Isabel Herrero

Director de tesis: Gabriela Talí Jeronimo

Director asistente: Juan Vicente Rafael Sabia

Consejero de estudios: Gabriela Talí Jeronimo

Buenos Aires, 2013

Sistemas de ecuaciones polinomiales ralas: aspectos teóricos y algoritmos

Resumen

Esta tesis se centra en la resolución efectiva de sistemas de ecuaciones polinomiales ralas (es decir, dadas por polinomios con estructura monomial prefijada). A lo largo del trabajo, se analizan distintos aspectos teóricos de las variedades afines definidas por estos sistemas y, en base a los resultados de este análisis, se diseñan nuevos algoritmos simbólicos probabilísticos para describirlas cuyas complejidades dependen de invariantes algebraico-combinatorios asociados al sistema.

En primer lugar, se presenta un algoritmo para el cálculo de las soluciones aisladas en $\mathbb{C}^n$ de sistemas polinomiales ralos de n ecuaciones y se prueba una cota superior genéricamente exacta para la cantidad de estas soluciones.

A continuación, se considera el problema de la descomposición equidimensional de variedades afines definidas por sistemas ralos. Para sistemas genéricos, se da una caracterización combinatoria de esta descomposición en función de la estructura de las ecuaciones y se construye un algoritmo para su cálculo. Para sistemas ralos cuadrados arbitrarios, se obtiene una cota superior para el grado de la variedad que definen, que mejora las cotas previas conocidas, y se exhibe un algoritmo que calcula conjuntos finitos de puntos representativos de cada componente equidimensional con complejidad polinomial en la cota hallada para el grado.

Finalmente, se construye un algoritmo que, dada una variedad definida por un sistema ralo genérico, calcula la clausura de Zariski de su proyección a un subespacio de coordenadas con complejidades del mismo tipo que para los problemas anteriores.

Palabras claves: Sistemas polinomiales ralos, descomposición equidimensional de variedades algebraicas, grado de variedades afines, teoría de eliminación, algoritmos y complejidad

Sparse polynomial equation systems: theoretical aspects and algorithms

Abstract

This thesis focuses on effective solving of sparse polynomial equation systems (that is, equations given by polynomials with prescribed monomial structure). Throughout this work, we analyze different theoretical aspects of the affine varieties defined by these systems and, from the results of this analysis, we design new probabilistic symbolic algorithms to describe them with complexities depending on algebraic-combinatorial invariants associated with the system.

First, we present an algorithm for the computation of the isolated solutions in $\mathbb{C}^n$ of sparse polynomial systems with n equations, and we prove a generically sharp upper bound for the number of these solutions.

Then, we consider the problem of the equidimensional decomposition of affine varieties defined by sparse systems. For generic systems, we give a combinatorial characterization of this decomposition depending on the structure of the equations, and we construct an algorithm for its computation. For arbitrary square sparse systems, we obtain an upper bound for the degree of the variety the system defines, which improves the previous known bounds, and we exhibit an algorithm that computes finite sets of representative points of each equidimensional component within a complexity which is polynomial in our bound for the degree.

Finally, we construct an algorithm that, given a variety defined by a generic sparse system, computes the Zariski closure of its projection to a coordinate subspace within a complexity depending on invariants of the same kind as in the previous problems.

Keywords: Sparse polynomial systems, equidimensional decomposition of algebraic varieties, degree of affine varieties, elimination theory, algorithms and complexity

Agradecimientos

A Juan y Gabriela, por todo todo lo que me enseñaron. Por las incontables explicaciones y la infinita paciencia. Por todo el tiempo que me dedicaron y la forma increíble en que me acompañaron. Por siete años siendo mis maestros. Por esta tesis.

A mamá por el apoyo, la ayuda incondicional. Por siempre encontrar la forma de hacer que todo sea un poquito más fácil. A ella, mi papá y mis hermanos por bancarse mis nervios y mis ausencias, por apoyar mis decisiones y creer en mí. A mi abuela que es mi símbolo de fe y mi abuelo de dedicación.

A Eli y Flor por media vida de amistad, y por estar en los momentos más difíciles. A Euge, por tratar de trasmitirme esa forma de enfrentar la vida de frente, con ganas. A Nico, por una y otra vez hacerme un lugarcito. A Xime, Meli y Mer, por esta amistad tan linda que creció rodeada de cosas ricas. A todos los otros amigos de la facu que hicieron más ameno (y me atrevo a decir menos largo?) este camino. Y a Martín, por siempre estar. Por escucharme, aconsejarme y ni una vez dejar de ser el amigo que necesitaba.

A mis profes y alumnitos que me recordaron a veces la belleza, la poesía de la matemática, y el porqué de haberla elegido. A Pablo, Joni y Magui, cuyo apoyo y cariño alguna vez significó tanto.

A la pioja, Sofi, por tu risa, tu alegría, tu vitalidad. Por llenarme de ternura y darme fe en el futuro.

Gracias.

Índice general

Introducción

Los algoritmos *generales* conocidos para resolver sistemas de ecuaciones polinomiales requieren realizar una gran cantidad de operaciones. Ésta es una de las razones por las que se intenta desarrollar procedimientos para resolver familias *particulares* de sistemas de ecuaciones polinomiales, por ejemplo, sistemas dados por polinomios con estructura fija.

Bernstein [7], Kushnirenko [50] y Khovanski [48] probaron que la cantidad de soluciones aisladas en $(\mathbb{C}^*)^n$ de un sistema polinomial de n ecuaciones está acotada superiormente por un invariante combinatorio, llamado *volumen mixto*, asociado al conjunto de soportes de los polinomios involucrados (el soporte de un polinomio es el conjunto formado por los exponentes de los monomios que aparecen con coeficientes no nulos). Este resultado es considerado la base del estudio de los sistemas polinomiales *ralos*, que son sistemas dados por polinomios con soportes preestablecidos, y dio lugar al desarrollo de la teoría de eliminación rala (ver [33]).

En esta tesis, se analizan los conjuntos de soluciones en $\mathbb{C}^n$ de sistemas polinomiales ralos en n incógnitas y se diseñan algoritmos para el tratamiento de estos sistemas con complejidades que dependen de invariantes algebraico-combinatorios asociados a los soportes de las ecuaciones. Más precisamente, se consideran tres problemas:

- Cálculo de las soluciones aisladas en $\mathbb{C}^n$ de un sistema ralo.
- Descomposición equidimensional algorítmica de variedades afines definidas por sistemas ralos en $\mathbb{C}^n$.
- Cálculo de la proyección de variedades definidas por sistemas ralos genéricos a un subespacio de coordenadas.

Los algoritmos más eficientes para resolver sistemas polinomiales ralos en $(\mathbb{C}^*)^n$, tanto numérica como simbólicamente, usan *deformaciones poliedrales* (ver, por ejemplo, [71], [42], [58], [45]). Un método de deformación para calcular los ceros aislados de un sistema polinomial consiste en considerar el sistema como una instancia particular de una familia paramétrica de sistemas genéricos cero-dimensionales para luego obtener sus ceros a partir

de las soluciones de otra instancia, suficientemente genérica, fácil de resolver. Estas técnicas, utilizadas en un principio para resolver sistemas de ecuaciones numéricamente (ver, por ejemplo, [4], [52], [65] y las referencias allí citadas), han sido aplicadas también en procedimientos simbólicos por medio del levantamiento de Newton-Hensel (ver, por ejemplo, [36], [41], [51], [44]). Las deformaciones poliedrales, además, preservan la estructura monomial del sistema de polinomios considerado, con lo cual el número de "caminos" a seguir a lo largo de la deformación coincide con el número esperado de soluciones. Para sistemas ralos, esto da lugar a menores tiempos de ejecución que los algoritmos generales.

Las primeras cotas para la cantidad de ceros aislados en $\mathbb{C}^n$ de sistemas de n ecuaciones polinomiales ralos se presentaron en [57] y fueron luego mejoradas en [54] y [59]. La cota más precisa conocida hasta el momento fue dada en [43] en función del *volumen mixto estable* que, al igual que el volumen mixto, es un invariante combinatorio que depende solamente de los soportes de los polinomios del sistema. Las demostraciones efectivas de estas cotas dieron lugar al desarrollo de algoritmos numéricos para el cálculo de ceros aislados en $\mathbb{C}^n$ (ver, por ejemplo, [54] y [43]). Un algoritmo simbólico que describe las soluciones aisladas de sistemas ralos tales que todos sus polinomios tienen término constante no nulo fue presentado en [45].

El algoritmo de [43] utiliza deformaciones poliedrales sucesivas, lo cual se refleja negativamente en la complejidad. Una mejora a este procedimiento es el algoritmo de [31] (ver también [26]), que utiliza solamente dos deformaciones poliedrales. Estos algoritmos reducen el problema a la resolución en $(\mathbb{C}^*)^n$ de una familia finita de subsistemas de ecuaciones construida a partir de una deformación particular.

En el Capítulo 2 de esta tesis, presentamos un algoritmo probabilístico simbólico que calcula los ceros aislados en $\mathbb{C}^n$ de un sistema polinomial ralo de n ecuaciones. Al igual que el procedimiento de [31], nuestro algoritmo está basado en resultados de [43] y evita también hacer deformaciones poliedrales sucesivas. Además, requiere resolver menos sistemas de ecuaciones y en menos variables que los algoritmos previos. Nuestro procedimiento extiende el resultado de [45] a sistemas con soportes arbitrarios y tiene una complejidad (salvo por un pre-procesamiento) que depende polinomialmente de volúmenes mixtos estables asociados al sistema (ver el Teorema 2.13).

El input del algoritmo es la *representación rala* de los polinomios $f_1, \ldots, f_n$ del sistema y las *celdas mixtas* de una *subdivisión mixta fina* de la familia de conjuntos obtenidos agregando el origen de coordenadas a sus soportes, que consideramos precalculadas (ver, por ejemplo, [25], [70], [53], [30] y [55] para diversos algoritmos que calculan estas celdas). El output del algoritmo es una *resolución geométrica*, es decir, una representación por medio de polinomios univariados, de un conjunto finito de puntos que contiene los ceros

aislados del sistema, donde los puntos están parametrizados por los valores que toma en ellos una forma lineal genérica (ver, por ejemplo, [37]). La idea general del algoritmo es recuperar las soluciones aisladas del sistema original haciendo una deformación homotópica a partir de las soluciones de un sistema genérico con los mismos soportes. Para hallar las soluciones aisladas del sistema genérico, adaptamos las técnicas poliedrales introducidas en [43] y refinadas en [31] con el fin de hacer un análisis detallado que nos permite determinar los subsistemas a resolver. Finalmente, aplicamos las técnicas de deformación simbólica para eliminación rala presentadas en [45].

Los resultados que determinan la correctitud de nuestro algoritmo podrían también aplicarse para diseñar un procedimiento numérico como en [43] y [31]. Si bien estos trabajos no presentan estimaciones explícitas de complejidad, nuestro enfoque permite trabajar con un número menor de sistemas cuadrados en una cantidad menor de variables lo que implicaría mejores tiempos de ejecución.

Como consecuencia del análisis teórico desarrollado, obtenemos también una nueva cota superior genéricamente exacta para la cantidad de soluciones afines aisladas contadas sin multiplicidad de un sistema ralo de n ecuaciones con n incógnitas (ver Teorema 2.19) y una caracterización de los sistemas que solo tienen finitas soluciones afines (ver la Proposición 2.23) equivalente a la dada en [59, Lemma 3], generalizando un resultado probado en [13] para sistemas binomiales.

Una vez calculadas las soluciones aisladas, el siguiente paso natural es caracterizar las componentes de dimensión positiva de la variedad afín definida por un sistema polinomial ralo teniendo en cuenta los soportes de los polinomios involucrados.

Existen diversos algoritmos simbólicos para describir la descomposición equidimensional de una variedad algebraica que solo tienen en cuenta el grado de los polinomios que la definen y no su estructura monomial. Los primeros algoritmos determinísticos que realizan esta tarea pueden hallarse en [15] y [35] (ver también [34] para un análisis del problema más general de la descomposición primaria de ideales). Posteriormente, en [24] y [46], se diseñaron algoritmos probabilísticos con menores tiempos de ejecución. Las complejidades de estos algoritmos son polinomiales en el número de Bézout del sistema, el cual genéricamente coincide con el grado de la variedad que el sistema define. En [51] y [44] se presentan otros algoritmos probabilísticos con complejidades que dependen de un invariante nuevo asociado al sistema, el *grado geométrico*, que refina la cota de Bézout. El Teorema de Schwartz-Zippel (ver [61], [73]) permite transformar algunos de estos algoritmos en determinísticos si se conocen cotas superiores para los grados de los polinomios que caracterizan las instancias excepcionales.

El problema de la descomposición equidimensional ha sido tratado también desde el pun-

to de vista numérico. A partir del algoritmo dado en [64] se fueron obteniendo mejoras sucesivas hasta llegar al algoritmo descripto en [65] basado en métodos de continuación homotópica para la descomposición de una variedad algebraica en componentes irreducibles (ver las referencias allí citadas).

Para el caso de los sistemas ralos, en el marco numérico, en [69] dan certificados para la existencia de curvas en el conjunto de soluciones. Por otro lado, en [3] y [2], se presentan métodos algorítmicos para la determinación de desarrollos en series de Puiseux para curvas y componentes de dimensión positiva arbitraria, respectivamente, de variedades definidas por sistemas ralos bajo ciertas hipótesis sobre las ecuaciones.

En el Capítulo 3 de esta tesis analizamos, tanto desde el punto de vista teórico como algorítmico, la descomposición equidimensional de variedades afines definidas por sistemas polinomiales ralos.

En primer lugar, consideramos el caso de sistemas ralos genéricos. En este contexto aparece una diferencia importante con respecto al caso de sistemas densos: el conjunto de soluciones de un sistema genérico de n polinomios en n variables con grados fijos consta solamente de puntos aislados, mientras que si se fija la familia de soportes de los n polinomios en n variables involucrados en un sistema ralo, para elecciones genéricas de los coeficientes puede haber componentes afines de dimensión positiva. Mostramos que la existencia de estas componentes de dimensión positiva para sistemas genéricos depende solamente de la estructura combinatoria de los soportes y damos condiciones que permiten encontrarlas. Estas condiciones dan una descripción teórica de la descomposición equidimensional de una variedad afín $V(P)$ definida por un sistema ralo *genérico* P en función de conjuntos de soluciones en el toro de sistemas P_I más chicos asociados a ciertos conjuntos $I \subset \{1, \ldots, n\}$. Por otra parte, nos permiten exhibir una fórmula para el grado de $V(P)$ en el caso genérico (ver el Teorema 3.8).

A continuación, usamos los resultados teóricos obtenidos para diseñar un algoritmo probabilístico simbólico que calcula la descomposición equidimensional de $V(P)$ para un sistema ralo genérico P con una complejidad que depende del grado de $V(P)$ y de invariantes combinatorios asociados a los soportes del sistema (ver el Teorema 3.20). El algoritmo calcula, en primer lugar, una familia de subconjuntos $I \subset \{1, \ldots, n\}$ que permiten encontrar las componentes de $V(P)$ y luego resuelve los sistemas polinomiales P_I asociados aplicando métodos simbólicos de deformación poliedral (ver [45] y [37]). El output del algoritmo es una lista de resoluciones geométricas que representan las componentes equidimensionales de la variedad.

El paso siguiente es considerar la descomposición equidimensional de una variedad afín definida por un sistema ralo *arbitrario*. Para desarrollar un algoritmo que resuelva este

problema es necesario analizar qué parámetros deberían estar involucrados en la complejidad del algoritmo. Un invariante natural esperado en las cotas de complejidad es el grado de la variedad que, en particular, acota superiormente la cantidad de componentes irreducibles.

En el contexto ralo, a diferencia de la cota de Bézout para polinomios densos, el grado de una variedad afín definida por un sistema genérico cuadrado *no es* una cota superior para el grado de la variedad definida por un sistema arbitrario con los mismos soportes (ver el Ejemplo 3.21). En [49], se presenta una cota para el grado de una variedad afín definida por un sistema de polinomios ralo arbitrario que depende de un volumen mixto asociado a la *unión* de los soportes (ver también [58, Theorem 1]). En esta tesis, obtenemos una cota superior más exacta para el grado de variedades definidas por sistemas ralos cuadrados, la cual también está dada en función del volumen mixto de una familia de conjuntos asociados a los soportes de las ecuaciones pero no involucra la unión (ver el Teorema 3.22).

También en el Capítulo 3 mostramos un algoritmo que, dada una variedad definida por un sistema ralo cuadrado arbitrario, calcula un conjunto de puntos representativo de cada componente equidimensional de la variedad cuya complejidad depende de la cota de grado ya mencionada (ver el Teorema 3.31). El algoritmo se basa en que, intersecando la variedad con una variedad lineal genérica de codimensión k, se consiguen puntos en todas las componentes irreducibles de dimensión k. Para controlar la complejidad, en lugar de calcular esta intersección, buscamos soluciones aisladas de un sistema auxiliar, lo que nos permite obtener un conjunto finito contenido en la variedad que contiene dicha intersección. La representación de una variedad equidimensional de dimensión positiva mediante un conjunto finito de puntos apropiado es un enfoque conocido en geometría algebraica numérica (ver la noción de *witness point superset* en [65]).

El último capítulo de esta tesis se centra en un problema clásico de cálculo de proyecciones pero en el contexto de polinomios ralos. Más precisamente, si $V \subset \mathbb{C}^n$ es una variedad afín definida por un sistema polinomial ralo genérico y, para $\ell < n$ fijo, $\pi : \mathbb{C}^n \to \mathbb{C}^\ell$ es la proyección $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_\ell)$, consideramos el problema de calcular, mediante un algoritmo simbólico, una descripción de la clausura de Zariski $\overline{\pi(V)} \subset \mathbb{C}^\ell$ con una complejidad que dependa de la estructura del sistema.

El cálculo de (la clausura de Zariski) de proyecciones lineales de variedades es una tarea básica en teoría de eliminación. Una formulación más general de este problema es la eliminación de cuantificadores algorítmica sobre cuerpos algebraicamente cerrados (ver, por ejemplo, en [67], [40], [14], [28] y [56], algoritmos cuyas complejidades dependen de la cantidad de polinomios, sus grados y el número de variables que involucran). El cálculo de formas de Chow (ver, por ejemplo, [11], [35], [44]), de resultantes clásicas (ver [19] y las

referencias allí citadas) y de resultantes ralas (ver, por ejemplo, [66], [12], [18], [47]) son casos particulares del cálculo de clausuras de Zariski de proyecciones.

En el Capítulo 4, presentamos un algoritmo probabilístico simbólico que calcula la clausura de Zariski $\overline{\pi(V(P))} \subset \mathbb{C}^\ell$ para un sistema ralo P con soportes fijos y coeficientes genéricos. Reducimos el problema al caso de variedades equidimensionales tales que todas sus componentes intersecan el toro usando la descomposición de $V(P)$ probada en el Capítulo 3. Para el caso de estas variedades, calculamos una resolución geométrica de la variedad respecto a un subconjunto adecuado de variables libres y, a partir de esta resolución geométrica, obtenemos una resolución geométrica de la clausura de Zariski de la proyección buscada. La complejidad del algoritmo es polinomial en invariantes combinatorios asociados al conjunto de los soportes de los polinomios del input (ver el Teorema 4.15).

La tesis está organizada como sigue:

En el Capítulo 1 introducimos algunas nociones preliminares, algunos resultados previos sobre sistemas de ecuaciones polinomiales ralos y los conceptos algorítmicos básicos que usamos a lo largo de la tesis. En el Capítulo 2 presentamos el algoritmo diseñado para la determinación de las soluciones afines aisladas de un sistema polinomial ralo de n ecuaciones con n incógnitas y la cota superior hallada para la cantidad de estas soluciones. El Capítulo 3 contiene los resultados obtenidos en relación a la descomposición equidimensional efectiva de variedades afines definidas por sistemas ralos: en primer lugar, presentamos nuestro algoritmo de descomposición equidimensional para sistemas genéricos y, posteriormente, tanto la cota para el grado de la variedad afín definida por un sistema ralo arbitrario de n ecuaciones con n incógnitas como el algoritmo construido para el cálculo de puntos representativos de las componentes de la variedad. En el Capítulo 4, exhibimos el algoritmo que calcula la clausura de Zariski de la proyección a un subespacio de coordenadas de la variedad definida por un sistema ralo genérico.

Capítulo 1

Preliminares

En este capítulo vamos a dar algunas definiciones, fijar notación y establecer algunos resultados básicos que serán necesarios para esta tesis.

1.1. Algunas nociones de geometría algebraica

Las definiciones y propiedades presentadas en esta sección pueden encontrarse en la bibliografía básica de geometría algebraica (ver, por ejemplo [38], [39], [16] y [23]).

1.1.1. Variedades algebraicas

Denotaremos por k un cuerpo y K un cuerpo algebraicamente cerrado, ambos de característica 0. Usaremos la notación $k^* = k\backslash\{0\}$ y $\overline{k}$ para una clausura algebraica de k.

Sean $X_1, \ldots, X_n$ indeterminadas sobre k. Un *monomio* en $X_1, \ldots, X_n$ es un producto de la forma $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$, donde los exponentes $\alpha_1, \ldots, \alpha_n$ son números enteros no negativos. El grado total de este monomio es $\alpha_1 + \cdots + \alpha_n$. Para simplificar la notación escribimos $X = (X_1, \ldots, X_n)$. Para una n-upla $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{Z}_{\geq 0})^n$ usamos la notación $X^\alpha = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$. Un *polinomio* f en $X_1, \ldots, X_n$ con coeficientes en k es una combinación lineal finita $f(X_1, \ldots, X_n) = \sum_\alpha a_\alpha X^\alpha$ de monomios con coeficientes $a_\alpha \in k$. El conjunto de todos los polinomios en $X_1, \ldots, X_n$ con coeficientes en k se nota $k[X_1, \ldots, X_n]$. Se define $\deg(f)$, el *grado total* de f, como el máximo $\alpha_1 + \cdots + \alpha_n$ sobre todos los $\alpha = (\alpha_1, \ldots, \alpha_n)$ tales que el coeficiente correspondiente a_α es no nulo. El *grado* de f en X_i se nota $\deg_{X_i}(f)$ y es el máximo α_i sobre todos los $\alpha = (\alpha_1, \ldots, \alpha_n)$ tales que el coeficiente correspondiente a_α es no nulo.

Un *sistema de ecuaciones polinomiales* es un conjunto de ecuaciones simultáneas $f_1(X) = 0, \ldots, f_m(X) = 0$, donde, para todo $1 \leq j \leq m$, $f_j \in k[X_1, \ldots, X_n]$ es un polinomio con

coeficientes en un cuerpo k. Una *solución* del sistema es un elemento $x \in \overline{k}^n$ que cumple todas las ecuaciones del sistema, es decir, tal que $f_j(x) = 0$ para todo $1 \leq j \leq m$.

Vamos a definir a continuación la noción de variedad algebraica.

Definición 1.1 *Sean $f_1, \ldots, f_m$ polinomios en $k[X_1, \ldots, X_n]$. Entonces*

$$V(f_1, \ldots, f_m) = \{x \in \overline{k}^n \mid f_j(x) = 0 \text{ para todo } 1 \leq j \leq m\}$$

es la variedad algebraica *definida por $f_1, \ldots, f_m$.*

Un conjunto $V \subset \overline{k}^n$ es una variedad algebraica (definible sobre k) si existe un conjunto finito de polinomios $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ tales que $V = V(f_1, \ldots, f_m)$.

A partir de las variedades algebraicas se puede definir una topología en $\overline{k}^n$ si consideramos como los conjuntos cerrados en $\overline{k}^n$ a todas las variedades algebraicas definibles sobre k. Esta topología se llama *topología de Zariski sobre k* (ver [23, Chapter 1, Section 6]). La *clausura de Zariski* de un conjunto $S \subset \overline{k}^n$ es la menor variedad algebraica de $\overline{k}^n$ que lo contiene, y se la nota $\overline{S}$. Además, un conjunto en $\overline{k}^n$ es *denso Zariski* si la menor variedad algebraica que lo contiene es $\overline{k}^n$. Todo abierto Zariski no vacío resulta ser denso.

Dada una familia de objetos $\{X_p\}_{p \in \overline{k}^N}$, se dice que una propiedad p vale para un elemento genérico X de $\{X_p\}_{p \in \overline{k}^N}$, o que vale *genéricamente* en $\{X_p\}_{p \in \overline{k}^N}$, si el subconjunto de puntos $p \in \overline{k}^N$ tales que el objeto X_p tiene la propiedad p contiene un abierto Zariski no vacío de $\overline{k}^N$. Por ejemplo, una propiedad vale genéricamente para puntos del espacio afín si vale para todo punto fuera de un cerrado Zariski propio.

Una variedad algebraica $V \subset \overline{k}^n$ se dice *irreducible* si cada vez que $V = W_1 \cup W_2$ con $W_1, W_2 \subset \overline{k}^n$ variedades algebraicas, entonces $W_1 = V$ o $W_2 = V$.

Toda variedad algebraica $V \subset \overline{k}^n$ puede descomponerse de manera única como una unión finita $V = \bigcup_{i=1}^{s} W_i$ de variedades algebraicas irreducibles W_i donde $W_i \nsubseteq W_j$ para todo $i \neq j$. En este caso, se dice que cada W_i es una *componente irreducible de V*.

Dado que las variedades algebraicas se definen a partir de polinomios, se les puede asociar objetos algebraicos.

Definición 1.2

- *Si S es un conjunto en $\overline{k}^n$, llamamos el* ideal de S *al ideal*

  $$I(S) = \{f \in k[X_1, \ldots, X_n] \mid f(p) = 0 \ \forall p \in S\}$$

  de los polinomios que se anulan sobre S.

- *Sea $V \subset \overline{k}^n$ una variedad algebraica. Una función $\varphi : V \longrightarrow k$ es una función polinomial si existe un polinomio $f \in k[X_1, \ldots, X_n]$ tal que $\varphi(x) = f(x)$ para todo $x \in V$. Llamamos* anillo de coordenadas *de V, y lo notamos $k[V]$, al conjunto de todas las funciones polinomiales $\varphi : V \longrightarrow k$.*

Observar que $f, g \in k[X_1, \ldots, X_n]$ representan la misma función polinomial en V si y solo si $f - g \in I(V)$. Por lo tanto, $k[V]$ se puede identificar con el anillo $k[X_1, \ldots, X_n]/I(V)$.

Una variedad algebraica V es irreducible si y solo si el ideal $I(V)$ es primo. Como consecuencia, si $V \subset \overline{k}^n$ es una variedad algebraica irreducible, el anillo de coordenadas $k[V]$ es un dominio íntegro. Entonces, puede construirse su cuerpo de fracciones, que se llama *cuerpo de funciones racionales* de V y se nota $k(V)$.

Sean $V \subset \overline{k}^m, W \subset \overline{k}^n$ dos variedades algebraicas irreducibles. Un *morfismo* $f : V \longrightarrow W$ es una aplicación tal que existen $f_1, \ldots, f_n \in k[V]$ para las cuales $f(x) = (f_1(x), \ldots, f_n(x))$ pertenece a W para todo $x \in V$. Un morfismo $f : V \longrightarrow W$ se dice *dominante* si la clausura de Zariski de $f(V)$ es W.

La *dimensión* de una variedad algebraica irreducible V es la máxima cantidad de elementos en $k(V)$ algebraicamente independientes sobre k, es decir el grado de trascendencia de $k(V)$ sobre k. Hay diferentes definiciones equivalentes para la dimensión de una variedad (ver [38, Part II, Lecture 11]). La dimensión de una variedad algebraica irreducible $V \subset \overline{k}^n$ también puede definirse como la máxima dimensión de un subespacio $H \subset \overline{k}^n$ tal que la proyección de V en H es densa Zariski. Alternativamente, la dimensión de V es el número entero $r \geq 0$ tal que para r formas lineales afines $l_1, \ldots, l_r \in k[X_1, \ldots, X_n]$ con coeficientes genéricos, la variedad algebraica $H_1 \cap \cdots \cap H_r \cap V$ es un conjunto finito y no vacío, donde $H_i = \{x \in \overline{k}^n \mid l_j(x) = 0\}$ para todo $1 \leq j \leq r$.

Para una variedad algebraica arbitraria $V \subset \overline{k}^n$, se define la dimensión de V como la máxima de las dimensiones de sus componentes irreducibles. Una variedad algebraica V se dice *equidimensional* si todas sus componentes irreducibles tienen la misma dimensión.

Sea $V \subset \overline{k}^n$ una variedad algebraica de dimensión r y, para todo $0 \leq i \leq r$, sea V_i la unión de todas las componentes irreducibles de V de dimensión i, o bien el conjunto vacío si V no tiene componentes irreducibles de dimensión i. Entonces,

$$V = \bigcup_{i=0}^{r} V_i$$

se llama la *descomposición equidimensional de V* y las variedades algebraicas $V_0, \ldots, V_r$ que no son vacías son las *componentes equidimensionales de V*.

Otro invariante asociado a una variedad algebraica que utilizaremos es su grado. La definición que vamos a usar es la de [40]:

Definición 1.3 *Si $V \subset \overline{k}^n$ es una variedad algebraica irreducible de dimensión r, se define el* grado *de V como* $\deg(V) = \max\{\#(H_1 \cap \cdots \cap H_r \cap V) \mid H_1, \ldots, H_r$ *son hiperplanos afines en $\overline{k}^n$ tales que $H_1 \cap \cdots \cap H_r \cap V$ es un conjunto finito*$\}$.

Si $V \subset \overline{k}^n$ es una variedad algebraica arbitraria, el grado de V es la suma de los grados de todas las componentes irreducibles de V.

Por [40, Proposition 1], la cantidad de puntos en la intersección de V con $r = \dim(V)$ hiperplanos afines en $\overline{k}^n$ es genéricamente finita y, en los casos en los que es finita, está acotada superiormente. Entonces, el grado de una variedad irreducible es un número entero no negativo. Más aún, genéricamente la cantidad de puntos en la intersección es exactamente el grado de la variedad.

1.1.2. Resoluciones geométricas

Una manera de describir variedades algebraicas equidimensionales ampliamente usada en álgebra computacional simbólica es mediante resoluciones geométricas. Éstas son descripciones paramétricas de la variedad. Una reseña de sus usos en el contexto algorítmico puede encontrarse en [37].

Para variedades algebraicas cero-dimensionales, el Shape Lemma (ver, por ejemplo, [22, Section 6.5.4]) es un resultado clásico que nos asegura que podemos describirlas mediante resoluciones geométricas definidas de la siguiente manera:

Sea $V = \{\xi^{(1)}, \ldots, \xi^{(D)}\}$ una variedad algebraica cero-dimensional definible sobre k. Una forma lineal afín $\mu \in k[X_1, \ldots, X_n]$ se llama *forma lineal separante o elemento primitivo* para V si $\mu(\xi^{(i)}) \neq \mu(\xi^{(j)})$ cuando $i \neq j$. Notar que una forma lineal afín con coeficientes genéricos es separante para V.

Definición 1.4 *Sea $V = \{\xi^{(1)}, \ldots, \xi^{(D)}\} \subset \overline{k}^n$ una variedad algebraica cero-dimensional. Dada una forma lineal $\mu \in k[X_1, \ldots, X_n]$ separante para V, la familia de polinomios $(q, v_1, \ldots, v_n) \in (k[U])^{n+1}$ (con U una nueva variable), donde*

- $q = \prod_{i=1}^{D} (U - \mu(\xi^{(i)})) \in k[U]$ *es el polinomio minimal de la forma lineal μ respecto de V, y*
- *los polinomios $v_1, \ldots, v_n \in k[U]$ son tales que $\deg(v_j) < D$ para todo $1 \leq j \leq n$ y cumplen $V = \{(\frac{v_1}{q'}(\eta), \ldots, \frac{v_n}{q'}(\eta)) \in \overline{k}^n \mid \eta \in \overline{k}, q(\eta) = 0\}$, donde $q'(U) = \frac{\partial q}{\partial U}(U)$,*

se llama resolución geométrica de V respecto a μ.

Para una forma lineal separante fija μ, la resolución geométrica de V respecto a μ es única y caracteriza completamente la variedad V.

Como el polinomio q' es inversible en $k[U]/\langle q(U)\rangle$, tomando

$$\overline{v}_j(U) = (q')^{-1}(U)v_j(U) \text{ (mód } q(U)) \text{ para todo } 1 \leq j \leq n,$$

obtenemos una definición equivalente de resolución geométrica. Ésta es una familia de polinomios $(q, \overline{v}_1, \ldots, \overline{v}_n)$ en $k[U]$, donde q es el polinomio minimal de la forma lineal μ respecto de V de la definición anterior, que cumplen $V = \{(\overline{v_1}(\eta), \ldots, \overline{v_n}(\eta)) \in \overline{k}^n \mid \eta \in \overline{k}, q(\eta) = 0\}$ y $\deg(\overline{v}_j) < D$ para todo $1 \leq j \leq n$. A lo largo de esta tesis usaremos ambas definiciones indistintamente.

Dadas finitas variedades cero-dimensionales en $\overline{k}^n$ disjuntas y una forma lineal μ separante para la unión de todas ellas, podemos hallar una resolución geométrica de la unión respecto a μ a partir de resoluciones geométricas respecto a μ de cada una de las variedades originales: Sean $V = \{\xi^{(1)}, \ldots, \xi^{(D)}\}$ y $\widetilde{V} = \{\xi^{(D+1)}, \ldots, \xi^{(D+\widetilde{D})}\}$ dos variedades en $\overline{k}^n$. Sean $(q, v_1, \ldots, v_n)$ la resolución geométrica de V y $(\widetilde{q}, \widetilde{v}_1, \ldots, \widetilde{v}_n)$ la resolución geométrica de $\widetilde{V}$. Como estas variedades son disjuntas, q y $\widetilde{q}$ son coprimos. Entonces $(q\tilde{q}, v_1\tilde{q} + \tilde{v}_1 q, \ldots, v_n\tilde{q} + \tilde{v}_n q)$ es una resolución geométrica de $V \cup \widetilde{V}$ respecto a μ pues

- Como μ es separante para $V \cup \widetilde{V}$, $q\widetilde{q} = \prod_{i=1}^{D+\widetilde{D}} (U - \mu(\xi^{(i)})) \in k[U]$ es el polinomio minimal de la forma lineal μ respecto de $V \cup \widetilde{V}$.
- Para todo $1 \leq j \leq n$, el polinomio $v_j\widetilde{q} + \widetilde{v}_j q$ tiene grado menor a $D + \widetilde{D}$. Además, si $\overline{\eta}$ es un cero de $q\widetilde{q}$, existe $1 \leq i \leq D + \widetilde{D}$ tal que $\overline{\eta} = \mu(\xi^{(i)})$. Supongamos sin pérdida de generalidad que $\overline{\eta}$ es un cero de q. Entonces $\dfrac{v_j\widetilde{q} + \widetilde{v}_j q}{q'\widetilde{q} + q\widetilde{q}'}(\overline{\eta}) = \dfrac{v_j}{q'}(\overline{\eta}) = \xi_j^{(i)}$. En consecuencia $V \cup \widetilde{V} = \{(\frac{v_1\widetilde{q}+\widetilde{v}_1 q}{q'\widetilde{q}+q\widetilde{q}'}(\eta), \ldots, \frac{v_n\widetilde{q}+\widetilde{v}_n q}{q'\widetilde{q}+q\widetilde{q}'}(\eta)) \in \overline{k}^n \mid \eta \in \overline{k},\ q\widetilde{q}(\eta) = 0\}$.

Se puede extender la idea de resolución geométrica a variedades algebraicas equidimensionales de la siguiente manera:

Sea $V \subset \overline{k}^n$ una variedad equidimensional de dimensión r. Mediante un cambio lineal de variables podemos suponer que para cada componente irreducible W de V vale $I(W) \cap k[X_1, \ldots, X_r] = \{0\}$. Entonces, $k(X_1, \ldots, X_r) \otimes k[V]$ es un $k(X_1, \ldots, X_r)$-espacio vectorial de dimensión finita. Sea δ la dimensión de $k(X_1, \ldots, X_r) \otimes k[V]$. Una forma lineal $\mu = \mu_{r+1}X_{r+1} + \cdots + \mu_n X_n$ no nula se llama *elemento primitivo* de la variedad algebraica V si $\{1, \mu, \ldots, \mu^{\delta-1}\}$ es una base de $k(X_1, \ldots, X_r) \otimes k[V]$ como $k(X_1, \ldots, X_r)$-espacio vectorial. Una forma lineal genérica en $k[X_{r+1}, \ldots, X_n]$ es un elemento primitivo de V.

Para $\mu \in k[X_{r+1}, \ldots, X_n]$ un elemento primitivo de V, llamamos resolución geométrica de V respecto a μ a la familia de polinomios $(q, v_{r+1}, \ldots, v_n) \in (k[X_1, \ldots, X_r][U])^{n-r+1}$, donde

- $q \in k[X_1, \ldots, X_r][U]$ es un múltiplo (por un factor en $k[X_1, \ldots, X_r]$) del polinomio minimal del endomorfismo de multiplicar por la forma lineal μ en $k(X_1, \ldots, X_r) \otimes k[V]$ sin factores no constantes en $k[X_1, \ldots, X_r]$ (es único salvo un factor en k),
- los polinomios $v_{r+1}, \ldots, v_n \in k[X_1, \ldots, X_r][U]$ son tales que $\deg_U(v_j) < \deg_U(q)$ para todo $r+1 \leq j \leq n$ y cumplen $\frac{\partial q}{\partial U}(\mu)\, X_j = v_j(\mu)$ en $k(X_1, \ldots, X_r) \otimes k[V]$.

1.2. Aspectos algorítmicos

Un algoritmo es un procedimiento que, a partir de un conjunto finito de datos iniciales, llamado *input*, y realizando una cantidad finita de operaciones sucesivas, devuelve un *output*, el conjunto finito de datos buscado. En nuestros algoritmos, cada una de las operaciones es una operación aritmética o una comparación entre elementos de $\mathbb{Q}$.

Como trabajamos con polinomios en varias variables con coeficientes en $\mathbb{Q}$, necesitamos una forma de codificarlos mediante un conjunto finito de datos. Utilizamos tres maneras diferentes de codificar polinomios:

- *Codificación densa*: Es la codificación usual, que presenta el polinomio a codificar a través de un vector de todos sus coeficientes. Esto es, conociendo la cantidad n de variables involucradas y una cota d para el grado del polinomio, damos un orden al conjunto de todos los monomios de grado menor o igual a d en n variables y la codificación densa del polinomio es el vector con todos los coeficientes del polinomio (incluyendo los nulos) en ese orden.
- *Codificación rala*: Mediante la lista de pares ordenados (α, a_α) donde consideramos todos los exponentes α de los monomios en un conjunto prefijado que contiene todos los exponentes de los monomios que aparecen con coeficiente no nulo en el polinomio.
- *Codificación como straight-line program* (slp): Es la representación mediante una secuencia finita de funciones racionales $\beta = (Q_1, \ldots, Q_m) \in \mathbb{Q}(X_1, \ldots, X_n)^m$ que permiten evaluar el polinomio codificado en todos los puntos con coordenadas racionales de un abierto Zariski no vacío. Para todo $1 \leq i \leq m$, $Q_i \in \mathbb{Q} \cup \{X_1, \ldots, X_n\}$ o bien existen $1 \leq i_1, i_2 < i$ y una operación aritmética $* \in \{+, -, \times, \div\}$ tales que $Q_i = Q_{i_1} * Q_{i_2}$. La *longitud* del straight-line program es la cantidad total de operaciones aritméticas llevadas a cabo durante el proceso de evaluación de esta codificación (ver [10] para una definición más precisa y propiedades de esta forma de codificación).

A lo largo de esta tesis vamos a usar la codificación densa solo para polinomios en una variable.

La noción de *complejidad* de algoritmos que consideraremos es el número de operaciones y comparaciones en $\mathbb{Q}$ que el algoritmo realiza.

En nuestros cálculos de complejidad usamos la siguiente notación:

- Sean $\varphi, \psi : \mathbb{Z}_{\geq 0} \longrightarrow \mathbb{R}$. Escribimos $\varphi(d) = O(\psi(d))$ si existe una constante c positiva tal que $|\varphi(d)| \leq c|\psi(d)|$ para todo $d \in \mathbb{Z}_{\geq 0}$.
- Ω es el exponente en la complejidad $O(d^{\Omega})$ de la multiplicación de dos matrices en $k^{d\times d}$. Se sabe que $\Omega < 2,376$ (ver [32, Chapter 12], [8, Chapter 2, Section 2]).
- $\overline{\Omega}$ es el exponente en $O(d^{\overline{\Omega}})$, que cuenta la cantidad de operaciones en un anillo conmutativo R necesarias para calcular el determinante de una matriz en $R^{d\times d}$. Se sabe que $\overline{\Omega}$ es estrictamente menor a 4 (ver [6]).
- $M(d) = d\log^2(d)\log(\log(d))$ donde log es el logaritmo en base 2.

La evaluación de un polinomio en una variable de grado d con coeficientes en un anillo R de característica cero en tantos puntos como su grado o su interpolación puede llevarse a cabo con $O(M(d))$ operaciones. La multiplicación o división con resto de dos polinomios de grado d puede hacerse con $O(\frac{M(d)}{\log(d)})$ operaciones en R (ver [32, Chapter 10]).

La inversión de una matriz en $k^{d\times d}$ puede realizarse con $O(d^{\Omega})$ operaciones. Sobre un anillo conmutativo, el cálculo de la adjunta y el polinomio característico de una matriz puede hacerse con $O(d^{\overline{\Omega}})$ operaciones (ver [32] y [6]).

Los algoritmos que presentamos en esta tesis son probabilísticos. Esto es, hacen elecciones al azar de puntos que, siempre y cuando estén fuera de un cerrado Zariski propio, permitirán llegar a un resultado correcto. El Teorema de Scwhartz-Zippel (ver [61, 73]) asegura que, eligiendo los valores de las coordenadas de estos puntos al azar en un conjunto suficientemente grande de números enteros, la probabilidad de error puede controlarse. El tamaño de dicho conjunto de números enteros depende del grado de los polinomios que definen el cerrado Zariski fuera del cual se los quiere elegir. Más precisamente:

Teorema 1.5 *(Schwartz-Zippel) Sea $\mathbf{S} \subset \mathbb{Z}$ un conjunto finito. Sea $f \in \mathbb{Q}[X_1, \ldots, X_n]\backslash\{0\}$ un polinomio de grado total d. Entonces, para una elección al azar de elementos $p_1, \ldots, p_n \in \mathbf{S}$, la probabilidad de que $f(p_1, \ldots, p_n) = 0$ es menor o igual que $\dfrac{d}{|\,\mathbf{S}\,|}$.*

A lo largo de toda esta tesis no consideraremos el costo de elegir valores al azar, ya que éste se considera despreciable respecto a los demás costos involucrados. Tampoco haremos estimaciones de la probabilidad de error de los algoritmos. Fijada la probabilidad de error que se desea, el cálculo del tamaño del conjunto de números enteros donde se eligen valores al azar para lograrla puede llevarse a cabo acotando los grados de los polinomios que definen los abiertos Zariski de los puntos que conducen a resultados correctos (ver, por ejemplo, [45]).

1.3. Sistemas de ecuaciones polinomiales ralas

Nuestro objeto de estudio a lo largo de toda esta tesis son los conjuntos de soluciones de sistemas polinomiales, pero no de sistemas arbitrarios sino tales que el conjunto de monomios que aparece en los polinomios que lo conforman está fijado previamente. En este sentido hablamos de polinomios ralos.

La noción de polinomio puede generalizarse tomando las n-uplas de exponentes en $\mathbb{Z}^n$. Un *monomio de Laurent* en $X_1, \ldots, X_n$ es un producto de la forma $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$, donde los exponentes $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$. El grado total de este monomio de Laurent es $\alpha_1 + \cdots + \alpha_n$. Un *polinomio de Laurent* f en $X_1, \ldots, X_n$ con coeficientes en k es una combinación lineal finita de monomios de Laurent con coeficientes en k. El conjunto de todos los polinomios de Laurent en $X_1, \ldots, X_n$ con coeficientes en k se nota $k[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$.

Definición 1.6 *Sean $\mathcal{S}$ un subconjunto finito de $\mathbb{Z}^n$ y $X_1, \ldots, X_n$ variables sobre k. Un polinomio de Laurent* ralo f con soporte $\mathcal{S}$ *es una combinación lineal finita, con coeficientes en k^*, de monomios cuyos exponentes pertenecen a S.*

Sea $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ una familia de subconjuntos finitos de $\mathbb{Z}^n$. Un sistema de polinomios de Laurent ralos *con soportes $\mathcal{A}$ es de la forma $F = (f_1, \ldots, f_m)$ tal que f_j es un polinomio de Laurent ralo con soporte $\mathcal{A}_j$ para todo $1 \leq j \leq m$.*

Vamos a precisar la noción de genericidad para sistemas ralos. Esto es un caso particular de la definición de la Sección 1.1. Para ello, dado un conjunto finito de exponentes $\mathcal{S} \subset \mathbb{Z}^n$, notamos $\mathcal{L}(\mathcal{S}) = \{ \sum_{\alpha \in \mathcal{S}} a_\alpha X^\alpha \mid a_\alpha \in k \text{ para todo } \alpha \in \mathcal{S}\}$ el conjunto de los polinomios de Laurent en $k[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ tales que todos sus monomios tienen exponentes en $\mathcal{S}$.

Definición 1.7 *Sean $\mathcal{A}_1, \ldots, \mathcal{A}_m \subset \mathbb{Z}^n$ subconjuntos finitos. Una propiedad se dice que vale* genéricamente *para polinomios de Laurent $(f_1, \ldots, f_m) \in \mathcal{L}(\mathcal{A}_1) \times \cdots \times \mathcal{L}(\mathcal{A}_m)$ si existe un polinomio no nulo* p *en los coeficientes de $f_1, \ldots, f_m$ tal que la propiedad se cumple para todos aquellos $f_1, \ldots, f_m$ cuyos coeficientes no anulan a* p.

1.3.1. Sistemas ralos y polítopos

Cuando los conjuntos de soportes están prefijados, algunas propiedades de los sistemas de ecuaciones dependen de su estructura geométrico-combinatoria. Para las definiciones que siguen y algunas propiedades básicas, ver [17].

Dado $\mathcal{S} \subset \mathbb{R}^n$, notamos $Conv(\mathcal{S})$ a su cápsula convexa. Un *polítopo* en $\mathbb{R}^n$ es la cápsula convexa de un conjunto finito en $\mathbb{R}^n$. Un *polítopo entero* es aquél que se puede definir a partir de un conjunto finito que está en $\mathbb{Z}^n$. A lo largo de esta tesis trabajamos solamente con polítopos enteros, y nos referiremos a ellos como polítopos.

Sea $\mathbf{P}$ un polítopo en $\mathbb{R}^n$. La *dimensión de* $\mathbf{P}$ es la dimensión del menor subespacio afín que contiene a $\mathbf{P}$. Para $\eta \in \mathbb{Q}^n \backslash \{0\}$, se llama la *cara* de $\mathbf{P}$ determinada por η a

$$\mathbf{P}_\eta = \mathbf{P} \cap \{p \in \mathbb{R}^n \mid \langle p, \eta \rangle = \min_{x \in \mathbf{P}} \langle x, \eta \rangle\}.$$

A η se la llama una *normal interior* de la cara $\mathbf{P}_\eta$ de $\mathbf{P}$. A las normales $\eta \in \mathbb{Z}^n$ tales que el máximo común divisor de sus coordenadas es 1 las llamamos *primitivas*.

Las caras de un polítopo son a su vez polítopos. Las caras de dimensión $n-1$ de un polítopo $\mathbf{P} \subset \mathbb{R}^n$ de dimensión n se llaman facetas. A diferencia de las caras de dimensión menor, las facetas tienen una única (salvo por un factor en $\mathbb{Q}$) normal interior.

A la cápsula convexa del soporte de un polinomio de Laurent f se la llama el *polítopo de Newton* de f.

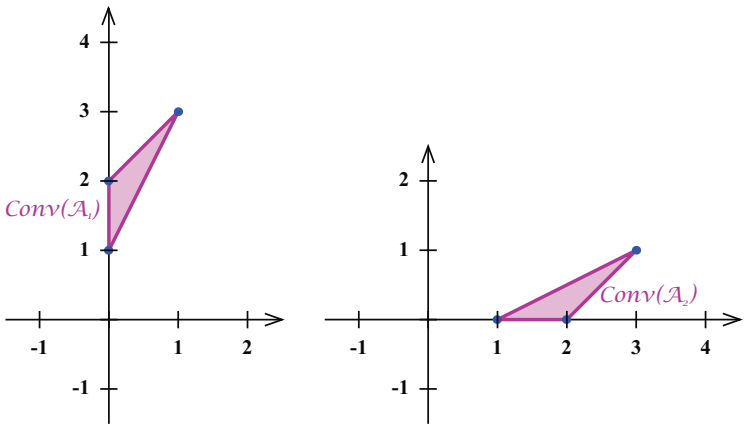
Ejemplo 1.8 El sistema $F = (f_1, f_2)$ de polinomios en $\mathbb{Q}[X_1, X_2]$, donde

$$f_1(X_1, X_2) = X_2 + 2X_2^2 - X_1X_2^3 \qquad \text{y} \qquad f_2(X_1, X_2) = -X_1 + 3X_1^2 - 2X_1^3X_2,$$

es un sistema ralo con soportes

$$\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2), \quad \text{con} \quad \mathcal{A}_1 = \{(0,1), (0,2), (1,3)\}, \ \mathcal{A}_2 = \{(1,0), (2,0), (3,1)\}$$

y polítopos de Newton



Sean $\mathbf{P}, \mathbf{Q} \subset \mathbb{R}^n$ polítopos. Se define la *suma de Minkowski de* $\mathbf{P}$ *y* $\mathbf{Q}$ como el polítopo $\mathbf{P} + \mathbf{Q} = \{p + q \mid p \in \mathbf{P}, q \in \mathbf{Q}\}$. Además, para $\lambda \in \mathbb{R}_{\geq 0}$ se define el polítopo $\lambda.\mathbf{P}$ (no necesariamente entero) como $\lambda.\mathbf{P} = \{\lambda.p \mid p \in \mathbf{P}\}$.

Una noción importante es la de volumen mixto, que introducimos a continuación:

Definición 1.9 *Sea $\mathcal{V}ol_n$ el volumen euclideano en $\mathbb{R}^n$. Dados $\mathcal{A}_1, \ldots, \mathcal{A}_n \subseteq \mathbb{Z}^n$ conjuntos finitos, se define el* volumen mixto (de Minkowski) *de $(\mathcal{A}_1, \ldots, \mathcal{A}_n)$ como*

$$\mathcal{MV}_n(\mathcal{A}_1, \ldots, \mathcal{A}_n) = \sum_{k=1}^{n} (-1)^{n-k} \sum_{\substack{\mathrm{J} \subset \{1,\ldots,n\} \\ \#\mathrm{J} = k}} \mathcal{V}ol_n(\sum_{j \in \mathrm{J}} Conv(\mathcal{A}_j)).$$

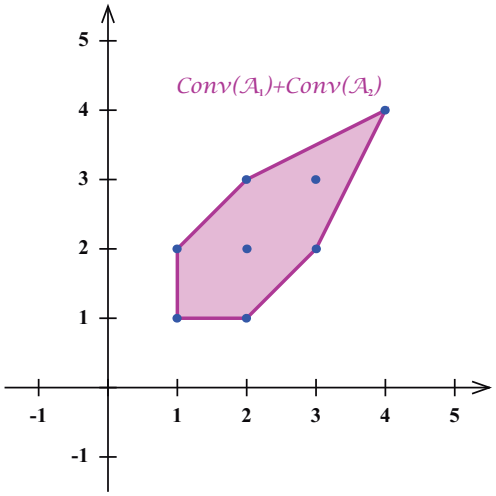
Para una familia $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ de conjuntos finitos en $\mathbb{Z}^n$ vamos a notar $\mathcal{MV}_n(\mathcal{A})$ al volumen mixto $\mathcal{MV}_n(\mathcal{A}_1, \ldots, \mathcal{A}_n)$.

El volumen mixto de $\mathcal{A}$ también puede definirse de la siguiente forma: Si consideramos el polinomio homogéneo

$$P_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\lambda_1, \ldots, \lambda_n) = \mathcal{V}ol_n(\lambda_1 Conv(\mathcal{A}_1) + \cdots + \lambda_n Conv(\mathcal{A}_n))$$

en las variables $\lambda_1, \lambda_2, \ldots, \lambda_n$, el volumen mixto de $(\mathcal{A}_1, \ldots, \mathcal{A}_n)$ es el coeficiente correspondiente al monomio $\lambda_1 \lambda_2 \ldots \lambda_n$ en el desarrollo del polinomio $P_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(\lambda_1, \ldots, \lambda_n)$ (ver [17, Chapter 7]).

Ejemplo 1.10 Volviendo al Ejemplo 1.8, la suma de los polítopos de Newton de f_1 y f_2 es



El volumen mixto de $\mathcal{A}$ es

$$\mathcal{MV}_2(\mathcal{A}) = \mathcal{V}ol_2(Conv(\mathcal{A}_1) + Conv(\mathcal{A}_2)) - \mathcal{V}ol_2(Conv(\mathcal{A}_1)) - \mathcal{V}ol_2(Conv(\mathcal{A}_2)) = 3.$$

Haremos uso del siguiente resultado referente al volumen mixto (ver [9] y [63, Lemma 6]).

Proposición 1.11 *Sean $\mathbf{P}_1, \ldots, \mathbf{P}_k$ polítopos en $\mathbb{R}^{n+k}$ y $\mathbf{Q}_1, \ldots, \mathbf{Q}_n$ polítopos en $\mathbb{R}^n \subset \mathbb{R}^{n+k}$. Entonces*

$$\mathcal{MV}_{n+k}(\mathbf{Q}_1, \ldots, \mathbf{Q}_n, \mathbf{P}_1, \ldots, \mathbf{P}_k) = \mathcal{MV}_n(\mathbf{Q}_1, \ldots, \mathbf{Q}_n)\mathcal{MV}_k(\pi(\mathbf{P}_1), \ldots, \pi(\mathbf{P}_k))$$

donde $\pi : \mathbb{R}^{n+k} \longrightarrow \mathbb{R}^k$ es la proyección a las últimas k coordenadas.

En [27, Chapter IV, Theorem 4.13]) puede encontrarse un resultado equivalente a la siguiente proposición:

Proposición 1.12 *Sea $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ una familia de conjuntos finitos en $\mathbb{Z}^n$. Entonces, el volumen mixto $\mathcal{MV}_n(\mathcal{A})$ es positivo si y solo si para todo $J \subset \{1, \ldots, n\}$ vale que* $\dim(\sum_{j \in J} \mathcal{A}_j) \geq \#J$.

El Teorema de Bernstein es la base del estudio de sistemas polinomiales ralos y da una cota (conocida como la cota BKK por los trabajos de Bernstein [7], Kushnirenko [50] y Khovanskii [48]) para la cantidad de ceros aislados en $(\mathbb{C}^*)^n$ de un sistema de n polinomios de Laurent con coeficientes en $\mathbb{C}$. Esta cota es exacta para elecciones genéricas de los coeficientes de los polinomios del sistema. Más aún, el Teorema de Bernstein da las condiciones de genericidad bajo las cuales esa cota se alcanza, que están expresadas en función de ciertos sistemas asociados.

Definición 1.13 *Sean $\eta = (\eta_1, \ldots, \eta_n) \in \mathbb{Q}^n \backslash \{0\}$, $\mathcal{S} \subset \mathbb{Z}^n$ un conjunto finito, y notemos $\mathcal{S}_\eta = \{\beta \in \mathcal{S} \mid \langle \eta, \beta \rangle = \min_{\alpha \in \mathcal{S}} \langle \eta, \alpha \rangle\}$. Si $f(X) = \sum_{\alpha \in \mathcal{S}} a_\alpha X^\alpha$ es un polinomio en n variables con soporte $\mathcal{S}$, definimos*

$$f_\eta(X) = \sum_{\beta \in \mathcal{S}_\eta} a_\beta X^\beta$$

y, para un sistema de polinomios $F = (f_1, \ldots, f_m)$, notamos $F_\eta = (f_{1\eta}, \ldots, f_{m\eta})$.

Ya podemos enunciar del Teorema de Bernstein:

Teorema 1.14 *([7, Theorems A & B]) Sea $F = (f_1, \ldots, f_n)$ un sistema de n polinomios de Laurent en n variables con coeficientes en $\mathbb{C}$ y soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $\mathbb{Z}^n$. La cantidad de ceros aislados del sistema F en $(\mathbb{C}^*)^n$ contados con su multiplicidad está acotada superiormente por $\mathcal{MV}_n(\mathcal{A})$. Más aún:*

- *Si F_η no tiene raíces en $(\mathbb{C}^*)^n$ para todo $\eta \in \mathbb{Q}^n\backslash\{0\}$, todas las raíces de F en $(\mathbb{C}^*)^n$ son aisladas y la cota se alcanza.*
- *Si F_η tiene alguna raíz en $(\mathbb{C}^*)^n$ para algún $\eta \in \mathbb{Q}^n\backslash\{0\}$, la cota es estrictamente mayor que la cantidad de raíces aisladas del sistema F en $(\mathbb{C}^*)^n$ si $\mathcal{MV}_n(\mathcal{A}) > 0$, o bien el sistema F no tiene ceros aislados en $(\mathbb{C}^*)^n$ si $\mathcal{MV}_n(\mathcal{A}) = 0$.*

Este resultado vale, más generalmente, sobre un cuerpo K algebraicamente cerrado arbitrario de característica cero (ver [21] y [68, Theorem 3.1]).

1.3.2. Subdivisiones y funciones de levantamiento

A continuación vamos a introducir el concepto de subdivisión mixta, que fue definido en [42] para hallar soluciones aisladas en $(\mathbb{C}^*)^n$ de sistemas ralos y permite calcular volúmenes mixtos.

Definición 1.15 *Sea $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ una familia de subconjuntos finitos de $\mathbb{Z}^n$ tal que la cápsula convexa de su unión tiene dimensión n. Una* celda *de $\mathcal{A}$ es una n-upla $C = (C_1, \ldots, C_n)$ de subconjuntos no vacíos $C_j \subset \mathcal{A}_j$ para todo $1 \leq j \leq n$.*

La cápsula convexa de una celda *C se define como $Conv(C) = Conv(C_1 + \cdots + C_n)$, y el* tipo *de una celda como tipo$(C) = (\dim(Conv(C_1)), \ldots, \dim(Conv(C_n)))$. Una* cara *de C es una subcelda $\widetilde{C} = (\widetilde{C}_1, \ldots, \widetilde{C}_n)$ tal que existe algún $\eta \in \mathbb{Q}^n\backslash\{0\}$ tal que para todo $1 \leq j \leq n$, $\widetilde{C}_j = C_j \cap \{p \in \mathbb{Z}^n \mid \langle p, \eta\rangle = \min_{x \in C_j}\langle x, \eta\rangle\}$.*
Una subdivisión *de $\mathcal{A}$ es una colección de celdas $S = (C^{(1)}, \ldots, C^{(r)})$ tal que*

i) $\dim(Conv(C^{(i)})) = n$ *para todo* $1 \leq i \leq r$.

ii) $Conv(C^{(i)}) \cap Conv(C^{(l)})$ *es una cara de* $C^{(i)}$ *y de* $C^{(l)}$ *para todo* $1 \leq i, l \leq r$.

iii) $\bigcup_{i=1}^{r} Conv(C^{(i)}) = Conv(\mathcal{A})$.

Decimos que una subdivisión S es mixta fina *si además cumple que*

iv) $\sum_{j=1}^{n} \dim(Conv(C_j^{(i)})) = n$ *para toda celda* $C^{(i)} \in S$.

v) $\sum_{j=1}^{n} (\#C_j^{(i)} - 1) = n$ *para toda celda* $C^{(i)} \in S$.

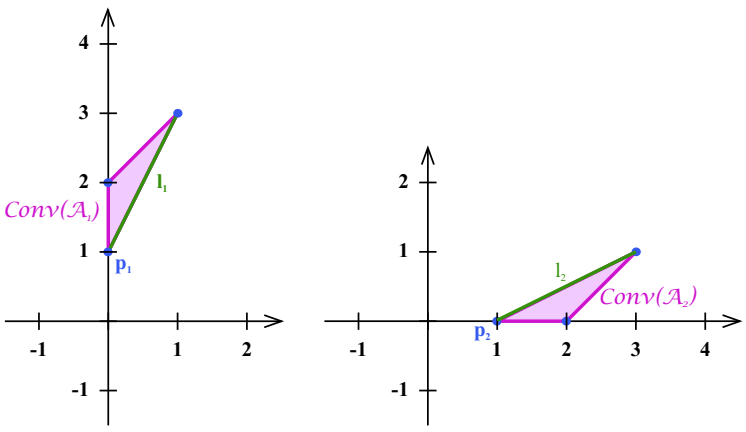
El volumen mixto $\mathcal{MV}_n(\mathcal{A})$ puede calcularse como la suma de los volúmenes mixtos de todas las celdas de tipo $(1, \ldots, 1)$ (también llamadas *celdas mixtas*) de una subdivisión mixta fina de $\mathcal{A}$ (ver [42]). Una subdivisión mixta fina puede encontrarse mediante un proceso de levantamiento genérico:

Definición 1.16 *Dada una familia de soportes* $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ *en* $\mathbb{Z}^n$*, sean funciones* $\omega_j : \mathcal{A}_j \longrightarrow \mathbb{R}$ *para todo* $1 \leq j \leq n$*. La* n*-upla* $\omega = (\omega_1, \ldots, \omega_n)$ *se llama* función de levantamiento *de* $\mathcal{A}$*. Se nota* $\mathcal{A}(\omega) = (\mathcal{A}_1(\omega_1), \ldots, \mathcal{A}_n(\omega_n))$*, donde* $\mathcal{A}_j(\omega_j)$ *es el gráfico de* ω_j *en* $\mathbb{R}^{n+1}$ *para todo* $1 \leq j \leq n$*.*

Para los resultados y algoritmos que presentamos en los capítulos posteriores, usaremos funciones de levantamiento $\omega = (\omega_1, \ldots, \omega_n)$ tales que $\omega_j : \mathcal{A}_j \longrightarrow \mathbb{Z}_{\geq 0}$ para todo $1 \leq j \leq n$.

Sea $\mathbf{P} \subset \mathbb{R}^{n+1}$ el polítopo obtenido tomando la suma de Minkowski de las cápsulas convexas de $\mathcal{A}_j(\omega_j)$ para todo $1 \leq j \leq n$. Notar que $\mathbf{P} = Conv(\mathcal{A}(\omega))$. Se define una subdivisión $S_\omega(\mathcal{A})$ de $\mathcal{A}$ a partir de la proyección a sus primeras n coordenadas de las facetas inferiores de $\mathbf{P}$, esto es, las caras de $\mathbf{P}$ de dimensión n y normal interior con última coordenada positiva: Toda faceta inferior $\mathbf{F}$ de $\mathbf{P}$ es una suma $\mathbf{F} = \mathbf{F}_1 + \cdots + \mathbf{F}_n$, donde $\mathbf{F}_j$ es una cara inferior de $Conv(\mathcal{A}_j(\omega_j))$. Si $\pi : \mathbb{R}^{n+1} \longrightarrow \mathbb{R}^n$ es la proyección a las primeras n coordenadas, entonces el conjunto de las n-uplas $(\pi(\mathbf{F}_1) \cap \mathcal{A}_1, \ldots, \pi(\mathbf{F}_n) \cap \mathcal{A}_n)$ tales que $\mathbf{F}_1 + \cdots + \mathbf{F}_n$ es una faceta inferior de $\mathbf{P}$ es una subdivisión de $\mathcal{A}$, que notamos $S_\omega(\mathcal{A})$. En este caso decimos que $S_\omega(\mathcal{A})$ es la subdivisión de $\mathcal{A}$ *inducida por* ω. Diremos que η es una normal asociada a la celda $C = (C_1, \ldots, C_n)$ de $S_\omega(\mathcal{A})$ si es una normal interior de la faceta inferior $\mathbf{F}$ de $\mathbf{P}$ tal que $C_j = \pi(\mathbf{F}_j) \cap \mathcal{A}_j$ para todo $1 \leq j \leq n$. Para una función de levantamiento ω genérica, la subdivisión inducida $S_\omega(\mathcal{A})$ resulta ser mixta fina.

Ejemplo 1.17 Sea $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ la familia de subconjuntos finitos de $\mathbb{Z}^2$ tal que $\mathcal{A}_1 = \{(0,1), (0,2), (1,3)\}$ y $\mathcal{A}_2 = \{(1,0), (2,0), (3,1)\}$ (ver el Ejemplo 1.8). Sus cápsulas convexas son:

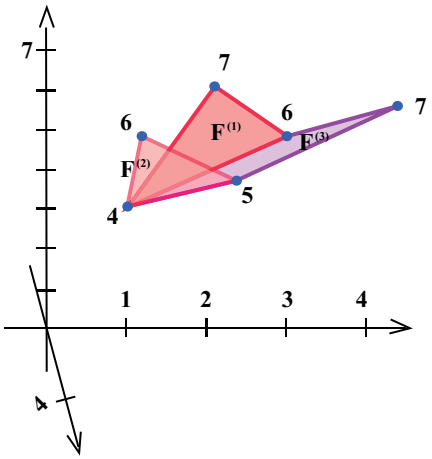


Sea $\omega = (\omega_1, \omega_2)$ la función de levantamiento de $\mathcal{A}$:

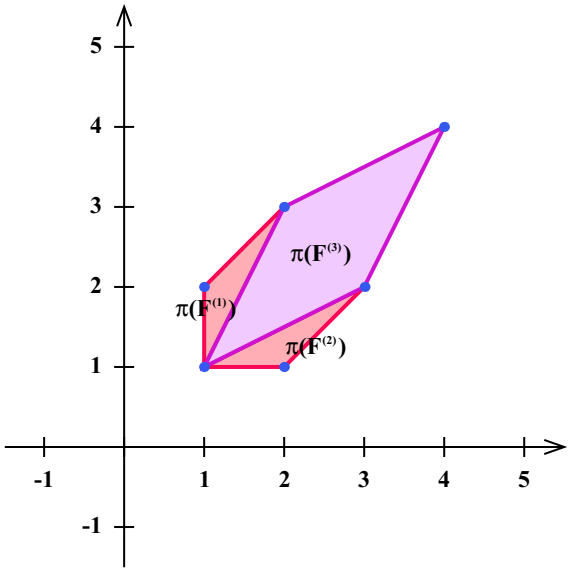
- $\omega_1(0,1) = 3$, $\omega_1(0,2) = 6$ y $\omega_1(1,3) = 5$.

- $\omega_2(1,0) = 1,\ \omega_2(2,0) = 3$ y $\omega_2(3,1) = 2$.

Las facetas inferiores de $Conv(\mathcal{A}(\omega))$ son:



Al proyectar las facetas inferiores de $Conv(\mathcal{A}(\omega))$ a sus primeras 2 coordenadas obtenemos:



donde $\pi(\mathbf{F}^{(1)}) = Conv(\mathcal{A}_1) + \{\mathbf{p}_2\}$, $\pi(\mathbf{F}^{(2)}) = \{\mathbf{p}_1\} + Conv(\mathcal{A}_2)$ y $\pi(\mathbf{F}^{(3)}) = l_1 + l_2$ con l_1 el segmento de extremos $(0,1)$ y $(1,3)$, y l_2 el de extremos $(1,0)$ y $(3,1)$.

Entonces, la subdivisión mixta fina de $\mathcal{A}$ inducida por ω es $S_\omega(\mathcal{A}) = (C^{(1)}, C^{(2)}, C^{(3)})$ donde $C^{(1)} = (\mathcal{A}_1, \{(1,0)\})$, $C^{(2)} = (\{(0,1)\}, \mathcal{A}_2)$ y $C^{(3)} = (\{(0,1),(1,3)\}, \{(1,0),(3,1)\})$.

Podemos observar que la única celda mixta es $C^{(3)}$ ($\dim(l_1) = \dim(l_2) = 1$). En particular, esto implica que $\mathcal{MV}_2(\mathcal{A}) = \mathcal{MV}_2(C^{(3)}) = 3$.

Como existe una biyección entre cada faceta $\mathbf{F}$ inferior de $Conv(\mathcal{A}(\omega))$ y la celda C de $S_\omega(\mathcal{A})$ que genera, en los gráficos para facilitar la notación nos referiremos a $\pi(\mathbf{F})$ como C.

Existen algoritmos para hallar las celdas mixtas de una subdivisión usando programación lineal. En [25] presentan un algoritmo usando esta técnica cuya complejidad, bajo ciertas hipótesis, es a lo sumo del orden de $(\text{máx}_i \#\mathcal{A}_i)^{O(n)}$. Pueden encontrarse algunas mejoras en [53] y [30]. Una alternativa por programación dinámica fue presentada en [70]. El algoritmo más eficiente que conocemos para el cálculo de celdas mixtas es el de [55]. En nuestros algoritmos, consideraremos el cálculo de las celdas mixtas un proceso previo y, por la falta de cálculos precisos y explícitos de su complejidad, no incluiremos el costo de ese pre-procesamiento en nuestras estimaciones de complejidad.

Con el mismo espíritu que en la Definición 1.13 podemos definir, dado un sistema F y una celda C de una subdivisión de su familia de soportes, un subsistema asociado a F y a C:

Definición 1.18 *Sean $F = (f_1, \ldots, f_n)$ un sistema de polinomios de Laurent con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $\mathbb{Z}^n$ donde $f_j(X) = \sum_{\alpha \in \mathcal{A}_j} a_{j\alpha} X^\alpha$ para todo $1 \leq j \leq n$, ω una función de levantamiento de $\mathcal{A}$ y $C = (C_1, \ldots, C_n)$ una celda de $S_\omega(\mathcal{A})$. Definimos*

$$F_C = (f_{1C}, \ldots, f_{nC}) \text{ donde } f_{jC}(X) = \sum_{\alpha \in C_j} a_{j,\alpha} X^\alpha.$$

Notar que, si η es la normal asociada a C, entonces los sistemas F_η (ver la Definición 1.13) y F_C son iguales.

1.3.3. Soluciones afines

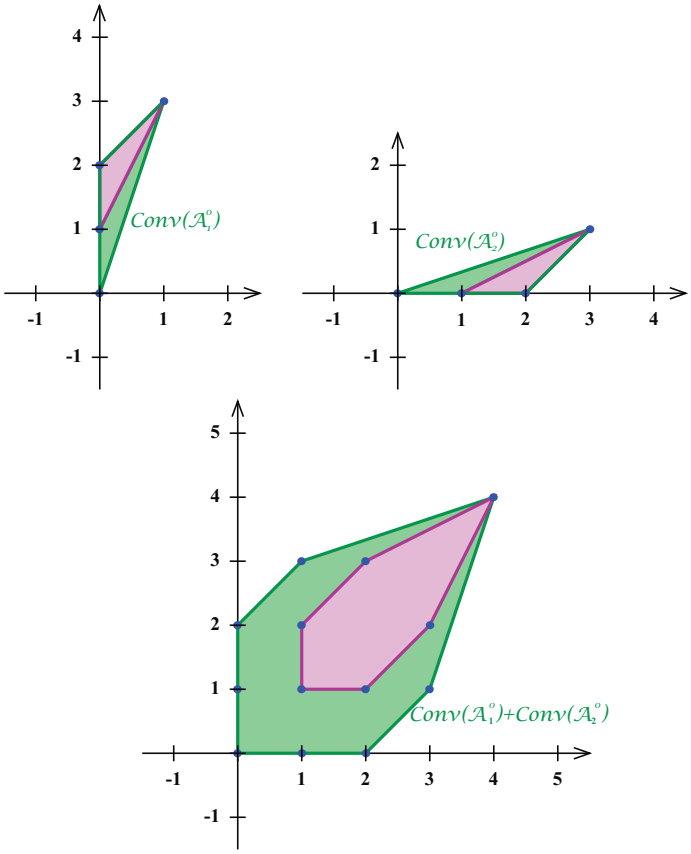
En [43] los autores extendieron los resultados de [42] sobre ceros aislados de sistemas ralos en $(\mathbb{C}^*)^n$ al caso de ceros aislados afines. Presentamos a continuación los conceptos allí introducidos.

Para una familia $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ de conjuntos finitos en $(\mathbb{Z}_{\geq 0})^n$, se define la función de levantamiento $\omega^0 = (\omega_1^0, \ldots, \omega_n^0)$ de la siguiente manera: Para todo $1 \leq j \leq n$ sean $\mathcal{A}_j^0 = \mathcal{A}_j \cup \{0\}$ y $\omega_j^0 : \mathcal{A}_j^0 \longrightarrow \mathbb{R}$ dada por

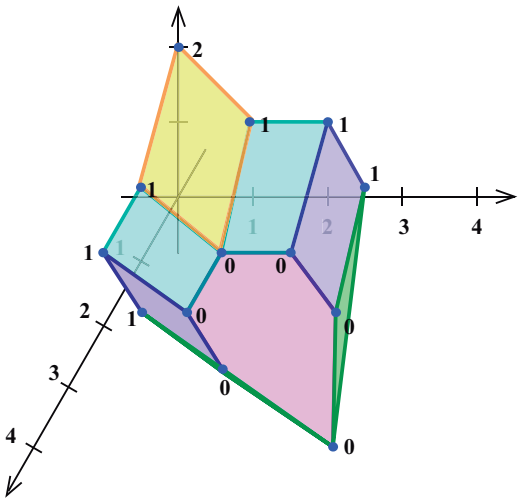
$$\omega_j^0(\alpha) = 0 \text{ para todo } \alpha \in \mathcal{A}_j \text{ y } \omega_j^0(0) = 1 \text{ si } 0 \notin \mathcal{A}_j.$$

Este levantamiento induce una subdivisión de $\mathcal{A}^0 = (\mathcal{A}_1^0, \ldots, \mathcal{A}_n^0)$ que en general no es mixta fina.

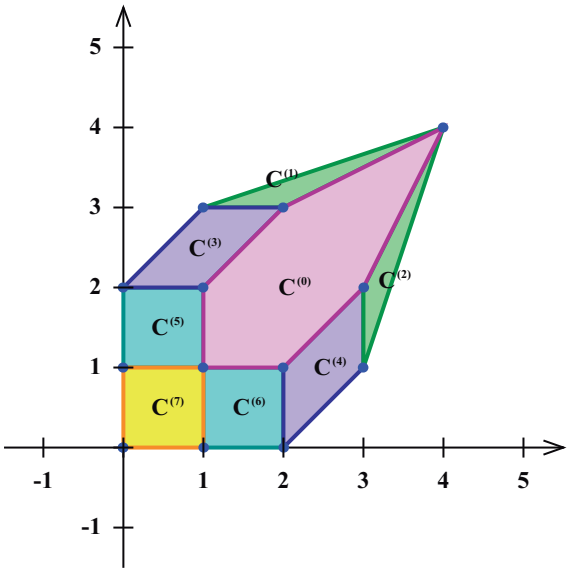
Ejemplo 1.19 Para el Ejemplo 1.8 (ver [43, Example 3]), la familia $\mathcal{A}^0 = (\mathcal{A}_1^0, \mathcal{A}_2^0)$ y la suma de sus cápsulas convexas son:



Usando el levantamiento ω^0, las facetas del "piso" (de normal interior con última coordenada positiva) de $Conv(\mathcal{A}^0(\omega^0))$ son:



A partir de esas facetas y proyectando a sus primeras 2 coordenadas, se consigue la siguiente subdivisión $S_{\omega^0}(\mathcal{A}^0)$ de $Conv(\mathcal{A}^0)$:



Utilizando la subdivisión de $\mathcal{A}^0$ inducida por la función de levantamiento ω^0, en [43] los autores introdujeron la noción de volumen mixto estable que damos a continuación:

Definición 1.20 *El* volumen mixto estable *de $\mathcal{A}$, denotado $\mathcal{SM}(\mathcal{A})$, es la suma de los volúmenes mixtos de todas las celdas en $S_{\omega^0}(\mathcal{A}^0)$ definidas a partir de facetas de $Conv(\mathcal{A}^0(\omega^0))$ cuya normal interior tiene todas sus coordenadas no negativas.*

A partir de esta noción, en [43] se presenta una cota para la cantidad de ceros aislados en $\mathbb{C}^n$ de un sistema ralo de n ecuaciones en n variables que generaliza el resultado del Teorema de Bernstein (Teorema 1.14). Para ello, se prueba una versión más general del siguiente resultado, que en el contexto en el que vamos a trabajar establece:

Teorema 1.21 *([43, Theorem 2]) Sea $F = (f_1, \ldots, f_n)$ un sistema de n polinomios ralos en n variables, con coeficientes en $\mathbb{C}$ y soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$. La cantidad de ceros aislados de F en $\mathbb{C}^n$ está acotada superiormente por el volumen mixto estable $\mathcal{SM}(\mathcal{A})$. La cota es genéricamente exacta para familias de soportes tales que para coeficientes genéricos, el sistema correspondiente tiene solo finitas soluciones en $\mathbb{C}^n$.*

Ejemplo 1.22 El Teorema 1.21 nos dice que la cantidad ceros aislados en $\mathbb{C}^2$ del sistema $F := \begin{cases} f_1(X_1, X_2) = X_2 + 2X_2^2 - X_1X_2^3 \\ f_2(X_1, X_2) = -X_1 + 3X_1^2 - 2X_1^3X_2 \end{cases}$ del Ejemplo 1.8 está acotada superiormente por $\mathcal{SM}(\mathcal{A})$, es decir, la suma de los volúmenes mixtos correspondientes a las celdas $C^{(0)}, C^{(5)}, C^{(6)}$ y $C^{(7)}$ de la subdivisión del Ejemplo 1.19, es decir por 6.

1.4. Series formales

1.4.1. Series y parametrización de curvas

Presentaremos aquí algunas definiciones y resultados básicos sobre series formales y series de Puiseux (para más detalles ver [72, Chapter 4] y [1, Lectures 11, 12 & 14]).

Definición 1.23 *Llamaremos* conjunto de las series de potencias formales sobre k, *y lo notaremos* $k[\![T]\!]$, *al conjunto de todas las combinaciones lineales (no necesariamente finitas) de potencias de* T *de la forma* $p(T) = \sum_{n=0}^{\infty} a_n T^n$, *donde* $a_n \in k$ *para todo* $n \in \mathbb{Z}_{\geq 0}$.

El conjunto de series de potencias formales con las operaciones usuales es un dominio íntegro. Su cuerpo de fracciones se nota $k(\!(T)\!)$. Todo $p \in k(\!(T)\!)$ puede escribirse en forma única como $p(T) = T^h \sum_{n=0}^{\infty} a_n T^n$ donde $h \in \mathbb{Z}$ y $a_0 \neq 0$. Se llama a h el *orden* de p y se nota $\mathrm{ord}(p)$.

La definición de series de potencias formales puede extenderse a series con exponentes racionales.

Definición 1.24 *Llamaremos* cuerpo de series de potencias racionales sobre k *o* series de Puiseux *al conjunto* $k\{\{T\}\} = \bigcup_{n \in \mathbb{N}} k(\!(T^{\frac{1}{n}})\!)$.

Los elementos de $k\{\{T\}\}$ son de la forma $p(T) = T^{\frac{h}{n}} \sum_{j=0}^{\infty} a_j T^{\frac{j}{n}}$ con $h \in \mathbb{Z}$, $n \in \mathbb{N}$, $a_j \in k$ para todo $j \in \mathbb{Z}_{\geq 0}$ y $a_0 \neq 0$.

Teorema 1.25 *(Newton-Puiseux, ver [1, Lecture 12], [72, Chapter 4, Theorem 3.1]) Si* K *es un cuerpo algebraicamente cerrado, el cuerpo de las series de Puiseux* $K\{\{T\}\}$ *es algebraicamente cerrado.*

Sea $F \in K[X_1, X_2]$ un polinomio no constante y $\mathcal{C} = \{(x_1, x_2) \in K^2 \mid F(x_1, x_2) = 0\}$ una curva plana. Una *parametrización* de $\mathcal{C}$ en un punto (a, b) de $\mathcal{C}$ está dada por $\lambda_1(T), \lambda_2(T) \in K[\![T]\!]$ tales que

$$(\lambda_1(0), \lambda_2(0)) = (a, b) \text{ y } F(\lambda_1(T), \lambda_2(T)) = 0.$$

Una parametrización $(\lambda_1(T), \lambda_2(T))$ de $\mathcal{C}$ en (a, b) se dice *irredundante* si no existe una parametrización $(\lambda_1'(T), \lambda_2'(T))$ de $\mathcal{C}$ tal que $(\lambda_1(T), \lambda_2(T)) = (\lambda_1'(\sigma(T)), \lambda_2'(\sigma(T)))$ para algún $\sigma \in K[\![T]\!]$ tal que $\mathrm{ord}(\sigma) > 1$. Notar que si una parametrización de $\mathcal{C}$ en (a, b) es irredundante, entonces no puede ser constante. Dos parametrizaciones $(\lambda_1(T), \lambda_2(T))$ y

$(\lambda_1'(T), \lambda_2'(T))$ de $\mathcal{C}$ en (a,b) se dicen *equivalentes* si $(\lambda_1(T), \lambda_2(T)) = (\lambda_1'(\sigma(T)), \lambda_2'(\sigma(T)))$ para algún $\sigma \in K[\![T]\!]$ tal que $\mathrm{ord}(\sigma) = 1$. Una *rama* de $\mathcal{C}$ en (a,b) es una clase de equivalencia de parametrizaciones irredundantes de $\mathcal{C}$ en (a,b). En un sistema de coordenadas adecuado, toda parametrización es equivalente a una de la forma $(T^n, \lambda_2(T))$ con $n \in \mathbb{N}$, $\lambda_2(T) \in K[\![T]\!]$ y $\mathrm{ord}(\lambda_2) > 0$.

Teorema 1.26 *(ver [72, Chapter 4, Theorem 2.3]) Dado un punto $(a,b) \in K^2$ de una curva plana $\mathcal{C}$, existe al menos un rama de $\mathcal{C}$ en (a,b).*

1.4.2. Levantamiento de Newton-Hensel

Una herramienta ampliamente utilizada en cálculo simbólico es el procedimiento de levantamiento de Newton-Hensel.

Sean $T_1, \ldots, T_m, X_1, \ldots, X_n$ indeterminadas sobre k, y, para $t \in \overline{k}^m$, notemos $T - t = (T_1 - t_1, \ldots, T_m - t_m)$. Sea $F = (f_1, \ldots, f_n)$ un sistema de polinomios en $k[T, X]$. Notemos DF a su matriz Jacobiana respecto a X y JF al determinante de DF.

Lema 1.27 *([41, Lemma 3]) Con las hipótesis y notación anteriores, sea $(t, \xi) \in \overline{k}^m \times \overline{k}^n$ tal que*

$$f_1(t,\xi) = \cdots = f_n(t,\xi) = 0 \text{ y } JF(t,\xi) \neq 0.$$

Entonces, existe una única familia de series de potencias formales $\mathcal{R} = (\mathcal{R}_1, \ldots, \mathcal{R}_n) \in \overline{k}[[T-t]]^n$ tal que

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

El método de levantamiento de Newton-Hensel nos da una manera constructiva de aproximar el vector $\mathcal{R}$ de series de potencias formales: Al sistema F se le asocia el operador de Newton

$$N_F(X)^t = X^t - DF(X)^{-1} F(X)^t,$$

y se define la sucesión

- $\mathcal{R}^{(0)} = \xi$,
- $\mathcal{R}^{(l)} = N_F(\mathcal{R}^{(l-1)})$ para todo $l \geq 1$.

En [41, Lemma 3] se prueba que $\mathcal{R}_i^{(l)} - \mathcal{R}_i^{(l-1)}$ y $f_j(T, \mathcal{R}^{(l-1)})$ pertenecen al ideal $\langle T_1 - t_1, \ldots, T_n - t_n \rangle^{2^{l-1}} \subset \overline{k}[[T-t]]$ para todo $1 \leq i, j \leq n$ y $l \in \mathbb{N}$. Entonces la sucesión $(\mathcal{R}^{(l)})_{l \in \mathbb{N}_0}$ converge y el límite es una familia de series formales $\mathcal{R} = (\mathcal{R}_1, \ldots, \mathcal{R}_n)$ que cumple las condiciones del Lema 1.27 (ver [37] para otra versión algorítmica de este resultado).

1.4.3. Aproximación de Padé

Una aproximación de Padé es la mejor aproximación de una serie a través de funciones racionales de grado dado. La idea es la siguiente:

Sea $g \in k[\![T]\!]$ una serie de potencias formales. Sean $\tau, \varsigma \in \mathbb{N}$ tales que $\tau \geq \varsigma$. Una $(\varsigma, \tau-\varsigma)$-*aproximación de Padé* para g es una función racional $\frac{\mathrm{p}}{\mathrm{q}} \in k(T)$, con $\mathrm{p}, \mathrm{q} \in k[T]$ que cumplen

$$\frac{\mathrm{p}}{\mathrm{q}} \equiv g \ (\text{mód } T^{\tau}),$$

donde $\deg(\mathrm{p}) < \varsigma$, $\deg(\mathrm{q}) \leq \tau - \varsigma$ y $\mathrm{q}(0) \neq 0$.

Por ejemplo, para todo $\tau \in \mathbb{N}$, si p es el polinomio de Taylor de orden τ alrededor del 0 de g y $\mathrm{q} = 1$, entonces $\frac{\mathrm{p}}{\mathrm{q}}$ es una $(\tau+1, 0)$-aproximación de Padé de g.

Una forma de obtener aproximaciones de Padé es por medio del algoritmo de Euclides extendido. Sean $f, g \in k[T]$ polinomios univariados. El algoritmo de Euclides extendido (ver [32, Chapter 3, Section 2, Algorithm 3.6]) calcula polinomios $r_i, s_i, t_i \in k[T]$ con $0 \leq i \leq l+1$ y $q_i \in k[T]$ con $1 \leq i \leq l$ tales que $\{r_i\}_{i=0}^{l+1}$ son los restos y $\{q_i\}_{i=1}^{l}$ los cocientes del algoritmo de Euclides clásico, y

- $r_0 = f, r_1 = g$, $r_{i-2} = q_{i-1} r_{i-1} + r_i$ para todo $2 \leq i \leq l+1$, donde l es el mínimo tal que $r_{l+1} = 0$,
- $s_0 = 1, s_1 = 0$ y $s_i = s_{i-2} - q_{i-1} s_{i-1}$ para todo $2 \leq i \leq l+1$,
- $t_0 = 0, t_1 = 1$ y $t_i = t_{i-2} - q_{i-1} t_{i-1}$ para todo $2 \leq i \leq l+1$,

cumplen que $s_i f + t_i g = r_i$ para todo $0 \leq i \leq l+1$.

Lema 1.28 *(Ver [32, Chapter 5, Section 9, Corollary 5.21]) Sean $\tau \in \mathbb{N}$ y $\varsigma \in \{0, \ldots, \tau\}$. Sean $g \in k[T]$ un polinomio de grado menor a τ y $r_j, s_j, t_j \in k[T]$ los polinomios del algoritmo de Euclides extendido aplicado a T^{τ} y g, con j minimal tal que $\deg(r_j) < \varsigma$. Entonces:*

1. *$\mathrm{p} := r_j$ y $\mathrm{q} := t_j$ cumplen que $\mathrm{p} \equiv \mathrm{q} g \ (\text{mód } T^{\tau})$ con $\deg(\mathrm{p}) < \varsigma$ y $\deg(\mathrm{q}) \leq \tau - \varsigma$. Además, si $\gcd(r_j, t_j) = 1$ entonces $\frac{\mathrm{p}}{\mathrm{q}}$ es una $(\varsigma, \tau-\varsigma)$-aproximación de Padé de g.*
2. *Si $\frac{\mathrm{p}}{\mathrm{q}} \in k(T)$ es una $(\varsigma, \tau-\varsigma)$-aproximación de Padé de g con q mónico y $\gcd(\mathrm{p}, \mathrm{q}) = 1$, y $c \in k \backslash \{0\}$ es el coeficiente principal de t_j, vale que $\mathrm{p} = c^{-1} r_j$ y $\mathrm{q} = c^{-1} t_j$. En particular, existe una $(\varsigma, \tau-\varsigma)$-aproximación de Padé de g si y sólo si $\gcd(r_j, t_j) = 1$, y en ese caso es única (salvo por una constante en $k \backslash \{0\}$).*

De esta forma, sea $\frac{\mathrm{p}}{\mathrm{q}} \in k(T)$ una función racional en una variable con coeficientes en k tal que $\deg(\mathrm{p}) < \varsigma$, $\deg(\mathrm{q}) \leq \tau - \varsigma$ y $\mathrm{q}(0) \neq 0$. Sea $\mathcal{P}$ el polinomio de Taylor de orden $\tau - 1$ de $\frac{\mathrm{p}}{\mathrm{q}}$. Entonces, usando el lema anterior para T^τ y $\mathcal{P}$ podemos recuperar el numerador y denominador de $\frac{\mathrm{p}}{\mathrm{q}}$ hallando su $(\varsigma, \tau - \varsigma)$-aproximación de Padé.

Esta aproximación de Padé puede hallarse utilizando *subresultantes* (ver [32, Corollary 6.48]). La idea es, para todo $l = 0, \ldots, \varsigma - 1$, calcular el determinante de la matriz subresultante $S_l \in k^{(2\tau-2l-1)\times(2\tau-2l-1)}$ de T^τ y $\mathcal{P}$. Por [32, Corollary 6.49], el máximo l para el cual el determinante de S_l es no nulo es exactamente $l = \deg(r_j)$, con j minimal tal que $\deg(r_j) < \varsigma$ (ver el Lema 1.28). Buscando la solución del sistema lineal $S_l(s^{(j)}_{\tau-l-2}, \ldots, s^{(j)}_0, t^{(j)}_{\tau-l-1}, \ldots, t^{(j)}_0)^t = (0, \ldots, 0, 1)^t$, se obtienen los coeficientes de los polinomios $s_j(T) = \sum_{i=0}^{\tau-l-2} s^{(j)}_i T^i$, $t_j(T) = \sum_{i=0}^{\tau-l-1} t^{(j)}_i T^i$ y, finalmente, $r_j(T) = s_j(T)T^\tau + t_j(T)\mathcal{P}(T)$. Así obtenemos el numerador y el denominador (salvo por un factor constante en $k\backslash\{0\}$).

La complejidad de este algoritmo, donde los cálculos de determinantes se llevan a cabo sin hacer divisiones, es del orden de $O(\tau^{\overline{\Omega}+1})$. Para estimar esta complejidad observamos que se calculan a lo sumo $\varsigma \leq \tau$ subresultantes de matrices de tamaño a los sumo $2\tau - 1$ con $O(\tau^{\overline{\Omega}})$ operaciones cada una, y luego se resuelve un sistema lineal cuadrado de tamaño a lo sumo $2\tau - 1$.

Usaremos aproximaciones de Padé para recuperar el numerador y denominador de una función racional en n variables a partir de su desarrollo de Taylor alrededor de un punto. Sea $\frac{\mathrm{p}}{\mathrm{q}} \in k(X_1, \ldots, X_n)$, donde $\mathrm{p}, \mathrm{q} \in k[X_1, \ldots, X_n]$ son polinomios de grado a lo sumo D tales que $\mathrm{q}(0) \neq 0$ (esto puede suponerse luego de una traslación respecto a un punto genérico). Sea $\mathcal{P}$ el polinomio de Taylor centrado en 0 de orden $2D$ de la función racional $\frac{\mathrm{p}}{\mathrm{q}}$. La idea para hallar los polinomios p y q es reducir el problema al caso univariado.

Siguiendo [60, Section 4.3], en primer lugar tomamos T una nueva variable y sustituimos $\overline{\mathcal{P}} := \mathcal{P}(X_1T, \ldots, X_nT) \in k(X_1, \ldots, X_n)[T]$. Notar que $\overline{\mathcal{P}}$ es un polinomio de grado $2D$ en T. Aplicando el algoritmo anterior, sea $\frac{\overline{\mathrm{p}}}{\overline{\mathrm{q}}}$ la $(D+1, D)$-aproximación de Padé de $\overline{\mathcal{P}}$. Como los polinomios $\mathrm{p}(X_1T, \ldots, X_nT)$, $\mathrm{q}(X_1T, \ldots, X_nT)$ también forman una $(D+1, D)$-aproximación de Padé de $\overline{\mathcal{P}}$, la unicidad de la misma dada por el Lema 1.28 dice que difieren en un factor en $k(X_1, \ldots, X_n)$. Dividiendo $\overline{\mathrm{p}}$ y $\overline{\mathrm{q}}$ por $\overline{\mathrm{q}}(0) \in k(X_1, \ldots, X_n)$ y evaluando $T = 1$ se obtiene la aproximación de Padé $\frac{\mathrm{p}}{\mathrm{q}}$. Llamaremos `PadéAprox` a este algoritmo.

Capítulo 2

Soluciones afines aisladas

En este capítulo presentamos un algoritmo probabilístico simbólico que desarrollamos para encontrar las soluciones aisladas en el espacio afín de sistemas polinomiales ralos de n ecuaciones con n incógnitas con mejor complejidad que los algoritmos anteriores. Exhibimos también una cota superior genéricamente exacta para la cantidad de ceros aislados de estos sistemas en $\mathbb{C}^n$ obtenida a partir de los resultados teóricos que dan lugar al algoritmo.

2.1. Métodos de deformación

Dado un sistema polinomial de n ecuaciones en n variables $X_1, \ldots, X_n$ con coeficientes en un cuerpo algebraicamente cerrado K, los métodos de deformación permiten encontrar los ceros aislados del sistema considerándolo una instancia particular de una familia paramétrica de sistemas. La deformación se realiza utilizando un sistema polinomial construido a partir del original agregando una nueva variable T.

2.1.1. Resultados generales

Utilizaremos los siguientes resultados teóricos para asegurar que las soluciones aisladas del sistema original puedan recuperarse a partir de las soluciones aisladas de los sistemas asociados en la deformación.

Lema 2.1 *Sea $P = (p_1, \ldots, p_n)$ un sistema de n polinomios en $K[T, X_1, \ldots, X_n]$ y sea $\tau_0 \in K$. Para todo cero aislado $\xi_0 \in K^n$ de $P(\tau_0, X)$, existe una componente irreducible W de dimensión 1 de $\{(\tau, \xi) \in K^{n+1} \mid P(\tau, \xi) = 0\}$ tal que $(\tau_0, \xi_0) \in W$ y la proyección π_T a la primera coordenada satisface $\overline{\pi_T(W)} = K$ (es decir, π_T es un morfismo dominante de W a K).*

Demostración: Como el sistema P tiene n polinomios en $n+1$ variables, el punto (τ_0, ξ_0) tiene que pertenecer a una componente irreducible W del conjunto de soluciones en K^{n+1} de dimensión al menos uno. Pero como (τ_0, ξ_0) es un cero aislado en $W \cap \{T = \tau_0\}$, la dimensión de W es a lo sumo 1. Entonces, la dimensión de W es exactamente 1. Por el Teorema de la dimensión de la fibra (ver [62, Chapter 1, Section 6.3, Theorem 7]), $\overline{\pi_T(W)} = K$. □

Lema 2.2 *Sea $P = (p_1, \ldots, p_n)$ un sistema de n polinomios en $K[T, X_1, \ldots, X_n]$ y sea $\mathcal{W}$ la unión de todas las componentes irreducibles W de $\{(\tau, \xi) \in K^{n+1} \mid P(\tau, \xi) = 0\}$ de dimensión 1 tales que π_T es un morfismo dominante de W en K. Entonces, para todo $z \in K^n$ tal que $(0, z) \in \mathcal{W}$, existe un vector de series de Puiseux $x_z \in \{x \in \overline{K(T)}^n \mid P(x) = 0\}$ tal que $x_z(0) = z$.*

Demostración: Sea $I(\mathcal{W}) \subset K[T, X]$ el ideal de $\mathcal{W}$ y llamemos $I(\mathcal{W})^e$ al ideal extendido en $K(T)[X]$. Sean $\mathcal{W}^e$ la variedad cero-dimensional definida por $I(\mathcal{W})^e$ en $\overline{K(T)}^n$ y μ una forma lineal que cumple las condiciones de [5, Lemma 12.32]. Por ese lema, μ es una forma lineal separante para los puntos en $\mathcal{W} \cap \{T = 0\}$. A partir del desarrollo en [5, Section 12.4], sean $\widehat{\chi}_\mu(U), \widehat{\varphi}_{\mu,1}(U), \widehat{\varphi}_{\mu,X_i}(U) \in K[T][U]$, con $1 \leq i \leq n$, polinomios que dan resoluciones geométricas tanto de $\mathcal{W}^e$ como de $\mathcal{W}$.

Para todo $(0, z) \in \mathcal{W}$ vale que $(0, \mu(z))$ está en la curva $\{(\tau, u) \in K^2 \mid \widehat{\chi}_\mu(\tau, u) = 0\}$. Además, existe u_z en $\{u \in \overline{K(T)} \mid \widehat{\chi}_\mu(u) = 0\}$ tal que $\lim_{T \to 0} u_z = \mu(z)$ (ver el Teorema 1.26). Para cada $1 \leq j \leq n$, sea $(x_z)_j = \widehat{\varphi}_{\mu,X_j}(u_z)/\widehat{\varphi}_{\mu,1}(u_z)$ (está bien definido pues $\widehat{\chi}_\mu(U)$ y $\widehat{\varphi}_{\mu,1}(U)$ son coprimos). Entonces $x_z \in \mathcal{W}^e$ y, por [5, Section 12.5], sabemos que existe $z' := \lim_{T \to 0} x_z$ y $(0, z')$ es un punto de $\mathcal{W}$. Como $\mu(x_z) = u_z$, vale que $\mu(z') = \lim_{T \to 0} \mu(x_z) = \lim_{T \to 0} u_z = \mu(z)$. Pero como μ es una forma lineal separante para los puntos en $\mathcal{W} \cap \{T = 0\}$, $z = z'$. □

2.1.2. Soluciones en $(\mathbb{C}^*)^n$

Para encontrar las soluciones aisladas en $(\mathbb{C}^*)^n$ de un sistema ralo se buscan las soluciones de sistemas asociados con los mismos soportes que permiten recuperar las soluciones del sistema original. Los métodos más eficientes para hallar los ceros aislados en $(\mathbb{C}^*)^n$ de un sistema ralo son los que utilizan métodos de *deformación poliedral* (ver por ejemplo [71], [42], [43], [31] y [45]).

La idea de las deformaciones poliedrales, introducidas en [42], es la siguiente: sea $P = (p_1, \ldots, p_n)$ un sistema de polinomios de Laurent en $\mathbb{Q}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ genérico cuya familia de soportes es $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$, donde $\mathcal{A}_j \subset \mathbb{Z}^n$ y $p_j(X) = \sum_{\alpha \in \mathcal{A}_j} a_{j,\alpha} X^\alpha$ para todo

$1 \leq j \leq n$. Cada monomio de los polinomios de Laurent involucrados se multiplica por una potencia de un nuevo parámetro T y se obtiene un nuevo sistema de n polinomios en $n+1$ variables. Más precisamente, a partir de una función de levantamiento $\omega = (\omega_1, \ldots, \omega_n)$ (ver la Definición 1.16), se define el sistema deformado $P^\omega = (p_1^{\omega_1}, \ldots, p_n^{\omega_n})$, donde

$$p_j^{\omega_j}(T, X) = \sum_{\alpha \in \mathcal{A}_j} a_{j,\alpha} X^\alpha T^{\omega_j(\alpha)} \in \mathbb{Q}[T, X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$$

para todo $1 \leq j \leq n$, con soportes $\mathcal{A}(\omega)$.

En [42] se prueba que si ω es un levantamiento genérico y el sistema $P^\omega(T, X)$ tiene un cero de la forma

$$X(T) = (x_{01}T^{\gamma_1} + o(T^{\gamma_1}), \ldots, x_{0n}T^{\gamma_n} + o(T^{\gamma_n})),$$

donde $o(T^{\gamma_i})$ es una serie de Puiseux que tiene todos sus términos con exponentes en T mayores a γ_i y $x_{0i} \neq 0$ para todo $1 \leq i \leq n$, entonces $(\gamma, 1) = (\gamma_1, \ldots, \gamma_n, 1)$ es normal asociada a una celda mixta $C = (C_1, \ldots, C_n)$ de la subdivisión $S_\omega(\mathcal{A})$. Además, $(x_{01}, \ldots, x_{0n})$ es un cero en $(\mathbb{C}^*)^n$ del sistema $P_C = (p_{1C}, \ldots, p_{nC})$ donde $p_{jC} = \sum_{\alpha \in C_j} a_{j,\alpha} X^\alpha$ (ver la Definición 1.18) para todo $1 \leq j \leq n$. Si el sistema P es genérico, para cada celda C, el sistema P_C tiene $\mathcal{MV}_n(C)$ soluciones aisladas distintas en $(\mathbb{C}^*)^n$. En función de lo anterior, los autores proponen un algoritmo para encontrar todos los ceros aislados de un sistema ralo en $(\mathbb{C}^*)^n$.

La idea del algoritmo es, dado un sistema ralo F cuya familia de soportes es $\mathcal{A}$ para el cual se quiere hallar los ceros aislados en $(\mathbb{C}^*)^n$, se toma G un sistema genérico con los mismos soportes. El algoritmo halla en primer lugar los ceros aislados en $(\mathbb{C}^*)^n$ de los sistemas G_C asociados a cada una de las celdas mixtas C de una subdivisión mixta fina de $\mathcal{A}$ (sistemas binomiales que pueden resolverse fácilmente) y posteriormente sigue numéricamente cada una de las "ramas" para aproximar las soluciones del sistema G. Luego se aproximan las soluciones de F mediante otra deformación homotópica de la forma

$$H(T, X) = (1 - T)F(X) + TG(X).$$

Siguiendo esta misma estrategia, en [45, Section 5] los autores desarrollaron un algoritmo simbólico probabilístico que calcula una resolución geométrica del conjunto de los ceros comunes en $(\mathbb{C}^*)^n$ de un sistema genérico de n ecuaciones polinomiales ralas. A continuación describimos el algoritmo de [45, Algorithm 5.1] que llamamos `ToricSolve` y que usaremos como subrutina en nuestros algoritmos.

Para un sistema ralo genérico $P = (p_1, \ldots, p_n)$ con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ donde $\mathcal{A}_j \subset (\mathbb{Z}_{\geq 0})^n$ para todo $1 \leq j \leq n$, se nota $\widehat{V}$ a la unión de todas las componentes irreducibles W de $\{(t, x) \in \mathbb{C}^{n+1} \mid p_1^{\omega_1}(t, x) = \cdots = p_n^{\omega_n}(t, x) = 0\}$ no incluidas en hiperplanos

$\{x_i = 0\}$ para todo $1 \leq i \leq n$ y tales que $\overline{\pi_T(W)} = \mathbb{C}$, donde $\pi_T : \mathbb{C}^{n+1} \longrightarrow \mathbb{C}$ es la proyección $\pi_T(t, x) = t$. La variedad algebraica $\widehat{V}$ es equidimensional de dimensión 1.

Algoritmo 2.3 `ToricSolve` *([45, Algorithm 5.1])*

INPUT: Un sistema de polinomios $P = (p_1, \ldots, p_n)$ en $\mathbb{Q}[X_1, \ldots, X_n]$ genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ y las celdas mixtas de una subdivisión mixta fina $S_\omega(\mathcal{A})$ inducida por una función de levantamiento ω.

1. *Elegir una forma lineal $\mu \in \mathbb{Z}[X_1, \ldots, X_n]$ al azar.*
2. *Para cada celda mixta C:*
   a) *Hallar una resolución geométrica respecto a μ del conjunto de los ceros en $(\mathbb{C}^*)^n$ de P_C. Llamamos $q_{\mu,C}$ al minimal de esa resolución geométrica.*
   b) *Mediante un procedimiento de Newton-Hensel simbólico, levantar el minimal $q_{\mu,C}$ a una aproximación adecuada $\widetilde{q}_{\mu,C}$ del minimal $\widehat{q}_{\mu,C}$ de μ en las ramas de $\widehat{V}$ correspondientes a los ceros de P_C.*
3. *Obtener una resolución geométrica de $\widehat{V}$:*
   a) *Calcular $\widetilde{q}_\mu = \prod_{C \text{ celda mixta}} \widetilde{q}_{\mu,C}$.*
   b) *Hallar $\widehat{q}_\mu = \prod_{C \text{ celda mixta}} \widehat{q}_{\mu,C}$, el polinomio minimal de μ respecto de $\widehat{V}$, a partir de $\widetilde{q}_\mu$.*
   c) *Hallar una resolución geométrica de $\widehat{V}$ respecto a μ a partir de $\widehat{q}_\mu$.*
4. *Sustituir $T = 1$ en la resolución geométrica obtenida en el paso 3.*

OUTPUT: Una resolución geométrica de los ceros en $(\mathbb{C}^*)^n$ de P.

La complejidad del algoritmo (ver [45, Proposition 5.13]) es del orden de

$$O((n^3 N \log(d) + n^{1+\Omega}) M(\Upsilon) M(\mathcal{D})(M(\mathcal{D}) + M(\mathcal{E})))$$

donde

- $N := \sum_{1 \leq j \leq n} \#\mathcal{A}_j$,
- $d := \text{máx}_{1 \leq j \leq n}\{\deg(p_j)\}$,

- $\mathcal{D} := \mathcal{MV}_n(\mathcal{A})$,
- $\Upsilon :=$ máx$\{\|\eta\|\}$ donde el máximo se toma sobre todas las normales primitivas asociadas a celdas mixtas en $S_\omega(\mathcal{A})$,
- $\mathcal{E} := \mathcal{MV}_{n+1}(\Delta \times \{0\}, \mathcal{A}_1(\omega_1), \ldots, \mathcal{A}_n(\omega_n))$ (donde Δ es el conjunto de vértices del símplex standard de $\mathbb{R}^n$).

En el caso en que $0 \in \bigcap_{j=1}^{n} \mathcal{A}_j$, un sistema genérico con soportes $\mathcal{A}_1, \ldots, \mathcal{A}_n$ no tiene soluciones con coordenadas nulas. Entonces, el algoritmo `ToricSolve` calcula todos los ceros del sistema en el espacio afín.

2.1.3. Soluciones en $\mathbb{C}^n$

Para hallar los ceros aislados en el espacio afín en el caso de soportes arbitrarios, en [43] se propone un algoritmo basado en deformaciones poliedrales que surge de la función de levantamiento ω^0 introducida en el Capítulo 1, Sección 1.3.3: Sea $P = (p_1, \ldots, p_n)$ un sistema ralo genérico en $K[X_1, \ldots, X_n]$ cuya familia de soportes es $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ donde $\mathcal{A}_j \subset (\mathbb{Z}_{\geq 0})^n$ para todo $1 \leq j \leq n$, y sea $\mathcal{A}^0 = (\mathcal{A}_1^0, \ldots, \mathcal{A}_n^0)$ la familia de soportes extendidos $\mathcal{A}_j^0 = \mathcal{A}_j \cup \{0\}$ para todo $1 \leq j \leq n$. Se define el sistema deformado $P^0 = (p_1^0, \ldots, p_n^0)$ cuya familia de soportes es $\mathcal{A}^0$, donde para todo $1 \leq j \leq n$,

$$p_j^0 = \begin{cases} p_j & \text{si } 0 \in \mathcal{A}_j \\ p_j + a_{j,0}T^\kappa & \text{si } 0 \notin \mathcal{A}_j \end{cases}$$

con coeficientes $a_{j,0} \in K$ genéricos si $0 \notin \mathcal{A}_j$ y $\kappa \in \mathbb{N}$.

Así, si $0 \notin \bigcap_{j=1}^{n} \mathcal{A}_j$ y P es un sistema genérico, como se prueba en [43] (ver también el Lema 2.2), los ceros comunes aislados de P pueden obtenerse como límites de las soluciones del sistema deformado P^0 cuando T tiende a cero. Más precisamente, para todo $I \subset \{1, \ldots, n\}$, los ceros aislados de P en

$$O_I := \{x \in K^n \mid x_i = 0 \iff i \in I\}$$

se obtienen de los ceros de P^0 del tipo $X(T) = (x_{01}T^{\gamma_1} + o(T^{\gamma_1}), \ldots, x_{0n}T^{\gamma_n} + o(T^{\gamma_n}))$, con

$$\gamma_i = 0 \text{ si } i \notin I \text{ y } \gamma_i > 0 \text{ si } i \in I.$$

Para cada cero $X(T)$ de P^0 de este tipo, el vector formado por los mínimos exponentes $(\gamma_1, \ldots, \gamma_n)$ de T en cada coordenada de $X(T)$ corresponde a las primeras n coordenadas de la normal interior $(\gamma, 1) \in \mathbb{Q}^{n+1}$ de alguna de las facetas de $Conv(\mathcal{A}^0(\omega^0))$ (ver la

Sección 1.3.3 para una descripción de $\mathcal{A}^0(\omega^0)$ y la subdivisión de $\mathcal{A}^0$ inducida por ω^0). Dada la celda $C = (C_1, \ldots, C_n)$ de la subdivisión $S_{\omega^0}(\mathcal{A}^0)$ que tiene como normal asociada el vector $(\gamma, 1)$, el vector $x_0 = (x_{01}, \ldots, x_{0n}) \in (K^*)^n$ de los coeficientes correspondientes a los términos de orden mínimo en T en cada coordenada de $X(T)$ es un cero aislado del sistema $P_C^0 = (p_{1C}^0, \ldots, p_{nC}^0)$ (ver la Definición 1.18). Notar que además en este caso vale

$$\lim_{T\to 0}(X(T))_i = x_{0i} \text{ si } i \notin I, \text{ y } \lim_{T\to 0}(X(T))_i = 0 \text{ si } i \in I.$$

Luego, el punto $\xi = (\xi_1, \ldots, \xi_n) \in \mathbb{C}^n$ tal que $\xi_i = x_{0i}$ para $i \notin I$ y $\xi_i = 0$ para $i \in I$ es un cero de P. De esta forma, los ceros aislados de P en O_I pueden conseguirse reemplazando por 0 las coordenadas indexadas por I en los ceros aislados en $(K^*)^n$ de los sistemas P_C^0 correspondientes a celdas C de $S_\omega(\mathcal{A})$ con normal asociada $(\gamma, 1)$ tal que $\gamma_i = 0$ si $i \notin I$ y $\gamma_i > 0$ si $i \in I$.

Como el sistema P_C^0 es genérico y tiene un cero x_0 aislado de coordenadas no nulas, la familia de soportes C de P_C^0 tiene volumen mixto positivo. De lo anterior, se deduce la siguiente observación:

Observación 2.4 *Si P es un sistema genérico con soportes $\mathcal{A}$ y tiene ceros aislados que están en O_I, existe una celda $C \in S_{\omega^0}(\mathcal{A}^0)$ que tiene volumen mixto positivo y cuya normal asociada $(\gamma, 1)$ cumple que $\gamma_i = 0$ si $i \notin I$ y $\gamma_i > 0$ si $i \in I$.*

Para hallar los ceros aislados de P, la idea es entonces la siguiente: para cada celda C de la subdivisión $S_{\omega^0}(\mathcal{A}^0)$ con normal asociada $(\gamma, 1)$ de coordenadas no negativas se genera una subdivisión mixta fina nueva y mediante una deformación poliedral se buscan los ceros aislados x_0 en $(K^*)^n$ del sistema P_C^0. Reemplazando con cero en las coordenadas x_{0i} tales que $\gamma_i > 0$, se obtienen los ceros aislados en K^n de P.

Finalmente, los ceros aislados de un sistema arbitrario se encuentran a partir de deformaciones homotópicas de los ceros de un sistema genérico P con los mismos soportes.

Como este algoritmo requiere que, para cada celda C cuya normal asociada tenga todas sus coordenadas no negativas, se genere una subdivisión mixta fina nueva, los tiempos de ejecución pueden ser muy grandes. En [31] presentaron un refinamiento a este algoritmo que no requiere el uso de levantamientos sucesivos sino que involucra solamente dos levantamientos de los soportes $\mathcal{A}^0$. Vamos a describir brevemente los resultados allí obtenidos (ver también [26]).

Para un sistema $P = (p_1, \ldots, p_n)$ cuya familia de soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$ cumple que $0 \notin \bigcap_{j=1}^{n} \mathcal{A}_j$ y un número $\kappa \in \mathbb{R}_{>0}$ elegido al azar, los autores definen las funciones de levantamiento de los soportes $\mathcal{A}^0$:

1. $\omega^{0\kappa} = (\omega_1^{0\kappa}, \ldots, \omega_n^{0\kappa})$ dada por
   - $\omega_j^{0\kappa}(\alpha) = 0$ si $\alpha \in \mathcal{A}_j$, y
   - $\omega_j^{0\kappa}(0) = \kappa$ si $0 \notin \mathcal{A}_j$.
2. $\omega^{\kappa} = (\omega_1^{\kappa}, \ldots, \omega_n^{\kappa})$ dada por
   - $\omega_j^{\kappa}(\alpha) = b_{j,\alpha} \in \mathbb{R}$ si $\alpha \in \mathcal{A}_j$, donde $0 < b_{j,\alpha} < 1$ se eligen al azar y
   - $\omega_j^{\kappa}(0) = \kappa$ si $0 \notin \mathcal{A}_j$.

La función $\omega^{0\kappa}$ define la misma subdivisión de $\mathcal{A}^0$ que ω^0 y el conjunto de celdas cuya normal asociada tiene todas sus coordenadas no negativas se mantiene.

Sea $d = \text{máx}_{1\leq j\leq n}\{\deg(p_j)\}$. En [31, Proposition 1] probaron que si $\kappa \in \mathbb{R}$ se elige al azar con la condición que $\kappa > n(n+1)d^n$, entonces la subdivisión $S_{\omega^\kappa}(\mathcal{A}^0)$ refina a la subdivisión $S_{\omega^{0\kappa}}(\mathcal{A}^0)$ de $\mathcal{A}^0$. Esto es, para toda celda $D \in S_{\omega^\kappa}(\mathcal{A}^0)$ existe alguna celda $C \in S_{\omega^{0\kappa}}(\mathcal{A}^0)$ tal que D es una subcelda de C. Si además ω^κ es un levantamiento genérico, entonces $S_{\omega^\kappa}(\mathcal{A}^0)$ es una subdivisión mixta fina con la propiedad de que subcolecciones de celdas de $S_{\omega^\kappa}(\mathcal{A}^0)$ dan subdivisiones mixtas finas de las celdas de $S_{\omega^{0\kappa}}(\mathcal{A}^0)$. Esto es, para toda celda C de $S_{\omega^{0\kappa}}(\mathcal{A}^0)$, restringiendo ω^κ a C se tiene la subdivisión

$$S_{\omega^\kappa}(C) = \{D \text{ celda de } C \mid Conv(D(\omega^\kappa)) \text{ es una cara inferior de } Conv(C(\omega^\kappa))\}.$$

Entonces todas las celdas de $S_{\omega^\kappa}(C)$ son celdas de $S_{\omega^\kappa}(\mathcal{A}^0)$. Además, como $S_{\omega^\kappa}(\mathcal{A}^0)$ es una subdivisión mixta fina, el volumen mixto de C puede calcularse como la suma de los volúmenes mixtos de las celdas mixtas de $S_{\omega^\kappa}(C)$.

Con el objeto de obtener un sistema *polinomial* al deformar el sistema inicial usando la función de levantamiento considerada, vamos a modificar ω^κ. Tomando M suficientemente grande, sea $\omega = (\omega_1, \ldots, \omega_n)$ donde

- $\omega_j(\alpha) = b_{j,\alpha} \in \mathbb{N}$ donde $b_{j,\alpha} < M$ para todo $\alpha \in \mathcal{A}_j$ y $1 \leq j \leq n$. (2.1)
- $\omega_j(0) = \kappa$ si $0 \notin \mathcal{A}_j$ para $\kappa > n(n+1)d^n M$.

Podemos extender el resultado de [31, Proposition 1]:

Lema 2.5 *Sea ω una función de levantamiento genérica como en (2.1). Entonces la subdivisión $S_\omega(\mathcal{A}^0)$ es mixta fina y refina a $S_{\omega^{0\kappa}}(\mathcal{A}^0)$.*

Demostración: Empezaremos definiendo un nuevo levantamiento asociado a ω : Sea $\widetilde{\kappa} = \dfrac{\kappa}{M}$ y $\widetilde{\omega} = (\widetilde{\omega}_1, \ldots, \widetilde{\omega}_n)$, donde para todo $1 \leq j \leq n$ vale que $\widetilde{\omega}_j(\alpha) = \dfrac{\omega_j(\alpha)}{M}$ para todo

$\alpha \in \mathcal{A}_j$, y $\widetilde{\omega}_j(0) = \widetilde{\kappa}$ si $0 \notin \mathcal{A}_j$. Como $\omega_j(\alpha) < M$, entonces $0 < \widetilde{\omega}_j(\alpha) < 1$ para todo $\alpha \in \mathcal{A}_j$. Además, $\widetilde{\kappa} = \dfrac{\kappa}{M} > n(n+1)d^n$.

Observemos que $S_{\widetilde{\omega}}(\mathcal{A}^0) = S_{\omega}(\mathcal{A}^0)$ pues toda celda C de $S_{\widetilde{\omega}}(\mathcal{A}^0)$ con normal asociada $(\gamma_1, \ldots, \gamma_n, 1)$ es también una celda de $S_{\omega}(\mathcal{A}^0)$ con normal asociada $(M\gamma_1, \ldots, M\gamma_n, 1)$. De la misma forma se puede ver que $S_{\omega^{0\widetilde{\kappa}}}(\mathcal{A}^0) = S_{\omega^{0\kappa}}(\mathcal{A}^0)$.

Como ω es genérica, usando [45, Lemma 2.1] la función de levantamiento $\widetilde{\omega}$ es también genérica, y por [31, Section 4] sabemos que la subdivisión $S_{\widetilde{\omega}}(\mathcal{A}^0)$ es mixta fina. Por lo tanto, $S_{\omega}(\mathcal{A}^0)$ es mixta fina. Por [31, Proposition 1], sabemos que $S_{\widetilde{\omega}}(\mathcal{A}^0)$ refina a $S_{\omega^{0\widetilde{\kappa}}}(\mathcal{A}^0)$ con lo cual $S_{\omega}(\mathcal{A}^0)$ refina a $S_{\omega^{0\kappa}}(\mathcal{A}^0)$. □

2.2. Reducción al caso tórico

Sean $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ una familia de conjuntos finitos en $(\mathbb{Z}_{\geq 0})^n$, y $P = (p_1, \ldots, p_n)$ un sistema genérico de n polinomios en n variables $X = (X_1, \ldots, X_n)$ con coeficientes en un cuerpo algebraicamente cerrado K tal que la familia de soportes de P es $\mathcal{A}$.

Para hallar las soluciones aisladas de P, al igual que en procedimientos anteriores, asociamos al sistema original un conjunto de subsistemas y buscamos sus ceros aislados de coordenadas no nulas usando solo dos deformaciones poliedrales. Para construir estos subsistemas analizamos los soportes de los polinomios para decidir para qué conjuntos $I \subset \{1, \ldots, n\}$, el sistema P tiene ceros aislados con coordenadas nulas en los lugares indexados por I. Esto nos permitirá que los sistemas asociados a resolver sean menos sistemas en menos incógnitas que los de los algoritmos previos.

Para todo $I \subset \{1, \ldots, n\}$ definimos un sistema polinomial P_I asociado a P de la siguiente forma:

Definición 2.6 *Dado $I \subset \{1, \ldots, n\}$, se define el sistema P_I formado por los polinomios en $K[\{X_i \mid i \notin I\}]$ que resultan de evaluar el sistema P en $X_i = 0$ para todo $i \in I$, y descartar aquellos polinomios que se anulan idénticamente al hacer esta evaluación.*

A continuación demostraremos algunos resultados teóricos en los que se basa nuestro algoritmo.

Lema 2.7 *Sea $I \subset \{1, \ldots, n\}$ tal que el sistema P tiene ceros aislados que están en $O_I = \{x \in K^n \mid x_i = 0 \iff i \in I\}$. Entonces, el sistema P_I tiene exactamente $n - \#I$ polinomios. Más aún, para cada celda C de $S_{\omega^0}(\mathcal{A}^0)$ cuya normal asociada $(\gamma, 1)$ cumple*

que $\gamma_i = 0$ si $i \notin I$ y $\gamma_i > 0$ si $i \in I$, el sistema P_C^0 está compuesto por los polinomios de P_I y $\#I$ polinomios que se hacen constantes cuando son evaluados en $X_i = 0$ para todo $i \in I$.

Demostración: Como P tiene ceros aislados en O_I, el sistema P_I tiene también ceros aislados en $O_I \cong (K^*)^{n-\#I}$. Entonces, el sistema P_I no puede tener menos de $n - \#I$ polinomios. Supongamos que la cantidad de polinomios es estrictamente mayor. Eligiendo $n - \#I$ polinomios entre ellos, como P es un sistema genérico, el Teorema de Bernstein nos dice que esos $n - \#I$ polinomios tienen finitos ceros comunes en $(K^*)^{n-\#I}$. Tomando uno de los polinomios no elegidos del sistema P_I, este polinomio no se anula en ninguno de esos ceros comunes por la genericidad de P. Por lo tanto, el sistema P_I no tendría ceros en $(K^*)^{n-\#I}$. Entonces, el sistema P_I tiene exactamente $n - \#I$ polinomios.

Sea $C \in S_{\omega^0}(\mathcal{A}^0)$ una celda cuya normal asociada $(\gamma, 1) = (\gamma_1, \ldots, \gamma_n, 1)$ cumple que $\gamma_i = 0$ si $i \notin I$ y $\gamma_i > 0$ si $i \in I$. Para todo $1 \leq j \leq n$, sea $\beta_j := \text{mín}\{\sum_{i=1}^{n} \gamma_i\alpha_i + \omega_j^0(\alpha) \mid \alpha \in \mathcal{A}_j^0\} \geq 0$. Entonces $C = (C_1, \ldots, C_n)$, donde $C_j = \{\alpha \in \mathcal{A}_j^0 \mid \sum_{i=1}^{n} \gamma_i\alpha_i + \omega_j^0(\alpha) = \beta_j\}$.

Sean $p_{j_1}, \ldots, p_{j_{n-\#I}}$ los polinomios de P a partir de los que se obtiene P_I. Como estos polinomios no se anulan al evaluarse en 0 las coordenadas X_i con $i \in I$, existe al menos un monomio en p_{j_k} que no pertenece al ideal $\langle X_i : i \in I\rangle$ para todo $1 \leq k \leq n - \#I$. Para el exponente $\alpha \in \mathcal{A}_{j_k}$ de ese monomio, se tiene que $\sum_{i=1}^{n} \gamma_i\alpha_i + \omega_{j_k}^0(\alpha) = 0$, con lo cual $\beta_{j_k} = 0$. Más aún, si notamos $(p_{j_k})_I$ al polinomio que resulta de evaluar p_{j_k} en cero en las coordenadas indexadas por I, para todo monomio de $(p_{j_k})_I$ el vector α de sus exponentes cumple que $\sum_{i=1}^{n} \gamma_i\alpha_i + \omega_{j_k}^0(\alpha) = 0$, y por lo tanto está en C_{j_k}. Por otro lado, para todo α tal que $X^\alpha \in \langle X_i : i \in I\rangle$, vale que $\alpha_{i_0} > 0$ para algún $i_0 \in I$ y por lo tanto $\sum_{i=1}^{n} \gamma_i\alpha_i \geq \gamma_{i_0}\alpha_{i_0} > 0$. Entonces, todo vector de exponentes α de un monomio que se anula al evaluar $X_i = 0$ para todo $i \in I$ no pertenece a C_{j_k}. Para el caso del origen, p_{j_k} tiene término independiente si y solo si $0 \in \mathcal{A}_{j_k}$. Esto es lo mismo que pedir $\omega_{j_k}^0(0) = 0$, que a su vez equivale a que $0 \in C_{j_k}$. Se puede entonces deducir que C_{j_k} contiene exactamente los exponentes en $\mathbb{Z}^n$ correspondientes a los monomios de $(p_{j_k})_I$.

Para cada $j \notin \{j_1, \ldots, j_{n-\#I}\}$, el polinomio p_j se anula idénticamente al evaluar en cero las variables indexadas por el conjunto I. Entonces, p_{jC}^0 es una suma de monomios en $\langle X_i : i \in I\rangle$ y posiblemente un término constante (si $0 \notin \mathcal{A}_j$). Por lo tanto, al evaluar $X_i = 0$ para todo $i \in I$ da lugar a una constante. □

Usaremos un levantamiento genérico ω de la forma (2.1). Por el Lema 2.5 sabemos que si M es suficientemente grande la subdivisión que genera es mixta fina y la restricción de ω a toda celda C de $S_{\omega^0}(\mathcal{A}^0)$ induce una subdivisión mixta fina de C.

Observación 2.8 *Sea C una celda de $S_{\omega^0}(\mathcal{A}^0)$. El sistema P_C^0 tiene ceros aislados en $(K^*)^n$ si y solo si la celda C tiene volumen mixto positivo, lo que equivale a que C contenga una celda mixta de la subdivisión $S_\omega(\mathcal{A}^0)$.*

Introducimos la siguiente notación: para todo $I \subset \{1,\dots,n\}$, definimos el conjunto

$$J_I = \{j \in \{1,\dots,n\} \mid \exists \alpha \in \mathcal{A}_j : \alpha_i = 0 \ \forall\, i \in I\}$$

de los índices de los polinomios de P_I. Sea $\pi_I : K^n \to K^{n-\#I}$ la proyección definida como $\pi_I(\alpha) = (\alpha_l)_{l \notin I}$ y $\varphi_I : K^{n-\#I} \to K^n$ la función que inserta ceros en las coordenadas indexadas por I. Llamamos $\mathcal{A}^I = (\mathcal{A}_j^I)_{j \in J_I}$ donde para todo $1 \le j \le n$,

$$\mathcal{A}_j^I = \{\pi_I(\alpha) \mid \alpha \in \mathcal{A}_j,\ \alpha_i = 0 \ \forall\, i \in I\}.$$

De esta manera $\mathcal{A}^I$ es la familia de soportes de los polinomios de P_I. Notamos además $\omega^I = (\omega_j^I)_{j \in J_I}$ donde $\omega_j^I : \mathcal{A}_j^I \to \mathbb{Z}_{\ge 0}$ es la función $\omega_j^I(\overline{\alpha}) = \omega_j(\varphi_I(\overline{\alpha}))$. Así, a partir de ω, obtenemos una función de levantamiento para la familia de soportes $\mathcal{A}^I$.

Lema 2.9 *Sea P un sistema genérico con soportes $\mathcal{A} = (\mathcal{A}_1,\dots,\mathcal{A}_n)$ en $(\mathbb{Z}_{\ge 0})^n$. Sean $I \subset \{1,\dots,n\}$ tal que el sistema P tiene ceros aislados que están en O_I, y $C \in S_{\omega^0}(\mathcal{A}^0)$ una celda de volumen mixto positivo cuya normal asociada $(\gamma, 1)$ cumple $\gamma_i = 0$ si $i \notin I$ y $\gamma_i > 0$ si $i \in I$. Entonces, para todo ξ cero de P_I en $(K^*)^{n-\#I}$ existe un cero aislado $\widetilde{\xi}$ de P_C^0 tal que $\pi_I(\widetilde{\xi}) = \xi$.*

Demostración: Sin perder generalidad, sean $I = \{r+1,\dots,n\}$ y $J_I = \{1,\dots,r\}$.

Por la estructura del sistema P_C^0 que caracterizamos en el Lema 2.7, $(\xi_1,\dots,\xi_r,\xi_{r+1},\dots,\xi_n)$ es un cero en $(K^*)^n$ de P_C^0 si y solo si $(\xi_1,\dots,\xi_r)$ es un cero de P_I y $(\xi_{r+1},\dots,\xi_n)$ es un cero aislado del sistema de $n-r$ polinomios en $K[X_{r+1},\dots,X_n]$ dado por $p_{jC}^0(\xi_1,\dots,\xi_r, X_{r+1},\dots,X_n)$ para todo $1 \le j \le n$. Observar que este sistema tiene soportes $\pi_{\overline{I}}(C_{r+1}),\dots,\pi_{\overline{I}}(C_n)$, donde $\overline{I} = \{1,\dots,r\}$.

Por las hipótesis sabemos que $\mathcal{MV}_n(C) > 0$ y, por la Proposición 1.11, que

$$\mathcal{MV}_n(C) = \mathcal{MV}_r(\mathcal{A}^I)\mathcal{MV}_{n-r}(\pi_{\overline{I}}(C_{r+1}),\dots,\pi_{\overline{I}}(C_n)). \tag{2.2}$$

En particular, $\mathcal{MV}_{n-r}(\pi_{\overline{I}}(C_{r+1}),\dots,\pi_{\overline{I}}(C_n)) > 0$.

Como para cada $(\xi_1,\dots,\xi_r)$ cero en $(K^*)^r$ de P_I hay a lo sumo $\mathcal{MV}_{n-r}(\pi_{\overline{I}}(C_{r+1}),\dots,\pi_{\overline{I}}(C_n))$ ceros aislados en $(K^*)^{n-r}$ de $p_{jC}^0(\xi_1,\dots,\xi_r,X_{r+1},\dots,X_n)$ para todo $1 \le j \le n$, para que valga la igualdad (2.2) tiene que haber exactamente esa cantidad de ceros. □

Sea $\xi = (\xi_1, \ldots, \xi_n)$ un cero aislado del sistema genérico P que está en O_I. Por un lado, el algoritmo de [43] requiere para hallarlo resolver los sistemas P_C^0 para aquellas celdas C de $S_{\omega^0}(\mathcal{A}^0)$ con volumen mixto positivo y cuya normal asociada $(\gamma, 1)$ cumple que $\gamma_i = 0$ si $i \notin I$ y $\gamma_i > 0$ si $i \in I$, para lo cual se utiliza una subdivisión mixta fina de cada una de estas celdas C. Por otro lado, $(\xi_i)_{i \notin I}$ es un cero de P_I en $(K^*)^{n-\#I}$ y, como el sistema P_I es cuadrado y genérico, sus ceros en $(K^*)^{n-\#I}$ pueden obtenerse usando una subdivisión mixta fina de $\mathcal{A}^I$. El lema que sigue relaciona las celdas de una subdivisión de los soportes de P_I con las celdas de una subdivisión de los soportes de P_C^0.

Lema 2.10 *Sea ω una función de levantamiento genérica de la forma (2.1). Sean $I \subset \{1, \ldots, n\}$ tal que el sistema genérico P tiene ceros aislados que están en O_I, y $C \in S_{\omega^0}(\mathcal{A}^0)$ una celda de volumen mixto positivo cuya normal asociada $(\gamma, 1)$ cumple $\gamma_i = 0$ si $i \notin I$ y $\gamma_i > 0$ si $i \in I$. Entonces, cada celda mixta de $S_{\omega^I}(\mathcal{A}^I)$ es de la forma $\pi_I(D) := (\pi_I(D_j))_{j \in J_I}$ para una celda mixta $D = (D_1, \ldots, D_n) \in S_\omega(C)$.*

Demostración: Podemos suponer que $I = \{r+1, \ldots, n\}$ y $J_I = \{1, \ldots, r\}$. Sea $C \in S_{\omega^0}(\mathcal{A}^0)$ una celda que cumple las hipótesis. Por el Lema 2.7, para todo $1 \leq j \leq r$ vale que $C_j = \mathcal{A}_j^I \times \{0\}$ (donde $0 \in \mathbb{R}^{n-r}$) y por lo tanto, $C_j(\omega_j) \simeq \mathcal{A}_j^I(\omega_j^I) \times \{0\}$ para todo $1 \leq j \leq r$.

Sea D una celda mixta de $S_\omega(C)$ y π la proyección a las primeras n coordenadas. Por la definición de una subdivisión inducida por un levantamiento, existe $\nu \in \mathbb{Q}^n$ tal que $Conv(C(\omega))_{(\nu,1)} = \Big(\sum_{j=1}^n Conv(C_j(\omega_j)) \Big)_{(\nu,1)} = \sum_{j=1}^n Conv(C_j(\omega_j))_{(\nu,1)}$ y $D_j = \pi(C_j(\omega_j)_{(\nu,1)})$ para todo $1 \leq j \leq n$.

Sea $\nu_I := \pi_I(\nu)$. Entonces $Conv(\mathcal{A}^I(\omega^I))_{(\nu_I,1)} = \sum_{j=1}^r Conv(\mathcal{A}_j^I(\omega_j^I))_{(\nu_I,1)}$. Como $C_j(\omega_j) \simeq \mathcal{A}_j^I(\omega_j^I) \times \{0\}$, considerando la cara de normal interior $(\nu, 1)$ tenemos que $C_j(\omega_j)_{(\nu,1)} \simeq \mathcal{A}_j^I(\omega_j^I)_{(\nu_I,1)} \times \{0\}$, y por lo tanto la celda de $S_{\omega^I}(\mathcal{A}^I)$ asociada a la normal $(\nu_I, 1)$ es $(\pi_I(D_1), \ldots, \pi_I(D_r))$. Además, para todo $1 \leq j \leq r$ sabemos que $D_j \subset C_j$, con lo cual $D_j = \pi_I(D_j) \times \{0\}$. Entonces, la celda $(\pi_I(D_1), \ldots, \pi_I(D_r))$ es mixta.

A la inversa, sea $D^I = (D_1^I, \ldots, D_r^I)$ una celda mixta de la subdivisión $S_{\omega^I}(\mathcal{A}^I)$. Llamando $(\nu_I, 1)$ a la normal interior de la cara de $Conv(\mathcal{A}^I(\omega^I))$ que define la celda D^I, ν_I es el vector de exponentes de los términos iniciales de una solución $\xi(T)$ del sistema $P_I^{\omega^I}(X, T)$ (ver la Sección 2.1.2).

Sea C una celda de $S_{\omega^0}(\mathcal{A}^0)$ de volumen mixto positivo cuya normal asociada $(\gamma, 1)$ cumple que $\gamma_i = 0$ si $i \notin I$ y $\gamma_i > 0$ si $i \in I$. Por el Lema 2.7, el sistema P_C^0 está compuesto por los polinomios P_I y $\#I$ polinomios que se hacen constantes cuando especializamos $X_i = 0$

para todo $i \in I$. Por lo tanto el sistema $(P_C^0)^\omega(X,T)$ está compuesto por los polinomios $P_I^{\omega^I}(X,T)$ y $\#I$ polinomios. Por el Lema 2.9, de cada solución de $P_I^{\omega^I}(X,T) = 0$ obtenemos una solución de $(P_C^0)^\omega(X,T) = 0$. Entonces, existe una solución $\widetilde{\xi}(T)$ cuyas primeras r coordenadas son $\xi(T)$. Llamando ν a los exponentes de los términos iniciales de $\widetilde{\xi}(T)$, $(\nu, 1)$ es la normal interior de una cara de $Conv(C(\omega))$ correspondiente a una celda mixta D de la subdivisión $S_\omega(C)$. Por el razonamiento anterior, D^I es la proyección de D. □

2.3. Cálculo de soluciones afines aisladas

2.3.1. Algoritmo

Sea $F = (f_1, \ldots, f_n)$ un sistema de polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$ para el cual queremos hallar una descripción de su conjunto de ceros aislados en $\mathbb{C}^n$. La idea del algoritmo es considerar un sistema $G = (g_1, \ldots, g_n)$ de polinomios genéricos en $\mathbb{Q}[X_1, \ldots, X_n]$ con los mismos soportes $\mathcal{A}$, una nueva variable T y la deformación homotópica

$$H(T, X) = (1 - T)F(X) + TG(X).$$

Para cada cero aislado $z \in \mathbb{C}^n$ de $F(X) = H(0, X)$ tenemos que $(0, z)$ es un cero del sistema $H(T, X)$ y, por el Lema 2.1, existe W una componente irreducible de $V(H) \subset \mathbb{C}^{n+1}$ de dimensión 1 tal que $(0, z) \in W$ y $\overline{\pi_T(W)} = \mathbb{C}$. Por otro lado, consideremos a H como un sistema de n polinomios en las variables $X_1, \ldots, X_n$ y coeficientes en $\mathbb{Q}[T]$. Por el Lema 2.2 las componentes irreducibles de dimensión 1 asociadas a los ceros aislados de F en $\mathbb{C}^n$ se corresponden con ceros aislados de H en $\overline{\mathbb{C}(T)}^n$. Observar que H, como sistema de n polinomios en n variables, es un sistema genérico con soportes $\mathcal{A}_1, \ldots, \mathcal{A}_n$ y por lo tanto podemos aplicar los resultados de la Sección 2.2. La idea es buscar en primer lugar los ceros aislados de H en $\overline{\mathbb{C}(T)}^n$.

En función de los resultados de la sección anterior, el algoritmo que proponemos para hallar los ceros aislados en $\mathbb{C}^n$ de F es el siguiente:

Incluimos en el input del algoritmo las celdas mixtas de una subdivisión mixta fina de los soportes extendidos $\mathcal{A}^0 = (\mathcal{A}_1^0, \ldots, \mathcal{A}_n^0)$, donde $\mathcal{A}_j^0 = \mathcal{A}_j \cup \{0\}$ para todo $1 \leq j \leq n$, obtenida a partir de una función de levantamiento $\omega = (\omega_1, \ldots, \omega_n)$ genérica de la forma (2.1). El Lema 2.5 y el Teorema 1.5 nos aseguran que, si M es suficientemente grande, un levantamiento construido eligiendo los valores de $\omega_j(\alpha)$ para todo $\alpha \in \mathcal{A}_j$ y κ al azar induce una subdivisión mixta fina que refina $S_{\omega^0}(\mathcal{A}^0)$ con probabilidad alta.

Para poder encontrar los ceros aislados del sistema H en $\overline{\mathbb{C}(T)}^n$ buscamos en primer lugar el conjunto $\mathcal{I}$ de los subconjuntos $I \subset \{1, \ldots, n\}$ tales que H tiene ceros aislados en

$O_I = \{x \in \overline{\mathbb{C}(T)}^n \mid x_i = 0 \iff i \in I\}$. Para hallar $\mathcal{I}$, calculamos primero en el paso 1, para cada celda mixta $D \in S_\omega(\mathcal{A}^0)$, la normal $(\gamma, 1)$ asociada a la celda $Conv(D(\omega^0))$ de $S_{\omega^0}(\mathcal{A}^0)$. Descartamos todas las celdas tales que γ tiene alguna coordenada negativa. Por las Observaciones 2.4 y 2.8, $\mathcal{I}$ es el conjunto de todos los $I \subset \{1, \ldots, n\}$ tales que existe $(\gamma, 1)$ entre las normales interiores calculadas y no descartadas tal que $\gamma_i > 0$ si y solo si $i \in I$.

En el paso 2 calculamos este conjunto $\mathcal{I}$ y, para cada $I \in \mathcal{I}$, el conjunto S_I de todas las celdas mixtas de $S_{\omega^I}(\mathcal{A}^I)$. A partir del conjunto de las celdas mixtas de $S_\omega(\mathcal{A}^0)$ del input, por el Lema 2.10, tomando una celda $C \in S_{\omega^0}(\mathcal{A}^0)$ para cada $I \in \mathcal{I}$ cuya normal asociada tiene todas sus coordenadas no negativas y $\{i \mid \gamma_i > 0\} = I$, se tiene que $S_I = \{\pi_I(D) \mid D \in S_\omega(C)$ celda mixta$\}$.

Observación 2.11 *Cada I en el conjunto $\mathcal{I}$ corresponde al menos a una de las celdas $C \in S_{\omega^0}(\mathcal{A}^0)$ que contribuyen al cálculo del volumen mixto estable de [43].*

En el paso 3, elegimos un sistema G con los mismos soportes $\mathcal{A}_1, \ldots, \mathcal{A}_n$ que el sistema F tomando sus coeficientes en $\mathbb{Z}$ al azar.

Para cada $I \in \mathcal{I}$, en el paso 4 consideramos $J_I = \{j \in \{1, \ldots, n\} \mid \exists \alpha \in \mathcal{A}_j : \alpha_i = 0 \; \forall\, i \in I\}$. En el caso en que $\#J_I \neq n - \#I$, descartamos I. Si $\#J_I = n - \#I$, consideramos los sistemas F_I, G_I y H_I como fueron introducidos en la Definición 2.6. Observamos que $H_I = (1-T)F_I + TG_I$. Para hallar los ceros de H_I en $(\overline{\mathbb{C}(T)}^*)^{n-\#I}$, en primer lugar buscamos los ceros en $(\mathbb{C}^*)^{n-\#I}$ del sistema genérico G_I, que tiene $n - \#I$ ecuaciones en $n - \#I$ variables. Éstos se obtienen mediante el algoritmo `ToricSolve` (Algoritmo 2.3). Este algoritmo toma como input los polinomios del sistema genérico G_I, sus soportes $\mathcal{A}^I$ y las celdas mixtas de la subdivisión mixta fina $S_{\omega^I}(\mathcal{A}^I)$. Estas celdas son exactamente los elementos del conjunto S_I calculado en el paso 2. El algoritmo `ToricSolve` produce como output una resolución geométrica del conjunto de ceros de G_I en $(\mathbb{C}^*)^{n-\#I}$. En el proceso de este algoritmo es necesario elegir una forma lineal genérica μ_I. Tomamos una única forma lineal $\mu = \sum_{1 \leq l \leq n} \mu_l X_l$, donde los coeficientes de μ se eligen al azar en un conjunto de enteros suficientemente grande y, para todo $I \in \mathcal{I}$, usaremos $\mu_I = \sum_{l \notin I} \mu_l X_l$ para hallar la resolución geométrica de los ceros de G_I. A partir de la resolución geométrica obtenida y, como G_I es un sistema genérico, se calcula una resolución geométrica de los ceros de H_I en $(\overline{\mathbb{C}(T)}^*)^{n-\#I}$ respecto a la forma lineal μ_I como en [45, Section 6.1]. Llamamos a este proceso `NewtonHenselLifting` (ver la Sección 1.4.2). Insertando polinomios nulos en las coordenadas indexadas por I en la resolución geométrica de los ceros de H_I obtenemos una resolución geométrica respecto a la forma lineal μ_I de un conjunto finito de puntos

que contiene los ceros aislados de H en O_I. Como $\mu_I(x) = \mu(x)$ para todo $x \in O_I$, ésta es una resolución geométrica de ese mismo conjunto de puntos respecto a la forma lineal μ.

En el paso 5 obtenemos una única resolución geométrica $R = (Q(T,U), w_1(T,U), \ldots, w_n(T,U))$ que representa todos los ceros aislados de H en $\overline{\mathbb{C}(T)}^n$ uniendo las resoluciones geométricas obtenidas en el paso anterior como se explica en la Sección 1.1.2.

En el último paso calculamos el límite de la resolución geométrica R cuando $T \to 0$, siguiendo el procedimiento de [45, Section 6.2]. Para ello, calculamos $a(U) = \gcd(Q(0,U), \frac{\partial Q}{\partial U}(0,U))$ y los polinomios $q(U) = \frac{Q(0,U)}{a(U)}$, $b(U) = (\frac{\frac{\partial Q}{\partial U}(0,U)}{a(U)})^{-1}$ (mód $q(U)$), y $v_j(U) = b(U)\frac{w_j(0,U)}{a(U)}$ (mód $q(U)$) $(1 \leq j \leq n)$. Entonces, $r = (q, v_1, \ldots, v_n)$ es una resolución geométrica de un conjunto finito de puntos que contiene todos los ceros aislados en $\mathbb{C}^n$ del sistema F.

A continuación resumimos el algoritmo descripto, al que llamamos `AffineSolve`:

Algoritmo 2.12 `AffineSolve`

INPUT: Un sistema de polinomios $F = (f_1, \ldots, f_n)$ en $\mathbb{Q}[X_1, \ldots, X_n]$ con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$ codificados en forma rala, y las celdas mixtas de una subdivisión mixta fina $S_\omega(\mathcal{A}^0)$ que refina $S_{\omega^0}(\mathcal{A}^0)$.

1. *Para toda celda mixta $D \in S_\omega(\mathcal{A}^0)$:*
   a) *Hallar la normal interior $(\gamma, 1)$ de $Conv(D(\omega^0))$.*
   b) *Si alguna coordenada de γ es negativa, descartar D y γ.*
2. *Calcular $\mathcal{I} = \{I \subset \{1, \ldots, n\} \mid \exists \gamma$ tal que $\gamma_i > 0 \iff i \in I\}$ y, para cada $I \in \mathcal{I}$, el conjunto S_I de todas las celdas mixtas de $S_{\omega^I}(\mathcal{A}^I)$.*
3. *Elegir al azar coeficientes en $\mathbb{Z}$ para un sistema de polinomios $G = (g_1, \ldots, g_n)$ con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ y para una forma lineal $\mu = \sum_{1 \leq l \leq n} \mu_l X_l$.*
4. *Para cada $I \in \mathcal{I}$ tal que $\#J_I = n - \#I$:*
   a) *Aplicar la subrutina* `ToricSolve` *usando las celdas de S_I para hallar una resolución geométrica r_I asociada a la forma lineal $\mu_I = \sum_{l \notin I} \mu_l X_l$ de los ceros comunes de G_I en $(\mathbb{C}^*)^{n-\#I}$.*

b) Aplicar la subrutina `NewtonHenselLifting` *a* r_I *para hallar una resolución geométrica* R_I *de los ceros comunes en* $(\overline{\mathbb{C}(T)}^*)^{n-\#I}$ *de* H_I *.*

c) Insertar en R_I *ceros en las coordenadas indexadas por* I *para obtener una resolución geométrica* $\widetilde{R}_I$ *de un conjunto finito de puntos que contiene a los ceros comunes aislados de* H *en* O_I*.*

5. *A partir de* $(\widetilde{R}_I)_{I\in\mathcal{I}}$*, calcular una única resolución geométrica* R *de un conjunto finito de puntos que contiene a los ceros aislados de* H *en* $\overline{\mathbb{C}(T)}^n$*.*

6. *Calcular la resolución geométrica* $r = \lim_{T\to 0} R$*.*

OUTPUT: La resolución geométrica r *de un conjunto finito de puntos que contiene los ceros aislados en* $\mathbb{C}^n$ *de* $F = (f_1, \ldots, f_n)$*.*

Teorema 2.13 *Sea* $F = (f_1, \ldots, f_n)$ *un sistema de polinomios en* $\mathbb{Q}[X_1, \ldots, X_n]$ *con soportes* $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ *en* $(\mathbb{Z}_{\geq 0})^n$*. El algoritmo* `AffineSolve` *es un procedimiento probabilístico que, tomando como input la codificación rala de* F *y las celdas mixtas de una subdivisión mixta fina adecuada de* $\mathcal{A}^0 = (\mathcal{A}_1 \cup \{0\}, \ldots, \mathcal{A}_n \cup \{0\})$*, calcula una resolución geométrica de un conjunto finito de puntos que contiene los ceros aislados en* $\mathbb{C}^n$ *del sistema* F *con complejidad*

$$O(n^\Omega \Gamma + (n^3 N \log(d) + n^{\Omega+1}) M(\mathcal{D})(M(\Upsilon)(M(\mathcal{D}) + M(\mathcal{E})) + M(\mathcal{E}'))),$$

donde

- Γ *es la cantidad de celdas mixtas en* $S_\omega(\mathcal{A}^0)$*,*
- $N := \sum_{1\leq j\leq n} \#\mathcal{A}_j$*,*
- $d := \max_{1\leq j\leq n}\{\deg(f_j)\}$*,*
- $\mathcal{D} := \mathcal{SM}(\mathcal{A})$*,*
- $\Upsilon := \max\{\|\eta\|\}$ *donde el máximo se toma sobre todas las normales primitivas asociadas a celdas mixtas en* $S_\omega(\mathcal{A}^0)$*,*
- $\mathcal{E} := \mathcal{SM}(\Delta \times \{0\}, \mathcal{A}_1(\omega_1), \ldots, \mathcal{A}_n(\omega_n))$ *(donde* Δ *es el conjunto de vértices del símplex standard de* $\mathbb{R}^n$*),*
- $\mathcal{E}' := \mathcal{SM}(\{0\} \times \Delta, \{0,1\} \times \mathcal{A}_1, \ldots, \{0,1\} \times \mathcal{A}_n)$*.*

Demostración: Solo resta estimar la complejidad del algoritmo dado que su correctitud es consecuencia de los resultados probados en la Sección 2.2.

En el primer paso, cada normal $(\gamma, 1)$ asociada a una celda puede calcularse con $O(n^\Omega)$ operaciones usando técnicas standard de álgebra lineal efectiva (ver [32, Chapter 12]). Recorremos cada coordenada de $(\gamma, 1)$ y la comparamos con cero, descartándola si alguna de sus coordenadas es negativa con $O(n)$ operaciones, lo que no cambia el orden de complejidad.

Por la Observación 2.11 y sabiendo que el volumen mixto de cada celda C que contribuye al cálculo de $\mathcal{SM}(\mathcal{A})$ es la suma de los volúmenes mixtos de las celdas mixtas de $S_\omega(\mathcal{A}^0)$ contenidas en C, la cantidad de celdas mixtas no descartadas en el primer paso está acotada superiormente por $\mathcal{SM}(\mathcal{A})$. Luego, el cálculo del conjunto $\mathcal{I}$ y las celdas de S_I para todo $I \in \mathcal{I}$ puede llevarse a cabo en $O(n \log(\mathcal{SM}(\mathcal{A}))\mathcal{SM}(\mathcal{A}))$ operaciones aplicando un algoritmo de ordenamiento standard: Para cada celda mixta $D \in S_\omega(\mathcal{A}^0)$ que no descartamos en el primer paso, tomemos la terna (D, γ, χ_γ), donde $(\gamma, 1)$ es la normal interior de $Conv(D(\omega^0))$ y χ_γ se define como $(\chi_\gamma)_i = 0$ si $\gamma_i = 0$ y $(\chi_\gamma)_i = 1$ si $\gamma_i > 0$. Ordenamos estas ternas lexicográficamente en la coordenada χ_γ. Para cada $\chi = \chi_\gamma$ distinto, el algoritmo agrega $I = \{k \mid \chi_k = 1\}$ al conjunto $\mathcal{I}$, toma el primer elemento con tercera coordenada χ de la lista de ternas ordenadas (D, γ, χ) y forma el conjunto S_I a partir de todos los otros pares (D', γ, χ) con el mismo γ en la segunda coordenada. Se descartan todas las otras ternas con tercera coordenada χ y segunda coordenada distinta de γ.

Para estimar el costo de calcular $\widetilde{R}_I$ para cada $I \in \mathcal{I}$ vamos a usar los cálculos de complejidad de [45, Theorem 6.2]: Con la notación e hipótesis anteriores, para cada $I \in \mathcal{I}$ el paso 4 tiene un costo total de

$$O(((n - \#I)^3 N_I \log d_I + (n - \#I)^{\Omega+1}) M(\mathcal{D}_I)(M(\Upsilon_I)(M(\mathcal{D}_I) + M(\mathcal{E}_I)) + M(\mathcal{E}'_I))),$$

donde

- $N_I := \sum_{j \in J_I} \#(\mathcal{A}_j^I)$,
- $d_I := \text{máx}_{j \in J_I}\{\deg((f_j)_I)\}$,
- $\mathcal{D}_I := \mathcal{MV}_{n-\#I}(\mathcal{A}^I)$,
- $\Upsilon_I := \text{máx}\{\|\eta_I\|\}$ tomando el máximo sobre todas las normales primitivas asociadas a celdas mixtas de la subdivisión $S_{\omega^I}(\mathcal{A}^I)$,
- $\mathcal{E}_I := \mathcal{MV}_{n-\#I+1}(\Delta \times \{0\}, (\mathcal{A}_j^I(\omega_j^I))_{j \in J_I})$, donde Δ es el conjunto de vértices del símplex standard de $\mathbb{R}^{n-\#I}$,
- $\mathcal{E}'_I := \mathcal{MV}_{n-\#I+1}(\{0\} \times \Delta, (\{0,1\} \times \mathcal{A}_j^I)_{j \in J_I})$.

La complejidad total del paso 4 es la suma de las complejidades anteriores. Para acotar esta suma, observar que para todo $I \in \mathcal{I}$ vale que $N_I \leq N$, $d_I \leq d$ y $\Upsilon_I \leq \Upsilon$. Para ver que $\sum_{I\in\mathcal{I}} \mathcal{D}_I \leq \mathcal{D}$ (y por lo tanto $\sum_{I\in\mathcal{I}} M(\mathcal{D}_I) \leq M(\mathcal{D})$), notemos que por la Observación 2.11 a cada $I \in \mathcal{I}$ le corresponde al menos una celda mixta C cuya normal asociada tiene coordenadas no negativas. Pero en la demostración del Lema 2.9 vimos que $\mathcal{MV}_n(C) = \mathcal{MV}_{n-\#I}(\mathcal{A}^I)\mathcal{MV}_{\#I}(\pi_{\overline{I}}(C_{j_1}), \ldots, \pi_{\overline{I}}(C_{j_{\#I}})) \geq \mathcal{MV}_{n-\#I}(\mathcal{A}^I)$, donde notamos $\overline{I} = \{1, \ldots, n\}\backslash I$ y $\{j_1, \ldots, j_{\#I}\}$ para los subíndices de los polinomios que se descartan al evaluar $X_i = 0$ para todo $i \in I$. Entonces $\sum_{I\in\mathcal{I}} \mathcal{D}_I \leq \sum \mathcal{MV}_n(C) \leq \mathcal{D}$ donde la segunda suma es, siguiendo la Observación 2.11, sobre las celdas C correspondientes a cada $I \in \mathcal{I}$. Además, si para cada $I \in \mathcal{I}$ tomamos una celda C asociada que contribuye al cálculo del volumen mixto estable $\mathcal{SM}(\mathcal{A})$, y consideramos la celda correspondiente en el cálculo de $\mathcal{SM}((\Delta \times \{0\}, \mathcal{A}_1(\omega_1), \ldots, \mathcal{A}_n(\omega_n)))$, se deduce que $\sum_{I\in\mathcal{I}} \mathcal{E}_I \leq \mathcal{E}$. De igual forma se puede ver que $\sum_{I\in\mathcal{I}} \mathcal{E}'_I \leq \mathcal{E}'$. A partir de estas cotas superiores, la complejidad total de calcular las resoluciones geométricas $\widetilde{R}_I$ de los ceros aislados de H en O_I para todo $I \in \mathcal{I}$ es $O((n^3 N \log d + n^{\Omega+1})M(\mathcal{D})(M(\Upsilon)(M(\mathcal{D}) + M(\mathcal{E})) + M(\mathcal{E}')))$.

Sea U una nueva variable tal que los polinomios que conforman cada resolución geométrica $\widetilde{R}_I$ son elementos de $\mathbb{Q}[T][U]$. Para unir todas estas resoluciones geométricas $\widetilde{R}_I$ en una única resolución geométrica R asociada a μ (ver la Sección 1.1.2) usamos la estrategia de división de [32, Algorithm 10.3]. Notar que para cada $I \in \mathcal{I}$, el grado en U de los $n+1$ polinomios de la resolución geométrica $\widetilde{R}_I$ es a lo sumo $\mathcal{D}_I$ y sus coeficientes tienen grados en T acotados por $\mathcal{E}'_I$. Entonces, los polinomios involucrados en cálculos intermedios tienen grado en U acotado por $\mathcal{D}$ y sus coeficientes tienen grados en T acotados por $\mathcal{E}'$. Usando [32, Lemma 10.4], el algoritmo requiere de $O(nM(\mathcal{D}))$ operaciones en $\mathbb{Q}[T]$ y por lo tanto, la complejidad del paso 5 es de orden $O(nM(\mathcal{D})M(\mathcal{E}'))$.

El último paso, siguiendo [45, Section 6.2] como se explicó antes, tiene una complejidad del orden de $O(nM(\mathcal{D})\mathcal{E}')$. □

2.3.2. Ejemplo

A continuación ilustramos los distintos pasos del Algoritmo 2.12 en el sistema del Ejemplo 1.8 expuesto en el Capítulo 1.

Ejemplo 2.14 Consideramos el sistema

$$P = \begin{cases} p_1(X_1, X_2) = aX_2 + bX_2^2 + cX_1X_2^3 \\ p_2(X_1, X_2) = dX_1 + eX_1^2 + fX_1^3X_2 \end{cases}$$

con coeficientes genéricos a, b, c, d, e, f en $\mathbb{Q}$. La familia de soportes del sistema es $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, con $\mathcal{A}_1 = \{(0,1), (0,2), (1,3)\}$, $\mathcal{A}_2 = \{(1,0), (2,0), (3,1)\}$. Para este sistema, en el Ejemplo 1.19 graficamos la subdivisión $S_{\omega^0}(\mathcal{A}^0)$ compuesta por las celdas $C^{(0)}, \ldots, C^{(7)}$, que se muestra en la Figura 2.1.

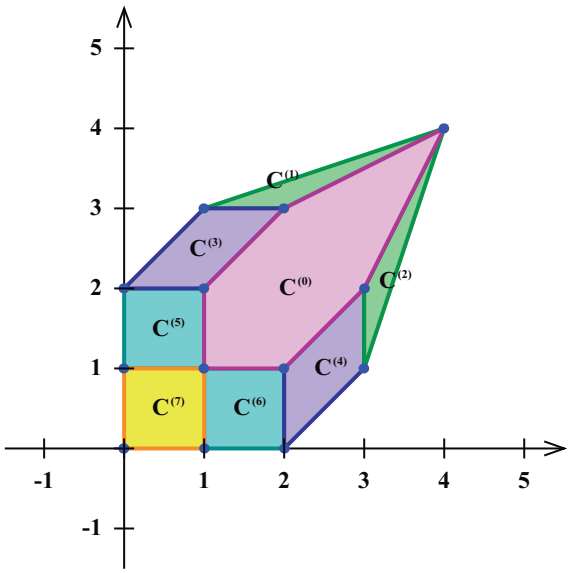


Figura 2.1: Subdivisión de $\mathcal{A}^0$ inducida por ω^0

Una subdivisión mixta fina puede obtenerse a partir de la función de levantamiento $\omega = (\omega_1, \omega_2)$ tal que

- $\omega_1(0,1) = 3, \omega_1(0,2) = 6, \omega_1(1,3) = 5$ y $\omega_1(0,0) = 11$.
- $\omega_2(1,0) = 1, \omega_2(2,0) = 3, \omega_2(3,1) = 2$ y $\omega_2(0,0) = 11$.

Las facetas inferiores de la suma de las cápsulas convexas de $\mathcal{A}^0 = (\mathcal{A}_1^0, \mathcal{A}_2^0)$ levantadas por ω y la subdivisión de $\mathcal{A}^0$ resultante de proyectarlas a las primeras dos coordenadas se muestran en la Figura 2.2 a continuación. Puede observarse claramente en las Figuras 2.1 y 2.2 que la subdivisión $S_\omega(\mathcal{A}^0)$ refina a $S_{\omega^0}(\mathcal{A}^0)$.
El input del algoritmo, en este caso, son los polinomios p_1 y p_2 y las celdas mixtas de la subdivisión $S_\omega(\mathcal{A}^0)$. Las cápsulas convexas de las celdas de $S_\omega(\mathcal{A}^0)$ fueron graficadas en la Figura 2.2. Las celdas mixtas para esa subdivisión son $D^{(0)}, D^{(3)}, D^{(4)}, D^{(5)}, D^{(6)}, D^{(7)}$.

En el primer paso del algoritmo, calculamos las normales interiores $(\gamma, 1)$ de $Conv(D^{(l)}(\omega^0))$ para toda $D^{(l)}$ del input $(0 \leq l \leq 9)$, y descartamos aquellas celdas cuya normal asociada tiene alguna coordenada negativa. En la tabla que sigue mostramos las normales asociadas a cada celda $D^{(l)}$ de $S_\omega(\mathcal{A}^0)$, la celda de $S_{\omega^0}(\mathcal{A}^0)$ en la que $D^{(l)}$ está contenida, y analizamos en cada caso si $D^{(l)}$ aporta un conjunto I a $\mathcal{I}$.

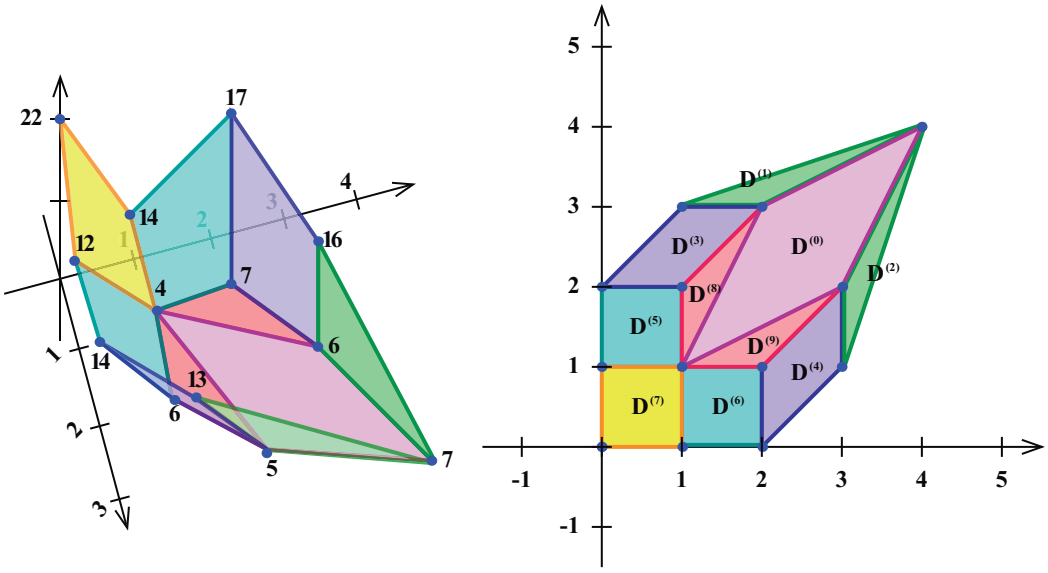


Figura 2.2: Subdivisión de $\mathcal{A}^0$ inducida por ω

Celda	Mixta?	Normal γ	Sirve?	$I \in \mathcal{I}$	S_I
$D^{(0)} \subseteq C^{(0)}$	Sí	$(0,0,1)$	sí	$I = \emptyset$	$D^{(0)} \in S_\emptyset$
$D^{(1)} \subseteq C^{(1)}$	No	no es mixta	no		
$D^{(2)} \subseteq C^{(2)}$	No	no es mixta	no		
$D^{(3)} \subseteq C^{(3)}$	Sí	$(1,-1,1)$	no, $\gamma_2 < 0$		
$D^{(4)} \subseteq C^{(4)}$	Sí	$(-1,1,1)$	no, $\gamma_1 < 0$		
$D^{(5)} \subseteq C^{(5)}$	Sí	$(1,0,1)$	sí	$I = \{1\}$	$D^{(5)} \in S_{\{1\}}$
$D^{(6)} \subseteq C^{(6)}$	Sí	$(0,1,1)$	sí	$I = \{2\}$	$D^{(6)} \in S_{\{2\}}$
$D^{(7)} \subseteq C^{(7)}$	Sí	$(1,1,1)$	sí	$I = \{1,2\}$	$D^{(7)} \in S_{\{1,2\}}$
$D^{(8)} \subseteq C^{(0)}$	No	no es mixta	no		
$D^{(9)} \subseteq C^{(0)}$	No	no es mixta	no		

Como muestra la tabla, a partir de las celdas $D^{(0)}, D^{(5)}, D^{(6)}$ y $D^{(7)}$ que obtenemos en el paso 1, en el paso 2 construimos $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$, y para cada $I \in \mathcal{I}$, el conjunto de celdas S_I:

$$S_\emptyset = \{D^{(0)}\},\ S_{\{1\}} = \{D^{(5)}\},\ S_{\{2\}} = \{D^{(6)}\} \text{ y } S_{\{1,2\}} = \{D^{(7)}\}.$$

Entonces, para cada $I \in \mathcal{I}$, los sistemas asociados a resolver sobre $\mathbb{C}^*$ en el paso 4 son:

I	Sistemas asociados	$\pi_I(D^{(l)}) \in S_I$
$\emptyset$	$\begin{cases} aX_2 + bX_2^2 + cX_1X_2^3 \\ dX_1 + eX_1^2 + fX_1^3X_2 \end{cases}$	$\pi_\emptyset(D^{(0)}) = (\{(0,1),(1,3)\},\{(1,0),(3,1)\})$
$\{1\}$	$aX_2 + bX_2^2$	$\pi_{\{1\}}(D^{(5)}) = \{1,2\}$
$\{2\}$	$dX_1 + eX_1^2$	$\pi_{\{2\}}(D^{(6)}) = \{1,2\}$
$\{1,2\}$	$\emptyset$	$\pi_{\{1,2\}}(D^{(7)}) = \emptyset$

Notar que $D^{(0)}, D^{(8)}$ y $D^{(9)}$ forman una subdivisión mixta fina de $C^{(0)}$ pero solo $D^{(0)}$ es una celda mixta. Entonces, por el Lema 2.10, para el sistema asociado al conjunto $\emptyset$ trabajando únicamente con la celda $\pi_\emptyset(D^{(0)})$ de la subdivisión $S_{\omega^\emptyset}(\mathcal{A}^\emptyset)$ podremos encontrar sus soluciones en $(\mathbb{C}^*)^2$. En el caso de los otros tres sistemas asociados, $\pi_I(D^{(l)})$ es exactamente el soporte del sistema.

Sea $F = \begin{cases} X_2 + 2X_2^2 - X_1X_2^3 \\ -X_1 + 3X_1^2 - 2X_1^3X_2 \end{cases}$ el sistema del Ejemplo 1.8. Usaremos este sistema, que resulta de tomar valores concretos para los coeficientes de P, para ilustrar los pasos restantes.

Como el sistema F ya es genérico, en el paso 3 basta con elegir una forma lineal separante, por ejemplo $\mu(X_1, X_2) = X_1 + X_2$, y podemos obviar la deformación homotópica H.

En el paso 4 se resuelven los sistemas F_I asociados a los conjuntos $I \in \mathcal{I}$ y se insertan ceros en las coordenadas correspondientes. Se obtienen así las siguientes resoluciones geométricas:

I	Sistemas asociados F_I	Resolución geométrica de los ceros de F en O_I
$\emptyset$	$\begin{cases} X_2+2X_2^2-X_1X_2^3 \\ -X_1+3X_1^2-2X_1^3X_2 \end{cases}$	$\left\{\left(\frac{-3U^2+4U+4}{12U^2+22U+14}, \frac{-8U^2-32U-10}{12U^2+22U+14}\right) \mid 4U^3+11U^2+14U+2=0\right\}$
$\{1\}$	$X_2 + 2X_2^2$	$\{(0, -\frac{1}{2}) \mid 2U + 1 = 0\}$
$\{2\}$	$-X_1 + 3X_1^2$	$\{(\frac{1}{3}, 0) \mid 3U - 1 = 0\}$
$\{1,2\}$	$\emptyset$	$\{(0,0) \mid U = 0\}$

En el paso 5 obtenemos una única resolución geométrica del conjunto de los ceros aislados de F en $\mathbb{C}^2$ uniendo las cuatro resoluciones geométricas del paso anterior:

$$\left\{\left(\frac{-10U^5+47U^4+70U^3+18U^2-2U}{144U^5+350U^4+364U^3+45U^2-24U-2}, \frac{-60U^5-229U^4-115U^3+30U^2+12U}{144U^5+350U^4+364U^3+45U^2-24U-2}\right) \mid 24U^6+70U^5+91U^4+15U^3-12U^2-2U=0\right\}.$$

2.3.3. Comparación con algoritmos previos

Una de las ventajas del Algoritmo 2.12 respecto a los algoritmos de [43] y [31] es que requiere resolver sistemas en menos variables. Como los tres algoritmos encuentran los ceros aislados de sistemas arbitrarios a partir de deformar homotópicamente soluciones de un sistema genérico, basta considerar el caso de un sistema P genérico.

Para cada $I \subset \{1,\dots,n\}$ que analiza nuestro algoritmo tal que $\mathcal{MV}_{n-\#I}(\mathcal{A}^I) > 0$, el sistema P_I es cuadrado y tiene ceros aislados en $(\mathbb{C}^*)^{n-\#I}$. Por la construcción del conjunto $\mathcal{I}$, existe al menos una celda C de $S_{\omega^0}(\mathcal{A}^0)$ con volumen mixto positivo y normal asociada $(\gamma,1)$ tal que $\gamma_i > 0$ si $i \in I$ y $\gamma_i = 0$ si $i \notin I$. Se puede ver que el sistema P_C^0 tiene la estructura probada en el Lema 2.7 aún si P no tiene ceros aislados que están en O_I pero P_I es un sistema cuadrado con ceros aislados en $(\mathbb{C}^*)^{n-\#I}$. De la misma forma, si P_I es un sistema cuadrado con ceros aislados en $(\mathbb{C}^*)^{n-\#I}$ y $C \in S_{\omega^0}(\mathcal{A}^0)$ una celda que cumple las hipótesis del Lema 2.9, entonces para todo ξ cero de P_I en $(\mathbb{C}^*)^{n-\#I}$ existe un cero aislado $\widetilde{\xi}$ de P_C^0 tal que $\pi_I(\widetilde{\xi}) = \xi$. Así, para cada $I \in \mathcal{I}$:

- el algoritmo `AffineSolve` resuelve exactamente un sistema P_I de $n-\#I$ ecuaciones en $n-\#I$ variables, mientras que los algoritmos de [43] y [31] resuelven *al menos* un sistema P_C^0 de n polinomios en n variables. Podría eventualmente haber más de una celda cuya normal asociada corresponda a I que implique resolver más de un sistema (ver el Ejemplo 2.16 más abajo).
- P_I es un subsistema de P_C^0 y resolver P_C^0 implica resolver P_I.
- Por cada cero aislado ξ de P_I que permite hallar un cero $\varphi_I(\xi)$ de P, los algoritmos de [43] y [31] encuentran *al menos* un cero aislado de P_C^0 que permite hallar $\varphi_I(\xi)$ (ver el Ejemplo 2.15 a continuación).

Ejemplo 2.15 Sea P un sistema genérico con la misma familia de soportes $\mathcal{A}$ que el sistema Katsura4 del PoSSo test suite (ver [31, Example 6]), es decir

$$P = \begin{cases} a_{11}X_1^2 + a_{12}X_2^2 + a_{13}X_3^2 + a_{14}X_4^2 + a_{15}X_5^2 + a_{16}X_5 \\ a_{21}X_1X_2 + a_{22}X_2X_3 + a_{23}X_3X_4 + a_{24}X_4X_5 + a_{25}X_4 \\ a_{31}X_1X_3 + a_{32}X_2X_4 + a_{33}X_4^2 + a_{34}X_3X_5 + a_{35}X_3 \\ a_{41}X_1X_4 + a_{42}X_3X_4 + a_{43}X_2X_5 + a_{44}X_2 \\ a_{51}X_1 + a_{52}X_2 + a_{53}X_3 + a_{54}X_4 + a_{55}X_5 + a_{56} \end{cases}.$$

En [31, Example 6] calculan el volumen mixto y el volumen mixto estable de la familia de soportes $\mathcal{A}$. Como $\mathcal{MV}_5(\mathcal{A}) = 12$ y $\mathcal{SM}(\mathcal{A}) = 16$, genéricamente el sistema tiene 12 ceros aislados en $(\mathbb{C}^*)^5$ y a lo sumo 16 ceros aislados en $\mathbb{C}^5$ contados con su multiplicidad.

Además, muestran que existen solo tres celdas $C^{(1)}, C^{(2)}$ y $C^{(3)}$ en $S_{\omega^0}(\mathcal{A}^0)$ con volumen mixto positivo y tales que sus normales asociadas $(\gamma^{(i)}, 1)$ tienen todas sus coordenadas no negativas. Éstas son:

$$(\gamma^{(1)}, 1) = (0,0,0,0,0,1),\ (\gamma^{(2)}, 1) = (0,1,0,1,0,1) \text{ y } (\gamma^{(3)}, 1) = (0,1,1,1,0,1).$$

Aplicando el algoritmo de [31], deben resolverse tres sistemas en cinco variables asociados a las tres celdas. En el caso de nuestro algoritmo, en cambio, los conjuntos $I \in \mathcal{I}$ a tener en cuenta son:

$$I^{(1)} = \emptyset,\ I^{(2)} = \{2,4\} \text{ y } I^{(3)} = \{2,3,4\}.$$

Tenemos entonces que resolver también tres sistemas P_I, pero solo para el sistema P se buscan los ceros aislados en $(\mathbb{C}^*)^5$ (éste es el mismo sistema que se analizaría en el caso del algoritmo de [31] asociado a $C^{(1)}$). Los otros dos sistemas

$$P_{I^{(2)}} = \begin{cases} a_{11}X_1^2 + a_{13}X_3^2 + a_{15}X_5^2 + a_{16}X_5 \\ a_{31}X_1X_3 + a_{34}X_3X_5 + a_{35}X_3 \\ a_{51}X_1 + a_{53}X_3 + a_{55}X_5 + a_{56} \end{cases}$$

y

$$P_{I^{(3)}} = \begin{cases} a_{11}X_1^2 + a_{15}X_5^2 + a_{16}X_5 \\ a_{51}X_1 + a_{55}X_5 + a_{56} \end{cases}$$

dependen de 3 y 2 variables y se resuelven en $(\mathbb{C}^*)^3$ y $(\mathbb{C}^*)^2$, insertando finalmente ceros en las coordenadas indexadas por los conjuntos $I^{(2)}$ e $I^{(3)}$ respectivamente, para obtener todos los ceros aislados de P.

El algoritmo `AffineSolve` no solo requiere resolver sistemas asociados con menos variables que los algoritmos de [43] y [31], sino que cada uno de estos sistemas es un subsistema de al menos uno de los sistemas a resolver en esos algoritmos previos. El ejemplo que sigue ilustra estas dos ventajas.

Ejemplo 2.16 Sea P el sistema genérico

$$P = \begin{cases} a_{11}X_1^2 + a_{12}X_1^2X_2^2 + a_{13}X_1X_3 + a_{14}X_1X_2^2X_3 + a_{15}X_3^4 + a_{16}X_2^2X_3^4 \\ a_{21}X_1^4 + a_{22}X_1^4X_2^2 + a_{23}X_1^2X_3 + a_{24}X_1^2X_2^2X_3 + a_{25}X_3^4 + a_{26}X_2^2X_3^4 \\ a_{31}X_1 + a_{32}X_1X_2^2 + a_{33} + a_{34}X_2^2 + a_{35}X_3 + a_{36}X_2^2X_3 \end{cases}.$$

Tanto el algoritmo de [43] como el de [31] requieren resolver dos subsistemas en 3 variables asociados a dos celdas $C^{(1)}$ y $C^{(2)}$ de $S_{\omega^0}(\mathcal{A}^0)$ con volumen mixto positivo y normal asociada con coordenadas no negativas. Sin embargo, como estas normales son $\gamma^{(1)} = (\frac{3}{4}, 0, \frac{1}{4}, 1)$ y $\gamma^{(2)} = (\frac{1}{3}, 0, \frac{1}{3}, 1)$, para una subdivisión $S_\omega(\mathcal{A}^0)$ mixta fina existen celdas mixtas $D^{(1)}$ y

$D^{(2)}$ de $S_\omega(\mathcal{A}^0)$ tales que $D^{(l)} \subset C^{(l)}$ $(l = 1, 2)$ y a ambas $D^{(l)}$ les corresponde el conjunto $I = \{1, 3\}$ de los subíndices de las coordenadas no nulas de las normales.

Para calcular los ceros aislados del sistema P en O_I (es decir, donde $X_1 = X_3 = 0$ y $X_2 \neq 0$), el algoritmo `AffineSolve` resuelve el sistema que resulta de evaluar $X_1 = 0$ y $X_3 = 0$ en el sistema original y descartar los polinomios que se anulan. En este caso, esto es buscar los ceros de

$$P_I = a_{33} + a_{34}X_2^2.$$

Las soluciones de esta ecuación permiten obtener los dos ceros aislados de P en O_I.

Por otro lado, el algoritmo de [43] (al igual que el algoritmo de [31]), requiere resolver los sistemas asociados a las celdas $C^{(1)}$ y $C^{(2)}$:

$$P_{C^{(1)}} = \begin{cases} a_{13}X_1X_3 + a_{14}X_1X_2^2X_3 + a_{15}X_3^4 + a_{16}X_2^2X_3^4 + a_{10} \\ a_{25}X_3^4 + a_{26}X_2^2X_3^4 + a_{20} \\ a_{33} + a_{34}X_2^2 \end{cases}$$

$$P_{C^{(2)}} = \begin{cases} a_{11}X_1^2 + a_{12}X_1^2X_2^2 + a_{13}X_1X_3 + a_{14}X_1X_2^2X_3 \\ a_{23}X_1^2X_3 + a_{24}X_1^2X_2^2X_3 + a_{20} \\ a_{33} + a_{34}X_2^2 \end{cases}$$

con a_{10} y a_{20} constantes genéricas. Como $\mathcal{MV}_3(C^{(1)}) = 8$ y $\mathcal{MV}_3(C^{(2)}) = 6$, por el Teorema de Bernstein, estos sistemas tienen 8 y 6 ceros aislados respectivamente en $(\mathbb{C}^*)^3$. El algoritmo de [43] calcula entonces estas 14 soluciones y reemplaza luego por cero las coordenadas X_1 y X_3. Pero, como la tercera ecuación de cada sistema es exactamente P_I, al hacer esto se consiguen las únicas dos soluciones en O_I de P que nuestro algoritmo encuentra resolviendo solo la ecuación $P_I = 0$.

2.4. Cantidad de soluciones afines aisladas

En esta sección, presentamos una nueva cota superior para la cantidad de soluciones aisladas de un sistema ralo de n ecuaciones en n variables con soportes prefijados que mejora las anteriores (ver [54], [59] y [43]). Nuestra cota es exacta para sistemas genéricos, contando las soluciones sin multiplicidades y, para sistemas arbitrarios, es una cota superior para la cantidad de ceros aislados del sistema. Asimismo, damos una condición combinatoria, equivalente a la dada en [59, Lemma 3], que caracteriza cuándo estos sistemas tienen finitos ceros en $\mathbb{C}^n$.

2.4.1. La cota

Consideremos en primer lugar un sistema P genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$. Como consecuencia del desarrollo realizado en la sección anterior, podemos deducir que la cantidad de ceros aislados del sistema P es menor o igual a la cantidad de puntos que halla el algoritmo `AffineSolve`. Este número es exactamente $\sum \mathcal{MV}_{n-\#I}(\mathcal{A}^I)$, donde la suma es sobre los conjuntos $I \subset \{1, \ldots, n\}$ tales que $\#J_I = n - \#I$ y existe una celda mixta D de la subdivisión $S_\omega(\mathcal{A}^0)$ asociada a una función de levantamiento ω genérica como en (2.1) tal que la normal interior $(\gamma, 1)$ de $Conv(D(\omega^0))$ cumple $\gamma_i > 0$ si $i \in I$ y $\gamma_i = 0$ si $i \notin I$. Sin embargo, alguno de los puntos hallados por el algoritmo puede no ser un cero aislado de P. Caractericemos cuándo los ceros aislados de P_I se corresponden con ceros aislados de P.

Lema 2.17 *Sean P un sistema genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$ e $I \subset \{1, \ldots, n\}$ tal que P_I tiene ceros aislados en $(\mathbb{C}^*)^{n-\#I}$. Entonces existe un cero aislado ξ de P_I en $(\mathbb{C}^*)^{n-\#I}$ tal que $\varphi_I(\xi)$ es un cero no aislado de P si y solo si existe $\widetilde{I} \subset I$ tal que $\#J_{\widetilde{I}} < n - \#\widetilde{I}$. En ese caso, para todo cero aislado ξ de P_I en $(\mathbb{C}^*)^{n-\#I}$, se tiene que $\varphi_I(\xi)$ es un cero no aislado de P en $\mathbb{C}^n$.*

Demostración: Observar en primer lugar que, como P_I es un sistema genérico y tiene ceros aislados en $(\mathbb{C}^*)^{n-\#I}$, entonces $\#J_I = n - \#I$.

Por un lado, sean $\widetilde{I} \subset I$ tal que $\#J_{\widetilde{I}} < n - \#\widetilde{I}$ y $\xi \in (\mathbb{C}^*)^{n-\#I}$ un cero aislado de P_I. Luego $\varphi_I(\xi)$ es un cero de P. Como $\widetilde{I} \subset I$, tomando $\widetilde{\xi} := \pi_{\widetilde{I}}(\varphi_I(\xi)) = \varphi_{I \setminus \widetilde{I}}(\xi)$ se obtiene un cero de $P_{\widetilde{I}}$. Sabiendo que $P_{\widetilde{I}}$ es un sistema con más variables que ecuaciones, $\widetilde{\xi}$ es un cero no aislado de $P_{\widetilde{I}}$, y por lo tanto $\varphi_{\widetilde{I}}(\widetilde{\xi}) = \varphi_I(\xi)$ es un cero no aislado de P.

Por otro lado, sea W el conjunto de ceros de P_I en $(\mathbb{C}^*)^{n-\#I}$. Sabiendo que $\varphi_I(W) \subset V(P) \cap \{x \in \mathbb{C}^n \mid x_i \neq 0 \ \forall i \notin I\}$ y $\{x \in \mathbb{C}^n \mid x_i \neq 0 \ \forall i \notin I\}$ es un abierto Zariski denso en $\mathbb{C}^n$, tenemos que el conjunto $V(P) \cap \{x \in \mathbb{C}^n \mid x_i \neq 0 \ \forall i \notin I\}$ tiene infinitos puntos. Pero este conjunto es la unión sobre todo $I' \subset I$ de los ceros de P en $O_{I'}$, con lo cual existe $\widetilde{I} \subset I$ tal que $P_{\widetilde{I}}$ tiene infinitos ceros en $(\mathbb{C}^*)^{n-\#\widetilde{I}}$. Como $P_{\widetilde{I}}$ es un sistema genérico, $\#J_{\widetilde{I}} < n - \#\widetilde{I}$. □

En el ejemplo que sigue, el Lema 2.17 permite descartar soluciones conseguidas a partir de algunos sistemas asociados.

Ejemplo 2.18 Consideramos un sistema genérico P de 3 ecuaciones en 3 variables con soportes $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$, donde $\mathcal{A}_1 = \{(0,0,0), (0,1,0), (0,0,1)\}$, y $\mathcal{A}_2, \mathcal{A}_3$ están incluidos en el subconjunto de $(\mathbb{Z}_{\geq 0})^3$ formado por las ternas con primera coordenada mayor o

igual que 1. Es decir, el sistema es de la forma

$$P = \begin{cases} p_1(X_1, X_2, X_3) = a_1X_2 + b_1X_3 + c_1 \\ p_2(X_1, X_2, X_3) = X_1q_2(X_1, X_2, X_3) \\ p_3(X_1, X_2, X_3) = X_1q_3(X_1, X_2, X_3) \end{cases}$$

donde $q_2, q_3 \in \mathbb{C}[X_1, X_2, X_3]$ son polinomios genéricos no nulos y a_1, b_1, c_1 coeficientes genéricos.

Los subsistemas asociados a $\{1,2\}$ y $\{1,3\}$ tienen como soluciones aisladas en $\mathbb{C}^*$ a $-\frac{c_1}{b_1}$ y $-\frac{c_1}{a_1}$ respectivamente. Sin embargo, los ceros de P que inducen, $(0, 0, -\frac{c_1}{b_1})$ y $(0, -\frac{c_1}{a_1}, 0)$, no son aislados. De hecho, para todo $t \in \mathbb{C}$, $(0, t, -\frac{c_1+a_1t}{b_1})$ es un cero de P.

Si analizamos las condiciones del Lema 2.17, podemos observar que

$$\#J_{\{1,2\}} = 1 = n - \#\{1,2\}, \quad \#J_{\{1,3\}} = 1 = n - \#\{1,3\} \text{ y } \#J_{\{1\}} = 1 < 2 = n - \#\{1\}.$$

De esta forma, como $\{1\}$ es un subconjunto propio de ambos, podemos asegurar que las soluciones inducidas por $\{1,2\}$ y $\{1,3\}$ no son aisladas, como ya habíamos observado.

A partir del Lema 2.17, probamos la siguiente cota para la cantidad de ceros aislados de un sistema polinomial ralo de n ecuaciones en n incógnitas.

Teorema 2.19 *La cantidad de ceros aislados en $\mathbb{C}^n$ de un sistema polinomial ralo de n ecuaciones con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$ es a lo sumo*

$$\mathcal{B}(\mathcal{A}) := \sum \mathcal{MV}_{n-\#I}(\mathcal{A}^I),$$

donde la suma es sobre todos los conjuntos $I \subset \{1, \ldots, n\}$ tales que

- $\#J_I = n - \#I$, *y*
- *para todo $\widetilde{I} \subset I$, $\#J_{\widetilde{I}} \geq n - \#\widetilde{I}$.*

La cota es genéricamente exacta para la cantidad de ceros aislados del sistema en $\mathbb{C}^n$ contados sin multiplicidad.

Demostración: Si P es un sistema genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$, para cada $I \subset \{1, \ldots, n\}$ tal que $\#J_I = n - \#I$, por el Teorema de Bernstein, la cantidad de ceros aislados de P_I en $(\mathbb{C}^*)^{n-\#I}$ es $\mathcal{MV}_{n-\#I}(\mathcal{A}^I)$. Por el Lema 2.17, la cantidad total de soluciones aisladas de P en $\mathbb{C}^n$ es $\mathcal{B}(\mathcal{A})$. Si F es un sistema arbitrario, tomando G un sistema genérico con los mismos soportes, el sistema $H(T, X) = (1 - T)F(X) + TG(X)$ tiene $\mathcal{B}(\mathcal{A})$ ceros aislados en $\overline{\mathbb{C}(T)}^n$ y, a partir de estos ceros, tomando límite cuando T tiende a 0, se obtienen todos los ceros aislados de F (ver la Sección 2.1.1). Por lo tanto, la cantidad de ceros aislados de F es a lo sumo $\mathcal{B}(\mathcal{A})$. □

Observación 2.20 *El volumen mixto estable $\mathcal{SM}(\mathcal{A})$ acota la cantidad de ceros aislados en $\mathbb{C}^n$ contados con multiplicidad de un sistema con soportes $\mathcal{A}$ y, bajo ciertas condiciones sobre $\mathcal{A}$, esta cota es genéricamente exacta (ver el Teorema 1.21). Por otro lado, nuestra cota $\mathcal{B}(\mathcal{A})$ para la cantidad de ceros aislados en $\mathbb{C}^n$ contados sin multiplicidad es genéricamente exacta para familias arbitrarias de soportes. Se deduce que $\mathcal{B}(\mathcal{A}) \leq \mathcal{SM}(\mathcal{A})$.*

El ejemplo que sigue es una variación del Ejemplo 2.14 donde puede observarse que nuestra cota puede ser estrictamente menor que el volumen mixto estable de los soportes.

Ejemplo 2.21 Consideremos el sistema bivariado

$$P = \begin{cases} p_1(X_1, X_2) = aX_2 + bX_2^2 + cX_1^2X_2^3 \\ p_2(X_1, X_2) = dX_1^2 + eX_1^4 + fX_1^6X_2 \end{cases}$$

con coeficientes genéricos a, b, c, d, e, f en $\mathbb{Q}$. La familia de soportes es

$$\mathcal{A} = (\{(0,1),(0,2),(2,3)\}, \{(2,0),(4,0),(6,1)\}).$$

En la Figura 2.3 se puede ver una subdivisión mixta fina de $\mathcal{A}^0$ similar a la del Ejemplo 2.14.

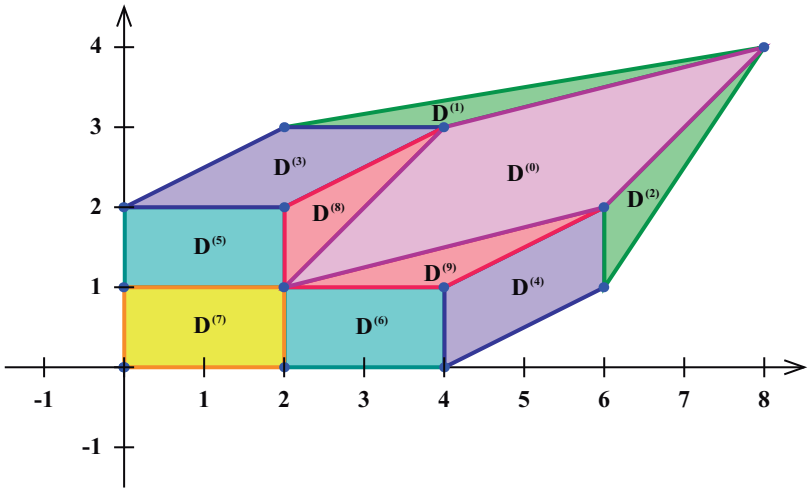


Figura 2.3: Subdivisión mixta fina de $\mathcal{A}^0$

Las celdas que permiten calcular $\mathcal{SM}(\mathcal{A})$ son $D^{(0)}, D^{(5)}, D^{(6)}$ y $D^{(7)}$. Como $\mathcal{MV}_3(D^{(5)}) = \mathcal{MV}_3(D^{(6)}) = \mathcal{MV}_3(D^{(7)}) = 2$ y $\mathcal{MV}_3(D^{(0)}) = 6$, la cota de [43] es $\mathcal{SM}(\mathcal{A}) = 12$. En este ejemplo, nuestra cota es $\mathcal{B}(\mathcal{A}) = \mathcal{MV}_1(\mathcal{A}^{\{1\}}) + \mathcal{MV}_1(\mathcal{A}^{\{2\}}) + \mathcal{MV}_0(\mathcal{A}^{\{1,2\}}) + \mathcal{MV}_2(\mathcal{A}) = 1 + 2 + 1 + 6 = 10$.

La diferencia en este caso se encuentra en las multiplicidades de los ceros. Al igual que en el Ejemplo 2.14 todos los subconjuntos del $\{1,2\}$ aportan soluciones, pero mientras que para un sistema P genérico las soluciones de P en $(\mathbb{C}^*)^2$ y de $P_{\{2\}}$ en $\mathbb{C}^*$ son todas simples, los ceros $(0,-\frac{a}{b})$ y $(0,0)$ conseguidos a partir de resolver los sistemas $P_{\{1\}} = \begin{cases} X_2(a+bX_2)=0 \end{cases}$ en $\mathbb{C}^*$ y $P_{\{1,2\}}=0$ tienen multiplicidad 2.

Si bien el hecho de que nuestra cota no considera la multiplicidad de los ceros de un sistema ralo genérico es una razón por la cual mejora las anteriores, no es la única causa. Veamos esto en otra variación del Ejemplo 2.14:

Ejemplo 2.22 Consideremos el sistema con coeficientes genéricos en $\mathbb{Q}$

$$P = \begin{cases} p_1(X_1,X_2) = aX_2 + bX_2^2 + cX_1X_2^3 \\ p_2(X_1,X_2) = dX_1X_2 + eX_1^2X_2 + fX_1^3X_2^2 \end{cases}$$

La familia de soportes es $\mathcal{A} = (\{(0,1),(0,2),(1,3)\},\{(1,1),(2,1),(3,2)\})$ y la subdivisión de $\mathcal{A}^0$ inducida por ω^0 puede verse en la Figura 2.4.

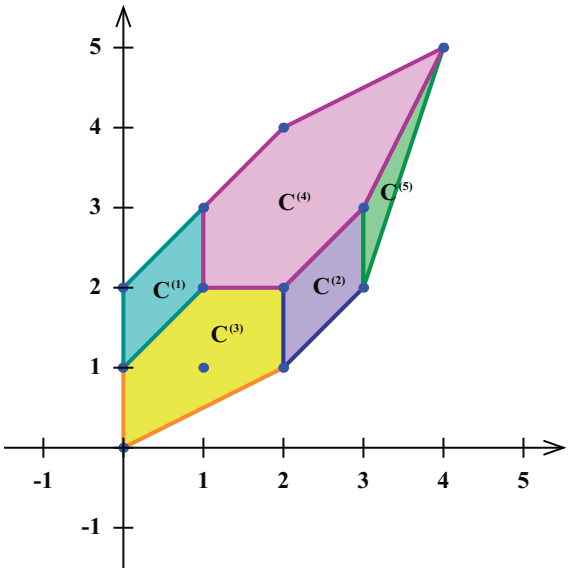


Figura 2.4: Subdivisión de $\mathcal{A}^0$

La siguiente tabla muestra las normales asociadas a cada celda de volumen mixto positivo y sus respectivos volúmenes mixtos:

Celda	$C^{(1)}$	$C^{(2)}$	$C^{(3)}$	$C^{(4)}$
Normal	$(1,0,1)$	$(-1,1,1)$	$(0,1,1)$	$(0,0,1)$
Volumen mixto	1	1	2	3

El volumen mixto de $\mathcal{A}^0$ es 7. Como la celda $C^{(2)}$ tiene una coordenada negativa el volumen mixto estable es 6 (la suma de los volúmenes mixtos de las otras tres celdas). Sin embargo, la cantidad de ceros aislados en $\mathbb{C}^2$ del sistema es solo 4.

La diferencia se debe en este caso a que la celda $C^{(3)}$ tiene volumen mixto positivo pero el sistema P no tiene soluciones aisladas de la forma $(x, 0)$ ya que para todo $x \in \mathbb{C}$ se tiene que $(x, 0)$ es solución (no aislada) del sistema. Como $\#J_{\{2\}} < n - \#\{2\}$, solo $\emptyset$ y $\{1\}$ cumplen las condiciones del Teorema 2.19 y por lo tanto $\mathcal{B}(\mathcal{A}) = 4$.

Notar además que el algoritmo `AffineSolve` descarta el sistema $P_{\{2\}}$ por no tener la misma cantidad de ecuaciones que de variables y encuentra exactamente 4 soluciones a partir de los ceros en $(\mathbb{C}^*)^2$ de P y en $\mathbb{C}^*$ de $P_{\{1\}}$.

2.4.2. Sistemas ralos cero-dimensionales

Nos interesa caracterizar, en función de los soportes, cuándo un sistema ralo de n ecuaciones con n incógnitas tiene una cantidad finita de ceros en $\mathbb{C}^n$.

En [43, Lemma 5] los autores presentan una condición suficiente para que un sistema $P = (p_1, \ldots, p_n)$ genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$ tenga finitas soluciones en $\mathbb{C}^n$. Además, en este caso, la cota que presentan para la cantidad de ceros de P contados con multiplicidad es genéricamente exacta. Dicha condición consiste en que para todo subconjunto $I \subset \{1, \ldots, n\}$, $\#I \geq \#\{j \in \{1, \ldots, n\} \mid p_j \in \langle X_i : i \in I \rangle\}$.

Observar que $\{j \in \{1, \ldots, n\} \mid p_j \in \langle X_i : i \in I \rangle\}$ es el conjunto de los $j \in \{1, \ldots, n\}$ tales que todo monomio de p_j se anula al evaluar $X_i = 0$ para todo $i \in I$, con lo cual $\#\{j \in \{1, \ldots, n\} \mid p_j \in \langle X_i : i \in I \rangle\} = n - \#J_I$. Así, la condición de [43] suficiente para que el sistema tenga finitas soluciones en $\mathbb{C}^n$ consiste en pedir que $\#J_I \geq n - \#I$ para todo $I \subset \{1, \ldots, n\}$.

A continuación probaremos una condición necesaria y suficiente para que un sistema genérico de n ecuaciones con n incógnitas con soportes prefijados tenga finitos ceros en $\mathbb{C}^n$ (comparar con [59, Lemma 3]) que refina la condición de [43]:

Proposición 2.23 *Sea P un sistema genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$. Entonces, P tiene finitas soluciones en $\mathbb{C}^n$ si y solo si para todo $I \subset \{1, \ldots, n\}$ tal que $\#J_I < n - \#I$ existe $J \subset J_I$ tal que $\dim(\sum_{j \in J} \mathcal{A}_j^I) < \#J$.*

Demostración: Notar que para todo $I \subset \{1, \ldots, n\}$ tal que P_I tiene solución en $(\mathbb{C}^*)^{n-\#I}$, $\#J_I \leq n - \#I$ y vale la igualdad si y solo si las soluciones son aisladas. Luego, como

$\mathbb{C}^n = \bigcup_{I\subset\{1,\dots,n\}} O_I$, tenemos que P tiene solo finitos ceros en $\mathbb{C}^n$ exactamente en los casos en que para todo $I \subset \{1,\dots,n\}$ tal que $\#J_I < n-\#I$ el sistema P_I no tiene ceros en $(\mathbb{C}^*)^{n-\#I}$. Para sistemas genéricos esto vale si y solo si existe $J \subset J_I$ tal que $\dim(\sum_{j\in J} \mathcal{A}_j^I) < \#J$ (ver la demostración de [66, Theorem 1.1]). □

Veamos un ejemplo sencillo donde nuestra condición sobre los soportes del sistema asegura que tendrá solo finitos ceros en $\mathbb{C}^n$, pero la condición de [43] no alcanza para predecirlo:

Ejemplo 2.24 Sea P el sistema genérico dado por

$$P = \begin{cases} p_1(X_1,X_2,X_3,X_4) = a_{11}X_1 + a_{12}X_4 + a_{13} \\ p_2(X_1,X_2,X_3,X_4) = a_{21}X_1^2 + a_{22}X_4 + a_{23} \\ p_3(X_1,X_2,X_3,X_4) = a_{31}X_1X_4 + a_{32}X_2X_4 + a_{33}X_3X_4 + a_{34}X_4 \\ p_4(X_1,X_2,X_3,X_4) = a_{41}X_1X_4 + a_{42}X_2X_4 + a_{43}X_3X_4 + a_{44}X_4 \end{cases}.$$

El volumen mixto de los soportes del sistema es 2, y de hecho el sistema solo tiene dos ceros en $\mathbb{C}^2$, ambos de coordenadas no nulas.

Como los ceros son todos aislados, la cota de [43] es genéricamente exacta, pero la condición que allí presentan no alcanza para predecirlo pues el conjunto $I = \{4\}$ cumple que $\#J_I = 2 < 3 = n - \#I$. Sin embargo, como en ese caso (el único que no cumple $\#J_I \geq n - \#I$) tenemos que $\dim(\sum_{j\in\{1,2\}} \mathcal{A}_j^{\{4\}}) = 1 < \#\{1,2\}$, la Proposición 2.23 asegura que todos los ceros del sistema son aislados.

Capítulo 3

Descomposición equidimensional

En este capítulo analizamos, tanto desde el punto de vista teórico como algorítmico, la descomposición equidimensional de variedades afines definidas por sistemas ralos con soportes prefijados.

En primer lugar consideramos sistemas ralos genéricos. Damos condiciones combinatorias sobre los soportes que describen la descomposición equidimensional de la variedad definida por el sistema y una fórmula para el grado de esta variedad. Presentamos también un algoritmo simbólico probabilístico que calcula la descomposición equidimensional de la variedad cuyo tiempo de ejecución depende de su grado y de la estructura combinatoria de los soportes de los polinomios.

Para sistemas ralos arbitrarios de n polinomios en n variables y soportes fijos, exhibimos una cota superior para el grado de la variedad que definen que mejora las cotas ya conocidas, dada por el volumen mixto de conjuntos asociados a los soportes del sistema. Finalmente, diseñamos un algoritmo que calcula un conjunto finito de puntos representativos de cada componente equidimensional de la variedad y cuya complejidad es polinomial en ciertos invariantes combinatorios asociados al sistema, entre ellos la cota para el grado ya mencionada.

3.1. Sistemas genéricos

3.1.1. Componentes que intersecan $(\mathbb{C}^*)^n$

Sean $n, m \in \mathbb{N}$ y $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ una familia de conjuntos finitos en $(\mathbb{Z}_{\geq 0})^n$. Para todo $1 \leq j \leq m$, sea $f_j(A_j, X) = \sum_{\alpha \in \mathcal{A}_j} A_{j,\alpha} X^\alpha$ donde $X = (X_1, \ldots, X_n)$ y $A_j = (A_{j,\alpha})_{\alpha \in \mathcal{A}_j}$ son $N_j = \#\mathcal{A}_j$ coeficientes indeterminados.

Consideramos la variedad

$$\{(a,x) \in (\mathbb{P}^{N_1-1} \times \cdots \times \mathbb{P}^{N_m-1}) \times (\mathbb{C}^*)^n \mid f_j(a_j,x) = 0 \text{ para todo } 1 \leq j \leq m\}$$

y su proyección

$$Z = \{a \in \mathbb{P}^{N_1-1} \times \cdots \times \mathbb{P}^{N_m-1} \mid \exists\, x \in (\mathbb{C}^*)^n \text{ tal que } f_j(a_j,x) = 0 \text{ para todo } 1 \leq j \leq m\}.$$

Los elementos de Z corresponden a los coeficientes de sistemas con soportes $\mathcal{A}$ que tienen soluciones en $(\mathbb{C}^*)^n$.

Lema 3.1 *La clausura de Zariski de Z es $\mathbb{P}^{N_1-1} \times \cdots \times \mathbb{P}^{N_m-1}$ si y solo si, para todo $J \subseteq \{1,\ldots,m\}$, $\dim\big(\sum_{j\in J} \mathcal{A}_j\big) \geq \#J$. En particular, si $m > n$, un sistema genérico con soportes $\mathcal{A}$ no tiene ceros en $(\mathbb{C}^*)^n$. Más aún, si $m \leq n$ y $\dim\big(\sum_{j\in J} \mathcal{A}_j\big) \geq \#J$ para todo $J \subseteq \{1,\ldots,m\}$, la clausura de Zariski en $\mathbb{C}^n$ del conjunto de ceros en $(\mathbb{C}^*)^n$ de un sistema genérico con soportes $\mathcal{A}$ es una variedad equidimensional de dimensión $n-m$ y grado $\mathcal{MV}_n(\mathcal{A}_1,\ldots,\mathcal{A}_m,\Delta^{(n-m)})$, donde Δ es el conjunto de vértices del símplex standard de $\mathbb{R}^n$ y el supraíndice $(n-m)$ indica que se repite $n-m$ veces.*

Demostración: La primera parte del Lema puede probarse de la misma forma que se prueba el resultado [66, Theorem 1.1].

Si $m \leq n$ y para todo $J \subseteq \{1,\ldots,m\}$, $\dim\big(\sum_{j\in J} \mathcal{A}_j\big) \geq \#J$, sea $\widetilde{\mathcal{A}} = (\widetilde{\mathcal{A}}_1,\ldots,\widetilde{\mathcal{A}}_n)$ tal que $\widetilde{\mathcal{A}}_j = \mathcal{A}_j$ si $j \leq m$ y $\widetilde{\mathcal{A}}_j = \Delta$ si $j > m$. Observamos que $\dim\big(\sum_{j\in \widetilde{J}} \widetilde{\mathcal{A}}_j\big) \geq \#\widetilde{J}$ para todo $\widetilde{J} \subseteq \{1,\ldots,n\}$, ya que si $\widetilde{J} \not\subseteq \{1,\ldots,m\}$, se tiene que $\widetilde{\mathcal{A}}_j = \Delta$ para algún $j \in \widetilde{J}$ y como $\dim(\Delta) = n$, entonces $\dim(\sum_{j\in \widetilde{J}} \widetilde{\mathcal{A}}_j) = n$. Por lo tanto, $\mathcal{MV}_n(\widetilde{\mathcal{A}}) > 0$ (ver la Proposición 1.12), y esto implica que un sistema genérico con soportes $\widetilde{\mathcal{A}}$ tiene una cantidad finita, no nula, de ceros en $(\mathbb{C}^*)^n$ (tantos como el volumen mixto $\mathcal{MV}_n(\widetilde{\mathcal{A}})$).

El conjunto de los finitos ceros en $(\mathbb{C}^*)^n$ de un sistema genérico con soportes $\widetilde{\mathcal{A}}$ es exactamente la intersección de una variedad cuyas componentes irreducibles tienen todas dimensión al menos $n-m$ (el conjunto de los ceros en $(\mathbb{C}^*)^n$ de un sistema de m ecuaciones con soportes $\mathcal{A}$) con $n-m$ hiperplanos genéricos. Entonces, la clausura de Zariski del conjunto de soluciones en $(\mathbb{C}^*)^n$ de un sistema genérico con soportes $\mathcal{A}$ es una variedad equidimensional de dimensión $n-m$ y grado $\mathcal{MV}_n(\widetilde{\mathcal{A}})$. □

Definición 3.2 *Sean $\mathcal{A} = (\mathcal{A}_1,\ldots,\mathcal{A}_m)$ una familia de conjuntos finitos en $(\mathbb{Z}_{\geq 0})^n$ y $G = (g_1,\ldots,g_m)$ un sistema de polinomios en $k[X_1,\ldots,X_n]$ con soportes $\mathcal{A}$. Llamamos $V^*(G)$ a la variedad algebraica de $\overline{k}^n$ compuesta por la unión de todas las componentes irreducibles de $V(G)$ tales que su intersección con $(\overline{k}^*)^n$ es no vacía.*

Notar que $V^*(G)$ es exactamente la clausura de Zariski en $\overline{k}^n$ del conjunto de los ceros en $(\overline{k}^*)^n$ de G.

En lo que resta de esta sección, vamos a suponer que $m \leq n$. Sea $P = (p_1, \ldots, p_m)$ un sistema ralo genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$, donde $m \leq n$ y $\mathcal{A}_j \subset (\mathbb{Z}_{\geq 0})^n$ para todo $1 \leq j \leq m$. Por el Lema 3.1, la variedad algebraica $V^*(P)$ es o bien el conjunto vacío o bien una variedad equidimensional de dimensión $n - m$.

El algoritmo `ToricSolve` descripto en el Capítulo 2 (Algoritmo 2.3) calcula una resolución geométrica de $V^*(P)$ para el caso $m = n$. A continuación extendemos este algoritmo al caso $m < n$.

Algoritmo 3.3 `GenericToricSolve`

INPUT: Un sistema de polinomios $P = (p_1, \ldots, p_m)$ en $\mathbb{Q}[X_1, \ldots, X_n]$ genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ codificado en forma rala. Las celdas mixtas de una subdivisión mixta fina $S_\omega(\mathcal{A}, \Delta^{(n-m)})$ inducida por una función de levantamiento ω.

1. *Si la subdivisión mixta fina de $(\mathcal{A}, \Delta^{(n-m)})$ no contiene ninguna celda mixta, devolver $R = \emptyset$. Caso contrario, continuar al paso 2.*
2. *Elegir al azar las coordenadas de una matriz $B = (b_{hl}) \in \mathbb{Z}^{n \times n}$ y un vector $b = (b_1, \ldots, b_{n-m}) \in \mathbb{Z}^{n-m}$.*
3. *Para todo $1 \leq h \leq n - m$, tomar la forma lineal afín $L_h = \sum_{l=1}^{n} b_{hl} X_l - b_h$.*
4. *Aplicar el algoritmo `ToricSolve` para obtener una resolución geométrica $(q(U), v_1(U), \ldots, v_n(U))$ de los ceros aislados en $(\mathbb{C}^*)^n$ del sistema dado por los polinomios $P, L_1, \ldots, L_{n-m}$.*
5. *Hallar un slp para los polinomios $G := P(B^{-1}Y)$, donde $Y = (Y_1, \ldots, Y_n)$ son nuevas variables.*
6. *Calcular $(w_1(U), \ldots, w_n(U))^t := B(v_1(U), \ldots, v_n(U))^t$.*
7. *Aplicar el algoritmo `GlobalNewton` ([37, Algorithm 1]) a los polinomios del sistema $G(Y)$ y la resolución geométrica $(q(U), w_{n-m+1}(U), \ldots, w_n(U))$ de $V(G(b, Y_{n-m+1}, \ldots, Y_n))$ con precisión $\mathcal{MV}_n(\mathcal{A}, \Delta^{(n-m)})$ para obtener una resolución geométrica R_Y.*
8. *Hallar la resolución geométrica $R := B^{-1}R_Y$ de $V^*(P)$.*

OUTPUT: Una resolución geométrica R de $V^*(P)$.

La idea del algoritmo es elegir $n-m$ formas lineales afines al azar y, si $V^*(P)$ no es el conjunto vacío, calcular en primer lugar una resolución geométrica de $V^*(P) \cap V(L_1, \ldots, L_{n-m})$. Como P es un sistema genérico, por el Lema 3.1, sabemos que si $L_1, \ldots, L_{n-m}$ son formas lineales afines genéricas, la variedad $V^*(P) \cap V(L_1, \ldots, L_{n-m})$ es o bien el conjunto vacío o bien un conjunto finito en $(\mathbb{C}^*)^n$. Además, es vacío si y solo si $V^*(P)$ es vacío. En caso de no ser vacío, el conjunto $V^*(P) \cap V(L_1, \ldots, L_{n-m})$ puede considerarse una fibra genérica de una proyección lineal sobreyectiva genérica y, en consecuencia, permite recuperar $V^*(P)$. Entonces, a partir de la resolución geométrica de esta fibra y mediante un levantamiento de Newton-Hensel, hallamos una resolución geométrica de $V^*(P)$. Para hacer esto algorítmicamente, realizamos un cambio de variables de manera que la proyección considerada sea la proyección a las primeras coordenadas.

Proposición 3.4 *Sea $P = (p_1, \ldots, p_m)$ un sistema de $m \leq n$ polinomios genéricos en $\mathbb{Q}[X_1, \ldots, X_n]$ con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ en $(\mathbb{Z}_{\geq 0})^n$. El algoritmo probabilístico* `GenericToricSolve` *calcula una resolución geométrica de la variedad algebraica $V^*(P)$ formada por la unión de todas las componentes irreducibles de $V(P) \subset \mathbb{C}^n$ que tienen intersección no vacía con $(\mathbb{C}^*)^n$. La complejidad de este algoritmo es del orden de*

$$O\left(n^3(N + (n-m)n)\log(d)M(\mathcal{D})(M(\Upsilon)(M(\mathcal{D}) + M(\mathcal{E})) + \mathcal{D}^2)\right),$$

donde

- $N := \sum_{1 \leq j \leq m} \#\mathcal{A}_j$,
- $d := \text{máx}_{1 \leq j \leq m}\{\deg(p_j)\}$,
- $\mathcal{D} := \mathcal{MV}_n(\mathcal{A}, \Delta^{(n-m)})$,
- $\Upsilon := \text{máx}\{\|\eta\|\}$, *donde el máximo se toma sobre todas las normales primitivas asociadas a celdas mixtas de la subdivisión de $(\mathcal{A}, \Delta^{(n-m)})$ inducida por una función de levantamiento genérica ω,*
- $\mathcal{E} := \mathcal{MV}_{n+1}(\Delta \times \{0\}, \mathcal{A}_1(\omega_1), \ldots, \mathcal{A}_m(\omega_m), \Delta(\omega_{m+1}), \ldots, \Delta(\omega_n))$.

Demostración: En el paso 1 determinamos si el conjunto $V^*(P) \cap V(L_1, \ldots, L_{n-m})$ (y consecuentemente $V^*(P)$) es vacío o no. Como el sistema dado por los polinomios $P, L_1, \ldots, L_{n-m}$ es genérico, vale

$$V^*(P) \cap V(L_1, \ldots, L_{n-m}) = (V(P) \cap (\mathbb{C}^*)^n) \cap V(L_1, \ldots, L_{n-m}) \tag{3.1}$$

y entonces, la cantidad de puntos en $V^*(P) \cap V(L_1, \ldots, L_{n-m})$ es el volumen mixto de los soportes $\mathcal{A}, \Delta^{(n-m)}$. Por [42], éste puede calcularse como la suma de los volúmenes mixtos de las celdas mixtas de $S_\omega(\mathcal{A}, \Delta^{(n-m)})$.

En el paso 2 elegimos al azar los coeficientes de un cambio de variables y de las formas lineales afines $L_1, \ldots, L_{n-m}$. En el paso 3 obtenemos la codificación rala de estas formas lineales.

En el paso 4 buscamos una resolución geométrica de $V^*(P) \cap V(L_1, \ldots, L_{n-m})$. Por la igualdad (3.1), éste es el conjunto de los ceros aislados en $(\mathbb{C}^*)^n$ del sistema genérico $P, L_1, \ldots, L_{n-m}$ con soportes $\mathcal{A}, \Delta^{(n-m)}$. Para encontrar una resolución geométrica de este conjunto, aplicamos el algoritmo `ToricSolve` cuya complejidad expusimos en la Sección 2.1.2. De acuerdo a esto, la complejidad de este paso es $O\big((n^3(N+(n-m)n)\log d + n^{1+\Omega})$ $M(\mathcal{D})M(\Upsilon)(M(D)+M(\mathcal{E}))\big)$.

En los pasos 5 y 6 consideramos el cambio de variables dado por $Y = BX$ y lo aplicamos a los polinomios de P, obteniendo un nuevo sistema polinomial G, y a la resolución geométrica calculada en el paso 4. Una forma de aplicar este cambio de variables es calculando B^{-1} con $O(n^\Omega)$ operaciones y usando B^{-1} para calcular un slp para los polinomios de G. Como la longitud del slp no depende del costo de invertir B sino de multiplicar B^{-1} por un vector, lo cual requiere $O(n^2)$ operaciones, la longitud de este slp es $L = O(n^2 + n\log(d)N)$. Finalmente, como los grados totales de los polinomios $v_1, \ldots, v_n$ están acotados superiormente por $\mathcal{D}$, la resolución geométrica $(w_1(U), \ldots, w_n(U))^t = B(v_1(U), \ldots, v_n(U))^t$ puede calcularse con $O(n^2\mathcal{D})$ operaciones. Con ese cambio de variables, $(w_1(U), \ldots, w_{n-m}(U)) = b$ y $(q(U), w_{n-m+1}(U), \ldots, w_n(U))$ es una resolución geométrica de los ceros aislados de $V(G(b, Y_{n-m+1}, \ldots, Y_n))$ que se corresponden con los ceros en $(\mathbb{C}^*)^n$ de $V(P, L_1, \ldots, L_{n-m})$.

Los polinomios que conforman la resolución geométrica de $V^*(P)$ respecto de la proyección lineal dada por las variables Y están en $\mathbb{Q}[Y_1, \ldots, Y_{n-m}, U]$ y tienen grados totales acotados por $\mathcal{D}$. Luego, basta hallar sus representantes en $(\mathbb{Q}[Y_1, \ldots, Y_{n-m}]/\langle Y_1 - b_1,$ $\ldots, Y_{n-m} - b_{n-m}\rangle^{\mathcal{D}+1})[U]$. Como los polinomios de la resolución geométrica $(q(U),$ $w_{n-m+1}(U), \ldots, w_n(U))$ pueden considerarse representantes en $(\mathbb{Q}[Y_1, \ldots, Y_{n-m}]/\langle Y_1 - b_1,$ $\ldots, Y_{n-m} - b_{n-m}\rangle)[U]$, en el paso 7 aplicamos sucesivamente a estos polinomios el algoritmo `GlobalNewton` de [37, Algorithm 1] con precisión $\mathcal{D} = \mathcal{MV}_n(\mathcal{A}, \Delta^{(n-m)})$. Por [37, Lemma 2], codificando para cada aplicación sucesiva los elementos de $\mathbb{Q}[Y_1, \ldots, Y_{n-m}]/\langle Y_1 - b_1,$ $\ldots, Y_{n-m} - b_{n-m}\rangle^k$ como $(k+1)$-uplas de slp (un slp por cada componente homogénea del polinomio codificado), este paso requiere $O((mL + m^{\overline{\Omega}})M(\mathcal{D})\mathcal{D}^2)$ operaciones.

En el último paso, el algoritmo vuelve a las variables originales de forma de obtener la resolución geométrica de $V^*(P)$ buscada. Si la resolución geométrica obtenida en el paso anterior es $R_Y = (\hat{q}(Y_1, \ldots, Y_{n-m}, U), \hat{w}_{n-m+1}(Y_1, \ldots, Y_{n-m}, U), \ldots, \hat{w}_n(Y_1, \ldots, Y_{n-m}, U))$, se calcula $(\hat{v}_1, \ldots, \hat{v}_n)^t = B.(Y_1, \ldots, Y_{n-m}, \hat{w}_{n-m+1}, \ldots, \hat{w}_n)^t$ y finalmente se reemplaza en los polinomios $\hat{q}, \hat{v}_1, \ldots, \hat{v}_n$, para todo $1 \leq h \leq n-m$, la variable Y_h por $\sum_{l=1}^{n} b_{hl}X_l$. La

complejidad total de este paso es de orden $O(n^2\mathcal{D})$. □

3.1.2. Componentes afines

Dado un sistema polinomial ralo *genérico*, en esta sección consideramos las componentes irreducibles de dimensión positiva que no intersecan $(\mathbb{C}^*)^n$ de la variedad que definen los polinomios del sistema.

En primer lugar, mostramos en un ejemplo que un sistema ralo genérico con n polinomios en n variables puede definir una variedad algebraica de dimensión positiva. Este ejemplo también muestra que ni el volumen mixto ni el volumen mixto estable de los soportes del sistema son cotas superiores para el grado de la variedad algebraica definida por los polinomios.

Ejemplo 3.5 Sea $P = (p_1, p_2, p_3)$ un sistema ralo genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$, donde $\mathcal{A}_1 = \{(1,1,2), (1,1,1)\}$, $\mathcal{A}_2 = \{(2,0,1),\ (1,0,1)\}$ y $\mathcal{A}_3 = \{(0,2,1), (0,1,1)\}$:

$$P = \begin{cases} p_1(X_1, X_2, X_3) = aX_1X_2X_3^2 + bX_1X_2X_3 \\ p_2(X_1, X_2, X_3) = cX_1^2X_3 + dX_1X_3 \\ p_3(X_1, X_2, X_3) = eX_2^2X_3 + fX_2X_3 \end{cases}$$

con $a, b, c, d, e, f \in \mathbb{C}^*$ valores genéricos.

La variedad afín definida por los polinomios del sistema tiene 5 componentes irreducibles:

- $\{(x_1, x_2, x_3) \in \mathbb{C}^3 \mid x_3 = 0\}$,
- $\{(x_1, x_2, x_3) \in \mathbb{C}^3 \mid x_1 = 0, x_2 = -\frac{f}{e}\}$,
- $\{(x_1, x_2, x_3) \in \mathbb{C}^3 \mid x_1 = -\frac{d}{c}, x_2 = 0\}$,
- $\{(x_1, x_2, x_3) \in \mathbb{C}^3 \mid x_1 = 0, x_2 = 0\}$ y
- $\{(-\frac{d}{c}, -\frac{f}{e}, -\frac{b}{a})\}$.

Cada una de estas componentes tiene grado 1, con lo cual el grado de $V(P)$ es 5. Sin embargo, $\mathcal{MV}_3(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3) = 1$ y $\mathcal{SM}(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3) \leq \mathcal{MV}_3(\mathcal{A}_1 \cup \{0\}, \mathcal{A}_2 \cup \{0\}, \mathcal{A}_3 \cup \{0\}) = 4$.

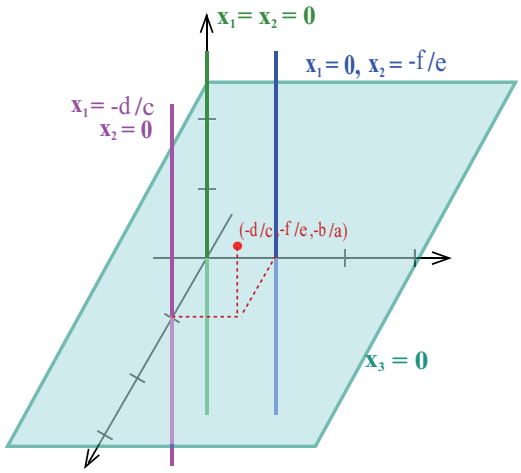


Figura 3.1: Componentes irreducibles de $V(P)$

Sea $P = (p_1, \ldots, p_m)$ un sistema polinomial genérico en las variables $X = (X_1, \ldots, X_n)$ (donde m puede ser mayor a n), con coeficientes en $\mathbb{C}$ y soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$, donde $\mathcal{A}_j \subset (\mathbb{Z}_{\geq 0})^n$ para todo $j = 1, \ldots, m$. Para todo $I \subset \{1, \ldots, n\}$, sean P_I y J_I como en la Sección 2.2:

- P_I es el sistema que resulta de evaluar $X_i = 0$ para todo $i \in I$ y decartar los polinomios que se hacen idénticamente cero.
- J_I es el conjunto de subíndices de los polinomios del sistema P que no se anulan al construir el sistema P_I.

Recordemos que notamos $\pi_I : \mathbb{C}^n \to \mathbb{C}^{n-\#I}$ a la proyección $\pi_I(x_1, \ldots, x_n) = (x_i)_{i \notin I}$, $\varphi_I : \mathbb{C}^{n-\#I} \to \mathbb{C}^n$ a la función que inserta ceros en las coordenadas i tales que $i \in I$ y $\mathcal{A}_j^I$ a los soportes de los polinomios $(p_j)_I$ de P_I.

Para una componente irreducible W de $V(P)$, definimos el conjunto

$$I_W = \{i \in \{1, \ldots, n\} \mid W \subset \{x_i = 0\}\}.$$

Lema 3.6 *Bajo las hipótesis anteriores, sea W una componente irreducible de $V(P)$. Entonces $\dim W = n - \#I_W - \#J_{I_W}$. Más aún, $\pi_{I_W}(W)$ es una componente irreducible de $V(P_{I_W}) \subset \mathbb{C}^{n-\#I_W}$ cuya intersección con $(\mathbb{C}^*)^{n-\#I_W}$ es no vacía.*

Demostración: Si $I_W = \{1, \ldots, n\}$, $W = \{0\}$ y $\#J_{I_W} = 0$, y no hay nada que probar. Si no, sin perder generalidad, podemos suponer que $I_W = \{r+1, \ldots, n\}$ y $J_{I_W} = \{1, \ldots, s\}$, con $r > 0$ y $s \leq n$. Notar que $\pi_{I_W} : \mathbb{C}^n \to \mathbb{C}^r$ es la proyección a las primeras r coordenadas

y $P_{I_W} = (p_1(X_1, \ldots, X_r, 0), \ldots, p_s(X_1, \ldots, X_r, 0))$, donde 0 es el origen en $\mathbb{C}^{n-r}$. Además, $W = \pi_{I_W}(W) \times \{0\}$ y $\pi_{I_W}(W) \subset V(P_{I_W})$ es irreducible.

Sea C una componente irreducible de $V(P_{I_W})$ tal que $\pi_{I_W}(W) \subset C \subset V(P_{I_W})$. Entonces, $W \subset C \times \{0\} \subset V(P)$. Como $C \times \{0\}$ es una variedad irreducible y W es una componente irreducible de $V(P)$, vale $W = C \times \{0\}$. Por lo tanto, $\pi_{I_W}(W) = C$ es una componente irreducible de $V(P_{I_W})$.

Además, $W \cap \left(\bigcap_{i=1}^{r} \{x_i \neq 0\} \right) \neq \emptyset$ pues, de lo contrario, $W \subset \bigcup_{i=1}^{r} \{x_i = 0\}$, y como W es irreducible, entonces $W \subset \{x_i = 0\}$ para algún $1 \leq i \leq r$. Luego, $\pi_{I_W}(W) \cap (\mathbb{C}^*)^r \neq \emptyset$.

Como P_{I_W} es un sistema genérico de s ecuaciones con ceros en $(\mathbb{C}^*)^r$, por el Lema 3.1, $\dim(\pi_{I_W}(W)) = r - s = (n - \#I_W) - \#J_{I_W}$ y, en consecuencia, $\dim(W) = \dim(\pi_{I_W}(W)) = n - \#I_W - \#J_{I_W}$. □

En el resto de esta sección vamos a describir la descomposición equidimensional de $V(P) \subset \mathbb{C}^n$ en función de los soportes de los polinomios del sistema. Comenzamos caracterizando los conjuntos $I \subset \{1, \ldots, n\}$ tales que las componentes irreducibles de $V(P_I)$ con intersección no vacía con $(\mathbb{C}^*)^{n-\#I}$ dan lugar a componentes irreducibles de $V(P)$. En este sentido, la siguiente proposición es una generalización del Lema 2.17. Notar que de la primera parte de la proposición se deduce la condición necesaria y suficiente para que un sistema ralo tenga solo finitos ceros en $\mathbb{C}^n$ que presentamos en la Proposición 2.23.

Proposición 3.7 *Con la notación anterior, sea $I \subset \{1, \ldots, n\}$. Entonces $V(P_I) \cap (\mathbb{C}^*)^{n-\#I}$ es un conjunto no vacío si y solo si para todo $J \subset J_I$, $\dim(\sum_{j \in J} \mathcal{A}_j^I) \geq \#J$ y, en ese caso, $V^*(P_I)$ es una variedad equidimensional de dimensión $n - \#I - \#J_I$. Si W es una componente irreducible de $V^*(P_I)$, $\varphi_I(W)$ es una subvariedad de $V(P)$ que interseca $\bigcap_{i \notin I} \{x_i \neq 0\}$. Además, $\varphi_I(W)$ es una componente irreducible de $V(P)$ si y solo si para todo $\widetilde{I} \subset I$, $\#\widetilde{I} + \#J_{\widetilde{I}} \geq \#I + \#J_I$.*

Demostración: Por el Lema 3.1 sabemos que, siendo P_I un sistema genérico con soportes $(\mathcal{A}_j^I)_{j \in J_I}$, $V(P_I) \cap (\mathbb{C}^*)^{n-\#I} \neq \emptyset$ si y solo si para todo $J \subset J_I$, $\dim(\sum_{j \in J} \mathcal{A}_j^I) \geq \#J$. Además, como P_I es un sistema de $\#J_I$ ecuaciones en $n - \#I$ variables, la variedad $V^*(P_I)$ es o bien el conjunto vacío o bien una variedad equidimensional de dimensión $n - \#I - \#J_I$.

Sin perder generalidad podemos suponer que $I = \{r+1, \ldots, n\}$. Sea W una componente irreducible de $V^*(P_I) \subset \mathbb{C}^r$. Notaremos 0_k al origen en $\mathbb{C}^k$ para cada $k \in \mathbb{N}$.

Por un lado, supongamos que existe un subconjunto $\widetilde{I} \subset I$ para el cual $\#\widetilde{I} + \#J_{\widetilde{I}} < \#I + \#J_I$. Nuevamente, podemos suponer, para facilitar la notación, que $\widetilde{I} = \{\tilde{r}+1, \ldots, n\}$ con

$\tilde{r} > r$. La variedad $W \times \{0_{\tilde{r}-r}\}$ está incluida en $V(P_{\widetilde{I}})$ pues para todo cero $\xi = (\xi_1, \ldots, \xi_r)$ de P_I vale que $(\xi, 0_{n-r}) \in V(P)$ y por lo tanto $(\xi, 0_{\tilde{r}-r})$ es un cero de $P_{\widetilde{I}}$. Como $W \times \{0_{\tilde{r}-r}\}$ es irreducible, está contenida en una componente irreducible $\widetilde{W}$ de $V(P_{\widetilde{I}})$, y como $P_{\widetilde{I}}$ es un sistema de $\#J_{\widetilde{I}}$ polinomios en $n-\#\widetilde{I}$ variables, la dimensión de $\widetilde{W}$ es al menos $n-\#\widetilde{I}-\#J_{\widetilde{I}}$. En consecuencia, tenemos que

$$\dim(\widetilde{W}) \geq n - \#\widetilde{I} - \#J_{\widetilde{I}} > n - \#I - \#J_I = \dim(W),$$

donde la última igualdad vale por el Lema 3.1 aplicado al sistema P_I y la componente irreducible W de $V^*(P_I)$. Entonces, $\varphi_I(W) = W \times \{0_{n-r}\} \subsetneq \widetilde{W} \times \{0_{n-\tilde{r}}\} \subset V(P)$ y, por lo tanto, $\varphi_I(W)$ no es una componente irreducible de $V(P)$.

Por otro lado, si $\varphi_I(W) = W \times \{0_{n-r}\}$ no es una componente irreducible de $V(P)$, existe una componente irreducible $\widetilde{W}$ de esta variedad tal que $W \times \{0_{n-r}\} \subsetneq \widetilde{W}$. Por lo tanto, $I_{\widetilde{W}} \subsetneq I$. Sin pérdida de generalidad, supongamos que $I_{\widetilde{W}} = \{\tilde{r}+1, \ldots, n\}$ con $\tilde{r} > r$. Por el Lema 3.6, $\pi_{I_{\widetilde{W}}}(\widetilde{W})$ es una componente irreducible de $V(P_{I_{\widetilde{W}}})$ que interseca $(\mathbb{C}^*)^{\tilde{r}}$. Entonces,

$$n - \#I_{\widetilde{W}} - \#J_{I_{\widetilde{W}}} = \dim(\pi_{I_{\widetilde{W}}}(\widetilde{W})) = \dim(\widetilde{W}) > \dim(W) = n - \#I - \#J_I,$$

y por lo tanto, $\#I + \#J_I > \#I_{\widetilde{W}} + \#J_{I_{\widetilde{W}}}$. □

Por la proposición anterior, si Φ es el conjunto

$$\Phi = \Big\{ I \subset \{1, \ldots, n\} \mid \forall J \subset J_I,\ \dim(\sum_{j \in J} \mathcal{A}_j^I) \geq \#J;\ \forall \widetilde{I} \subset I,\ \#J_{\widetilde{I}} + \#\widetilde{I} \geq \#J_I + \#I \Big\}, \tag{3.2}$$

las componentes irreducibles de la variedad $V(P) \subset \mathbb{C}^n$ están contenidas en la familia de los subespacios lineales $\bigcap_{i \in I} \{x_i = 0\}$ indexados por los $I \in \Phi$.

Recordemos que usamos la notación $V^*(P_I)$ para referirnos a la unión de todas las componentes irreducibles de $V(P_I)$ que cortan a $(\mathbb{C}^*)^{n-\#I}$. Por el Lema 3.6 y la Proposición 3.7, para todo $I \in \Phi$,

$$\varphi_I(V^*(P_I)) = \bigcup_{\substack{W \text{ componente irreducible} \\ \text{de } V(P) \text{ tal que } I_W = I}} W.$$

Esto nos permite dar la caracterización de la descomposición equidimensional de $V(P)$ mencionada al principio de la sección. Además, usando el Lema 3.1, podemos calcular el grado de $V(P)$:

Teorema 3.8 *Sea $P = (p_1, \ldots, p_m)$ un sistema genérico de polinomios en n variables con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ contenidos en $(\mathbb{Z}_{\geq 0})^n$. Para $k = 0, \ldots, n$, sea $V_k(P)$ la componente equidimensional de dimensión k de $V(P)$. Entonces, con la notación previa,*

$$V_k(P) = \bigcup_{\substack{I \in \Phi, \\ \#I + \#J_I = n-k}} \varphi_I(V^*(P_I)).$$

Además,

$$\deg(V(P)) = \sum_{I \in \Phi} \mathcal{MV}_{n-\#I}(\mathcal{A}^I, \Delta^{(n-\#I-\#J_I)}).$$

Usemos el teorema anterior en un ejemplo para hallar las componentes equidimensionales de la variedad definida por un sistema polinomial ralo genérico.

Ejemplo 3.9 Consideremos un sistema de polinomios en $\mathbb{Q}[X_1, X_2, X_3, X_4]$ genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4)$, donde $\mathcal{A}_1 = \{(1,0,0,1), (2,0,0,2), (1,1,1,0), (0,1,1,0)\}$, $\mathcal{A}_2 = \{(1,1,0,0), (1,2,0,0), (1,0,1,1), (0,0,1,1), (0,0,1,2)\}$, $\mathcal{A}_3 = \{(1,1,0,1), (1,0,1,1), (0,1,1,0), (0,1,1,1)\}$ y $\mathcal{A}_4 = \{(1,0,0,0), (2,0,0,0), (1,1,0,0), (0,0,2,0), (0,0,1,1)\}$:

$$P = \begin{cases} p_1(X_1, X_2, X_3, X_4) = a_{11}X_1X_4 + a_{12}X_1^2X_4^2 + a_{13}X_1X_2X_3 + a_{14}X_2X_3 \\ p_2(X_1, X_2, X_3, X_4) = a_{21}X_1X_2 + a_{22}X_1X_2^2 + a_{23}X_1X_3X_4 + a_{24}X_3X_4 + a_{25}X_3X_4^2 \\ p_3(X_1, X_2, X_3, X_4) = a_{31}X_1X_2X_4 + a_{32}X_1X_3X_4 + a_{33}X_2X_3 + a_{34}X_2X_3X_4 \\ p_4(X_1, X_2, X_3, X_4) = a_{41}X_1 + a_{42}X_1^2 + a_{43}X_1X_2 + a_{44}X_3^2 + a_{45}X_3X_4 \end{cases}.$$

Con la notación anterior, el conjunto Φ definido en (3.2) es

$$\Phi = \{\emptyset, \{1,2\}, \{1,3\}, \{2,3\}, \{2,4\}, \{3,4\}\}.$$

Calculando $n - \#I - \#J_I$ para cada elemento de Φ, vemos que las componentes equidimensionales de $V(P)$ son:

- $V_0(P) = V^*(P) \cup \{(0, 0, \frac{a_{24}a_{45}}{a_{25}a_{44}}, -\frac{a_{24}}{a_{25}}), (-\frac{a_{41}}{a_{42}}, 0, 0, \frac{a_{11}a_{42}}{a_{12}a_{41}}), (-\frac{a_{41}}{a_{42}} + \frac{a_{21}a_{43}}{a_{22}a_{42}}, -\frac{a_{21}}{a_{22}}, 0, 0)\}$ pues:
  - Para $I = \emptyset$, por el Teorema de Bernstein, existen exactamente $\mathcal{MV}_4(\mathcal{A}) = 19$ ceros aislados en $(\mathbb{C}^*)^4$.
  - Para $I = \{1,2\}$, buscamos los ceros en $(\mathbb{C}^*)^2$ de

$$P_{\{1,2\}} = \begin{cases} a_{24}X_3X_4 + a_{25}X_3X_4^2 \\ a_{44}X_3^2 + a_{45}X_3X_4 \end{cases}.$$

Como $V^*(P_{\{1,2\}}) = \Big\{\Big(\dfrac{a_{24}a_{45}}{a_{25}a_{44}}, -\dfrac{a_{24}}{a_{25}}\Big)\Big\}$, obtenemos el cero de P:

$$\varphi_{\{1,2\}}(V^*(P_{\{1,2\}})) = \Big\{\Big(0, 0, \frac{a_{24}a_{45}}{a_{25}a_{44}}, -\frac{a_{24}}{a_{25}}\Big)\Big\}.$$

- Para $I = \{2,3\}$, buscamos los ceros en $(\mathbb{C}^*)^2$ de

$$P_{\{2,3\}} = \begin{cases} a_{11}X_1X_4 + a_{12}X_1^2X_4^2 \\ a_{41}X_1 + a_{42}X_1^2 \end{cases}.$$

Como $V^*(P_{\{2,3\}}) = \Big\{\Big(-\dfrac{a_{41}}{a_{42}}, \dfrac{a_{11}a_{42}}{a_{12}a_{41}}\Big)\Big\}$, obtenemos el cero de P:

$$\varphi_{\{2,3\}}(V^*(P_{\{2,3\}})) = \Big\{\Big(-\frac{a_{41}}{a_{42}}, 0, 0, \frac{a_{11}a_{42}}{a_{12}a_{41}}\Big)\Big\}.$$

- Para $I = \{3,4\}$, buscamos los ceros en $(\mathbb{C}^*)^2$ de

$$P_{\{3,4\}} = \begin{cases} a_{21}X_1X_2 + a_{22}X_1X_2^2 \\ a_{41}X_1 + a_{42}X_1^2 + a_{43}X_1X_2 \end{cases}.$$

Como $V^*(P_{\{3,4\}}) = \Big\{\Big(-\dfrac{a_{41}}{a_{42}} + \dfrac{a_{21}a_{43}}{a_{22}a_{42}}, -\frac{a_{21}}{a_{22}}\Big)\Big\}$, obtenemos el cero de P:

$$\varphi_{\{3,4\}}(V^*(P_{\{3,4\}})) = \Big\{\Big(-\frac{a_{41}}{a_{42}} + \frac{a_{21}a_{43}}{a_{22}a_{42}}, -\frac{a_{21}}{a_{22}}, 0, 0\Big)\Big\}.$$

- $V_1(P) = \{x \in \mathbb{C}^4 \mid x_2 = 0, x_4 = 0, a_{41}x_1 + a_{42}x_1^2 + a_{44}x_3^2 = 0\}$ pues:

  - Para $I = \{2,4\}$ buscamos los ceros en $(\mathbb{C}^*)^2$ de

$$P_{\{2,4\}} = \Big\{a_{41}X_1 + a_{42}X_1^2 + a_{44}X_3^2.$$

Como $V^*(P_{\{2,4\}}) = \Big\{(x_1, x_3) \mid a_{41}x_1 + a_{42}x_1^2 + a_{44}x_3^2 = 0\Big\}$, obtenemos la curva de ceros de P:

$$\varphi_{\{2,4\}}(V^*(P_{\{2,4\}})) = \Big\{x_2 = 0, x_4 = 0, a_{41}x_1 + a_{42}x_1^2 + a_{44}x_3^2 = 0\Big\}.$$

- $V_2(P) = \{x \in \mathbb{C}^4 \mid x_1 = 0, x_3 = 0\}$ pues:

  - Para $I = \{1,3\}$ buscamos los ceros en $(\mathbb{C}^*)^2$ de

$$P_{\{1,3\}} = \emptyset.$$

Como $V^*(P_{\{1,3\}}) = \mathbb{C}^2$, obtenemos el plano de ceros de P:

$$\varphi_{\{1,3\}}(V^*(P_{\{1,3\}})) = \Big\{x_1 = 0, x_3 = 0\Big\}.$$

- $V_3(P) = \emptyset$ pues $n - \#I - \#J_I < 3$ para todo $I \in \Phi$.

3.2. Algoritmos para sistemas genéricos

En esta sección analizamos las condiciones que definen el conjunto Φ introducido en (3.2) y desarrollamos un algoritmo que permite encontrar una familia de conjuntos $I \subset \{1, \ldots, n\}$ apropiada que contiene a Φ. A continuación, usamos esa familia para hallar algorítmicamente la descomposición equidimensional de $V(P)$.

3.2.1. Conjuntos de índices

Por la Proposición 3.7, para hallar las componentes afines de $V(P)$ buscamos los $I \subset \{1, \ldots, n\}$ que sean elementos del conjunto Φ definido en (3,2), es decir que cumplan que:

1. $\forall J \subset J_I$, $\dim(\sum_{j \in J} \mathcal{A}_j^I) \geq \#J$,
2. $\forall \widetilde{I} \subset I$, $\#J_{\widetilde{I}} + \#\widetilde{I} \geq \#J_I + \#I$.

Estos son exactamente los conjuntos I tales que $I = I_W$ para alguna componente irreducible W de $V(P)$ en $\mathbb{C}^n$.

Para todo $I \subset \{1, \ldots, n\}$ que cumpla la condición 2 tenemos que $\#I + \#J_I \leq \#\emptyset + \#J_\emptyset = m$. En particular, $\#I \leq m$. Además, en el caso en que $m > n$, como P es genérico, una condición necesaria para que P_I tenga ceros en $(\mathbb{C}^*)^{n-\#I}$ es que $\#I + \#J_I \leq n$ (es decir que la cantidad de ecuaciones $\#J_I$ no supere la cantidad de variables $n - \#I$). Esta condición es más débil pero más fácil de chequear que la condición 1. Veamos un algoritmo que busca los conjuntos I que satisfacen esa desigualdad y la condición 2.

Algoritmo 3.10 `SpecialSets`

INPUT: Una familia $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ de conjuntos finitos en $(\mathbb{Z}_{\geq 0})^n$.

1. $S_\emptyset := \min\{n, m\}$.
2. $\widetilde{\Phi} = \emptyset$.

   Si $S_\emptyset = m$, agregar $(\emptyset, \{1, \ldots, m\})$ al conjunto $\widetilde{\Phi}$.
3. *Para $k = 1, \ldots, \min\{n, m\}$:*

   Para todo I tal que $\#I = k$:

   a) $S_I = \min\{\{S_{I'}\}_{I' \subset I, \#I' = k-1}, k + \#J_I\}$.

b) Si $S_I = k + \#J_I$, agregar (I, J_I) al conjunto $\widetilde{\Phi}$.

OUTPUT: El conjunto $\widetilde{\Phi}$ de todos los pares de subconjuntos (I, J_I), tales que $I \subset \{1, \ldots, n\}$, $\#I + \#J_I \leq n$ y para todo $\widetilde{I} \subset I$, $\#\widetilde{I} + \#J_{\widetilde{I}} \geq \#I + \#J_I$.

El siguiente resultado nos permite asegurar que el conjunto obtenido por el algoritmo satisface las propiedades enunciadas en el output:

Lema 3.11 *Con la notación anterior, para cada $I \subset \{1, \ldots, n\}$ tal que $\#I \leq m$ vale la igualdad $S_I = \min_{\widetilde{I} \subset I}\{n, \#\widetilde{I} + \#J_{\widetilde{I}}\}$.*

Demostración: Usando inducción en $\#I$, en primer lugar si $\#I = 0$ tenemos que $S_\emptyset = \min\{n, \#\emptyset\ + \#J_\emptyset\}$ ya que $\#J_\emptyset = m$.

Sabiendo que la igualdad vale para todo subconjunto de $k-1$ elementos, sea $I \subset \{1, \ldots, n\}$ tal que $\#I = k$. Para todo $\widetilde{I}_0 \subsetneq I$ subconjunto propio de I, existe $I' \subset I$ tal que $\#I' = k-1$ y $\widetilde{I}_0 \subset I'$. Por la hipótesis inductiva, $S_{I'} = \min_{\widetilde{I} \subset I'}\{n, \#\widetilde{I} + \#J_{\widetilde{I}}\}$; en particular, $S_{I'} \leq \#\widetilde{I}_0 + \#J_{\widetilde{I}_0}$. Como por la definición de S_I sabemos que $S_I \leq S_{I'}$, entonces $S_I \leq \#\widetilde{I}_0 + \#J_{\widetilde{I}_0}$ y $S_I \leq n$. □

En cuanto a la complejidad del algoritmo `SpecialSets`, usaremos la notación de los algoritmos anteriores $N = \sum_{j=1}^{m} \#\mathcal{A}_j$. Podemos observar que para cada I tal que $\#I = k$, en el paso 3 basta chequear para cada $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathcal{A}_j$, $1 \leq j \leq m$, si $\alpha_i > 0$ para algún $i \in I$. Entonces, se requieren a lo sumo $kN + \#J_I + 1$ operaciones para calcular $k + \#J_I$. Tomar el mínimo entre $k+1$ números requiere hacer k comparaciones, con lo cual el paso $3a$ tiene una complejidad de $k(N+1) + \#J_I + 1$. Esto se realiza para cada subconjunto de $\{1, \ldots, n\}$ de k elementos con $1 \leq k \leq \min\{n, m\}$, con lo cual la cantidad de operaciones del algoritmo está acotada superiormente por $1 + \sum_{k=1}^{\min\{n,m\}} \binom{n}{k}(k(N+1) + m + 1) \leq 1 + n2^{n-1}(N+1) + (2^n - 1)(m+1)$. Como $m \leq N$, esta complejidad es del orden de $O(nN2^n)$.

Los ejemplos que siguen muestran que no es posible evitar una complejidad exponencial en el número de variables, ya que la cantidad de elementos del conjunto Φ puede ser de ese orden.

Ejemplo 3.12 Sean $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ la familia de conjuntos finitos en $(\mathbb{Z}_{\geq 0})^n$ tal que $\mathcal{A}_j = \{e_j, e_1 + e_j, \ldots, e_n + e_j\}$ para todo $1 \leq j \leq n$ y $P = (p_1, \ldots, p_n)$ un sistema de polinomios genéricos con soportes $\mathcal{A}$. Observar que, para todo $1 \leq j \leq n$, $p_j(X) = X_j L_j(X)$, donde $L_j(X)$ es una forma lineal afín genérica. Para este sistema y para todo $I \subsetneq \{1, \ldots, n\}$, el sistema P_I tiene $n - \#I$ ecuaciones en $n - \#I$ variables y exactamente una solución de coordenadas no nulas. Es fácil ver que en este caso $\Phi = \{I \mid I \subseteq \{1, \ldots, n\}\}$, que tiene 2^n elementos.

Ejemplo 3.13 Sea P el sistema genérico de n polinomios en $2n$ variables

$$P = \begin{cases} p_1(X_1, \ldots, X_{2n}) = a_{11}X_1X_2 + a_{12}X_3X_4 + \cdots + a_{1n}X_{2n-1}X_{2n} \\ \vdots \\ p_n(X_1, \ldots, X_{2n}) = a_{n1}X_1X_2 + a_{n2}X_3X_4 + \cdots + a_{nn}X_{2n-1}X_{2n} \end{cases}.$$

Usando la notación e_j para referirnos al $j-$ésimo vector de la base canónica de $\mathbb{R}^{2n}$, para todo $1 \leq j \leq n$, el soporte de p_j es $\mathcal{A}_j = \{e_{2k-1} + e_{2k} \mid 1 \leq k \leq n\}$. Los elementos de Φ son los conjuntos de la forma $I_S = \{2k - 1 \mid k \in S\} \cup \{2k \mid k \in \{1, \ldots, n\} \setminus S\}$ para todo $S \subset \{1, \ldots, n\}$. Este sistema define una variedad afín con 2^n componentes irreducibles de dimensión n: los subespacios de la forma $\{(x_1, \ldots, x_{2n}) \in \mathbb{C}^{2n} \mid x_i = 0 \text{ para todo } i \in I\}$ para todo $I \in \Phi$.

El output del algoritmo `SpecialSets` está formado por $2^n + 1$ elementos y todos ellos corresponden a un subconjunto de $\{1, \ldots, 2n\}$ que pertenece a Φ excepto uno: el par $(\emptyset, \{1, \ldots, 2n\})$. Como el soporte de los polinomios tiene n puntos, su dimensión es menor que n, con lo cual $\emptyset$ no está en Φ.

En el siguiente ejemplo el algoritmo `SpecialSets` devuelve como output únicamente los pares (I, J_I) que permiten conseguir las componentes de ceros del sistema:

Ejemplo 3.14 Sea $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ una familia de subconjuntos finitos de $(\mathbb{Z}_{\geq 0})^n$ tales que $\mathcal{MV}_n(\mathcal{A}) > 0$, para todo $1 \leq j \leq n$ vale $0 \notin \mathcal{A}_j$, y para todo $1 \leq i \leq n$ existe un entero d_{j_i} positivo que cumple $d_{j_i}e_i \in \mathcal{A}_j$. Para todo $1 \leq j \leq n$, sea p_j un polinomio genérico con soporte $\mathcal{A}_j$. Notar que para todo $I \neq \{1, \ldots, n\}$ el polinomio $(p_j)_I$ es no nulo. Luego, para todo $1 \leq k \leq n - 1$ y todo I tal que $\#I = k$ tenemos que $k + \#J_I > n$ con lo cual $\widetilde{\Phi} \subset \{(\emptyset, \{1, \ldots, n\}), (\{1, \ldots, n\}, \emptyset)\}$. Como la cantidad de polinomios es la misma que la de variables y $\#J_{\{1,\ldots,n\}} = 0$, $\widetilde{\Phi} = \{(\emptyset, \{1, \ldots, n\}), (\{1, \ldots, n\}, \emptyset)\} = \Phi$.

Un caso particular de sistemas ralos es el de los denominados *unmixed*, que son aquellos cuya familia de soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ cumple que $\mathcal{A}_1 = \cdots = \mathcal{A}_m$. Observar que, en este caso, para todo $I \subset \{1, \ldots, n\}$ vale que o bien $J_I = \emptyset$ o bien $J_I = \{1, \ldots, m\}$.

En lo que sigue, reformularemos nuestra caracterización de los elementos del conjunto Φ para estas familias de soportes y daremos un algoritmo para el cálculo de este conjunto.

Lema 3.15 *Sea $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ una familia de conjuntos finitos en $(\mathbb{Z}_{\geq 0})^n$ tal que $\mathcal{A}_1 = \cdots = \mathcal{A}_m$. El conjunto $\emptyset$ es un elemento de Φ si y solo si $\dim(\mathcal{A}_1) \geq m$. Un conjunto $I \subset \{1, \ldots, n\}$ no vacío es un elemento de Φ si y solo si $\#I \leq m$, $\#J_I = 0$ y $\#J_{\widetilde{I}} = m$ para todo $\widetilde{I} \subsetneq I$.*

Demostración: Como todos los soportes son iguales y $J_\emptyset = \{1, \ldots, m\}$, en el caso de $\emptyset$ la condición $\dim(\sum_{j \in J} \mathcal{A}_j^\emptyset) \geq \#J$ para todo $J \subset J_\emptyset$ es equivalente a que $\dim(\mathcal{A}_1) \geq m$.

Si $I \in \Phi$ es no vacío, como $\#J_I < \#J_I + \#I \leq \#J_\emptyset + \#\emptyset = m$, entonces $\#J_I = 0$. De la misma forma, $\#I \leq m$. Además, para todo $\widetilde{I} \subsetneq I$ vale $\#J_{\widetilde{I}} > 0$ pues $\#J_{\widetilde{I}} + \#\widetilde{I} \geq \#J_I + \#I = \#I > \#\widetilde{I}$.

Si $I \subset \{1, \ldots, n\}$ no vacío es tal que $\#I \leq m$, $\#J_I = 0$ y $\#J_{\widetilde{I}} = m$ para todo $\widetilde{I} \subsetneq I$, entonces para todo $\widetilde{I} \subset I$ vale que $\#J_{\widetilde{I}} + \#\widetilde{I} \geq m \geq \#J_I + \#I$. Además, como $\#J_I = 0$, la condición sobre la dimensión de $\sum_{j \in J_I} \mathcal{A}_j^I$ es trivial. □

Observemos que, para $I \subset \{1, \ldots, n\}$, vale que $\#J_I = 0$ si y solo si $X^\alpha \in \langle X_i \mid i \in I \rangle$ para todo $\alpha \in \mathcal{A}_1$.

Dado $\alpha \in \mathcal{A}_1$ llamamos ν_α al vector de n coordenadas tales que $(\nu_\alpha)_i = 0$ si $\alpha_i = 0$ y $(\nu_\alpha)_i = 1$ si $\alpha_i > 0$. Sea $\mathcal{I}$ el ideal de $\mathbb{Q}[X_1, \ldots, X_n]$ definido por $\mathcal{I} = \langle X^{\nu_\alpha} \mid \alpha \in \mathcal{A}_1 \rangle$. Notar que $\mathcal{I} = \sqrt{\langle X^\alpha \mid \alpha \in \mathcal{A}_1 \rangle}$ y que las componentes irreducibles de $V(\mathcal{I})$ son subespacios coordenados de $\mathbb{C}^n$ (ver [16, Chapter 9, Section 1, Proposition 1]). Usando la notación

$$\mathcal{W}_I = \{x \in \mathbb{C}^n \mid x_i = 0 \ \forall i \in I\}$$

para todo $I \subset \{1, \ldots, n\}$, para cada W componente irreducible de $V(\mathcal{I})$ existe $I \subset \{1, \ldots, n\}$ tal que $W = \mathcal{W}_I$.

Proposición 3.16 *Dado $I \subset \{1, \ldots, n\}$, son equivalentes:*

a) I es un conjunto minimal con la propiedad de que $\#J_I = 0$.

b) El subespacio lineal $\mathcal{W}_I$ es una componente irreducible de $V(\mathcal{I})$.

Demostración: Por un lado, si I es tal que $\#J_I = 0$, X^{ν_α} se anula sobre $\mathcal{W}_I$ para todo $\alpha \in \mathcal{A}_1$, con lo cual $\mathcal{W}_I$ está contenido en $V(\mathcal{I})$. Como $\mathcal{W}_I$ es irreducible, está contenido

en alguna componente irreducible $\mathcal{W}_{I'}$ de $V(\mathcal{I})$. Entonces $I' \subset I$, y por la minimalidad de I son iguales.

Por otro lado, si $\mathcal{W}_I$ es una componente irreducible de $V(\mathcal{I})$, se tiene que $\#J_I = 0$. Si $I' \subset I$ cumple que $\#J_{I'} = 0$, $\mathcal{W}_{I'}$ es una variedad irreducible contenida en $V(\mathcal{I})$. Como contiene la componente irreducible $\mathcal{W}_I$, son iguales y, por lo tanto, $I' = I$. □

Teniendo en cuenta esta proposición y el Lema 3.15, nos interesa hallar los conjuntos I no vacíos de cardinal menor o igual a m que dan lugar a componentes irreducibles de $V(\mathcal{I})$. Notemos $\mathcal{A}_1 = \{\alpha^{(1)}, \ldots, \alpha^{(N_1)}\}$ y, para todo $1 \leq k \leq N_1$, $\mathcal{I}_k = \langle X^{\nu_{\alpha^{(1)}}}, \ldots, X^{\nu_{\alpha^{(k)}}} \rangle$. Observando que $V(\mathcal{I}_1) = \bigcup_{i|(\nu_{\alpha^{(1)}})_i \neq 0} \{x_i = 0\}$ y $V(\mathcal{I}_{k+1}) = V(\mathcal{I}_k) \cap (\bigcup_{i|(\nu_{\alpha^{(k+1)}})_i \neq 0} \{x_i = 0\})$, obtenemos el siguiente algoritmo:

Algoritmo 3.17 `SpecialSetsUnmixed`
INPUT: Un conjunto finito $\mathcal{A}_1 = \{\alpha^{(1)}, \ldots, \alpha^{(N_1)}\} \subset (\mathbb{Z}_{\geq 0})^n$ y un número natural m.

1. *$SL = SL' = \emptyset$.*
2. *Para $i = 1, \ldots, n$, si $\alpha_i^{(1)} \neq 0$, agregar $\{i\}$ al conjunto SL.*
3. *Para $k = 2, \ldots, N_1$:*
   a) *Tomar $SL' := SL$ y $SL := \emptyset$.*
   b) *Para $i = 1, \ldots, n$, si $\alpha_i^{(k)} \neq 0$,*
   Para todo $I \in SL'$, si $\#I \cup \{i\} \leq m$, agregar $I \cup \{i\}$ a SL.
   c) *Para todo $I \in SL$*
   Para todo $I' \in SL \backslash \{I\}$, si $I' \subset I$ descartar I de SL.

OUTPUT: El conjunto $SL = \Phi \backslash \{\emptyset\}$

Aplicando el paso 3 para cada k obtenemos los conjuntos I tales que $\mathcal{W}_I$ es una componente irreducible de $V(\mathcal{I}_k)$ de dimensión mayor o igual a $n - m$. Cuando $k = N_1$, por el Lema 3.15 y la Proposición 3.16 el output del algoritmo es exactamente $\Phi \backslash \{\emptyset\}$.

Esto nos permite dar una caracterización más precisa de la descomposición equidimensional para sistemas unmixed y un algoritmo para calcularla.

Proposición 3.18 *Sea* $P = (p_1, \ldots, p_m)$ *un sistema ralo genérico con soportes* $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ *en* $(\mathbb{Z}_{\geq 0})^n$ *tales que* $\mathcal{A}_1 = \cdots = \mathcal{A}_m$. *Para* $k = 0, \ldots, n-1$, *sea* $V_k(P)$ *la componente equidimensional de* $V(P)$ *de dimensión* k. *Entonces,*

- *si* $k \neq n-m$, $V_k(P) = \bigcup_{\substack{\#I=n-k, \#J_I=0, \\ \#J_{\widetilde{I}}=m \ \forall \widetilde{I} \subset I}} \{x \in \mathbb{C}^n \mid x_i = 0 \text{ para todo } i \in I\}$
- *si* $m \leq n$, $V_{n-m}(P) = V^*(P) \cup \bigcup_{\substack{\#I=m, \#J_I=0, \\ \#J_{\widetilde{I}}=m \ \forall \widetilde{I} \subset I}} \{x \in \mathbb{C}^n \mid x_i = 0 \text{ para todo } i \in I\}$.

Esta descomposición equidimensional se puede obtener algorítmicamente aplicando los algoritmos `GenericToricSolve` y `SpecialSetsUnmixed`. La complejidad del algoritmo `SpecialSetsUnmixed` y del cálculo de la descomposición equidimensional para sistemas unmixed genéricos será calculada al final de la Sección 3.3.

3.2.2. Descomposición equidimensional

Presentamos a continuación un algoritmo que calcula la descomposición equidimensional de $V(P) \subset \mathbb{C}^n$ para un sistema de polinomios $P = (p_1, \ldots, p_m)$ en $\mathbb{Q}[X_1, \ldots, X_n]$ genérico con soportes arbitrarios $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$, donde $\mathcal{A}_j \subset (\mathbb{Z}_{\geq 0})^n$ para todo $1 \leq j \leq m$. Usaremos como antes la notación $\widetilde{\Phi}$ para la colección de pares de conjuntos (I, J_I) donde $I \subset \{1, \ldots, n\}$, $\#I + \#J_I \leq n$ y $\forall \widetilde{I} \subset I$, $\#\widetilde{I} + \#J_{\widetilde{I}} \geq \#I + \#J_I$.

Algoritmo 3.19 `GenericAffineSolve`

INPUT: Un sistema de polinomios $P = (p_1, \ldots, p_m)$ *en* $\mathbb{Q}[X_1, \ldots, X_n]$ *genérico con soportes* $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ *en* $(\mathbb{Z}_{\geq 0})^n$, *codificado en forma rala.*

1. *Aplicar el algoritmo* `SpecialSets` *a la familia* $\mathcal{A}$ *para obtener el conjunto* $\widetilde{\Phi}$.
2. $\mathcal{V}_k := \emptyset$ *para todo* $0 \leq k \leq n-1$.
3. *Para todo* $(I, J_I) \in \widetilde{\Phi}$:
   a) *Para cada* $j \in J_I$, *calcular* $\mathcal{A}_j^I := \{\pi_I(\alpha) \mid \alpha \in \mathcal{A}_j \text{ tal que } \alpha_i = 0 \ \forall i \in I\}$. *Obtener la representación rala del sistema* P_I *con esos soportes.*
   b) *Aplicar el algoritmo* `GenericToricSolve` *al sistema ralo* P_I *para obtener una resolución geométrica* R^I *de* $V^*(P_I)$.
   c) *Si* $R^I \neq \emptyset$:

1) Obtener la resolución geométrica $\varphi_I(R^I)$ de la unión de todas las componentes irreducibles W de $V(P)$ tales que $I_W = I$.

2) Si $n - \#I - \#J_I = k$, agregar $\varphi_I(R^I)$ a la lista $\mathcal{V}_k$.

OUTPUT: Una familia de listas $\mathcal{V}_k$, $0 \leq k \leq n-1$, de resoluciones geométricas, donde cada lista $\mathcal{V}_k$ describe la componente equidimensional de $V(P)$ de dimensión k o es vacía si dicha componente lo es.

Por la Proposición 3.7 y el Teorema 3.8, aplicando el paso 3 para cada $I \in \Phi$ obtendríamos todas las componentes equidimensionales de $V(P)$ para un sistema genérico P con soportes $\mathcal{A}$. En lugar de buscar Φ, el algoritmo anterior obtiene en primer lugar el conjunto $\widetilde{\Phi}$ por medio de la subrutina `SpecialSets`. Observar que, para todo $I \in \Phi$, $(I, J_I) \in \widetilde{\Phi}$. Luego, el paso $3b$ permite chequear para cada conjunto I encontrado con la subrutina `SpecialSets` si $I \in \Phi$ y al mismo tiempo (en caso de que así sea) encontrar las componentes de ceros de $V(P)$ que intersecan $\bigcap_{i \notin I} \{x_i \neq 0\}$.

En cuanto a la complejidad del algoritmo, en el paso 1 la complejidad de aplicar la subrutina `SpecialSets` es $O(nN2^n)$. El paso $3a$ no modifica el orden de la complejidad. En el paso $3b$, utilizamos un pre-procesamiento que calcule las celdas mixtas en una subdivisión mixta fina de $(\mathcal{A}^I, \Delta^{(n-\#I-\#J_I)})$ inducida por un levantamiento genérico (como en los algoritmos anteriores, no incluimos el costo de este proceso previo en nuestras estimaciones de complejidad). Este pre-procesamiento permite también decidir si un conjunto I cumple que $\dim(\sum_{j \in J} \mathcal{A}^I_j) \geq \#J$ para todo $J \subset J_I$, es decir, decidir si el conjunto $I \in \Phi$ (es la condición que no le pedimos a los elementos de $\widetilde{\Phi}$), ya que por la Proposición 1.12 esta condición es equivalente a que $\mathcal{MV}_{n-\#I}(\mathcal{A}^I, \Delta^{(n-\#I-\#J_I)}) > 0$. Entonces, la complejidad del paso 3 se considera solo para los conjuntos $I \in \Phi$. Para cada uno de ellos, en el paso $3b$ aplicamos el algoritmo `GenericToricSolve`. Si llamamos N_I, d_I, $\mathcal{D}_I$, Υ_I y $\mathcal{E}_I$ a los valores asociados a la complejidad de aplicar el algoritmo al sistema P_I para cada $I \in \Phi$, por la Proposición 3.4, la complejidad total de este paso es del orden de

$$O\Big(\sum_{I \in \Phi} (n - \#I)^3 \big(N_I + (n - \#I - \#J_I)(n - \#I)\big) \log(d_I) M(\mathcal{D}_I)$$

$$\big(M(\Upsilon_I)\,(M(\mathcal{D}_I) + M(\mathcal{E}_I)) + \mathcal{D}_I^2\big)\Big).$$

Para estimar la suma sobre Φ, se puede observar que para todo $I \in \Phi$ vale $N_I \leq \sum_{j=1}^{m} \#\mathcal{A}_j = N$ y $d_I \leq \max_{1 \leq j \leq m}\{\deg(p_j)\} = d$. Además, por el Teorema 3.8, $\mathcal{D} := \sum_{I \in \Phi} \mathcal{D}_I =$

$\deg(V(P))$. Para acotar $\mathcal{E}_I$, tomamos $\omega_{\text{máx}}$ el máximo valor que toman las funciones de levantamiento de los soportes $\mathcal{A}^I$ para todo $I \in \Phi$. Entonces, para cada conjunto $I \in \Phi$, vale

$$\begin{aligned}\mathcal{E}_I &\leq \mathcal{MV}_{n-\#I+1}(\Delta \times \{0\}, (\mathcal{A}_j^I \times \{0, \omega_{\text{máx}}\})_{j\in J_I}, (\Delta \times \{0, \omega_{\text{máx}}\})^{(n-\#I-\#J_I)}) \\ &\leq \omega_{\text{máx}}\Big((n-\#I-\#J_I)\mathcal{MV}_{n-\#I}(\mathcal{A}^I, \Delta^{(n-\#I-\#J_I)}) \\ &\quad + \sum_{\ell\in J_I} \mathcal{MV}_{n-\#I}((\mathcal{A}_j^I)_{j\neq\ell}, \Delta^{(n-\#I-\#J_I+1)})\Big),\end{aligned}$$

donde la primera desigualdad es consecuencia de la monotonía del volumen mixto y la segunda se prueba como en [45, Lemma 2.3]. De esta manera, y como el paso 3*c* no cambia esta complejidad, si $\mathcal{E}_{\text{máx}} := \text{máx}_{I\in\Phi}\{(n-\#I-\#J_I)\mathcal{MV}_{n-\#I}(\mathcal{A}^I, \Delta^{(n-\#I-\#J_I)}) + \sum_{\ell\in J_I} \mathcal{MV}_{n-\#I}((\mathcal{A}_j^I)_{j\neq\ell}, \Delta^{(n-\#I-\#J_I+1)})\}$ y $\Upsilon_{\text{máx}} := \text{máx}_{I\in\Phi}\{\Upsilon_I\}$, obtenemos el siguiente resultado:

Teorema 3.20 *Sea $P = (p_1, \ldots, p_m)$ un sistema de polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ genérico con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ en $(\mathbb{Z}_{\geq 0})^n$. El algoritmo probabilístico* `GenericAffineSolve` *calcula, para todo $0 \leq k \leq n-1$, una lista $\mathcal{V}_k$ de resoluciones geométricas. Cada lista $\mathcal{V}_k$ describe la componente equidimensional de $V(P)$ de dimensión k o es vacía si dicha componente lo es. Usando la notación anterior, la complejidad del algoritmo es del orden de*

$$O\left(n2^n N + n^3(N+n^2)\log(d)M(\mathcal{D})\left(M(\Upsilon_{\text{máx}})\left(M(\mathcal{D}) + M(\omega_{\text{máx}}\mathcal{E}_{\text{máx}})\right) + \mathcal{D}^2\right)\right).$$

3.3. Cota para el grado

Para un sistema ralo genérico P con soportes fijos, el Teorema 3.8 nos permite calcular exactamente el grado de la variedad $V(P)$. Sin embargo, a diferencia de las cotas para la cantidad de soluciones aisladas, este "grado genérico" no es una cota superior para el grado de una variedad definida por un sistema particular con los mismos soportes. Veamos un ejemplo de esto:

Ejemplo 3.21 Sea $F = (f_1, f_2, f_3)$ el sistema de 3 polinomios en 3 variables dado por los polinomios

$$\begin{cases} f_1 = X_1X_2 - X_1 - X_2 + 1 = (X_1-1)(X_2-1) \\ f_2 = X_1X_3 - X_1 - X_3 + 1 = (X_1-1)(X_3-1) \\ f_3 = X_2X_3 - X_2 - X_3 + 1 = (X_2-1)(X_3-1) \end{cases}$$

La familia de soportes de este sistema es $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$, donde $\mathcal{A}_1 = \{(0,0,0),(1,0,0),(0,1,0),(1,1,0)\}$, $\mathcal{A}_2 = \{(0,0,0),(1,0,0),(0,0,1),(1,0,1)\}$ y $\mathcal{A}_3 = \{(0,0,0),(0,1,0),(0,0,1),(0,1,1)\}$. La variedad definida por el sistema F está compuesta por las rectas

$$\{(1,1,x_3) \mid x_3 \in \mathbb{C}\}, \qquad \{(1,x_2,1) \mid x_2 \in \mathbb{C}\} \quad \text{y} \quad \{(x_1,1,1) \mid x_1 \in \mathbb{C}\}$$

y tiene grado 3. Sin embargo, la variedad definida por un sistema polinomial genérico con los mismos soportes tiene grado $\mathcal{MV}_3(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3) = 2$. Dado que el volumen mixto de los soportes acota la cantidad de ceros aislados de coordenadas no nulas del sistema, podría pensarse que esta diferencia está relacionada con las componentes de ceros que no intersecan $(\mathbb{C}^*)^3$. Sin embargo, esto no es así, ya que en este ejemplo cada una de las componentes irreducibles tiene intersección no vacía con $(\mathbb{C}^*)^3$.

Para sistemas arbitrarios F de n ecuaciones en n variables, presentamos la siguiente cota para el grado de la variedad $V(F)$:

Teorema 3.22 *Sea $F = (f_1, \ldots, f_n)$ un sistema de n polinomios en $\mathbb{C}[X_1, \ldots, X_n]$ con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$. Sea Δ el conjunto de vértices del símplex standard de $\mathbb{R}^n$. Entonces*

$$\deg(V(F)) \leq \mathcal{MV}_n(\mathcal{A}_1 \cup \Delta, \ldots, \mathcal{A}_n \cup \Delta).$$

Antes de probar el teorema, introduciremos cierta notación y probaremos un resultado previo. Sean $r_j = \#(\mathcal{A}_j \cup \Delta) - 1$ para todo $1 \leq j \leq n$ y $\varphi : \mathbb{C}^n \to \mathbb{P}^n \times \mathbb{P}^{r_1} \times \cdots \times \mathbb{P}^{r_n}$ el morfismo

$$\varphi(x) = ((1:x), (x^\alpha)_{\alpha \in \mathcal{A}_1 \cup \Delta}, \ldots, (x^\alpha)_{\alpha \in \mathcal{A}_n \cup \Delta}). \tag{3.3}$$

Notando $f_j = \sum_{\alpha \in \mathcal{A}_j} a_{j,\alpha} X^\alpha$ para todo $1 \leq j \leq n$, sea L_j la forma lineal en $\mathbb{P}^{r_j}$ dada por $L_j = \sum_{\alpha \in \mathcal{A}_j} a_{j,\alpha} X_{j,\alpha}$. Llamemos $\mathcal{X} = \overline{\varphi(\mathbb{C}^n)}$.

Para todo $0 \leq k \leq n$ y todo $S \subset \{1, \ldots, k\}$ definimos recursivamente las variedades $\mathcal{X}_{k,S}$ de la siguiente manera:

1. $\mathcal{X}_{0,\emptyset} = \mathcal{X}$.
2. Para todo $1 \leq k \leq n$ y $S \subset \{1, \ldots, k\}$:
   - Si $k \notin S$, $\mathcal{X}_{k,S}$ es la unión de las componentes irreducibles de $\mathcal{X}_{k-1,S}$ incluidas en $\{L_k = 0\}$.
   - Si $k \in S$, $\mathcal{X}_{k,S}$ es la intersección de $\{L_k = 0\}$ con la unión de las componentes irreducibles de $\mathcal{X}_{k-1,S\setminus\{k\}}$ que no están incluidas en $\{L_k = 0\}$.

Notar que, para todo $0 \leq k \leq n$ y todo $S \subset \{1, \ldots, k\}$, la variedad $\mathcal{X}_{k,S}$ es equidimensional de dimensión $n - \#S$: En el caso de $\mathcal{X}_{0,\emptyset} = \overline{\varphi(\mathbb{C}^n)}$, la dimensión es claramente n. Con $k > 0$, tenemos dos casos posibles. Para $\mathcal{X}_{k,S}$ con $k \notin S$, por definición, $\mathcal{X}_{k,S}$ es la unión de algunas componentes irreducibles de $\mathcal{X}_{k-1,S}$ que tienen dimensión $n - \#S$. Por otro lado, para $\mathcal{X}_{k,S}$ con $k \in S$, esta variedad es la unión de la intersección de $\{L_k = 0\}$ con algunas componentes irreducibles de $\mathcal{X}_{k-1,S\setminus\{k\}}$ que tienen dimensión $n - \#S + 1$. Como las componentes consideradas son aquéllas que no están contenidas en $\{L_k = 0\}$, cada una de las intersecciones es o bien vacía o bien tiene dimensión $n - \#S$.

Sean W una subvariedad equidimensional de $\mathcal{X}$ y $r, k \in \mathbb{Z}_{\geq 0}$ tales que $n - k + r = \dim(W)$. En el mismo espíritu que la definición de grado de una variedad definimos

$$\deg_{(r,0_k,1_{n-k})}(W) = \max\left\{\#\Big(W \cap \bigcap_{j=1}^{r}\{\ell_{0,j} = 0\} \cap \bigcap_{j=k+1}^{n}\{\ell_j = 0\}\Big)\right\}$$

donde el máximo es sobre las intersecciones finitas $W \cap \bigcap_{j=1}^{r}\{\ell_{0,j} = 0\} \cap \bigcap_{j=k+1}^{n}\{\ell_j = 0\}$ de W con los ceros comunes de las $(n-k+r)$-uplas $(\ell_{0,1}, \ldots, \ell_{0,r}, \ell_{k+1}, \ldots, \ell_n)$ tales que $\ell_{0,1}, \ldots, \ell_{0,r}$ son formas lineales en $\mathbb{P}^n$ y $\ell_{k+1}, \ldots, \ell_n$ son formas lineales en $\mathbb{P}^{r_{k+1}}, \ldots, \mathbb{P}^{r_n}$ respectivamente. El número $k \geq 0$ indica que intersecamos los últimos $n - k$ espacios proyectivos $\mathbb{P}^{r_{k+1}}, \ldots, \mathbb{P}^{r_n}$ con hiperplanos mientras que $\mathbb{P}^{r_1}, \ldots, \mathbb{P}^{r_k}$ no se cortan. Al igual que para el grado de una variedad (ver la Definición 1.3 y [40]), la cantidad de puntos en la intersección $W \cap \bigcap_{j=1}^{r}\{\ell_{0,j} = 0\} \cap \bigcap_{j=k+1}^{n}\{\ell_j = 0\}$, cuando es finita, está acotada superiormente y el máximo se alcanza genéricamente.

En el caso de $r = k = 0$ y $W = \mathcal{X}$, sean $\widetilde{L}_1, \ldots, \widetilde{L}_n$ las formas lineales genéricas $\widetilde{L}_j = \sum_{\alpha \in \mathcal{A}_j \cup \Delta} \widetilde{a}_{j,\alpha} X_{j,\alpha}$. Tenemos que $\deg_{(0,0_0,1_n)}(\mathcal{X})$ es la cantidad de ceros comunes en $(\mathbb{C}^*)^n$ de $\widetilde{L}_j((X^\alpha)_{\alpha \in \mathcal{A}_j \cup \Delta}) = \sum_{\alpha \in \mathcal{A}_j \cup \Delta} \widetilde{a}_{j,\alpha} X^\alpha$ para todo $1 \leq j \leq n$. Sea $g_j(X) = \sum_{\alpha \in \mathcal{A}_j \cup \Delta} \widetilde{a}_{j,\alpha} X^\alpha$ para todo $1 \leq j \leq n$. Observamos que $G = (g_1, \ldots, g_n)$ es un sistema genérico con soportes $(\mathcal{A}_1 \cup \Delta, \ldots, \mathcal{A}_n \cup \Delta)$. Luego,

$$\deg_{(0,0_0,1_n)}(\mathcal{X}) = \mathcal{MV}_n(\mathcal{A}_1 \cup \Delta, \ldots, \mathcal{A}_n \cup \Delta). \tag{3.4}$$

Lema 3.23 *Con las hipótesis y notaciones previas,*

$$\deg_{(k-\#S,0_k,1_{n-k})}(\mathcal{X}_{k,S}) \geq$$

$$\geq \deg_{(k+1-\#S,0_{k+1},1_{n-k-1})}(\mathcal{X}_{k+1,S}) + \deg_{(k-\#S,0_{k+1},1_{n-k-1})}(\mathcal{X}_{k+1,S\cup\{k+1\}}).$$

Demostración: Para toda variedad $\mathcal{X}_{k,S}$, llamando $\widetilde{\mathcal{X}_{k,S}}$ a la unión de todas las componentes irreducibles de $\mathcal{X}_{k,S}$ que no están contenidas en $\{L_{k+1}=0\}$, tenemos que $\mathcal{X}_{k,S} = \mathcal{X}_{k+1,S} \cup \widetilde{\mathcal{X}_{k,S}}$. Dada una variedad equidimensional W tal que $\dim(W) = n-k+r$, sabemos que el grado $\deg_{(r,0_k,1_{n-k})}(W)$ es genéricamente la cantidad de puntos en $W \cap \bigcap_{j=1}^{r} \{\ell_{0,j}=0\} \cap \bigcap_{j=k+1}^{n} \{\ell_j = 0\}$ para $\ell_{0,1},\ldots,\ell_{0,r}$ formas lineales genéricas en $\mathbb{P}^n$ y $\ell_{k+1},\ldots,\ell_n$ formas lineales genéricas en $\mathbb{P}^{r_{k+1}},\ldots,\mathbb{P}^n$. Usando esta propiedad para las tres variedades $\mathcal{X}_{k,S}$, $\mathcal{X}_{k+1,S}$ y $\widetilde{\mathcal{X}_{k,S}}$, tenemos que

$$\deg_{(k-\#S,0_k,1_{n-k})}(\mathcal{X}_{k,S}) = \deg_{(k-\#S,0_k,1_{n-k})}(\mathcal{X}_{k+1,S}) + \deg_{(k-\#S,0_k,1_{n-k})}(\widetilde{\mathcal{X}_{k,S}}).$$

Al definir el morfismo φ en (3.3) agregamos a cada uno de los soportes $\mathcal{A}_1,\ldots,\mathcal{A}_n$ el conjunto Δ de los vértices del símplex standard de $\mathbb{R}^n$. Por esta razón, las coordenadas en $\mathbb{P}^n$ de cada punto de las variedades $\mathcal{X}_{k,S} \subset \mathbb{P}^n \times \mathbb{P}^{r_1} \times \cdots \times \mathbb{P}^{r_n}$ figuran nuevamente entre las coordenadas de ese punto en $\mathbb{P}^{r_j}$ para todo $1 \le j \le n$. En consecuencia, si cortamos $\mathcal{X}_{k+1,S}$ con el hiperplano definido por una forma lineal ℓ_0 en $\mathbb{P}^n$ da como resultado la misma variedad que al cortar $\mathcal{X}_{k+1,S}$ con el hiperplano definido por una forma lineal ℓ_{k+1} en $\mathbb{P}^{r_{k+1}}$ que involucre las mismas variables y tenga los mismos coeficientes en esas variables que ℓ_0, es decir $\mathcal{X}_{k+1,S} \cap \{\ell_0 = 0\} = \mathcal{X}_{k+1,S} \cap \{\ell_{k+1} = 0\}$. De esta manera, y nuevamente usando la genericidad del grado definido y que es cota superior para la cantidad de puntos en la intersección considerada, tenemos que

$$\begin{aligned}
\deg_{(k-\#S,0_k,1_{n-k})}(\mathcal{X}_{k+1,S}) &\ge \deg_{(k+1-\#S,0_{k+1},1_{n-k-1})}(\mathcal{X}_{k+1,S}), \text{ y} \\
\deg_{(k-\#S,0_k,1_{n-k})}(\widetilde{\mathcal{X}_{k,S}}) &\ge \deg_{(k-\#S,0_{k+1},1_{n-k-1})}\left(\widetilde{\mathcal{X}_{k,S}} \cap \{L_{k+1}=0\}\right) \\
&= \deg_{(k-\#S,0_{k+1},1_{n-k-1})}(\mathcal{X}_{k+1,S\cup\{k+1\}}).
\end{aligned}$$

□

Ya podemos probar nuestra cota para el grado de la variedad definida por un sistema ralo arbitrario de n ecuaciones con n incógnitas:

Demostración del Teorema 3.22: Sea $\pi : \mathbb{P}^n \times \mathbb{P}^{r_1} \times \cdots \times \mathbb{P}^{r_n} \to \mathbb{P}^n$ la proyección al primer factor. Inductivamente, vemos que, para todo $0 \le k \le n$, $V(f_1,\ldots,f_k) \subseteq \bigcup_{S\subset\{1,\ldots,k\}} \pi(\mathcal{X}_{k,S})$ en $\mathbb{P}^n$: si $k \ge 1$ y $(1:x) \in V(f_1,\ldots,f_k)$, por hipótesis inductiva existe $S_0 \subset \{1,\ldots,k-1\}$ tal que $(1:x) \in \pi(\mathcal{X}_{k-1,S_0})$. Entonces, $\varphi(x) \in \mathcal{X}_{k-1,S_0}$ y $L_k(\varphi(x)) = f_k(x) = 0$. Según a qué componente irreducible de $\mathcal{X}_{k-1,S_0}$ pertenece $\varphi(x)$, tenemos que $\varphi(x) \in \mathcal{X}_{k,S_0}$ o bien $\varphi(x) \in \mathcal{X}_{k,S_0\cup\{k\}}$, con lo cual $(1:x) = \pi(\varphi(x)) \in \bigcup_{S\subset\{1,\ldots,k\}} \pi(\mathcal{X}_{k,S})$.

En particular, $V(F) \subseteq \bigcup_{S\subset\{1,\ldots,n\}} \pi(\mathcal{X}_{n,S})$. En consecuencia,

$$\deg(V(F)) \leq \deg\Big(\bigcup_{S\subset\{1,\ldots,n\}} \pi(\mathcal{X}_{n,S})\Big) \leq \sum_{S\subset\{1,\ldots,n\}} \deg \pi(\mathcal{X}_{n,S}).$$

Como el grado de $\pi(\mathcal{X}_{n,S})$ es la cantidad de puntos en la intersección de esa variedad con tantos hiperplanos genéricos como su dimensión, que es la misma que la cantidad de puntos en la intersección de $\mathcal{X}_{n,S}$ con tantos hiperplanos genéricos en $\mathbb{P}^n$ como su dimensión, por la definición del grado $\deg_{(n-\#S,0_n,1_0)}(\mathcal{X}_{n,S})$, tenemos que $\deg \pi(\mathcal{X}_{n,S}) = \deg_{(n-\#S,0_n,1_0)}(\mathcal{X}_{n,S})$ para todo $S \subset \{1,\ldots,n\}$ Luego,

$$\deg(V(F)) \leq \sum_{S\subset\{1,\ldots,n\}} \deg_{(n-\#S,0_n,1_0)}(\mathcal{X}_{n,S}).$$

Por inducción, aplicando el Lema 3.23, tenemos que la sucesión de números $\sum_{S\subset\{1,\ldots,k\}} \deg_{(k-\#S,0_k,1_{n-k})}(\mathcal{X}_{k,S})$ para $0 \leq k \leq n$ es decreciente. En particular,

$$\sum_{S\subset\{1,\ldots,n\}} \deg_{(n-\#S,0_n,1_0)}(\mathcal{X}_{n,S}) \leq \deg_{(0,0_0,1_n)}(\mathcal{X}_{0,\emptyset}).$$

Teniendo en cuenta las desigualdades anteriores y la igualdad (3.3), concluimos que

$$\begin{aligned} \deg(V(F)) &\leq \sum_{S\subset\{1,\ldots,n\}} \deg_{(n-\#S,0_n,1_0)}(\mathcal{X}_{n,S}) \\ &\leq \deg_{(0,0_0,1_n)}(\mathcal{X}_{0,\emptyset}) = \mathcal{MV}_n(\mathcal{A}_1 \cup \Delta, \ldots, \mathcal{A}_n \cup \Delta). \end{aligned}$$

□

En el siguiente ejemplo mostramos un sistema de polinomios para el cual la cota para el grado dada en el Teorema 3.22 resulta ser mucho mayor que el grado de una variedad definida por polinomios genéricos con los mismos soportes, y sin embargo para el sistema particular considerado, dicha cota se alcanza.

Ejemplo 3.24 Sea $r < n$ y sean $f_1, \ldots, f_n \in \mathbb{Q}[X_1, \ldots, X_n]$ polinomios con soportes $S = \{\alpha \in (\mathbb{Z}_{\geq 0})^n \mid \alpha_i \leq d$ para todo $1 \leq i \leq r$ y $\alpha_i = 0$ para todo $r+1 \leq i \leq n\}$ (es decir, $f_1, \ldots, f_n$ son polinomios en las variables $X_1, \ldots, X_r$ de grado d).

Podemos observar que $\mathcal{MV}_n(S^{(n)}) = 0$ y $\mathcal{SM}(S^{(n)}) = 0$. Más aún, como todos los soportes contienen el origen, para todo $I \subset \{1, \ldots, n\}$ no vacío vale $\#I + \#J_I > n$. Entonces, la variedad definida por un sistema genérico de n ecuaciones con esos soportes es vacía. Sin embargo, la cota que presentamos en el teorema anterior para el grado de $V(F)$ es

$\mathcal{MV}_n((S \cup \Delta)^{(n)}) = d^r$. Para calcular este volumen mixto, observamos que la cápsula convexa de $S \cup \Delta$ es la misma que la del conjunto $\{0, de_1, \ldots, de_r, e_{r+1}, \ldots, e_n\}$ donde $\{e_i\}_{i=1}^n$ es la base canónica de $\mathbb{R}^n$ y 0 el origen de coordenadas. Consideremos un sistema genérico G con esos soportes y apliquemos el cambio de variables $Z_i = X_i^d$ para todo $i \leq r$ y $Z_i = X_i$ para todo $i > r$. Resolviendo el sistema lineal resultante vemos que el sistema genérico G tiene d^r soluciones de coordenadas no nulas. El Teorema de Bernstein asegura que el volumen mixto de la familia de soportes del sistema G es d^r.

Consideremos ahora el caso en que los coeficientes de $f_1, \ldots, f_n$ son tales que $f_1, \ldots, f_r$ tienen d^r ceros en $(\mathbb{C}^*)^r$ y $f_{r+1}, \ldots, f_n$ son combinaciones lineales de $f_1, \ldots, f_r$. La cota del Teorema 3.22 se alcanza: como el subsistema $f_1, \ldots, f_r$ tiene d^r ceros comunes en $\mathbb{C}^r$ que anulan también a $f_{r+1}, \ldots, f_n$, el sistema $F = (f_1, \ldots, f_n)$ define una variedad en $\mathbb{C}^n$ formada por d^r variedades lineales de dimensión $n - r$.

En el ejemplo anterior la cota de grado se alcanza para un sistema de polinomios no genérico. A continuación presentamos un ejemplo donde esto ocurre en el caso genérico.

Ejemplo 3.25 Sea P el sistema genérico del Ejemplo 3.12. Como mencionamos en ese ejemplo, la variedad definida por los polinomios del sistema está compuesta por 2^n puntos aislados. Llamando $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ a su familia de soportes, tenemos que $\mathcal{A}_j = \{e_j, e_i + e_j \mid 1 \leq i \leq n\} = \{0, e_j\} + \Delta$ para todo $1 \leq j \leq n$. Luego, usando la multilinealidad del volumen mixto y la Proposición 1.11 tenemos que $\mathcal{MV}_n(\mathcal{A}_1 \cup \Delta, \ldots, \mathcal{A}_n \cup \Delta) = \sum_{\substack{0 \leq k \leq n \\ \{j_1, \ldots, j_k\} \subset \{1, \ldots, n\}}} \mathcal{MV}_n(\{0, e_{j_1}\}, \ldots, \{0, e_{j_k}\}, \Delta^{(n-k)}) = 2^n$.

Al final de la Sección 3.2.1 planteamos un algoritmo para hallar el conjunto Φ que determina las componentes irreducibles de la variedad definida por un sistema ralo genérico de polinomios con todos sus soportes iguales. Usaremos la cota del Teorema 3.22 para estimar la complejidad de ese algoritmo.

Sea $P = (p_1, \ldots, p_m)$ un sistema genérico de polinomios con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ en $(\mathbb{Z}_{\geq 0})^n$ tal que $\mathcal{A}_1 = \cdots = \mathcal{A}_m$. Notamos $\mathcal{A}_1 = \{\alpha^{(1)}, \ldots, \alpha^{(N_1)}\}$. Para todo $1 \leq k \leq N_1$, en la Sección 3.2.1 definimos los ideales $\mathcal{I}_k = \langle X^{\nu_{\alpha^{(1)}}}, \ldots, X^{\nu_{\alpha^{(k)}}} \rangle$ donde para todo $\alpha \in \mathcal{A}_1$, ν_α es el vector en $\mathbb{Z}^n$ tal que $(\nu_\alpha)_i = 0$ si $\alpha_i = 0$ y $(\nu_\alpha)_i = 1$ si $\alpha_i \geq 1$. Sea $\mathcal{A}_1^{(k)} = \{\alpha^{(1)}, \ldots, \alpha^{(k)}\}$ y sea $G^{(k)} = (g_1^{(k)}, \ldots, g_n^{(k)})$ un sistema genérico de n polinomios con soportes en $\mathcal{A}_1^{(k)}$. De la misma forma, para cada $I \subset \{1, \ldots, n\}$, sea $J_I^{(k)}$ el conjunto de índices de $G_I^{(k)}$. Sea $\Phi^{(k)}$ el conjunto de los $I \subset \{1, \ldots, n\}$ tales que $\#J_I^{(k)} = 0$ y $\#J_{\widetilde{I}}^{(k)} = n$ para todo $\widetilde{I} \subsetneq I$.

Lema 3.26 *Con la notación anterior,* $\#\Phi^{(k)} = \deg(V(\mathcal{I}_k)) \leq \mathcal{MV}_n((\mathcal{A}_1 \cup \Delta)^{(n)})$ *para todo* $1 \leq k \leq N_1$.

Demostración: Recordemos que notamos $\mathcal{W}_I = \{x \in \mathbb{C}^n \mid x_i = 0 \ \forall \ i \in I\}$. Por la Proposición 3.16, $I \in \Phi^{(k)}$ si y solo si $\mathcal{W}_I$ es una componente irreducible de $V(\mathcal{I}_k)$. Entonces, $\deg(V(\mathcal{I}_k)) = \#\Phi^{(k)}$. Además, por el Lema 3.15 aplicado a la familia de soportes de $G^{(k)}$, $I \in \Phi^{(k)}$ si y solo si $\mathcal{W}_I$ es una componente irreducible de $V(G^{(k)})$ para $I \neq \emptyset$. En consecuencia, $\#\Phi^{(k)} \leq \deg(V(G^{(k)}))$. Finalmente $\deg(V(G^{(k)})) \leq \mathcal{MV}_n((\mathcal{A}_1^{(k)} \cup \Delta)^{(n)}) \leq \mathcal{MV}_n((\mathcal{A}_1 \cup \Delta)^{(n)})$ donde la primera desigualdad vale por el Teorema 3.22 y la segunda por la monotonía del volumen mixto. □

Podemos entonces estimar la complejidad del algoritmo `SpecialSetsUnmixed` (Algoritmo 3.17). El paso 2 requiere a lo sumo n comparaciones. Recordando que $V(\mathcal{I}_1) = \bigcup_{i|(\nu_{\alpha^{(1)}})_i \neq 0} \{x_i = 0\}$ y $V(\mathcal{I}_{k+1}) = V(\mathcal{I}_k) \cap (\bigcup_{i|(\nu_{\alpha^{(k+1)}})_i \neq 0} \{x_i = 0\})$, observamos que en la k-ésima instancia del paso 3 (con $2 \leq k \leq N_1$), el algoritmo calcula los $I \in \Phi^{(k)}$ con $\#I \leq m$. Por el Lema 3.26, hay a lo sumo $D = \mathcal{MV}_n((\mathcal{A}_1 \cup \Delta)^{(n)})$ elementos de SL'. En el paso $3b$, tenemos n comparaciones de las coordenadas de $\alpha^{(k)}$ con cero para construir a lo sumo Dn elementos posibles para SL. En el paso $3c$, comparar dos elementos de SL precisa $O(n)$ operaciones. La complejidad total del algoritmo es entonces del orden de $O(N_1 D^2 n^3)$.

La complejidad del algoritmo subyacente a la Proposición 3.18 se obtiene sumando a esta complejidad la del algoritmo `GenericToricSolve` para el cálculo de la descomposición equidimensional de $V(P)$.

3.4. Sistemas no genéricos

En la Sección 3.2.2 presentamos un algoritmo para el cálculo de la descomposición equidimensional de la variedad afín definida por un sistema ralo genérico. A diferencia del caso de ceros aislados, no todas las componentes de una variedad definida por polinomios ralos pueden hallarse mediante una homotopía encontrando en primer lugar las componentes de una variedad definida por polinomios genéricos con los mismos soportes. Veamos un ejemplo trivial de esto.

Ejemplo 3.27 Sea F el sistema $F = \begin{cases} f_1(X_1, X_2) = X_1(X_2 - 1) \\ f_2(X_1, X_2) = X_1(X_2 - 1) \end{cases}$.

La variedad $V(F) \subset \mathbb{C}^2$ tiene dos componentes de dimensión 1: $W_1 = \{(0, x_2) \mid x_2 \in \mathbb{C}\}$ y $W_2 = \{(x_1, 1) \mid x_1 \in \mathbb{C}\}$. Sin embargo, un sistema genérico con los mismos soportes solo tendría a W_1 como conjunto de soluciones.

En esta sección presentamos un algoritmo para describir el conjunto de ceros de un sistema ralo cuadrado de polinomios arbitrarios. En este caso lo describiremos a través de un conjunto finito de puntos representativos de cada componente irreducible de la variedad. La complejidad de este nuevo algoritmo depende polinomialmente de la cota para el grado obtenida en la Sección 3.3. El algoritmo se basa en el hecho de que intersecando una variedad con una variedad lineal genérica de dimensión $n-k$ se consiguen puntos en cada componente irreducible de dimensión k.

Sea $F = (f_1, \ldots, f_n)$ un sistema de polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$. Para todo $k = 0, \ldots, n-1$ sea $V_k(F)$ la componente equidimensional de $V(F)$ de dimensión k. En [65, Chapter 13, Section 1] se introduce la idea de *conjuntos de puntos testigo* que, para cada $0 \leq k \leq n-1$, consiste en el conjunto finito de puntos que se obtiene intersecando $V_k(F)$ con k hiperplanos genéricos $\{L_1 = 0\}, \ldots, \{L_k = 0\}$ definidos a partir de formas lineales afines genéricas $L_1, \ldots, L_{n-1}$ en $\mathbb{Q}[X_1, \ldots, X_n]$.

Ejemplo 3.28 Sea F el sistema de 3 polinomios en 3 variables:

$$F = \begin{cases} f_1 = X_1^3X_2X_3 - X_1X_2X_3^3 - X_1^2 + X_3^2 = (X_1X_2X_3 - 1)(X_1 - X_3)(X_1 + X_3) \\ f_2 = X_1^2X_2^2X_3 - X_1^2X_2X_3 - X_1X_2^2X_3^2 + X_1X_2X_3^2 - X_1X_2 + X_1 + X_2X_3 - X_3 = \\ \quad = (X_1X_2X_3 - 1)(X_1 - X_3)(X_2 - 1) \\ f_3 = X_1X_2^3X_3 - X_1X_2X_3^2 - X_2^2 + X_3 = (X_1X_2X_3 - 1)(X_2^2 - X_3) \end{cases}$$

Las componentes equidimensionales de $V(F)$ son

$$V_0(F) = \{(-1, 1, 1)\}, \quad V_1(F) = \{x_1 - x_3 = 0, x_2^2 - x_3 = 0\}, \text{ y } V_2(F) = \{x_1x_2x_3 - 1 = 0\}.$$

Las componentes de dimensión positiva $V_1(F)$ y $V_2(F)$ tienen grado 2 y 3 respectivamente. Sean L_1 y L_2 las formas lineales $L_1 = X_1 - X_2$ y $L_2 = 6X_2 - X_3 + 7$. Entonces:

- El conjunto de los ceros aislados del sistema f_1, f_2, f_3, L_1 es $\{(1, 1, 1), (0, 0, 0)\}$, que es un subconjunto de $2 = \deg(V_1(F))$ puntos de $V_1(F)$.
- El conjunto de los ceros aislados del sistema f_1, f_2, f_3, L_1, L_2 es $\{(-1, -1, 1)$, $(-\frac{1}{2}, -\frac{1}{2}, 4)$, $(\frac{1}{3}, \frac{1}{3}, 9)\}$, que es un subconjunto de $3 = \deg(V_2(F))$ puntos de $V_2(F)$.

Usando la idea de puntos testigo, consideramos $n-1$ formas lineales afines genéricas $L_1, \ldots, L_{n-1}$ en $\mathbb{Q}[X_1, \ldots, X_n]$ y para cada $0 \leq k \leq n-1$, buscaremos los ceros aislados comunes del sistema $f_1, \ldots, f_n, L_1, \ldots, L_k$. Representaremos cada componente equidimensional $V_k(F)$ mediante un conjunto finito de puntos que contiene un conjunto de puntos

testigo de $V_k(F)$ y está contenido en $V(F)$ (ver la noción de *witness superset* en [65, Definition 13.6.1]).

Podemos observar que los sistemas $f_1, \ldots, f_n, L_1, \ldots, L_k$ tienen más polinomios que variables. Para poder aplicar el algoritmo `ToricSolve` (ver el Algoritmo 2.3) construimos sistemas auxiliares con la misma cantidad de ecuaciones que de incógnitas.

Para todo $0 \leq k \leq n-1$ fijo, tomando n combinaciones lineales genéricas de los polinomios $f_1, \ldots, f_n, L_1, \ldots, L_k$ obtenemos un sistema de n polinomios en n variables que contiene en el conjunto de sus ceros aislados los ceros aislados del sistema $f_1, \ldots, f_n, L_1, \ldots, L_k$ (ver [40]). Además, alcanza con tomar combinaciones lineales de la forma

$$f_j(X) + \sum_{i=1}^{k} b_{j,i} L_i(X), \text{ para todo } 1 \leq j \leq n, \tag{3.5}$$

donde $b_{j,i}$ es genérico para todo $1 \leq j \leq n$ y $1 \leq i \leq k$. Para ver esto, para combinaciones lineales $\sum_{i=1}^{n} C_{j,i} f_i(X) + \sum_{i=n+1}^{n+k} C_{j,i} L_{i-n}(X)$ $(j = 1, \ldots, n)$ existe un polinomio p no nulo en los coeficientes $\{C_{j,i}\}_{\substack{1 \leq j \leq n \\ 1 \leq i \leq n+k}}$ tal que si $\mathrm{p}(\{c_{j,i}\}) \neq 0$ entonces los ceros aislados de $f_1, \ldots, f_n, L_1, \ldots, L_k$ son ceros aislados de esas n combinaciones lineales. Notemos C al conjunto de los coeficientes $C_{j,i}$ con $1 \leq j, i \leq n$, $\widehat{C}$ al conjunto de los restantes, y $\mathrm{p}(C, \widehat{C}) = \sum_{s \in S} \mathrm{p}_s(C) \widehat{C}^s$ con S un conjunto finito en $(\mathbb{Z}_{\geq 0})^{n \times k}$. Entonces, para $c = \{c_{j,i}\}_{1 \leq j,i \leq n}$ tales que $\det \begin{pmatrix} c_{1,1} & \ldots & c_{1,n} \\ \vdots & & \vdots \\ c_{n,1} & \ldots & c_{n,n} \end{pmatrix} \prod_{s \in S} \mathrm{p}_s(c) \prod_{1 \leq j,i \leq n} c_{j,i} \neq 0$ tenemos que $\mathrm{q}(B) = \sum_{s \in S} \mathrm{p}_s(c) (\sum_{l=1}^{n} c_{j,l} B_{l,i})^s$ es un polinomio no nulo en un conjunto de nuevas variables $B = (B_{l,i})_{\substack{1 \leq l \leq n \\ 1 \leq i \leq k}}$ y toda elección de $\{b_{j,i}\}_{\substack{1 \leq j \leq n \\ 1 \leq i \leq k}}$ que no anula a q cumple lo pedido, pues los coeficientes de la matriz que resulta del producto

$$\begin{pmatrix} c_{1,1} & \ldots & c_{1,n} \\ \vdots & & \vdots \\ c_{n,1} & \ldots & c_{n,n} \end{pmatrix} \begin{pmatrix} 1 & \ldots & 0 & b_{1,1} & \ldots & b_{1,k} \\ & \ddots & & \vdots & & \vdots \\ 0 & \ldots & 1 & b_{n,1} & \ldots & b_{n,k} \end{pmatrix}$$

no anulan a p, y el sistema lineal asociado a ella es equivalente al sistema asociado a

$$\begin{pmatrix} 1 & & 0 & b_{1,1} & \ldots & b_{1,k} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & b_{n,1} & \ldots & b_{n,k} \end{pmatrix}.$$

El conjunto de los ceros aislados del sistema (3.5) puede contener puntos que no pertenecen a $V(F)$. Por este motivo, utilizaremos una subrutina que, a partir de una resolución geométrica de un conjunto finito de puntos $\mathcal{P} \subset \mathbb{C}^n$ y los polinomios del sistema original F, calcula una resolución geométrica de $\mathcal{P} \cap V(F)$. La idea es descartar de $\mathcal{P}$ los puntos que no anulen a los polinomios de F. Llamamos a esta subrutina `CleanGR`:

Algoritmo 3.29 `CleanGR`

INPUT: Una resolución geométrica $(q(U), v_1(U), \ldots, v_n(U)) \in (\mathbb{Q}[U])^{n+1}$ *de un conjunto finito de puntos* $\mathcal{P} \subset \mathbb{C}^n$ *y un sistema de polinomios* $F = (f_1, \ldots, f_n)$ *en* $\mathbb{Q}[X_1, \ldots, X_n]$ *con soportes* $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ *en* $(\mathbb{Z}_{\geq 0})^n$ *codificado en forma rala.*

1. $Q_0(U) := q(U)$.
2. *Para* $j = 1, \ldots, n$:
   a) *Hallar la representación densa del polinomio* $F_j(U) = f_j(v_1(U), \ldots, v_n(U))$.
   b) *Hallar* $Q_j(U) := \gcd(Q_{j-1}(U), F_j(U))$
3. $Q(U) := Q_n(U)$.
4. *Para* $i = 1, \ldots, n$, *hallar* $V_i(U) := v_i(U) \pmod{Q(U)}$.

OUTPUT: Una resolución geométrica $(Q(U), V_1(U), \ldots, V_n(U))$ *del conjunto finito de puntos* $\mathcal{P} \cap V(F)$.

Notar que $\xi \in \mathcal{P} \cap V(F)$ si y solo si $\xi = (v_1(u), \ldots, v_n(u))$ para $u \in \mathbb{C}$ tal que $q(u) = 0$ y $f_1(v_1(u), \ldots, v_n(u)) = \ldots = f_n(v_1(u), \ldots, v_n(u)) = 0$. Como $Q(u) = \gcd(q(u), f_1(v_1(u), \ldots, v_n(u)), \ldots, f_n(v_1(u), \ldots, v_n(u)))$ y $V_i(u) = v_i(u)$ para todo $u \in \mathbb{C}$ tal que $Q(u) = 0$, $\xi \in \mathcal{P} \cap V(F)$ es equivalente a que exista $u \in \mathbb{C}$ tal que $\xi = (V_1(u), \ldots, V_n(u))$ y $Q(u) = 0$. Esto prueba la correctitud del algoritmo.

Para calcular la complejidad de este procedimiento, sean d una cota superior para los grados de $f_1, \ldots, f_n$ y $D = \deg(q)$. En primer lugar se obtiene un slp que codifica los polinomios $v_1, \ldots, v_n$ de longitud del orden de $O(nD \log D)$. Para cada $j = 1, \ldots, n$, en el paso $2a$, el algoritmo calcula un slp de longitud $\mathcal{L}_j = O(n \log d \# \mathcal{A}_j)$ para f_j y mediante interpolación obtiene la representación densa de $F_j(U)$ con una complejidad del orden de $O(M(dD)(\mathcal{L}_j + nD \log D))$; en el paso $2b$, se calcula el máximo común divisor $Q_j(U)$ con

$O(M(dD))$ operaciones. Finalmente, los polinomios del paso 4 se obtienen con $O(nM(D))$ operaciones. En consecuencia, la complejidad total del procedimiento `CleanGR` es de orden $O(M(dD)(n \log d \sum_{j=1}^{n} \#\mathcal{A}_j + n^2 D \log D))$.

Presentamos entonces el algoritmo `PointsInEquidComps` que calcula una familia de resoluciones geométricas $R^{(0)}, \ldots, R^{(n-1)}$ tales que, para todo $0 \leq k \leq n-1$, $R^{(k)}$ describe un conjunto finito de puntos que cumple que, para cada componente irreducible W de $V(F)$ de dimensión k, contiene al menos $\deg(W)$ puntos en W.

Algoritmo 3.30 `PointsInEquidComps`

INPUT: Un sistema de polinomios $F = (f_1, \ldots, f_n)$ en $\mathbb{Q}[X_1, \ldots, X_n]$ con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$ codificado en forma rala, una función de levantamiento genérica $\omega = (\omega_1, \ldots, \omega_n)$ para la familia $\mathcal{A}_\Delta = (\mathcal{A}_1 \cup \Delta, \ldots, \mathcal{A}_n \cup \Delta)$ y las celdas mixtas de la subdivisión mixta fina $S_\omega(\mathcal{A}_\Delta)$.

1. *Elegir al azar coeficientes en $\mathbb{Z}$ para un sistema de polinomios $G = (g_1, \ldots, g_n)$ con soportes $\mathcal{A}_\Delta$.*
2. *Aplicar el algoritmo `ToricSolve` (Algoritmo 2.3) al sistema G para obtener una resolución geométrica R_G de los ceros de G en $\mathbb{C}^n$.*
3. *Elegir al azar coeficientes para $n-1$ formas lineales $L_1, \ldots, L_{n-1}$ en las variables $X = (X_1, \ldots, X_n)$ y $n(n-1)$ números $(b_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n-1}$ en $\mathbb{Z}$.*
4. *Para $k = 0, \ldots, n-1$:*
   a) *Obtener la representación rala del sistema de polinomios $H^{(k)} = (h_1^{(k)}, \ldots, h_n^{(k)})$ donde $h_j^{(k)}(X) = f_j(X) + \sum_{i=1}^{k} b_{j,i} L_i(X)$ para cada $1 \leq j \leq n$.*
   b) *Aplicar el algoritmo de [45, Section 6] al sistema $H^{(k)}$ para hallar a partir de R_G una resolución geométrica de un conjunto finito $\mathcal{P}_k$ que contiene los ceros aislados de $H^{(k)}$ en $\mathbb{C}^n$.*
   c) *Aplicar la subrutina `CleanGR` a la resolución geométrica del conjunto $\mathcal{P}_k$ obtenida en el paso 4b y a los polinomios de F para obtener una resolución geométrica $R^{(k)}$ de $\mathcal{P}_k \cap V(F)$.*

OUTPUT: La familia de n resoluciones geométricas $(R^{(0)}, \ldots, R^{(n-1)})$.

A continuación, calcularemos la complejidad del algoritmo `PointsInEquidComps`. En primer lugar, el costo de aplicar el algoritmo `ToricSolve` (ver la Sección 2.1.2) en el paso 2 es

$$O((n^3 N_\Delta \log(d) + n^{1+\Omega}) M(\mathcal{D}_\Delta) M(\Upsilon_\Delta)(M(\mathcal{D}_\Delta) + M(\mathcal{E}_\Delta)))$$

donde, siguiendo la notación previa,

- $N_\Delta := \sum_{j=1}^{n} \#(\mathcal{A}_j \cup \Delta)$,
- $d := \text{máx}_{1 \leq j \leq n}\{\deg(f_j)\}$,
- $\mathcal{D}_\Delta := \mathcal{MV}_n(\mathcal{A}_1 \cup \Delta, \ldots, \mathcal{A}_n \cup \Delta)$,
- $\Upsilon_\Delta := \text{máx}\{\|\eta\|\}$ donde el máximo es sobre todas las normales interiores primitivas asociadas a celdas mixtas en la subdivisión mixta fina $S_\omega(\mathcal{A}_\Delta)$ inducida por ω,
- $\mathcal{E}_\Delta := \mathcal{MV}_{n+1}(\Delta \times \{0\}, (\mathcal{A}_1 \cup \Delta)(\omega_1), \ldots, (\mathcal{A}_n \cup \Delta)(\omega_n))$.

En el paso 4, el ítem 4*a* no aumenta la complejidad total. Por [45, Proposition 6.1], sabemos que la complejidad del paso 4*b* es $O((n^2 N_\Delta \log d + n^{1+\Omega}) M(\mathcal{D}_\Delta) M(\mathcal{E}'_\Delta))$, donde $\mathcal{E}'_\Delta := \mathcal{MV}_{n+1}(\{0\} \times \Delta, \{0,1\} \times (\mathcal{A}_1 \cup \Delta), \ldots, \{0,1\} \times (\mathcal{A}_n \cup \Delta))$ y, por nuestros cálculos de complejidad previos, el paso 4*c* tiene un costo de orden $O(M(d\mathcal{D}_\Delta)(n \log d \sum_{j=1}^{n} \#\mathcal{A}_j + n^2 \mathcal{D}_\Delta \log \mathcal{D}_\Delta))$.

Procediendo como en la demostración de [45, Lemma 2.3] (ver también los cálculos de complejidad del Teorema 3.20), podemos acotar los parámetros $\mathcal{E}'_\Delta$ y $\mathcal{E}_\Delta$ como sigue:

$$\mathcal{E}'_\Delta = \sum_{j=1}^{n} \mathcal{MV}_n(\Delta, \mathcal{A}_1 \cup \Delta, \ldots, \widehat{\mathcal{A}_j \cup \Delta}, \ldots, \mathcal{A}_n \cup \Delta) \leq n\mathcal{D}_\Delta$$

usando la monotonía del volumen mixto y, si $\omega_{\text{máx}} := \text{máx}_{j,\alpha}\{\omega_j(\alpha) \mid 1 \leq j \leq n,\ \alpha \in \mathcal{A}_j \cup \Delta\}$,

$$\mathcal{E}_\Delta \leq \mathcal{MV}_{n+1}(\Delta \times \{0\}, (\mathcal{A}_1 \cup \Delta) \times \{0, \omega_{\text{máx}}\}, \ldots, (\mathcal{A}_n \cup \Delta) \times \{0, \omega_{\text{máx}}\}) \leq \omega_{\text{máx}} n \mathcal{D}_\Delta.$$

Por lo tanto, la complejidad total del algoritmo es la expresada en el siguiente teorema:

Teorema 3.31 *Sea $F = (f_1, \ldots, f_n)$ un sistema de n polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ en $(\mathbb{Z}_{\geq 0})^n$. Para todo $0 \leq k \leq n-1$, sea $V_k(F)$ la componente equidimensional de dimensión k de $V(F)$. El algoritmo probabilístico* `PointsInEquidComps` *calcula una familia de n resoluciones geométricas $(R^{(0)}, R^{(1)}, \ldots, R^{(n-1)})$ tales que, para cada $0 \leq k \leq n-1$, $R^{(k)}$ representa un conjunto finito de puntos que contiene $\deg(V_k(F))$ puntos en $V_k(F)$. Con la notación previa, la complejidad del algoritmo es de orden*

$$O(\omega_{\text{máx}} n^4 N_\Delta \log(d) M(d\mathcal{D}_\Delta) M(\mathcal{D}_\Delta) M(\Upsilon_\Delta)).$$

Apliquemos los pasos del algoritmo `PointsInEquidComps` a los polinomios del Ejemplo 3.21:

Ejemplo 3.32 Sea F el sistema de 3 polinomios en 3 variables

$$F = \begin{cases} f_1(X_1, X_2, X_3) = X_1X_2 - X_1 - X_2 + 1 \\ f_2(X_1, X_2, X_3) = X_1X_3 - X_1 - X_3 + 1 \\ f_3(X_1, X_2, X_3) = X_2X_3 - X_2 - X_3 + 1 \end{cases}$$

con soportes $\mathcal{A}_1 = \{(1,1,0),(1,0,0),(0,1,0),(0,0,0)\}$, $\mathcal{A}_2 = \{(1,0,1),(1,0,0),(0,0,1),(0,0,0)\}$ y $\mathcal{A}_3 = \{(0,1,1),(0,1,0),(0,0,1),(0,0,0)\}$.

En el paso 1 se elige al azar un sistema G con soportes $(\mathcal{A}_1 \cup \Delta, \mathcal{A}_2 \cup \Delta, \mathcal{A}_3 \cup \Delta)$. Tomemos

$$G = \begin{cases} g_1(X_1, X_2, X_3) = 2X_1X_2 - 2X_1 + X_2 - X_3 + 1 \\ g_2(X_1, X_2, X_3) = X_1X_3 - X_1 + 2X_2 + 2X_3 + 2 \\ g_3(X_1, X_2, X_3) = X_2X_3 + X_1 - 2X_2 + X_3 - 1 \end{cases} .$$

En el paso 2 el algoritmo calcula una resolución geométrica R_G del conjunto de ceros aislados de G en $\mathbb{C}^3$ asociada a una forma lineal. En este caso, elegimos $\mu(X_1, X_2, X_3) = X_1 + 2X_2 + X_3$:

$$R_G = \begin{cases} U^5 - \frac{9}{2}U^4 - 17U^3 + 80U^2 - 2U - \frac{155}{2} = 0 \\ X_1 = -\frac{9}{100}U^4 + \frac{7}{40}U^3 + \frac{351}{200}U^2 - \frac{543}{200}U - \frac{137}{40} \\ X_2 = -\frac{1}{200}U^4 - \frac{1}{80}U^3 - \frac{1}{400}U^2 + \frac{233}{400}U + \frac{7}{80} \\ X_3 = \frac{1}{10}U^4 - \frac{3}{20}U^3 - \frac{7}{4}U^2 + \frac{51}{20}U + \frac{13}{4} \end{cases} .$$

En el paso 3 se toman al azar 2 formas lineales:

$$\begin{aligned} L_1(X_1, X_2, X_3) &= X_1 + X_2 + 2X_3 \\ L_2(X_1, X_2, X_3) &= X_1 + 2X_2. \end{aligned}$$

En este paso también se eligen al azar los coeficientes que se usarán en el primer ítem $4a$ del paso recursivo para construir los polinomios $h_j^{(k)}$ para todo $1 \leq j \leq 3$ y $0 \leq k \leq 2$. Para cada k estos polinomios se obtienen sumando a cada polinomio de F una combinación lineal de las formas lineales L_i (con $0 \leq i \leq k$). Tomemos

$$H^{(0)} = F, \quad H^{(1)} = \begin{cases} h_1^{(1)} = f_1(X) + L_1(X) &= X_1X_2 + 2X_3 + 1 \\ h_2^{(1)} = f_2(X) - L_1(X) &= X_1X_3 - 2X_1 - 3X_3 - X_2 + 1 \\ h_3^{(1)} = f_3(X) + 2L_1(X) &= X_2X_3 + X_2 + 3X_3 + 2X_1 + 1 \end{cases}$$

$$H^{(2)} = \begin{cases} h_1^{(2)} = f_1(X) + L_1(X) + L_2(X) & = & X_1X_2 + X_1 + 2X_2 + 2X_3 + 1 \\ h_2^{(2)} = f_2(X) - L_1(X) + 2L_2(X) & = & X_1X_3 + 3X_2 - 3X_3 + 1 \\ h_3^{(3)} = f_3(X) + 2L_1(X) + L_2(X) & = & X_2X_3 + 3X_2 + 3X_3 + 3X_1 + 1 \end{cases}$$

En el paso 4, para cada $k = 0, 1, 2$ se buscan los ceros aislados de $H^{(k)}$. Para ello, en el paso 4*b* a partir de la resolución geométrica R_G el algoritmo obtiene resoluciones geométricas $R_{H^{(k)}}$ de conjuntos finitos $\mathcal{P}_k$ que contienen a los ceros aislados de $H^{(k)}$ para cada k:

$$R_{H^{(0)}} = \begin{cases} U^3 - 7U^2 + 2U + 40 = 0 \\ X_1 = 1 \\ X_2 = -\frac{1}{14}U^2 + \frac{9}{14}U - \frac{3}{7} \\ X_3 = \frac{1}{7}U^2 - \frac{2}{7}U - \frac{1}{7} \end{cases}$$

$$R_{H^{(1)}} = \begin{cases} U^5 - \frac{9}{2}U^4 - 13U^3 + 68U^2 - 64U = 0 \\ X_1 = \frac{57}{200}U^4 - \frac{369}{400}U^3 - \frac{953}{200}U^2 + \frac{647}{50}U - 3 \\ X_2 = -\frac{269}{600}U^4 + \frac{1573}{1200}U^3 + \frac{1567}{200}U^2 - \frac{2599}{150}U + 1 \\ X_3 = \frac{367}{600}U^4 - \frac{2039}{1200}U^3 - \frac{2181}{200}U^2 + \frac{3407}{150}U + 1 \end{cases}$$

$$R_{H^{(2)}} = \begin{cases} U^5 + \frac{49}{2}U^4 - \frac{1549}{9}U^3 + \frac{538}{9}U^2 + \frac{679}{6}U - \frac{769}{18} = 0 \\ X_1 = -\frac{101214}{1803049}U^4 - \frac{2537721}{1803049}U^3 + \frac{15987545}{1803049}U^2 + \frac{3986650}{1803049}U - \frac{7719426}{1803049} \\ X_2 = \frac{58338}{9015245}U^4 + \frac{277533}{1803049}U^3 - \frac{11347628}{9015245}U^2 + \frac{5343077}{9015245}U + \frac{8036523}{9015245} \\ X_3 = \frac{389394}{9015245}U^4 + \frac{1982655}{1803049}U^3 - \frac{57242469}{9015245}U^2 - \frac{21604159}{9015245}U + \frac{22524084}{9015245} \end{cases}$$

En el paso 4*c* se modifican las resoluciones geométricas $R_{H^{(k)}}$ descartándose los puntos que no corresponden a ceros del sistema F, y de esa manera el algoritmo obtiene para cada k una resolución geométrica $R^{(k)}$ de un conjunto finito de puntos que contiene un conjunto de puntos que representa la componente equidimensional de dimensión k de $V(F)$:

$$R^{(0)} = \begin{cases} U^3 - 7U^2 + 2U + 40 = 0 \\ X_1 = 1 \\ X_2 = -\frac{1}{14}U^2 + \frac{9}{14}U - \frac{3}{7} \\ X_3 = \frac{1}{7}U^2 - \frac{2}{7}U - \frac{1}{7} \end{cases} \qquad R^{(1)} = \begin{cases} U^3 + 2U^2 - 8U = 0 \\ X_1 = \frac{1}{2}U^2 + U - 3 \\ X_2 = -\frac{1}{6}U^2 + \frac{1}{3}U + 1 \\ X_3 = -\frac{1}{6}U^2 - \frac{2}{3}U + 1 \end{cases} \qquad R^{(2)} = \emptyset$$

Como $R^{(2)} = \emptyset$ sabemos que $V(F)$ no tiene componentes irreducibles de dimensión 2. Por otro lado, como los polinomios minimales de $R^{(0)}$ y $R^{(1)}$ son $U^3 - 7U^2 + 2U + 40 = (U + 2)(U - 4)(U - 5)$ y $U^3 + 2U^2 - 8U = (U + 4)U(U - 2)$, reemplazando sus raíces en $R^{(0)}$ y $R^{(1)}$ respectivamente obtenemos los siguientes conjuntos de puntos en $V(F)$:

$$\mathcal{W}_0 = \{(1, -2, 1), (1, 1, 1), (1, 1, 2)\} \quad \text{y} \quad \mathcal{W}_1 = \{(-3, 1, 1), (1, 1, -1), (1, -3, 1)\}.$$

En este caso, $\mathcal{W}_1$ contiene exactamente un punto por cada una de las 3 componentes irreducibles de dimensión 1 de $V(F)$. Sin embargo, aunque F no tiene ceros aislados, el algoritmo encuentra $\mathcal{W}_0 \subset V(F)$ un conjunto no vacío.

Capítulo 4

Cálculo de proyecciones

Sean $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ una familia de conjuntos finitos en $(\mathbb{Z}_{\geq 0})^n$ y $P = (p_1, \ldots, p_m)$ un sistema de polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ con soportes $\mathcal{A}$ y coeficientes genéricos. Sean $\ell < n$ y $\pi : \mathbb{C}^n \to \mathbb{C}^\ell$ la proyección dada por $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_\ell)$. En este capítulo presentamos un algoritmo probabilístico simbólico que calcula la clausura de Zariski de $\pi(V(P)) \subset \mathbb{C}^\ell$ cuya complejidad se expresa en función de invariantes combinatorios asociados a la familia de soportes.

4.1. Sistemas con coeficientes indeterminados

Sea $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ una familia de conjuntos finitos en $(\mathbb{Z}_{\geq 0})^n$. Consideraremos en primer lugar un sistema $F = (f_1, \ldots, f_m)$ con soportes $\mathcal{A}$ y coeficientes indeterminados. Para todo $1 \leq j \leq m$, sea

$$f_j(A_j, X) = \sum_{\alpha \in \mathcal{A}_j} A_{j,\alpha} X^\alpha, \tag{4.1}$$

donde $A_j = (A_{j,\alpha})_{\alpha \in \mathcal{A}_j}$ es un conjunto de $N_j = \#\mathcal{A}_j$ nuevas variables. Sea $\mathbb{K} := \mathbb{Q}(A_1, \ldots, A_m)$.

La estrategia que usaremos para el cálculo de la proyección de la variedad $V(F)$ es la siguiente: Usando la descomposición en componentes equidimensionales calculada en el Capítulo 3 reducimos el problema a trabajar con variedades tales que cada una de sus componentes irreducibles tiene puntos con todas sus coordenadas no nulas. Para cada una de estas nuevas variedades a considerar, elegimos un conjunto de variables libres apropiado y calculamos una resolución geométrica respecto a esas variables libres de la clausura de Zariski de su proyección.

4.1.1. Reducción al caso tórico

Sea $I \subset \{1\ldots,n\}$. Para cada polinomio $f_j \in \mathbb{K}[X_1,\ldots,X_n]$, $1 \leq j \leq m$, notamos $(f_j)_I$ el polinomio que resulta de especializar $X_i = 0$ para todo $i \in I$ en f_j. Sean F_I y J_I como se definieron en la Sección 2.2 y

$$\Phi = \{I \subset \{1,\ldots,n\} \mid \forall\, J \subset J_I,\ \dim(\sum_{j\in J} \mathcal{A}_j^I) \geq \#J; \forall\, \widetilde{I} \subset I,\ \#J_{\widetilde{I}} + \#\widetilde{I} \geq \#J_I + \#I\}$$

como se definió en (3.2), donde $\mathcal{A}_j^I \subset (\mathbb{Z}_{\geq 0})^{n-\#I}$ es el soporte de $(f_j)_I$ para todo $j \in J_I$. Recordemos que $\varphi_I : \overline{\mathbb{K}}^{n-\#I} \to \overline{\mathbb{K}}^n$ es la función que inserta ceros en las coordenadas indexadas por I. El Teorema 3.8 nos dice que

$$V(F) = \bigcup_{I\in\Phi} \varphi_I(V^*(F_I)), \tag{4.2}$$

donde $V^*(F_I) = \overline{V(F_I) \cap (\overline{\mathbb{K}}^*)^{n-\#I}}$ es la unión de todas las componentes irreducibles de $V(F_I)$ que intersecan $(\overline{\mathbb{K}}^*)^{n-\#I}$ (ver la Definición 3.2).

Sea $\pi : \overline{\mathbb{K}}^n \to \overline{\mathbb{K}}^\ell$ la proyección a las primeras ℓ coordenadas. Para todo $I \subset \{1,\ldots,n\}$, llamamos $\ell_I = \ell - \#(I \cap \{1,\ldots,\ell\})$, $\pi_{\ell_I} : \overline{\mathbb{K}}^{n-\#I} \to \overline{\mathbb{K}}^{\ell_I}$ a la proyección a las primeras ℓ_I coordenadas y $\varphi_{I\cap\{1,\ldots,\ell\}} : \overline{\mathbb{K}}^{\ell_I} \to \overline{\mathbb{K}}^\ell$ a la función que inserta ceros en las coordenadas indexadas por $I \cap \{1,\ldots,\ell\}$. Observando que para todo I vale $\pi(\varphi_I(V^*(F_I))) = \varphi_{I\cap\{1,\ldots,\ell\}}(\pi_{\ell_I}(V^*(F_I)))$, de la igualdad (4.2), resulta que

$$\pi(V(F)) = \bigcup_{I\in\Phi} \varphi_{I\cap\{1,\ldots,\ell\}}(\pi_{\ell_I}(V^*(F_I))).$$

Esto nos permite reducir el problema de calcular la proyección de $V(F)$ a calcular finitas proyecciones de variedades que tienen la propiedad de que el conjunto de sus puntos con coordenadas no nulas es un abierto denso de la variedad. Más específicamente, basta calcular para todo $I \in \Phi$, la clausura de Zariski de la proyección por π_{ℓ_I} de la variedad $V^*(F_I)$.

4.1.2. Ideal de la proyección

En lo que sigue nos concentraremos en la proyección de las variedades $V^*(F_I)$ para todo $I \in \Phi$. En particular, sabemos que la cantidad de polinomios de sistema F_I es menor o igual a la cantidad de variables. Entonces, basta considerar el caso de un sistema $F = (f_1,\ldots,f_m)$ con soportes $\mathcal{A} = (\mathcal{A}_1,\ldots,\mathcal{A}_m)$ en $(\mathbb{Z}_{\geq 0})^n$ para el cual $m \leq n$ y, para todo $J \subset \{1,\ldots,m\}$, vale $\dim(\sum_{j\in J} \mathcal{A}_j) \geq \#J$. Con estas hipótesis, $V^*(F)$ es no vacío (ver el Lema 3.1).

Veamos algunos resultados respecto de los ideales $I(V^*(F))$ y $I(\overline{\pi(V^*(F))})$.

Para un ideal $J \subset \mathbb{K}[X_1, \ldots, X_n]$ notamos $J : (X_1 \ldots X_n)^\infty$ al ideal cociente

$$J : (X_1 \ldots X_n)^\infty = \{f \in \mathbb{K}[X_1, \ldots, X_n] \mid (X_1 \ldots X_n)^r f \in J \text{ para algún } r \in \mathbb{Z}_{\geq 0}\}.$$

Lema 4.1 *Con la notación e hipótesis anteriores, $\langle f_1, \ldots, f_m\rangle : (X_1 \ldots X_n)^\infty$ es un ideal primo en $\mathbb{K}[X_1, \ldots, X_n]$ de dimensión $n - m$. Además,*

$$I(V^*(F)) = \langle f_1, \ldots, f_m\rangle : (X_1 \ldots X_n)^\infty.$$

Demostración: Para todo $1 \leq j \leq m$, elegimos $\alpha_{j,0} \in \mathcal{A}_j$ y sean $\mathcal{A}'_j := \mathcal{A}_j \backslash \{\alpha_{j,0}\}$ y $A'_j := A_j \backslash \{A_{j,\alpha_{j,0}}\}$. Notamos $A := (A_1, \ldots, A_m)$ a la lista de coeficientes indeterminados de F, $A' := (A'_1, \ldots, A'_m)$ y $\mathbb{Q}[A', X]_{X_1 \ldots X_n}$ a la localización de $\mathbb{Q}[A', X]$ en el conjunto multiplicativo $\{(X_1 \ldots X_n)^i \mid i \in \mathbb{Z}_{\geq 0}\}$. Sea ψ el morfismo de anillos $\psi : \mathbb{Q}[A, X] \to \mathbb{Q}[A', X]_{X_1 \ldots X_n}$ definido por $\psi(X_i) = X_i$ para todo $1 \leq i \leq n$, $\psi(A_{j,\alpha}) = A_{j,\alpha}$ para todo $1 \leq j \leq m$, $\alpha \in \mathcal{A}'_j$, y $\psi(A_{j,\alpha_{j,0}}) = -X^{-\alpha_{j,0}}(\sum_{\alpha \in \mathcal{A}'_j} A_{j,\alpha} X^\alpha)$ para todo $1 \leq j \leq m$.

Veamos que $\mathrm{Ker}(\psi) = \langle f_1, \ldots, f_m\rangle : (X_1 \ldots X_n)^\infty$: Como $f_j \in \mathrm{Ker}(\psi)$ para todo $1 \leq j \leq m$, si consideramos un polinomio $g \in \langle f_1, \ldots, f_m\rangle : (X_1 \ldots X_n)^\infty$, es claro que $\psi(g) = 0$. Por otro lado, sea $g \in \mathbb{Q}[A, X]$ un polinomio tal que $\psi(g) = 0$. Notemos $A_0 := (A_{1,\alpha_{1,0}}, \ldots, A_{m,\alpha_{m,0}})$ y sea $\widehat{A}_0 := (\widehat{A}_{1,0}, \ldots, \widehat{A}_{m,0})$ un conjunto de m nuevas variables. Calculando el desarrollo de Taylor de g, tenemos que $g(\widehat{A}_0, A', X) = g(A_0, A', X) + \sum_{1 \leq j \leq m} (\widehat{A}_{j,0} - A_{j,\alpha_{j,0}}) \cdot G_j$ para polinomios $G_j \in \mathbb{Q}[\widehat{A}_0, A, X]$. Especializando $\widehat{A}_{j,0} = -X^{-\alpha_{j,0}}(\sum_{\alpha \in \mathcal{A}'_j} A_{j,\alpha} X^\alpha)$ para todo $1 \leq j \leq m$, se obtiene que

$$\psi(g) = g(A_0, A', X) - \sum_{1 \leq j \leq m} X^{-\alpha_{j,0}} f_j(X) \cdot G_j(-X^{-\alpha_{j,0}}(\sum_{\alpha \in \mathcal{A}'_j} A_{j,\alpha} X^\alpha), A, X).$$

Luego, $g(A, X) = \sum_{1 \leq j \leq m} X^{-\alpha_{j,0}} f_j(X) \cdot G_j(-X^{-\alpha_{j,0}}(\sum_{\alpha \in \mathcal{A}'_j} A_{j,\alpha} X^\alpha), A, X)$. Multiplicando por $(X_1 \ldots X_n)^r$ con r suficientemente grande, tenemos que $(X_1 \ldots X_n)^r g(A, X) \in \langle f_1, \ldots, f_m\rangle$.

En consecuencia, $\langle f_1, \ldots, f_m\rangle : (X_1 \ldots X_n)^\infty$ es un ideal primo de $\mathbb{Q}[A, X]$. Localizando en $\mathbb{Q}[A] \backslash \{0\}$, concluimos que $\langle f_1, \ldots, f_m\rangle : (X_1 \ldots X_n)^\infty$ es un ideal primo de $\mathbb{K}[X_1, \ldots, X_n]$. Como ψ es sobreyectiva, este ideal tiene dimensión $n - m$.

Para terminar la demostración, tomemos un polinomio $g \in \langle f_1, \ldots, f_m\rangle : (X_1 \ldots X_n)^\infty$, y r un entero no negativo tal que $(X_1 \ldots X_n)^r g \in \langle f_1, \ldots, f_m\rangle$. Entonces, $(X_1 \ldots X_n)^r g$ se anula sobre $V(F)$ y por lo tanto g se anula sobre $V(F) \cap (\overline{\mathbb{K}}^*)^n$. Luego, $g \in I(V^*(F))$. Por

otro lado, sea $g \in I(V^*(F))$. Este polinomio se anula sobre cada componente irreducible de $V(F)$ que tiene intersección no vacía con $(\overline{\mathbb{K}}^*)^n$. Por lo tanto, $(X_1 \dots X_n)g$ se anula sobre $V(F)$. Entonces, existe $r \in \mathbb{Z}_{\geq 0}$ tal que $(X_1 \dots X_n)^r g^r \in \langle f_1, \dots, f_m \rangle$. Así, $g^r \in \langle f_1, \dots, f_m \rangle : (X_1 \dots X_n)^\infty$ y, como éste es un ideal primo, $g \in \langle f_1, \dots, f_m \rangle : (X_1 \dots X_n)^\infty$. □

Corolario 4.2 *La variedad algebraica $V^*(F) \subset \overline{\mathbb{K}}^n$ es una variedad irreducible sobre $\mathbb{K}$ de dimensión $n - m$.*

Para una variedad algebraica $V \subset \overline{\mathbb{K}}^n$ definible sobre $\mathbb{K}$, se tiene que $I(\overline{\pi(V)}) = I(V) \cap \mathbb{K}[X_1, \dots, X_\ell]$ (ver, por ejemplo, [16, Chapter 4, Section 4, Theorem 3]). Luego por el Lema 4.1:

Corolario 4.3 *Bajo las hipótesis anteriores,*

$$I(\overline{\pi(V^*(F))}) = (\langle f_1, \dots, f_m \rangle : (X_1 \dots X_n)^\infty) \cap \mathbb{K}[X_1, \dots, X_\ell].$$

Sea $t := \dim(\overline{\pi(V^*(F))})$. Sin perder generalidad podemos renombrar las variables de forma que $\{X_1, \dots, X_t\} \subset \{X_1, \dots, X_\ell\}$ sea una base de trascendencia de $\mathbb{K}(\overline{\pi(V^*(F))})$ sobre $\mathbb{K}$ y que $\{X_{t+m+1}, \dots, X_n\}$ la complete a una base de trascendencia $\{X_1, \dots, X_t, X_{t+m+1}, \dots, X_n\}$ de $\mathbb{K}(V^*(F))$ sobre $\mathbb{K}$. Usaremos la siguiente proposición para trabajar con proyecciones con fibras genéricas cero-dimensionales.

Proposición 4.4 *Existe un abierto Zariski denso $\mathcal{O} \subseteq \overline{\mathbb{K}}^{n-t-m}$ tal que para todo $b \in (\mathbb{K}^*)^{n-t-m} \cap \mathcal{O}$ vale la igualdad*

$$I(\overline{\pi(V^*(F))}) =$$
$$= (\langle f_1(X_1, \dots, X_{t+m}, b), \dots, f_m(X_1, \dots, X_{t+m}, b) \rangle : (X_1 \dots X_{t+m})^\infty) \cap \mathbb{K}[X_1, \dots, X_\ell].$$

Demostración: Por el Corolario 4.3, si $g \in I(\overline{\pi(V^*(F))})$, entonces existe $r \geq 0$ tal que $(X_1 \dots X_n)^r g(X_1, \dots, X_\ell) = \sum_{j=1}^{m} q_j(X) f_j(X)$. Notemos $\widehat{X} := (X_1, \dots, X_{t+m})$. Para todo $b = (b_{t+m+1}, \dots, b_n)$ tal que $b_i \neq 0$ para todo $t + m + 1 \leq i \leq n$, evaluando en b,

$$(X_1 \dots X_{t+m})^r g(X_1, \dots, X_\ell) = \sum_{j=1}^{m} \frac{q_j(\widehat{X}, b)}{(b_{t+m+1} \dots b_n)^r} f_j(\widehat{X}, b),$$

con lo cual $I(\overline{\pi(V^*(F))}) \subset (\langle f_1(\widehat{X}, b), \dots, f_m(\widehat{X}, b) \rangle : (X_1 \dots X_{t+m})^\infty) \cap \mathbb{K}[X_1, \dots, X_\ell]$.

Por otro lado, queremos ver que existe un abierto Zariski $\mathcal{O}$ no vacío tal que si $b \in \mathbb{K}^{n-t-m} \cap \mathcal{O}$ entonces $(\langle f_1(\widehat{X}, b), \dots, f_m(\widehat{X}, b) \rangle : (X_1 \dots X_{t+m})^\infty) \cap \mathbb{K}[X_1, \dots, X_\ell] \subset I(\overline{\pi(V^*(F))})$. Podemos observar que, para todo $1 \leq j \leq m$, vale

$$\mathbb{K}[X_1, \dots, X_n]/\langle f_1, \dots, f_j \rangle : (X_1 \dots X_n)^\infty \simeq \mathbb{K}[X_1, \dots, X_n]_{X_1 \dots X_n}/\langle f_1, \dots, f_j \rangle \simeq$$

$$\simeq \mathbb{K}[Y, X_1, \ldots, X_n]/\langle YX_1 \ldots X_n - 1, f_1, \ldots, f_j\rangle.$$

Aplicando el Lema 4.1 sabemos que el ideal $\langle f_1, \ldots, f_j\rangle : (X_1 \ldots X_n)^\infty$ es un ideal primo de dimensión $n-j$ para todo $1 \leq j \leq m$. Entonces, la lista de polinomios $YX_1 \ldots X_n - 1$, $f_1, \ldots, f_m$ es una sucesión regular reducida en $\mathbb{K}[Y, X_1, \ldots, X_n]$ (recordar que una lista de polinomios $g_1, \ldots, g_s \in \mathbb{K}[X_1, \ldots, X_n]$ es una *sucesión regular* si g_j no es un divisor de cero en $\mathbb{K}[X_1, \ldots, X_n]/\langle g_1, \ldots, g_{j-1}\rangle$ para cada $1 \leq j \leq s$; y una sucesión regular es *reducida* si, para todo $1 \leq j \leq s$, el ideal $\langle g_1, \ldots, g_j\rangle \in \mathbb{K}[X_1, \ldots, X_n]$ es radical para todo $1 \leq j \leq s$). Además, el conjunto de las variables $\{X_{t+m+1}, \ldots, X_n\}$ es algebraicamente independiente módulo $\langle YX_1 \ldots X_n - 1, f_1, \ldots, f_m\rangle$. Entonces, por [20, Corollary 17 & Theorem 19], existe $\mathcal{O} \subset \overline{\mathbb{K}}^{n-t-m}$ un abierto Zariski denso definible sobre $\mathbb{K}$ contenido en $\{x \in \overline{\mathbb{K}}^{n-t-m} \mid x_i \neq 0 \ \forall\, 1 \leq i \leq t+m\}$ que cumple que, para todo $b \in \mathcal{O} \cap \mathbb{K}^{n-t-m}$, la lista de polinomios $c_b\, YX_1 \ldots X_{t+m} - 1, f_1(\widehat{X}, b), \ldots, f_m(\widehat{X}, b)$ (donde $c_b := b_{t+m+1} \ldots b_n$) es una sucesión regular reducida en $\mathbb{K}[\widehat{X}]$ y $\{X_1, \ldots, X_t\}$ es algebraicamente independiente módulo cada uno de los primos asociados al ideal generado por esta sucesión regular reducida. Como $\mathbb{K}[\widehat{X}]/\langle f_1(\widehat{X}, b), \ldots, f_m(\widehat{X}, b)\rangle : (X_1 \ldots X_{t+m})^\infty \simeq \mathbb{K}[\widehat{X}]/\langle c_b\, YX_1 \ldots X_{t+m} - 1, f_1(\widehat{X}, b), \ldots, f_m(\widehat{X}, b)\rangle$, deducimos que el ideal $\langle f_1(\widehat{X}, b), \ldots, f_m(\widehat{X}, b)\rangle : (X_1 \ldots X_{t+m})^\infty$ es un ideal radical equidimensional de dimensión t y el conjunto de variables $\{X_1, \ldots, X_t\}$ es algebraicamente independiente módulo cada uno de sus primos asociados. En consecuencia, lo mismo vale para $(\langle f_1(\widehat{X}, b), \ldots, f_m(\widehat{X}, b)\rangle : (X_1 \ldots X_{t+m})^\infty) \cap \mathbb{K}[X_1, \ldots, X_\ell]$. Como este ideal contiene al ideal primo $I(\overline{\pi(V^*(F))})$ y éste también tiene dimensión t, vale la proposición. □

4.1.3. Variables libres

El siguiente lema da una condición en función de los soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ que permiten determinar si un subconjunto de variables es algebraicamente independiente módulo $I(V^*(F))$.

Lema 4.5 *Sea $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$ el sistema polinomial ralo con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ en $(\mathbb{Z}_{\geq 0})^n$ definido en (4.1), y sea $\mathcal{J} = \langle f_1, \ldots, f_m\rangle : (X_1 \ldots X_n)^\infty \subset \mathbb{K}[X_1, \ldots, X_n]$. Sea $\{e_1, \ldots, e_n\}$ la base canónica de $\mathbb{Q}^n$. Entonces, el conjunto $\{X_{i_1}, \ldots, X_{i_k}\} \subset \{X_1, \ldots, X_n\}$ con $1 \leq i_1 < \ldots < i_k \leq n$ es algebraicamente independiente módulo $\mathcal{J}$ si y solo si $\mathcal{MV}_n(\mathcal{A}_1, \ldots, \mathcal{A}_m, \{0, e_{i_1}\}, \ldots, \{0, e_{i_k}\}, \Delta^{(n-m-k)}) > 0$.*

Demostración: Supongamos primero que el volumen mixto $\mathcal{MV}_n(\mathcal{A}_1, \ldots, \mathcal{A}_m, \{0, e_{i_1}\}, \ldots, \{0, e_{i_k}\}, \Delta^{(n-m-k)})$ es positivo. Sea q un polinomio no nulo en los coeficientes de un sistema de n ecuaciones en n variables con soportes $(\mathcal{A}, \{0, e_{i_1}\}, \ldots, \{0, e_{i_k}\}, \Delta^{(n-m-k)})$ tal que para cada vector de coeficientes $(a, \eta) = (a_1, \ldots, a_m, \eta_{m+1}, \ldots, \eta_n)$ de coordenadas racionales

no nulas tal que $\mathrm{q}(a,\eta) \neq 0$, el sistema ralo con esos coeficientes y soportes tiene tantos ceros aislados en $(\mathbb{C}^*)^n$ como el volumen mixto de sus soportes (ver el Teorema 1.14).

Sea $p \in \mathcal{J} \cap \mathbb{K}[X_{i_1}, \ldots, X_{i_k}]$. Sin perder generalidad podemos suponer que p es un elemento de $\mathbb{Q}[A, X_{i_1}, \ldots, X_{i_k}]$. Luego, existen $r \in \mathbb{Z}_{\geq 0}$ y un polinomio $p_0 \in \mathbb{Q}[A]$ no nulo tales que

$$p_0(A)(X_1 \ldots X_n)^r p(A, X_{i_1}, \ldots, X_{i_k}) = g_1 f_1 + \cdots + g_m f_m \tag{4.3}$$

donde $g_1, \ldots, g_m \in \mathbb{Q}[A, X_1, \ldots, X_n]$. Queremos ver que $p \equiv 0$.

Para cada vector de coeficientes (a, η) con coordenadas en $\mathbb{Q}^*$ tales que $p_0(a)\mathrm{q}(a,\eta) \neq 0$, tomemos $\xi \in (\mathbb{C}^*)^n$ un cero del sistema dado por los polinomios

$$f_1(a_1, X), \ldots, f_m(a_m, X), \eta_{m+1,1} + \eta_{m+1,2} X_{i_1}, \ldots, \eta_{m+k,1} + \eta_{m+k,2} X_{i_k},$$

$$\eta_{m+k+1,0} + \sum_{1 \leq i \leq n} \eta_{m+k+1,i} X_i, \ldots, \eta_{n,0} + \sum_{1 \leq i \leq n} \eta_{n,i} X_i.$$

Especializando en (a, η, ξ) la igualdad (4.3) tenemos que $p(a, -\frac{\eta_{m+1,1}}{\eta_{m+1,2}}, \ldots, -\frac{\eta_{m+k,1}}{\eta_{m+k,2}}) = 0$. Como esto vale para todo $(a, -\frac{\eta_{m+1,1}}{\eta_{m+1,2}}, \ldots, -\frac{\eta_{m+k,1}}{\eta_{m+k,2}})$ con coordenadas racionales no nulas en un abierto Zariski de $\mathbb{C}^{\sum_{j=1}^{m} \#\mathcal{A}_j + k}$, $p \equiv 0$.

Sea ahora $\{X_{i_1}, \ldots, X_{i_k}\}$ un subconjunto de variables algebraicamente independiente módulo $\mathcal{J} = I(V^*(F))$. Sean $l_1, \ldots, l_{n-m-k}$ formas lineales en las variables $X_1, \ldots, X_n$ con coeficientes en $\mathbb{K}^*$ tales que $\{X_{i_1}, \ldots, X_{i_k}, l_1, \ldots, l_{n-m-k}\}$ es una base de trascendencia de $\mathbb{K}(V^*(F))$. Como $V^*(F) \cap (\overline{\mathbb{K}}^*)^n$ es un abierto denso de $V^*(F)$, para $(\zeta_1, \ldots, \zeta_{n-m}) \in (\overline{\mathbb{K}}^*)^{n-m}$ genérico vale que

$$V^*(F) \cap \{x_{i_j} = \zeta_j \ \forall\, 1 \leq j \leq k\} \cap \{l_j(x) = \zeta_{k+j} \ \forall\, 1 \leq j \leq n-m-k\}$$

es un conjunto finito no vacío en $(\overline{\mathbb{K}}^*)^n$. Este conjunto está formado por los ceros en $(\overline{\mathbb{K}}^*)^n$ del sistema dado por los polinomios

$$f_1(X), \ldots, f_m(X), X_{i_1} - \zeta_1, \ldots, X_{i_k} - \zeta_k, l_1(X) - \zeta_{k+1}, \ldots, l_{n-m-k}(X) - \zeta_{n-m},$$

con soportes $\mathcal{A}_1, \ldots, \mathcal{A}_m, \{0, e_{i_1}\}, \ldots, \{0, e_{i_k}\}, \Delta^{(n-m-k)}$. Entonces, por el Teorema de Bernstein (ver el Teorema 1.14) vale $\mathcal{MV}_n(\mathcal{A}_1, \ldots, \mathcal{A}_m, \{0, e_{i_1}\}, \ldots, \{0, e_{i_k}\}, \Delta^{(n-m-k)}) > 0$. $\square$

Observación 4.6 *Por la Proposición 1.11, para cada subconjunto $\{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$ vale que el volumen mixto $\mathcal{MV}_n(\mathcal{A}_1, \ldots, \mathcal{A}_m, \{0, e_{i_1}\}, \ldots, \{0, e_{i_k}\}, \Delta^{(n-m-k)})$ es igual a $\mathcal{MV}_{n-k}(\varpi(\mathcal{A}_1), \ \ldots, \varpi(\mathcal{A}_m), \Delta^{(n-m-k)})$, donde $\varpi : \mathbb{R}^n \to \mathbb{R}^{n-k}$ es la proyección a las coordenadas indexadas por $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$. En función de esto, para decidir si un conjunto de k variables es algebraicamente independiente módulo $I(V^*(F))$ alcanza con calcular un volumen mixto en $\mathbb{R}^{n-k}$.*

4.2. Resultados algorítmicos

En esta sección vamos a presentar el algoritmo $\mathbb{K}$-`Projection` que permite calcular la clausura de Zariski de la proyección de $V^*(F)$ a sus primeras ℓ coordenadas, donde F es el sistema definido en (4.1). Previamente, describiremos algunas subrutinas utilizadas en este algoritmo.

4.2.1. Subrutinas

La primera de las subrutinas que utilizaremos, que se obtiene a partir del Lema 4.5, calcula una base de trascendencia de $\mathbb{K}(V^*(F))$ que contiene una base de trascendencia de $\mathbb{K}(\overline{\pi(V^*(F))})$.

Algoritmo 4.7 `TransBasis`

INPUT: Una familia $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ *de conjuntos finitos en* $(\mathbb{Z}_{\geq 0})^n$ *tal que* $\dim(\sum_{j\in J} \mathcal{A}_j) \geq \#J$ *para todo* $J \subset \{1, \ldots, m\}$.

1. $TB := \emptyset$.
2. $k := 1$.
3. *While* $\#TB < n - m$ *do*
   a) *Calcular* $D := \mathcal{MV}_n(\mathcal{A}_1, \ldots, \mathcal{A}_m, \left(\{0, e_{i_j}\}\right)_{i_j \in TB}, \{0, e_k\}, \Delta^{(n-m-\#TB-1)})$.
   b) *Si* $D > 0$, $TB := TB \cup \{k\}$.
   c) $k := k + 1$.

OUTPUT: El conjunto $TB = \{i_1, \ldots, i_{n-m}\}$ *con* $i_1 < \ldots < i_{n-m}$, *tal que* $\{X_{i_1}, \ldots, X_{i_{n-m}}\}$ *es una base de transcendencia de* $\mathbb{K}(V^*(F))$ *sobre* $\mathbb{K}$ *y, para cada* $1 \leq j \leq n - m$, $\{X_{i_1}, \ldots, X_{i_j}\}$ *es un subconjunto de* $\{X_1, \ldots, X_{i_j}\}$ *algebraicamente independendiente sobre* $\mathbb{K}$ *y maximal con esta propiedad.*

Consideremos la base de trascendencia de $\mathbb{K}(V^*(F))$ obtenida a partir del algoritmo `TransBasis`. Sin pérdida de generalidad, renombrando variables, podemos suponer que esta base es $\{X_1, \ldots, X_t, X_{t+m+1}, \ldots, X_n\}$ con $t \leq \ell$ y $\ell \leq t + m$. Entonces $\{X_1, \ldots, X_t\}$ es una base de trascendencia de $\mathbb{K}(\overline{\pi(V^*(F))})$.

Sea F_b el sistema que resulta de evaluar $X_{t+m+1}, \ldots, X_n$ en valores genéricos. Por la Proposición 4.4 podremos obtener $\overline{\pi(V^*(F))}$ trabajando con el sistema F_b. Para esto, en primer lugar calcularemos una resolución geométrica de $V^*(F_b)$ y luego obtendremos, a partir de ella, una resolución geométrica de $\overline{\pi(V^*(F))}$. Para hacer esto utilizaremos las dos subrutinas que introducimos a continuación.

Sean k un cuerpo y $G := (g_1, \ldots, g_m)$ un sistema en $k[X_1, \ldots, X_{t+m}]$ genérico con soportes $\mathcal{S} = (\mathcal{S}_1, \ldots, \mathcal{S}_m)$ en $(\mathbb{Z}_{\geq 0})^{t+m}$. Supongamos que $\{X_1, \ldots, X_t\}$ es un conjunto de variables algebraicamente independientes módulo cada primo asociado a $\langle g_1, \ldots, g_m \rangle : (X_1 \ldots X_{t+m})^\infty$. La subrutina `ParametricToricGeomRes`, basada en el algoritmo para el cálculo de resoluciones geométricas paramétricas de [60, Theorem 2], calcula una resolución geométrica de la variedad $V^*(G)$ con $X_1, \ldots, X_t$ como parámetros.

Algoritmo 4.8 `ParametricToricGeomRes`

INPUT: Un sistema de polinomios $G := (g_1, \ldots, g_m)$ en $k[X_1, \ldots, X_{t+m}]$ genérico con soportes $\mathcal{S} := (\mathcal{S}_1, \ldots, \mathcal{S}_m)$ en $(\mathbb{Z}_{\geq 0})^{t+m}$, codificado en forma rala, tal que el conjunto $\{X_1, \ldots, X_t\}$ es algebraicamente independiente módulo cada uno de los primos asociados a $\langle g_1, \ldots, g_m \rangle : (X_1 \ldots X_{t+m})^\infty$.

1. *Elegir al azar $\xi = (\xi_1, \ldots, \xi_t)$ con $\xi_i \in \mathbb{Z} \backslash \{0\}$ para todo $1 \leq i \leq t$.*
2. *Calcular una resolución geométrica de los ceros de $G(\xi, X_{t+1}, \ldots, X_{t+m})$ en $(\overline{k}^*)^m$.*
3. *Obtener una codificación como slp de los polinomios del sistema G.*
4. *Usando como parámetros a las variables $X_1, \ldots, X_t$, aplicar un levantamiento de Newton-Hensel simbólico a la resolución geométrica del paso 2 con precisión $2\mathcal{MV}_{m+t}(\mathcal{S}, \Delta^{(t)})$.*
5. *Aplicar el algoritmo* `PadéAprox` *(ver la Sección 1.4.3) al output del paso 4 para hallar los numeradores y denominadores en $k[X_1, \ldots, X_t]$ de los coeficientes de los polinomios que conforman la resolución geométrica de $V^*(G)$.*

OUTPUT: Una resolución geométrica de $V^*(G)$ con variables libres $X_1, \ldots, X_t$.

A continuación analizamos los pasos del algoritmo y estimamos la cantidad de operaciones en k que realiza. Usaremos la notación $N = \sum_{j=1}^{m} \#\mathcal{S}_j$ y $d = \max_{1 \leq j \leq m}\{\deg(g_j)\}$.

En el paso 2, el algoritmo calcula la codificación rala de $G(\xi, X_{t+1}, \ldots, X_{t+m})$ con $O(m(t+m)N\log(d))$ operaciones. Luego aplica el algoritmo `ToricSolve` (ver la Sección 2.1.2) con

$$O((m^3 N\log(d) + m^{1+\Omega})M(\Upsilon)M(\mathcal{MV}_m(\varpi(\mathcal{S})))(M(\mathcal{MV}_m(\varpi(\mathcal{S}))) + M(\mathcal{E})))$$

operaciones en k, donde ϖ es la proyección a las últimas m coordenadas, $\Upsilon = \max\{\|\eta\|\}$ donde el máximo se toma sobre todas las normales primitivas asociadas a celdas mixtas en una subdivisión de $\varpi(\mathcal{S}) = (\varpi(\mathcal{S}_1), \ldots, \varpi(\mathcal{S}_m))$ inducida por una función de levantamiento genérica ω, y $\mathcal{E} = \mathcal{MV}_{m+1}(\Delta \times \{0\}, \varpi(\mathcal{S}_1)(\omega_1), \ldots, \varpi(\mathcal{S}_m)(\omega_m))$.

Llamando $\omega_{\max}$ al máximo de los valores que toma ω y acotando $\mathcal{E}$ como en la estimación de la complejidad del Algoritmo 3.19 tenemos que la complejidad total de este paso es de $O(mtN\log(d) + m^3 N\log(d)\ M(\Upsilon)M(\mathcal{MV}_m(\varpi(\mathcal{S})))(M(\mathcal{MV}_m(\varpi(\mathcal{S}))) + M(\omega_{\max}\sum_{1\le k\le m}\mathcal{MV}_m(\varpi(\mathcal{S}_j)_{j\neq k}, \Delta))))$.

En el paso 3 se codifican como slp los polinomios $g_1, \ldots, g_m$ a partir de su codificación rala. La longitud del slp es del orden de $O((t+m)N\log(d))$.

El paso 4 del algoritmo se lleva a cabo modificando el procedimiento `Lift(F,T)` de [60, Section 4.2] para trabajar con series de potencias truncadas en varias variables codificadas como vectores de sus componentes homogéneas y cada componente como un slp. Para poder recuperar los numeradores y denominadores de los polinomios en la resolución geométrica de $V^*(G)$ mediante el proceso de aproximación de Padé (ver la Sección 1.4.3) necesitamos conocer sus desarrollos como series con precisión $2\deg(V^*(G))$. Por el Lema 3.1 este grado es $\mathcal{MV}_{t+m}(\mathcal{S}, \Delta^{(t)})$. La complejidad de este paso es $O((m(t+m)N\log(d) + m^4)M(\mathcal{MV}_m(\varpi(\mathcal{S})))\mathcal{MV}_{t+m}(\mathcal{S}, \Delta^{(t)})^2)$ y produce un slp que codifica los coeficientes del output con una longitud del mismo orden (comparar con [60, Section 4.2, Prop 5]).

En el paso 5, aplicamos el algoritmo `PadéAprox` para hallar los coeficientes de los polinomios de la resolución geométrica codificados como slp. La complejidad de este paso es del orden de $O(m\mathcal{MV}_{t+m}(\mathcal{S}, \Delta^{(t)})^{\overline{\Omega}+2})$ ya que para cada uno de los $O(m\mathcal{MV}_{t+m}(\mathcal{S}, \Delta^{(t)}))$ slp conseguidos en el paso anterior se calcula una $(\mathcal{MV}_{t+m}(\mathcal{S}, \Delta^{(t)}) + 1,\ \mathcal{MV}_{t+m}(\mathcal{S}, \Delta^{(t)}))$-aproximación de Padé (ver la Sección 1.4.3). Además, añade $O(m\mathcal{MV}_{t+m}(\mathcal{S}, \Delta^{(t)})^{\overline{\Omega}+1})$ operaciones a la longitud del slp.

Observando que

$$\mathcal{MV}_m(\varpi(\mathcal{S})) = \mathcal{MV}_{t+m}(\mathcal{S}, \{0, e_1\}, \ldots, \{0, e_t\}) \le \mathcal{MV}_{t+m}(\mathcal{S}, \Delta^{(t)}), \tag{4.4}$$

donde la igualdad de la izquierda vale por la Proposición 1.11 y la desigualdad de la derecha por la monotonía del volumen mixto, en base a los cálculos previos concluimos que la cantidad de operaciones en k que realiza el algoritmo es de orden

$$O((m^3 + mt)N\log(d)M(\Upsilon)M(\mathcal{MV}_m(\varpi(\mathcal{S})))\big(\mathcal{MV}_{t+m}(\mathcal{S}, \Delta^{(t)})^2 +$$

$$+M(\omega_{\text{máx}} \sum_{1\leq h\leq m} \mathcal{MV}_m(\varpi((\mathcal{S}_j)_{j\neq h}),\Delta))) + m\mathcal{MV}_{t+m}(\mathcal{S},\Delta^{(t)})^{\overline{\Omega}+2}).$$

El slp que codifica los coeficientes del output tiene una longitud de

$$O(m\mathcal{MV}_{t+m}(\mathcal{S},\Delta^{(t)})^2(((t+m)N\log(d)+m^3)M(\mathcal{MV}_m(\varpi(\mathcal{S}))) + \mathcal{MV}_{t+m}(\mathcal{S},\Delta^{(t)})^{\overline{\Omega}-1})).$$

Proposición 4.9 *Sea $G := (g_1,\ldots,g_m)$ un sistema en $k[X_1,\ldots,X_{t+m}]$ genérico con soportes $\mathcal{S} := (\mathcal{S}_1,\ldots,\mathcal{S}_m)$ en $(\mathbb{Z}_{\geq 0})^{t+m}$ tal que el conjunto $\{X_1,\ldots,X_t\}$ es algebraicamente independiente módulo cada uno de los primos asociados a $\langle g_1,\ldots,g_m\rangle : (X_1\ldots X_{t+m})^\infty$. El algoritmo probabilístico* `ParametricToricGeomRes` *calcula una resolución geométrica de $V^*(G)$ con variables libres $X_1,\ldots,X_t$. Con la notación anterior, la cantidad de operaciones en k que realiza el algoritmo es del orden de $O((m^3+mt)N\log(d)M(\Upsilon)M(\mathcal{MV}_m(\varpi(\mathcal{S})))$ $\big(\mathcal{MV}_{t+m}(\mathcal{S},\Delta^{(t)})^2+M(\omega_{\text{máx}}\sum_{1\leq k\leq m}\mathcal{MV}_m(\varpi((\mathcal{S}_j)_{j\neq k}),\Delta))\big)+m\mathcal{MV}_{t+m}(\mathcal{S},\Delta^{(t)})^{\overline{\Omega}+2})$. Además, la longitud del slp sobre k que codifica los coeficientes del output es del orden de $O(m\mathcal{MV}_{t+m}(\mathcal{S},\Delta^{(t)})^2(((t+m)N\log(d)+m^3)M(\mathcal{MV}_m(\varpi(\mathcal{S}))) + \mathcal{MV}_{t+m}(\mathcal{S},\Delta^{(t)})^{\overline{\Omega}-1}))$.*

La siguiente subrutina que utilizaremos, a la que llamamos `GeomResProj`, permite describir la proyección a un subespacio de coordenadas de una variedad equidimensional V dada por una resolución geométrica, en el caso en que la proyección tenga la misma dimensión que V.

Sean $\ell > t$, $\pi : \overline{k}^{t+m} \to \overline{k}^{\ell}$ la proyección $\pi(x_1,\ldots,x_{t+m}) = (x_1,\ldots,x_\ell)$ y $V \subset \overline{k}^{t+m}$ una variedad algebraica equidimensional de dimensión t tal que cada componente irreducible W de V cumple que $I(W)\cap k[X_1,\ldots,X_t] = \{0\}$. Entonces, $\{X_1,\ldots,X_t\}$ es un conjunto de variables libres para cada componente irreducible de $\overline{\pi(V)}$. Notando $\mathcal{K} := k(X_1,\ldots,X_t)$, sea $\lambda \in k[X_{t+1},\ldots,X_{t+m}]$ una forma lineal que sea un elemento primitivo de $\mathcal{K}\otimes k[V]$ y $(q_\lambda, w_{t+1},\ldots,w_{t+m}) \in \mathcal{K}[U]^{m+1}$ la resolución geométrica de V respecto a λ (ver la Sección 1.1.2). Sea D la dimensión de $\mathcal{K}\otimes k[V]$ como $\mathcal{K}$-espacio vectorial.

Sea $\mu = \mu_{t+1}X_{t+1}+\cdots+\mu_\ell X_\ell \in k[X_{t+1},\ldots,X_\ell]$ un elemento primitivo de $\mathcal{K}\otimes k[\overline{\pi(V)}]$. Para obtener una resolución geométrica $(q_\mu, v_{t+1},\ldots,v_\ell)$ de $\overline{\pi(V)}$ respecto a μ necesitamos encontrar el polinomio minimal de μ respecto de $\overline{\pi(V)}$. Como $I(\overline{\pi(V)}) = I(V)\cap k[X_1,\ldots,X_\ell]$, basta encontrar un polinomio $q_\mu \in \mathcal{K}[U]$ de grado mínimo tal que $q_\mu(\mu) \in \mathcal{K}\otimes I(V)$. Una vez encontrado este polinomio, los polinomios $v_{t+1},\ldots,v_\ell$ tales que $X_j = v_j(\mu)$ en $\mathcal{K}\otimes k[\overline{\pi(V)}]$, para todo $t+1 \leq j \leq \ell$, pueden obtenerse buscando la combinación lineal (con coeficientes en $\mathcal{K}$) de $\{1,\mu,\ldots,\mu^{\delta-1}\}$ en $\mathcal{K}\otimes k[V]$ tal que $X_j = \sum_{i=0}^{\delta-1} v_{j,i}\mu^i$, donde $\delta := \deg_U(q_\mu)$ es la dimensión de $\mathcal{K}\otimes k[\overline{\pi(V)}]$ como $\mathcal{K}$-espacio vectorial.

Usaremos la base $B_\lambda := \{1,\lambda,\ldots,\lambda^{D-1}\}$ de $\mathcal{K}\otimes k[V]$ para calcular estas combinaciones lineales. En primer lugar, buscamos la menor potencia δ de μ tal que μ^δ es combinación

lineal de $\{1, \mu, \ldots, \mu^{\delta-1}\}$ en $\mathcal{K} \otimes k[V]$. Como $X_j = w_j(\lambda)$ para todo $t+1 \leq j \leq t+m$, entonces $\mu = \sum_{j=t+1}^{\ell} \mu_j X_j = \sum_{j=t+1}^{\ell} \mu_j w_j(\lambda) = p_\mu(\lambda)$, donde definimos $p_\mu(U) \in \mathcal{K}[U]$ como el polinomio $p_\mu(U) := \sum_{j=t+1}^{\ell} \mu_j w_j(U)$. Así, para todo $i \in \mathbb{Z}_{>0}$ vale $\mu^i = p_\mu(\lambda)^i = (p_\mu(U)^i \pmod{q_\lambda(U)})|_{U=\lambda}$. Entonces, la matriz de $D \times D$ tal que sus columnas son los coeficientes de los polinomios $p_{\mu^i}(U) := (p_\mu(U)^i \mod q_\lambda(U))$ para $i = 0, \ldots, D-1$, tiene rango exactamente δ.

Igualando los coeficientes de cada potencia de λ en las igualdades

$$p_{\mu^\delta}(\lambda) = \sum_{i=0}^{\delta-1} (-q_{\mu,i}) p_{\mu^i}(\lambda) \quad \text{y} \quad w_j(\lambda) = \sum_{i=0}^{\delta-1} v_{j,i}\, p_{\mu^i}(\lambda),\ t+1 \leq j \leq \ell,$$

obtenemos sistemas lineales cuyas soluciones son los coeficientes de $q_\mu(U) = U^\delta + \sum_{i=0}^{\delta-1} q_{\mu,i} U^i$ y de $v_j(U) = \sum_{i=0}^{\delta-1} v_{j,i} U^i$ para todo $t+1 \leq j \leq \ell$, los polinomios de la resolución geométrica de $\overline{\pi(V)}$ respecto a μ.

Con la notación y las hipótesis previas, la subrutina `GeomResProj` es la siguiente:

Algoritmo 4.10 `GeomResProj`

INPUT: Un conjunto $\{X_1, \ldots, X_t\}$ *de variables libres y una resolución geométrica* $(q_\lambda, w_{t+1}, \ldots, w_{t+m})$ *de* V *en* $k(X_1, \ldots, X_t)[U]$. *Una forma lineal* $\mu = \sum_{j=1}^{\ell-t} \mu_{t+j} X_{t+j} \in k[X_{t+1}, \ldots, X_\ell]$ *que sea un elemento primitivo de* $\mathcal{K} \otimes k[\overline{\pi(V)}]$.

1. $p_{\mu^0}(U) := 1$ *y* $p_\mu(U) := \sum_{h=0}^{D-1} (\sum_{j=t+1}^{\ell} \mu_j w_{j,h}) U^h$, *donde* $(w_{j,0}, \ldots, w_{j,D-1}) =: \mathbf{w}_j$ *es el vector de coeficientes de* $w_j(U)$ *para todo* $j = t+1, \ldots, t+m$.
2. *Para* $i = 2, \ldots, D$, *calcular* $p_{\mu^i}(U) := (p_\mu(U) \cdot p_{\mu^{i-1}}(U) \pmod{q_\lambda(U)})$.
3. *Calcular* $\delta := rg(\mathbf{p}_{\mu^0}, \mathbf{p}_\mu, \ldots, \mathbf{p}_{\mu^{D-1}})$, *donde* $\mathbf{p}_{\mu^i} \in \mathcal{K}^{D\times 1}$ *es el vector de coeficientes de* p_{μ^i} *para todo* $0 \leq i \leq D-1$.
4. $\mathbf{P} := (\mathbf{p}_{\mu^0}, \mathbf{p}_\mu, \ldots, \mathbf{p}_{\mu^{\delta-1}}) \in \mathcal{K}^{D\times\delta}$.
5. *Hallar* $\mathbf{q} := (q_0, \ldots, q_{\delta-1})$ *y* $\mathbf{v}_j := (v_{j,0}, \ldots, v_{j,\delta-1})$ *las soluciones de los sistemas lineales* $\mathbf{P} \cdot \mathbf{q} = \mathbf{p}_{\mu^\delta}$ *y* $\mathbf{P} \cdot \mathbf{v}_j = \mathbf{w}_j$ *para todo* $t+1 \leq j \leq \ell$.

6. *Tomar* $q_\mu(U) := U^\delta - \sum_{i=0}^{\delta-1} q_i U^i$ *y* $v_j(U) := \sum_{i=0}^{\delta-1} v_{j,i} U^i$ *para todo* $t+1 \leq j \leq \ell$.

OUTPUT: La resolución geométrica $(q_\mu, v_{t+1}, \ldots, v_\ell)$ *en* $k(X_1, \ldots, X_t)[U]$ *de la proyección* $\overline{\pi(V)} \subset \overline{k}^\ell$ *respecto a la forma lineal* μ.

Proposición 4.11 *Con la notación e hipótesis anteriores, el algoritmo probabilístico* `GeomResProj` *calcula, a partir de una resolución geométrica* $(q_\lambda, w_{t+1}, \ldots, w_{t+m})$ *de* V *asociada a la forma lineal* λ *y variables libres* $X_1, \ldots, X_t$*, una resolución geométrica de* $\overline{\pi(V)}$ *con las mismas variables libres. Si* $q_\lambda, w_{t+1}, \ldots, w_{t+m}$ *están codificados en forma densa como polinomios de grado a lo sumo* D *en la variable* U *y sus coeficientes están codificados por un slp sobre* k *de longitud* L*, el algoritmo realiza* $O(L + D^{\overline{\Omega}} + D^2(\ell - t))$ *operaciones sobre* k *y produce un slp sobre* k *para los coeficientes de los polinomios del output cuya longitud es del mismo orden.*

Demostración: Solo debemos probar la cota de complejidad del algoritmo, ya que la correctitud del mismo surge de la explicación previa.

En el paso 1, el algoritmo calcula un slp que codifica los coeficientes del polinomio p_μ de longitud acotada por $L + 2D(\ell - t)$.

Para llevar a cabo el paso 2, se calculan en primer lugar recursivamente las potencias $U^D, \ldots, U^{2D-2}$ módulo $q_\lambda(U)$. Expandiendo el producto $p_\mu(U) \cdot p_{\mu^{i-1}}(U)$ y sustituyendo estas potencias de U se obtiene un slp de los coeficientes de $p_{\mu^i}(U)$ para $i = 2, \ldots, D$ de longitud $O(L + D(\ell - t) + D^3)$.

En el paso 3, el algoritmo calcula el rango de un matriz cuyas entradas son funciones racionales en $k(X_1, \ldots, X_t)$. Este rango se puede calcular de forma probabilística eligiendo un punto $x = (x_1, \ldots, x_t)$ al azar en el cual evaluar esas funciones racionales y calculando el rango δ de $(\mathbf{p}_{\mu^0}(x), \mathbf{p}_\mu(x), \ldots, \mathbf{p}_{\mu^{D-1}}(x))$. La evaluación se realiza con $O(L + D(\ell - t) + D^3)$ operaciones en k y el cálculo del rango con $O(D^\Omega)$ operaciones en k.

En el paso 5, el algoritmo resuelve $\ell - t + 1$ sistemas lineales. Para ello, calcula la matriz inversible $\mathbf{P}^t\mathbf{P}$ en $O(D\delta^2)$ operaciones en k, la matriz adjunta y el determinante de $\mathbf{P}^t\mathbf{P}$ con $O(\delta^{\overline{\Omega}})$ operaciones y los productos $\mathrm{adj}(\mathbf{P}^t\mathbf{P})\mathbf{p}_{\mu^\delta}$ y $\mathrm{adj}(\mathbf{P}^t\mathbf{P})\mathbf{w}_j$ para $t+1 \leq j \leq \ell$ con una complejidad del orden de $O(\delta^2(\ell - t))$.

En función de esto, el algoritmo produce un slp de longitud $O(L + D^3 + D\delta(\ell - t) + \delta^{\overline{\Omega}})$ sobre k con una complejidad del mismo orden. Finalmente, la cantidad de operaciones del enunciado se obtiene observando que $D \geq \delta$. □

4.2.2. Algoritmo

A continuación describimos el algoritmo $\mathbb{K}$-`Projection` que permite hallar una resolución geométrica de $\overline{\pi(V^*(F))}$ sobre $\mathbb{K}$.

Algoritmo 4.12 $\mathbb{K}$-`Projection`

INPUT: Una familia $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ *de conjuntos finitos en* $(\mathbb{Z}_{\geq 0})^n$ *tales que* $\dim(\sum_{j\in J} \mathcal{A}_j) \geq \#J$ *para todo* $J \subset \{1, \ldots, m\}$ *y un conjunto de variables* $\{X_1, \ldots, X_\ell\} \subset \{X_1, \ldots, X_n\}$.

1. *Aplicar el algoritmo* `TransBasis` *a la familia de conjuntos* $\mathcal{A}$. *Sin perder generalidad, suponemos que la base de trascendencia obtenida es* $\{X_1, \ldots, X_t, X_{t+m+1}, \ldots, X_n\}$ *donde* $t \leq \ell$ *y* $t + m + 1 > \ell$.
2. *Elegir* $b = (b_{t+m+1}, \ldots, b_n)$ *y* $(\lambda_{t+1}, \ldots, \lambda_{t+m})$ *con coordenadas en* $\mathbb{Z}$ *al azar.*
3. *Hallar la representación rala del sistema de polinomios* $F_b = (f_1(X_1, \ldots, X_{t+m}, b), \ldots, f_m(X_1, \ldots, X_{t+m}, b))$ *en* $\mathbb{K}[X_1, \ldots, X_{t+m}]$.
4. *Aplicar el algoritmo* `ParametricToricGeomRes` *al sistema* F_b *y las variables* $X_1, \ldots, X_t$ *para obtener una resolución geométrica* $(q_\lambda, w_{t+1}, \ldots, w_{t+m})$ *de* $V^*(F_b)$ *con variables libres* $X_1, \ldots, X_t$ *asociada a la forma lineal* $\lambda = \lambda_{t+1}X_{t+1} + \cdots + \lambda_{t+m}X_{t+m}$.
5. *Elegir* $(\mu_{t+1}, \ldots, \mu_\ell)$ *con coordenadas en* $\mathbb{Z}$ *al azar.*
6. *Aplicar el algoritmo* `GeomResProj` *a la resolución geométrica* $(q_\lambda, w_{t+1}, \ldots, w_{t+m})$ *y la forma lineal* $\mu = \mu_{t+1}X_{t+1} + \cdots + \mu_\ell X_\ell$.

OUTPUT: Una resolución geométrica $(q_\mu, v_{t+1}, \ldots, v_\ell)$ *de la variedad* $\overline{\pi(V^*(F))} \subset \overline{\mathbb{K}}^\ell$, *donde* $\pi : \overline{\mathbb{K}}^n \to \overline{\mathbb{K}}^\ell$ *es la proyección* $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_\ell)$.

Teorema 4.13 *Dada una familia* $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ *de conjuntos finitos en* $(\mathbb{Z}_{\geq 0})^n$ *tales que* $\dim(\sum_{j\in J} \mathcal{A}_j) \geq \#J$ *para todo* $J \subset \{1, \ldots, m\}$ *y la proyección* $\pi : \overline{\mathbb{K}}^n \to \overline{\mathbb{K}}^\ell$ *a las primeras* ℓ *coordenadas, el algoritmo probabilístico* $\mathbb{K}$-`Projection` *calcula una resolución geométrica de* $\overline{\pi(V^*(F))}$ *para el sistema ralo* F *con soportes* $\mathcal{A}$ *y coeficientes indeterminados. El algoritmo realiza*

$$O((n^2 + m^3)N \log(d) M(\mathcal{D})(\mathcal{D}^2 + M(\mathcal{E}))\Xi + m\mathcal{D}^{\overline{\Omega}+2})$$

operaciones en $\mathbb{K}$*, donde*

- $\mathcal{D} = \mathcal{MV}_n(\mathcal{A}, \Delta^{(n-m)})$,
- $d = \max_{1\leq j\leq m}\{\deg_X(f_j)\}$,
- $\mathcal{E} = \sum_{1\leq h\leq m} \mathcal{MV}_n(((\mathcal{A}_j)_{j\neq h}), \Delta^{(n-m+1)})$,
- $N = \sum_{1\leq j\leq m} \#\mathcal{A}_j$,
- Ξ *es una constante que mide el tamaño de ciertos objetos combinatorios, relacionados con la familia de soportes, involucrados en cálculos intermedios.*

Demostración: La correctitud sigue de las consideraciones previas y de la correctitud de las subrutinas involucradas.

El paso 1 se basa en el cálculo de volúmenes mixtos (ver el Algoritmo 4.7). Por este motivo, al igual que en los algoritmos anteriores no incluimos su costo en las estimaciones de complejidad. Entonces, para calcular la complejidad total del algoritmo es suficiente considerar el número de operaciones en $\mathbb{K}$ que se realizan en los pasos 3, 4 y 6.

El paso 3 puede realizarse con $O((n-t-m)N\log(d)+n(t+m)N\log(d)) = O(n^2N\log(d))$ operaciones en $\mathbb{K}$.

La complejidad del paso 4 está dada por la Proposición 4.9. Llamando $\mathcal{S}_j \subset (\mathbb{Z}_{\geq 0})^{t+m}$ a los conjuntos obtenidos al proyectar a las primeras $t+m$ coordenadas los conjuntos $\mathcal{A}_j$ para todo $1 \leq j \leq m$, el sistema F_b es un sistema genérico con soportes $\mathcal{S}$ para b genérico. Al igual que en la ecuación (4.4) podemos obtener las desigualdades

- $\mathcal{MV}_{t+m}(\mathcal{S}, \Delta^{(t)}) \leq \mathcal{MV}_n(\mathcal{A}, \Delta^{(n-m)})$,
- $\mathcal{MV}_m(\varpi(\mathcal{S})) \leq \mathcal{MV}_n(\mathcal{A}, \Delta^{(n-m)})$,
- $\mathcal{MV}_m(\varpi((\mathcal{S}_j)_{j\neq h}), \Delta) \leq \mathcal{MV}_n(((\mathcal{A}_j)_{j\neq h}), \Delta^{(n-m+1)})$ para todo $1 \leq h \leq m$.

En función de estas desigualdades, la complejidad de este paso resulta

$$O((m^3+mt)N\log(d)M(\Upsilon)M(\mathcal{D})(\mathcal{D}^2 + M(\omega_{\max}\mathcal{E})) + m\mathcal{D}^{\overline{\Omega}+2}).$$

Tomando Ξ una constante tal que $M(\Upsilon)M(\omega_{\max}) \leq \Xi$, la complejidad queda acotada por $O((m^3+mt)N\log(d)M(\mathcal{D})(\mathcal{D}^2 + M(\mathcal{E}))\Xi + m\mathcal{D}^{\overline{\Omega}+2})$.

La complejidad del paso 6 se calcula a partir de la Proposición 4.11. En este caso, $L = O(m\mathcal{D}^2(((t+m)N\log(d) + m^3)M(\mathcal{D}) + \mathcal{D}^{\overline{\Omega}-1}))$ es la longitud del slp que se obtuvo en el paso 4 y $D = \deg_U(q_\lambda) \leq \mathcal{MV}_n(\mathcal{A}, \Delta^{(n-m)})$.

Sumando las complejidades de los pasos recién mencionados obtenemos la complejidad del enunciado del teorema. □

A continuación ilustramos con un ejemplo cada uno de los pasos del algoritmo $\mathbb{K}$-`projection`.

Ejemplo 4.14 Sea F el sistema de 2 polinomios en 5 variables con soportes $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, donde $\mathcal{A}_1 = \{(0,0,0,0,0), (1,1,1,0,0), (2,0,0,4,2), (0,0,0,8,4)\}$ y $\mathcal{A}_2 = \{(1,0,1,1,2), (0,1,2,5,4), (1,3,0,5,4)\}$, con coeficientes indeterminados:

$$F = \begin{cases} f_1 = A_{11} + A_{12}X_1X_2X_3 + A_{13}X_1^2X_4^4X_5^2 + A_{14}X_4^8X_5^4 \\ f_2 = A_{21}X_1X_3X_4X_5^2 + A_{22}X_2X_3^2X_4^5X_5^4 + A_{23}X_1X_2^3X_4^5X_5^4 \end{cases}$$

y sea $\pi : \mathbb{C}^5 \to \mathbb{C}^3$ la proyección a las primeras tres coordenadas $\pi(x_1, x_2, x_3, x_4, x_5) = (x_1, x_2, x_3)$. Vamos a hallar una resolución geométrica de $\overline{\pi(V^*(F))}$ siguiendo los pasos del algoritmo $\mathbb{K}$-`Projection`.

En el paso 1, si se aplica el algoritmo `TransBasis` a los soportes, se obtiene que $\{X_1, X_2, X_4\}$ es una base de trascendencia de $\mathbb{K}(V^*(F))$ que cumple que $\{X_1, X_2\}$ es una base de trascendencia de $\mathbb{K}(\overline{\pi(V^*(F))})$.

En el paso 2, el algoritmo elige al azar un valor de b para especializar la variable X_4 y coeficientes para construir una forma lineal $\lambda = \lambda_3 X_3 + \lambda_5 X_5$. Sean $b = 1$ y $\lambda = X_5$.

En el paso 3, especializando $X_4 = 1$, se obtiene el sistema:

$$F_1 := \begin{cases} f_{11} = A_{11} + A_{12}X_1X_2X_3 + A_{13}X_1^2X_5^2 + A_{14}X_5^4 \\ f_{21} = A_{21}X_1X_3X_5^2 + A_{22}X_2X_3^2X_5^4 + A_{23}X_1X_2^3X_5^4 \end{cases}$$

En el paso 4, se aplica el algoritmo `ParametricToricGeomRes` para obtener la resolución geométrica de la variedad $V^*(F_b)$ con variables libres X_1, X_2 asociada a la forma lineal λ:

$$q_{X_5}(U) = U^{10} + \frac{2A_{13}X_1^2}{A_{14}}U^8 + \frac{A_{13}^2X_1^4 + 2A_{11}A_{14}}{A_{14}^2}U^6 + \frac{(-A_{12}A_{21}A_{14} + 2A_{11}A_{22}A_{13})X_1^2}{A_{22}A_{14}^2}U^4 +$$

$$+ \frac{-A_{12}A_{21}A_{13}X_1^4 + A_{11}^2A_{22} + A_{12}^2A_{23}X_1^3X_2^4}{A_{22}A_{14}^2}U^2 - \frac{A_{12}A_{21}A_{11}X_1^2}{A_{22}A_{14}^2} \qquad (4.5)$$

$$w_3(U) = -\frac{A_{14}}{A_{12}X_1X_2}U^4 - \frac{A_{13}X_1}{A_{12}X_2}U^2 - \frac{A_{11}}{A_{12}X_1X_2}$$

$$w_5(U) = U.$$

En el paso 5, se elige una forma lineal μ al azar como elemento primitivo de $\mathbb{K}(\overline{\pi(V^*(F))})$. En este caso, tomamos $\mu = X_3$.

En el último paso, se aplica el algoritmo `GeomResProj` a la resolución geométrica (q_{X_5}, w_3, w_5) y la forma lineal μ para hallar una resolución geométrica (q_{X_3}, v_3) de la variedad $\overline{\pi(V^*(F))}$. En este caso, el resultado es:

$$q_{X_3}(U) = U^5 + \frac{A_{11}}{A_{12}X_1X_2}U^4 + \frac{2A_{12}A_{23}X_1X_2^4 - A_{13}A_{21}X_1^2}{A_{12}A_{22}X_2^2}U^3 + \tag{4.6}$$

$$+\frac{2A_{23}A_{22}A_{11}X_2^4 + A_{21}^2A_{14}X_1}{A_{12}A_{22}^2X_2^3}U^2 + \frac{A_{12}A_{23}^2X_1^2X_2^4 - A_{13}A_{21}A_{23}X_1^3}{A_{12}A_{22}^2}U + \frac{A_{23}^2A_{11}X_1X_2^3}{A_{22}^2A_{12}}$$

$$v_3(U) = U.$$

4.3. Sistemas con coeficientes racionales genéricos

Consideremos ahora el problema planteado al inicio de este capítulo. Dado un sistema P de m polinomios con soportes $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ en $(\mathbb{Z}_{\geq 0})^n$ y coeficientes racionales genéricos, queremos calcular una resolucion geométrica de la clausura de Zariski de $\pi(V^*(P))$. Veremos en esta sección que llevando a cabo los mismos pasos del algoritmo $\mathbb{K}$-`Projection` conseguimos la resolución geométrica buscada.

Sea $\{X_1, \ldots, X_t, X_{t+m+1}, \ldots, X_n\}$ la base de trascendencia de $\mathbb{K}(V^*(F))$ tal que $\{X_1, \ldots, X_t\}$ es un subconjunto algebraicamente independiente maximal de $\{X_1, \ldots, X_\ell\}$ que hallamos con el algoritmo `TransBasis`. A partir de los resultados de [20, Appendix A], existe un abierto Zariski $\mathcal{U}_1$ no vacío tal que si $a = (a_1, \ldots, a_m) \in \mathcal{U}_1 \cap \mathbb{Q}^N$, entonces

- $I_a := \langle f_1(a, X), \ldots, f_m(a, X)\rangle : X^\infty$ es un ideal radical equidimensional de dimensión $n - m$,
- $\{X_1, \ldots, X_t, X_{t+m+1}, \ldots, X_n\}$ es un conjunto algebraicamente independiente módulo cada uno de los primos asociados a I_a,
- $\{X_1, \ldots, X_t, X_{t+h}\}$ es un conjunto algebraicamente dependiente módulo I_a para todo $1 \leq h \leq \ell - t$.

Sean $a \in \mathcal{U}_1 \cap \mathbb{Q}^N$ y $P = (p_1, \ldots, p_m)$ el sistema ralo con soportes $\mathcal{A}$ que resulta de evaluar el conjunto A de coeficientes indeterminados de F en a, es decir

$$p_j(X) = \sum_{\alpha \in \mathcal{A}_j} a_{j,\alpha}X^\alpha, \quad \text{para todo } 1 \leq j \leq m.$$

Sea W una componente irreducible de $V^*(P) \subset \mathbb{C}^n$. Entonces, $\dim(W) = n - m$ y $\{X_1, \ldots, X_t, X_{t+m+1}, \ldots, X_n\}$ es una base de transcendencia de $\mathbb{Q}(W)$. Por lo tanto, la proyección de W a las últimas $n - t - m$ coordenadas es un morfismo dominante. Por el Teorema de dimensión de la fibra y nuevamente [20, Appendix A], existe un abierto Zariski $\mathcal{O}_W \subset \mathbb{C}^{n-t-m}$ no vacío tal que, para todo $b \in \mathcal{O}_W \cap \mathbb{Q}^{n-t-m}$, vale

- $W_b := W \cap \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid x_{t+m+1} = b_{t+m+1}, \ldots, x_n = b_n\}$ es una variedad equidimensional de dimensión t,
- $\{X_1, \ldots, X_t\}$ es un conjunto algebraicamente independiente módulo $I(W_b)$.

Luego, para todo $b \in \mathcal{O}_W \cap \mathbb{Q}^{n-t-m}$ vale $\overline{\pi(W)} = \overline{\pi(W_b)}$.

Sea $\partial(V^*(P)) := V^*(P) \setminus \{x \in (\mathbb{C}^*)^n \mid P(x) = 0\})$. Como $\dim \partial(V^*(P)) < \dim V^*(P) = n - m$, para todo conjunto $\{i_1, \ldots, i_t\} \subset \{1, \ldots, t + m\}$ existe un polinomio no nulo $\mathbf{p}_{i_1,\ldots,i_t}(X_{i_1}, \ldots, X_{i_t}, X_{t+m+1}, \ldots, X_n)$ que se anula sobre $\partial(V^*(P))$. Sea $\mathcal{O}_1 = \{(x_{t+m+1}, \ldots, x_n) \in \mathbb{C}^{n-t-m} \mid \prod_{\{i_1,\ldots,i_t\}} \mathbf{p}_{i_1,\ldots,i_t}(X_{i_1}, \ldots, X_{i_t}, x_{t+m+1}, \ldots, x_n) \not\equiv 0\}$. Se tiene que $\mathcal{O}_1$ es un abierto Zariski no vacío y, para todo $b \in \mathcal{O}_1$, la dimensión de $\partial(V^*(P)) \cap \{x_{t+m+1} = b_{t+m+1}, \ldots, x_n = b_n\}$ es menor a t, ya que ningún subconjunto de t variables de $\{X_1, \ldots, X_{t+m}\}$ es libre para este conjunto.

Sea $b \in \mathcal{O}_1 \cap \bigcap_W \mathcal{O}_W \cap (\mathbb{Q}^*)^{n-t-m}$. Como

- $V^*(P) \cap \{x_{t+m+1} = b_{t+m+1}, \ldots, x_n = b_n\}$ es equidimensional de dimensión t pues $b \in \bigcap_W \mathcal{O}_W \cap (\mathbb{Q}^*)^{n-t-m}$, y
- $\overline{\partial(V^*(P)) \cap \{x_{t+m+1} = b_{t+m+1}, \ldots, x_n = b_n\}}$ tiene dimensión menor a t pues $b \in \mathcal{O}_1 \cap (\mathbb{Q}^*)^{n-t-m}$,

entonces,

$$V^*(P) \cap \{x_{t+m+1} = b_{t+m+1}, \ldots, x_n = b_n\} =$$
$$= \overline{\{x \in (\mathbb{C}^*)^n \mid P(x) = 0\} \cap \{x_{t+m+1} = b_{t+m+1}, \ldots, x_n = b_n\}} =$$
$$= \overline{\{\hat{x} \in (\mathbb{C}^*)^{t+m} \mid P(\hat{x}, b) = 0\} \times \{b\}}.$$

Por otra parte, como $b \in \bigcap_W \mathcal{O}_W \cap (\mathbb{Q}^*)^{n-t-m}$,

$$\overline{\pi(V^*(P))} = \bigcup_W \overline{\pi(W)} = \bigcup_W \overline{\pi(W_b)} = \overline{\pi(V^*(P) \cap \{x_{t+m+1} = b_{t+m+1}, \ldots, x_n = b_n\})}.$$

Por lo tanto

$$\overline{\pi(V^*(P))} = \overline{\pi(\{\hat{x} \in (\mathbb{C}^*)^{t+m} \mid P(\hat{x}, b) = 0\} \times \{b\})}.$$

Para cada $1 \leq j \leq m$, notemos $\mathcal{S}_j \subset (\mathbb{Z}_{\geq 0})^{t+m}$ a la proyección de $\mathcal{A}_j$ a sus primeras $t+m$ coordenadas y escribamos $f_j = \sum_{\hat{\alpha} \in \mathcal{S}_j} (\sum_{(\hat{\alpha},\tilde{\alpha}) \in \mathcal{A}_j} A_{j,(\hat{\alpha},\tilde{\alpha})} \tilde{X}^{\tilde{\alpha}}) \hat{X}^{\hat{\alpha}}$.

Recordemos que, para una familia de soportes $\mathcal{S} = (\mathcal{S}_1, \ldots, \mathcal{S}_m)$ en $(\mathbb{Z}_{\geq 0})^n$, el algoritmo `ParametricToricGeomRes` se aplica para sistemas genéricos G con esos soportes. Esto es, existe un polinomio $\mathrm{p}_{\mathcal{S}}$ en los coeficientes del sistema con soportes $\mathcal{S}$ tal que si $\hat{a}$ es un vector de coeficientes para el cual $\mathrm{p}_{\mathcal{S}}(\hat{a}) \neq 0$, entonces el algoritmo calcula una resolución geométrica de $V^*(G)$. Sea $\mathcal{U}_2 \subset \mathbb{C}^N$ un abierto Zariski no vacío tal que, para todo $a = (a_1, \ldots, a_m) \in \mathcal{U}_2$, el polinomio $\mathrm{p}_{\mathcal{S}}((\sum_{(\hat{\alpha},\tilde{\alpha}) \in \mathcal{A}_j} a_{j,(\hat{\alpha},\tilde{\alpha})} \tilde{X}^{\tilde{\alpha}})_{1 \leq j \leq m, \hat{\alpha} \in \mathcal{S}_j})$ no es el polinomio nulo.

Para todo $a \in \mathcal{U}_2 \cap \mathbb{Q}^N$, existe un abierto Zariski no vacío $\mathcal{O}_2 \subset \mathbb{C}^{n-t-m}$ tal que para todo $b \in \mathcal{O}_2 \cap \mathbb{Q}^{n-t-m}$, el algoritmo `ParametricToricGeomRes` puede aplicarse al sistema $P(\hat{x}, b)$, donde P es el sistema que resulta de evaluar $A = a$ en el sistema F con coeficientes indeterminados.

Llamemos $\mathbb{Q}$-`Projection` al algoritmo probabilístico que sigue los mismos pasos que el algoritmo $\mathbb{K}$-`Projection` para un sistema P con vector de coeficientes $a \in (\mathbb{Q}^*)^N$. Por lo anterior, para $a \in \mathcal{U}_1 \cap \mathcal{U}_2 \cap (\mathbb{Q}^*)^N$, el algoritmo $\mathbb{Q}$-`Projection` calcula una resolución geométrica de $\overline{\pi(V^*(P))}$. Tenemos entonces el siguiente resultado:

Teorema 4.15 *Sea $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_m)$ una familia de conjuntos finitos en $(\mathbb{Z}_{\geq 0})^n$ tal que $\dim(\sum_{j \in J} \mathcal{A}_j) \geq \#J$ para todo $J \subset \{1, \ldots, m\}$. Sean $P = (p_1, \ldots, p_m)$ un sistema genérico de polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ con soportes $\mathcal{A}$ y $\pi : \mathbb{C}^n \to \mathbb{C}^\ell$ la proyección a las primeras ℓ coordenadas. El algoritmo probabilístico* $\mathbb{Q}$-`Projection` *calcula una resolución geométrica de $\overline{\pi(V^*(P))}$ con*

$$O((n^2 + m^3) N \log(d) M(\mathcal{D})(\mathcal{D}^2 + M(\mathcal{E}))\Xi + m\mathcal{D}^{\overline{\Omega}+2})),$$

operaciones en $\mathbb{Q}$, donde

- $\mathcal{D} = \mathcal{MV}_n(\mathcal{A}, \Delta^{(n-m)})$,
- $N = \sum_{1 \leq j \leq m} \#\mathcal{A}_j$,
- $d = \max_j\{\deg(p_j)\}$,
- $\mathcal{E} = \sum_{1 \leq h \leq m} \mathcal{MV}_n(((\mathcal{A}_j)_{j \neq h}), \Delta^{(n-m+1)})$,
- Ξ *es una constante asociada al tamaño de ciertos objetos combinatorios relacionados con la familia de soportes (para más precisión, ver la demostración del Teorema 4.13).*

Para finalizar, veamos un ejemplo donde, siguiendo los pasos del algoritmo $\mathbb{Q}$-`projection` se obtiene una resolución geométrica de $\overline{\pi(V^*(P))}$ para un sistema ralo P con coeficientes racionales.

Ejemplo 4.16 Sea P el siguiente sistema con la misma familia de soportes $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ del Ejemplo 4.14:

$$P = \begin{cases} p_1 = 3 + 2X_1X_2X_3 - X_1^2X_4^4X_5^2 + 5X_4^8X_5^4 \\ p_2 = 2X_1X_3X_4X_5^2 - 3X_2X_3^2X_4^5X_5^4 + 7X_1X_2^3X_4^5X_5^4 \end{cases}$$

y sea $\pi : \mathbb{C}^5 \to \mathbb{C}^3$ la proyección a las primeras tres coordenadas $\pi(x_1, x_2, x_3, x_4, x_5) = (x_1, x_2, x_3)$.

Usaremos las mismas elecciones $b = 1$, $\lambda = X_5$ y $\mu = X_3$ que en el Ejemplo 4.14. Por lo tanto, solo nos interesan los pasos 4 y 6.

En el paso 4, el algoritmo `ParametricToricGeomRes` encuentra la resolución geométrica de $V^*(P_1)$ asociada a la forma lineal λ con variables libres X_1, X_2:

$$\widehat{q}_{X_5}(U) = U^{10} - \frac{2X_1^2}{5}U^8 + \frac{X_1^4 + 30}{25}U^6 + \frac{2X_1^2}{75}U^4 - \frac{4X_1^4 - 27 + 28X_1^3X_2^4}{75}U^2 + \frac{4X_1^2}{25}$$

$$\widehat{w}_3(U) = \frac{-5}{2X_1X_2}U^4 + \frac{X_1}{2X_2}U^2 - \frac{3}{2X_1X_2}$$

$$\widehat{w}_5(U) = U.$$

En el paso 6, si se aplica el algoritmo `GeomResProj` a la resolución geométrica del paso 4 y la forma lineal μ, se obtiene la resolución geométrica $(\widehat{q}_{X_3}, \widehat{v}_3)$, donde

$$\widehat{q}_{X_3}(U) = U^5 + \frac{3}{2X_1X_2}U^4 - \frac{14X_1X_2^4 + X_1^2}{3X_2^2}U^3 +$$

$$+\frac{-63X_2^4 + 10X_1}{9X_2^3}U^2 + \frac{49X_1^2X_2^4 + 7X_1^3}{9}U + \frac{49X_1X_2^3}{6}$$

$$\widehat{v}_3(U) = U.$$

Ésta resulta ser, en efecto, la resolución geométrica de $\overline{\pi(V^*(F))}$ con variables libres X_1, X_2 respecto a la forma lineal $\mu = X_3$, como se puede comprobar, por ejemplo, haciendo eliminación con bases de Groebner.

Bibliografía

[1] S. S. Abhyankar, *Algebraic geometry for scientists and engineers.* Mathematical Surveys and Monographs, vol. 35, American Mathematical Society, Providence, RI, 1990.

[2] D. Adrovic, J. Verschelde, *Computing Puiseux series for algebraic surfaces.* Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation (ISSAC 2012), Grenoble, France, July 22-25, 2012, 20–27.

[3] D. Adrovic, J. Verschelde, *Polyhedral methods for space curves exploiting symmetry.* arXiv:1109.0241v1 [math.NA].

[4] E. L. Allgower, K. Georg, *Numerical continuation methods: an introduction.* Springer Ser. Comput. Math., vol. 13, Springer, New York, 1990.

[5] S. Basu, R. Pollack, M.-F. Roy, *Algorithms in real algebraic geometry.* Algorithms and Computation in Mathematics, vol. 10, Springer-Verlag, Berlin, 2003.

[6] S. J. Berkowitz, *On computing the determinant in small parallel time using a small number of processors.* Inform. Process. Lett. 18 (1984), no. 3, 147–150.

[7] D. N. Bernstein, *The number of roots of a system of equations.* Funct. Anal. Appl. 9 (1975), 183–185.

[8] D. Bini, V. Y. Pan. *Polynomial and matrix computations. Volume 1. Fundamental algorithms.* Progress in Theoretical Computer Science, Birkhäuser Boston, Inc., Boston, MA, 1994.

[9] Y. D. Burago, V. A. Zalgaller, *Geometric inequalities.* Springer Series in Soviet Mathematics, Springer-Verlag, Berlin, 1988.

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

[11] L. Caniglia, *How to compute the Chow form of an unmixed polynomial ideal in single exponential time.* Appl. Algebra Engrg. Comm. Comput. 1 (1990), no. 1, 25–41.

[12] J. Canny, I. Z. Emiris, *A subdivision-based algorithm for the sparse resultant.* J. ACM 47 (2000), no. 3, 417–451.

[13] E. Cattani, A. Dickenstein, *Counting solutions to binomial complete intersections.* J. Complexity, 23 (2007), no. 1, 82-107.

[14] A. L. Chistov, D. Y. Grigor'ev, *Complexity of quantifier elimination in the theory of algebraically closed fields.* Mathematical foundations of computer science, 1984 (Prague, 1984), 17–31, Lecture Notes in Comput. Sci., vol. 176, Springer, Berlin, 1984.

[15] A. L. Chistov, D. Y. Grigor'ev, *Subexponential time solving systems of algebraic equations.* LOMI preprint E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.

[16] D. Cox, J. Little, D. O'Shea, *Ideals, varieties and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Undergrad. Texts in Math., vol. 10. Springer-Verlag, New York, 1992.

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

[18] C. D'Andrea, *Macaulay style formulas for sparse resultants.* Trans. Amer. Math. Soc. 354 (2002), no. 7, 2595–2629.

[19] C. D'Andrea, A. Dickenstein, *Explicit formulas for the multivariate resultant.* J. Pure Appl. Algebra 164 (2001), no. 1-2, 59–86.

[20] L. D'Alfonso, G. Jeronimo, F. Ollivier, A. Sedoglavic, P. Solernó, *A geometric index reduction method for implicit systems of differential algebraic equations.* J. Symbolic Comput. 46 (2011), 1114–1138.

[21] V. I. Danilov, *The geometry of toric varieties.* Russ. Math. Surv. 33 (1978), 97–154.

[22] A. Dickenstein, I. Z. Emiris, *Solving polynomial equations: foundations, algorithms, and applications.* Algorithms and Computation in Mathematics, vol. 14, Springer-Verlag, Berlin, 2005.

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

[24] M. Elkadi, B. Mourrain, *A new algorithm for the geometric decomposition of a variety.* Proceedings of ISSAC'99, 9–16 (electronic), ACM, New York, 1999.

[25] I. Z. Emiris, J. F. Canny, *Efficient incremental algorithms for the sparse resultant and the mixed volume.* J. Symbolic Comput. 20 (1995), no. 2, 117–149.

[26] I. Z. Emiris, J. Verschelde, *How to count efficiently all affine roots of a polynomial system.* 13th European Workshop on Computational Geometry CG'97 (Würzburg, 1997). Discrete Appl. Math. 93 (1999), no. 1, 21–32.

[27] G. Ewald, *Combinatorial convexity and algebraic geometry.* Grad. Texts in Math., vol. 168. Springer-Verlag, New York, 1996.

[28] N. Fitchas, A. Galligo, J. Morgenstern, *Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields.* J. Pure Appl. Algebra 67 (1990), no. 1, 1–14.

[29] W. Fulton, *Intersection theory.* Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 2. Springer-Verlag, Berlin, 1998.

[30] T. Gao, T. Y. Li, *Mixed volume computation for semi-mixed systems.* Discrete Comput. Geom. 29 (2003), no. 2, 257–277.

[31] T. Gao, T. Y. Li, X. Wang, *Finding all isolated zeroes of polynomial systems in $\mathbb{C}^n$ via stable mixed volumes.* J. Symbolic Comput. 28 (1999), no. 1-2, 187–211.

[32] J. von zur Gathen, J. Gerhard, *Modern computer algebra.* Cambridge University Press, Cambridge, 1999.

[33] I. M. Gelfand, M. M. Kapranov, A. V. Zelevinsky, *Discriminants, resultants, and multidimensional determinants.* Mathematics: Theory & Applications. Birkhäuser Boston, Boston, MA, 1994.

[34] P. Gianni, B. Trager, G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals.* J. Symbolic Comput. 6 (1988), no. 2-3, 149-167.

[35] M. Giusti, J. Heintz, *Algorithmes - disons rapides - pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionelles.* Proc. Effective methods in algebraic geometry (Castiglioncello, 1990), 169–194, Progr. Math., 94 Birkhäuser Boston, Boston, MA, 1991.

[36] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, L. M. Pardo, *Straight-line programs in geometric elimination theory.* J. Pure Appl. Algebra 124 (1998), no. 1–3, 101–146.

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

[38] J. Harris, *Algebraic geometry. A first course.* Grad. Texts in Math., vol. 133. Springer-Verlag, New York, 1992.

[39] R. Hartshorne, *Algebraic geometry.* Grad. Texts in Math., vol. 52. Springer-Verlag, New York-Heidelberg, 1977.

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

[41] J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, *Deformation techniques for efficient polynomial equation solving.* J. Complexity 16 (2000), no. 1, 70–109.

[42] B. Huber, B. Sturmfels, *A polyhedral method for solving sparse polynomial systems.* Math. Comp. 64 (1995), no. 212, 1541–1555.

[43] B. Huber, B. Sturmfels, *Bernstein's theorem in affine space.* Discrete Comput. Geom. 17 (1997), no. 2, 137–141.

[44] G. Jeronimo, T. Krick, J. Sabia, M. Sombra, *The computational complexity of the Chow form.* Found. Comput. Math. 4 (2004), no. 1, 41–117.

[45] G. Jeronimo, G. Matera, P. Solernó, A. Waissbein, *Deformation techniques for sparse systems.* Found. Comput. Math. 9 (2009), no. 1, 1–50.

[46] G. Jeronimo, J. Sabia, *Effective equidimensional decomposition of affine varieties.* J. Pure Appl. Algebra 169 (2002), no. 2-3, 229–248.

[47] G. Jeronimo, J. Sabia, *Computing multihomogeneous resultants using straight-line programs.* J. Symbolic Comput. 42 (2007), no. 1-2, 218–235.

[48] A. G. Khovanskii, *Newton polyhedra and toroidal varieties.* Funct. Anal. Appl. 11 (1978), 289–296.

[49] T. Krick, L. M. Pardo, M. Sombra, *Sharp estimates for the arithmetic Nullstellensatz.* Duke Math. J. 109 (2001), no. 3, 521–598.

[50] A. G. Kushnirenko, *Newton polytopes and the Bézout theorem.* Funct. Anal. Appl. 10 (1976), 233-235.

[51] G. Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers.* J. Complexity 19 (2003), no. 4, 564–596.

[52] T. Y. Li, *Numerical solution of multivariate polynomial systems by homotopy continuation methods.* Acta Numer. 6 (1997), 399–436.

[53] T. Y. Li, X. Li, *Finding mixed cells in the mixed volume computation.* Found. Comput. Math. 1 (2001), no. 2, 161–181.

[54] T. Y. Li, X. Wang, *The BKK root count in* $\mathbb{C}^n$. Math. Comp. 65 (1996), no. 216, 1477-1484.

[55] T. Mizutani, A. Takeda, M. Kojima, *Dynamic enumeration of all mixed cells.* Discrete Comput. Geom. 37 (2007), no. 3, 351–367.

[56] S. Puddu, J. Sabia, *An effective algorithm for quantifier elimination over algebraically closed fields using straight line programs.* J. Pure Appl. Algebra 129 (1998), no. 2, 173–200.

[57] J. M. Rojas, *A convex geometrical approach to counting the roots of a polynomial system.* Theoret. Comput. Sci. 133 (1994), no. 1, 105–140.

[58] J. M. Rojas, *Why polyhedra matter in non-linear equation solving.* Topics in algebraic geometry and geometric modeling. 293–320, Contemp. Math. 334, Amer. Math. Soc., Providence, RI, 2003.

[59] J. M. Rojas, X. Wang, *Counting affine roots of polynomial systems via pointed Newton polytopes.* J. Complexity 12 (1996), no. 2, 116–133.

[60] É. Schost, *Computing parametric geometric resolutions.* Appl. Algebra Eng. Commun. Comput. 13 (2003), no. 5, 349–393.

[61] J. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities.* J. ACM 27 (1980), 701-717.

[62] I. R. Shafarevich, *Basic algebraic geometry I. Varieties in projective space.* Springer-Verlag, Berlin, 1994.

[63] R. Steffens, T. Theobald, *Mixed volume techniques for embeddings of Laman graphs.* J. Comput. Geom. 43 (2010), no. 2, 84–93.

[64] A. Sommese, C. Wampler, *Numerical algebraic geometry.* The mathematics of numerical analysis. 749-763, Lectures in Appl. Math., 32, Amer. Math. Soc., Providence, RI, 1996.

[65] A. J. Sommese, C. W. Wampler, *The numerical solution of systems of polynomials arising in engineering and science.* World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.

[66] B. Sturmfels, *On the Newton polytope of the resultant.* J. Algebraic Combin. 3 (1994), no. 2, 207–236.

[67] A. Tarski, *A decision method for elementary algebra and geometry.* 2nd ed. University of California Press, Berkeley and Los Angeles, CA, 1951.

[68] N. V. Trung, J. Verma, *Mixed multiplicities of ideals versus mixed volumes of polytopes.* Trans. Amer. Math. Soc. 359 (2007), 4711-4727.

[69] J. Verschelde, *Polyhedral methods in numerical algebraic geometry.* Interactions of Classical and Numerical Algebraic Geometry. 243–263, Contemp. Math. 496, Amer. Math. Soc., Providence, RI, 2009.

[70] J. Verschelde, K. Gatermann, R. Cools, *Mixed-volume computation by dynamic lifting applied to polynomial system solving.* Discrete Comput. Geom. 16 (1996), no. 1, 69–112.

[71] J. Verschelde, P. Verlinden, R. Cools, *Homotopies exploiting Newton polytopes for solving sparse polynomial systems.* SIAM J. Numer. Anal. 31 (1994), no. 3, 915–930.

[72] R. Walker, *Algebraic curves.* Springer, New York, 1978.

[73] R. Zippel, *Effective polynomial computation.* Kluwer Int. Ser. Eng. Comput. Sci., vol. 241, Kluwer, Dordrecht, 1993.