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

ASPECTOS ALGORÍTMICOS DE GEOMETRÍA SEMIALGEBRAICA

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

Daniel Perrucci

Directores de tesis: Dr. Juan Sabia
Dra. Gabriela Jeronimo
Consejero de estudios: Dr. Juan Sabia

Buenos Aires, 2008

Aspectos algorítmicos de geometría semialgebraica

Esta tesis versa sobre distintos aspectos algorítmicos de geometría semialgebraica; más concretamente, sobre la resolución efectiva de sistemas de ecuaciones e inecuaciones polinomiales sobre el cuerpo de los números reales. El trabajo se encuentra dividido en tres capítulos en los que se consideran problemas encuadrados en este marco general.

En el primer capítulo, estudiamos cotas inferiores de complejidad para los algoritmos de resolución de ecuaciones polinomiales sobre los reales. Probamos resultados relacionados con la intratabilidad tanto de decidir la existencia como de aproximar las raíces reales para polinomios univariados con coeficientes enteros codificados vía *straight-line programs*.

En el segundo capítulo presentamos nuevos métodos probabilísticos para decidir la existencia de soluciones de un sistema de ecuaciones e inecuaciones polinomiales sobre los reales y para encontrar puntos en el conjunto de soluciones de estos sistemas. La complejidad de estos métodos mejora la de los algoritmos anteriores conocidos que resuelven el mismo problema.

Finalmente, en el tercer capítulo estudiamos un problema proveniente de la teoría de juegos que se modela mediante sistemas de ecuaciones e inecuaciones polinomiales sobre los reales. Para tratar con estos sistemas, desarrollamos métodos específicos de manera de aprovechar las particularidades que presentan.

Palabras clave: sistemas de ecuaciones e inecuaciones polinomiales, teoría de complejidad, *straight-line programs*, cálculo simbólico, equilibrios de Nash.

Algorithmic aspects in semialgebraic geometry

This thesis deals with different algorithmic aspects in semialgebraic geometry; more precisely, with the effective resolution of polynomial systems of equations and inequalities over the real numbers. The thesis is divided into three chapters in which problems within this general frame are considered.

In the first chapter, we study lower bounds for the complexity of algorithms solving polynomial equation systems over the real numbers. We prove some results related to the intractability of both the problem of deciding the existence of real roots and the problem of approximating real roots of univariate polynomials with integer coefficients encoded by straight-line programs.

In the second chapter, we present new probabilistic methods to decide the existence of solutions to polynomial systems of equations and inequalities over the real numbers and to find points in the solution sets of these systems. The complexity of these methods is lower than the ones of the previous known algorithms solving the same problem.

Finally, in the third chapter, we study a problem from game theory that can be modeled by means of polynomial systems of equations and inequalities over the real numbers. To deal with these systems, we develop specific methods in order to exploit the particularities they present.

Key words: polynomial systems of equations and inequalities, complexity theory, straight-line programs, symbolic computation, Nash equilibria.

Agradecimientos:

A Juan y a Gabriela.
A Flor.
A mis viejos.
A mis amigos del almuerzo y la merienda.

Índice general

Introducción

Los sistemas de ecuaciones e inecuaciones polinomiales multivariadas son útiles para modelar diversos problemas de distintas áreas tales como robótica, procesamiento de señales, biología molecular, diseño por computadora, estadística y teoría de juegos entre otras. El desarrollo de la computación hizo factible la resolución de estos sistemas algorítmicamente; de allí el interés por obtener procedimientos efectivos para encontrar y describir sus soluciones.

Desde el punto de vista computacional, uno de los principales problemas es el de estimar el tiempo necesario para la ejecución de un algoritmo. Esto puede medirse en una primera aproximación por medio de su complejidad algebraica, es decir, la cantidad de operaciones que el algoritmo efectúa a partir de un *input* dado.

Esta tesis se centra en el estudio de aspectos algorítmicos de la resolución de sistemas de ecuaciones e inecuaciones polinomiales sobre los reales y en el análisis de la complejidad de este problema. En este contexto, resultan importantes tanto el diseño de algoritmos eficientes, como un estudio que pueda brindar información sobre los mismos, por ejemplo, la imposibilidad teórica de encontrar algoritmos que funcionen en cierto tiempo deseado.

Uno de los problemas básicos de geometría algebraica real que consideraremos en esta tesis consiste en decidir algorítmicamente si un sistema de ecuaciones polinomiales con coeficientes reales en n variables tiene o no una solución en $\mathbb{R}^n$. Este problema es difícil de resolver en toda su generalidad. Por "difícil de resolver" nos referimos concretamente a que no existe un algoritmo con complejidad polinomial en el tamaño de los datos de entrada que permita constestar la pregunta planteada, a menos que P = NP.

Por otro lado, dado que el sistema de ecuaciones $f_1 = \cdots = f_m = 0$, donde $f_1, \ldots, f_m$ son polinomios en $\mathbb{R}[x_1, \ldots, x_n]$, admite una solución en $\mathbb{R}^n$ si y solo si la ecuación $f_1^2 + \cdots + f_m^2 = 0$ admite una solución en $\mathbb{R}^n$, tenemos que el problema de decidir si un sistema de ecuaciones polinomiales tiene una solución en $\mathbb{R}^n$ es equivalente al

de decidir si una ecuación polinomial tiene una solución en $\mathbb{R}^n$.

Ante la dificultad de resolver este problema en toda su generalidad, surge la idea de restringir el mismo a familias de ecuaciones polinomiales con una estructura particular e intentar aprovechar dicha estructura para encontrar un algoritmo de complejidad polinomial que permita decidir la existencia de soluciones reales.

En [Pla77] se mostró que el problema de decidir si un polinomio univariado con coeficientes enteros dado mediante la codificación rala tiene o no una raíz compleja de módulo 1 es NP-hard. Este resultado fue utilizado luego por Bürgisser para probar que el problema de decidir si un polinomio univariado con coeficientes enteros codificado por un *straight-line program* tiene o no una raíz real es también NP-hard (esta demostración no fue publicada, pero un bosquejo de la misma puede encontrarse en [Roj00]). El mismo resultado fue obtenido de manera independiente en [RGK02, Theorem 5.10] en el contexto de geometría dinámica.

En el primer capítulo de esta tesis, daremos una nueva demostración de que decidir si un polinomio univariado con coeficientes enteros codificado por un *straight-line program* tiene o no una raíz real es NP-hard. Nuestra demostración se basa en una adaptación conveniente al contexto real de la construcción descripta en [Pla77], utilizando los polinomios de Tchebychev de primer tipo. Esta nueva demostración nos permite asimismo obtener un nuevo resultado: el problema de la aproximación de raíces reales para polinomios univariados con coeficientes enteros, codificados por *straight-line programs*, es NP-hard.

A pesar de las limitaciones mencionadas, es importante desarrollar herramientas algorítmicas eficientes que permitan obtener información sobre el conjunto de soluciones de sistemas de ecuaciones e inecuaciones polinomiales sobre los reales, en particular, para determinar la consistencia de sistemas de este tipo. En el segundo capítulo de la tesis, estudiaremos este problema.

Más precisamente, dados polinomios $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$, consideraremos sistemas de igualdades y desigualdades

$$\left\{ \begin{array}{lll} f_1 & \sigma_1 & 0, \\ & \vdots & \\ f_m & \sigma_m & 0, \end{array} \right. \qquad (*)$$

donde $\sigma = (\sigma_1, \ldots, \sigma_m)$ y $\sigma \in \{<, =, >\}^m$ o $\sigma \in \{\leq, =, \geq\}^m$. En este caso, diremos que σ es una *condición de signo* o *condición de signo cerrada* respectivamente para los polinomios dados y llamaremos *realización* de σ al conjunto de soluciones en $\mathbb{R}^n$

del sistema de igualdades y desigualdades $(*)$. Cuando este conjunto sea no vacío, diremos que σ es *factible* y que el sistema es *consistente*.

El problema de determinar si una condición de signo para una familia de polinomios es factible es un caso particular del problema de eliminación de cuantificadores en la teoría de primer orden sobre los reales y, por otro lado, muchos algoritmos de eliminación utilizan la subrutina de decidir cuáles son todas las condiciones de signo factibles para una familia de polinomios. Es por esto que los sucesivos avances en el diseño de algoritmos que resuelven uno u otro problema han estado siempre estrechamente ligados.

Los primeros algoritmos de eliminación sobre los reales se deben a Tarski [Tar51] y Seidenberg [Sei54], pero la complejidad de los mismos es una función que no es recursiva elemental. El siguiente gran avance fue un algoritmo, presentado en [Col75], cuya complejidad es doblemente exponencial. Posteriormente, en [GV88], se dio un algoritmo de complejidad simplemente exponencial para decidir la consistencia de sistemas de desigualdades polinomiales no estrictas sobre $\mathbb{R}$ mediante el estudio de puntos críticos de funciones. Esta idea fue luego reutilizada en [HRS90, Ren92, BPR96] para obtener algoritmos de eliminación de complejidad simplemente exponencial. Estos algoritmos se basan en el cálculo de un conjunto finito de puntos que interseca a cada componente conexa de un conjunto semialgebraico.

El problema específico de la consistencia de un sistema de igualdades polinomiales sobre $\mathbb{R}$ fue también tratado mediante el estudio de puntos críticos (ver, por ejemplo, [RRSED00] y [ARSED02]). Varios procedimientos probabilísticos llevaron luego a mejorar las complejidades de estos algoritmos. Mediante el estudio de variedades polares clásicas, en [BGHM97, BGHM01] se trata el caso de variedades suaves compactas definidas por polinomios que forman una sucesión regular, obteniéndose un algoritmo cuya complejidad depende polinomialmente del grado intrínseco de los sistemas de ecuaciones involucrados y la longitud de los datos de entrada. Para obtener esta complejidad, se utilizan la codificación de polinomios mediante *straight-line programs* junto con procedimientos eficientes para resolver sistemas de ecuaciones polinomiales sobre $\mathbb{C}$ ([GHH$^+$97]). La hipótesis de compacidad es suprimida en [BGHP04, BGHP05, SEDS03] y en [SEDT] se extienden estos resultados al caso no equidimensional.

En el segundo capítulo de esta tesis presentaremos un algoritmo probabilístico para calcular, dada una familia de polinomios $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$, un conjunto finito con la propiedad de intersecar la clausura de cada componente conexa de

la realización de cada condición de signo definida por estos polinomios en tres situaciones diferentes: bajo ciertas hipótesis de regularidad sobre los polinomios (ver Hipótesis 2.31), en el caso de polinomios bivariados arbitrarios y en el caso de un único polinomio multivariado arbitrario. Además presentaremos, para el caso general, un algoritmo probabilístico para calcular un conjunto finito con la propiedad de intersecar cada componente conexa de la realización de cada condición de signo cerrada. Estos algoritmos se basan en el cálculo de puntos extremales para funciones coordenadas. En cualquiera de los casos mencionados, evaluando los signos de los polinomios $f_1, \ldots, f_m$ en los puntos del conjunto hallado obtenemos la lista de todas las condiciones de signo *cerradas* factibles para la familia de polinomios dada. Además, en la primera de las situaciones descriptas, estos resultados nos permiten obtener también todas las condiciones de signo factibles para dicha familia de polinomios.

La complejidad de los métodos presentados en este capítulo mejora la complejidad en el peor caso, que es a su vez el caso genérico, de los algoritmos previos que resuelven el mismo problema. Una herramienta fundamental para lograr este objetivo es el uso de técnicas de deformación especialmente diseñadas (ver [HJSS05]) para tratar con los sistemas de ecuaciones utilizados para caracterizar los puntos extremales. Hasta ahora, estos sistemas eran tratados mediante algoritmos generales de resolución de sistemas de ecuaciones ([ABRW96, Rou99, GLS01, Lec03]) y la estructura de los mismos solamente había sido aprovechada para obtener cotas sobre la cantidad de componentes conexas de las realizaciones de las condiciones de signo definidas por la familia de polinomios de entrada ([SEDT]), pero no desde el punto de vista algorítmico. Nuestro trabajo también puede ser considerado una extensión de los trabajos [SEDS03] y [BGHP05], en el sentido en que trabajamos no solamente con igualdades sino también con desigualdades.

En el último capítulo de esta tesis, trataremos un problema proveniente de la teoría de juegos que puede modelarse por medio de sistemas de ecuaciones e inecuaciones polinomiales sobre los reales.

La teoría de juegos se ocupa de analizar interacciones estratégicas. Esta teoría ha jugado un rol fundamental en economía (ver por ejemplo [vNM07]) y también ha sido aplicada en diversas áreas como política, sociología, psicología y biología.

Un juego *no cooperativo* es una situación de interacción entre varios jugadores en la que cada uno busca maximizar su propia ganancia sin comunicarse con los demás. Un juego *en forma normal* es uno que se desarrolla en un único paso en el que cada

uno de los jugadores elige una entre una cantidad finita de estrategias, llamadas *estrategias puras*, y, de acuerdo a la combinación resultante de elecciones, obtiene una cierta ganancia. Si el juego se repite más de una vez, cada jugador puede asignar una probabilidad a la opción de adoptar cada una de sus estrategias puras, de modo que los demás no sepan cuál será su comportamiento de antemano. Una tal asignación de probabilidades recibe el nombre de *estrategia mixta*.

Uno de los conceptos principales en este modelo es el de *equilibrio de Nash*, que consiste en una elección de una estrategia mixta por parte de cada jugador, de modo que ninguno puede incrementar la esperanza de su ganancia simplemente cambiando su propia elección. En [Nas51] se demuestra que todo juego no cooperativo en forma normal tiene equilibrios de Nash.

Los equilibrios de Nash en un juego no cooperativo en forma normal pueden verse como las soluciones reales de un sistema de ecuaciones e inecuaciones polinomiales dadas por polinomios multilineales (ver por ejemplo [Stu02, Chapter 6]). Para el cálculo de equilibrios de Nash se han aplicado algoritmos simbólicos de resolución de sistemas de ecuaciones e inecuaciones polinomiales sobre los números reales (ver [LM04, MM96]); sin embargo, no hay resultados significativos en cuanto a la adaptación de estos algoritmos para aprovechar las propiedades particulares de los sistemas de ecuaciones involucrados. Un estudio comparativo de distintos métodos conocidos para calcular todos los equilibrios de Nash de un juego puede encontrarse en [Dat] (ver también [HP05] para un algoritmo numérico reciente). Herramientas relacionadas con la resolución de ecuaciones polinomiales se han utilizado también para estimar la cantidad de equilibrios de Nash para un juego dado (ver, por ejemplo, [Roj97]).

En esta tesis estudiamos los equilibrios de Nash *totalmente mixtos* de un juego, es decir, aquéllos en los que cada jugador asigna una probabilidad positiva a cada una de sus estrategias puras. Para esto, consideramos el conjunto de los *cuasi-equilibrios* del juego, es decir, las soluciones complejas del sistema de ecuaciones que caracteriza los equilibrios buscados. Los juegos en los que cada cuasi-equilibrio da lugar a un equilibrio de Nash totalmente mixto tienen la máxima cantidad finita posible de tales equilibrios. En [MM97], se probó la existencia de juegos con esta propiedad, pero sin proveer una caracterización de los mismos.

Nuestro primer resultado es un algoritmo simbólico para hallar una descripción del conjunto de cuasi-equilibrios de un juego genérico con una estructura fija, tratando a los valores de las ganancias obtenidas por los jugadores como parámetros. Este

algoritmo está basado en un procedimiento simbólico descripto en [JS07] para el cálculo de resultantes multihomogéneas. El resultado siguiente es un algoritmo para caracterizar los juegos con la máxima cantidad finita de equilibrios de Nash totalmente mixtos: presentaremos un algoritmo que, a partir del *output* del algoritmo anterior, calcula un número finito de desigualdades polinomiales sobre dichas ganancias que, para juegos genéricos, son equivalentes a la existencia de la máxima cantidad finita de equilibrios de Nash totalmente mixtos. Finalmente, analizaremos juegos particulares cuyo conjunto de cuasi-equilibrios resulta finito: daremos algoritmos para verificar esta condición, para hallar una descripción del conjunto de cuasi-equilibrios y para calcular la cantidad de equilibrios de Nash totalmente mixtos del juego en cuestión. La complejidad de los algoritmos presentados en este capítulo es polinomial en la cantidad de jugadores, la cantidad de estrategias de cada jugador y la máxima cantidad finita de equilibrios de Nash totalmente mixtos que puede tener un juego con la estructura considerada.

Preliminares

0.1. Notación general

Notaremos $\mathbb{N}$ al conjunto de los números naturales, $\mathbb{N}_0$ a $\mathbb{N} \cup \{0\}$, $\mathbb{Z}$ al anillo de los números enteros, y $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ a los cuerpos de los números racionales, reales y complejos respectivamente.

Sea R un anillo. Si R es un dominio integro y $f, g \in R$, notaremos $\gcd(f, g)$ y $\operatorname{lcm}(f, g)$ al máximo común divisor y al mínimo común múltiplo entre f y g respectivamente, los cuales están bien definidos salvo por una unidad de R.

Sean $n, m \in \mathbb{N}$. Notaremos $R[x_1, \ldots, x_n]$, o simplemente $R[x]$, al anillo de polinomios en las variables $x_1, \ldots, x_n$ con coeficientes en R. Para $f \in R[x_1, \ldots, x_n]$, notaremos $\deg f$ al grado total de f y para $1 \leq i \leq n$, notaremos $\deg_{x_i} f$ al grado de f en la variable x_i. Además, si el coeficiente principal de f visto como elemento de $R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n][x_i]$ es un elemento de R, diremos que f es *cuasimónico* en la variable x_i. Finalmente, para $f \in R[x_1, \ldots, x_n, y_1, \ldots, y_m]$, notaremos $\deg_x f$ al grado de f en las variables x, es decir, visto como elemento de $R[y][x]$.

Sea K un cuerpo. Notaremos $\overline{K}$ a la clausura algebraica de K. Todos los cuerpos que consideraremos serán de característica 0; por lo tanto, de aquí en adelante omitiremos esta aclaración.

Para una matriz $A \in K^{n \times m}$, notaremos $\ker A$ a su núcleo y $\operatorname{rank} A$ a su rango.

Notaremos respectivamente $\mathbb{A}^n_{\overline{K}}$ y $\mathbb{P}^n_{\overline{K}}$ a los espacios afín y proyectivo sobre $\overline{K}$ de dimensión n. A lo largo de este trabajo consideraremos variedades algebraicas V en espacios ambiente de distinto tipo: afines, proyectivos y productos de éstos. En cualquiera de estos casos, notaremos $\dim V$ y $\deg V$ respectivamente a la dimensión y el grado de V. Para subconjuntos X de estos espacios ambientes, notaremos $\overline{X}$ a su clausura respecto a la topología Zariski (ver, por ejemplo, [Sha77] para una definición de estos conceptos). Por omisión, nos referiremos por $\mathbb{A}^n$ y $\mathbb{P}^n$ a $\mathbb{A}^n_{\mathbb{C}}$ y $\mathbb{P}^n_{\mathbb{C}}$

respectivamente.

Para subconjuntos X de $\mathbb{R}$, notaremos $\inf X$ y $\sup X$ a su ínfimo y a su supremo respectivamente cuando existan. Por último, para subconjuntos X de $\mathbb{R}^n$, notaremos $\overline{X}$ a su clausura respecto a la topología euclídea.

Para funciones $h_1, h_2 : \mathbb{N}_0^m \to \mathbb{R}$, notaremos

$$h_1(n_1, \ldots, n_m) = O(h_2(n_1, \ldots, n_m))$$

para indicar que existen $c, N \in \mathbb{N}$ tales que $|h_1(n_1, \ldots, n_m)| \leq c|h_2(n_1, \ldots, n_m)|$ para todo $(n_1, \ldots, n_m) \in \mathbb{N}^m$ con $\sum_{1 \leq i \leq m} n_i^2 \geq N$.

0.2. Aspectos algorítmicos

Un *algoritmo* es un procedimiento que, a partir de un *input*, que consiste en un conjunto finito de datos, siguiendo ciertas reglas prefijadas produce un *output*, que también consiste en un conjunto finito de datos.

Por *problema*, entenderemos una pregunta a ser contestada, generalmente dependiendo de ciertas variables. En este contexto, una *instancia* del problema es una especificación particular de todas las variables involucradas.

El nexo entre los problemas y los algoritmos está dado por la elección de un esquema de codificación de las variables que definen cada instancia del problema como un conjunto finito de datos. Una vez elegido el esquema de codificación, un algoritmo resuelve el problema para una instancia particular si la ejecución del algoritmo con el *input* correspondiente a la codificación de dicha instancia requiere un número finito de pasos y produce la respuesta correcta. Un algoritmo resuelve el problema si lo resuelve para todas las instancias posibles.

En el segundo y el tercer capítulo de esta tesis nos ocuparemos del diseño de algoritmos para resolver ciertos problemas relacionados con la resolución de ecuaciones e inecuaciones polinomiales sobre el cuerpo de los números reales. En todos los algoritmos que consideraremos, las instancias correspondientes al problema en cuestión serán codificadas como secuencias finitas de elementos en un cuerpo $K \subset \mathbb{R}$. De acuerdo al esquema de codificación preestablecido, el *tamaño* del *input*, que es la longitud de la secuencia que lo forma, se medirá en función de un vector de elementos de $\mathbb{N}_0$.

La *complejidad* de un algoritmo es una noción que se define para medir la eficiencia con la que lleva a cabo la tarea para la que fue diseñado, en función del tamaño

del *input*. En el contexto que describimos en el párrafo anterior, si en el esquema de codificación preestablecido el tamaño del *input* se mide por una función s que depende de m parámetros, diremos que la *complejidad* del algoritmo es la función $C : \mathbb{N}_0^m \to \mathbb{N}_0$ definida por

$$C(n_1, \ldots, n_m) = \max\Big\{k \in \mathbb{N}_0 \mid \text{existe un } \textit{input} \text{ de tamaño } s(n_1, \ldots, n_m) \text{ tal}$$
$$\text{que la ejecución del algoritmo requiere } k \text{ operaciones en } K\Big\}.$$

Un algoritmo *probabilístico* es un algoritmo en el que, en determinados pasos, se eligen algunos parámetros al azar dentro de un conjunto finito preestablecido, y el éxito de la ejecución depende de que dichos parámetros pertenezcan a un cierto subconjunto. En el segundo capítulo de esta tesis, los algoritmos que diseñaremos serán algoritmos probabilísticos. En todos ellos habrá una cantidad fija de pasos de elección al azar y ésta se realiza siempre en $\mathcal{Q}^n$ para algún $n \in \mathbb{N}$, siendo $\mathcal{Q}$ un subconjunto finito de $\mathbb{Q}$. El éxito de la ejecución del algoritmo dependerá de que la elección no pertenezca a la intersección de $\mathcal{Q}^n$ con una hipersuperficie de $\mathbb{A}^n$, lo cual ocurre con probabilidad tan alta como se quiera con tal que el conjunto $\mathcal{Q}$ sea suficientemente grande.

En el primer capítulo de esta tesis estudiaremos cotas inferiores de complejidad para algoritmos de resolución de sistemas de ecuaciones polinomiales sobre el cuerpo de los números reales desde un punto de vista teórico, para lo que necesitaremos más formalidad sobre los conceptos que acabamos de describir. A tal efecto, adoptaremos el modelo clásico de máquinas de Turing, el cual describimos en la Sección 0.2.1. En la Sección 0.2.2, incluimos una breve introducción a la teoría de NP-completitud, que se utiliza para clasificar problemas de acuerdo a su dificultad para resolverlos algorítmicamente. Aunque esta teoría fue llevada también a otros modelos (ver, por ejemplo, [BCSS98]), su desarrollo original se basó en el modelo de máquinas de Turing. Un estudio más amplio de los temas introducidos en las próximas dos secciones puede encontrarse, por ejemplo, en [GJ79].

0.2.1. Máquinas de Turing

Una *máquina de Turing determinística (de una cinta)* consiste de una *unidad de control de estado*, un *cabezal lector/escritor* y una *cinta* infinita formada por *casillas* numeradas sucesivamente por los enteros.

Un *algoritmo* para esta máquina se define mediante

- un conjunto finito Γ de *símbolos*, que incluye un subconjunto Σ de símbolos *de entrada* y un símbolo distinguido $b \in \Gamma \setminus \Sigma$,
- un conjunto finito Q de *estados*, que incluye un estado q_0, llamado estado *de inicio*, y dos estados q_Y y q_N, llamados estados *de finalización*,
- una *función de transición* $\delta : (Q - \{q_Y, q_N\}) \times \Gamma \to Q \times \Gamma \times \{-1, +1\}$.

Un *input* para el algoritmo es una secuencia finita formada por elementos de Σ. Dado un *input* x de longitud n, la máquina ejecuta el algoritmo como se explica a continuación.

Primeramente, los elementos de x se imprimen uno a continuación del otro en la cinta ocupando las casillas numeradas de 1 a n, y en todas las otras casillas se imprime el símbolo b. El cabezal lector/escritor se sitúa sobre la casilla 1 y la unidad de control de estado adopta el estado q_0.

Luego, la máquina procede en sucesivos pasos. En cada paso, si la unidad de control de estado se encuentra en un estado q distinto de q_Y y q_N, el cabezal lector/escritor se sitúa sobre una casilla que contiene un símbolo s y $\delta(q, s) = (q', s', \Delta)$, entonces la unidad de control de estado pasa a adoptar el estado q', el cabezal lector/escritor imprime un símbolo s' sobre la casilla que se sitúa (borrando el símbolo s) y el cabezal lector/escritor se mueve una casilla hacia el sentido de los números positivos o negativos según sea $\Delta = 1$ o $\Delta = -1$ respectivamente. Si la unidad de control de estado se encuentra en estado q_Y o q_N, la ejecución del algoritmo finaliza.

En los casos en los que corresponda, se interpreta que el algoritmo ha producido una respuesta afirmativa o negativa según la unidad de control de estado haya finalizado en estado q_Y o q_N respectivamente. Cuando el algoritmo fue diseñado para el cómputo de una función definida del conjunto de secuencias finitas de elementos de Σ al conjunto de secuencias finitas de elementos de Γ, el *output* producido por el algoritmo es la secuencia formada por los símbolos que se encuentran, al finalizar la ejecución, desde la casilla 1 en el sentido de los números positivos hasta incluir todos los símbolos distintos de b. Notemos que si el algoritmo ha finalizado su ejecución en un número finito de pasos, esta secuencia tiene, en efecto, longitud finita.

En este modelo, la complejidad de un algoritmo está dada por la función $C : \mathbb{N}_0 \to \mathbb{N}_0$, definida por

$$C(n) = \max\Big\{k \in \mathbb{N}_0 \mid \text{existe un } \textit{input } x \text{ de longitud } n \text{ tal}$$

$$\text{que la ejecución del algoritmo requiere } k \text{ pasos}\Big\}.$$

La complejidad en este moedelo considera el costo de acceder al símbolo que se encuentra en cada una de las casillas de la cinta, a diferencia de lo que ocurre en la descripción más informal dada al comienzo de la Sección 0.2, en la que todos los resultados de cómputos anteriores se consideran disponibles en todo momento.

0.2.2. Teoría de NP-completitud

Un *problema de decisión* Π es un problema cuya respuesta es "sí" o "no". El problema Π queda determinado definiendo el conjunto de instancias D_Π y el conjunto $Y_\Pi \subset D_\Pi$ de instancias para las cuales la respuesta es afirmativa.

La *clase de problemas P* es la clase de los problemas de decisión Π para los cuales existen un algoritmo para una máquina de Turing determinística y un polinomio $p : \mathbb{N} \to \mathbb{N}$ tales que el algoritmo resuelve el problema y su complejidad C verifica $C(n) \leq p(n)$ para todo $n \in \mathbb{N}_0$.

La *clase de problemas NP* es la clase de los problemas de decisión Π para los cuales existen un algoritmo para una máquina de Turing determinística y un polinomio $p : \mathbb{N} \to \mathbb{N}$ que verifican la siguiente propiedad:

- para toda instancia $I \in Y_\Pi$ codificada mediante una secuencia x formada por n símbolos de entrada, existe un secuencia finita x' formada por n' símbolos que si se imprimen en la cinta ocupando las casillas numeradas de $-n'$ a -1 luego de que se imprimen en la cinta los elementos de x, la ejecución del algoritmo produce la respuesta "sí" y requiere una cantidad de pasos acotada por $p(n)$.
- para toda instancia $I \in D_\Pi \setminus Y_\Pi$ codificada mediante una secuencia finita x de símbolos de entrada, no existe ninguna secuencia finita x' formada por n' símbolos que si se imprimen en la cinta ocupando las casillas numeradas de $-n'$ a -1 luego de que se imprimen en la cinta los elementos de x, la ejecución del algoritmo finaliza en una cantidad finita de pasos produciendo la respuesta "sí".

Informalmente, la clase de problemas NP es la clase de los problemas de decisión Π tales que las instancias $I \in Y_\Pi$ pueden ser reconocidas en una cantidad de pasos acotada polinomialmente en función de la longitud de la secuencia de símbolos que codifica a I, a partir de un conjunto de datos que permitan corroborar que la respuesta correcta al problema para la instancia I es "sí".

Es claro que la clase de problemas P está incluida en la clase de problemas NP (tomando, por ejemplo, la secuencia finita x' vacía en la definición anterior). Un problema abierto ampliamente difundido consiste en decidir si estas clases son iguales.

Una *reducción polinomial* de un problema de decisión Π' a un problema de decisión Π es un algoritmo para una máquina de Turing determinística tal que existe un polinomio $p : \mathbb{N} \to \mathbb{N}$ de manera que se verifica la siguiente propiedad: el algoritmo calcula una función que, para cada *input* formado por n símbolos que codifican una instancia $I' \in D_{\Pi'}$, el *output* es una secuencia finita de símbolos que codifica una instancia $I \in D_\Pi$ de manera que $I \in Y_\Pi$ si y solo si $I' \in Y_{\Pi'}$, y la ejecución del algoritmo requiere una cantidad de pasos acotada por $p(n)$. Un *problema NP-completo* es un problema de decisión Π en la clase NP tal que todo problema de decisión Π' en la clase NP se reduce polinomialmente a Π.

Estas definiciones implican que si Π' se reduce polinomialmente a Π y $\Pi \in$ P, entonces $\Pi' \in$ P; luego, si existe un problema NP-completo Π tal que $\Pi \in$ P, entonces P = NP, de donde surge la importancia de estudiar los problemas NP completos.

Un *problema de búsqueda* Π es un problema cuya respuesta es un conjunto de objetos llamados *soluciones*. El problema Π queda determinado definiendo el conjunto de instancias D_Π y el conjunto de soluciones $S_\Pi(I)$ para cada instancia I. Vale la pena aclarar que un algoritmo resuelve el problema de búsqueda Π para una instancia particular I si, a partir de una secuencia finita de símbolos que codifica a I, el *output* es una secuencia finita de símbolos que codifica algún elemento de $S_\Pi(I)$ o la respuesta "no" si $S_\Pi(I)$ es vacío. Todo problema de decisión es un problema de búsqueda, definiendo $S_\Pi(I) = \{\text{"sí"}\}$ para $I \in Y_\Pi$ y $S_\Pi(I) = \{\text{"no"}\}$ para $I \in D_\Pi \setminus Y_\Pi$.

La noción de reducción polinomial entre problemas de búsqueda exige un cierto desarrollo formal que excede lo necesario para la comprensión de los resultados de esta tesis. En forma algo imprecisa, podemos decir que una *reducción polinomial* de un problema de búsqueda Π' a un problema de búsqueda Π es un algoritmo para una máquina de Turing determinística tal que existe un polinomio $p : \mathbb{N} \to \mathbb{N}$ de manera que se verifica la siguiente propiedad: para cada secuencia finita formada por n símbolos que codifica una instancia I de Π', el algoritmo resuelve el problema Π' para I utilizando una subrutina que resuelve el problema Π, y la ejecución del algoritmo requiere una cantidad de pasos acotada por $p(n)$, contando cada ejecución de la subrutina como un único paso.

Un *problema NP-hard* es un problema de búsqueda Π tal que existe un problema de decisión NP-completo Π' que se reduce polinomialmente a Π. Al igual que antes, si existe un problema NP-*hard* Π tal que $\Pi \in$ P, entonces P = NP.

Dos ejemplos clásicos de problemas NP-completos son los problemas SAT y 3-SAT ([Coo71], [Kar72]). En lo que sigue damos la formulación de estos problemas, para lo cual introducimos en primer lugar algunos conceptos.

Una *fórmula bien formada del cálculo proposicional*, o simplemente, una *fórmula proposicional*, es una fórmula obtenida a partir de *símbolos de predicado* $P_1, \ldots, P_n$, utilizando los *conectivos proposicionales* $\wedge, \vee$ y $\neg$. Un *literal* es una fórmula proposicional de la forma P o $\neg P$, donde P es un símbolo de predicado. Una *interpretación* de los símbolos de predicado $P_1, \ldots, P_n$ es una función $I : \{P_1, \ldots, P_n\} \to \{V, F\}$, es decir, una asignación a cada uno de estos símbolos de predicado de un valor de verdad "verdadero" o "falso" simbolizado por V o F respectivamente. Una interpretacion de los símbolos de predicado $P_1, \ldots, P_n$ *satisface* a una fórmula proposicional W obtenida a partir de ellos si el valor de verdad que la interpretación le hace corresponder a W es "verdadero". Una fórmula proposicional W es *satisfacible* si existe una interpretación de los símbolos de predicado a partir de los cuales W fue obtenida que satisface a W.

El problema *SAT* es el siguiente problema de decisión: dada una fórmula proposicional W obtenida a partir de símbolos de predicado $P_1, \ldots, P_n$ de la forma

$$W = \big(L_{11} \vee \cdots \vee L_{1l_1}\big) \wedge \cdots \wedge \big(L_{m1} \vee \cdots \vee L_{ml_m}\big), \tag{1}$$

donde para $1 \leq i \leq m, 1 \leq j \leq l_i$, L_{ij} es o bien el literal $P_{k_{ij}}$ o bien el literal $\neg P_{k_{ij}}$ para algún $1 \leq k_{ij} \leq n$, decidir si W es satisfacible.

El problema *3-SAT* es el problema de decisión SAT restringiendo el conjunto de instancias a las fórmulas proposicionales W como en (1) que verifican $l_i = 3$ para $1 \leq i \leq m$.

Como consecuencia de la NP-completitud de los problemas SAT y 3-SAT, resulta que los problemas de búsqueda que consisten en encontrar para cada instancia W de SAT o de 3-SAT una interpretación de los símbolos de predicado involucrados en la escritura de W que satisfaga a W (o decidir que no existe tal interpretación), son NP-*hard*.

0.2.3. Codificación de polinomios

Sea R un anillo. Todo polinomio en $R[x_1, \ldots, x_n]$ queda definido conociendo su grado y los coeficientes correspondientes a monomios de grado menor o igual a él. Esta es la manera usual en la que se representan polinomios, pero no es la única forma de hacerlo. Actualmente coexisten varios esquemas de codificación de polinomios muy utilizados en álgebra computacional y cada una de ellos presenta ventajas y desventajas sobre los demás. A continuación describimos los esquemas de codificación que utilizaremos en esta tesis.

Codificación densa: Es la codificación usual recién descripta. Consiste en el grado d del polinomio y la lista de todos los coeficientes correspondientes a monomios de grado menor o igual a d en algún orden prefijado.

Codificación rala: Consiste en la lista de todos los coeficientes no nulos del polinomio junto con el vector de grados en cada variable del monomio al que acompaña dicho coeficiente.

Codificación por straight-line programs*:* Consiste en una lista de instrucciones que permiten evaluar al polinomio en cualquier elemento de R^n. Cada instrucción de la lista es una suma, resta o multiplicación entre variables, elementos de R o el resultado de instrucciones anteriores de la lista. Cuando R es un cuerpo, la división de una variable, un elemento de R o el resultado de una instrucción anterior por un elemento de R también es admitida. La *longitud* del *straight-line program* es la cantidad de instrucciones que lo compone. En adelante escribiremos *slp* como abreviatura de *straight-line program*.

En esta tesis, utilizaremos frecuentemente los siguientes algoritmos para polinomios codificados por *slps*:

[BCS97, Lema 21.25]: A partir de un *slp* de longitud L que codifica un polinomio $f \in R[x_1]$ de grado acotado por d, calcula con complejidad $O(d^2L)$ un *slp* de longitud del mismo orden que codifica simultáneamente a todos los coeficientes de f.

[Str73]: A partir de un *slp* de longitud L que codifica simultáneamente polinomios $f_1, f_2 \in R[x_1]$ con R dominio tales que f_2 divide a f_1 en $R_0[x_1]$ donde R_0 es el cuerpo de fracciones de R, de una cota d para el grado del cociente f_1/f_2, y de un elemento $s \in R$ tal que $f_2(s) \neq 0$, calcula con complejidad $O(d^2(d+L))$ un *slp* con coeficientes en R_0 de longitud del mismo orden que codifica el cociente f_1/f_2. Si $f_2(s)$ es una unidad de R, entonces el cociente $f_1/f_2 \in R[x_1]$ y el *slp* obtenido tiene coeficientes en R.

[BS83]: A partir de un *slp* de longitud L que codifica un polinomio $f \in R[x_1, \ldots, x_n]$, calcula con complejidad $O(L)$ un *slp* de longitud del mismo orden que codifica simultáneamente a f y a todas sus derivadas parciales.

0.3. Nociones geométricas

0.3.1. Resolucion geométrica de variedades cero-dimensionales

Una manera de representar variedades cero-dimensionales muy utilizada actualmente en álgebra computacional es por medio de *resoluciones geométricas*. Esta noción fue introducida en los trabajos de Kronecker y König ([Kro82], [Koe03]) en los últimos años del Siglo XIX y actualmente figura en la literatura también bajo el nombre de *representación racional univariada*. Un resumen de la historia del uso de esta representación en el área puede encontrarse en [GLS01].

Una resolución geométrica de una variedad cero-dimensional describe a la misma mediante una parametrización o bien polinomial o bien racional, en la que el parámetro toma valores en el conjunto de raíces de un polinomio univariado. Más precisamente, sea K un cuerpo y $V \subset \mathbb{A}^n_{\overline{K}}$ una variedad no vacía formada por p puntos. El conjunto $\{q, w_1, \ldots, w_n\} \subset K[U]$ es una *resolución geométrica* (polinomial) de V si $\deg q = p$, $\deg w_i < p$ para $1 \leq i \leq n$ y

$$V = \Big\{ \big(w_1(u), \ldots, w_n(u)\big) \mid u \in \overline{K},\ q(u) = 0 \Big\}.$$

A su vez, el conjunto $\{q, q_0, w_1, \ldots, w_n\} \subset K[U]$ es una *resolución geométrica* (racional) de V si $\deg q = p$, $\deg q_0 < p$, $\deg w_i < p$ para $1 \leq i \leq n$, $\gcd(q, q_0) = 1$ y

$$V = \Big\{ \Big(\frac{w_1(u)}{q_0(u)}, \ldots, \frac{w_n(u)}{q_0(u)}\Big) \mid u \in \overline{K},\ q(u) = 0 \Big\}.$$

La condición $\gcd(q, q_0) = 1$ asegura que ninguno de los denominadores en la expresión anterior resulta nulo y, a su vez, que es posible obtener un inverso $r_0 \in K[U]$ para q_0 módulo q. Luego llamando $\tilde{w}_i$ al polinomio $w_i r_0$ módulo q para $1 \leq i \leq n$, obtenemos que $V = \big\{(\tilde{w}_1(u), \ldots, \tilde{w}_n(u)) \mid u \in \overline{K},\ q(u) = 0\big\}$. Por lo tanto, es posible pasar de una representación racional a una polinomial con un costo computacional bajo que, en nuestro caso, no incrementa la complejidad de los algoritmos que presentaremos. Esto nos permitirá hacer uso indistinto de ambas representaciones una vez calculada una de ellas.

La práctica usual para obtener una resolución geométrica de una variedad 0-dimensional es considerar una forma lineal que tome distintos valores sobre los puntos de la variedad V, para luego tomar q como el polinomio que tiene a dichos valores por raíces. En el caso de representaciones polinomiales, la resolución geométrica se completa con los polinomios que interpolan los valores de las coordenadas de los puntos de V en los ceros de q. En el caso de representaciones racionales, esta construcción se adapta convenientemente.

La noción de resolución geométrica puede adaptarse fácilmente al caso de variedades proyectivas cero-dimensionales y, más aún, al caso de variedades multiproyectivas cero-dimensionales. Sean $n_1, \ldots, n_r \in \mathbb{N}$ y $V \subset \mathbb{P}^{n_1}_{\overline{K}} \times \cdots \times \mathbb{P}^{n_r}_{\overline{K}}$ una variedad no vacía formada por p puntos. El conjunto $\{q, w_{10}, \ldots, w_{1n_1}, \ldots, w_{r0}, \ldots, w_{rn_r}\} \subset K[U]$ es una *resolución geométrica* de V si $\deg q = p$, $\deg w_{ij} < p$ para $1 \leq i \leq r, 0 \leq j \leq n_i$, los polinomios $w_{i0}, \ldots, w_{in_i}$ no se anulan simultáneamente en ninguna raíz en $\overline{K}$ de q para $1 \leq i \leq r$ y

$$V = \Big\{\big((w_{10}(u) : \cdots : w_{1n_1}(u)), \ldots, (w_{r0}(u) : \cdots : w_{rn_r}(u))\big) \mid u \in \overline{K},\ q(u) = 0\Big\}.$$

0.3.2. Teorema de Bézout multihomogéneo

Sea K un cuerpo y sean $n_1, \ldots, n_r \in \mathbb{N}$. Para $1 \leq i \leq r$ llamemos x_i al grupo de variables $x_{i0}, \ldots, x_{in_i}$. Un polinomio $f \in K[x_1, \ldots, x_r]$ es *multihomogéneo* si es homogéneo en las variables de cada grupo x_i para $1 \leq i \leq r$ y, en tal caso, su *multigrado* es el vector $(\deg_{x_1} f, \ldots, \deg_{x_r} f) \in \mathbb{N}_0^r$.

Sean $n = \sum_{i=1}^r n_i$ y $f_1, \ldots, f_n \in K[x_1, \ldots, x_r]$ polinomios multihomogéneos con f_i de multigrado $d_i := (d_{i1}, \ldots, d_{ir})$ para $1 \leq i \leq n$. El Teorema de Bézout Multihomogéneo, proveniente de la teoría de intersección de divisores, establece que el grado de la variedad definida en $\mathbb{P}^{n_1}_{\overline{K}} \times \cdots \times \mathbb{P}^{n_r}_{\overline{K}}$ por $f_1, \ldots, f_n$ está acotado por

$$\mathrm{Bez}_{n_1,\ldots,n_r}(d_1, \ldots, d_n) := \sum_{(j_1,\ldots,j_n)\in\mathfrak{J}} \Big(\prod_{1\leq i\leq n} d_{ij_i}\Big), \tag{2}$$

donde

$$\mathfrak{J} := \Big\{(j_1, \ldots, j_n) \in \{1, \ldots, r\}^n \mid \#\{k \mid j_k = i\} = n_i \text{ para } 1 \leq i \leq r\Big\}$$

siempre que $\mathrm{Bez}_{n_1,\ldots,n_r}(d_1, \ldots, d_n)$ sea positivo (ver [Sha77, Chapter 4] y [Hei83]; para demostraciones alternativas utilizando técnicas de deformación ver [MSW95],

[McL99], [HJSS05]). Notemos que este resultado puede ser visto también como un caso particular del Teorema de Bernstein sobre el número de raíces comunes de sistemas ralos (ver [Ber75]).

El número $\mathrm{Bez}_{n_1,\dots,n_r}(d_1,\dots,d_n)$ es llamado el *número de Bézout* del sistema polinomial genérico con la estructura de multihomogeneidad considerada. Para $k_1,\dots,k_t \in \mathbb{N}_0$ con $\sum_{1\leq i\leq t} k_i = n$, notaremos $\mathrm{Bez}_{n_1,\dots,n_r}(d_1,k_1;\dots;d_t,k_t)$ al número de Bézout de un sistema multihomogéneo con k_i polinomios de multigrado d_i para cada $1 \leq i \leq t$.

0.4. Otras herramientas

Varias construcciones que realizaremos en este trabajo están basadas en utilizar convenientemente las propiedades que satisfacen las matrices de Cauchy y los polinomios de Tchebychev de primer tipo, a los cuales nos referiremos en adelante simplemente por polinomios de Tchebychev. Incluimos a continuación breves resúmenes de estas propiedades.

0.4.1. Matrices de Cauchy

Una *matriz de Cauchy* en $\mathbb{Q}^{m_1\times m_2}$ es una matriz A de la forma

$$A = \begin{pmatrix} \frac{1}{\alpha_1-\beta_1} & \cdots & \frac{1}{\alpha_1-\beta_{m_2}} \\ \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{m_1}-\beta_1} & \cdots & \frac{1}{\alpha_{m_1}-\beta_{m_2}} \end{pmatrix} \tag{3}$$

con $\alpha_1,\dots,\alpha_{m_1},\beta_1,\dots,\beta_{m_2} \in \mathbb{Q}$, $\alpha_i \neq \beta_j$ para todos $1 \leq i \leq m_1$ y $1 \leq j \leq m_2$.

Si A es una matriz cuadrada de Cauchy como en (3) con $m = m_1 = m_2$, entonces

$$\det(A) = \frac{\big(\prod_{1\leq i_1\leq m}\prod_{i_1<i_2\leq m}(\alpha_{i_1}-\alpha_{i_2})\big)\big(\prod_{1\leq j_1\leq m}\prod_{j_1<j_2\leq m}(\beta_{j_2}-\beta_{j_1})\big)}{\prod_{1\leq i\leq m}\prod_{1\leq j\leq m}(\alpha_i-\beta_j)}.$$

A partir de esta fórmula, podemos ver que para toda matriz de Cauchy A como en (3), si $\alpha_{i_1} \neq \alpha_{i_2}$ y $\beta_{j_1} \neq \beta_{j_2}$ para todos $1 \leq i_1 < i_2 \leq m_1$ y $1 \leq j_1 < j_2 \leq m_2$, la matriz A tiene rango $\min\{m_1, m_2\}$.

Podemos observar además que toda submatriz de una matriz de Cauchy es a su vez una matriz de Cauchy.

0.4.2. Polinomios de Tchebychev

Sea x una variable. Para $n \in \mathbb{N}_0$, el n-ésimo polinomio de Tchebychev $T_n \in \mathbb{Z}[x]$ es el polinomio que se obtiene siguiendo la siguiente definición recursiva:

- $T_0 = 1$,
- $T_1 = x$,
- $T_n = 2xT_{n-1} - T_{n-2}$ para $n \geq 2$.

Inductivamente, se puede ver que T_n es un polinomio de grado n para $n \in \mathbb{N}_0$, que su coeficiente principal es 2^{n-1} si $n \geq 1$ y además, que para todo $x \in [-1, 1]$,

$$T_n(x) = \cos(n \arc\cos(x)).$$

(ver, por ejemplo, [KC91, Section 6.1]). Como consecuencia de esta identidad tenemos que las raíces de T_n son los n números reales en el intervalo $(-1, 1)$ de la forma $\cos(t\pi/2n)$ con t entero impar entre 1 y $2n - 1$ inclusive, todas con multiplicidad 1, y que las raíces de T_n' son los $n - 1$ números reales en el intervalo $(-1, 1)$ de la forma $\cos(t\pi/2n)$ con t entero par entre 2 y $2n - 2$ inclusive. La evaluación de T_n en cualquier raíz de T_n' da por resultado ± 1, de donde se deduce que para n par, $T_n(x) \geq -1$ para todo $x \in \mathbb{R}$.

Notemos además que la definición recursiva de los polinomios de Tchebychev brinda una manera de calcular para todo $n \in \mathbb{N}$, un *slp* de longitud $O(n)$ que codifica a T_n.

Capítulo 1

Cotas inferiores de complejidad

1.1. Introducción al problema

Uno de los problemas principales en geometría algebraica real consiste en decidir si un sistema de ecuaciones polinomiales con coeficientes reales en n variables tiene una solución en $\mathbb{R}^n$. Para analizar este problema desde el punto de vista de la teoría de NP-completitud en el modelo de máquinas de Turing, debemos restringirnos al estudio del mismo en el caso de polinomios con coeficientes en un subanillo de $\mathbb{R}$ cuyos elementos sea posible describir por medio de una secuencia finita de símbolos. Nos enfocamos entonces en el problema de decidir si un sistema de ecuaciones polinomiales con coeficientes enteros en n variables tiene una solución en $\mathbb{R}^n$, ya que cualquier cota inferior de complejidad para la resolución algorítmica de este problema implica la misma cota inferior si se considera otro subanillo de $\mathbb{R}$ que contenga al de los números enteros. Es sabido que este problema es NP-*hard*; de hecho, existe una reducción polinomial clásica del problema NP-completo 3-SAT que describimos a continuación.

Dada la instancia W de 3-SAT

$$W = \big(L_{11} \vee L_{12} \vee L_{13}\big) \wedge \cdots \wedge \big(L_{m1} \vee L_{m2} \vee L_{m3}\big), \tag{1.1}$$

donde para $1 \leq i \leq m, 1 \leq j \leq 3$, L_{ij} es o bien el literal $P_{k_{ij}}$ o bien el literal $\neg P_{k_{ij}}$

para algún $1 \leq k_{ij} \leq n$, consideremos el sistema de ecuaciones

$$\begin{cases} x_1^2 - 1 & = & 0, \\ & \vdots & \\ x_n^2 - 1 & = & 0, \\ l_{11}(x_{k_{11}})l_{12}(x_{k_{12}})l_{13}(x_{k_{13}}) & = & 0, \\ & \vdots & \\ l_{m1}(x_{k_{m1}})l_{m2}(x_{k_{m2}})l_{m3}(x_{k_{m3}}) & = & 0, \end{cases}$$

donde para $1 \leq i \leq m, 1 \leq j \leq 3$, $l_{ij}(x_{k_{ij}}) = x_{k_{ij}} - 1$ si $L_{ij} = P_{k_{ij}}$ y $l_{ij}(x_{k_{ij}}) = x_{k_{ij}} + 1$ si $L_{ij} = \neg P_{k_{ij}}$. Este sistema tiene una solución en $\mathbb{R}^n$ si y solo si la fórmula W es satisfacible, ya que cada solución $(x_1, \ldots, x_n) \in \mathbb{R}^n$ del mismo se corresponde con una interpretación I de los símbolos de predicado $P_1, \ldots, P_n$ que satisface a W del siguiente modo: para $1 \leq k \leq n$, $I(P_k) = V$ si $x_k = 1$ e $I(P_k) = F$ si $x_k = -1$. Como para cada instancia W de 3-SAT, la codificación del sistema de ecuaciones asociado, ya sea densa, rala o por *slp*, puede calcularse en una cantidad de pasos polinomial en el tamaño de W, se obtiene que el problema de decidir si un sistema de ecuaciones polinomiales con coeficientes enteros tiene una solución real es NP-*hard* para cualquiera de estas codificaciones.

A su vez, el problema de decidir si un sistema de ecuaciones polinomiales con coeficientes enteros tiene una solución en $\mathbb{R}^n$ es equivalente al de decidir si una única ecuación polinomial con coeficientes enteros tiene una solución en $\mathbb{R}^n$, ya que el sistema de ecuaciones $f_1 = \cdots = f_m = 0$ admite una solución en $\mathbb{R}^n$ si y solo si la ecuación $f_1^2 + \cdots + f_m^2 = 0$ admite una solución en $\mathbb{R}^n$. Entonces, ante la probable imposibilidad de encontrar un algoritmo de complejidad polinomial para decidir si una ecuación polinomial con coeficientes enteros tiene una solución en $\mathbb{R}^n$, en adelante nos enfocamos en el estudio de este problema restringiendo el conjunto de instancias al conjunto de polinomios univariados.

Para la codificación densa, es sabido que es posible resolver este problema con complejidad polinomial, por ejemplo mediante el estudio de *secuencias de Sturm* (ver [BPR03, Chapter 2]). Para la codificación rala, no se conocen resultados al respecto. Para la codificación por *slp*, Bürgisser probó que el problema es NP-*hard* (esta demostración no fue publicada pero un bosquejo de la misma puede encontrarse en [Roj00]). La idea de su demostración consiste en componer el polinomio en cuestión con una transformación de Möbius (u homografía) que manda el eje real en la circunferencia unitaria, para luego utilizar de manera apropiada un resultado en [Pla77]

que establece que el problema de decidir si un polinomio univariado con coeficientes enteros codificado de manera rala tiene una raíz compleja de módulo 1 es NP-*hard*. Otra demostración del mismo resultado fue obtenida de manera independiente en [RGK02, Theorem 5.10].

En este capítulo, damos una nueva demostración de que el problema de decidir si un polinomio univariado con coeficientes enteros codificado por un *slp* tiene una raíz real es NP-*hard*. Nuestra demostración se basa en adaptar directamente al contexto real la idea de la reducción polinomial del problema 3-SAT dada en [Pla77], utilizando convenientemente propiedades de los polinomios de Tchebychev. A tal efecto, primeramente definimos una función sobreyectiva I_M del conjunto de raíces del M-ésimo polinomio de Tchebychev T_M para un $M \in \mathbb{N}$ apropiado al conjunto de interpretaciones de los símbolos de predicado $P_1, \ldots, P_n$. Luego exhibimos una forma de calcular algorítmicamente para cada instancia W de 3-SAT obtenida a partir de los símbolos de predicado $P_1, \ldots, P_n$ y en una cantidad de pasos polinomial en el tamaño de W, un polinomio F con la siguiente propiedad: el conjunto de raíces reales de F está contenido en el conjunto de raíces de T_M y, además, para cada raíz r de T_M, r es raíz de F si y solo si $I_M(r)$ satisface a W, con lo cual F tiene una raíz real si y solo si W es satisfacible.

Una consecuencia de nuestra construcción es que permite saber a priori que las posibles raíces reales del polinomio calculado son raíces de un polinomio de Tchebychev. Esto nos lleva luego a obtener un nuevo resultado: el problema de aproximar las raíces reales de un polinomio univariado con coeficientes enteros codificado por un *slp* es también NP-*hard*.

Este capítulo está organizado de la siguiente manera. En la Sección 1.2 damos nuestra demostración de que el problema de decidir la existencia de raíces reales en polinomios univariados con coeficientes enteros codificados por *slps* es NP-*hard*. En la Sección 1.3, retomamos la construcción hecha en la sección anterior para probar que el problema de aproximar las raíces reales en polinomios univariados con coeficientes enteros codificados por *slps* es también NP-*hard*.

1.2. Existencia de raíces reales

En este capítulo notaremos, para $j \in \mathbb{N}$, q_j al j-ésimo número primo impar. Como explicamos en la Sección 1.1, el primer paso en nuestra demostración es definir, para $M \in \mathbb{N}$, una función que asigna a cada raíz del M-ésimo polinomio de Tcheby-

chev T_M, una interpretación de determinados símbolos de predicado. A tal efecto, introducimos las siguientes definiciones.

Definición 1.1 *Para $M \in \mathbb{N}$, notamos $d(M)$ al conjunto de los números impares entre 1 y $2M-1$ inclusive y r_M a la función biyectiva*

$$r_M : d(M) \to \{\textit{raíces de } T_M\}, \quad r_M(t) = \cos\Big(\frac{t\pi}{2M}\Big).$$

Para cada r raíz de T_M, definimos la interpretación $I_M(r)$ de los símbolos de predicado $\{P_j \mid q_j \text{ divide a } M\}$ de la siguiente manera:

$$I_M(r)(P_j) = V \text{ si y solo si } r \text{ es una raíz de } T_{M/q_j}.$$

Para cada J interpretación de $\{P_j \mid q_j \text{ divide a } M\}$, notamos $\alpha(J) = \prod_{\{j \,|\, J(P_j)=V\}} q_j$.

Observación 1.2 *Notemos que para todo $t \in d(M)$,*

$$I_M(r_M(t))(P_j) = V \text{ si y solo si } q_j \text{ divide a } t.$$

Además, para cada interpretación J de $\{P_j \,|\, q_j \text{ divide a } M\}$ hay al menos una raíz r de T_M tal que $I_M(r) = J$, por ejemplo, $r = r_M(\alpha(J))$. Más aún, si M es libre de cuadrados entonces $\{t \in d(M) \mid I_M(r_M(t)) = J\} = \{t \in d(M) \mid \gcd(t, M) = \alpha(J)\}$. Luego, la función I_M definida del conjunto de raíces de T_M al conjunto de interpretaciones de $\{P_j \,|\, q_j \text{ divide a } M\}$ es sobreyectiva.

Para comenzar a relacionar fórmulas proposicionales con polinomios univariados y sus raíces reales, consideremos la siguiente definición.

Definición 1.3 *Para una fórmula proposicional W, decimos que $M \in \mathbb{N}$ es* apropiado *si M es libre de cuadrados y, para todo $j \in \mathbb{N}$, si la escritura de W involucra el símbolo de predicado P_j, entonces q_j divide a M. En tal caso, definimos $\mathrm{PolyS}_M(W) \in \mathbb{R}[x]$ como el polinomio mónico que tiene por raíces simples a las raíces r de T_M tales que $I_M(r)$ satisface a W.*

Observación 1.4 *Dadas fórmulas proposicionales W y W', siempre que M sea apropiado, vale que:*

1. $\mathrm{PolyS}_M(\neg W) = \frac{T_M}{2^{M-1}\mathrm{PolyS}_M(W)}$,

2. $\mathrm{PolyS}_M(W \wedge W') = \gcd(\mathrm{PolyS}_M(W), \mathrm{PolyS}_M(W'))$,

3. $\mathrm{PolyS}_M(W \vee W') = \mathrm{lcm}(\mathrm{PolyS}_M(W), \mathrm{PolyS}_M(W'))$,

4. $\mathrm{PolyS}_M(W) = \mathrm{PolyS}_M(W')$ *si y solo si* W *y* W' *son equivalentes (es decir, toda interpretación de los símbolos de predicado satisface a una si y solo si satisface a la otra).*

El siguiente lema provee una manera de calcular $\mathrm{PolyS}_M(W)$ en algunos casos particulares.

Lema 1.5 *Siempre que* M *sea apropiado, vale que:*

1. $\mathrm{PolyS}_M(P_{i_1} \wedge \cdots \wedge P_{i_l}) = \frac{T_{M/(q_{i_1} \ldots q_{i_l})}}{2^{(M/(q_{i_1} \ldots q_{i_l}))-1}}$,

2. $\mathrm{PolyS}_M(\neg P_{i_1} \vee \neg P_{i_2} \vee \neg P_{i_3}) = \frac{T_M}{2^{M-1}\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2} \wedge P_{i_3})}$,

3. $\mathrm{PolyS}_M(P_{i_1} \vee \neg P_{i_2} \vee \neg P_{i_3}) = \frac{T_M \mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2} \wedge P_{i_3})}{2^{M-1}\mathrm{PolyS}_M(P_{i_2} \wedge P_{i_3})}$,

4. $\mathrm{PolyS}_M(P_{i_1} \vee P_{i_2} \vee \neg P_{i_3}) = \frac{T_M \mathrm{PolyS}_M(P_{i_1} \wedge P_{i_3})\mathrm{PolyS}_M(P_{i_2} \wedge P_{i_3})}{2^{M-1}\mathrm{PolyS}_M(P_{i_3})\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2} \wedge P_{i_3})}$,

5. $\mathrm{PolyS}_M(P_{i_1} \vee P_{i_2} \vee P_{i_3}) = \frac{\mathrm{PolyS}_M(P_{i_1})\mathrm{PolyS}_M(P_{i_2})\mathrm{PolyS}_M(P_{i_3})\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2} \wedge P_{i_3})}{\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2})\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_3})\mathrm{PolyS}_M(P_{i_2} \wedge P_{i_3})}$.

Demostración: En cada ítem, ambos miembros de la igualdad son polinomios mónicos. Para probar el primer ítem, notemos que el conjunto de raíces de $T_{M/(q_{i_1} \ldots q_{i_l})}$ es

$$\left\{ r_{M/(q_{i_1} \ldots q_{i_l})}(t) \mid t \in d(M/(q_{i_1} \ldots q_{i_l})) \right\} = \left\{ r_M(t') \mid t' \in d(M),\ q_{i_1} \ldots q_{i_l} | t' \right\},$$

que es el conjunto de raíces de $\mathrm{PolyS}_M(P_{i_1} \wedge \cdots \wedge P_{i_l})$. En los demás ítems puede verse fácilmente que ambos miembros de la igualdad tienen las mismas raíces, todas simples. □

Dado que toda fórmula proproposicional W es equivalente a una conjunción de disyunciones de literales, podemos notar que como consecuencia de la Observación 1.4 y del primer ítem del Lema 1.5, para todo M apropiado, $\mathrm{PolyS}_M(W) \in \mathbb{Q}[x]$.

Introducimos a continuación una familia de polinomios análoga a la de los polinomios ciclotómicos que nos permitirá describir más precisamente los polinomios $\mathrm{PolyS}_M(W)$.

Definición 1.6 *Para $M \in \mathbb{N}$, definimos $\hat{C}_M$ como el polinomio*

$$\hat{C}_M(x) = \prod_{\substack{t \in d(M) \\ \gcd(t:M)=1}} \big(x - r_M(t)\big).$$

Podemos observar que $\deg \hat{C}_M = \phi(2M)$, donde ϕ es la función de Euler, y que el conjunto de raíces de este polinomio es simétrico con respecto al 0. Además, para $M' \in \mathbb{N}$, si $M \neq M'$, entonces $\hat{C}_M(x)$ y $\hat{C}_{M'}(x)$ son polinomios coprimos.

Veamos que, utilizando los polinomios recién definidos, para una fórmula proposicional W y M apropiado, podemos descomponer el polinomio $\mathrm{PolyS}_M(W)$ como producto de polinomios agrupando en cada factor todas las raíces que tienen asociada la misma interpretación de los símbolos de predicado.

Lema 1.7 *Sea W una fórmula proposicional, sea M apropiado y sean $J_1, \ldots, J_k$ todas las interpretaciones de los símbolos de predicado involucrados en la escritura de W que satisfacen a W. Entonces* $\mathrm{PolyS}_M(W) = \prod_{1 \leq h \leq k} \hat{C}_{M/\alpha(J_h)}$.

Demostración: Como ambos polinomios son mónicos y libres de cuadrados, es suficiente con probar que tienen las mismas raíces. Para $1 \leq h \leq k$, el conjunto de raíces de $\hat{C}_{M/\alpha(J_h)}$ es

$$\Big\{ r_{M/\alpha(J_h)}(t) \mid t \in d(M/\alpha(J_h)),\ \gcd(t, M/\alpha(J_h)) = 1 \Big\} =$$

$$= \Big\{ r_M(t') \mid t' \in d(M),\ \gcd(t', M) = \alpha(J_h) \Big\} =$$

$$= \Big\{ r_M(t') \mid t' \in d(M),\ I_M(r_M(t')) = J_h \Big\};$$

luego la unión de estos conjuntos es el conjunto de raíces de $\mathrm{PolyS}_M(W)$. ▫

A continuación probaremos dos lemas auxiliares que nos permitirán calcular el polinomio $\mathrm{PolyS}_M(W)$ en determinadas situaciones.

Lema 1.8 *Sean $q, M \in \mathbb{N}$. Si q es un primo impar que no divide a M, entonces*

$$\hat{C}_{qM}\hat{C}_M = \frac{\hat{C}_M \circ T_q}{2^{(q-1)\deg \hat{C}_M}}.$$

Si M es impar, entonces

$$\hat{C}_{2M} = \frac{\hat{C}_M \circ T_2}{2^{\deg \hat{C}_M}}.$$

Demostración: Comencemos probando la primera afirmación. Ambos polinomios son mónicos y de grado $q\phi(2M)$. Como el primer polinomio es libre de cuadrados, es suficiente con probar que cada una de sus raíces es una raíz del segundo polinomio. Si r es una raíz de $\hat{C}_{qM}$, entonces $r = \cos(\frac{t\pi}{2qM})$ para algún $t \in d(qM)$ tal que $\gcd(t, qM) = 1$. Si $t = t' + s2M$ con $t' \in d(M)$ y $s \in \mathbb{N}_0$, entonces $\gcd(t', M) = 1$ y, por lo tanto,

$$T_q(r) = \cos\Big(q \arccos\Big(\cos\Big(\frac{t\pi}{2qM}\Big)\Big)\Big) = \cos\Big(\frac{t\pi}{2M}\Big) =$$

$$= (-1)^s \cos\Big(\frac{t'\pi}{2M}\Big) = (-1)^s r_M(t'),$$

que es una raíz de $\hat{C}_M$. Análogamente, si r una raíz de $\hat{C}_M$, entonces $r = \cos(\frac{t\pi}{2M})$ para algún $t \in d(M)$ tal que $\gcd(t, M) = 1$. Si $qt = t' + s2M$ con $t' \in d(M)$ y $s \in \mathbb{N}_0$, entonces $\gcd(t', M) = 1$ y, por lo tanto,

$$T_q(r) = \cos\Big(q \arccos\Big(\cos\Big(\frac{t\pi}{2M}\Big)\Big)\Big) = \cos\Big(\frac{qt\pi}{2M}\Big) =$$

$$= (-1)^s \cos\Big(\frac{t'\pi}{2M}\Big) = (-1)^s r_M(t'),$$

que es una raíz de $\hat{C}_M$.

Podemos probar de manera análoga la segunda afirmación. Ambos polinomios son mónicos y de grado $2\phi(M)$. Si r es una raíz de $\hat{C}_{2M}$, entonces $r = \cos(\frac{t\pi}{4M})$ para algún $t \in d(2M)$ tal que $\gcd(t, M) = 1$. Si $t = t' + s2M$ con $t' \in d(M)$ y $s \in \{0, 1\}$, entonces $\gcd(t', M) = 1$ y, por lo tanto,

$$T_2(r) = \cos\Big(2 \arccos\Big(\cos\Big(\frac{t\pi}{4M}\Big)\Big)\Big) = \cos\Big(\frac{t\pi}{2M}\Big) =$$

$$= (-1)^s \cos\Big(\frac{t'\pi}{2M}\Big) = (-1)^s r_M(t'),$$

que es una raíz de $\hat{C}_M$. □

Lema 1.9 *Sea W una fórmula proposicional y sea M apropiado. Si la escritura de W no involucra al símbolo de predicado P_j y $q_j \nmid M$, entonces*

$$\mathrm{PolyS}_{q_j M}(W) = \frac{\mathrm{PolyS}_M(W) \circ T_{q_j}}{2^{(q_j-1)\deg \mathrm{PolyS}_M(W)}}.$$

Si M es impar, entonces

$$\mathrm{PolyS}_{2M}(W) = \frac{\mathrm{PolyS}_M(W) \circ T_2}{2^{\deg \mathrm{PolyS}_M(W)}}.$$

Demostración: Comencemos probando la primera afirmación. Sean $J_1, \ldots, J_k$ todas las interpretaciones de los símbolos de predicado $\{P_l \mid q_l \text{ divide a } M\}$ que satisfacen a W. Para $1 \leq h \leq k$, sean J_h^F y J_h^V las interpretaciones de los símbolos de predicado $\{P_l \mid q_l \text{ divide a } M\} \cup \{P_j\}$ que extienden a J_h con $J_h^F(P_j) = F$ y $J_h^V(P_j) = V$ respectivamente. Como la definición de W no involucra a P_j, tenemos que $J_1^F, J_1^V, \ldots, J_k^F, J_k^V$ son todas las interpretaciones de los símbolos de predicado $\{P_l \mid q_l \text{ divide a } M\} \cup \{P_j\}$ que satisfacen a W. Por el Lema 1.7, es suficiente con probar que para $1 \leq h \leq k$,

$$\hat{C}_{q_j M/\alpha(J_h^F)} \hat{C}_{q_j M/\alpha(J_h^V)} = \frac{\hat{C}_{M/\alpha(J_h)} \circ T_{q_j}}{2^{(q_j-1)\deg \hat{C}_{M/\alpha(J_h)}}}.$$

Dado que $\alpha(J_h^F) = \alpha(J_h)$ y $\alpha(J_h^V) = q_j \alpha(J_h)$, esta igualdad es cierta por la primera afirmación del Lema 1.8 aplicada a q_j y a $M/\alpha(J_h)$.

Podemos probar de manera análoga la segunda afirmación, ya que para cualquier interpretación J de los símbolos de predicado $\{P_l \mid q_l \text{ divide a } M\}$ que satisface a W,

$$\hat{C}_{2M/\alpha(J)} = \frac{\hat{C}_{M/\alpha(J)} \circ T_2}{2^{\deg \hat{C}_{M/\alpha(J)}}}$$

por la segunda afirmación del Lema 1.8 aplicada a $M/\alpha(J)$. ▫

Podemos dar ahora nuestra demostración del resultado principal de la sección.

Teorema 1.10 *El problema de decidir si un polinomio univariado con coeficientes enteros codificado por un* slp *tiene una raíz real es NP-*hard*.*

Demostración: Veamos que el problema NP-completo 3-SAT se reduce polinomialmente al problema considerado. Más precisamente, veamos que para cualquier instancia W de 3-SAT es posible calcular en una cantidad de pasos polinomial en el tamaño de W, un *slp* que codifica un polinomio $F \in \mathbb{Z}[x]$ con las mismas raíces reales que $\text{PolyS}_M(W)$ para un M apropiado. Luego, F tiene una raíz real si y solo si W es satisfacible.

Sea $W = (L_{11} \vee L_{12} \vee L_{13}) \wedge \cdots \wedge (L_{m1} \vee L_{m2} \vee L_{m3})$ donde para $1 \leq i \leq m, 1 \leq j \leq 3$, L_{ij} es o bien el literal $P_{k_{ij}}$ o bien el literal $\neg P_{k_{ij}}$ para algún $1 \leq k_{ij} \leq n$.

Dado que $q_k = O(k \log(k))$ (ver [HW79, Chapter I]), podemos calcular q_j para todo $1 \leq j \leq n$, en una cantidad de pasos polinomial en n; por ejemplo, escribiendo los números de 1 a $\tilde{q}$ para $\tilde{q} \in \mathbb{N}$ suficientemente grande y luego eliminando los múltiplos

de cada uno de los números de la lista. Tomemos $M = 2\prod_{1\leq k\leq n} q_k$ (podríamos prescindir del factor 2 en la demostración de este teorema, pero éste tendrá su utilidad en la siguiente sección). Para cada $1 \leq i \leq m$, sea $W_i = L_{i1} \vee L_{i2} \vee L_{i3}$ y $N_i = q_{k_{i1}} q_{k_{i2}} q_{k_{i3}} = O(n^3 \log^3(n))$.

El primer paso consiste en calcular, para cada $1 \leq i \leq m$, un *slp* que codifique un múltiplo escalar en $\mathbb{Z}[x]$ de $\mathrm{PolyS}_{N_i}(W_i)$. Aplicando la fórmula del primer ítem del Lema 1.5 en la de los demás ítems, tenemos que, para cada $1 \leq i \leq m$, $\mathrm{PolyS}_{N_i}(W_i)$ es un cociente entre polinomios de grado acotado por $O(N_i)$ que pueden codificarse por un *slp* de longitud del mismo orden. Utilizamos entonces el algoritmo para división de polinomios codificados por *slp* en [Str73], que requiere una cota para el grado del cociente y un elemento que no anule al denominador. En nuestro caso, conocemos dicha cota y dicho elemento, ya que ignorando los escalares involucrados en las fórmulas del Lema 1.5, obtenemos que la evaluación del denominador en 1 da por resultado 1 por ser un producto de polinomios de Tchebychev. El algoritmo en [Str73] calcula entonces, en una cantidad de pasos polinomial en n y m, un *slp* de longitud $O(n^9 \log^9(n))$ que codifica un múltiplo escalar en $\mathbb{Z}[x]$ de $\mathrm{PolyS}_{N_i}(W_i)$ para cada $1 \leq i \leq m$.

El segundo paso consiste en calcular un *slp* para un múltiplo escalar de $\mathrm{PolyS}_M(W_i)$ en $\mathbb{Z}[x]$ para cada $1 \leq i \leq m$. Siguiendo el Lema 1.9, debemos agregar al *slp* calculado para un múltiplo escalar de $\mathrm{PolyS}_{N_i}(W_i)$ en $\mathbb{Z}[x]$, la codificación correspondiente a la composición con los polinomios T_q para cada primo $q \leq q_n$ distinto de $q_{k_{i1}}, q_{k_{i2}}$ y $q_{k_{i3}}$ y con el polinomio T_2, uno a la vez. Esto puede hacerse en una cantidad de pasos polinomial en n y m y la longitud de los *slps* obtenidos es $O(n^9 \log^9(n))$.

Para finalizar, calculamos en una cantidad de pasos polinomial en n y m un *slp* de longitud $O(mn^9 \log^9(n))$ para la suma de los cuadrados de los múltiplos escalares de los polinomios $\mathrm{PolyS}_M(W_i)$ calculados en el paso anterior para $1 \leq i \leq m$. Si llamamos F al polinomio codificado por este *slp*, las raíces reales de F son las raíces reales comunes de los polinomios $\mathrm{PolyS}_M(W_i)$ para $1 \leq i \leq m$, que son las raíces reales de $\mathrm{PolyS}_M(W)$. Esto concluye la demostración del teorema. ▫

Dado que el polinomio F construido a partir de una instancia W de 3-SAT en la demostración del Teorema 1.10 tiene todas sus raíces reales, si es que tiene alguna, en el intervalo $(-1, 1)$, obtenemos que aun para intervalos con extremos "pequeños" es "difícil" decidir la existencia de raíces reales. Es decir, hemos demostrado también que el problema de decidir si un polinomio univariado con coeficientes enteros

codificado por un *slp* tiene una raíz en un intervalo (a, b) con $a, b \in \mathbb{Q}$ es NP-*hard* en *sentido fuerte* (ver [GJ79, Section 4.2.1]).

1.3. Aproximación de raíces reales

En esta sección reutilizaremos la construcción hecha en la sección anterior para obtener nuevos resultados acerca de la complejidad del problema de aproximar las raíces reales de polinomios univariados con coeficientes enteros codificados por *slps*. Enunciamos a continuación nuestro resultado principal.

Teorema 1.11 *Los dos siguientes problemas son NP-*hard*:*

- *Dados un polinomio $F \in \mathbb{Z}[x]$ codificado por un* slp*, un intervalo abierto, semiabierto o cerrado I con extremos $a, b \in \mathbb{Q}$ tal que F tiene una raíz en I, y $\varepsilon \in \mathbb{Q}$ con $\varepsilon > 0$, encontrar $c, d \in (I \cup \{a, b\}) \cap \mathbb{Q}$ tales que $0 \leq d - c \leq \varepsilon$ y F tiene una raíz en $[c, d] \cap I$.*
- *Dados un polinomio $F \in \mathbb{Z}[x]$ codificado por un* slp*, un intervalo abierto, semiabierto o cerrado I con extremos $a, b \in \mathbb{Q}$ y $\varepsilon \in \mathbb{Q}$ con $\varepsilon > 0$, encontrar $c, d \in (I \cup \{a, b\}) \cap \mathbb{Q}$ tales que $0 \leq d - c \leq \varepsilon$ con la propiedad de que si F tiene una raíz en I, entonces F tiene una raíz en $[c, d] \cap I$.*

Demostración: Consideremos el siguiente problema de búsqueda: dada una instancia satisfacible de 3-SAT, encontrar una interpretación de los símbolos de predicado involucrados en su escritura que la satisfaga. Este problema es NP-*hard*, ya que si existiera un algoritmo con complejidad polinomial que lo resolviera, sería posible adaptarlo para resolver 3-SAT como explicamos a continuación. Dada una instancia cualquiera W de 3-SAT, si luego de la cantidad de pasos necesaria el algoritmo no finalizó, entonces W no es satisfacible. Si finalizó, si la interpretación dada por el algoritmo satisface a W, entonces W es satisfacible; si no, entonces W no estaba en el conjunto de instancias para el cual el algoritmo funciona, es decir, W no es satisfacible.

Para empezar, mostremos una reducción polinomial del problema NP-*hard* descripto en el párrafo anterior al primero de los problemas en el enunciado del teorema. Supongamos que existe un algoritmo de complejidad polinomial en la longitud L del *slp* que codifica a F y del tamaño de los números racionales a, b y ε que lo resuelve

(donde el tamaño de un número racional es la suma de los tamaños de su numerador y su denominador), y que podemos disponer de este algoritmo como subrutina.

Sea $W = (L_{11} \vee L_{12} \vee L_{13}) \wedge \cdots \wedge (L_{m1} \vee L_{m2} \vee L_{m3})$ donde para $1 \leq i \leq m, 1 \leq j \leq 3$, L_{ij} es o bien el literal $P_{k_{ij}}$ o bien el literal $\neg P_{k_{ij}}$ para algún $1 \leq k_{ij} \leq n$, tal que W es satisfacible. Sea $M = 2\prod_{1 \leq k \leq n} q_k$ y sea F el polinomio construido en la demostración del Teorema 1.10, cuyas raíces reales son las raíces del polinomio $\mathrm{PolyS}_M(W)$. Sabemos que podemos calcular en una cantidad de pasos polinomial en m y n un *slp* de longitud $L = O(mn^9 \log^9(n))$ que codifica a F.

Como W es satisfacible, sabemos que F tiene una raíz $r = r_M(t) \in (-1, 1)$, para algún $t \in d(M)$. De hecho, el factor 2 en M asegura que habrá al menos una tal raíz en el intervalo $(-3/4, 3/4)$: si $M/2 \leq t \leq 3M/2$, $r_M(t) \in [-\sqrt{2}/2, \sqrt{2}/2] \subset (-3/4, 3/4)$; si $t < M/2$, entonces $M/2 < t + M < 3M/2$ e $I_M(r_M(t)) = I_M(r_M(t + M))$, luego podemos reemplazar t por $t + M$; finalmente, si $t > 3M/2$, entonces $M/2 < t - M < 3M/2$ e $I_M(r_M(t)) = I_M(r_M(t - M))$, luego podemos reemplazar t por $t - M$. Por lo tanto, podemos suponer que t es un entero impar entre $M/2$ y $3M/2$, con lo cual $r_M(t)$ pertenece el intervalo $(-3/4, 3/4)$.

Notemos que si $-3/4 < r_1 < r_2 < 3/4$, con $r_1 = r_M(t_1), r_2 = r_M(t_2)$ para ciertos enteros $t_1 > t_2$ en $d(M)$, entonces por el Teorema del Valor Medio existe $\xi \in (\arccos(3/4), \arccos(-3/4))$ tal que

$$r_2 - r_1 = \cos(t_2\pi/2M) - \cos(t_1\pi/2M) = \frac{\sin(\xi)(t_1 - t_2)\pi}{2M} \geq \frac{\sqrt{1 - (3/4)^2}\pi}{M} > \frac{2}{M}.$$

Es decir, cualquier par de raíces del polinomio de Tchebychev T_M en el intervalo $(-3/4, 3/4)$ están separadas por una distancia mayor a $2/M$.

Consideremos $\varepsilon = 1/2M$. Observemos que, como $\log(M) = \Theta(q_n) = O(n)$, donde Θ es la función de Tchebychev $\Theta(x) = \sum_{p \leq x,\, p \text{ primo}} \log(p)$ (ver [HW79, Chapter XXII, Theorem 415]), el tamaño de ε es polinomial en n.

Supongamos que utilizamos la subrutina disponible para encontrar en una cantidad de pasos polinomial en n y m, números $c, d \in [-3/4, 3/4] \cap \mathbb{Q}$ con $0 \leq d - c \leq \varepsilon$ tales que F tiene una raíz real en $[c, d] \cap (-3/4, 3/4)$. Como $d - c$ es menor que la mínima separación entre raíces reales de F, concluimos que existe exactamente una raíz real $r_0 = r_M(t_0)$ de F en $[c, d]$, que nos provee una interpretación de los símbolos de predicado $P_1, \ldots, P_n$ que satisface a W. Basta entonces probar que podemos hallar t_0 y decidir cuál es la interpretación asociada a $r_M(t_0)$ en una cantidad de pasos polinomial en n y m para concluir que podemos resolver el problema NP-

hard descripto al comienzo de la demostración con complejidad polinomial en n y m utilizando la subrutina disponible.

Primeramente, utilizamos la siguiente fórmula (ver [BBP97]):

$$\pi = \sum_{i=0}^{\infty} \frac{1}{16^i}\Big(\frac{4}{8i+1} - \frac{2}{8i+4} - \frac{1}{8i+5} - \frac{1}{8i+6}\Big),$$

para encontrar una aproximación $p \in \mathbb{Q}$ al número π tal que $|p-\pi| < 1/4M$ en una cantidad de pasos polinomial en $\log(M)$, y por lo tanto, también en n.

Para $t \in d(M)$, podemos dar una aproximación $s(t)$ en $\mathbb{Q}$ para el número $\cos(tp/2M)$ usando el desarrollo de Taylor con error acotado por $1/4M$, también en una cantidad de pasos polinomial en n; luego tenemos

$$\Big|s(t) - \cos\Big(\frac{t\pi}{2M}\Big)\Big| \leq \Big|s(t) - \cos\Big(\frac{tp}{2M}\Big)\Big| + \Big|\cos\Big(\frac{tp}{2M}\Big) - \cos\Big(\frac{t\pi}{2M}\Big)\Big| \leq$$

$$\leq \Big|s(t) - \cos\Big(\frac{tp}{2M}\Big)\Big| + \Big|\frac{tp}{2M} - \frac{t\pi}{2M}\Big| \leq \frac{1}{2M}.$$

Notemos que si para un cierto $t \in d(M)$, $s(t) \in [c - 1/2M, d + 1/2M]$, entonces $t = t_0$, porque de otro modo $|r_M(t) - r_M(t_0)| \leq |r_M(t) - s(t)| + |s(t) - r_M(t_0)| \leq 1/2M + 1/M < 2/M$, lo que es imposible. Luego, para determinar t_0, basta hallar el único $t \in d(M)$ tal que $r_M(t) \in s(t) \in [c-1/2M, d+1/2M]$; para lo cual, usando el método de bisección en $d(M)$, calculamos las aproximaciones $s(t)$ para a lo sumo $O(\log M)$ elementos de $d(M)$ en una cantidad de pasos polinomial en n.

Para encontrar cuál es la interpretación asociada a $r_M(t_0)$, simplemente determinamos para cada $1 \leq j \leq n$ si el primo q_j divide a t_0 o no, lo cual puede hacerse en una cantidad de pasos polinomial en n, e indica si $I_M(r_M(t_0)) = V$ o si $I_M(r_M(t_0)) = F$ respectivamente.

Para probar que el segundo de los problemas en el enunciado del teorema es NP-*hard*, podemos proceder de manera análoga para mostrar una reducción polinomial a él del problema 3-SAT. Supongamos que existe un algoritmo de complejidad polinomial en la longitud L del *slp* que codifica a F y del tamaño de los números racionales a, b y ε que lo resuelve, y que podemos disponer de este algoritmo como subrutina.

Sea $W = (L_{11} \vee L_{12} \vee L_{13}) \wedge \cdots \wedge (L_{m1} \vee L_{m2} \vee L_{m3})$ donde para $1 \leq i \leq m, 1 \leq j \leq 3$, L_{ij} es o bien el literal $P_{k_{ij}}$ o bien el literal $\neg P_{k_{ij}}$ para algún $1 \leq k_{ij} \leq n$. Consideramos entonces nuevamente el polinomio F construido en la demostración del Teorema 1.10, $I = (-3/4, 3/4)$ y $\varepsilon = 1/2M$ para $M = 2\prod_{1\leq k\leq n} q_k$ y utilizamos

la subrutina disponible para encontrar en una cantidad de pasos polinomial en n y m, números $c, d \in [-3/4, 3/4] \cap \mathbb{Q}$ con $0 \leq d - c \leq \varepsilon$ tales que si F tiene una raíz real en $(-3/4, 3/4)$, entonces F tiene una raíz real en $[c, d] \cap (-3/4, 3/4)$. Repitiendo los razonamientos anteriores, tenemos que existe a lo sumo un $t_0 \in d(M)$ tal que $r_M(t_0) \in [c - 1/2M, d + 1/2M]$. Más aún, podemos decidir si existe, y en tal caso, encontrarlo, en una cantidad de pasos polinomial en n. Luego, si no existe tal t_0, la fórmula no es satisfacible. Si existe, procediendo igual que anteriormente, podemos obtener la interpretación I asociada a $r_M(t_0)$; solamente resta entonces evaluar la fórmula W en la interpretación I, lo cual puede hacerse en una cantidad de pasos polinomial en n y m, para encontrar una interpretación que satisface a W si es que existe alguna, y por lo tanto, para decidir si W es satisfacible. ▫

Capítulo 2

Condiciones de signo

2.1. Introducción al problema

Dados polinomios $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$, una *condición de signo* para estos polinomios es un elemento $\sigma = (\sigma_1, \ldots, \sigma_m) \in \{<, =, >\}^m$ y una *condición de signo cerrada* para ellos es un elemento $\sigma = (\sigma_1, \ldots, \sigma_m) \in \{\leq, =, \geq\}^m$. La *realización* de una condición de signo o de una condición de signo cerrada σ es el conjunto de soluciones en $\mathbb{R}^n$ del sistema de igualdades y desigualdades

$$\begin{cases} f_1 \quad \sigma_1 \quad 0, \\ \qquad \vdots \\ f_m \quad \sigma_m \quad 0. \end{cases} \tag{2.1}$$

Cuando este conjunto es no vacío, decimos que σ es *factible* y que el sistema (2.1) es *consistente*. Una *celda* es una componente conexa de la realización de una condición de signo.

Un problema básico en geometría semialgebraica efectiva es, dados $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$ y una condición de signo para ellos, decidir si ésta es factible o no lo es. Este problema es un caso particular del problema de eliminación de cuantificadores sobre los reales, que ha sido ampliamente estudiado. Una estrategia usual en los algoritmos de eliminación de cuantificadores, aun en los más eficientes (ver, por ejemplo, [BPR96]), es obtener una familia finita de puntos que interseca cada componente conexa de un conjunto semialgebraico. Una técnica muy utilizada para esto consiste en introducir infinitesimales y tomar sumas de cuadrados con el objeto de reducir el problema al caso particular de hipersuperficies suaves y compactas,

al precio de incrementar tanto el número de variables como el grado de los polinomios involucrados. Entre los trabajos que evitan este incremento artificial de los parámetros, en el caso de conjuntos definidos por igualdades, podemos mencionar [BGHM97, BGHM01, SEDS03, BGHP04, BGHP05, SEDT]. Asimismo, la complejidad de los algoritmos en estos trabajos depende de cierto parámetro intrínseco de los sistemas de polinomios considerados y, por lo tanto, resultan más eficientes en los casos en los que este parámetro es menor que el valor que toma en el caso genérico.

En este capítulo presentaremos un algoritmo probabilístico para calcular, dada una familia de polinomios $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$, un conjunto finito con la propiedad de intersecar la clausura de cada celda definida por estos polinomios en tres situaciones diferentes: cuando se cumplen ciertas hipótesis de regularidad (Sección 2.6.1), en el caso de polinomios bivariados arbitrarios (Sección 2.6.2) y en el caso de un único polinomio multivariado arbitrario (Sección 2.6.3). Además presentaremos, para el caso general, un algoritmo probabilístico para calcular un conjunto finito con la propiedad de intersecar cada componente conexa de la realización de cada condición de signo cerrada (Sección 2.6.4). El *output* producido por estos algoritmos es una familia de resoluciones geométricas que describen conjuntos finitos cuya unión es el conjunto buscado. En cualquiera de los casos mencionados, evaluando los signos de los polinomios $f_1, \ldots, f_m$ en los puntos del conjunto hallado, obtenemos la lista de todas las condiciones de signo cerradas factibles para la familia de polinomios dada. En la primera de las situaciones descriptas, estos resultados nos permiten obtener también todas las condiciones de signo factibles para dicha familia de polinomios.

Describimos a continuación cómo funcionan los algoritmos que presentaremos para el cálculo de un conjunto finito que interseque la clausura de cada celda definida por $f_1, \ldots, f_m$ en las tres primeras situaciones o cada componente conexa de cada condición de signo cerrada para $f_1, \ldots, f_m$ en el caso general.

El algoritmo es de naturaleza inductiva en el número de variables. En el caso $n = 1$, los mismos $f_1, \ldots, f_m$ proveen la familia de resoluciones geométricas buscada. Cuando $n > 1$, procedemos como se explica a continuación.

Para comenzar efectuamos un cambio lineal genérico de variables, lo que asegura que para cada componente conexa de la realización de cada condición de signo factible o de cada condición de signo cerrada factible, se evita un cierto comportamiento de tipo asintótico con respecto a la proyección sobre la primera coordenada: la imagen de su clausura por la proyección es o bien todo $\mathbb{R}$ o bien un intervalo cerrado, acotado superior o inferiormente, cuyos extremos tienen finitas preimágenes.

Para cada componente conexa que se encuentre en la segunda situación, existirán puntos en su clausura en los cuales la función x_1 se maximiza o minimiza. A fin de localizar estos puntos, consideramos un sistema de ecuaciones de estructura similar al proveniente del Teorema de Multiplicadores de Lagrange. Sin embargo, en el caso general los puntos buscados no son las únicas soluciones de este sistema, que incluso puede tener infinitas soluciones. Para solucionar este problema, utilizamos técnicas de deformación que recuperan un número finito de soluciones y probamos que entre ellas se encuentran los puntos buscados originalmente.

Para las otras componentes conexas, como la imagen de la función x_1 restringida a ellas es todo el conjunto $\mathbb{R}$, podemos intersecarlas a todas simultáneamente con un único hiperplano de la forma $\{x_1 = p_1\}$ y eliminar así una variable. Razonando de manera inductiva, recomenzamos nuestro algoritmo con los polinomios $f_1(p_1, x_2, \ldots, x_n), \ldots, f_m(p_1, x_2, \ldots, x_n)$, que involucran una variable menos, y a cada punto del conjunto calculado para estos polinomios le agregamos el valor p_1 como primera coordenada. Este conjunto junto con el obtenido en el párrafo anterior forman un conjunto con la propiedad de intersecar la clausura de todas las componentes conexas de condiciones de signo definidas por $f_1, \ldots, f_m$.

La complejidad de los métodos presentados en este capítulo mejora la complejidad en el peor caso, que es a su vez el caso genérico, de los algoritmos previos que resuelven el mismo problema. Esto se debe en parte a que el trabajar directamente con los polinomios dados sin considerar sumas de cuadrados ni perturbaciones infinitesimales nos permite evitar el incremento artificial de los parámetros. Además, una herramienta fundamental para lograr esta mejora en la complejidad es el uso de técnicas de deformación especialmente diseñadas para el caso bihomogéneo (ver [HJSS05]) para tratar los sistemas de ecuaciones con los que localizamos los puntos extremales. Hasta ahora, la caracterización de puntos extremales mediante sistemas con estructura particular solamente había sido aprovechada para obtener cotas sobre la cantidad de celdas definidas por la familia de polinomios de entrada ([SEDT]); sin embargo, para la resolución de los sistemas utilizados para caracterizar estos puntos, se aplicaban algoritmos generales de resolución de sistemas de ecuaciones ([ABRW96, Rou99, GLS01, Lec03])

Nuestros resultados pueden ser considerados a su vez como una extensión de los obtenidos en [SEDS03] y [BGHP05], en el sentido de que trabajamos no solamente con igualdades sino también con desigualdades. De hecho, el algoritmo descripto en [SEDS03] para el caso particular de variedades equidimensionales regulares defini-

das por un ideal radical, considera una familia de sistemas de ecuaciones que son equivalentes a los definidos en las etapas recursivas de nuestro algoritmo. Sin embargo, estos sistemas involucran una gran cantidad de polinomios y no presentan una estructura particular. Por otro lado, la justificación teórica de la correctitud del algoritmo en dicho trabajo no sigue nuestro razonamiento inductivo sino que se basa en considerar conjuntamente una familia de proyecciones sobre variedades polares que, bajo las hipótesis mencionadas, resultan propias.

Este capítulo está organizado de la siguiente manera. En la próxima sección incluimos algunos conocimientos preliminares de geometría semialgebraica. En la Sección 2.3 probamos que, efectuando un único cambio lineal de variables genérico al comienzo de los algoritmos que desarrollaremos, podemos suponer que no se dan situaciones de tipo asintótico en ninguna de las etapas recursivas de los mismos. En la Sección 2.4 presentamos los sistemas de ecuaciones que utilizaremos para caracterizar los puntos extremales de la proyección sobre la primera coordenada, y en la Sección 2.5 desarrollamos las técnicas de deformación que utilizaremos para tratar con estos sistemas. Finalmente, en la Sección 2.6 probamos que, en las distintas situaciones mencionadas, los puntos encontrados utilizando la deformación incluyen a los puntos extremales buscados, y combinamos las herramientas desarrolladas en las secciones anteriores para resolver los problemas planteados.

2.2. Preliminares de geometría semialgebraica

Incluimos en esta sección los conceptos principales de geometría semialgebraica que utilizaremos en el resto del capítulo. Para demostraciones y mayores detalles referimos al lector a [BCR98, Chapter 2].

Un *conjunto semialgebraico* de $\mathbb{R}^n$ es un conjunto de la forma

$$\bigcup_{1\leq i\leq s}\ \bigcap_{1\leq j\leq r_i}\ \Big\{x\in\mathbb{R}^n \mid f_{ij}(x)\sigma_{ij}0\Big\},$$

donde, para $1\leq i\leq s$ y $1\leq j\leq r_i$, $f_{ij}\in\mathbb{R}[x_1,\ldots,x_n]$ y $\sigma_{ij}\in\{<,=,>\}$.

Dados $A\subset\mathbb{R}^n$ y $B\subset\mathbb{R}^m$ semialgebraicos, una *función semialgebraica* es una función $f:A\to B$ tal que su gráfico es un conjunto semialgebraico de $\mathbb{R}^{n+m}$.

Los conjuntos semialgebraicos y las funciones semialgebraicas satisfacen numerosas propiedades. A continuación incluimos un muy breve resumen de las mismas.

- Uniones finitas e intersecciones finitas de conjuntos semialgebraicos de $\mathbb{R}^n$ son conjuntos semialgebraicos de $\mathbb{R}^n$. El complemento de un conjunto semialgebraico de $\mathbb{R}^n$ también es un conjunto semialgebraico de $\mathbb{R}^n$.
- Un conjunto semialgebraico tiene finitas componentes conexas, y cada una de ellas es a su vez un conjunto semialgebraico.
- La suma, resta, producto, división y composición de funciones semialgebraicas (cuando estén bien definidas) dan por resultado funciones semialgebraicas.
- La imagen y preimagen de conjuntos semialgebraicos por funciones semialgebraicas son conjuntos semialgebraicos.
- Las proyecciones son funciones semialgebraicas.

El siguiente resultado es conocido como el *lema de selección de curvas* y, si bien es quizás un poco técnico, resulta muy útil para trabajar con conjuntos semialgebraicos.

Lema 2.1 *Sea $A \subset \mathbb{R}^n$ un conjunto semialgebraico y $x \in \overline{A}$. Existe una curva continua semialgebraica $\gamma : [0,1] \to \mathbb{R}^n$ tal que $\gamma(0) = x$ y $\gamma((0,1]) \subset A$.*

Para ejemplificar el significado de este lema, podemos agregar que, en realidad, cualquier conjunto cerrado de $\mathbb{R}^n$ satisface el lema de selección de curvas (tomando curvas constantes) y que, en cambio, el conjunto $A = \{\frac{1}{n} \mid n \in \mathbb{N}\}$ no satisface el lema de selección de curvas.
Para finalizar, incluimos la siguiente definición clásica en geometría semialgebraica.

Definición 2.2 *Sean $g_1, \ldots, g_l \in \mathbb{R}[x_1, \ldots, x_n]$, $h_1, \ldots, h_{l'} \in \mathbb{R}[x_1, \ldots, x_{n-1}]$. Los polinomios $h_1, \ldots, h_{l'}$* particionan *$g_1, \ldots, g_l$ si existe una partición de $\mathbb{R}^{n-1}$ formada por conjuntos semialgebraicos $A_1, \ldots, A_r$ tales que para todo $1 \leq s \leq r$, A_s puede definirse utilizando disyunciones y conjunciones sobre los signos que toman los polinomios $h_1, \ldots, h_{l'}$ en $\mathbb{R}^{n-1}$ y además existen funciones continuas semialgebraicas $\xi_{s,1} < \ldots < \xi_{s,a_s} : A_s \to \mathbb{R}$ tales que:*

- *para todo $p \in A_s$, $\{\xi_{s,1}(p), \ldots, \xi_{s,a_s}(p)\}$ es el conjunto de todas las raíces de todos los polinomios univariados $g_1(p, x_n), \ldots, g_l(p, x_n)$ que no resulten idénticamente nulos,*
- *para todo $(p, q) \in A_s \times \mathbb{R}$, los signos de $g_1(p, q), \ldots, g_l(p, q)$ quedan determinados a partir de los signos de $q - \xi_{s,1}(p), \ldots, q - \xi_{s,a_s}(p)$.*

2.3. Cambios de variables que evitan situaciones asintóticas

Como explicamos en la Sección 2.1, para que los algoritmos que presentaremos en este capítulo funcionen de manera correcta, debemos efectuar primeramente un cambio lineal de variables con el objetivo de evitar ciertas situaciones de tipo asintótico. En esta sección precisaremos este enunciado. Introducimos a continuación la notación que utilizaremos.

Definición 2.3 *Notamos Π_k la proyección sobre la k-ésima coordenada; es decir, $\Pi_k : \mathbb{R}^n \to \mathbb{R}$, $\Pi_k(x_1, \ldots, x_n) = x_k$. Para $A \subset \mathbb{R}^n$ no vacío, definimos:*

- $Z_{\inf}(A,k) = \begin{cases} \overline{A} \cap \Pi_k^{-1}(\inf \Pi_k(A)) & \text{si } \Pi_k(A) \text{ es acotado inferiormente,} \\ \emptyset & \text{en caso contrario,} \end{cases}$
- $Z_{\sup}(A,k) = \begin{cases} \overline{A} \cap \Pi_k^{-1}(\sup \Pi_k(A)) & \text{si } \Pi_k(A) \text{ es acotado superiormente,} \\ \emptyset & \text{en caso contrario,} \end{cases}$
- $Z(A,k) = Z_{\inf}(A,k) \cup Z_{\sup}(A,k)$.

Por último, notamos $Z_{\inf}(A)$, $Z_{\sup}(A)$ y $Z(A)$ a los conjuntos $Z_{\inf}(A,1)$, $Z_{\sup}(A,1)$ y $Z(A,1)$ respectivamente.

Notemos que $Z_{\inf}(A,k)$ puede ser vacío aun cuando $\Pi_k(A)$ sea acotado inferiormente. Tal es el caso, por ejemplo, cuando $n = 2, k = 1$ y $A = \{x_1 > 0, x_1 x_2 = 1\}$. Veremos que un único cambio lineal genérico de variables evita este tipo de situación asintótica simultáneamente para todas las componentes conexas de conjuntos definidos por condiciones de signo para la familia de polinomios de entrada, tanto para la familia original, como también para las sucesivas familias que obtendremos al evaluar de a una las variables. El enunciado preciso de este hecho se encuentra en la siguiente proposición.

Proposición 2.4 *Luego de un cambio lineal genérico de variables con coeficientes en $\mathbb{Q}$, para todo conjunto semialgebraico $D \subset \mathbb{R}^n$ definido utilizando disyunciones y conjunciones sobre los signos que toman los polinomios $f_1, \ldots, f_m$ y para todo $p = (p_1, \ldots, p_n) \in \mathbb{R}^n$, si $1 \leq k \leq n$ y C es una componente conexa de $D \cap \{x_1 = p_1, \ldots, x_{k-1} = p_{k-1}\}$, entonces:*

- *$Z(C,k)$ es finito (posiblemente vacío),*
- *si $\Pi_k(C)$ está acotado inferiormente, entonces $Z_{\inf}(C,k)$ es no vacío,*
- *si $\Pi_k(C)$ está acotado superiormente, entonces $Z_{\sup}(C,k)$ es no vacío.*

Para demostrar la Proposición 2.4, demostremos primero el siguiente lema auxiliar, en el que extendemos la familia de polinomios $f_1,\dots,f_m$ y damos condiciones suficientes sobre la familia extendida para que se cumpla lo enunciado en esta proposición.

Lema 2.5 *Sea $\{f_{ij}\}_{1\le i\le n,1\le j\le l_i}\subset\mathbb{R}[x_1,\dots,x_n]$ un conjunto de polinomios no nulos que satisface las siguientes propiedades:*

a) para $1\le i\le n$, el conjunto $\{f_{ij}\}_{1\le j\le l_i}$ está incluido en $\mathbb{R}[x_1,\dots,x_i]$, es estable por derivación con respecto a la variable x_i y está formado por polinomios cuasimónicos con respecto a esta variable,

b) para $1<i\le n$, $f_{(i-1)1},\dots,f_{(i-1)l_{i-1}}$ particionan $f_{i1},\dots,f_{il_i}$

Sea $p=(p_1,\dots,p_n)\in\mathbb{R}^n$. Sea $1\le i\le n$ y sea D un conjunto semialgebraico de $\mathbb{R}^i$ definido utilizando disyunciones y conjunciones sobre los signos que toman los polinomios $f_{ij}, 1\le j\le l_i$. Sea $1\le k\le i$ y sea C una componente conexa de $D\cap\{x_1=p_1,\dots,x_{k-1}=p_{k-1}\}$. Entonces

- *$Z(C,k)$ es finito (posiblemente vacío),*
- *si $\Pi_k(C)$ está acotado inferiormente, entonces $Z_{\inf}(C,k)$ es no vacío,*
- *si $\Pi_k(C)$ está acotado superiormente, entonces $Z_{\sup}(C,k)$ es no vacío.*

Demostración: Podemos suponer que $k=1$, ya que para todo $1\le k\le n$, la familia $\{f_{ij}(p_1,\dots,p_{k-1},x_k,\dots,x_n)\}_{k\le i\le n,1\le j\le l_i}\subset\mathbb{R}[x_k,\dots,x_n]$ también satisface las hipótesis de este lema y la coordenada x_k toma el rol de la primera coordenada.

Procedamos por inducción en i. Para $i=1$, el resultado es claro pues C resulta un intervalo de $\mathbb{R}$. Supongamos ahora que $i\ge 2$ y que el resultado vale para $i-1$. Sea $\Pi:\mathbb{R}^i\to\mathbb{R}^{i-1}$ la proyección sobre las primeras $i-1$ coordenadas.

Como los polinomios $f_{(i-1)1},\dots,f_{(i-1)l_{i-1}}$ particionan $f_{i1},\dots,f_{il_i}$, existen conjuntos semialgebraicos $A_1,\dots,A_r\subset\mathbb{R}^{i-1}$ y, para $1\le s\le r$, funciones continuas

semialgebraicas $\xi_{s,1} < \ldots < \xi_{s,a_s} : A_s \to \mathbb{R}$ como en la Definición 2.2. Llamemos $A_{s,1}, \ldots, A_{s,u_s}$ a las componentes conexas de A_s y $B_{s,u,1}, \ldots, B_{s,u,2a_s+1}$ a la partición de $A_{s,u} \times \mathbb{R}$ dada por las funciones $\xi_{s,1}, \ldots, \xi_{s,a_s}$, es decir, $B_{s,u,1}$ es el subconjunto de $A_{s,u} \times \mathbb{R}$ por debajo del gráfico de $\xi_{s,1}$, $B_{s,u,2}$ es el gráfico de $\xi_{s,1}$ restringida a $A_{s,u}$, $B_{s,u,3}$ es el subconjunto de $A_{s,u} \times \mathbb{R}$ entre el gráfico de $\xi_{s,1}$ y $\xi_{s,2}$, etc. Luego C puede expresarse como una unión finita de conjuntos del tipo $B_{s,u,v}$ y $\Pi(C)$ como una unión finita de conjuntos del tipo $A_{s,u}$.

Si $\Pi(C) = \cup_h A_{s_h,u_h}$, entonces $Z(\Pi(C)) \subset \cup_h Z(A_{s_h,u_h})$. Cada A_{s_h,u_h} es una componente conexa del conjunto A_{s_h}, que puede ser descripto por condiciones de signo para los polinomios $f_{(i-1)1}, \ldots, f_{(i-1)l_{i-1}}$; luego, por hipótesis inductiva, tenemos que cada $Z(A_{s_h,u_h})$ es finito y por lo tanto $Z(\Pi(C))$ también es finito.

Sea $w = (w_1, \ldots, w_i) \in Z(C)$, veamos que $\Pi(w) \in Z(\Pi(C))$. Como $w \in Z(C) \subset \overline{C}$, $\Pi(w) \in \Pi(\overline{C}) \subset \overline{\Pi(C)}$. Además, dado que $\Pi_1(C) = \Pi_1(\Pi(C))$, tenemos que $w_1 = \inf \Pi_1(C)$ implica que $w_1 = \inf \Pi_1(\Pi(C))$, y $w_1 = \sup \Pi_1(C)$ implica que $w_1 = \sup \Pi_1(\Pi(C))$; luego $\Pi(w) \in Z(\Pi(C))$.

Como $w \in Z(C)$, al menos uno de los polinomios $f_{i1}, \ldots, f_{il_i}$ debe anularse en w (en caso contrario, todos los $f_{ij}, 1 \leq j \leq l_i$, tendrían signo constante en un entorno de w y este entorno estaría contenido en C, lo que contradice que $w \in Z(C)$). Podemos concluir entonces que $Z(C)$ es un conjunto finito, ya que $\Pi(w)$ pertenece al conjunto finito $Z(\Pi(C))$ y w_i es una raíz de alguno de los polinomios $f_{i1}(\Pi(w), x_i), \ldots, f_{il_i}(\Pi(w), x_i)$, que son todos no idénticamente nulos pues cada f_{ij} es cuasimónico en la variable x_i.

Supongamos ahora que $\Pi_1(C)$ es un intervalo acotado inferiormente (el otro caso es análogo). Dado que $\Pi_1(\Pi(C)) = \Pi_1(C)$, por hipótesis inductiva existe $z = (z_1, \ldots, z_{i-1}) \in Z_{\inf}(\Pi(C)) \subset \overline{\Pi(C)}$. Supongamos además que $A_{1,1} \subset \Pi(C)$, $z \in Z_{\inf}(A_{1,1})$ y que $\gamma : [0,1] \to \overline{A_{1,1}}$ es una curva continua semialgebraica tal que $\gamma((0,1]) \subset A_{1,1}$ y $\gamma(0) = z$. Llamemos $\tilde{x}$ a $\gamma(1)$. Dado que $\tilde{x} \in A_{1,1} \subset \Pi(C)$, existe $y \in \mathbb{R}$ tal que $(\tilde{x}, y) \in C$. Bajo las hipótesis de este lema, para $1 \leq a \leq a_1$ la función $\xi_{1,a}$ se puede extender de manera continua a $\overline{A_1}$ ([BCR98, Lema 2.5.6]); llamemos también $\xi_{1,a}$ a dicha extensión. Considerando los distintos casos posibles, definimos la función $h : [0,1] \to \mathbb{R}$:

- si $y = \xi_{1,a}(\tilde{x})$ para algún $1 \leq a \leq a_1$, entonces $h(t) = \xi_{1,a}(\gamma(t))$,
- si $\xi_{1,a}(\tilde{x}) < y < \xi_{1,a+1}(\tilde{x})$ para algún $1 \leq a < a_1$, entonces,

$$h(t) = \xi_{1,a}(\gamma(t)) \frac{y - \xi_{1,a}(\tilde{x})}{\xi_{1,a+1}(\tilde{x}) - \xi_{1,a}(\tilde{x})} + \xi_{1,a+1}(\gamma(t)) \frac{\xi_{1,a+1}(\tilde{x}) - y}{\xi_{1,a+1}(\tilde{x}) - \xi_{1,a}(\tilde{x})},$$

- si $y < \xi_{1,1}(\tilde{x}),\ h(t) = \xi_{1,1}(\gamma(t)) + y - \xi_{1,1}(\tilde{x})$,
- si $\xi_{1,a_1}(\tilde{x}) < y,\ h(t) = \xi_{1,a_1}(\gamma(t)) + y - \xi_{1,a_1}(\tilde{x})$,
- si $a_1 = 0,\ h(t) \equiv y$.

En cualquier caso, $\tilde{\gamma} : [0,1] \to \mathbb{R}^i$ definida por $\tilde{\gamma}(t) = (\gamma(t), h(t))$ es una curva continua, tal que $\tilde{\gamma}((0,1]) \subset C$ (pues los signos de los polinomios $f_{i1}, \ldots, f_{il_i}$ permanecen constantes sobre $\tilde{\gamma}((0,1])$) y por lo tanto $(z, h(0)) = \tilde{\gamma}(0) \in \overline{C}$. Además, $z_1 = \inf \Pi_1(\Pi(C)) = \inf \Pi_1(C)$, por lo tanto $(z, h(0)) \in Z_{\inf}(C)$, y este conjunto es no vacío. □

Podemos dar ahora una demostración de la Proposición 2.4:

Demostración: Haciendo uso del Lema 2.5, alcanza con ver que hay un abierto Zariski $\mathcal{U}$ incluido en el conjunto de matrices inversibles en $\mathbb{C}^{n\times n}$ tal que para toda matriz V_0 en $\mathbb{Q}^{n\times n} \cap \mathcal{U}$ existe un conjunto de polinomios $\{f_{ij}\}_{1\le i\le n, 1\le j\le l_i} \subset \mathbb{R}[x]$ que satisface las hipótesis de dicho lema y tal que para $1 \le j \le m$, $f_{nj}(x) = f_j(V_0 x)$.

Consideremos una matriz V cuyas entradas son las nuevas variables v_{rs}, $1 \le r, s \le n$, y construimos el conjunto de polinomios $\{F_{ij}\}_{1\le i\le n, 1\le j\le l_i} \subset \mathbb{R}[v, x]$ de la siguiente manera:

- Definimos $l'_n = m$ y para $1 \le j \le l'_n$, tomamos $F_{nj}(V, x) = f_j(Vx)$. Luego, para cada $1 \le j_0 \le l'_n$, si F_{nj_0} tiene grado d_{nj_0} con respecto a las variables x, agregamos al conjunto $\{F_{nj}\}_{1\le j\le l'_n}$ las primeras $d_{nj_0} - 1$ derivadas de F_{nj_0} con respecto a x_n, formando así el conjunto $\{F_{nj}\}_{1\le j\le l_n}$.
- Sea $1 \le i \le n-1$. Definido el conjunto $\{F_{(i+1)j}\}_{1\le j\le l_{i+1}} \subset \mathbb{R}[v, x_1, \ldots, x_{i+1}]$, definimos $\{F_{ij}\}_{1\le j\le l_i}$ como explicamos a continuación. En primer lugar, formamos un conjunto $\{F_{ij}\}_{1\le j\le l'_i} \subset \mathbb{R}[v, x_1, \ldots, x_i]$ tomando todas las resultantes y subresultantes entre pares de elementos de $\{F_{(i+1)j}\}_{1\le j\le l_{i+1}}$ con respecto a la variable x_{i+1}, descartando aquéllas que resulten idénticamente nulas. Luego, para cada $1 \le j_0 \le l'_i$, si F_{ij_0} tiene grado d_{ij_0} con respecto a las variables x, agregamos al conjunto $\{F_{ij}\}_{1\le j\le l'_i}$ las primeras $d_{ij_0} - 1$ derivadas de F_{ij_0} con respecto a x_i, formando así el conjunto $\{F_{ij}\}_{1\le j\le li}$.

Para $1 \le i \le n$, $1 \le j \le l_i$, sea d_{ij} el grado de F_{ij} con respecto a las variables x, y sea q_{ij} el polinomio en las variables v que acompaña a $x_i^{d_{ij}}$ viendo a F_{ij} como polinomio

en x_i. Queremos ver que, para $1 \leq j \leq l'_i$, q_{ij} no es idénticamente nulo, lo cual da sentido a tomar las $d_{ij} - 1$ derivadas con respecto a la variable x_i en la construcción anterior y además prueba que para $l'_i + 1 \leq j \leq l_i$, q_{ij} no es idénticamente nulo.

A tal efecto, probaremos simultáneamente el siguiente resultado auxiliar: si para $B \in \mathbb{Q}^{i\times i}$ notamos $\tilde{B}$ y $\hat{B}$ a las matrices

$$\tilde{B} = \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{Q}^{(i+1)\times(i+1)} \qquad \text{y} \qquad \hat{B} = \begin{pmatrix} B & 0 \\ 0 & I_{n-i} \end{pmatrix} \in \mathbb{Q}^{n\times n},$$

entonces para $1 \leq j \leq l'_i$ y para toda $B \in \mathbb{Q}^{i\times i}$ vale que $F_{ij}(V, Bx) = F_{ij}(V\hat{B}, x)$ y para $l'_i + 1 \leq j \leq l_i$ y para toda $B \in \mathbb{Q}^{(i-1)\times(i-1)}$ vale que $F_{ij}(V, \tilde{B}x) = F_{ij}(V\hat{B}, x)$.

Procedamos por inducción decreciente en i. Si $i = n, 1 \leq j \leq l'_n$, es claro que q_{nj} no es idénticamente nulo pues existe un cambio de variables $V_0 \in \mathbb{Q}^{n\times n}$ que hace al polinomio f_j cuasimónico y de grado d_{nj} con respecto a la variable x_n. Además, para $B \in \mathbb{Q}^{n\times n}$ vale que $F_{nj}(V, Bx) = f_j(VBx) = F_{nj}(VB, x)$. Por último, para $l'_n + 1 \leq j \leq l_n$ y para $B \in \mathbb{Q}^{(n-1)\times(n-1)}$, podemos pensar que F_{nj} es la derivada con respecto a x_n de un polinomio $F_{nj'}(V, x)$, con $1 \leq j' < j$, para el cual vale que $F_{nj'}(V, \tilde{B}x) = F_{nj'}(V\hat{B}, x)$. Dada la estructura de $\tilde{B}$, derivando esta igualdad con respecto a x_n obtenemos la igualdad buscada.

Sea ahora $i < n$ y $B \in \mathbb{Q}^{i\times i}$. Para $1 \leq j \leq l_{i+1}$, consideremos la escritura

$$F_{(i+1)j}(V, x) = \sum_{0\leq h\leq d_{(i+1)j}} q_{(i+1)j,h}(V, x_1, \ldots, x_i)x_{i+1}^h$$

en la que $q_{(i+1)j,d_{(i+1)j}}(V, x_1, \ldots, x_i)$ es el polinomio $q_{(i+1)j}(V)$. Entonces, el hecho de que $F_{(i+1)j}(V, \tilde{B}x) = F_{(i+1)j}(V\hat{B}, x)$ implica que $q_{(i+1)j,h}(V, Bx) = q_{(i+1)j,h}(V\hat{B}, x)$ para $1 \leq h \leq d_{(i+1)j}$.

Para $1 \leq j \leq l'_i$, supongamos que F_{ij} corresponde a una resultante o a una subresultante entre los polinomios $F_{(i+1)1}$ y $F_{(i+1)2}$. Como sabemos que los grados de $F_{(i+1)1}$ y $F_{(i+1)2}$ con respecto a la variable x_{i+1} son $d_{(i+1)1}$ y $d_{(i+1)2}$ respectivamente, podemos pensar que F_{ij} es la evaluación de un cierto polinomio R en los polinomios $q_{(i+1)1,h}$ y $q_{(i+1)2,h}$; luego $F_{ij}(V, Bx) = R(q_{(i+1)1,1}(V, Bx), \ldots, q_{(i+1)2,d_{(i+1)2}}(V, Bx)) = R(q_{(i+1)1,1}(V\hat{B}, x), \ldots, q_{(i+1)2,d_{(i+1)2}}(V\hat{B}, x)) = F_{ij}(V\hat{B}, x)$. Para $l'_i + 1 \leq j \leq l_i$ podemos proceder de igual manera que en el caso $i = n$.

Veamos ahora que para $1 \leq j \leq l'_i$, q_{ij} es no nulo. Sea $B \in \mathbb{Q}^{i\times i}$ tal que $F_{ij}(V, Bx)$ tiene grado d_{ij} en la variable x_i. Como $F_{ij}(V, Bx) = F_{ij}(V\hat{B}, x)$, resulta que $q_{ij}(V\hat{B})$ es no nulo y por lo tanto q_{ij} no es idénticamente nulo.

Definimos entonces $\mathcal{U} = \{V \in \mathbb{C}^{n\times n} \mid q_{ij}(V) \neq 0 \text{ para } 1 \leq i \leq n, 1 \leq j \leq l_i\}$. Para toda $V_0 \in \mathbb{Q}^{n\times n} \cap \mathcal{U}$, el conjunto $\{f_{ij}(x)\}_{1\leq i\leq n, 1\leq j\leq l_i}$ definido por $f_{ij}(x) = F_{ij}(V_0, x)$ claramente cumple la primera condición del Lema 2.5 y la segunda condición se sigue de [BPR03, Proposition 4.34 y Theorem 5.14]. ▫

Habiendo explicado las propiedades que podemos suponer luego de efectuar un cambio lineal genérico de variables, en la siguiente proposición damos de manera más precisa la idea principal de los algoritmos que presentaremos. La misma surge de reinterpretar y generalizar el resultado que se da en [SEDS03, Theorem 2] para conjuntos algebraicos que cumplen determinadas hipótesis.

Proposición 2.6 *Luego de un cambio lineal genérico de variables con coeficientes en $\mathbb{Q}$, para todo conjunto semialgebraico $D \subset \mathbb{R}^n$ definido utilizando disyunciones y conjunciones sobre los signos que toman los polinomios $f_1, \ldots, f_m$ y para todo $p = (p_1, \ldots, p_n) \in \mathbb{R}^n$, si para $1 \leq k \leq n$, $\mathcal{D}(k, p)$ es el conjunto de componentes conexas de $D \cap \{x_1 = p_1, \ldots, x_{k-1} = p_{k-1}\}$, entonces*

$$\{p\} \bigcup \Big(\bigcup_{1\leq k\leq n} \bigcup_{C\in\mathcal{D}(k,p)} Z(C, k) \Big)$$

es un conjunto finito que interseca la clausura de cada componente conexa de D.

Demostración: La finitud de este conjunto es consecuencia de la Proposición 2.4. Podemos observar que $\mathcal{D}(1, p)$ es el conjunto de componentes conexas de D. Sea $C_1 \in \mathcal{D}(1, p)$. Si $\Pi_1(C_1)$ es acotado inferior o superiormente, nuevamente por la Proposición 2.4, el conjunto finito $Z(C_1, 1)$ es no vacío y está incluido en $\overline{C_1}$. Si $\Pi_1(C_1)$ no es acotado ni inferior ni superiormente, entonces $\Pi_1(C_1) = \mathbb{R}$ y por lo tanto $C_1 \cap \{x_1 = p_1\} \neq \emptyset$. Sea $C_2 \in \mathcal{D}(2, p)$ una componente conexa de $C_1 \cap \{x_1 = p_1\}$. Nuevamente, si $\Pi_2(C_2)$ es acotado inferior o superiormente, el conjunto $Z(C_2, 2)$ es no vacío y está incluido en $\overline{C_2} \subset \overline{C_1}$. Si $\Pi_2(C_2)$ no es acotado ni inferior ni superiormente, entonces $\Pi_2(C_2) = \mathbb{R}$ y por lo tanto $C_1 \cap \{x_1 = p_1, x_2 = p_2\} \neq \emptyset$. Siguiendo de esta manera, llegamos a que o bien existen algún $1 \leq k \leq n$ y $C_k \in \mathcal{D}(k, p)$ tal que $Z(C_k, k)$ es no vacío y está incluido en $\overline{C_k} \subset \overline{C_1}$, o bien $p \in C_1$. ▫

Dado que para $k \geq 2$ podemos pensar la k-ésima variable como la primera variable en los polinomios $f_j(p_1, \ldots, p_{k-1}, x_k, \ldots, x_n), 1 \leq j \leq m$, en las próximas secciones nos enfocaremos en el problema de encontrar los puntos extremales para la proyección sobre la primera coordenada en las clausuras de componentes conexas de conjuntos semialgebraicos.

2.4. Ecuaciones que definen puntos extremales

En esta sección presentaremos los sistemas de ecuaciones que utilizaremos para localizar los puntos extremales buscados.

Sean $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$. Supongamos que z es un punto en una componente conexa del conjunto $\{x \in \mathbb{R}^n \mid f_{i_1}(x) = \cdots = f_{i_s}(x) = 0\}$ para ciertos $i_1, \ldots, i_s \in \{1, \ldots, m\}$ con $1 \leq s \leq n-1$, en el cual la función x_1 tiene un máximo o un mínimo local. Luego z satisface las siguientes condiciones:

$$f_{i_1}(z) = \cdots = f_{i_s}(z) = 0, \quad \operatorname{rank} \begin{pmatrix} \frac{\partial f_{i_1}}{\partial x_2}(z) & \cdots & \frac{\partial f_{i_1}}{\partial x_n}(z) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_{i_s}}{\partial x_2}(z) & \cdots & \frac{\partial f_{i_s}}{\partial x_n}(z) \end{pmatrix} < s, \tag{2.2}$$

ya que en caso contrario, por el Teorema de la Función Implícita, podríamos despejar de manera continua en el conjunto $\{f_{i_1}(x) = \cdots = f_{i_s}(x) = 0\}$, $n - s$ funciones coordenadas incluyendo a x_1 en función de otras s funciones coordenadas en un entorno de z, lo cual contradice que la función x_1 se minimiza o maximiza sobre una componente conexa de dicho conjunto en z.

Las condiciones (2.2) son equivalentes a decir que existe $\mu = (\mu_1, \ldots, \mu_s) \in \mathbb{R}^s - \{0\}$ tal que

$$f_{i_1}(z) = \cdots = f_{i_s}(z) = 0, \quad \sum_{1 \leq j \leq s} \mu_j \overline{\nabla} f_{i_j}(z) = (0, \ldots, 0) \in \mathbb{R}^{n-1}, \tag{2.3}$$

donde $\overline{\nabla} f_{i_j}(z)$ indica que se le quita la primera coordenada a $\nabla f_{i_j}(z)$. En el caso particular en que $s = 1$, las condiciones (2.2) son equivalentes a

$$f_{i_1}(z) = \frac{\partial f_{i_s}}{\partial x_2}(z) = \cdots = \frac{\partial f_{i_s}}{\partial x_n}(z) = 0. \tag{2.4}$$

Por otro lado, podemos considerar las condiciones (2.2) aun para $s \geq n$, pero en tal caso resultan equivalentes a

$$f_{i_1}(z) = \cdots = f_{i_s}(z) = 0. \tag{2.5}$$

La estructura homogénea del sistema (2.3) con respecto a las variables $\mu_1, \ldots, \mu_s$ nos permite dar las definiciones siguientes.

Definición 2.7 *Sea $S = \{i_1, \ldots, i_s\} \subset \{1, \ldots, m\}$. Si $2 \leq s \leq n-1$, definimos $W_S \subset \mathbb{A}^n \times \mathbb{P}^{s-1}$ como la variedad definida por las ecuaciones (2.3) y notamos Π a*

la proyección $\Pi : \mathbb{A}^n \times \mathbb{P}^{s-1} \to \mathbb{A}^n$. *Si* $s = 1$ *o* $s \geq n$, *definimos* $W_S \subset \mathbb{A}^n$ *como la variedad definida por las ecuaciones (2.4) o (2.5) respectivamente. Con el objeto de unificar la notación para estos dos últimos casos, notamos también* $\Pi : \mathbb{A}^n \to \mathbb{A}^n$ *a la función identidad.*

Observemos que, si bien hasta ahora todos los razonamientos que hemos hecho han tenido lugar en el contexto de los números reales, hemos definido las variedades W_S como variedades complejas. Esto nos permitirá utilizar técnicas de deformación de sistemas de ecuaciones sobre cuerpos algebraicamente cerrados en la Sección 2.5.

La siguiente proposición es una adaptación a nuestro contexto de las condiciones de Karush-Kuhn-Tucker (ver [Ped04, Chapter 3]), que constituyen una generalización del Teorema de los Multiplicadores de Lagrange al caso en que las restricciones están dadas por igualdades y desigualdades.

Proposición 2.8 *Sean* $\sigma \in \{\leq, <, =, \geq, >\}^m$ *y* $E_\sigma = \{i \mid \sigma_i = \text{“} = \text{”}\}$. *Para toda componente conexa* C *del conjunto* $\{x \in \mathbb{R}^n \mid f_1(x)\sigma_1 0, \ldots, f_m(x)\sigma_m 0\}$,

$$Z(C) \subset \bigcup_{\substack{E_\sigma \subset S \subset \{1,\ldots,m\} \\ S \neq \emptyset}} \Pi(W_S).$$

Demostración: Sin pérdida de generalidad supongamos $E_\sigma = \{1, \ldots, l\}$ (donde $l = 0$ si E_σ es vacío) y $Z_{\inf}(C) \neq \emptyset$. Sean $z = (z_1, \ldots, z_n) \in Z_{\inf}(C)$ y $S_0 = \{i \in \{1, \ldots, m\} \mid f_i(z) = 0\}$; luego $S_0 \neq \emptyset$ y podemos suponer que $S_0 = \{1, \ldots, t\}$ para cierto t con $l \leq t \leq m$. Veamos que $z \in \Pi(W_{S_0})$. Si $t \geq n$, por definición, $z \in \Pi(W_{S_0})$. Supongamos entonces que $t \leq n - 1$ y procedamos por el absurdo.

Si $z \notin \Pi(W_{S_0})$ entonces el conjunto $\{\overline{\nabla} f_i(z), i \in S_0\}$ es l.i. Llamemos f a la función $f : \mathbb{R}^n \to \mathbb{R}^t, f(x) = (f_1(x), \ldots, f_t(x))$. Podemos suponer que el menor correspondiente a las variables $n - t + 1, \ldots, n$ en la matriz $Df(z)$ es no nulo. Por el Teorema de la Función Inversa aplicado a la función $h : \mathbb{R}^n \to \mathbb{R}^n, h(x) = (x_1 - z_1, \ldots, x_{n-t} - z_{n-t}, f_1(x), \ldots, f_t(x))$, existe un entorno abierto U de z, un entorno abierto V de 0 y una función $\mathcal{C}^\infty$ $g : V \to U$ inversa de $h : U \to V$. Más aún, achicando los abiertos U y V, podemos suponer que para $t + 1 \leq i \leq m$, el signo de f_i es constante en U y que V es de la forma $(-\varepsilon, \varepsilon)^n$ para cierto $\varepsilon > 0$. Las primeras $n-t$ funciones coordenadas de g serán las funciones $x_1 + z_1, \ldots, x_{n-t} + z_{n-t}$. Sea $w \in C \cap U$ y sea $y = h(w)$. Sea $\tilde{\sigma} \in \{<, =, >\}^m$ tal que para $1 \leq i \leq m$, $f_i(w)\tilde{\sigma}_i 0$. Como $w \in C$, tenemos que para $1 \leq i \leq m$, la condición $\tilde{\sigma}_i$ implica la

condición σ_i (es decir, $\tilde{\sigma}_i \in \{<, =\}$ si $\sigma_i =$ " $\leq$ ", $\tilde{\sigma}_i \in \{>, =\}$ si $\sigma_i =$ " $\geq$ " y $\tilde{\sigma}_i = \sigma_i$ en los demás casos). Luego para para $1 \leq i \leq t$, $y_{n-t+i} = f_i(w)\sigma_i 0$.

Sea $\gamma : [-\varepsilon/2, y_1] \to V$ definida por $\gamma(u) = (u, y_2, \ldots, y_n)$. La curva imagen de $g \circ \gamma$ es conexa y $g \circ \gamma(y_1) = w \in C$. Para $u \in [-\varepsilon/2, y_1]$ y para $1 \leq i \leq t$, $f_i \circ g \circ \gamma(u) = y_{n-t+i}\sigma_i 0$; entonces, como para $t+1 \leq i \leq m$, el signo de f_i es constante en U, podemos concluir que la imagen de $g \circ \gamma$ está contenida en C. Sin embargo, la primera coordenada de $g \circ \gamma(-\varepsilon/2)$ es $-\varepsilon/2 + z_1 < z_1$. Esto es imposible pues $z \in Z_{\inf}(C)$ y entonces $z_1 = \inf \Pi_1(C)$. El absurdo provino de suponer que el conjunto $\{\overline{\nabla} f_i(z), i \in S_0\}$ es l.i., luego $z \in \Pi(W_{S_0})$. ▫

La Proposición 2.8 nos proporciona un conjunto que contiene a todos los puntos extremales buscados. Sin embargo, en el caso general los conjuntos del tipo $\Pi(W_S)$ pueden no ser finitos. Tal es el caso, por ejemplo, cuando $n = 2, m = 1, S = \{1\}$ y $f_1 = (x_1^2 + x_2^2 - 1)^2$ en el que $W_S = \{x_1^2 + x_2^2 - 1 = 0\}$, o cuando $n = 3, m = 1, S = \{1\}$ y $f_1 = (x_1 - x_3^2)^3 - x_2^2$ en el que $W_S = \{x_1 - x_3^2 = x_2 = 0\}$. Para solucionar este problema, en la próxima sección estudiaremos técnicas de deformación efectivas desde un punto de vista computacional, que nos proporcionarán un conjunto finito que contiene un subconjunto de $\Pi(W_S)$. En la Sección 2.6 probaremos en varias situaciones distintas que este conjunto finito contiene a los puntos extremales buscados; esto nos permitirá concluir que en la Proposición 2.8 podemos reemplazar las variedades $\Pi(W_S)$ por los conjuntos finitos encontrados por las técnicas de deformación.

2.5. Métodos de deformación para sistemas con dos juegos de variables

En esta sección describiremos los métodos simbólicos que utilizaremos para trabajar con los sistemas de ecuaciones del tipo de (2.3) que definen las variedades W_S (ver Definición 2.7). Estos métodos están basados en técnicas de deformación introducidas en [GHM+98, GHH+97, GLS01, HKP+00, Sch03] adaptadas al contexto bihomogéneo como en [HJSS05]. Consideraremos variedades algebraicas complejas y también variedades sobre otros cuerpos algebraicamente cerrados, pero, salvo indicación explícita, se debe suponer que estamos en el primer caso.

2.5.1. La deformación

Sea $\mathbb{K}$ un subcuerpo de $\mathbb{R}$. Sean $2 \leq s \leq n-1$ y $r = s+n-1$. Supongamos dado un sistema de ecuaciones formado por polinomios en $\mathbb{K}[x_1, \ldots, x_n, \mu_1, \ldots, \mu_s]$ del tipo:

$$h_1(x) = \cdots = h_s(x) = h_{s+1}(x, \mu) = \cdots = h_r(x, \mu) = 0, \tag{2.6}$$

con $h_{s+1}, \ldots, h_r$ homogéneos de grado 1 en las variables μ (podemos observar que los sistemas del tipo de (2.3) presentan esta estructura). Para $1 \leq i \leq r$, sea $d_i = \deg_x h_i$ y sea $d \geq 2$ una cota superior para $d_1, \ldots, d_r$.

Sea $W \subset \mathbb{A}^n \times \mathbb{P}^{s-1}$ la variedad definida por $h_1, \ldots, h_r$. El grado de W está acotado por el grado de la variedad definida en $\mathbb{P}^n \times \mathbb{P}^{s-1}$ por las homogeneizaciones respecto a las variables x (con una nueva variable x_0) de los polinomios $h_1(x), \ldots, h_s(x)$, $h_{s+1}(x, \mu), \ldots, h_r(x, \mu)$. Si para $1 \leq i \leq r$ llamamos e_i al multigrado de dichos polinomios, entonces por el Teorema de Bézout Multihomogéneo (ver Sección 0.3.2), $\deg W$ está acotado por

$$\delta := \mathrm{Bez}_{n,s-1}(e_1, \ldots, e_r) = \sum_{\substack{(j_1,\ldots,j_r)\in\{1,2\}^r \\ \#\{k|j_k=1\}=n,\ \#\{k|j_k=2\}=s-1}} \Big(\prod_{1\leq i\leq r} e_{ij_i} \Big).$$

El hecho de que $e_i = (d_i, 0)$ para $1 \leq i \leq s$ y $e_i = (d_i, 1)$ para $s+1 \leq i \leq r$ implica que en la expresión anterior solo suman los términos correspondientes a r-uplas $(j_1, \ldots, j_r)$ tales que $\{k \mid j_k = 2\}$ está contenido en $\{s+1, \ldots, r\}$ o, equivalentemente, tales que $\{k \mid j_k = 1\} = \{1, \ldots, s\} \cup E$ para algún $E \subset \{s+1, \ldots, r\}$ con $\#E = n-s$. Podemos concluir entonces que

$$\delta = \Big(\prod_{1\leq i\leq s} d_i \Big) \Big(\sum_{\substack{E\subset\{s+1,\ldots,r\} \\ \#E=n-s}} \prod_{k\in E} d_k \Big) \leq \binom{n-1}{s-1} d^n.$$

En las Secciones 2.5.2 y 2.5.3 especificaremos dos maneras concretas de "deformar" el sistema (2.6) y cada una tendrá su aplicación en la Sección 2.6. Estas deformaciones se definirán a partir de un sistema formado por polinomios $g_1(x), \ldots, g_s(x)$, $g_{s+1}(x, \mu), \ldots, g_r(x, \mu) \in \mathbb{Q}[x, \mu]$ al que llamaremos *sistema inicial*. En esta sección demostramos propiedades comunes a ambos tipos de deformación, las cuales dependen de que el sistema inicial satisfaga la siguiente hipótesis.

Hipótesis 2.9

1. *Para* $1 \leq i \leq r$, $\tilde{d}_i := \deg_x g_i \geq d_i$.

2. *Para* $s+1 \leq i \leq r$, g_i *es homogéneo de grado 1 en las variables* μ.

3. *Si para* $s+1 \leq i \leq r$ *definimos* $\bar{g}_i(x, \mu_1, \ldots, \mu_{s-1}) = g_i(x, \mu_1, \ldots, \mu_{s-1}, 1)$, *la variedad que definen* $g_1, \ldots, g_s, \bar{g}_{s+1}, \ldots, \bar{g}_r$ *en* $\mathbb{A}^r$ *está formada por* $\tilde{\delta}$ *puntos* $s_1, \ldots, s_{\tilde{\delta}}$ *con*

$$\tilde{\delta} = \Big(\prod_{1 \leq i \leq s} \tilde{d}_i \Big) \Big(\sum_{\substack{E \subset \{s+1, \ldots, r\} \\ \#E = n-s}} \prod_{k \in E} \tilde{d}_k \Big),$$

la matriz diferencial del sistema formado por $g_1, \ldots, g_s, \bar{g}_{s+1}, \ldots, \bar{g}_r$ *evaluada en* s_i *es inversible para todo* $1 \leq i \leq \tilde{\delta}$ *y además* $(s_{i1}, \ldots, s_{in}) \neq (s_{i'1}, \ldots, s_{i'n})$ *para* $1 \leq i < i' \leq \tilde{\delta}$.

Podemos observar que, bajo estas hipótesis, las homogeneizaciones respecto a las variables x (con una nueva variable x_0) de los polinomios $g_1(x), \ldots, g_s(x), g_{s+1}(x, \mu)$, $\ldots, g_r(x, \mu)$ definen una variedad 0-dimensional en $\mathbb{P}^n \times \mathbb{P}^{s-1}$, contenida en $\{x_0 \neq 0\} \cap \{\mu_s \neq 0\}$ y formada por $\tilde{\delta}$ puntos. Esto es así ya que, nuevamente por el Teorema de Bézout Multihomogéneo, la variedad definida en $\mathbb{P}^n \times \mathbb{P}^{s-1}$ tiene grado menor o igual a $\tilde{\delta}$ y, por la tercera de las condiciones de la Hipótesis 2.9, dicha variedad tiene esa cantidad de puntos aislados en el abierto $\{x_0 \neq 0\} \cap \{\mu_s \neq 0\}$.

A continuación damos las definiciones principales para el resto de la sección.

Definición 2.10 *Sea* t *una nueva variable. Para* $1 \leq i \leq r$, *notamos* F_i *al polinomio*

$$F_i = (1-t)h_i + tg_i \in \mathbb{K}[t, x, \mu]$$

e I *el ideal generado por* $F_1, \ldots, F_r$ *en el anillo* $\mathbb{C}[t, x, \mu]$.

Definimos $\hat{V} \subset \mathbb{A}^1 \times \mathbb{A}^n \times \mathbb{P}^{s-1}$ *como la variedad definida por* I. *Definimos además* $V^{(0)}$ *como la unión de las componentes irreducibles de* $\hat{V}$ *contenidas en* $\{t = 0\}$, $V^{(1)}$ *como la unión de las componentes irreducibles de* $\hat{V}$ *contenidas en* $\{t = t_0\}$ *para algún* $t_0 \in \mathbb{C} \setminus \{0\}$, *y* V *como la unión de las demás componentes irreducibles de* $\hat{V}$.

Notamos $\pi : \mathbb{A}^1 \times \mathbb{A}^n \times \mathbb{P}^{s-1} \to \mathbb{A}^n \times \mathbb{P}^{s-1}$ *a la proyección* $\pi(t, x, \mu) = (x, \mu)$ *y* $\tilde{\pi} : \mathbb{A}^1 \times \mathbb{A}^n \times \mathbb{P}^{s-1} \to \mathbb{A}^1 \times \mathbb{A}^n$ *a la proyección* $\tilde{\pi}(t, x, \mu) = (t, x)$.

Con estas definiciones, $\pi(\hat{V} \cap \{t = 0\}) = W$. Además, la proyección $\tilde{\pi}$ es cerrada (ver [Sha77, Chapter 1, Section 5, Theorem 3]). Comencemos a estudiar algunas de las propiedades de las variedades que acabamos de definir, para lo cual, de aquí en más supondremos que el sistema inicial satisface la Hipótesis 2.9,

Lema 2.11 *Toda componente irreducible de V es 1-dimensional e interseca a $\{t = 1\}$. Además, $\hat{V} \cap \{t = 1\} = V \cap \{t = 1\}$.*

Demostración: Toda componente irreducible de $\hat{V}$, y en particular de V, tiene dimensión mayor o igual a 1 dado que $\hat{V}$ está definida por $r = s + n - 1$ ecuaciones en $\mathbb{A}^1 \times \mathbb{A}^n \times \mathbb{P}^{s-1}$. Por otro lado, $\hat{V} \cap \{t = 1\}$ es 0-dimensional, ya que esta variedad es simplemente la variedad definida por los polinomios $g_1, \ldots, g_r$ incluida en el hiperplano $\{t = 1\}$ de $\mathbb{A}^1 \times \mathbb{A}^n \times \mathbb{P}^{s-1}$. Esto implica que $\hat{V}$ no tiene componentes irreducibles incluidas en el hiperplano $\{t = 1\}$; luego $\hat{V} \cap \{t = 1\} = V \cap \{t = 1\}$.
Sea V_1 una componente irreducible de V y sea $\overline{V_1}$ su clausura Zariski en $\mathbb{A}^1 \times \mathbb{P}^n \times \mathbb{P}^{s-1}$. Dado que $\mathbb{P}^n \times \mathbb{P}^{s-1}$ es una variedad proyectiva, la proyección de $\overline{V_1}$ a $\mathbb{A}^1$ es un conjunto cerrado (ver [Sha77, Chapter 1, Section 5, Theorem 3]) y, por definición de V, esta proyección debe ser igual a $\mathbb{A}^1$; luego $\overline{V_1} \cap \{t = 1\} \neq \emptyset$. La hipótesis sobre $g_1, \ldots, g_r$ implica que $\overline{V_1} \cap \{t = 1\} = V_1 \cap \{t = 1\}$, luego $V_1 \cap \{t = 1\}$ es una variedad no vacía y 0-dimensional. Por lo tanto, tenemos que $\dim(V_1) \leq 1$, con lo cual podemos concluir que $\dim(V_1) = 1$. ▫

Dado que cada componente irreducible de V es 1-dimensional y no está contenida en ningún hiperplano de la forma $\{t = t_0\}$ para ningún $t_0 \in \mathbb{C}$, tenemos el siguiente corolario.

Corolario 2.12 *El conjunto $\pi(V \cap \{t = 0\})$ es un subconjunto finito de W y contiene a todos sus puntos aislados.*

Los conjuntos $\Pi(\pi(V \cap \{t = 0\}))$ serán los subconjuntos finitos de las variedades $\Pi(W)$ a los cuales nos referimos en las observaciones hechas luego de la demostración de la Proposición 2.8. En las Secciones 2.5.2 y 2.5.3, desarrollaremos métodos simbólicos que permiten calcular una resolución geométrica de una variedad 0-dimensional que contiene a $\Pi(\pi(V \cap \{t = 0\}))$. A tal efecto, dado que solamente conocemos ecuaciones para la variedad $\hat{V}$, debemos eliminar las componentes irreducibles de esta variedad contenidas en hiperplanos de la forma $\{t = t_0\}$ para algún

$t_0 \in \mathbb{C}$. Para lograr esto, pensamos a la variable t como parte de los coeficientes de los polinomios $F_1, \ldots, F_r$ y consideramos la extensión del cuerpo $\mathbb{C}$ al cuerpo $\overline{\mathbb{C}(t)}$. Llamemos $I^{(e)}$ al ideal generado por los polinomios $F_1, \ldots, F_r$ en el anillo $\mathbb{C}(t)[x, \mu]$ y $V^{(e)} \subset \mathbb{A}^n_{\overline{\mathbb{C}(t)}} \times \mathbb{P}^{s-1}_{\overline{\mathbb{C}(t)}}$ a la variedad definida por $I^{(e)}$. Estudiemos algunas propiedades de esta nueva variedad.

Proposición 2.13 *La variedad $V^{(e)}$ es 0-dimensional y está formada por $\tilde{\delta}$ puntos. Más aún, existen $\tilde{\delta}$ elementos $S_1, \ldots, S_{\tilde{\delta}}$ en $\mathbb{K}[[t-1]]^r$ tales que*

$$V^{(e)} = \left\{ \big((S_{i1}, \ldots, S_{in}), (S_{i(n+1)} : \cdots : S_{ir} : 1)\big),\ 1 \leq i \leq \tilde{\delta} \right\} \subset \mathbb{A}^n_{\overline{\mathbb{C}(t)}} \times \{\mu_s \neq 0\}$$

y además $(S_{i1}, \ldots, S_{in}) \neq (S_{i'1}, \ldots, S_{i'n})$ para $1 \leq i < i' \leq \tilde{\delta}$.

Demostración: Por el Teorema de Bézout Multihomogéneo, sabemos que el grado de la variedad $V^{(e)}$ está acotado por $\tilde{\delta}$; por lo tanto, para ver que $V^{(e)}$ es 0-dimensional alcanza con ver que existen $\tilde{\delta}$ puntos aislados en $V^{(e)}$. Según la Hipótesis 2.9, existen $\tilde{\delta}$ puntos $s_1, \ldots, s_{\tilde{\delta}} \in \mathbb{A}^r$ tales que $\pi(V \cap \{t = 1\}) =$

$$= \left\{ \big((s_{i1}, \ldots, s_{in}), (s_{i(n+1)} : \cdots : s_{ir} : 1)\big),\ 1 \leq i \leq \tilde{\delta} \right\} \subset \mathbb{A}^n \times \mathbb{P}^{s-1}.$$

Notemos que, para $1 \leq i \leq \tilde{\delta}$, la parte de la matriz diferencial del sistema formado por $F_1(t, x), \ldots, F_s(t, x), F_{s+1}(t, x, \mu_1, \ldots, \mu_{s-1}, 1), \ldots, F_r(t, x, \mu_1, \ldots, \mu_{s-1}, 1)$ correspondiente a diferenciar con respecto a las variables $x, \mu_1, \ldots, \mu_{s-1}$, evaluada en $(t, x, \mu_1, \ldots, \mu_{s-1}) = (1, s_i)$, coincide con la matriz diferencial del sistema formado por $g_1(x), \ldots, g_s(x), \bar{g}_{s+1}(x, \mu_1, \ldots, \mu_{s-1}), \ldots, \bar{g}_r(x, \mu_1, \ldots, \mu_{s-1})$ con respecto a las variables $x, \mu_1, \ldots, \mu_{s-1}$, evaluada en $(x, \mu_1, \ldots, \mu_{s-1}) = s_i$, que es una matriz inversible según la Hipótesis 2.9. Luego, por [HKP$^+$00, Lemma 3], existen para $1 \leq i \leq \tilde{\delta}$, elementos $S_i \in \mathbb{K}[[t-1]]^r$ tales que

- $F_1(t, S_{i1}, \ldots, S_{in}) = \cdots = F_s(t, S_{i1}, \ldots, S_{in}) = F_{s+1}(t, S_i, 1) = \cdots = = F_r(t, S_i, 1) = 0$,
- $S_i(1) = s_i$, lo cual implica que son $\tilde{\delta}$ elementos distintos y que $(S_{i1}, \ldots, S_{in}) \neq (S_{i'1}, \ldots, S_{i'n})$ para $1 \leq i < i' \leq \tilde{\delta}$.

Por otro lado, para $1 \leq i \leq \tilde{\delta}$, el determinante de la matriz diferencial de $F_1(t, x)$, $\ldots, F_s(t, x), F_{s+1}(t, x, \mu_1, \ldots, \mu_{s-1}, 1), \ldots, F_r(t, x, \mu_1, \ldots, \mu_{s-1}, 1)$ correspondiente a diferenciar con respecto a las variables $x, \mu_1, \ldots, \mu_{s-1}$ evaluada en S_i es un elemento

no nulo de $\mathbb{C}[[t-1]]$, ya que comienza su desarrollo con un elemento no nulo de $\mathbb{C}$, que es el determinante de la matriz diferencial de $g_1(x), \ldots, g_s(x), \bar{g}_{s+1}(x, \mu_1, \ldots, \mu_{s-1}), \ldots, \bar{g}_r(x, \mu_1, \ldots, \mu_{s-1})$ con respecto a las variables $x, \mu_1, \ldots, \mu_{s-1}$, evaluada en s_i; luego cada $((S_{i1}, \ldots, S_{in}), (S_{i(n+1)} : \cdots : S_{ir} : 1))$ es un punto aislado de $V^{(e)}$. ▫

El siguiente paso para calcular la resolución geométrica buscada es analizar formas lineales sobre la variedad en cuestión. Con tal objetivo, introducimos la siguiente definición.

Definición 2.14 *Sean $y_1, \ldots, y_n$ nuevas variables. Notamos ℓ a la forma lineal definida tanto en $\mathbb{A}^n$ como en $\mathbb{A}^n_{\overline{\mathbb{C}(t)}}$ por $\ell(x, y) = \sum_{1 \leq j \leq n} y_j x_j$, donde las variables y se consideran como parámetros. Para $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ notamos ℓ_α a la forma lineal definida tanto en $\mathbb{A}^n$ como en $\mathbb{A}^n_{\overline{\mathbb{C}(t)}}$ por $\ell_\alpha(x) = \sum_{1 \leq j \leq n} \alpha_j x_j$.*
Extendiendo la definición de Π a la proyección $\Pi : \mathbb{A}^n_{\overline{\mathbb{C}(t)}} \times \mathbb{P}^{s-1}_{\overline{\mathbb{C}(t)}} \to \mathbb{A}^n_{\overline{\mathbb{C}(t)}}$, definimos P como el polinomio minimal de ℓ sobre la variedad $\Pi(V^{(e)})$; es decir,

$$P(t, U, y) = \prod_{1 \leq i \leq \tilde{\delta}} \Big(U - \ell\big((S_{i1}, \ldots, S_{in}), y\big) \Big) \in \mathbb{K}[[t-1]][U, y].$$

Dado que los polinomios $F_1, \ldots, F_r$ tienen sus coeficientes en $\mathbb{K}$, si llamamos $I_1^{(e)}$ al ideal que generan los polinomios $F_1(t, x), \ldots, F_s(t, x), F_{s+1}(t, x, \mu_1, \ldots, \mu_{s-1}, 1) \ldots, F_r(t, x, \mu_1, \ldots, \mu_{s-1}, 1)$ en $\mathbb{K}(t)[x, \mu_1, \ldots, \mu_{s-1}]$, entonces, $\mathbb{K}(t)[x, \mu]/I_1^{(e)}$ es un $\mathbb{K}(t)$-espacio vectorial de dimensión $\tilde{\delta}$ y $P(t, U, y)$ es el polinomio minimal y el polinomio característico de la transformación lineal de multiplicar por $\ell(x, y)$ en este espacio vectorial (considerando a las variables $y_1, \ldots, y_n$ como parámetros). Esto nos permite concluir que, en realidad, $P \in \mathbb{K}(t)[U, y]$. Consideremos entonces la escritura

$$P(t, U, y) = \frac{\hat{P}(t, U, y)}{q(t)} = \frac{\sum_{0 \leq h \leq \tilde{\delta}} p_h(t, y) U^h}{q(t)} \tag{2.7}$$

con $q \in \mathbb{K}[t]$ mónico, $\hat{P}$ y q coprimos en $\mathbb{K}[t, U, y]$, $p_h \in \mathbb{K}[t, y]$ para $0 \leq h \leq \tilde{\delta}$ y $p_{\tilde{\delta}}(t, y) = q(t)$.
En el siguiente lema auxiliar veremos una relación entre los polinomios recién definidos y la variedad de deformación definida al comienzo de la sección.

Lema 2.15 *El polinomio $\hat{P}(t, U, y)$ es libre de cuadrados y si $\Phi : V \times \mathbb{A}^n \to \mathbb{A}^{n+2}$ es el morfismo dado por*

$$\Phi(t, x, \mu, y) = (t, \ell(x, y), y),$$

entonces $\overline{\mathrm{Im}\Phi}$ es la hipersuperficie definida por el polinomio $\hat{P}(t, U, y)$.

Demostración: Sea $R(t,U,y) \in \mathbb{C}[t,U,y]$ un polinomio libre de cuadrados que define la hipersuperficie $\overline{\mathrm{Im}\Phi}$. Veamos que R y $\hat{P}$ se dividen mutuamente en $\mathbb{C}[t,U,y]$.

Para probar que R divide a $\hat{P}$, alcanza con demostrar que $\hat{P}$ se anula en $\mathrm{Im}\Phi$. Sea $(t_0,x_0,\mu_0,\beta) \in V \times \mathbb{A}^n$. Dado que $\hat{P}(t,\ell(x,\beta),\beta)$ se anula en $V^{(e)}$, existe $m \in \mathbb{N}$ tal que $\hat{P}(t,\ell(x,\beta),\beta)^m \in I^{(e)}$, y esto implica que existe $v(t) \in \mathbb{C}[t]$ tal que $v(t)\hat{P}(t,\ell(x,\beta),\beta)^m \in I$. Por lo tanto, el polinomio $v(t)\hat{P}(t,\ell(x,\beta),\beta)$ se anula en todas las componentes de $\hat{V}$, y luego $\hat{P}(t,\ell(x,\beta),\beta)$ se anula en todas las componentes de V, en particular $\hat{P}(t_0,\ell(x_0,\beta),\beta) = 0$ como queríamos probar.

Veamos ahora que $\hat{P}$ divide a R . Notemos que $P(t,U,y)$ es el generador del ideal de polinomios

$$\Big\{Q(U) \in \overline{\mathbb{C}(t,y)}[U] \mid Q\big(\ell(\Pi(S),y)\big) = 0 \text{ para todo } S \in V^{(e)}\Big\}$$

en el dominio principal $\overline{\mathbb{C}(t,y)}[U]$. Por otro lado, $R(t,\ell(x,y),y) = 0$ para $(t,x,\mu,y) \in V \times \mathbb{A}^n$, luego existe un polinomio $w(t) \in \mathbb{C}[t]$ y $m \in \mathbb{N}$ tal que $R^m(t,\ell(x,y),y)w^m(t) \in I\mathbb{C}[t,x,\mu,y] \subset I^{(e)}\mathbb{C}(t)[x,\mu,y]$, con lo cual $R(t,U,y)w(t)$ se anula en $\ell(\Pi(S),y)$ para todo $S \in V^{(e)}$. Tenemos entonces que $P(t,U,y)$ divide a $R(t,U,y)w(t)$ en $\overline{\mathbb{C}(t,y)}[U]$ y luego en $\mathbb{C}(t,y)[U]$. Como $\hat{P}(t,U,y) = q(t)P(t,U,y)$ no tiene factores en $\mathbb{C}[t,y]$, entonces $\hat{P}(t,U,y)$ divide a $R(t,U,y)$ en $\mathbb{C}[t,U,y]$. ▫

Podemos ahora enunciar el resultado principal de esta sección.

Proposición 2.16 *Siguiendo la notación en (2.7), sea $\prod_{1\le j\le a} q_j(U,y)^{d_j}$ la factorización de $\hat{P}(0,U,y)$ en $\mathbb{C}[U,y]$ y sea $g(U,y) = \prod_{1\le j\le a} q_j(U,y)^{d_j-1}$. Entonces para $\alpha \in \mathbb{C}^n$ genérico,*

$$\Big\{\frac{\hat{P}(0,U,\alpha)}{g(U,\alpha)}, \frac{-\frac{\partial \hat{P}}{\partial U}(0,U,\alpha)}{g(U,\alpha)}, \frac{\frac{\partial \hat{P}}{\partial y_1}(0,U,\alpha)}{g(U,\alpha)}, \ldots, \frac{\frac{\partial \hat{P}}{\partial y_n}(0,U,\alpha)}{g(U,\alpha)}\Big\}$$

es una resolución geométrica de un conjunto finito que contiene a $\Pi(\pi(V \cap \{t=0\}))$.

Demostración: Para empezar notemos que como $\hat{P}(t,U,y)$ no tiene factores en $\mathbb{C}[t]$, $\hat{P}(0,U,y)$ no es idénticamente nulo.

Sea $\{z_1,\ldots,z_p\} = \pi(V \cap \{t=0\}) \subset \mathbb{A}^n \times \mathbb{P}^{s-1}$. Como para $1 \le j \le p$, $(0,z_j) \in V$, por el Lema 2.15 tenemos que $\hat{P}(0,\ell(\Pi(z_j),\beta),\beta) = 0$ para todo $\beta \in \mathbb{C}^n$. Esto es equivalente a que el polinomio $U - \ell(\Pi(z_j),\beta)$ divide a $\hat{P}(0,U,\beta)$ en $\mathbb{C}[U]$ para todo $\beta \in \mathbb{C}^n$, que a su vez es equivalente a que el polinomio $U - \ell(\Pi(z_j),y)$ divide a

$\hat{P}(0,U,y)$ en $\mathbb{C}[U,y]$. Podemos suponer entonces que en la expresión $\hat{P}(0,U,y) = \prod_{1\leq j\leq a} q_j(U,y)^{d_j}$, a es mayor o igual a p y $q_j = U - \ell(\Pi(z_j),y)$ para $1 \leq j \leq p$. Por otro lado, tenemos

$$\frac{\partial \hat{P}}{\partial U}(0,U,y) = \sum_{1\leq j\leq a} d_j q_j(U,y)^{d_j-1} \frac{\partial q_j}{\partial U}(U,y) \prod_{\substack{1\leq j'\leq a \\ j'\neq j}} q_{j'}(U,y)^{d_{j'}},$$

y para $1 \leq k \leq n$,

$$\frac{\partial \hat{P}}{\partial y_k}(0,U,y) = \sum_{1\leq j\leq a} d_j q_j(U,y)^{d_j-1} \frac{\partial q_j}{\partial y_k}(U,y) \prod_{\substack{1\leq j'\leq a \\ j'\neq j}} q_{j'}(U,y)^{d_{j'}}.$$

Entonces

$$\frac{\hat{P}(0,U,y)}{g(U,y)} = \prod_{1\leq j\leq a} q_j(U,y), \qquad \frac{\frac{\partial \hat{P}}{\partial U}(0,U,y)}{g(U,y)} = \sum_{1\leq j\leq a} d_j \frac{\partial q_j}{\partial U}(U,y) \prod_{\substack{1\leq j'\leq a \\ j'\neq j}} q_{j'}(U,y),$$

y para $1 \leq k \leq n$,

$$\frac{\frac{\partial \hat{P}}{\partial y_k}(0,U,y)}{g(U,y)} = \sum_{1\leq j\leq a} d_j \frac{\partial q_j}{\partial y_k}(U,y) \prod_{\substack{1\leq j'\leq a \\ j'\neq j}} q_{j'}(U,y).$$

Sea $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{C}^n$ tal que para $1 \leq j \leq a$, $q_j(U,\alpha)$ tiene el mismo grado que $q_j(U,y)$ y es libre de cuadrados, y para $1 \leq j_1 < j_2 \leq a$, los polinomios $q_{j_1}(U,\alpha)$ y $q_{j_2}(U,\alpha)$ son coprimos en $\mathbb{C}[U]$. Estas condiciones se cumplen para valores de α genéricos ya que son equivalentes a que no se anulen los coeficientes principales de los polinomios q_j (pensados como polinomios en U) ni tampoco un conjunto de polinomios no nulos en $\mathbb{C}[y]$ formado por polinomios resultantes. En ese caso,

$$\frac{\hat{P}(0,U,\alpha)}{g(U,\alpha)} = \prod_{1\leq j\leq a} q_j(U,\alpha)$$

es libre de cuadrados y tiene a $\ell(\Pi(z_1),\alpha),\ldots,\ell(\Pi(z_p),\alpha)$ entre sus raíces. Además, para $1 \leq j \leq p$, $1 \leq k \leq n$, $\frac{\partial q_j}{\partial U}(U,y) = 1$ y $\frac{\partial q_j}{\partial y_k}(U,y) = -\Pi(z_j)_k$,. Luego, tenemos que

$$\frac{\frac{\partial \hat{P}}{\partial U}(0,U,y)}{g(U,y)}(\ell(\Pi(z_j),\alpha),\alpha) = d_j \prod_{\substack{1\leq j'\leq a \\ j'\neq j}} q_{j'}(\ell(\Pi(z_j),\alpha),\alpha) \neq 0$$

y

$$\frac{\frac{\partial \hat{P}}{\partial y_k}(0,U,y)}{g(U,y)}(\ell(\Pi(z_j),\alpha),\alpha) = -d_j\Pi(z_j)_k \prod_{\substack{1\le j'\le a\\ j'\neq j}} q_{j'}(\ell(\Pi(z_j),\alpha),\alpha),$$

lo que prueba la proposición. □

El siguiente lema nos será útil en las Secciones 2.5.2 y 2.5.3 para desarrollar la contraparte algorítmica de estos resultados.

Lema 2.17 *Siguiendo la notación en (2.7), el grado en t del polinomio $\hat{P}(t,U,y)$ es menor o igual a $n\tilde{\delta}$.*

Demostración: Para $\beta = (\beta_0,\beta_1,\ldots,\beta_n) \in \mathbb{C}^{n+1}$, definimos $\hat{P}_\beta(t) = \hat{P}(t,\beta)$. Para β genérico, $\deg \hat{P}_\beta = \deg_t \hat{P}(t,U,y)$ y $\hat{P}_\beta$ es libre de cuadrados por ser $\hat{P}(t,U,y)$ libre de cuadrados; luego, si Φ es el morfismo definido en el Lema 2.15, $\deg \hat{P}_\beta$ es igual a la cantidad de elementos en el conjunto $\overline{\mathrm{Im}\Phi} \cap \{U = \beta_0, y_1 = \beta_1, \ldots, y_n = \beta_n\}$.

Como $\dim \overline{\mathrm{Im}\Phi} = n+1$, existe una variedad Z de dimensión menor o igual a n tal que $\overline{\mathrm{Im}\Phi} = \mathrm{Im}\Phi \cup Z$. Observemos además que, para todo $t_0 \in \mathbb{C}$, la variedad $\overline{\mathrm{Im}\Phi} \cap \{t = t_0\}$ es vacía o de dimensión n, ya que $\overline{\mathrm{Im}\Phi}$ no tiene componentes irreducibles contenidas en hiperplanos del tipo $\{t = t_0\}$. Consideremos el conjunto $T = \{t_0 \in \mathbb{C} \mid \hat{V}$ tiene componentes irreducibles incluidas en $\{t = t_0\}\}$. Entonces, a partir de la descomposición de $\overline{\mathrm{Im}\Phi}$ como

$$\overline{\mathrm{Im}\Phi} = Z \bigcup \Big(\mathrm{Im}\Phi \bigcap \Big(\bigcup_{t_0\in T} \{t = t_0\}\Big)\Big) \bigcup \Big(\mathrm{Im}\Phi \bigcap \Big(\bigcap_{t_0\in T} \{t \neq t_0\}\Big)\Big)$$

podemos concluir que para β genérico,

$$\overline{\mathrm{Im}\Phi} \bigcap \Big\{U = \beta_0, y_1 = \beta_1, \ldots, y_n = \beta_n\Big\} =$$

$$= \mathrm{Im}\Phi \bigcap \Big(\bigcap_{t_0\in T} \{t \neq t_0\}\Big) \bigcap \Big\{U = \beta_0, y_1 = \beta_1, \ldots, y_n = \beta_n\Big\}.$$

Veamos ahora que podemos acotar la cantidad de elementos en $\mathrm{Im}\Phi \cap (\cap_{t_0\in T}\{t \neq t_0\}) \cap \{U = \beta_0, y_1 = \beta_1, \ldots, y_n = \beta_n\}$ para β genérico por la cantidad de soluciones

aisladas del sistema

$$\begin{cases} F_1(t,x) &= 0, \\ &\vdots \\ F_s(t,x) &= 0, \\ F_{s+1}(t,x,\mu) &= 0, \\ &\vdots \\ F_r(t,x,\mu) &= 0, \\ \ell_{(\beta_1,\ldots,\beta_n)}(x) - \beta_0 &= 0. \end{cases} \tag{2.8}$$

Para cada elemento $(t_1,\beta) \in \mathrm{Im}\Phi \cap (\cap_{t_0 \in T}\{t \neq t_0\}) \cap \{U = \beta_0, y_1 = \beta_1, \ldots, y_n = \beta_n\}$, existe un elemento $(t_1, x_1, \mu_1) \in V$ tal que $\ell_{(\beta_1,\ldots,\beta_n)}(x) = \beta_0$, por lo tanto, (t_1, x_1, μ_1) es una solución del sistema (2.8) con $t_1 \neq t_0$ para todo $t_0 \in T$.

Si $\hat{P}_\beta$ no es idénticamente nulo, la variedad V no tiene componentes incluidas en $\{\ell_{(\beta_1,\ldots,\beta_n)}(x) = \beta_0\}$ (y luego $V \cap \{\ell_{(\beta_1,\ldots,\beta_n)}(x) = \beta_0\}$ es una variedad 0-dimensional). Esto es así ya que la proyección de cada componente de V en la coordenada t es dominante y, si $(\tilde{t},\tilde{x},\tilde{\mu}) \in V \cap \{\ell_{(\beta_1,\ldots,\beta_n)}(x) = \beta_0\}$, entonces $(\tilde{t},\beta) = \Phi(\tilde{t},\tilde{x},\tilde{\mu},\beta_1,\ldots,\beta_n) \in \mathrm{Im}\Phi$ y, por lo tanto, $\hat{P}_\beta(\tilde{t}) = 0$.

Dividimos entonces el conjunto de soluciones del sistema (2.8) en aquéllas para las que $t = t_0$ para algún $t_0 \in T$ y aquéllas para las que $t \neq t_0$ para todo $t_0 \in T$. Como las soluciones en el segundo grupo son elementos de $V \cap \{\ell_{(\beta_1,\ldots,\beta_n)}(x) = \beta_0\}$, solo hay finitas de estas soluciones y, por lo tanto, son soluciones aisladas del sistema (2.8).

Para finalizar la demostración, veamos que el sistema (2.8) tiene a lo sumo $n\tilde{\delta}$ soluciones aisladas. Consideremos las homogeinizaciones de los polinomios que definen a este sistema considerando tres juegos de variables, uno formado solamente por la variable t, otro formado por las variables x y otro formado por las variables μ. Los multigrados correspondientes a estos polinomios son $(1,\tilde{d}_i,0)$ para $1 \leq i \leq s$, $(1,\tilde{d}_i,1)$ para $s+1 \leq i \leq r$ y $(0,1,0)$ y, por el Teorema de Bézout Multihomogéneo, el grado de la variedad que definen en $\mathbb{P}^1 \times \mathbb{P}^n \times \mathbb{P}^{s-1}$ está acotado por

$$\sum_{(E_t,E_x,E_\mu)} \prod_{k \in E_x} \tilde{d}_k$$

donde $\tilde{d}_{r+1} = 1$ y la terna (E_t, E_x, E_μ) recorre todas las particiones de $\{1,\ldots,r+1\}$ en conjuntos E_t, E_x y E_μ de cardinal $1, n$ y $s-1$ respectivamente, con $E_t \subset \{1,\ldots,r\}$ y $E_\mu \subset \{s+1,\ldots,r\}$. Cada una de estas ternas puede conseguirse de manera única a partir de un subconjunto E de $\{s+1,\ldots,r\}$ de cardinal $n-s$ y de un

elemento $e \in \{1,\dots,s\} \cup E$ tomando $E_t = \{e\}, E_x = (\{1,\dots,s,r+1\} \cup E) \setminus \{e\}$ y $E_\mu = \{s+1,\dots,r\} \setminus E$. Finalmente

$$\sum_{(E_t,E_x,E_\mu)} \prod_{k\in E_x} \tilde{d}_k \;=\; \sum_{(E,e)} \prod_{k\in(\{1,\dots,s,r+1\}\cup E)\setminus\{e\}} \tilde{d}_k \;\le\; \sum_{(E,e)} \prod_{k\in\{1,\dots,s\}\cup E} \tilde{d}_k \;\le\; n\tilde{\delta}.$$

□

2.5.2. Deformación de tipo 1

En esta sección definiremos sistemas iniciales particulares que cumplen la Hipótesis 2.9, a los que llamaremos *sistemas iniciales de tipo 1*. Exhibiremos un algoritmo para calcular una resolución geométrica como en la Proposición 2.16 cuando se utiliza alguno de estos sistemas iniciales. Cuando usemos este algoritmo, diremos que la resolución geométrica fue obtenida aplicando *deformaciones de tipo 1*.

Sistemas iniciales de tipo 1

Definición 2.18 *Llamamos* sistema inicial de tipo 1 *a un sistema del siguiente tipo:*

$$\begin{cases} g_i(x) = \displaystyle\prod_{1\le j\le d_i} (x_i - j) & \text{para } 1 \le i \le s, \\ g_i(x,\mu) = \Big(\displaystyle\prod_{1\le j\le d_i} \phi_{ij}(x)\Big)\psi_i(\mu) & \text{para } s+1 \le i \le r, \end{cases}$$

donde para $s+1 \le i \le r$ *y* $1 \le j \le d_i$,

$$\phi_{ij}(x) = \Big(\sum_{s+1\le k\le n} \frac{1}{(i-s-1)d+j-1+k-s} x_k\Big) + \frac{1}{(i-s-1)d+j-1+n+1-s},$$

$$y \quad \psi_i(\mu) = \sum_{1\le k\le s} \frac{1}{i-s-1+k}\mu_k.$$

Recordemos que $d \ge 2$ es una cota superior para $d_1,\dots,d_r$. Además, podemos observar que, siguiendo la notación dada en la Hipótesis 2.9, en el caso de estos sistemas iniciales tenemos $\tilde{d}_i = d_i$ para $1 \le i \le r$ y $\tilde{\delta} = \delta$.

Lema 2.19 *Los sistemas iniciales de tipo 1 satisfacen la Hipótesis 2.9.*

Demostración: Claramente estos sistemas satisfacen las dos primeras condiciones de dicha hipótesis. Veamos que cumplen también la tercera condición.

Sean $g_1, \ldots, g_r$ como en la Definición 2.18 y sea $(\bar{x}_1, \ldots, \bar{x}_n, \bar{\mu}_1, \ldots, \bar{\mu}_{s-1}) \in \mathbb{A}^{n+s-1}$ una solución del sistema $g_1 = \cdots = g_s = \bar{g}_{s+1} = \cdots = \bar{g}_r = 0$. Notemos que en este sistema las primeras s variables solamente aparecen en las primeras s ecuaciones y las restantes $n-1$ variables solamente aparecen en las restantes $n-1$ ecuaciones. Además, para $1 \leq i \leq s$, $\bar{x}_i$ debe ser alguna de las d_i raíces del polinomio g_i. Luego, estas $\prod_{1 \leq i \leq s} d_i$ soluciones $(\bar{x}_1, \ldots, \bar{x}_s)$ se combinan con las soluciones $(\bar{x}_{s+1}, \ldots, \bar{x}_n, \bar{\mu}_1, \ldots, \bar{\mu}_{s-1})$ del sistema $\bar{g}_{s+1} = \cdots = \bar{g}_r = 0$. Nos enfocamos ahora en este nuevo sistema, debemos ver que tiene $\sum_{E \subset \{s+1,\ldots,r\}, \#E = n-s} \prod_{k \in E} d_k$ soluciones distintas en $\mathbb{A}^{n-1}$.

Para $s+1 \leq i \leq r$, $\bar{g}_i$ es un producto de d_i funciones lineales $\phi_{ij}(x_{s+1}, \ldots, x_n)$ y la función lineal $\bar{\psi}_i(\mu_1, \ldots, \mu_{s-1}) := \psi_i(\mu_1, \ldots, \mu_{s-1}, 1)$; entonces toda solución $(\bar{x}_{s+1}, \ldots, \bar{x}_n, \bar{\mu}_1, \ldots, \bar{\mu}_{s-1})$ debe anular al menos una de estas d_i+1 funciones lineales para cada i. Supongamos que, en total, se anulan a funciones lineales $\phi_{ij}(x)$ y $b \geq r-s-a$ funciones lineales $\bar{\psi}_i(\mu)$. Si estas a funciones lineales son $\phi_{i_l j_l}$ para $1 \leq l \leq a$, entonces $(\bar{x}_{s+1}, \ldots, \bar{x}_n, 1)$ es un vector no nulo en el núcleo de la siguiente matriz de Cauchy en $\mathbb{Q}^{a \times (n-s+1)}$:

$$\begin{pmatrix} \frac{1}{(i_1-s-1)d+j_1-1+1} & \frac{1}{(i_1-s-1)d+j_1-1+2} & \cdots & \frac{1}{(i_1-s-1)d+j_1-1+n+1-s} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{(i_a-s-1)d+j_a-1+1} & \frac{1}{(i_a-s-1)d+j_a-1+2} & \cdots & \frac{1}{(i_a-s-1)d+j_a-1+n+1-s} \end{pmatrix}. \tag{2.9}$$

Como esta matriz tiene rango $\min\{a, n-s+1\}$, la existencia de este vector implica que $n-s \geq a$. A su vez, supongamos que las b ecuaciones lineales $\bar{\psi}_i(\mu)$ que se anulan son $\bar{\psi}_{i'_l}(\mu)$ para $1 \leq l \leq b$, entonces $(\bar{\mu}_1, \ldots, \bar{\mu}_{s-1}, 1)$ es un vector no nulo en el núcleo de la siguiente matriz de Cauchy en $\mathbb{Q}^{b \times s}$:

$$\begin{pmatrix} \frac{1}{i'_1-s-1+1} & \frac{1}{i'_1-s-1+2} & \cdots & \frac{1}{i'_1-s-1+s} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{i'_b-s-1+1} & \frac{1}{i'_b-s-1+2} & \cdots & \frac{1}{i'_b-s-1+s} \end{pmatrix}. \tag{2.10}$$

Nuevamente, como esta matriz tiene rango $\min\{b, s\}$, la existencia de este vector implica que $s-1 \geq b$. Como $a+b \geq r-s = n-1 = (n-s)+(s-1) \geq a+b$, entonces tenemos que $a = n-s$ y $b = s-1$. Esto nos dice que para $s+1 \leq i \leq r$, $(\bar{x}_{s+1}, \ldots, \bar{x}_n, \bar{\mu}_1, \ldots, \bar{\mu}_{s-1})$ anula exactamente una de las d_i+1 funciones lineales que definen a $\bar{g}_i$.

El número $\sum_{E\subset\{s+1,\dots,r\},\#E=n-s}\prod_{k\in E} d_k$ proviene de elegir el subconjunto de $n-s$ de las ecuaciones $\bar{g}_i = 0$ en las que se anula una función lineal correspondiente a las variables x y luego, dentro de cada ecuación, cuál es el factor que se anula. En las demás $s-1$ ecuaciones debe anularse la ecuación lineal correspondiente a las variables μ. Cualquier sistema de este tipo en las variables $x_{s+1},\dots,x_n,\mu_1,\dots,\mu_{s-1}$ determina un único punto en $\mathbb{A}^{n-1}$, ya que las matrices de Cauchy involucradas son inversibles.

Veamos ahora que todas las soluciones del sistema $g_1 = \cdots = g_s = \bar{g}_{s+1} = \cdots = \bar{g}_r = 0$ obtenidas de esta manera son distintas. Más aún, veamos que dos tales soluciones $(\bar{x}_1^{(1)},\dots,\bar{x}_n^{(1)},\bar{\mu}_1^{(1)},\dots,\bar{\mu}_{s-1}^{(1)})$, $(\bar{x}_1^{(2)},\dots,\bar{x}_n^{(2)},\bar{\mu}_1^{(2)},\dots,\bar{\mu}_{s-1}^{(2)})$ verifican $(\bar{x}_1^{(1)},\dots,\bar{x}_n^{(1)}) \neq (\bar{x}_1^{(2)},\dots,\bar{x}_n^{(2)})$. De no ser así, tenemos que $(\bar{x}_1^{(1)},\dots,\bar{x}_s^{(1)}) = (\bar{x}_1^{(2)},\dots,\bar{x}_s^{(2)})$; esto implica, por la manera en que todas las soluciones fueron obtenidas, que elecciones distintas de las $n-s$ funciones lineales $\phi_{i_l j_l}$ llevaron al mismo valor de $(\bar{x}_{s+1},\dots,\bar{x}_n) := (\bar{x}_{s+1}^{(1)},\dots,\bar{x}_n^{(1)}) = (\bar{x}_{s+1}^{(2)},\dots,\bar{x}_n^{(2)})$. Entonces el vector $(\bar{x}_{s+1},\dots,\bar{x}_n,1)$ anula al menos $n-s+1$ funciones lineales $\phi_{i_l j_l}$, lo cual es es imposible ya que cualesquiera $n-s+1$ de estas funciones lineales definen una matriz de Cauchy como en (2.9) que resulta inversible.

Finalmente veamos que la matriz diferencial del sistema $g_1 = \cdots = g_s = \bar{g}_{s+1} = \cdots = \bar{g}_r = 0$ evaluada en cualquier solución del mismo es inversible. Estas matrices tienen arriba a la izquierda un bloque diagonal de $s\times s$ con elementos no nulos en su diagonal. Arriba a la derecha y abajo a la izquierda tiene un bloque de $s\times(r-s)$ y $(r-s)\times s$ ceros respectivamente. De modo que alcanza con probar que el bloque de abajo a la derecha de tamaño $(r-s)\times(r-s)$ resulta inversible. Sea M esta submatriz. Sin pérdida de generalidad, supongamos que $(\bar{x}_{s+1},\dots,\bar{x}_n,\bar{\mu}_1,\dots,\bar{\mu}_{s-1})$ es una solución de $\bar{g}_{s+1} = \cdots = \bar{g}_r = 0$ en la que $(\bar{x}_{s+1},\dots,\bar{x}_n)$ anula las funciones lineales $\phi_{(s+1)1},\dots,\phi_{n1}$ y $(\bar{\mu}_1,\dots,\bar{\mu}_{s-1})$ anula las funciones lineales $\bar{\psi}_{n+1},\dots,\bar{\psi}_r$.

Entonces $M = M_1 M_2$ con $M_1 =$

$$\begin{pmatrix} \psi_{s+1}(\bar{\mu}) \prod_{j=2}^{d_{s+1}} \phi_{(s+1)j}(\bar{x}) & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & & & & \vdots \\ \vdots & & \psi_n(\bar{\mu}) \prod_{j=2}^{d_n} \phi_{nj}(\bar{x}) & & & \vdots \\ \vdots & & & \prod_{j=1}^{d_{n+1}} \phi_{(n+1)j}(\bar{x}) & & \vdots \\ \vdots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & \prod_{j=1}^{d_r} \phi_{rj}(\bar{x}) \end{pmatrix}$$

y $M_2 =$

$$\begin{pmatrix} \phi_{(s+1)1(s+1)} & \cdots & \phi_{(s+1)1n} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \phi_{n1(s+1)} & \cdots & \phi_{n1n} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \psi_{(n+1)1} & \cdots & \psi_{(n+1)(s-1)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \psi_{r1} & \cdots & \psi_{r(s-1)} \end{pmatrix},$$

donde para $s+1 \leq i, k \leq n$, ϕ_{i1k} es el coeficiente que acompaña a x_k en ϕ_{i1} y para $n+1 \leq i \leq r$, $1 \leq k \leq s-1$, ψ_{ik} es el coeficiente que acompaña a μ_k en ψ_i. Como los bloques superior izquierdo en inferior derecho de M_2 son matrices inversibles (de Cauchy), entonces $\det M \neq 0$. ▫

Métodos simbólicos de deformación

Exhibimos a continuación el esquema de un algoritmo probabilístico para calcular una resolución geométrica como en la Proposición 2.16, basado en la aplicación del operador de Newton-Hensel. Para esto, reutilizamos la notación introducida en la Sección 2.5.1. Luego en la proposición siguiente, especificamos cómo llevar a cabo cada paso y analizamos la complejidad total del algoritmo.

Algoritmo 2.20

Input*: Un* slp *que codifica simultáneamente polinomios* $h_1, \ldots, h_r$ *como en (2.6).*

Output*: Una resolución geométrica como en la Proposición 2.16 con* V *definida a partir de un sistema inicial* $g_1, \ldots, g_r$ *como en la Definición 2.18.*

Procedimiento*:*

1. *Calcular todas las soluciones* $s_1, \ldots, s_\delta \in \mathbb{Q}^r$ *del sistema inicial deshomogeneizado* $g_1(x) = \cdots = g_s(x) = \bar{g}_{s+1}(x, \mu) = \cdots = \bar{g}_r(x, \mu) = 0$.

2. *Para* $1 \leq i \leq \delta$*, calcular elementos* $\tilde{S}_i \in \mathbb{K}[t]^r$ *tales que para* $1 \leq k \leq r$*,* $(\tilde{S}_i - S_i)_k \in (t-1)^{2n\delta+1}\mathbb{K}[[t-1]]$.

3. *Elegir un valor de* $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}^n$ *al azar y calcular*

$$P(t, U, y) \mod ((t-1)^{2n\delta+1} + (y_1 - \alpha_1, \ldots, y_n - \alpha_n)^2)\mathbb{K}[[t-1]][U, y].$$

4. *Calcular para* $0 \leq h \leq \delta$*, los polinomios* $p_h(t, \alpha)$ *y* $\frac{\partial p_h}{\partial y_k}(t, \alpha)$*,* $1 \leq k \leq n$.

5. *Calcular* $\hat{P}(0, U, \alpha), \frac{\partial \hat{P}}{\partial U}(0, U, \alpha), \frac{\partial \hat{P}}{\partial y_k}(0, U, \alpha)$ *para* $1 \leq k \leq n$*,* $g(U, \alpha)$ *y hacer las divisiones necesarias.*

Proposición 2.21 *Dado un* slp *de longitud* L_1 *que codifica simultáneamente polinomios* $h_1, \ldots, h_r$ *como en (2.6), el Algoritmo 2.20 calcula probabilísticamente una resolución geométrica como en la Proposición 2.16 con* V *definida a partir de un sistema inicial* $g_1, \ldots, g_r$ *como en la Definición 2.18 con complejidad*

$$O\big(n^2(L_1 + n^2 d + n^2 \log(n) \log^2(d))\delta^2 \log(\delta) \log\log(\delta)\big).$$

Demostración: Calculemos la cantidad de operaciones necesarias en cada paso del algoritmo. Puede observarse luego que la complejidad total del algoritmo es la dada en el enunciado de esta proposición (utilizando la desigualdad $\delta \leq \binom{n-1}{s-1} d^n \leq (2d)^n$ en la simplificación de algunos términos).

Paso 1: Para obtener cada una de las δ soluciones del sistema debemos resolver un sistema cuadrado de $n - s$ variables y otro de $s - 1$ variables, ambos asociados a matrices de Cauchy. Resolviendo estos sistemas mediante el algoritmo [BP94, Chapter 2, Algorithm 4.2], tenemos que este paso requiere $O(n \log^2(n)\delta)$ operaciones en $\mathbb{Q}$.

Paso 2: En la demostración de la Proposición 2.13 usamos [HKP+00, Lemma 3] para probar la existencia de elementos $S_i \in \mathbb{K}[[t-1]]^r$ tales que

$$V^{(e)} = \Big\{\big((S_{i1},\ldots,S_{in}),(S_{i(n+1)} : \cdots : S_{ir} : 1)\big),\ 1 \le i \le \delta\Big\}.$$

La demostración de este lema es constructiva. A continuación, estudiamos en detalle una manera adaptada a nuestro contexto de llevar a cabo los cálculos necesarios para aproximar estos vectores de series de potencias. Sea F la función definida por $F(x,\mu_1,\ldots,\mu_{s-1}) = (F_1(x),\ldots,F_r(x,\mu_1,\ldots,\mu_{s-1},1))$ (ver Definición 2.10). Para cada $1 \le i \le \delta$, consideremos una sucesión de vectores $(\tilde{S}^{(m)})_{m\in\mathbb{N}_0}$ en $\mathbb{K}[t]^r$ y dos sucesiones de matrices $(A^{(m)})_{m\in\mathbb{N}_0}$, $(B^{(m)})_{m\in\mathbb{N}_0}$ en $\mathbb{K}[t]^{r\times r}$ que cumplen las siguientes propiedades:

i) $\tilde{S}^{(0)} = s_i$,

ii) para $m \in \mathbb{N}_0$, las entradas de $\tilde{S}^{(m)}, A^{(m)}$ y $B^{(m)}$ tienen grado menor que 2^m,

iii) $\tilde{S}^{(m+1)} \equiv \tilde{S}^{(m)} \mod (t-1)^{2^m}$,

iv) $F(\tilde{S}^{(m)}) \equiv 0 \mod (t-1)^{2^m}$,

v) $A^{(m)}B^{(m)} \equiv I \mod (t-1)^{2^m}$,

vi) $A^{(m+1)} \equiv DF(\tilde{S}^{(m)}) \mod (t-1)^{2^{m+1}}$.

Las condiciones iii) y iv) implican que la sucesión $(\tilde{S}^{(m)})_{m\in\mathbb{N}_0}$ determina un elemento $\tilde{S} \in \mathbb{K}[[t-1]]^r$ tal que $F(\tilde{S}) = 0$. Como $\tilde{S}(1) = s_i$, tenemos que $\tilde{S} = S_i$.
Para definir estas sucesiones, comenzamos con $A^{(0)} = Dg(s_i)$ y $B^{(0)} = (A^{(0)})^{-1} \in \mathbb{Q}^{r\times r}$, donde $g = (g_1,\ldots,g_s,\bar{g}_{s+1},\ldots,\bar{g}_r)$. Estas matrices pueden calcularse siguiendo la demostración del Lema 2.19 y la cantidad de operaciones necesarias no suma a la complejidad total. Una vez definidos $\tilde{S}^{(m)}, A^{(m)}$ y $B^{(m)}$, procedemos como se explica a continuación.

- Evaluamos primeramente la matriz

$$A^{(m+1)} \equiv DF(\tilde{S}^{(m)}) \mod (t-1)^{2^{m+1}}.$$

  Es fácil ver que los polinomios $g_1,\ldots,g_s,\bar{g}_{s+1},\ldots,\bar{g}_r$ pueden codificarse simultáneamente por un *slp* de longitud $O(dn^2)$; luego los polinomios $F_1,\ldots,F_r$

pueden codificarse simultáneamente por un *slp* de longitud $L_1 + O(dn^2)$ y podemos obtener un *slp* de longitud $O(nL_1 + dn^3)$ que codifique simultáneamente las entradas de la matriz DF. Como las operaciones de suma y multiplicación entre polinomios en $\mathbb{K}[t]$ de grado menor que 2^m pueden ser llevadas a cabo con $O(2^m m \log(m))$ operaciones $\mathbb{K}$ (ver [vzGG99, Chapter 8]), el costo de este paso es $O((nL_1 + dn^3)2^m m \log(m))$.

- Para definir $B^{(m+1)}$ procedemos como se explica a continuación.

  Para $m = 0$, como

  $$A^{(1)} \equiv DF(s_i) \equiv Dg(s_i) \equiv A^{(0)} \mod (t-1),$$

  tenemos que $A^{(1)}B^{(0)} = I + (t-1)U$ para cierta $U \in \mathbb{K}^{r\times r}$; tomamos entonces $B^{(1)} = B^{(0)} - B^{(0)}(t-1)U$.

  Si $m \geq 1$, como

  $$A^{(m+1)} \equiv DF(\tilde{S}^{(m)}) \equiv DF(\tilde{S}^{(m-1)}) \equiv A^{(m)} \bmod (t-1)^{2^{m-1}},$$

  definimos $(t-1)^{2^{m-1}}A' = A^{(m+1)} - A^{(m)}$ y $B' = B^{(m)} - B^{(m)}(t-1)^{2^{m-1}}A'B^{(m)}$. Si $A^{(m)}B^{(m)} = I + (t-1)^{2^m}R$, entonces $A^{(m+1)}B' = I + (t-1)^{2^m}U$ con

  $$U = R - A'B^{(m)}A'B^{(m)} - (t-1)^{2^{m-1}}RA'B^{(m)}.$$

  Por último, definimos $B^{(m+1)} = B' - B'(t-1)^{2^m}U$, con lo cual $A^{(m+1)}B^{(m+1)} = I - (t-1)^{2^{m+1}}U^2$. Luego $B^{(m+1)}$ es la aproximación buscada. Para calcular $B^{(m+1)}$, calculamos las matrices auxiliares $(t-1)^{2^{m-1}}A'$, B' y $(t-1)^{2^m}U = A^{(m+1)}B' - I$ y hacemos las multiplicaciones de matrices necesarias. Esto requiere $O(n^3 2^m m \log(m))$ operaciones en $\mathbb{K}$.

- Finalmente evaluamos

  $$\tilde{S}^{(m+1)} = \tilde{S}^{(m)} - B^{(m+1)}F(\tilde{S}^{(m)}) \tag{2.11}$$

  realizando $O((L_1 + dn^2)2^m m \log(m))$ operaciones en $\mathbb{K}$.

La demostración de que la sucesión $(\tilde{S}^{(m)})_{m\in\mathbb{N}_0}$ satisface la condición iv) es igual a la dada en [HKP$^+$00, Lemma 3], y consecuentemente, por (2.11) se satisface la condición iii). Las demás condiciones se satisfacen trivialmente a partir de las definiciones.

La cantidad de operaciones en $\mathbb{K}$ para calcular $\tilde{S}^{(\lceil \log(2n\delta+1)\rceil)}$ a partir de s_i es

$$O\big((nL_1 + dn^3) \sum_{1\leq m\leq \lceil \log(2n\delta+1)\rceil} 2^m m\log(m)\big) =$$

$$= O\big((n^2L_1 + dn^4)\delta\log(\delta)\log\log(\delta)\big).$$

Como esto debe hacerse para cada i entre 1 y δ, la cantidad de operaciones total en $\mathbb{K}$ de este paso está acotada por $O((n^2L_1 + dn^4)\delta^2\log(\delta)\log\log(\delta))$.

Paso 3: Dado que para $1 \leq i \leq \delta$, se verifica que

$$\tilde{S}_i \equiv S_i \mod (t-1)^{2n\delta+1}\mathbb{K}[[t-1]],$$

si definimos

$$\tilde{P}(t,U,y) = \prod_{1\leq i\leq\delta} \Big(U - \ell\big((\tilde{S}_{i1},\ldots,\tilde{S}_{in}),y\big)\Big) \in \mathbb{K}[t][U,y],$$

tenemos que

$$\tilde{P}(t,U,y) \equiv P(t,U,y) \mod (t-1)^{2n\delta+1}\mathbb{K}[[t-1]][U,y].$$

Luego, si desarrollamos $\tilde{P}$ en potencias de U e $(y_k - \alpha_k)$ para $1 \leq k \leq n$, solamente necesitamos calcular los coeficientes que acompañan a U^h y $U^h(y_k - \alpha_k)$, $0 \leq h \leq \delta$. Considerando entonces a $\tilde{P}$ como un polinomio en U en el que cada coeficiente es una tira de $n+1$ elementos en $\mathbb{K}[t]$ (uno correspondiente a U^h y uno a $U^h(y_k - \alpha_k)$, $1 \leq k \leq n$), podemos efectuar este paso mediante [vzGG99, Algorithm 10.3] efectuando $O(n^2\delta^2\log^3(\delta)\log\log^2(\delta))$ operaciones en $\mathbb{K}$.

Paso 4: En el paso anterior calculamos aproximaciones hasta grado $2n\delta$ de los coeficentes en $\mathbb{K}[[t-1]]$ correspondientes a U^h y $U^h(y_k - \alpha_k)$ para $1 \leq k \leq n$ y $0 \leq h \leq \delta$ en el desarrollo de P en potencias de U e $(y_k - \alpha_k)$. Según la definición de P, estos coeficientes son precisamente,

$$\frac{p_h(t,\alpha)}{q(t)}, \quad \frac{\frac{\partial p_h}{\partial y_k}(t,\alpha)}{q(t)}, \quad 1 \leq k \leq n, \quad 0 \leq h \leq \delta.$$

Dado que en cada una de estas fracciones, el grado en t (y luego en $t-1$) del numerador y el denominador está acotado por $n\delta$, tenemos que todos estos polinomios quedan determinados a partir de las aproximaciones calculadas para las series correspondientes a estas fracciones (ver [vzGG99, Corollary 5.21]). Más aún,

podemos recuperar $p_h(t,\alpha)$, $\frac{\partial p_h}{\partial y_k}(t,\alpha)$ para $1 \leq k \leq n$ y $0 \leq h \leq \delta$ y $q(t)$ con $O(n^2\delta^2 \log^2(\delta) \log\log(\delta))$ operaciones en $\mathbb{K}$ usando [vzGG99, Corollary 5.24 y Algorithm 11.4]. En la reconstrucción del numerador y denominador de cada fracción podrían aparecer distintos denominadores (divisores de $q(t)$) que deben ser llevados al denominador común $q(t)$, pero la cantidad de operaciones requeridas no suma a la complejidad total del paso.

Paso 5: Luego del paso anterior conocemos

$$\hat{P}(0,U,\alpha) = \sum_{0\leq h\leq\delta} p_h(0,\alpha)U^h,$$

$$\frac{\partial \hat{P}}{\partial y_k}(0,U,\alpha) = \sum_{0\leq h\leq\delta} \frac{\partial p_h}{\partial y_k}(0,\alpha)U^h \text{ para } 1 \leq k \leq n,$$

y podemos calcular fácilmente

$$\frac{\partial \hat{P}}{\partial U}(0,U,\alpha) = \sum_{1\leq h\leq\delta} hp_h(0,\alpha)U^{h-1}.$$

Sabemos que para α genérico el polinomio $\frac{\hat{P}(0,U,\alpha)}{g(U,\alpha)}$ es libre de cuadrados; luego podemos calcular $g(U,\alpha)$, salvo por algún factor no nulo en $\mathbb{C}$, como

$$g(U,\alpha) = \gcd\Big(\hat{P}(0,U,\alpha), \frac{\partial \hat{P}}{\partial U}(0,U,\alpha)\Big).$$

Este factor no es importante para definir la resolución geométrica ya que todos los otros polinomios que la componen se dividirán por el valor de $g(U,\alpha)$ calculado. La cantidad de operaciones en $\mathbb{K}$ necesarias en este paso es $O(\delta \log^2(\delta) \log\log(\delta))$. Las divisiones por $g(U,\alpha)$ no modifican esta complejidad. ▫

Adaptación a los casos $s = 1$ y $s = n$

Siguiendo la Definición 2.7, las variedades W_S que utilizaremos para localizar los puntos extremales buscados tienen una fórmula de definición distinta en cada uno de los casos $2 \leq s \leq n-1$, $s = 1$ y $s \geq n$. Hasta aquí hemos desarrollado un algoritmo orientado al primero de estos casos, en el cual los sistemas con los que trabajamos tienen un juego de variables x y un juego de variables μ. La adaptación de este algoritmo al caso $s = 1$ y al caso $s = n$, en los que solamente debemos manejar el juego de variables x y todas las variedades involucradas son variedades afines,

puede hacerse de manera directa. En estos casos, supongamos dado un sistema de ecuaciones

$$h_1(x) = \cdots = h_n(x) = 0 \tag{2.12}$$

formado por polinomios en $\mathbb{K}[x_1, \ldots, x_n]$ tal que, para $1 \leq i \leq n$, $d_i := \deg_x h_i \leq d$. Sea $W \subset \mathbb{A}^n$ la variedad definida por estos polinomios. Por el Teorema de Bézout, sabemos que $\deg W$ está acotado por $\delta := \prod_{1 \leq i \leq n} d_i \leq d^n$.

Para adaptar el algoritmo desarrollado, requeriremos que el sistema inicial $g_1(x), \ldots, g_n(x)$ satisfaga la siguiente hipótesis.

Hipótesis 2.22

1. *Para* $1 \leq i \leq r$, $\tilde{d}_i := \deg g_i \geq d_i$.
2. *La variedad que definen* $g_1, \ldots, g_n$ *en* $\mathbb{A}^n$ *está formada por* $\tilde{\delta}$ *puntos* $s_1, \ldots, s_{\tilde{\delta}}$ *con* $\tilde{\delta} = \prod_{1 \leq i \leq n} \tilde{d}_i$ *y la matriz diferencial del sistema formado por* $g_1, \ldots, g_n$ *evaluada en* s_i *es inversible para todo* $1 \leq i \leq \tilde{\delta}$.

Definición 2.23 *Sea* t *una nueva variable. Para* $1 \leq i \leq n$, *notamos* F_i *al polinomio*

$$F_i = (1-t)h_i + tg_i \in \mathbb{K}[t, x].$$

Definimos $\hat{V} \subset \mathbb{A}^1 \times \mathbb{A}^n$ *como la variedad definida por* $F_1, \ldots, F_n$. *Definimos además* $V^{(0)}$ *como la unión de las componentes irreducibles de* $\hat{V}$ *contenidas en* $\{t = 0\}$, $V^{(1)}$ *como la unión de las componentes irreducibles de* $\hat{V}$ *contenidas en* $\{t = t_0\}$ *para algún* $t_0 \in \mathbb{C} \setminus \{0\}$, *y* V *como la unión de las demás componentes irreducibles de* $\hat{V}$.

Notamos $\pi : \mathbb{A}^1 \times \mathbb{A}^n \to \mathbb{A}^n$ *a la proyección* $(t, x) \mapsto x$. *Con el objetivo de unificar la notación con el caso* $2 \leq s \leq n-1$, *consideramos* $r = n$ *y notamos* $\Pi : \mathbb{A}^n \to \mathbb{A}^n$ *y* $\tilde{\pi} : \mathbb{A}^1 \times \mathbb{A}^n \to \mathbb{A}^1 \times \mathbb{A}^n$ *a las respectivas funciones identidad.*

Es fácil ver que el sistema inicial

$$\begin{cases} g_i(x) = \displaystyle\prod_{1 \leq j \leq d_i} (x_i - j) \quad \text{para } 1 \leq i \leq n, \end{cases} \tag{2.13}$$

satisface la Hipótesis 2.22. Para este caso tenemos $\tilde{\delta} = \delta \leq d^n$ y adaptando lo desarrollado para el caso $2 \leq s \leq n-1$, obtenemos el siguiente resultado.

Proposición 2.24 *Hay un algoritmo probabilístico que, dado un* slp *de longitud L_1 que codifica simultáneamente polinomios $h_1, \ldots, h_n$ como en (2.12), calcula una resolución geométrica de un conjunto finito que contiene a $\pi(V \cap \{t = 0\})$ con complejidad*

$$O\big(n^2(L_1 + n^2 \log(n)d)\delta^2 \log(\delta) \log\log(\delta)\big).$$

Aclaración sobre la notación

En las Secciones 2.6.1 y 2.6.2 aplicaremos deformaciones de tipo 1 a sistemas que definen las variedades W_S (ver Definición 2.7) para distintos $S \subset \{1, \ldots, m\}$ con $1 \leq \#S \leq n$. Luego, para cada tal S notaremos $\hat{V}_S$, $V_S^{(0)}$, $V_S^{(1)}$ y V_S a las variedades de las Definiciones 2.10 y 2.23 cuando $h_1, \ldots, h_r$ son los polinomimos que definen W_S.

2.5.3. Deformación de tipo 2

En esta sección definiremos otros sistemas iniciales que cumplen la Hipótesis 2.9, a los que llamaremos *sistemas iniciales de tipo 2*. Al igual que en la Sección 2.5.2, daremos un algoritmo para calcular una resolución geométrica como en la Proposición 2.16 cuando se utiliza alguno de estos sistemas iniciales. Cuando usemos este algoritmo, diremos que la resolución geométrica fue obtenida aplicando *deformaciones de tipo 2*.

La complejidad de este algoritmo será mayor que la del algoritmo correspondiente cuando utilizamos sistemas de tipo 1, pero la razón por la que definimos estas nuevas deformaciones es que, al aplicarlas a los sistemas que consideraremos para caracterizar puntos extremales para la primera función coordenada ((2.3), (2.4) y (2.5)), se satisfacen ciertas propiedades geométricas que utilizaremos en las Secciones 2.6.3 y 2.6.4.

Sistemas iniciales de tipo 2

A diferencia de los sistemas iniciales que hemos llamado de tipo 1, los sistemas iniciales de tipo 2 dependerán de ciertos parámetros que especificaremos en la Sección 2.6 según la necesidad de cada caso.

Sea $\tilde{d} = 2\lceil \frac{d}{2} \rceil$, es decir, el menor entero par mayor o igual a d (recordemos que d es una cota para el grado de los polinomios del sistema dado (2.6)). Sea $T = T_{\tilde{d}}$

el polinomio de Tchebychev de grado $\tilde{d}$. Para $1 \leq i \leq s$, sea $\tau_i \in \{0,1\}$ y sean $0 \leq a_1 < \ldots < a_s$ números enteros tales que $q := a_s + n + 1$ es un número primo.

Definición 2.25 *Llamamos* sistema inicial de tipo 2 *a un sistema del siguiente tipo:*

$$\begin{cases} g_i(x) = (-1)^{\tau_i}\Big(n + \dfrac{1}{a_i+n+1} + \displaystyle\sum_{1\leq k\leq n} \frac{1}{a_i+k}T(x_k)\Big) & \text{para } 1 \leq i \leq s, \\ g_i(x,\mu) = \displaystyle\sum_{1\leq j\leq s} \mu_j \frac{\partial g_j}{\partial x_{i-s+1}}(x) & \text{para } s+1 \leq i \leq r, \end{cases}$$

Los sistemas de tipo 2 quedan completamente determinados al fijar los números $a_1, \ldots, a_s$ y $\tau_1, \ldots, \tau_s$. Observamos que si $\tau_i = 0$, entonces $g_i(x)$ es estrictamente positivo en $\mathbb{R}^n$ y si $\tau_i = 1$, entonces $g_i(x)$ es estrictamente negativo en $\mathbb{R}^n$. Notemos además que para estos sistemas, $\tilde{\delta} = \binom{n-1}{s-1}\tilde{d}^s(\tilde{d}-1)^{n-s} < \binom{n-1}{s-1}\tilde{d}^n$.

Por otro lado, podemos notar también que si para $1 \leq k \leq n+1$, definimos $b_k = -k$ y consideramos la matriz de Cauchy $A = (A_{ik})_{1\leq i\leq s, 1\leq k\leq n+1} = (\frac{1}{a_i - b_k})_{1\leq i\leq s, 1\leq k\leq n+1} \in \mathbb{Q}^{s\times(n+1)}$, para $1 \leq i \leq s$,

$$g_i(x) = (-1)^{\tau_i}\Big(n + A_{i(n+1)} + \sum_{1\leq k\leq n} A_{ik}T(x_k)\Big),$$

mientras que para $s+1 \leq i \leq r$,

$$g_i(x,\mu) = T'(x_{i-s+1})\Big(\sum_{1\leq j\leq s} A_{j(i-s+1)}\mu_j(-1)^{\tau_j}\Big). \tag{2.14}$$

A continuación empezamos a estudiar las propiedades de los sistemas iniciales de tipo 2.

Lema 2.26 *Los sistemas iniciales de tipo 2 satisfacen la Hipótesis 2.9.*

Demostración: Claramente estos sistemas satisfacen las dos primeras condiciones de dicha hipótesis. Veamos que cumplen también la tercera condición.

Sean $g_1, \ldots, g_r$ como en la Definición 2.25; recordemos que, para $s+1 \leq i \leq r$, notamos $\bar{g}_i$ al polinomio definido por $\bar{g}_i(x, \mu_1, \ldots, \mu_{s-1}) = g_i(x, \mu_1, \ldots, \mu_{s-1}, 1)$. La idea de la demostración será descomponer la variedad definida por $g_1, \ldots, g_s, \bar{g}_{s+1}, \ldots, \bar{g}_r$ en $\mathbb{A}^r$ en varias subvariedades finitas y estudiar separadamente cada una de estas subvariedades.

Sea $B \subset \{2, \dots, n\}$ con $\#B = n - s$, sea $e : B \to \{-1, 1\}$ y supongamos que $e(k) = 1$ para a elementos de B. Sea $S_{B,e}$ el conjunto de soluciones $(\bar{x}, \bar{\mu}) = (\bar{x}_1, \dots, \bar{x}_n, \bar{\mu}_1, \dots, \bar{\mu}_{s-1})$ del sistema

$$g_1(x) = \cdots = g_s(x) = \bar{g}_{s+1}(x, \mu) = \bar{g}_r(x, \mu) = 0 \tag{2.15}$$

que además satisfacen las condiciones

$$T'(x_k) = 0 \text{ y } T(x_k) = e(k) \text{ para todo } k \in B. \tag{2.16}$$

Calculemos la cantidad de elementos en $S_{B,e}$. Sin pérdida de generalidad, supongamos que $B = \{s + 1, \dots, n\}$. Dado que $\gcd(T', T + 1) = T_{\tilde{d}/2}$ y $\gcd(T', T - 1) = T'/T_{\tilde{d}/2}$, concluimos que la cantidad de $(n-s)$-uplas $(\bar{x}_{s+1}, \dots, \bar{x}_n)$ que satisfacen la condición (2.16) es $(\tilde{d}/2)^{n-s-a}(\tilde{d}/2 - 1)^a$. Veamos que cada uno de estos elementos puede extenderse a una solución $(\bar{x}, \bar{\mu})$ del sistema (2.15) de $\tilde{d}^s$ maneras distintas.

Sea $A' \in \mathbb{Q}^{s \times s}$ la matriz formada por las primeras s columnas de A. Las condiciones $g_1(x) = \cdots = g_s(x) = 0$, sumadas a la condición (2.16), implican

$$A' \begin{pmatrix} T(x_1) \\ \vdots \\ T(x_s) \end{pmatrix} = - \begin{pmatrix} n + A_{1(n+1)} + \displaystyle\sum_{s+1 \le k \le n} A_{1k} e(k) \\ \vdots \\ n + A_{s(n+1)} + \displaystyle\sum_{s+1 \le k \le n} A_{sk} e(k) \end{pmatrix}, \tag{2.17}$$

y la matriz A' es una matriz de Cauchy inversible. Veamos que en cada solución $(\bar{x}_1, \dots, \bar{x}_s)$ de (2.17), $T(\bar{x}_{k_0}) \neq \pm 1$ para $1 \le k_0 \le s$.

Para $1 \le k_0 \le s < k \le n + 1$, sea $A'_{(k_0|k)}$ la matriz de Cauchy que se obtiene reemplazando la k_0-ésima columna de A' por la k-ésima columna de A, $A'_{(k_0|0)}$ la matriz que se obtiene reemplazando la k_0-ésima columna de A' por un vector columna con el valor 1 en todas sus entradas y, para $1 \le i \le s$, A''_{ik_0} la matriz de Cauchy que se obtiene eliminando la i-ésima fila y la k_0-ésima columna de A'. Utilizando la regla de Cramer, sabemos que toda solución de (2.17) verifica

$$T(x_{k_0}) = \frac{-1}{\det(A')} \Big(n \det\left(A'_{(k_0|0)}\right) + \det\left(A'_{(k_0|n+1)}\right) + \sum_{s+1 \le k \le n} e(k) \det\left(A'_{(k_0|k)}\right) \Big).$$

Si calculamos $\det(A')$ con la fórmula para el determinante de una matriz de Cauchy (ver Sección 0.4.1), notamos que su numerador y denominador son coprimos con q, ya que cada elemento en cada productoria es un número entero no nulo de valor absoluto

menor a q. Análogamente, para $s+1 \leq k \leq n$, el numerador y el denominador de $\det(A'_{(k_0|k)})$ son coprimos con q. Por otro lado, el numerador de $\det(A'_{(k_0|n+1)})$ es coprimo con q pero el denominador es un múltiplo de q. Por último, desarrollando por la k_0-ésima columna, tenemos que

$$\det\left(A'_{(k_0|0)}\right) = \sum_{0\leq i\leq s} (-1)^{i+k_0} \det\left(A''_{ik_0}\right),$$

y cada $\det(A''_{ik_0})$ es un número racional con numerador y denominador coprimos con q. Todo esto nos permite concluir que $T(x_{k_0})$ se puede escribir como una suma de números racionales en la que en un sumando el numerador es coprimo con q, el denominador es múltiplo de q, y en todos los demás sumandos el numerador y el denominador son coprimos con q. Esto implica que $T(x_{k_0})$ es un número racional en cuya expresión irreducible el denominador es múltiplo del primo q, y por lo tanto $T(x_{k_0}) \neq \pm 1$.

Para cada $1 \leq k_0 \leq s$, habrá exactamente $\tilde{d}$ valores de $\bar{x}_{k_0}$ en los cuales el polinomio T tome el valor obtenido despejando en (2.17). Esto es así pues los únicos valores que toma el polinomio T con multiplicidad mayor a 1 son ± 1, que hemos visto que no son los valores obtenidos para $T(\bar{x}_{k_0})$.

Sea ahora $(\bar{x}_1, \ldots, \bar{x}_n)$ una solución de (2.16) y (2.17); veamos que puede extenderse de una única manera a una solución $(\bar{x}, \bar{\mu})$ de (2.15). Como $T'(\bar{x}_k) = 0$ para $s+1 \leq k \leq n$, las ecuaciones $\bar{g}_i(x,\mu) = 0$ se satisfacen trivialmente para $2s \leq i \leq r$ (ver (2.14). Para $1 \leq k_0 \leq s$, como $T(\bar{x}_{k_0}) \neq \pm 1$, entonces $T'(\bar{x}_{k_0}) \neq 0$; por lo tanto las condiciones $\bar{g}_{s+1}(x,\mu) = \cdots = \bar{g}_{2s-1}(x,\mu) = 0$ son equivalentes a

$$\begin{pmatrix} A_{12} & \cdots & A_{(s-1)2} \\ \vdots & \ddots & \vdots \\ A_{1s} & \cdots & A_{(s-1)s} \end{pmatrix} \begin{pmatrix} \mu_1(-1)^{\tau_1} \\ \vdots \\ \mu_{s-1}(-1)^{\tau_{s-1}} \end{pmatrix} = -(-1)^{\tau_s} \begin{pmatrix} A_{s2} \\ \vdots \\ A_{ss} \end{pmatrix}, \tag{2.18}$$

que tiene una única solución.

Observemos que, como para $(\bar{x}, \bar{\mu}) \in S_{B,e}$, $T(\bar{x}_k) = e(k) = \pm 1$ para todo $k \in B$, al probar que $T(\bar{x}_k) \neq \pm 1$ para $k \notin B$, probamos también que los conjuntos $S_{B,e}$ son disjuntos y que para cualquier par $(\bar{x}^{(1)}, \bar{\mu}^{(1)}), (\bar{x}^{(2)}, \bar{\mu}^{(2)})$ de soluciones de (2.15) construidas de esta manera se verifica que $\bar{x}^{(1)} \neq \bar{x}^{(2)}$. Por otro lado, notemos que recorriendo todos los posibles $B \subset \{2, \ldots, n\}$, todos los valores de a entre 0 y $n-s$ y todas las funciones $e : B \to \{-1, 1\}$ que toman el valor 1 en a elementos de B,

hemos encontrado un total de

$$\binom{n-1}{n-s}\sum_{0\le a\le n-s}\binom{n-s}{a}\Big(\frac{\tilde{d}}{2}\Big)^{n-s-a}\Big(\frac{\tilde{d}}{2}-1\Big)^{a}\tilde{d}^{s}=\binom{n-1}{n-s}\big(\tilde{d}-1\big)^{n-s}\tilde{d}^{s}=\tilde{\delta}$$

soluciones al sistema (2.15).

Probemos ahora que la matriz diferencial de este sistema evaluada en cada una de estas $\tilde{\delta}$ soluciones es inversible. Sin pérdida de generalidad, supongamos que $(\bar{x},\bar{\mu})$ es una solución correspondiente a $B=\{s+1,\dots,n\}$. Dividimos a la matriz diferencial del sistema (2.15) en nueve bloques de la siguiente manera:

$$\begin{array}{cc} s & \{ \\ s-1 & \{ \\ n-s & \{ \end{array}\left(\begin{array}{c|c|c} \text{I} & \text{II} & \text{III} \\ \hline \text{IV} & \text{V} & \text{VI} \\ \hline \text{VII} & \text{VIII} & \text{IX} \end{array}\right). \qquad \begin{array}{ccc} \overbrace{}^{s} & \overbrace{}^{n-s} & \overbrace{}^{s-1} \end{array}$$

Para probar lo afirmado, alcanza con ver que los bloques II, III y V son bloques de ceros y que los bloques I, VI y VIII son inversibles.

El bloque (I | II) corresponde a la matriz $((-1)^{\tau_i}A_{ik}T'(\bar{x}_k))_{1\le i\le s,1\le k\le n}$. Luego I es la matriz inversible

$$\begin{pmatrix} (-1)^{\tau_1} & & 0 \\ & \ddots & \\ 0 & & (-1)^{\tau_s} \end{pmatrix}\begin{pmatrix} A_{11} & \cdots & A_{1s} \\ \vdots & \ddots & \vdots \\ A_{s1} & \cdots & A_{ss} \end{pmatrix}\begin{pmatrix} T'(\bar{x}_1) & & 0 \\ & \ddots & \\ 0 & & T'(\bar{x}_s) \end{pmatrix}$$

y II es un bloque de ceros (ver (2.16)). El bloque III es un bloque de ceros pues las variables μ no aparecen en la fórmula que define a $g_1,\dots,g_s$.

Derivando $\bar{g}_{s+1},\dots,\bar{g}_r$ con respecto a las variables x (ver (2.14)), vemos que V es un bloque de ceros y que VIII es un bloque diagonal. Para ver que VIII es inversible debemos ver que para $s+1\le k\le n$, $T''(\bar{x}_k)(A_{sk}(-1)^{\tau_s}+\sum_{1\le j\le s-1}A_{jk}\bar{\mu}_j(-1)^{\tau_j})$ es no nulo. Como $\bar{x}_k$ es una raíz de T' que tiene todas sus raíces simples, $T''(\bar{x}_k)\neq 0$. Supongamos que para algún k, $A_{sk}(-1)^{\tau_s}+\sum_{1\le j\le s-1}A_{jk}\bar{\mu}_j(-1)^{\tau_j}=0$. Esta última ecuación, junto con las ecuaciones (2.18), equivalen a

$$\begin{pmatrix} A_{12} & \cdots & A_{(s-1)2} & A_{s2} \\ \vdots & \ddots & \vdots & \vdots \\ A_{1s} & \cdots & A_{(s-1)s} & A_{ss} \\ A_{1k} & \cdots & A_{(s-1)k} & A_{sk} \end{pmatrix}\begin{pmatrix} \bar{\mu}_1(-1)^{\tau_1} \\ \vdots \\ \bar{\mu}_{s-1}(-1)^{\tau_{s-1}} \\ (-1)^{\tau_s} \end{pmatrix}=0$$

lo cual es imposible pues implica que existe un vector no nulo en el núcleo de una matriz inversible. Por lo tanto VIII es inversible.

Por último, derivando $\bar{g}_{s+1}, \ldots, \bar{g}_{2s-1}$ con respecto a las variables μ, vemos que VI es la matriz inversible

$$\begin{pmatrix} T'(\bar{x}_2) & & 0 \\ & \ddots & \\ 0 & & T'(\bar{x}_s) \end{pmatrix} \begin{pmatrix} A_{12} & \cdots & A_{(s-1)2} \\ \vdots & \ddots & \vdots \\ A_{1s} & \cdots & A_{(s-1)s} \end{pmatrix} \begin{pmatrix} (-1)^{\tau_1} & & 0 \\ & \ddots & \\ 0 & & (-1)^{\tau_{s-1}} \end{pmatrix}.$$

□

Métodos simbólicos de deformación

Damos a continuación el esquema un algoritmo probabilístico para calcular una resolución geométrica como en la Proposición 2.16, nuevamente reutilizando la notación de la Sección 2.5.1. Luego en la proposición siguiente, especificamos cómo llevar a cabo cada paso y analizamos la complejidad total del algoritmo. En adelante, notaremos Ω a un número real positivo tal que para cualquier anillo R es posible efectuar la suma, multiplicación y cálculo de determinante y de adjunta para matrices en $R^{m\times m}$ con $O(m^\Omega)$ operaciones en R. Podemos suponer $\Omega \leq 4$ (ver [Ber84]) y, a fin de simplificar algunas cuentas de complejidad, supondremos $\Omega \geq 3$.

Algoritmo 2.27

Input*: Un* slp *que codifica simultáneamente polinomios $h_1, \ldots, h_r$ como en (2.6).*

Output*: Una resolución geométrica como en la Proposición 2.16 con V definida a partir de un sistema inicial $g_1, \ldots, g_r$ como en la Definición 2.25.*

Procedimiento*:*

1. *Elegir $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}^n$ al azar y calcular la resolución geométrica asociada a la forma lineal $\ell_\alpha(x)$ de la variedad definida en $\mathbb{A}^r$ por $g_1(x), \ldots, g_s(x)$, $\bar{g}_{s+1}(x,\mu), \ldots, \bar{g}_r(x,\mu)$.*

2. *Calcular*

$$P(t,U,y) \mod ((t-1)^{2n\delta+1} + (y_1-\alpha_1, \ldots, y_n-\alpha_n)^2)\mathbb{K}[[t-1]][U,y].$$

3. *Calcular para $0 \leq h \leq \delta$, los polinomios $p_h(t,\alpha)$ y $\frac{\partial p_h}{\partial y_k}(t,\alpha)$, $1 \leq k \leq n$.*

4. *Calcular* $\hat{P}(0,U,\alpha)$, $\frac{\partial \hat{P}}{\partial U}(0,U,\alpha)$, $\frac{\partial \hat{P}}{\partial y_k}(0,U,\alpha)$ *para* $1 \leq k \leq n$, $g(U,\alpha)$ *y hacer las divisiones necesarias.*

Proposición 2.28 *Dado un* slp *de longitud* L_1 *que codifica simultáneamente polinomios* $h_1,\ldots,h_r$ *como en (2.6), el Algoritmo 2.27 calcula probabilísticamente una resolución geométrica como en la Proposición 2.16 con* V *definida a partir de un sistema inicial* $g_1,\ldots,g_r$ *como en la Definición 2.25. con complejidad*

$$O\big(n^3(L_1+\tilde{d}n+n^{\Omega-1})\tilde{\delta}^2\log^2(\tilde{\delta})\log\log^2(\tilde{\delta})\big).$$

Demostración: Calculemos la cantidad de operaciones que realiza el algoritmo en cada paso.

Paso 1: Como vimos en la demostración del Lema 2.26, la variedad definida en $\mathbb{A}^r$ por $g_1(x),\ldots,g_s(x),\bar{g}_{s+1}(x,\mu),\ldots,\bar{g}_r(x,\mu)$ es una unión de conjuntos $S_{B,e}$, donde B recorre todos los subconjuntos de $\{2,\ldots,n\}$ de cardinal $n-s$ y e recorre todas las funciones de B en $\{-1,1\}$.
Para empezar, calculemos la resolución geométrica asociada a la forma lineal $\ell_\alpha(x)$ de cada $S_{B,e}$. Para fijar ideas, al igual que en la demostración del Lema 2.26, supongamos $B=\{s+1,\ldots,n\}$ y sea $(\bar{x}_1,\ldots,\bar{x}_n,\bar{\mu}_1,\ldots,\bar{\mu}_{s-1})\in S_{B,e}$. Para $s+1\leq k\leq n$, $\bar{x}_k$ es una de las raíces del polinomio univariado $\gcd(T'(x_k),T(x_k)-e(k))$; este polinomio es $T_{\tilde{d}/2}$ si $e(k)=-1$ y $T'/T_{\tilde{d}/2}$ si $e(k)=1$ (recordemos que $T_{\tilde{d}/2}$ es el polinomio de Tchebychev de grado $\tilde{d}/2$). Además, para $1\leq k\leq s$, $\bar{x}_k$ es una de las raíces de un polinomio univariado que se obtiene resolviendo el sistema (2.17). Para obtener la resolución geométrica de $S_{B,e}$ asociada a la forma lineal $\ell_\alpha(x)$, procedemos como en [JMSW, Section 5.2.1]. Si llamamos $\tilde{\delta}_{B,e}$ a la cantidad de elementos en $S_{B,e}$, la cantidad de operaciones en $\mathbb{K}$ necesarias es $O(\tilde{\delta}^2_{B,e}\log^2(\tilde{\delta}_{B,e})\log\log(\tilde{\delta}_{B,e}))$.
Finalmente obtenemos la resolución geométrica de la unión de los conjuntos $S_{B,e}$ asociada a la forma lineal $\ell_\alpha(x)$ procediendo como se explica a continuación. Dadas dos resoluciones geométricas $\{q,q_0,w_1,\ldots,w_r\}$ y $\{q',q'_0,w'_1,\ldots,w'_r\}$ de conjuntos disjuntos con q y q' coprimos, una resolución geométrica de su unión está dada por $\{qq', q_0q'+q'_0q, w_1q'+w'_1q,\ldots,w_rq'+w'_rq\}$. Para obtener la resolución geométrica de la unión de los conjuntos $S_{B,e}$, seguimos el esquema de unión de pares dado en [vzGG99, Algorithm 10.3]. De esta manera, este paso requiere $O(n\tilde{\delta}^2\log^2(\tilde{\delta})\log\log(\tilde{\delta}))$ operaciones en $\mathbb{Q}$.

Paso 2: Primeramente, consideremos la variedad definida por $g_1,\ldots,g_s,\bar{g}_{s+1},\ldots,\bar{g}_r$ en $\mathbb{A}^r_{\overline{\mathbb{K}(y)}}$. Sabemos que en realidad, esta variedad está formada por un conjunto finito de puntos con todas sus coordenadas en $\overline{\mathbb{Q}}$. Dado que los polinomios

$g_1, \ldots, g_s, \bar{g}_{s+1}, \ldots, \bar{g}_r$ pueden codificarse simultáneamente por un *slp* de longitud $O((\tilde{d}+s)n)$, podemos calcular la resolución geométrica de esta variedad asociada a la forma lineal $\ell(x,y)$ módulo el ideal $(y_1-\alpha_1,\ldots,y_n-\alpha_n)^2$ a partir de la resolución geométrica calculada en el paso anterior aplicando [GLS01, Algorithm 1]. La cantidad de operaciones en $\mathbb{K}$ que efectúa este algoritmo es $O((\tilde{d}n^2 + n^\Omega)\tilde{\delta}^2 \log^2(\tilde{\delta}) \log\log^2(\tilde{\delta}))$.

A continuación consideremos la variedad definida por $F_1, \ldots, F_r$ en $\mathbb{A}^r_{\overline{\mathbb{K}(t,y)}}$, que es un conjunto finito de puntos con todas sus coordenadas en $\mathbb{K}[[t-1]]$. Dado que $F_1, \ldots, F_r$ pueden codificarse simultáneamente por un *slp* de longitud $L_1 + O((\tilde{d}+s)n)$, podemos obtener la resolución geométrica de esta variedad asociada a la forma lineal $\ell(x,y)$ módulo el ideal $(t-1)^{2n\tilde{\delta}+1} + (y_1-\alpha_1,\ldots,y_n-\alpha_n)^2$ a partir de la resolución geométrica calculada en el paso anterior aplicando repetidas veces [GLS01, Algorithm 1]. La cantidad de operaciones en $\mathbb{K}$ que efectúa este algoritmo es $O(n^3(L_1 + \tilde{d}n + n^{\Omega-1})\tilde{\delta}^2 \log^2(\tilde{\delta}) \log\log^2(\tilde{\delta}))$. Notemos que en particular habremos calculado el polinomio buscado y la complejidad total del paso es la de esta última etapa.

Pasos 3 y 4: Estos pasos son los Pasos 4 y 5 en el Algoritmo 2.20 y, como vimos en la Proposición 2.21, pueden llevarse a cabo realizando $O(n^2\tilde{\delta}^2 \log^2(\tilde{\delta}) \log\log(\tilde{\delta}))$ y $O(\tilde{\delta} \log^2(\tilde{\delta}) \log\log(\tilde{\delta}))$ operaciones en $\mathbb{K}$ respectivamente. ▫

Adaptación a los casos $s = 1$ y $s = n$

Nuevamente, podemos adaptar de manera directa lo que hemos realizado a los casos $s = 1$ y $s = n$. De hecho, manteniendo las definiciones dadas al adaptar el algoritmo para deformaciones de tipo 1 a estos casos, solamente resta definir como se adaptan los sistemas iniciales. Sea $\tilde{d} = 2\lceil \frac{d}{2} \rceil$ y $T = T_{\tilde{d}}$ el polinomio de Tchebychev de grado $\tilde{d}$.

Para el caso $s = 1$, tomemos a_1 entero con $a_1 + n + 1$ primo y $\tau_1 \in \{0,1\}$ y consideremos el sistema inicial

$$\begin{cases} g_1(x) = (-1)^{\tau_1}\Big(n + \dfrac{1}{a_1+n+1} + \displaystyle\sum_{1\le k\le n} \frac{1}{a_1+k} T(x_k)\Big), \\ g_i(x) = \dfrac{\partial g_1(x)}{\partial x_i} \qquad \text{para } 2 \le i \le n. \end{cases} \tag{2.19}$$

En este caso, tenemos $\tilde{\delta} = \tilde{d}(\tilde{d}-1)^{n-1} \le \tilde{d}^n$.

Para el caso $s = n$, tomemos $0 \leq a_1 < \ldots < a_n$ números enteros con $a_n + n + 1$ primo y, para $1 \leq i \leq n$, $\tau_i \in \{0, 1\}$ y consideremos el sistema inicial

$$\begin{cases} g_i(x) = (-1)^{\tau_i}\Big(n + \dfrac{1}{a_i + n + 1} + \displaystyle\sum_{1 \leq k \leq n} \frac{1}{a_i + k} T(x_k)\Big) & \text{para } 1 \leq i \leq n. \end{cases} \quad (2.20)$$

En este caso, tenemos $\tilde{\delta} = \tilde{d}^n$.

Procediendo como en la demostración del Lema 2.26 podemos ver que ambos sistemas iniciales satisfacen la Hipótesis 2.22. Adaptando lo desarrollado para el caso $2 \leq s \leq n - 1$, obtenemos el siguiente resultado.

Proposición 2.29 *Hay un algoritmo probabilístico que, dado un* slp *de longitud L_1 que codifica simultáneamente polinomios $h_1, \ldots, h_n$ como en (2.12), calcula una resolución geométrica de un conjunto finito que contiene a $\pi(V \cap \{t = 0\})$ (ver Definición 2.22) con complejidad*

$$O\big(n^3(L_1 + \tilde{d}n + n^{\Omega-1})\tilde{\delta}^2 \log^2(\tilde{\delta}) \log\log^2(\tilde{\delta})\big).$$

Aclaración sobre la notación

En las Secciones 2.6.3 y 2.6.4 aplicaremos deformaciones de tipo 2 a sistemas que definen las variedades W_S (ver Definición 2.7) para distintos $S \subset \{1, \ldots, m\}$ con $\#S = s$ y $1 \leq s \leq n$. Como observamos anteriormente, para completar la definición de los sistemas iniciales correspondientes, debemos especificar $a_1, \ldots, a_s, \tau_1, \ldots, \tau_s$.

En la Sección 2.6.3, estudiaremos el caso $m = 1$ y luego solamente consideraremos el caso $S = \{1\}$. Definiremos los valores de a_1 y τ_1 al comienzo de dicha sección, de manera que todas las definiciones quedarán unívocamente determinadas.

En la Sección 2.6.4, consideraremos la lista $\mathcal{P} = q_1 - n - 1, \ldots, q_m - n - 1$, donde $q_1 < \ldots < q_m$ son los primeros números primos mayores a n. Para cualquier $S \subset \{1, \ldots, m\}$ con $\#S = s$ y $1 \leq s \leq n$, y cualquier lista $\tau = \tau_1, \ldots, \tau_s$, notaremos $\hat{V}_{S,\tau}$, $V^{(0)}_{S,\tau}$, $V^{(1)}_{S,\tau}$ y $V_{S,\tau}$ a las variedades de la Definiciones 2.10 y 2.23 tomando $h_1, \ldots, h_r$ como los polinomios que definen W_S (ver Definición 2.7), los parámetros $a_1, \ldots, a_s$ como los elementos de la sublista de $\mathcal{P}$ formada por los elementos correspondientes a las posiciones de S y $\tau_1, \ldots, \tau_s$ como los elementos de τ. Notemos que para todo elemento a de $\mathcal{P}$, $a + n + 1$ resulta un número primo tal como se pide en la definición de los sistemas iniciales de tipo 2.

2.6. Resolución del problema

En esta última sección, demostraremos en varias situaciones diferentes que los puntos encontrados siguiendo las técnicas de deformación desarrolladas en la sección anterior incluyen a los puntos extremales buscados. Esto nos permitirá hilvanar todo lo que hemos elaborado y probar los resultados principales del capítulo, que recordamos a continuación.

En las Secciones 2.6.1, 2.6.2 y 2.6.3, resolveremos el problema de encontrar un conjunto finito que contiene un punto en la clausura de cada celda definida por los polinomios $f_1, \ldots, f_m$, primero bajo ciertas hipótesis de regularidad, luego en el caso bivariado, y finalmente en el caso de un solo polinomio multivariado arbitrario.

Es claro que el conjunto hallado interseca cada componente conexa de la realización de cada condición de signo cerrada, y, por lo tanto, evaluando el signo de los polinomios $f_1, \ldots, f_m$ en el conjunto finito hallado podremos conocer todas las condiciones de signo cerradas factibles para esta familia de polinomios. En la Sección 2.6.1 analizaremos la complejidad de efectuar dicha evaluación y mostraremos además que, en la primera de las tres situaciones mencionadas, a partir de los resultados obtenidos podremos conocer también todas las condiciones de signo factibles para la familia de polinomios dada.

Seguidamente, en la misma Sección 2.6.1, efectuaremos algunas consideraciones para el caso regular sobre la complejidad de estudiar la factibilidad de una condición de signo en particular sin estudiar simultáneamente la factibilidad de todas las condiciones de signo posibles.

Finalmente, en la Sección 2.6.4, estudiaremos el problema de encontrar un conjunto finito que contenga un punto en cada componente conexa de la realización de cada condición de signo cerrada factible para $f_1, \ldots, f_m$ en el caso general. Nuevamente, este conjunto podrá utilizarse para conocer todas las condiciones de signo cerradas factibles evaluando el signo de los polinomios $f_1, \ldots, f_m$ en los puntos del conjunto finito hallado.

De aquí en más, consideraremos polinomios $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ con $\mathbb{K}$ un subcuerpo de $\mathbb{R}$, tales que para $1 \leq i \leq m$, $d_i := \deg(f_i) \leq d$ con $d \geq 2$, y $f_1, \ldots, f_m$ pueden evaluarse conjuntamente por un *slp* de longitud L. Introducimos además la siguiente definición:

Definición 2.30 *Definimos respectivamente $\mathcal{C}$ y $\tilde{\mathcal{C}}$ como los conjuntos de todas las*

celdas y de todas las componentes conexas de realizaciones de condiciones de signo cerradas definidas por los polinomios $f_1, \ldots, f_m$.
Para $1 \leq k \leq n$ *y para* $p = (p_1, \ldots, p_n) \in \mathbb{R}^n$, *definimos* $\mathcal{C}(k, p)$ *como el conjunto de todas las componentes conexas de subconjuntos de* $\mathbb{R}^n$ *del tipo* $C \cap \{x_1 = p_1, \ldots, x_{k-1} = p_{k-1}\}$ *con* $C \in \mathcal{C}$ *y* $\tilde{\mathcal{C}}(k, p)$ *como el conjunto de todas las componentes conexas de subconjuntos de* $\mathbb{R}^n$ *del tipo* $C \cap \{x_1 = p_1, \ldots, x_{k-1} = p_{k-1}\}$ *con* $C \in \tilde{\mathcal{C}}$.

Con estas definiciones, para todo $p \in \mathbb{R}^n$, $\mathcal{C}(1, p) = \mathcal{C}$ y $\tilde{\mathcal{C}}(1, p) = \tilde{\mathcal{C}}$.

2.6.1. El caso regular

A lo largo de esta sección supondremos que se cumple la siguiente hipótesis sobre los polinomios $f_1, \ldots, f_m$.

Hipótesis 2.31 *Para todo* $x \in \mathbb{C}^n$, *si* $f_{i_1}(x) = \cdots = f_{i_s}(x) = 0$, $\{\nabla f_{i_1}(x), \ldots, \nabla f_{i_s}(x)\}$ *es un conjunto linealmente independiente.*

Si para $S = \{i_1, \ldots, i_s\} \subset \{1, \ldots, m\}$ notamos U_S a la variedad definida en $\mathbb{A}^n$ por los polinomios $f_{i_1}, \ldots, f_{i_s}$, esta hipótesis nos asegura que U_S es o bien vacía, o bien una variedad no singular de dimensión $n - s$. En particular, si $s > n$, U_S es vacía y entonces la variedad W_S (ver Definición 2.7) también es vacía. Además, para toda condición de signo factible $\sigma \in \{<, =, >\}^m$, si $E_\sigma = \{i \mid \sigma_i = \text{“ = ”}\}$ entonces $\#E_\sigma \leq n$.
La siguiente proposición nos permitirá utilizar los algoritmos desarrollados en la Sección 2.5 en la presente situación.

Proposición 2.32 *Sea* $\sigma \in \{<, =, >\}^m$ *y* $E_\sigma = \{i \mid \sigma_i = \text{“ = ”}\}$. *Luego de un cambio lineal genérico de variables, para toda componente conexa* C *del conjunto* $\{x \in \mathbb{R}^n \mid f_1(x)\sigma_1 0, \ldots, f_m(x)\sigma_m 0\}$,

$$Z(C) \subset \bigcup_{\substack{E_\sigma \subset S \subset \{1,\ldots,m\} \\ 1 \leq \#S \leq n}} \Pi\Big(\pi\big(V_S \cap \{t = 0\}\big)\Big).$$

Antes de demostrar esta proposición, demostremos el siguiente lema auxiliar.

Lema 2.33 *Luego de un cambio lineal genérico de variables, para todo* $S \subset \{1, \ldots, m\}$ *con* $\#S = s$ *y* $1 \leq s \leq n$, W_S *es un conjunto finito.*

Demostración: Si $s = n$, $W_S = U_S$, que es una variedad algebraica vacía o 0-dimensional.

Si $s \leq n-1$, por los argumentos en [Voi03, Section 2.1] basados en el Teorema de Sard y la versión holomorfa del Lema de Morse, una forma lineal genérica tiene un número finito de puntos críticos en U_S. Dado que $\Pi(W_S)$ es por definición el conjunto de puntos críticos de la primera función coordenada, luego de un cambio lineal genérico de variables podemos suponer que $\Pi(W_S)$ es finito.

Para cada $x \in \Pi(W_S)$, como el conjunto $\{\nabla f_{i_1}(x), \ldots, \nabla f_{i_s}(x)\}$ es l.i., existe una submatriz no singular A de $s \times s$ en la matriz de $n \times s$ que tiene a estos vectores por columna. Como el conjunto $\{\overline{\nabla} f_{i_1}(x), \ldots, \overline{\nabla} f_{i_s}(x)\}$ es l.d., entonces A debe involucrar necesariamente a la primera fila. Sea A' la matriz de $(s-1) \times s$ que se obtiene quitándole a A la primera fila, entonces $\operatorname{rank} A' = s-1$ y $\dim \ker A' = 1$. Como $\{0\} \subsetneq \{(\mu_1, \ldots, \mu_s) \in \mathbb{C}^s \mid \sum_{1 \leq j \leq s} \mu_j \overline{\nabla} f_{i_j}(x) = 0\} \subset \ker A'$, concluimos que hay un único $\mu \in \mathbb{P}^{s-1}$ tal que $(x, \mu) \in W_S$. Luego W_S es finito. ▫

Probemos ahora la Proposición 2.32 .

Demostración: Por la Proposición 2.8 y la Hipótesis 2.31 tenemos que

$$Z(C) \subset \bigcup_{\substack{E_\sigma \subset S \subset \{1,\ldots,m\} \\ 1 \leq \#S \leq n}} \Pi(W_S).$$

Por el Lema 2.33, sabemos que para cada conjunto S en la unión anterior, W_S es un conjunto finito; luego cada uno de sus puntos es aislado y, por el Corolario 2.12, tenemos que $W_S = \pi(V_S \cap \{t = 0\})$. ▫

A continuación presentamos el algoritmo para encontrar un conjunto $\mathcal{M}$ con la propiedad de intersecar la clausura de cada celda definida por los polinomios $f_1, \ldots, f_m$. Luego en el teorema siguiente, demostramos que, en efecto, el conjunto $\mathcal{M}$ calculado cumple esta propiedad y analizamos la complejidad del algoritmo.

Algoritmo 2.34

Input*: Un* slp *de longitud L que codifica simultáneamente los polinomios $f_1, \ldots, f_m$.*

Output*: Un conjunto $\mathcal{M} \subset \mathbb{A}^n$ codificado como la unión de variedades 0-dimensionales de $\mathbb{A}^n$ dadas por una lista $\mathcal{R}$ de resoluciones geométricas.*

Procedimiento*:*

1. *Efectuar un cambio lineal de variables con coeficientes en* $\mathbb{Q}$ *elegidos al azar.*
2. *Elegir* $p = (p_1, \ldots, p_n) \in \mathbb{Q}^n$ *al azar.*
3. *Tomar* $\mathcal{R}$ *vacía y para* $1 \leq k \leq n-1$ *y para cada* $S \subset \{1, \ldots, m\}$ *con* $1 \leq \#S \leq n-k+1$*:*
   a) *Calcular un* slp *que codifique simultáneamente los polinomios que definen la variedad* W_S *asociada a los polinomios* $f_1(p_1, \ldots, p_{k-1}, x_k, \ldots, x_n), \ldots, f_m(p_1, \ldots, p_{k-1}, x_k, \ldots, x_n)$ *(donde la coordenada* x_k *toma el rol de la primera coordenada).*
   b) *Calcular una resolución geométrica* $\{q^{(k,S)}(U), w_k^{(k,S)}(U), \ldots, w_n^{(k,S)}(U)\} \subset \mathbb{K}[U]$ *de la variedad* $\Pi(\pi(V_S \cap \{t = 0\})) \subset \mathbb{A}^{n-k+1}$ *aplicando deformaciones de tipo 1 y agregar a la lista* $\mathcal{R}$ *la resolución geométrica*
   $$\Big\{q^{(k,S)}(U), p_1, \ldots, p_{k-1}, w_k^{(k,S)}(U), \ldots, w_n^{(k,S)}(U)\Big\}.$$
4. *Agregar a* $\mathcal{R}$ *las resoluciones geométricas* $\{f_i(p_1, \ldots, p_{n-1}, U), p_1, \ldots, p_{n-1}, U\}$*, para* $1 \leq i \leq m$*, y* $\{U, p_1, \ldots, p_n\}$.

Teorema 2.35 *Dado un* slp *de longitud* L *que codifica simultáneamente polinomios* $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ *de grados acotados por* $d \geq 2$*, sea* $\mathcal{M} \subset \mathbb{A}^n$ *el conjunto calculado por el Algoritmo 2.34. Si* $f_1, \ldots, f_m$ *cumplen la Hipótesis 2.31, para elecciones genéricas de los parámetros involucrados, el conjunto* $\mathcal{M}$ *contiene al menos un punto en la clausura de cada celda definida por estos polinomios. La complejidad del algoritmo es*

$$O\Big(n^4\big(L + nd + n\log(n)\log^2(d) + n^2\big)\log(d)\big(\log(n) + \log\log(d)\big)$$
$$d^{2n}\Big(\sum_{1 \leq s \leq \min\{m,n\}} \binom{m}{s}\binom{n-1}{s-1}^2\Big)\Big).$$

Demostración: Por la Proposición 2.6, es suficiente con demostrar que $\mathcal{M}$ contiene al conjunto

$$\{p\} \bigcup \Big(\bigcup_{1 \leq k \leq n} \bigcup_{C \in \mathcal{C}(k,p)} Z(C,k)\Big).$$

Notemos que $p \in \mathcal{M}$ por definición y es claro que

$$\bigcup_{C \in \mathcal{C}(n,p)} Z(C,n) \subset \mathcal{M}.$$

Al haber elegido las coordenadas de p de manera aleatoria, podemos suponer que para $1 \leq k \leq n-1$, los polinomios $f_i(p_1, \ldots, p_{k-1}, x_k, \ldots, x_n)$, $1 \leq i \leq m$, satisfacen la Hipótesis 2.31 (pensados como polinomios en las variables $x_k, \ldots, x_n$). Esto se debe a que esta condición es equivalente a que p_1 no sea uno de los finitos valores críticos de la función coordenada x_1 en alguno de los conjuntos $U_S \subset \mathbb{C}^n$ para $S \subset \{1, \ldots, m\}, 1 \leq \#S \leq n$, p_2 no sea uno de los finitos valores críticos de la función coordenada x_2 en alguno de los conjuntos $U_S \cap \{x_1 = p_1\} \subset \mathbb{C}^n$ para tales conjuntos S y así sucesivamente. Gracias a la Proposición 2.32, tenemos entonces que

$$\bigcup_{1 \leq k \leq n-1} \bigcup_{C \in \mathcal{C}(k,p)} Z(C,k) \subset \mathcal{M}$$

y esto nos permite concluir que el conjunto $\mathcal{M}$ tiene la propiedad buscada.

Para efectuar un cambio lineal de variables debemos agregar $O(n^2)$ instrucciones al comienzo del *slp* que codifica los polinomios $f_1, \ldots, f_m$, luego podemos simplemente suponer que los polinomios $f_1, \ldots, f_m$ vienen codificados por un *slp* de longitud $L + O(n^2)$.

Para $1 \leq k \leq n-1$ y para cada $S \subset \{1, \ldots, m\}$ con $\#S = s$ y $1 \leq s \leq n-k+1$, tenemos un *slp* de longitud $O(nL + n^3)$ que codifica los polinomios que definen la variedad W_S. Podemos calcular una resolución geométrica de la variedad $\Pi(\pi(V_S \cap \{t = 0\})) \subset \mathbb{A}^{n-k+1}$ utilizando deformaciones de tipo 1 mediante el Algoritmo 2.20. Si llamamos $\delta_{k,S}$ a la cantidad de puntos que componen esta variedad, sabemos que $\delta_{k,S} \leq \binom{n-k}{s-1} d^{n-k+1}$ y luego la cantidad de operaciones realizadas por dicho algoritmo se encuentra acotada por

$$O\Big(n^4\big(L + nd + n\log(n)\log^2(d) + n^2\big)\log(d)\big(\log(n) + \log\log(d)\big)d^{2(n-k+1)}\binom{n-1}{s-1}^2\Big).$$

La complejidad del enunciado se obtiene sumando esta cantidad de operaciones sobre todos los k y S posibles. □

Condiciones de signo factibles

A continuación explicaremos cómo es posible conseguir la lista completa de todas las condiciones de signo factibles para los polinomios $f_1, \ldots, f_m$ a partir de un conjunto $\mathcal{M}$ que contiene un punto en la clausura de cada celda definida por $f_1, \ldots, f_m$ cuando dichos polinomios satisfacen la Hipótesis 2.31.

Para empezar, estudiemos la complejidad de determinar los signos de una lista de polinomios en un conjunto dado por una resolución geométrica. En adelante, notaremos ω a un número real positivo tal que para todo $m \in \mathbb{N}$ es posible invertir matrices en $\mathbb{Q}^{m\times m}$ con $O(m^\omega)$ operaciones en $\mathbb{Q}$. Podemos suponer entonces $\omega \leq 2{,}376$ (ver [CW90]).

Observación 2.36 *Dada una resolución geométrica* $\{q(U), w_1(U), \ldots, w_n(U)\} \subset \mathbb{K}[U]$ *formada por polinomios de grado acotado por* δ *y una lista de polinomios* $f_1, \ldots, f_m$ *de grado acotado por* d *y codificados simultáneamente por un* slp *de longitud* L*, es posible obtener los signos de estos polinomios en los puntos del conjunto representado por la resolución geométrica con complejidad*

$$O\big(L\delta \log(\delta) \log\log(\delta) + m\delta^\omega\big).$$

Para ello calculamos primeramente, para $1 \leq i \leq m$*, el polinomio*

$$f_i(w_1(U), \ldots, w_n(U)) \mod q(U)$$

con complejidad $O(L\delta \log(\delta) \log\log(\delta))$ *([vzGG99, Chapter 8]) y luego evaluamos los signos de estos polinomios en los ceros de* q *aplicando el procedimiento descripto en [Can93, Section 3] con complejidad* $O(m\delta^\omega)$*.*

Introducimos a continuación la notación que utilizaremos.

Definición 2.37 *Para* $\sigma \in \{<, =, >\}^m$ *con exactamente* t *coordenadas iguales a "=", notamos* P_σ *al subconjunto de* $\{<, =, >\}^m$ *formado por* 3^t *elementos que se obtiene a partir de* σ *cambiando algunas de sus coordenadas "=" por "<" ó ">".*

Por ejemplo, si $\sigma = (=, <, =, >) \in \{<, =, >\}^4$, P_σ es el conjunto

$$\Big\{(<,<,<,>), (=,<,<,>), (>,<,<,>), (<,<,=,>), (=,<,=,>), (>,<,=,>),$$

$$(<,<,>,>), (=,<,>,>), (>,<,>,>)\Big\}.$$

El resultado principal que nos permite conocer todas las condiciones de signo factibles se encuentra en la siguiente proposición.

Proposición 2.38 *Sea* $\mathcal{L}$ *el conjunto de condiciones de signo factibles para* $f_1, \ldots, f_m$ *y sea* $\mathcal{L}'$ *el conjunto de condiciones de signo para* $f_1, \ldots, f_m$ *que se satisfacen en elementos de* $\mathcal{M}$*. Entonces* $\mathcal{L} = \cup_{\sigma\in\mathcal{L}'} P_\sigma$*.*

Para probar esta proposición usaremos el siguiente lema auxiliar.

Lema 2.39 *Sea* $\{w_1, \ldots, w_t\} \subset \mathbb{R}^n$ *un conjunto l.i. Dada* $\sigma \in \{<, =, >\}^t$ *existe* $v \in \mathbb{R}^n$ *tal que para* $1 \leq i \leq t$, $\langle w_i, v\rangle \sigma_i 0$.

Demostración: Sin pérdida de generalidad, supongamos $\sigma_1 = \cdots = \sigma_l =$ " $=$ ", $\sigma_{l+1} = \cdots = \sigma_t =$ " $>$ ". Sea $v_l \in \langle w_1, \ldots, w_l\rangle^{\perp}$. Supongamos que tenemos v_j que satisface $\langle w_i, v_j\rangle \sigma_i 0$ para $1 \leq i \leq j$, y queremos hallar v_{j+1} que además satisfaga $\langle w_{j+1}, v_{j+1}\rangle \sigma_{j+1} 0$. Sea $v' \in \langle w_1, \ldots, w_j\rangle^{\perp}$ tal que $\langle w_{j+1}, v'\rangle \neq 0$ (tal v' existe pues en caso contrario tendríamos que $\langle w_1, \ldots, w_j\rangle^{\perp} \subset \langle w_{j+1}\rangle^{\perp}$ y entonces $\langle w_{j+1}\rangle \subset \langle w_1, \ldots, w_j\rangle$, lo cual no ocurre). Para λ de módulo suficientemente grande y signo apropiado, $v_{j+1} = v_j + \lambda v'$ cumple la condición buscada. ▫

Probemos ahora la Proposición 2.38.

Demostración: Sea $\sigma \in \mathcal{L}$, sin pérdida de generalidad, supongamos $\sigma = (=, \ldots, =, >, \ldots, >)$ formada por l signos "$=$" y $m - l$ signos "$>$". Sea C una componente conexa de la realización de σ, sea $z \in \mathcal{M} \cap \overline{C}$ y sea $\sigma' \in \mathcal{L}'$ la condición de signo que satisface z. Por continuidad, σ' debe comenzar con l signos "$=$" y luego puede tener solamente signos "$=$" ó "$>$"; entonces $\sigma \in P_{\sigma'}$.
Sea ahora $\sigma' \in \mathcal{L}'$ y $z \in \mathcal{M}$ tal que para $1 \leq i \leq m$, $f_i(z)\sigma'_i 0$. Sin pérdida de generalidad, supongamos $\sigma' = (=, \ldots, =, >, \ldots, >)$ formada por t signos "$=$" y $m - t$ signos "$>$". Si $t = 0$, $P_{\sigma'} = \{\sigma'\} \subset \mathcal{L}$. Supongamos $t > 0$ y sea $\sigma \in P_{\sigma'}$; podemos suponer $\sigma = (=, \ldots, =, >, \ldots, >)$ formada por l signos "$=$" y $m - l$ signos "$>$" con $0 \leq l \leq t$. Como el conjunto $\{\nabla f_1(z), \ldots, \nabla f_t(z)\}$ es l.i., existe $v \in \mathbb{R}^n$ tal que para $1 \leq i \leq l$, $\langle \nabla f_i(z), v\rangle = 0$ y para $l + 1 \leq i \leq t$, $\langle \nabla f_i(z), v\rangle > 0$. Sea $\gamma : [-1, 1] \to \{f_1 = \cdots = f_l = 0\}$ una curva $\mathcal{C}^{\infty}$ tal que $\gamma(0) = z$ y $\gamma'(0) = v$. Tal curva existe pues $\{f_1 = \cdots = f_l = 0\}$ es una variedad diferencial de dimensión $n - l$ cuyo espacio tangente en z es $\langle \nabla f_1(z), \ldots, \nabla f_l(z)\rangle^{\perp}$. Para $l + 1 \leq i \leq t$, $(f_i \circ \gamma)'(0) = \langle \nabla f_i(z), v\rangle > 0$; por lo tanto, como $f_i \circ \gamma(0) = 0$, para u positivo y suficientemente chico, $f_i \circ \gamma(u) > 0$. Además, para tales u y para $1 \leq i \leq l$ será $f_i \circ \gamma(u) = 0$, mientras que para $t + 1 \leq i \leq m$, $f_i \circ \gamma(u) > 0$ por continuidad de f_i. Luego tenemos que $\sigma \in \mathcal{L}$. ▫

La Proposición 2.38 nos dice cómo un conjunto de puntos que interseca la clausura de todas las celdas nos sirve para listar todas las condiciones de signo factibles cuando se cumple la Hipótesis 2.31. En el siguiente teorema estudiamos la complejidad del algoritmo que se desprende de dicha proposición.

Teorema 2.40 *Dado un* slp *de longitud L que codifica simultáneamente polinomios $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ de grados acotados por $d \geq 2$ que cumplen la Hipótesis 2.31, si el conjunto $\mathcal{M}$ calculado por el Algoritmo 2.34 contiene un punto en la clausura de cada celda definida por estos polinomios (lo cual ocurre para elecciones genéricas de los parámetros involucrados), a partir del* output *de dicho algoritmo es posible listar todas las condiciones de signo factibles para $f_1, \ldots, f_m$ con complejidad*

$$O\Big(\sum_{1\leq s\leq \min\{m,n\}} \binom{m}{s}\Big(md^{\omega n}\binom{n-1}{s-1}^{\omega} + Ln\log(d)\big(\log(n)+\log\log(d)\big)d^n\binom{n-1}{s-1}\Big)\Big).$$

Demostración: Primeramente, calculamos el signo de los polinomios $f_1, \ldots, f_m$ en los puntos de $\mathcal{M}$: podemos calcular el valor (y en particular, el signo) de estos polinomios en el punto p efectuando L operaciones en $\mathbb{K}$. Luego, para $1 \leq k \leq n$ y $S \subset \{1, \ldots, m\}$ con $s = \#S$ y $1 \leq s \leq n - k + 1$, podemos calcular los signos de $f_1, \ldots, f_m$ en el subconjunto de $\mathcal{M}$ asociado a k y a S siguiendo el método descripto en la Observación 2.36. Para finalizar, la lista de todas las condiciones de signo factibles se obtiene utilizando la Proposición 2.38. La complejidad del enunciado se obtiene sumando estas complejidades sobre todos los k y S posibles. ▫

Una condición de signo en particular

Si solamente estamos interesados en estudiar la factibilidad de una condición de signo σ para $f_1, \ldots, f_m$ en particular, podemos adaptar convenientemente los algoritmos que acabamos de desarrollar para disminuir la cantidad de operaciones necesarias.

Concretamente, si $\sigma \in \{<, =, >\}^m$, $E_\sigma = \{i \mid \sigma_i = \text{“}=\text{”}\}$ y $\#E_\sigma = l$, gracias a la Proposición 2.32, podemos simplemente modificar el tercer paso del Algoritmo 2.34 considerando los subconjuntos S tales que $E_\sigma \subset S$. Luego, adaptando la demostración de los Teoremas 2.35 y 2.40, tenemos que es posible obtener probabilísticamente una familia finita de resoluciones geométricas de variedades 0-dimensionales que interseca la clausura de cada componente conexa de la realización de σ con complejidad

$$O\Big(n^4\big(L + nd + n\log(n)\log^2(d) + n^2\big)\log(d)\big(\log(n) + \log\log(d)\big)\Big)$$

$$d^{2n}\Big(\sum_{l\leq s\leq \min\{m,n\}} \binom{m-l}{s-l}\binom{n-1}{s-1}^2\Big)\Big),$$

para luego decidir la factibilidad de σ con complejidad

$$O\Big(\sum_{l\leq s\leq \min\{m,n\}} \binom{m-l}{s-l}\Big(md^{\omega n}\binom{n-1}{s-1}^{\omega}+Ln\log(d)\big(\log(n)+\log\log(d)\big)d^n\binom{n-1}{s-1}\Big)\Big).$$

2.6.2. Polinomios en dos variables

En esta sección mostraremos que, aun cuando no se cumple la hipótesis de regularidad requerida en la sección anterior, el Algoritmo 2.34 resuelve el problema de encontrar un conjunto finito que interseca la clausura de todas las celdas definidas por los polinomios $f_1,\ldots,f_m$ en el caso bivariado. Este algoritmo calcula resoluciones geométricas para las variedades $\pi(V_S\cap\{t=0\})$ con $S\subset\{1,\ldots,m\}$, $1\leq \#S\leq 2$. Como vimos anteriormente, en tales casos, en los sistemas involucrados no aparecen las variables μ, y todas las variedades en la deformación son variedades afines.

En los siguientes dos lemas estudiamos propiedades particulares de las variedades $\pi(V_S\cap\{t=0\})$ en la presente situación.

Lema 2.41 *Sea $S=\{i_1,i_2\}\subset\{1,\ldots,m\}$ con $f_{i_1}\neq 0$, $f_{i_2}\neq 0$ y sean $f_{i_1}=\prod_{1\leq j\leq a}q_j^{d_j}$ y $f_{i_2}=\prod_{1\leq j\leq b}r_j^{e_j}$ las factorizaciones de f_{i_1} y f_{i_2} en $\mathbb{C}[x_1,x_2]$. Sean $z\in\mathbb{R}^2$ y $1\leq k_1\leq a$ y $1\leq k_2\leq b$ tal que el único factor de f_{i_1} que se anula en z es q_{k_1} y el único factor de f_{i_2} que se anula en z es r_{k_2} con q_{k_1} y r_{k_2} no asociados. Entonces $z\in\pi(V_S\cap\{t=0\})$.*

Demostración: Por el Corolario 2.12, alcanza con demostrar que z es un punto aislado de W_S. Por un lado, tenemos que

$$W_S=V(f_{i_1},f_{i_2})=\bigcup_{1\leq j_1\leq a}\ \bigcup_{1\leq j_2\leq b}V(q_{j_1},r_{j_2}),$$

y $z\in V(q_{j_1},r_{j_2})$ si y solo si $j_1=k_1$ y $j_2=k_2$. Por otro lado, $V(q_{k_1},r_{k_2})$ tiene dimensión 0 ya que r_{k_2} no es un divisor de 0 en el anillo $\mathbb{C}[x_1,x_2]/(q_{k_1})$ puesto que q_{k_1} y r_{k_2} son primos no asociados en el DFU $\mathbb{C}[x_1,x_2]$. Luego, z es un punto aislado de W_S. □

Lema 2.42 *Sea $S=\{i_1\}\subset\{1,\ldots,m\}$ con $f_{i_1}\neq 0$ y sea $f_{i_1}=\prod_{1\leq j\leq a}q_j^{d_j}$ la factorización de f_{i_1} en $\mathbb{C}[x_1,x_2]$ luego de un cambio lineal genérico de variables. Sea $z\in\mathbb{R}^2$ tal que o bien existe $1\leq k\leq a$ con $q_k(z)=\frac{\partial q_k}{\partial x_2}(z)=0$, o bien existen $1\leq k_1<k_2\leq a$ con $q_{k_1}(z)=q_{k_2}(z)=0$. Entonces $z\in\pi(V_S\cap\{t=0\})$.*

Demostración: Para simplificar la notación, llamemos f y f' a los polinomios f_{i_1} y $\frac{\partial f_{i_1}}{\partial x_2}$ respectivamente. La variedad $\hat{V}_S$ está definida por los polinomios $F_1 = (1-t)f + tg_1, F_2 = (1-t)f' + tg_2$, con g_1, g_2 como en el sistema (2.13). Llamemos I al ideal generado por F_1 y F_2, entonces la variedad $V_S \cap \{t = 0\}$ está dada por el ideal $(I : t^\infty) + (t)$.

Consideremos los polinomios $h = \prod_{1\leq j\leq a} q_j^{d_j-1}$, $h_1 = f/h = \prod_{1\leq j\leq a} q_j$ y $h_2 = f'/h = \sum_{1\leq j\leq a} d_j \frac{\partial q_j}{\partial x_2}(\prod_{1\leq j'\leq a, j'\neq j} q_{j'})$. Al haber efectuado un cambio lineal genérico de variables, podemos suponer que para todo $1 \leq j \leq a$, el polinomio $\frac{\partial q_j}{\partial x_2}$ no es idénticamente nulo y luego coprimo con q_j, lo cual implica que $h = \gcd(f, f')$.

Notemos que bajo las hipótesis de este lema, $h_1(z) = h_2(z) = 0$; luego para demostrar lo enunciado es suficiente con probar que $(I : t^\infty) = (F_1, F_2, h_2g_1 - h_1g_2)$. Veamos que ambos ideales son iguales a $(I : t)$.

Para probar que $(I : t^\infty) = (I : t)$ alcanza con ver que $(I : t^2) \subset (I : t)$. Para demostrar esto es conveniente considerar el desarrollo de F_1 y F_2 en potencias de t, es decir, $F_1 = (g_1 - f)t + f, F_2 = (g_2 - f')t + f'$. Sea $p \in (I : t^2)$, entonces

$$p(x,t)t^2 = \Big(a_2(x,t)t^2 + a_1(x)t + a_0(x)\Big)\Big(\big(g_1(x) - f(x)\big)t + f(x)\Big) +$$

$$+\Big(b_2(x,t)t^2 + b_1(x)t + b_0(x)\Big)\Big(\big(g_2(x) - f'(x)\big)t + f'(x)\Big)$$

para ciertos polinomios $a_2, b_2 \in \mathbb{C}[t, x_1, x_2]$, $a_1, a_0, b_1, b_0 \in \mathbb{C}[x_1, x_2]$.

Comparando las partes de grado 0 en t, tenemos que $a_0 f = -b_0 f'$, y esto nos dice que existe $c \in \mathbb{C}[x_1, x_2]$ tal que $a_0 = ch_2$ y $b_0 = -ch_1$.

Comparando las partes de grado 1 en t, tenemos que $a_0g_1 + b_0g_2 = -a_1f - b_1f'$. Luego $c(h_2g_1 - h_1g_2) = h(-a_1h_1 - b_1h_2)$. Veamos que esto implica que h divide a c. Para eso alcanza con ver que $q_j^{d_j-1}$ divide a c para $1 \leq j \leq a$, y por lo tanto podemos suponer que $d_j > 1$. En tal caso, tenemos que $q_j \mid h_1$ y $q_j \nmid h_2g_1$ (f y g_1 pueden suponerse coprimos como consecuencia del cambio lineal genérico de variables), por lo tanto $q_j \nmid (h_2g_1 - h_1g_2)$ y luego $q_j^{d_j-1} \mid c$. Entonces existe $c_2 \in \mathbb{C}[x_1, x_2]$ tal que $c = c_2h$ y tenemos que

$$p(x,t)t = \Big(a_2(x,t)t + a_1(x)\Big)\Big(\big(g_1(x) - f(x)\big)t + f(x)\Big) +$$

$$+\Big(b_2(x,t)t + b_1(x)\Big)\Big(\big(g_2(x) - f'(x)\big)t + f'(x)\Big) + c_2(x)\Big(f'(x)g_1(x) - f(x)g_2(x)\Big).$$

Como $f'g_1 - fg_2 = -(g_2 - f')((g_1 - f)t + f) + (g_1 - f)((g_2 - f')t + f') \in I$, tenemos que $p \in (I : t)$, que es lo que queríamos demostrar.

Veamos ahora que $(I : t) = (F_1, F_2, h_2g_1 - h_1g_2)$. Por un lado,

$$\big(h_2g_1 - h_1g_2\big)t = h_2\big((g_1 - f)t + f\big) - h_1\big((g_2 - f')t + f'\big),$$

con lo cual queda probada una inclusión. Para probar la otra inclusión, procedemos de manera similar a la de recién. Sea $p(t, x) \in (I : t)$, entonces

$$p(x,t)t = \Big(\tilde{a}_1(t,x)t + \tilde{a}_0(x)\Big)\Big(\big(g_1(x) - f(x)\big)t + f(x)\Big) +$$

$$+\Big(\tilde{b}_1(t,x)t + \tilde{b}_0(x)\Big)\Big(\big(g_2(x) - f'(x)\big)t + f'(x)\Big)$$

para ciertos polinomios $\tilde{a}_1, \tilde{b}_1 \in \mathbb{C}[t, x_1, x_2]$, $\tilde{a}_0, \tilde{b}_0 \in \mathbb{C}[x_1, x_2]$. Comparando las partes de grado 0 en t, tenemos que $\tilde{a}_0 f = -\tilde{b}_0 f'$, y por lo tanto existe $\tilde{c} \in \mathbb{C}[x_1, x_2]$ tal que $\tilde{a}_0 = \tilde{c}h_2$ y $\tilde{b}_0 = -\tilde{c}h_1$. Luego

$$p(t,x) = \tilde{a}_1(t,x)\Big(\big(g_1(x) - f(x)\big)t + f(x)\Big) +$$

$$+\tilde{b}_1(t,x)\Big(\big(g_2(x) - f'(x)\big)t + f'(x)\Big) + \tilde{c}(x)\Big(h_2(x)g_1(x) - h_1(x)g_2(x)\Big),$$

lo que prueba la otra inclusión. □

Para poder proceder como en la sección anterior, en la siguiente proposición adaptamos el resultado contenido en la Proposición 2.32 a la situación actual.

Proposición 2.43 *Sea $\sigma \in \{<, =, >\}^m$. Luego de un cambio lineal genérico de variables, para toda componente conexa C del conjunto $\{x \in \mathbb{R}^2 \mid f_1(x)\sigma_1 0, \ldots, f_m(x)\sigma_m 0\}$,*

$$Z(C) \subset \bigcup_{\substack{S \subset \{1,\ldots,m\} \\ 1 \leq \#S \leq 2}} \pi\big(V_S \cap \{t = 0\}\big).$$

Demostración: Sea $z = (z_1, z_2) \in Z_{\inf}(C)$ (el caso $z \in Z_{\sup}(C)$ es análogo). Como $z \in \partial C$, z debe anular alguno de los polinomios $f_1, \ldots, f_m$ que no resulte idénticamente nulo.

Si existe $1 \leq i_0 \leq m$ tal que f_{i_0} no es idénticamente nulo, $f_{i_0}(z) = 0$ y en la factorización en $\mathbb{C}[x_1, x_2]$ de f_{i_0} hay dos o más factores que se anulan en z, o un factor tal que tanto él como su derivada con respecto a x_2 se anulan en z, entonces por el Lema 2.42, $(0, z) \in V_{\{i_0\}}$.

Supongamos ahora que no existe tal i_0. Sea i_1 tal que f_{i_1} no es idénticamente nulo, $f_{i_1}(z) = 0$ y sea q el único factor de f_{i_1} que se anula en z; luego q debe tener todos sus coeficientes reales ya que el polinomio conjugado de q también divide a f_{i_1} y se anula en z. Además, tenemos que $\frac{\partial q}{\partial x_2}(z) \neq 0$; entonces, por el Teorema de la Función Implícita aplicado a q y z, existen una curva continua $(x_1, x_2(x_1))$ definida para x_1 en un entorno de z_1 y un entorno de z tal que q tiene signo constante arriba, abajo, y sobre dicha curva. Restringiendo el entorno de z si es necesario, tenemos que también el polinomio f_{i_1} tiene signo constante arriba, abajo, y sobre dicha curva. Dado que $z_1 = \inf \Pi_1(C)$, debe existir $i_2 \neq i_1$ tal que f_{i_2} no es idénticamente nulo y $f_{i_2}(z) = 0$. Sea r el único factor de f_{i_2} que se anula en z; nuevamente r debe tener todos sus coeficientes reales. Además, podemos suponer que q y r no son asociados, ya que, en caso contrario, las funciones implícitas definidas por q y r coinciden y, por lo tanto, por ser $z_1 = \inf \Pi_1(C)$, deberá exisitir otro polinomio $f_{i_2'}$ que satisfaga además que su único factor que se anula en z no es asociado a q. Finalmente, por el Lema 2.41 tenemos que $(0, z) \in V_{\{i_1, i_2\}}$, lo cual termina de probar esta proposición. □

Podemos ahora enunciar el resultado principal de la sección.

Teorema 2.44 *Dado un* slp *de longitud L que codifica simultáneamente polinomios $f_1, \ldots, f_m \in \mathbb{K}[x_1, x_2]$ de grados acotados por $d \geq 2$, para elecciones genéricas de los parámetros involucrados, el conjunto $\mathcal{M} \subset \mathbb{A}^2$ calculado por el Algoritmo 2.34 contiene al menos un punto en la clausura de cada celda definida por estos polinomios. La complejidad del algoritmo es*

$$O\big(\big(L + d\big) \log(d) \log\log(d) d^4 m^2\big).$$

Demostración: Teniendo en cuenta la Proposición 2.6 y procediendo como en la demostración del Teorema 2.35, solamente resta demostrar que

$$\bigcup_{C \in \mathcal{C}} Z(C) \subset \mathcal{M},$$

lo cual es una consecuencia de la Proposición 2.43. Observemos además que podemos modificar el segundo paso del Algoritmo 2.34 eligiendo $p = (0, 0)$ en vez de hacerlo de manera aleatoria, ya que en este caso no necesitamos que el punto p satisfaga ninguna propiedad.

La complejidad del enunciado se obtiene tomando $n = 2$ en la complejidad del algoritmo en el caso general, que fue calculada en el Teorema 2.35. □

2.6.3. Un solo polinomio

En esta sección resolveremos el problema de encontrar un conjunto finito que interseque la clausura de cada celda definida por un único polinomio f_1 multivariado arbitrario. A diferencia de las Secciones 2.6.1 y 2.6.2, utilizaremos deformaciones de tipo 2, adaptadas al caso $s = 1$. Para comenzar, realicemos algunas observaciones relacionadas con estas deformaciones.

Para determinar completamente el sistema inicial (2.19), debemos fijar los valores de los elementos a_1 y τ_1 involucrados en la definición de dicho sistema. A lo largo de esta sección tomaremos $\tau_1 = 0$ (luego tenemos $g_1 > 0$ en $\mathbb{R}^n$) y, si llamamos q al menor primo mayor a n, $a_1 = q - n - 1$. Es decir, $g_1(x) = n + \frac{1}{q} + \sum_{1 \leq k \leq n} \frac{1}{q-n-1+k} T(x_k)$, donde T es el polinomio de Tchebychev de grado $\tilde{d} = 2\lceil \frac{\deg f_1}{2} \rceil$.

Como mencionamos al comienzo de la Sección 2.5.3, las deformaciones de tipo 2 satisfacen propiedades geométricas que no satisfacen las deformaciones de tipo 1; en la siguiente observación puntualizamos aquéllas que aprovecharemos en esta sección.

Observación 2.45 *Según vimos en la Sección 2.4, los puntos extremales para la primera función coordenada sobre las celdas definidas por el polinomio f_1 son caracterizados por un sistema del tipo de (2.4). Dado que el sistema inicial es del tipo de (2.19), siguiendo la Definición 2.23 tenemos que en esta situación*

$$F_1(t, x) = (1 - t) f_1(x) + t g_1(x) \quad y$$

$$F_i(t, x) = (1 - t) \frac{\partial f_1}{\partial x_i}(x) + t \frac{\partial g_1}{\partial x_i}(x) = \frac{\partial F_1}{\partial x_i}(t, x) \quad \text{para } 2 \leq i \leq n.$$

Esto implica que, para todo $t_0 \in \mathbb{R}$, si $x_0 \in \{x \in \mathbb{R}^n \mid F(t_0, x) = 0\}$ es un extremo local sobre dicho conjunto para la primera función coordenada, entonces, por el Teorema de la Función Implícita, $F_1(t_0, x_0) = F_2(t_0, x_0) = \cdots = F_n(t_0, x_0) = 0$ y, por lo tanto, $(t_0, x_0) \in \hat{V}$.

Para simplificar la notación, en adelante notaremos f y F a los polinomios f_1 y F_1 respectivamente.

Al igual que en la sección anterior, para poder hacer uso del Algoritmo 2.34, debemos primeramente adaptar la Proposición 2.32, lo cual hacemos en las siguientes dos proposiciones. Un resultado similar al que contiene la primera de ellas considerando otro tipo de deformación puede encontrarse en [RRSED00].

Proposición 2.46 *Luego de un cambio lineal genérico de variables, para toda componente conexa C del conjunto $\{x \in \mathbb{R}^n \mid f(x) = 0\}$,*

$$Z(C) \subset \pi\big(V \cap \{t = 0\}\big).$$

Demostración: Por la Proposición 2.4, sabemos que $Z(C)$ es finito. Sea $z \in Z_{\inf}(C)$ y sea $\varepsilon > 0$ tal que

- $\overline{B(z,\varepsilon)} \cap \{f = 0\} \subset C$,
- $\overline{B(z,\varepsilon)} \cap Z(C) = \{z\}$,
- $\varepsilon < |t_0|$ para todo $t_0 \in \mathbb{C}$ tal que $V^{(1)}$ tiene una componente incluida en $\{t = t_0\}$.

Como el conjunto compacto $\partial B(z,\varepsilon) \cap C$ está incluido en $\{x_1 > z_1\}$, existe $\mu \in (z_1, z_1 + \varepsilon)$ tal que $\partial B(z,\varepsilon) \cap C \subset \{x_1 > \mu\}$. Luego f tiene signo constante sobre el compacto $\partial B(z,\varepsilon) \cap \{x_1 \leq \mu\}$. Supongamos que f es positivo en dicho conjunto, entonces existe $\varepsilon_0 \in (0,\varepsilon)$ tal que F es positivo en $[-\varepsilon_0, \varepsilon_0] \times (\partial B(z,\varepsilon) \cap \{x_1 \leq \mu\})$. Sea $y = (y_1, \ldots, y_n) \in B(z,\varepsilon)$ con $y_1 < z_1$, con lo cual $f(y) \neq 0$. Consideremos la unión de los dos segmentos en $\mathbb{R}^{n+1}$ que unen a los puntos $(-\varepsilon_0, z)$ y $(0, y)$, y $(0, y)$ y (ε_0, z). Como $F(-\varepsilon_0, z) < 0$ y $F(\varepsilon_0, z) > 0$, existe un punto $(t_1, \tilde{y})$ en la unión de los dos segmentos tal que $F(t_1, \tilde{y}) = 0$. Si $\tilde{y} = (\tilde{y}_1, \ldots, \tilde{y}_n)$ sabemos que $\tilde{y}_1 < z_1$ y, además, como $F(0, y) = f(y) \neq 0$, tenemos que $(t_1, \tilde{y}) \neq (0, y)$ y por lo tanto $t_1 \neq 0$. Como $\{x \in \overline{B(z,\varepsilon)} \mid F(t_1, x) = 0\}$ es un conjunto compacto y no vacío, existe un punto w en dicho conjunto en el que la función x_1 se minimiza. Además, $w \notin \partial B(z,\varepsilon)$, ya que $w_1 \leq \tilde{y}_1 < z_1 < \mu$ y F es positiva en $[-\varepsilon_0, \varepsilon_0] \times (\partial B(z,\varepsilon) \cap \{x_1 \leq \mu\})$. Luego, por la Observación 2.45 tenemos que $(t_1, w) \in \hat{V}$, pero como $0 < |t_1| < \varepsilon$, entonces $(t_1, w) \in V$.

Como $0 < |(t_1, w) - (0, z)| < \sqrt{2}\varepsilon$ y esto puede hacerse para todo ε positivo y suficientemente chico, entonces $(0, z) \in V$, por ser V un conjunto cerrado. ▫

Proposición 2.47 *Luego de un cambio lineal genérico de variables, para toda componente conexa C del conjunto $\{x \in \mathbb{R}^n \mid f(x) > 0\}$ o del conjunto $\{x \in \mathbb{R}^n \mid f(x) < 0\}$,*

$$Z(C) \subset \pi\big(V \cap \{t = 0\}\big).$$

Demostración: Supongamos que C es una componente conexa de $\{f > 0\}$. Por la Proposición 2.4 sabemos que $Z(C)$ es finito. Sea $z \in Z_{\inf}(C)$, luego debe ser $f(z) = 0$. Sea $\tilde{C}$ la componente conexa de $\{f = 0\}$ que contiene a z y sea $\varepsilon > 0$ tal que

- $\overline{B(z,\varepsilon)} \cap \{f = 0\} \subset \tilde{C}$,
- $\overline{B(z,\varepsilon)} \cap Z(C) = \{z\}$,
- $\varepsilon < |t_0|$ para todo $t_0 \in \mathbb{C}$ tal que $V^{(1)}$ tiene una componente incluida en $\{t = t_0\}$.

Como el conjunto compacto $\partial B(z,\varepsilon) \cap \overline{C}$ está incluido en $\{x_1 > z_1\}$, existe $\mu \in (z_1, z_1 + \varepsilon)$ tal que $\partial B(z,\varepsilon) \cap \overline{C} \subset \{x_1 > \mu\}$. Sea $\gamma : [0,1] \to \mathbb{R}^n$ una curva continua semialgebraica tal que $\gamma(0) = z$ y $\gamma((0,1]) \subset C \cap B(z,\varepsilon) \cap \{x_1 < \mu\}$ y sea C_1 la componente conexa de $C \cap B(z,\varepsilon)$ tal que $\gamma((0,1]) \subset C_1$.

Sea $t_1 \in (-\varepsilon, 0)$ suficientemente chico para que $F(t_1, \gamma(1))$ sea positivo. Como $F(t_1, \gamma(0)) < 0$, existe $u \in (0,1)$ tal que $F(t_1, \gamma(u)) = 0$. Sea C' la componente conexa de $\{x \in B(z,\varepsilon) \mid F(t_1, x) = 0\}$ que contiene a $\gamma(u)$. Como $\gamma(u) \in C' \cap C_1$, $C' \cup C_1$ es conexo, además $C' \subset B(z,\varepsilon) \setminus \tilde{C}$. Luego, como C_1 es una componente conexa de $B(z,\varepsilon) \setminus \tilde{C}$, concluimos que $C' \subset C_1$.

Sea ahora $K = C' \cup (\overline{B(z,\varepsilon)} \cap \{x_1 \geq \mu\})$. Como $\overline{C'} = C' \cup (\partial B(z,\varepsilon) \cap \overline{C'}) \subset C' \cup (\partial B(z,\varepsilon) \cap \overline{C}) \subset K$, K resulta compacto. Sea $w \in K$ el punto de K en el que la función x_1 se minimiza. Entonces $w \notin \overline{B(z,\varepsilon)} \cap \{x_1 \geq \mu\}$, ya que $\gamma(u) \in C' \cap \{x_1 < \mu\}$. Luego w resulta el punto de $C' \cap B(z,\varepsilon) \cap \{x_1 < \mu\}$ en el que la función x_1 se minimiza. Por la Observación 2.45 tenemos que $(t_1, w) \in \hat{V}$, pero como $0 < |t_1| < \varepsilon$, entonces $(t_1, w) \in V$.

Como $0 < |(t_1, w) - (0, z)| < \sqrt{2}\varepsilon$ y esto puede hacerse para todo ε positivo y suficientemente chico, entonces $(0, z) \in V$, por ser V un conjunto cerrado. ▫

Teorema 2.48 *Dado un* slp *de longitud L que codifica un polinomio $f \in \mathbb{K}[x_1, \ldots, x_n]$ de grado acotado por $d \geq 2$, para elecciones genéricas de los parámetros involucrados, el conjunto $\mathcal{M} \subset \mathbb{A}^n$ calculado por el Algoritmo 2.34, modificado en su tercer paso para aplicar deformaciones de tipo 2 en lugar de tipo 1, contiene al menos un punto en la clausura de cada celda definida por f. La complejidad del algoritmo es*

$$O\Big(n^5\big(L + n\tilde{d} + n^{\Omega-1}\big)\log^2(\tilde{d})\big(\log(n) + \log\log(\tilde{d})\big)^2\tilde{d}^{2n}\Big),$$

donde $\tilde{d}$ es el menor entero par mayor o igual a d.

Demostración: Nuevamente, teniendo en cuenta la Proposición 2.6 y procediendo como en la demostración del Teorema 2.35, solamente resta demostrar que

$$\bigcup_{1\leq k\leq n-1}\ \bigcup_{C\in\mathcal{C}(k,p)} Z(C,k)\subset\mathcal{M},$$

lo cual es una consecuencia de la Proposiciones 2.46 y 2.47. Observemos que también en este caso es posible modificar el segundo paso del Algoritmo 2.34 eligiendo $p=(0,\ldots,0)$ en vez de hacerlo de manera aleatoria.

Considerando el cambio lineal de variables y siguiendo [BS83], para cada $1\leq k\leq n-1$ existe un *slp* de longitud $O(L+n^2)$ que codifica simultáneamente los polinomios $f,\frac{\partial f}{\partial x_2},\ldots,\frac{\partial f}{\partial x_n}$. La complejidad del enunciado se obtiene sumando la complejidad de las llamadas al Algoritmo 2.27 adaptado como en la Proposición 2.29. ▫

2.6.4. El caso general

En esta sección estudiaremos el problema de encontrar un conjunto finito que interseque cada componente conexa de la realización de cada condición de signo cerrada factible para polinomios $f_1,\ldots,f_m$ arbitrarios. El enfoque que adoptaremos sigue el espíritu de [BPR96].

Al igual que en la sección anterior, comencemos efectuando algunas consideraciones sobre las deformaciones de tipo 2 que utilizaremos en esta sección. Recordemos que d es una cota para el grado de $f_1,\ldots,f_m$, $\tilde{d}$ es el menor entero par mayor o igual a d y T es el $\tilde{d}$-ésimo polinomio de Tchebychev $T_{\tilde{d}}$.

Sean $q_1<\ldots<q_m$ los primeros m números primos mayores a n. De aquí en más, para $1\leq i\leq m$, notaremos

$$g_i^+(x)=n+\frac{1}{q_i}+\sum_{1\leq k\leq n}\frac{1}{q_i-n-1+k}T(x_k),\quad g_i^-(x)=-g_i^+(x).$$

Podemos observar que para cualquier $S=\{i_1,\ldots,i_s\}\subset\{1,\ldots,m\}$ con $1\leq s\leq n$ y para cualquier lista $*_1,\ldots,*_s$ de signos $+$ y $-$, los polinomios $g_{i_1}^{*_1},\ldots,g_{i_s}^{*_s}$ forman el sistema inicial de tipo 2 correspondiente a los parámetros $a_j=q_{i_j}-n-1$, $1\leq j\leq s$ y a la lista $\tau=\tau_1,\ldots,\tau_s$ definida por $\tau_j=0$ si $*_j=\text{“}+\text{”}$ y $\tau_j=1$ si $*_j=\text{“}-\text{”}$ para $1\leq j\leq s$ (ver Definición 2.25).

En la siguiente observación puntualizamos propiedades geométricas de las deformaciones de tipo 2 en el caso general.

Observación 2.49 *Según vimos en la Sección 2.4, los puntos extremales para la primera función coordenada sobre el conjunto* $\{x \in \mathbb{R}^n \mid f_{i_1}(x) = \cdots = f_{i_s}(x) = 0\}$ *en el caso* $2 \leq s \leq n$ *son caracterizados por el sistema (2.3). Al considerar un sistema inicial de tipo 2, siguiendo la Definición 2.10, tenemos que para* $1 \leq k \leq s$,

$$F_k(t,x) = (1-t)f_{i_k} + tg_{i_k}^{*_k}(x),$$

mientras que para $s+1 \leq k \leq r$,

$$F_k(t,x,\mu) = (1-t)\sum_{1\leq j\leq s} \mu_j \frac{\partial f_{i_j}}{\partial x_{k-s+1}}(x) + t\sum_{1\leq j\leq s} \mu_j \frac{\partial g_{i_j}^{*_j}}{\partial x_{k-s+1}}(x) =$$

$$= \sum_{1\leq j\leq s} \mu_j \frac{\partial F_j}{\partial x_{k-s+1}}(t,x).$$

Esto implica que, para todo $t_0 \in \mathbb{R}$, *si* $x_0 \in \{x \in \mathbb{R}^n \mid F_1(t_0,x) = \cdots = F_s(t_0,x) = 0\}$ *es un extremo local sobre dicho conjunto para la primera función coordenada, por el Teorema de la Función Implícita, el conjunto* $\{\overline{\nabla}F_1(t_0,x_0), \ldots, \overline{\nabla}F_s(t_0,x_0)\}$ *es l.d; luego existe* $\mu_0 = (\mu_1, \ldots, \mu_s) \in \mathbb{R}^s$ *tal que* $F_1(t_0,x_0) = \cdots = F_s(t_0,x_0) = F_{s+1}(t_0,x_0,\mu_0) = \cdots = F_r(t_0,x_0,\mu_0) = 0$ *y, por lo tanto,* $(t_0,x_0,\mu_0) \in \hat{V}_{S,\tau}$. *Consecuentemente,* $(t_0,x_0) \in \tilde{\pi}(\hat{V}_{S,\tau})$. *El mismo resultado vale en los casos* $s = 1$ *y* $s = n$.

En adelante, para simplificar la notación, notaremos para $1 \leq i \leq m$,

$$F_i^+(t,x) = (1-t)f_i(x) + tg_i^+(x) \quad \text{y} \quad F_i^-(t,x) = (1-t)f_i(x) + tg_i^-(x).$$

El siguiente lema auxiliar nos permitirá aplicar la Proposición 2.8 en este caso considerando conjuntos S de cardinal menor o igual a n.

Lema 2.50 *Sea* $S = \{i_1, \ldots, i_s\} \subset \{1, \ldots, m\}$ *con* $s = \#S > n$ *y sea* $*_1, \ldots, *_s$ *una lista de signos* $+$ *y* $-$. *Entonces el conjunto* $\{t \in \mathbb{C} \mid \exists x \in \mathbb{C}^n$ *con* $F_{i_1}^{*_1}(t,x) = \cdots = F_{i_s}^{*_s}(t,x) = 0\}$ *es finito (posiblemente vacío).*

Demostración: Sean $\hat{F}_{i_1}^{*_1}, \ldots, \hat{F}_{i_s}^{*_s}, \hat{g}_{i_1}^{*_1}, \ldots, \hat{g}_{i_s}^{*_s}$ los polinomios que se obtienen homogeneizando $F_{i_1}^{*_1}, \ldots, F_{i_s}^{*_s}$ y $g_{i_1}^{*_1}, \ldots, g_{i_s}^{*_s}$ con respecto a las variables x con una nueva variable x_0. Podemos observar que el grado de todos estos polinomios en las variables x es $\tilde{d}$.

Sea Z la variedad definida en $\mathbb{A}^1 \times \mathbb{P}^n$ por los polinomios $\hat{F}_{i_1}^{*_1}, \ldots, \hat{F}_{i_s}^{*_s}$ y sea P la proyección $P : \mathbb{A}^1 \times \mathbb{P}^s \to \mathbb{A}^1$. Para probar el lema, alcanza con demostrar que $P(Z)$ es un conjunto finito. Como P es cerrada, $P(Z)$ es un conjunto cerrado de $\mathbb{A}^1$; luego podemos ver que es 0-dimensional viendo que $1 \notin P(Z)$, o, equivalentemente, que el sistema $\hat{g}_{i_1}^{*_1}(x) = \cdots = \hat{g}_{i_s}^{*_s}(x) = 0$ no tiene solución en $\mathbb{P}^n$.

Primeramente, veamos que este sistema no tiene solución en el abierto $\{x_0 \neq 0\}$, para lo cual podemos considerar directamente el sistema $g_{i_1}^{*_1}(x) = \cdots = g_{i_s}^{*_s}(x) = 0$ en $\mathbb{A}^n$. Si definimos $a_j = q_{i_j} - n - 1$ para $1 \leq j \leq n+1$ y $b_k = -k$ para $1 \leq k \leq n+1$ y llamamos B a la matriz de Cauchy $(\frac{1}{a_j - b_k})_{1 \leq j \leq n+1, 1 \leq k \leq n} \in \mathbb{Q}^{(n+1)\times n}$, las primeras $n+1$ ecuaciones de este sistema son equivalentes a la ecuación

$$B \begin{pmatrix} T(x_1) \\ \vdots \\ T(x_n) \end{pmatrix} = - \begin{pmatrix} n + \dfrac{1}{a_1 - b_{n+1}} \\ \vdots \\ n + \dfrac{1}{a_{n+1} - b_{n+1}} \end{pmatrix}.$$

En caso de existir alguna solución, tendríamos que la matriz

$$\left(\begin{array}{c|c} & n + \dfrac{1}{a_1 - b_{n+1}} \\ B & \vdots \\ & n + \dfrac{1}{a_{n+1} - b_{n+1}} \end{array}\right)$$

tiene rango menor o igual a n. Veamos que esto no es así viendo que su determinante es no nulo. Sabemos que el determinante de esta matriz es igual a

$$n \det \left(\begin{array}{c|c} & 1 \\ B & \vdots \\ & 1 \end{array}\right) + \det \left(\begin{array}{c|c} & \dfrac{1}{a_1 - b_{n+1}} \\ B & \vdots \\ & \dfrac{1}{a_{n+1} - b_{n+1}} \end{array}\right).$$

Procediendo como en la demostración del Lema 2.26, podemos ver que éste es un número racional en cuya expresión irreducible el numerador no es múltiplo del primo $q_{i_{n+1}}$ y, por lo tanto, no nulo.

Finalmente, veamos que no hay soluciones en el conjunto $\{x_0 = 0\}$. Para $1 \leq j \leq s$,

$$\hat{g}_{i_j}^{*_j}(0, x_1, \ldots, x_n) = \pm 2^{\tilde{d}-1} \sum_{1 \leq k \leq n} \frac{1}{q_{i_j} - n - 1 + k} x_k^{\tilde{d}}.$$

Tomando solamente las primeras n ecuaciones, tenemos que el vector $(x_1^{\tilde{d}}, \ldots, x_n^{\tilde{d}})$ está en el núcleo de la matriz de Cauchy $(\frac{1}{q_{i_j}-n-1+k})_{1\leq j,k\leq n}$ y por lo tanto debe ser el vector nulo. Esto a su vez implica que el vector $(x_1, \ldots, x_n)$ es nulo, lo cual es imposible. □

La siguiente proposición nos permitirá adaptar el Algoritmo 2.34 a nuestros propósitos en esta sección.

Proposición 2.51 *Sean $\sigma \in \{\leq, =, \geq\}^m$, $E_\sigma = \{i \mid \sigma_i = \text{“}=\text{”}\}$, $U_\sigma = \{i \mid \sigma_i = \text{“}\geq\text{”}\}$ y $L_\sigma = \{i \mid \sigma_i = \text{“}\leq\text{”}\}$. Para $S \subset \{1, \ldots, m\}$ con $s = \#S$ y $1 \leq s \leq n$, sea $\mathcal{T}_S = \{\tau \in \{0,1\}^s \mid \tau_i = 0$ si el i-ésimo elemento de S pertenece a U_σ y $\tau_i = 1$ si el i-ésimo elemento de S pertenece a $L_\sigma\}$. Luego de un cambio lineal genérico de variables, para toda componente conexa C del conjunto $\{x \in \mathbb{R}^n \mid f_1(x)\sigma_1 0, \ldots, f_m(x)\sigma_m 0\}$,*

$$Z(C) \subset \bigcup_{\substack{S\subset\{1,\ldots,m\}\\ 1\leq \#S\leq n}} \bigcup_{\tau\in\mathcal{T}_S} \Pi\Big(\pi\big(V_{S,\tau} \cap \{t = 0\}\big)\Big).$$

Demostración: Sin pérdida de generalidad supongamos que para ciertos l y k con $0 \leq l \leq k \leq m$,

$$E_\sigma = \{1, \ldots, l\}, \quad U_\sigma = \{l+1, \ldots, k\}, \quad L_\sigma = \{k+1, \ldots, m\}.$$

Por la Proposición 2.4 sabemos que $Z(C)$ es finito. Como $\{f_1 = 0, \ldots, f_l = 0, f_{l+1} \geq 0, \ldots, f_k \geq 0, f_{k+1} \leq 0, \ldots, f_m \leq 0\}$ es un conjunto cerrado, cada una de sus componentes conexas también lo es y por lo tanto $Z(C) \subset C$.

Sea $z \in Z_{\inf}(C)$ y sea $0 < \varepsilon < 1$ tal que

- $\overline{B(z,\varepsilon)} \cap \{f_1 = 0, \ldots, f_l = 0, f_{l+1} \geq 0, \ldots, f_k \geq 0, f_{k+1} \leq 0, \ldots, f_m \leq 0\} \subset C$,
- $\overline{B(z,\varepsilon)} \cap Z(C) = \{z\}$,
- para todo $\hat{S} = \{i_1, \ldots, i_{\hat{s}}\} \subset \{1, \ldots, m\}$ con $\hat{s} = \#\hat{S} > n$ y toda lista $*_1, \ldots, *_{\hat{s}}$ de signos $+$ y $-$, $\varepsilon < |t_0|$ para todo t_0 en $\{t \in \mathbb{C} - \{0\} \mid \exists x \in \mathbb{C}^n$ con $F_{i_1}^{*_1}(t,x) = \cdots = F_{i_{\hat{s}}}^{*_{\hat{s}}}(t,x) = 0\}$ (lo cual es posible por el Lema 2.50),
- para todo $S \subset \{1, \ldots, m\}$ con $1 \leq \#S \leq n$ y todo $\tau \in \mathcal{T}_S$, $\varepsilon < |t_0|$ para todo $t_0 \in \mathbb{C}$ tal que $V_{S,\tau}^{(1)}$ tiene una componente incluida en $\{t = t_0\}$.

Sea ν la distancia entre los conjuntos $\partial B(z,\varepsilon)\cap\{x_1 \le z_1\}$ y $C\cap\overline{B(z,\varepsilon)}$. Como estos dos conjuntos son compactos y disjuntos, tenemos que $\nu > 0$.

Para $t \in \mathbb{R}$ llamemos R_t al conjunto

$$\{x \in \overline{B(z,\varepsilon)} \mid F_1^+(t,x) \ge 0, \dots, F_l^+(t,x) \ge 0, F_1^-(t,x) \le 0, \dots, F_l^-(t,x) \le 0,$$
$$F_{l+1}^+(t,x) \ge 0, \dots, F_k^+(t,x) \ge 0, F_{k+1}^-(t,x) \le 0, \dots, F_m^-(t,x) \le 0\}.$$

Es claro entonces que $R_0 = C \cap \overline{B(z,\varepsilon)}$ y que $z \in R_t$ para todo $t \in [0,1]$.

Veamos que existe t_1, $0 < t_1 < \varepsilon$, tal que la componente conexa C' del conjunto R_{t_1} que contiene a z se encuentra contenida en $\{x \in \overline{B(z,\varepsilon)} \mid \operatorname{dist}(x,R_0) \le \nu/2\}$. Supongamos que lo afirmado no es cierto. Sea $(t'_n)_{n\in\mathbb{N}}$ una sucesión decreciente de números positivos, convergente a 0 y con $t'_1 < \varepsilon$, y para cada $n \in \mathbb{N}$, sea C'_n la componente conexa de $R_{t'_n}$ que contiene a z. Como C'_n es conexo, contiene a z e interseca al conjunto $\{x \in \overline{B(z,\varepsilon)} \mid \operatorname{dist}(x,R_0) > \nu/2\}$, existe $r_n \in C'_n$ con $\operatorname{dist}(r_n,R_0) = \nu/2$. Como la sucesión $(r_n)_{n\in\mathbb{N}}$ está incluida en el conjunto compacto $\overline{B(z,\varepsilon)}$, tiene una subsucesión $(r_{n_j})_{j\in\mathbb{N}}$ convergente a un elemento $r \in \overline{B(z,\varepsilon)}$, y como la función que mide la distancia a un conjunto fijo es continua, debe ser $\operatorname{dist}(r,R_0) = \nu/2$. Sin embargo, tenemos que para $1 \le i \le k$,

$$F_i^+(t_{n_j},r_{n_j}) \ge 0, \quad \text{luego } F_i^+(0,r) = \lim_{j\to\infty} F_i^+(t_{n_j},r_{n_j}) \ge 0,$$

y para $1 \le i \le l$ y $k+1 \le i \le m$,

$$F_i^-(t_{n_j},r_{n_j}) \le 0, \quad \text{luego } F_i^-(0,r) = \lim_{j\to\infty} F_i^-(t_{n_j},r_{n_j}) \le 0.$$

Esto implica que $r \in R_0$, contradiciendo el hecho de que $\operatorname{dist}(r,R_0) = \nu/2 > 0$.

Como C' es un conjunto compacto, existe un punto $w \in C'$ en el cual la función x_1 se minimiza. Veamos que $w \in B(z,\varepsilon)$. Como $z \in C'$, tenemos que $w_1 \le z_1$. Si $w \in \partial B(z,\varepsilon)$, entonces $w \in \partial B(z,\varepsilon) \cap \{x_1 \le z_1\}$, luego $\operatorname{dist}(w,R_0) \ge \nu$, lo que contradice que $\operatorname{dist}(w,R_0) \le \nu/2$.

Como el signo de los polinomios $F_1^+,\dots,F_l^+,F_1^-,\dots,F_l^-,F_{l+1}^+,\dots,F_k^+,F_{k+1}^-,\dots,F_m^-$ que no se anulan en (t_1,w) es constante en un entorno de dicho punto, podemos concluir que, si $F_{i_1}^{*_1},\dots,F_{i_s}^{*_s}$ son todos los polinomios de la lista anterior que se anulan en (t_1,w), entonces w es un mínimo local para la función x_1 en el conjunto $\{x \in \mathbb{R}^n \mid F_{i_1}^{*_1}(t_1,x) = 0,\dots,F_{i_s}^{*_s}(t_1,x) = 0\}$.

Sea $S_0 = \{i_1,\dots,i_s\}$; sabemos entonces que $S_0 \neq \emptyset$. Dado que para $1 \le i \le m$, $F_i^+(t_1,w)$ y $F_i^-(t_1,w)$ no pueden anularse simultáneamente (porque g_i^+ es estrictamente positivo en $\mathbb{R}^n$), sabemos también que $i_1,\dots,i_s$ son todos distintos, luego

$s = \#S_0$. Por la manera en que elegimos ε, tenemos además que $s \leq n$. Sea τ_0 la lista $\tau_1, \ldots, \tau_s$, con $\tau_i = 0$ si $*_i =$ " $+$ " y $\tau_i = 1$ si $*_i =$ " $-$ " para $1 \leq i \leq s$. Por la Observación 2.49, tenemos que $(t_1, w) \in \tilde{\pi}(\hat{V}_{S_0,\tau_0})$, pero como $0 < t_1 < \varepsilon$, debe ser $(t_1, w) \in \tilde{\pi}(V_{S_0,\tau_0})$ y luego

$$(t_1, w) \in \bigcup_{\substack{S \subset \{1,\ldots,m\} \\ 1 \leq \#S \leq n}} \bigcup_{\tau \in \mathcal{T}_S} \tilde{\pi}(V_{S,\tau}).$$

Notemos que este último es un conjunto cerrado por ser una unión finita de conjuntos cerrados. Como $0 < |(t_1, w) - (0, z)| < \sqrt{2}\varepsilon$ y esto puede hacerse para todo ε positivo y suficientemente chico, entonces

$$(0, z) \in \bigcup_{\substack{S \subset \{1,\ldots,m\} \\ 1 \leq \#S \leq n}} \bigcup_{\tau \in \mathcal{T}_S} \tilde{\pi}(V_{S,\tau}),$$

o equivalentemente,

$$z \in \bigcup_{\substack{S \subset \{1,\ldots,m\} \\ 1 \leq \#S \leq n}} \bigcup_{\tau \in \mathcal{T}_S} \Pi\Big(\pi\big(V_{S,\tau} \cap \{t = 0\}\big)\Big).$$

□

Podemos ahora enunciar el resultado principal de la sección.

Teorema 2.52 *Dado un* slp *de longitud L que codifica simultáneamente polinomios $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ de grados acotados por $d \geq 2$, para elecciones genéricas de los parámetros involucrados, el conjunto $\mathcal{M} \subset \mathbb{A}^n$ calculado por el Algoritmo 2.34, cambiando el paso 3.b) por el siguiente*

b') Para cada posible $\tau \in \{0,1\}^s$, calcular una resolución geométrica $\{q^{(k,S,\tau)}(U), w_k^{(k,S,\tau)}(U), \ldots, w_n^{(k,S,\tau)}(U)\} \subset \mathbb{K}[U]$ de la variedad $\Pi(\pi(V_{S,\tau} \cap \{t = 0\})) \subset \mathbb{A}^{n-k+1}$ aplicando deformaciones de tipo 2 y agregar a la lista $\mathcal{R}$ la resolución geométrica

$$\Big\{q^{(k,S,\tau)}(U), p_1, \ldots, p_{k-1}, w_k^{(k,S,\tau)}(U), \ldots, w_n^{(k,S,\tau)}(U)\Big\}.$$

contiene al menos un punto en cada componente conexa de la realización de cada condición de signo cerrada factible para los polinomios $f_1, \ldots, f_m$. La complejidad del algoritmo es

$$O\Big(n^6\big(L + \tilde{d} + n^2\big)\log^2(\tilde{d})\big(\log(n) + \log\log(\tilde{d})\big)^2 \tilde{d}^{2n}\Big(\sum_{1 \leq s \leq \min\{m,n\}} 2^s \binom{m}{s}\binom{n-1}{s-1}^2\Big)\Big),$$

donde $\tilde{d}$ es el menor entero par mayor o igual a d.

Demostración: Una vez más, teniendo en cuenta la Proposición 2.6 y procediendo como en la demostración del Teorema 2.35, solamente resta demostrar que

$$\bigcup_{1\leq k\leq n-1}\ \bigcup_{C\in\mathcal{C}(k,p)} Z(C,k)\subset\mathcal{M},$$

lo cual es una consecuencia de la Proposición 2.51. Podemos observar que nuevamente es posible modificar también el segundo paso del Algoritmo 2.34 eligiendo $p=(0,\ldots,0)$ en vez de hacerlo de manera aleatoria.

Considerando el cambio lineal de variables, para $1\leq k\leq n-1$ y para cada $S\subset\{1,\ldots,m\}$ con $\#S=s$ y $1\leq s\leq n-k+1$, tenemos un *slp* de longitud $O(nL+n^3)$ que codifica los polinomios que definen la variedad W_S. Podemos calcular una resolución geométrica de la variedad $\Pi(\pi(V_{S,\tau}\cap\{t=0\}))\subset\mathbb{A}^{n-k+1}$ utilizando deformaciones de tipo 2 mediante el Algoritmo 2.27. La complejidad del enunciado se obtiene entonces sumando esta cantidad de operaciones sobre todos los k, S y τ posibles. ▫

A partir de un conjunto que interseca cada componente conexa de la realización de cada condición de si gno cerrada factible para los polinomios $f_1,\ldots,f_m$, evaluando los signos de estos polinomios en los puntos de dicho conjunto, obtenemos la lista de todas las condiciones de signo cerradas factibles para $f_1,\ldots,f_m$. Procediendo como se describe en la Observación 2.36, obtenemos el siguiente resultado.

Teorema 2.53 *Dado un* slp *de longitud L que codifica simultáneamente polinomios $f_1,\ldots,f_m\in\mathbb{K}[x_1,\ldots,x_n]$ de grados acotados por $d\geq 2$, si el conjunto $\mathcal{M}$ calculado por el Algoritmo 2.34 modificado como en el Teorema 2.52 contiene un punto en cada componente conexa de la realización de cada condición de signo cerrada factible definida por estos polinomios (lo cual ocurre para elecciones genéricas de los parámetros involucrados), a partir del* output *de dicho algoritmo es posible listar todas las condiciones de signo cerradas factibles para $f_1,\ldots,f_m$ con complejidad*

$$O\Big(\sum_{1\leq s\leq\min\{m,n\}}\binom{m}{s}\Big(m\tilde{d}^{\omega n}\binom{n-1}{s-1}^{\omega}+Ln\log(\tilde{d})\big(\log(n)+\log\log(\tilde{d})\big)\tilde{d}^{n}\binom{n-1}{s-1}\Big)\Big).$$

Capítulo 3

Equilibrios de Nash

3.1. Introducción al problema

Uno de los conceptos principales en teoría de juegos no cooperativos es el de *equilibrio de Nash*, que consiste en una elección de una estrategia mixta por parte de cada jugador (es decir, una distribución de probabilidades en el conjunto de las estrategias de las que dispone), de modo que ningún jugador pueda mejorar la esperanza de su ganancia simplemente cambiando su propia elección. Esto es decir que, para cada jugador, para esa elección de estrategias mixtas por parte de sus adversarios, su propia estrategia mixta resulta óptima. Dado que se supone que los jugadores no pueden comunicarse entre sí con el objetivo de sincronizar un cambio de elecciones, en un equilibrio de Nash el juego tiende a estabilizarse.

En [Nas51] se demuestra que todo juego no cooperativo en forma normal tiene al menos un equilibrio de Nash. Sin embargo, la demostración no es constructiva y no da información acerca de la existencia de más de un equilibrio. La pregunta que puede formularse entonces es cómo calcular algorítmicamente los equilibrios de Nash o la cantidad de equilibrios de Nash en un juego dado.

Los equilibrios de Nash en un juego no cooperativo en forma normal pueden verse como las soluciones reales de un sistema de ecuaciones e inecuaciones polinomiales (ver, por ejemplo, [Stu02, Chapter 6]). En el caso de juegos entre dos jugadores, los polinomios involucrados son lineales y, por lo tanto, los equilibrios pueden calcularse de manera exacta utilizando algoritmos de tipo simplex (ver, por ejemplo, [LH64]); no obstante, no se conocen algoritmos de complejidad polinomial para resolver el problema (ver [vS02]).

Un estudio comparativo de distintos métodos conocidos para calcular todos los equilibrios de Nash de un juego en el caso general puede encontrarse en [Dat]. En [HP05], se presenta un nuevo algoritmo que resuelve este problema para juegos genéricos mediante métodos homotópicos, pero no se exhiben cotas para la complejidad del mismo (un tratado reciente sobre métodos numéricos en la resolución de sistemas de ecuaciones polinomiales puede encontrarse en [SW05]). En cuanto a implementaciones, podemos mencionar el software Gambit ([MMT07]).

Por otro lado, la caracterización del conjunto de todos los equilibrios de Nash de un juego como un conjunto semialgebraico motivó la aplicación de algoritmos de eliminación de cuantificadores en este contexto (ver, por ejemplo, [MM96]), lo que llevó al desarrollo de un algoritmo para el cálculo de equilibrios aproximados ([LM04]). Sin embargo, no se han obtenido resultados significativos en cuanto a la adaptación de estos algoritmos para aprovechar las propiedades particulares de los sistemas de ecuaciones que surgen en la teoría de juegos.

En este capítulo estudiaremos el conjunto de equilibrios de Nash *totalmente mixtos* de un juego, es decir, los equilibrios de Nash en los que cada jugador asigna una probabilidad positiva a la opción de adoptar cada una de sus estrategias posibles. Notemos que un procedimiento para calcular estos equilibrios puede utilizarse como subrutina para calcular todos los equilibrios de Nash de un juego, recorriendo todos los posibles subconjuntos de estrategias utilizadas. Con este objetivo, consideramos en primer lugar el conjunto de *cuasi-equilibrios* del juego, que es el conjunto de las soluciones complejas del sistema de ecuaciones polinomiales que caracteriza los equilibrios buscados. Este sistema de ecuaciones presenta una estructura multilineal que aprovecharemos para obtener algoritmos con buenas cotas de complejidad.

En primer lugar, presentaremos un algoritmo simbólico para hallar una resolución geométrica del conjunto de cuasi-equilibrios de un juego genérico con una estructura fija, tratando a los valores de las ganancias obtenidas por los jugadores como parámetros. Este método está basado en un procedimiento simbólico descripto en [JS07] para el cálculo de resultantes multihomogéneas con complejidad polinomial en el grado y el número de variables de la resultante, lo que da lugar a una complejidad polinomial en la cantidad de jugadores, la cantidad de estrategias puras de las que disponen y la cantidad de cuasi-equilibrios de un juego genérico. Vale la pena mencionar que el procedimiento presentado es determinístico, a diferencia de otros métodos que podrían utilizarse para calcular la misma resolución geométrica paramétrica con similares cotas de complejidad ([Sch03], [HJSS05]) que son proba-

bilísticos.

El siguiente resultado que presentaremos es un algoritmo para caracterizar los juegos con la máxima cantidad finita de equilibrios de Nash totalmente mixtos para la estructura prefijada. La existencia de tales juegos fue probada en [MM97], pero sin proveer una caracterización de los mismos. Nuestro algoritmo calcula un número finito de desigualdades polinomiales sobre las ganancias que obtienen los jugadores, las cuales, para juegos genéricos, son equivalentes a la existencia de la máxima cantidad finita de equilibrios de Nash totalmente mixtos. Una clasificación exhaustiva del espacio de posibles valores de ganancias para los jugadores según la cardinalidad del conjunto de equilibrios de Nash podría obtenerse, por ejemplo, utilizando los algoritmos en [LR07] y [Wei92]. Sin embargo, estos enfoques, basados en el cálculo de bases de Gröbner, resultan computacionalmente más costosos.

Finalmente, analizaremos juegos particulares cuyo conjunto de cuasi-equilibrios resulta finito. Daremos algoritmos simbólicos para verificar esta condición, para calcular una resolución geométrica del conjunto de cuasi-equilibrios y para calcular la cantidad de equilibrios de Nash totalmente mixtos del juego en cuestión. Nuevamente, la complejidad de estos algoritmos es polinomial en ciertos invariantes naturales asociados al problema, menor que la que podría obtenerse aplicando directamente los algoritmos generales de resolución de sistemas de ecuaciones polinomiales.

Este capítulo está organizado de la siguiente manera. En la próxima sección incluimos algunos conocimientos preliminares de teoría de juegos. En la Sección 3.3 presentamos algoritmos para calcular una resolución geométrica del conjunto de cuasi-equilibrios de un juego genérico, tratando a los valores de las ganancias como parámetros, y para calcular un conjunto de desigualdades polinomiales en dichos parámetros bajo las cuales el juego asociado tiene la máxima cantidad finita de equilibrios de Nash totalmente mixtos para la estructura considerada. En la Sección 3.4 estudiamos equilibrios de Nash totalmente mixtos en juegos arbitrarios cuyo conjunto de cuasi-equilibrios resulta finito. Finalmente en la Sección 3.5 probamos algunos resultados complementarios relacionados con resultantes multihomogéneas.

3.2. Preliminares de teoría de juegos

Incluimos en esta sección los conceptos principales de teoría de juegos que utilizaremos en el resto del capítulo. Una introducción más profunda al tema puede encontrarse por ejemplo en [OR94].

Como explicamos anteriormente, en este capítulo consideramos juegos no cooperativos en forma normal, es decir, juegos que se desarrollan en un único paso en el que todos los jugadores actúan simultáneamente sin comunicarse entre sí. De aquí en más, supondremos que hay $r \geq 2$ jugadores en el juego y que para $1 \leq i \leq r$, el i-ésimo jugador dispone de $n_i + 1$ estrategias puras con $n_i \in \mathbb{N}$. Estos datos definen la *estructura* del juego.

Fijada la estructura, el juego queda completamente determinado definiendo para todo $1 \leq i \leq r$, la *matriz de pagos* $c^{(i)} = (c^{(i)}_{j_1 \dots j_r})_{0 \leq j_1 \leq n_1, \dots, 0 \leq j_r \leq n_r}$ del i-ésimo jugador, que es una suerte de matriz de r dimensiones cuya entrada $c^{(i)}_{j_1 \dots j_r} \in \mathbb{Q}$ equivale a la ganancia que el i-ésimo jugador obtiene si para cada $1 \leq t \leq r$, el t-ésimo jugador elige su estrategia pura j_t.

Para $1 \leq i \leq r$, cada estrategia mixta para el i-ésimo jugador está representada por un vector $x_i = (x_{i0}, \dots, x_{in_i})$ de números no negativos que suman 1. Si se juegan las estrategias mixtas $x_1, \dots, x_r$, entonces la esperanza de la ganancia del i-ésimo jugador es

$$\pi_i(x_1, \dots, x_r) := \sum_{0 \leq j_1 \leq n_1} \cdots \sum_{0 \leq j_r \leq n_r} c^{(i)}_{j_1 \dots j_r} x_{1j_1} \dots x_{rj_r}. \tag{3.1}$$

Un *equilibrio de Nash* es un vector de estrategias mixtas tal que ningún jugador puede incrementar la esperanza de su ganancia cambiando a otra estrategia mixta si los otros jugadores mantienen su elección, es decir, un vector de estrategias mixtas $(x_1, \dots, x_r)$ tal que para todo $1 \leq i \leq r$ y para toda estrategia mixta x'_i,

$$\pi_i(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_r) \geq \pi_i(x_1, \dots, x_{i-1}, x'_i, x_{i+1}, \dots, x_r). \tag{3.2}$$

Un equilibrio de Nash *totalmente mixto* es un equilibrio de Nash en el que a cada estrategia pura se le asigna una probabilidad positiva, es decir, un equilibrio de Nash tal que $x_{ij} > 0$ para $1 \leq i \leq r,\ 0 \leq j \leq n_i$.

Los equilibrios de Nash totalmente mixtos del juego asociado a un vector de matrices de pagos $c = (c^{(i)})_{1 \leq i \leq r}$ pueden caracterizarse como el conjunto de las soluciones reales del sistema de ecuaciones

$$\begin{cases} \displaystyle\sum_{J_{-i}} \left(c^{(i)}_{j_1 \dots j_{i-1} k j_{i+1} \dots j_r} - c^{(i)}_{j_1 \dots j_{i-1} 0 j_{i+1} \dots j_r} \right) x_{1j_1} \dots x_{i-1 j_{i-1}} x_{i+1 j_{i+1}} \dots x_{rj_r} = 0 \\ \text{para } 1 \leq i \leq r, 1 \leq k \leq n_i, \text{ donde la suma se realiza sobre todos los posibles} \\ J_{-i} := j_1 \dots j_{i-1} j_{i+1} \dots j_r \text{ con } 0 \leq j_t \leq n_t \text{ para todo } 1 \leq t \leq r \text{ con } t \neq i, \end{cases} \tag{3.3}$$

que satisfacen además $x_{ij} > 0$ para $1 \leq i \leq r, 0 \leq j_i \leq n_i$ y $\sum_{0 \leq j_i \leq n_i} x_{ij} = 1$ para $1 \leq i \leq r$. Para demostrar esto, siguiendo [Stu02, Sec. 6.3], notemos que para $1 \leq i \leq r$,

$$\pi_i(x_1, \ldots, x_r) = \sum_{0 \leq j_i \leq n_i} x_{ij_i} \pi_i(x_1, \ldots, x_{i-1}, e_{j_i}, x_{i+1}, \ldots, x_n) \tag{3.4}$$

con $e_j = (0, \ldots, 0, 1, 0, \ldots 0)$, donde el 1 se encuentra en el $(j+1)$-ésimo lugar. La desigualdad (3.2) implica que para un equilibrio de Nash $(x_1, \ldots, x_r)$, para todo $1 \leq i \leq r$,

$$\pi_i(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_r) \geq \pi_i(x_1, \ldots, x_{i-1}, e_{j_i}, x_{i+1}, \ldots, x_r)$$

para $0 \leq j_i \leq n_i$; luego por la igualdad (3.4) sumada a la condiciones $\sum_{0 \leq j_i \leq n_i} x_{ij_i} = 1$ y $x_{ij_i} > 0$, tenemos que

$$\pi_i(x_1, \ldots, x_{i-1}, e_0, x_{i+1}, \ldots, x_n) = \pi_i(x_1, \ldots, x_{i-1}, e_1, x_{i+1}, \ldots, x_n) =$$

$$= \cdots = \pi_i(x_1, \ldots, x_{i-1}, e_{n_i}, x_{i+1}, \ldots, x_n),$$

o, equivalentemente, para $1 \leq i \leq r$, $1 \leq k \leq n_i$,

$$\pi_i(x_1, \ldots, x_{i-1}, e_k, x_{i+1}, \ldots, x_n) - \pi_i(x_1, \ldots, x_{i-1}, e_0, x_{i+1}, \ldots, x_n) = 0.$$

Reemplazando la fórmula en (3.1) en estas ecuaciones, obtenemos el sistema (3.3). Recíprocamente, es fácil ver que cualquier solución de dicho sistema que satisfaga además $x_{ij} > 0$ para $1 \leq i \leq r, 0 \leq j_i \leq n_i$ y $\sum_{0 \leq j_i \leq n_i} x_{ij} = 1$ para $1 \leq i \leq r$, es un equilibrio de Nash totalmente mixto.

Observemos que (3.3) es un sistema de $n_1 + \cdots + n_r$ ecuaciones polinomiales multihomogéneas en los r grupos de variables $x_1, \ldots, x_r$ (formados por $n_1 + 1, \ldots, n_r + 1$ variables respectivamente) y por lo tanto define una variedad proyectiva (posiblemente vacía) en $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r}$. Como en [Dat], llamaremos *cuasi-equilibrios* del juego a las soluciones complejas proyectivas de este sistema, y cuasi-equilibrios *afines* del juego a aquéllas que no pertenezcan a ninguno de los hiperplanos $\{x_{i0} = 0\}$ para $1 \leq i \leq r$. Notaremos V_c y V_c^{af} al conjunto de cuasi-equilibrios y al conjunto de cuasi-equilibrios afines respectivamente del juego asociado al vector c de matrices de pagos.

Todo cuasi-equilibrio $\xi := (\xi_1, \ldots, \xi_r)$ determina a lo sumo un equilibrio de Nash totalmente mixto. De hecho, si para $1 \leq i \leq r$, $s_{\xi_i} := \sum_{0 \leq j \leq n_i} \xi_{ij} \neq 0$, la única

representación en $\mathbb{A}^{n_1+1} \times \cdots \times \mathbb{A}^{n_r+1}$ asociada a ξ tal que $\sum_{0 \leq j_i \leq n_i} x_{ij_i} = 1$ para $1 \leq i \leq r$ es $(\xi_1/s_{\xi_1}, \ldots, \xi_r/s_{\xi_r})$, y este vector será un equilibrio de Nash totalmente mixto si y solo si todas sus coordenadas son números reales positivos. Podemos notar además que los cuasi-equilibrios que determinan equilibrios de Nash totalmente mixtos se encuentran entre los cuasi-equilibrios afines del juego.

Más específicamente, notemos que (3.3) es un sistema formado por, para $1 \leq i \leq r$, n_i polinomios de multigrado $d_i := (1, \ldots, 1, 0, 1, \ldots, 1) \in \mathbb{N}_0^r$, donde el 0 se encuentra en el i-ésimo lugar. Notaremos δ al número de Bézout asociado a este sistema (ver Sección 0.3.2), es decir,

$$\delta = \mathrm{Bez}_{n_1,\ldots,n_r}(d_1, n_1; \ldots; d_r, n_r).$$

El Teorema de Bezout Multihomogéneo dice entonces que el grado de la variedad V_c es menor o igual a δ. Esto implica que si V_c es finito, está formado por a lo sumo δ elementos y que si V_c^{af} es finito y tiene δ elementos, entonces $V_c = V_c^{\mathrm{af}}$. Dado que $d_{ii} = 0$ y $d_{ik} = 1$ para $1 \leq i \leq r$, $1 \leq k \leq r$, $i \neq k$, es fácil ver que δ es igual al cardinal del conjunto

$$\begin{aligned} \mathfrak{J}_0 := \Big\{ (j_{11}, \ldots, j_{rn_r}) \in \{1, \ldots, r\}^{n_1+\cdots+n_r} \mid j_{ik} \neq i \ \text{ para } 1 \leq k \leq n_i \ \text{ y} \\ \#\{j_{hk} \,|\, j_{hk} = i\} = n_i \ \text{ para } 1 \leq i \leq r \Big\}. \end{aligned} \tag{3.5}$$

En este capítulo trabajaremos en el caso en que $\delta > 0$, lo cual ocurre si y solo si $n_i \leq \sum_{1 \leq k \leq r,\ k \neq i} n_k$ para todo $1 \leq i \leq r$. De aquí en más, supondremos que ésta es la situación.

3.3. Equilibrios de Nash totalmente mixtos de juegos genéricos

En esta sección estudiaremos los equilibrios de Nash totalmente mixtos de un juego tratando los valores de las ganancias como parámetros. En la Sección 3.3.1 daremos un algoritmo para calcular una resolución geométrica del conjunto de cuasi-equilibrios en este contexto. Para juegos genéricos con la estructura considerada, podrá evaluarse directamente la resolución geométrica paramétrica obtenida en las ganancias del juego dado para describir su conjunto de cuasi-equilibrios. A partir del *output* del algoritmo mencionado, en la Sección 3.3.2 mostraremos un procedimiento para calcular condiciones polinomiales sobre las ganancias para caracterizar juegos con máxima cantidad finita de equilibrios de Nash totalmente mixtos.

3.3.1. El conjunto de cuasi-equilibrios de un juego genérico

En esta sección exhibiremos un algoritmo para calcular una resolución geométrica del conjunto de cuasi-equilibrios de un juego entre r jugadores que disponen de $n_1+1, \ldots, n_r+1$ estrategias puras, considerando a los valores de las ganancias como parámetros.

Con tal objetivo, introducimos un grupo de variables

$$C = (C^{(i)}_{j_1 \ldots j_r})_{1 \leq i \leq r, 0 \leq j_1 \leq n_1, \ldots, 0 \leq j_r \leq n_r}$$

que representan dichas ganancias. Motivados por el sistema (3.3), introducimos, para cada $1 \leq i \leq r$ y cada $1 \leq k \leq n_i$, un grupo de nuevas variables

$$A^{(ik)} = (A^{(ik)}_{J_{-i}}),$$

donde J_{-i} recorre todas las $(r-1)$-uplas $j_1 \ldots j_{i-1} j_{i+1} \ldots j_r$ con $0 \leq j_t \leq n_t$ para todo $1 \leq t \leq r$ con $t \neq i$, y consideramos el polinomio

$$F^{(i)}_k = \sum_{J_{-i}} A^{(ik)}_{J_{-i}} \, x_{1 j_1} \ldots x_{(i-1) j_{i-1}} x_{(i+1) j_{i+1}} \ldots x_{r j_r} \ \in \mathbb{Q}[A^{(ik)}, x_1, \ldots, x_r].$$

Introducimos también un grupo de nuevas variables

$$A^{(0)} = (A^{(0)}_J),$$

donde J recorre todas las r-uplas $j_1 \ldots j_r$ con $0 \leq j_t \leq n_t$ para todo $1 \leq t \leq r$, y consideramos el polinomio multihomogéneo de multigrado $d_0 := (1, \ldots, 1)$ en los grupos de variables $x_1, \ldots, x_r$,

$$F^{(0)} = \sum_{J} A^{(0)}_J x_{1 j_1} \ldots x_{r j_r} \ \in \mathbb{Q}[A^{(0)}, x_1, \ldots, x_r].$$

Para simplificar la notación, en adelante notaremos $A^{(0)}_0$ a la variable $A^{(0)}_{0 \ldots 0}$ y $A^{(0)}_{ij}$ a la variable $A^{(0)}_{0 \ldots 0 j 0 \ldots 0}$, donde el índice $j > 0$ se encuentra en el i-ésimo lugar. Estas variables representarán los coeficientes de una forma lineal genérica en $\mathbb{A}^{n_1 + \cdots + n_r}$ homogeneizada.

Finalmente llamemos R a la resultante multihomogénea $\mathrm{Res}(F^{(0)}, F^{(1)}_1, \ldots, F^{(r)}_{n_r})$. Recordemos que R es el generador del ideal en $\mathbb{Q}[A^{(0)}, A^{(11)}, \ldots, A^{(r n_r)}]$

$$(F^{(0)}, F^{(1)}_1, \ldots, F^{(r)}_{n_r}) \mathbb{Q}[A^{(0)}, A^{(11)}, \ldots, A^{(r n_r)}, x_1, \ldots, x_r] \bigcap \mathbb{Q}[A^{(0)}, A^{(11)}, \ldots, A^{(r n_r)}]$$

y tiene la propiedad de anularse si y solo si el sistema $F^{(0)} = F_1^{(1)} = \cdots = F_{n_r}^{(r)} = 0$ tiene una solución en $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r}$ (ver [GKZ94]).

El algoritmo que presentaremos para obtener la resolución geométrica paramétrica buscada está basado en el cálculo de la resultante multihomogénea R y técnicas estándar para obtener la resolución geométrica a partir de dicha resultante. Podemos ver que R es un polinomio en

$$N := \prod_{1\leq i\leq r}(n_i+1) + \sum_{1\leq i\leq r} n_i \prod_{\substack{1\leq i'\leq r\\ i'\neq i}} (n_i+1)$$

variables. Siguiendo por ejemplo [PS93], sabemos además que R es homogéneo de grado δ en las variables del grupo $A^{(0)}$ y para $1 \leq i \leq r, 1 \leq k \leq n_i$, R es homogéneo de grado

$$\delta_i := \mathrm{Bez}_{n_1,\ldots,n_r}(d_0, 1; d_1, n_1; \ldots; d_i, n_i - 1; \ldots; d_r, n_r)$$

en las variables del grupo $A^{(ik)}$. Luego el grado total de R puede acotarse por

$$D := \delta + \sum_{1\leq i\leq r} n_i\delta_i.$$

Nuevamente motivados por el sistema (3.3), a cada vector $c = (c^{(i)})_{1\leq i\leq r}$ de matrices de pagos que define un juego particular le haremos corresponder el vector $a(c) = (a_{J_{-i}}^{(ik)})$ de la siguiente manera:

$$a_{J_{-i}}^{(ik)} = c_{j_1,\ldots,j_{i-1}kj_{i+1}\ldots j_r}^{(i)} - c_{j_1,\ldots,j_{i-1}0j_{i+1}\ldots j_r}^{(i)}$$

para $1 \leq i \leq r, 1 \leq k \leq n_i, J_{-i} = j_1 \ldots j_{i-1}j_{i+1} \ldots j_r$ con $0 \leq j_t \leq n_t$ para todo $1 \leq t \leq r$ con $t \neq i$.

Antes de enfocarnos en el algoritmo, probemos algunos resultados auxiliares sobre juegos con una cantidad finita de cuasi-equilibrios.

Lema 3.1 *Para todo vector de matrices de pagos c, V_c es finito si y solo si el polinomio $R(A^{(0)}, a(c)) \in \mathbb{Q}[A^{(0)}]$ no es idénticamente nulo.*

Demostración: Si V_c es cero-dimensional, existe un polinomio multihomogéneo $f \in \mathbb{C}[x_1, \ldots, x_r]$ de multigrado $(1, \ldots, 1)$ que no se anula en ninguno de sus puntos, luego $R(A^{(0)}, a(c))$ no se anula al ser evaluado en los coeficientes de f. Por otro lado, si V_c tiene dimensión positiva, cualquier polinomio multihomogéneo de multigrado $(1, \ldots, 1)$ tiene ceros comunes con V_c (ver [Sha77, Chapter 1, Section 6, Theorem 4]); luego $R(A^{(0)}, a(c))$ es idénticamente nulo. ▫

Consideremos todos los polinomios que resultan de realizar la sustitución

$$A^{(ik)}_{J_{-i}} \mapsto C^{(i)}_{j_1\dots j_{i-1}kj_{i+1}\dots j_r} - C^{(i)}_{j_1\dots j_{i-1}0j_{i+1}\dots j_r} \quad \begin{array}{l}\text{para } 1 \le i \le r, 1 \le k \le n_i,\\ J_{-i} = j_1\dots j_{i-1}j_{i+1}\dots j_r,\\ 0 \le j_t \le n_t, 1 \le t \le r, t \ne i,\end{array}$$

en los polinomios en las variables $A^{(11)}, \dots, A^{(rn_r)}$ que forman los coeficientes de $R(A^{(0)}, A^{(11)}, \dots, A^{(rn_r)})$ pensado como polinomio en las variables $A^{(0)}$. El lema anterior nos dice que para todo vector de matrices de pagos c, el juego asociado tendrá un conjunto de cuasi-equilibrios de dimensión positiva si y solo si todos estos polinomios se anulan simultáneamente al evaluarlos en c. La existencia de juegos con finitos cuasi-equilibrios nos dice que estos polinomios no son todos idénticamente nulos; luego, para c genérico, el juego asociado tendrá un conjunto finito de cuasi-equilibrios.

Para calcular la resolución geométrica buscada, consideraremos la forma lineal $\ell(x) = x_{11} + \cdots + x_{r1}$ definida en $\mathbb{A}^{n_1+\cdots+n_r}$ sobre el conjunto de cuasi-equilibrios afines de un juego genérico. En adelante, notaremos n a la suma $\sum_{1\le i\le r} n_i$. Introducimos a continuación las siguientes definiciones.

Definición 3.2 *Para $1 \le i \le r$, $1 \le j \le n_i$, definimos $Q, W_{i0}, W_{ij} \in \mathbb{Q}[C][U]$ como los polinomios en que se obtienen realizando la sustitución*

$$\begin{array}{lcll} A^{(0)}_0 & \mapsto & U, & \\ A^{(0)}_{i1} & \mapsto & -1 & \text{para } 1 \le i \le r, \\ A^{(0)}_J & \mapsto & 0 & \text{para las otras variables en } A^{(0)}, \\ A^{(ik)}_{J_{-i}} & \mapsto & C^{(i)}_{j_1\dots j_{i-1}kj_{i+1}\dots j_r} - C^{(i)}_{j_1\dots j_{i-1}0j_{i+1}\dots j_r} & \begin{array}{l}\text{para } 1 \le i \le r, 1 \le k \le n_i,\\ J_{-i} = j_1\dots j_{i-1}j_{i+1}\dots j_r,\\ 0 \le j_t \le n_t, 1 \le t \le r, t \ne i,\end{array} \end{array} \tag{3.6}$$

en R, $\frac{\partial R}{\partial A^{(0)}_0}$ y $\frac{\partial R}{\partial A^{(0)}_{ij}}$ respectivamente (los polinomios W_{i0} son el mismo polinomio para todo $1 \le i \le r$). Definimos $S^{(0)} \in \mathbb{Q}[C]$ como la resultante con respecto a la variable U entre Q y $\frac{\partial Q}{\partial U}$, tomando a priori el grado de Q en U como δ (lo cual tiene sentido pues sabemos que $\deg_U Q \le \delta$).

En adelante veremos que los polinomios Q y W_{ij}, $1 \leq i \leq r, 0 \leq j \leq n_i$ dan una resolución geométrica asociada a la forma lineal ℓ del conjunto de cuasi-equilibrios de un juego genérico y que le polinomio $S^{(0)}$ caracteriza esta genericidad.

Lema 3.3 *Para todo vector de matrices de pagos c, $S^{(0)}(c) \neq 0$ si y solo si el juego asociado tiene δ cuasi-equilibrios que resultan todos afines y la forma lineal ℓ separa las δ soluciones en $\mathbb{A}^n$ del sistema (3.3) afinizado mediante las evaluaciones $x_{i0} = 1$ para $1 \leq i \leq r$. Además, el polinomio $S^{(0)}$ no es idénticamente nulo.*

Demostración: Las raíces de $Q(c)(U)$ son los valores de $u \in \mathbb{C}$ tales que existe un cuasi-equilibrio $\xi = ((\xi_{10} : \cdots : \xi_{1n_1}), \ldots, (\xi_{r0} : \cdots : \xi_{rn_r}))$ del juego con

$$u \prod_{1 \leq i \leq r} \xi_{i0} - \sum_{1 \leq i \leq r} \xi_{i1} \prod_{\substack{1 \leq i' \leq r \\ i' \neq i}} \xi_{i'0} = 0. \tag{3.7}$$

Veamos para cada cuasi-equilibrio ξ qué valores de $u \in \mathbb{C}$ son soluciones de esta ecuación. Si ξ es un cuasi-equilibrio afín, hay una única solución de (3.7) que es el valor de la forma lineal ℓ en $(\xi_{11}/\xi_{10}, \ldots, \xi_{rn_r}/\xi_{r0})$. Por otro lado, si existen $1 \leq i_1 < i_2 \leq r$ tales que $\xi_{i_1 0} = \xi_{i_2 0} = 0$, todo $u \in \mathbb{C}$ es solución de (3.7). Finalmente, si existe un único $1 \leq i_1 \leq r$ tal que $\xi_{i_1 0} = 0$, entonces o bien todo $u \in \mathbb{C}$ es solución o bien no existe ninguna solución de (3.7) según sea $\xi_{i_1 1} = 0$ o $\xi_{i_1 1} \neq 0$ respectivamente.

Si c es tal que V_c^{af} tiene δ elementos y la formal lineal ℓ separa las soluciones del sistema (3.3) afinizado, entonces $Q(c)(U)$ es un polinomio de grado igual a δ y libre de cuadrados, por lo tanto $S^{(0)}(c) \neq 0$.

Recíprocamente, si $S^{(0)}(c) \neq 0$, $Q(c)(U)$ no es idénticamente nulo y $R(A^{(0)}, a(c))$ tampoco es idénticamente nulo. En tal caso, por el Lema 3.1, V_c es finito, y luego de cardinal menor o igual a δ. Como $Q(c)(U)$ tiene grado δ y es libre de cuadrados, por la caracterización realizada para las raíces de $Q(c)(U)$, todos los cuasi-equilibrios son afines y la forma lineal ℓ separa todas las soluciones del sistema (3.3) afinizado.

Para probar que $S^{(0)}$ no es idénticamente nulo, es suficiente con probar que existe un valor particular de c tal que el sistema (3.3) afinizado tiene δ soluciones y tal que la forma lineal ℓ toma valores distintos en todas ellas. A tal efecto, tomemos un vector c_0 de manera de obtener un sistema particular con δ soluciones afines, y una forma lineal $\ell_0 \in \mathbb{C}[x_{11}, \ldots, x_{rn_r}]$ que separe estas soluciones. Escribamos a ℓ_0 como una suma de formas lineales $\ell_{0i} \in \mathbb{C}[x_{i1}, \ldots, x_{in_i}]$ para $1 \leq i \leq r$; podemos suponer entonces que cada forma lineal ℓ_{0i} es no nula. Haciendo un cambio lineal

de variables en cada grupo x_i sin involucrar a la variable x_{i0}, la forma lineal ℓ_{0i} se convierte en x_{i1}, ℓ_0 se convierte en ℓ y el sistema particular correspondiente a c_0 nos lleva a un sistema correspondiente a un vector c con la propiedad buscada. □

Observación 3.4 *Dado que $S^{(0)}$ no es idénticamente nulo, tenemos que* $\deg_U Q = \delta$. *Además las cotas de grado para el polinomio R en las variables de cada grupo implican que* $\deg_C Q \leq D$ *y, para* $1 \leq i \leq r$, $0 \leq j \leq n_i$, $\deg_U W_{ij} < \delta$ *y* $\deg_C W_{ij} \leq D$.

Proposición 3.5 *Sea c un vector de matrices de pagos tal que $S^{(0)}(c) \neq 0$. Entonces $\{Q(c)(U), W_{10}(c)(U), \ldots, W_{rn_r}(c)(U)\}$ es una resolución geométrica del conjunto de cuasi-equilibrios del juego asociado a c.*

Demostración: Veamos que para todo vector c tal que $S^{(0)}(c) \neq 0$, V_c puede representarse de la siguiente manera:

$$\Big\{\big((W_{10}(c)(u) : W_{11}(c)(u) : \cdots : W_{1n_1}(c)(u)), \ldots, \\ (W_{r0}(c)(u) : W_{r1}(c)(u) : \cdots : W_{rn_r}(c)(u))\big) \mid u \in \mathbb{C},\ Q(c)(u) = 0\Big\}. \tag{3.8}$$

Por el Lema 3.3, sabemos que para un tal c el juego asociado tiene δ cuasi-equilibrios que resultan todos afines, la forma lineal ℓ toma valores distintos en todos ellos y estos valores son las raíces del polinomio $Q(c)(U)$ que es libre de cuadrados.
Para $1 \leq i \leq r, 1 \leq j \leq n_i$, sea L_{ij} una nueva variable y sea $A_L^{(0)}$ el vector que se obtiene especializando las variables del grupo $A^{(0)}$ de la siguiente manera:

$$\begin{aligned} A_0^{(0)} &\mapsto \textstyle\sum_{1\leq i\leq r, 1\leq j\leq n_i} L_{ij}x_{ij} \\ A_{ij}^{(0)} &\mapsto -L_{ij}x_{i0} && \text{para } 1 \leq i \leq r, 1 \leq j \leq n_i, \\ A_J^{(0)} &\mapsto 0 && \text{para las otras variables en } A^{(0)}. \end{aligned}$$

Sea

$$R_L(A^{(11)}, \ldots, A^{(rn_r)}, x_1, \ldots, x_r, L_{11}, \ldots, L_{rn_r}) = R(A_L^{(0)}, A^{(11)}, \ldots, A^{(rn_r)}) \in \\ \in \mathbb{Q}[A^{(11)}, \ldots, A^{(rn_r)}, x_1, \ldots, x_r, L_{11}, \ldots, L_{rn_r}].$$

Dado que $R \in (F^{(0)}, F_1^{(1)}, \ldots, F_{n_r}^{(r)})\mathbb{Q}[A^{(0)}, A^{(11)}, \ldots, A^{(rn_r)}, x_1, \ldots, x_r]$, $F^{(0)}(A_L^{(0)}) \equiv 0$, y los polinomios $F_1^{(1)}, \ldots, F_{n_r}^{(r)}$ no dependen de las variables $A^{(0)}$, tenemos que

$$R_L \in (F_1^{(1)}, \ldots, F_{n_r}^{(r)})\mathbb{Q}[A^{(11)}, \ldots, A^{(rn_r)}, x_1, \ldots, x_r, L_{11}, \ldots, L_{rn_r}].$$

Como además estos últimos polinomios tampoco dependen de las variables $L_{11}, \ldots,$ L_{rn_r}, tenemos que

$$\frac{\partial R_L}{\partial L_{ij}}(A^{(11)}, \ldots, A^{(rn_r)}, x_1, \ldots, x_r, L_{11}, \ldots, L_{rn_r}) =$$

$$= \frac{\partial R}{\partial A_0^{(0)}}(A_L^{(0)}, A^{(11)}, \ldots, A^{(rn_r)})x_{ij} - \frac{\partial R}{\partial A_{ij}^{(0)}}(A_L^{(0)}, A^{(11)}, \ldots, A^{(rn_r)})x_{i0} \in$$

$$\in (F_1^{(1)}, \ldots, F_{n_r}^{(r)})\mathbb{Q}[A^{(11)}, \ldots, A^{(rn_r)}, x_1, \ldots, x_r, L_{11}, \ldots, L_{rn_r}].$$

Evaluando entonces para todo $1 \leq i \leq r, 1 \leq j \leq n_i$, el polinomio $\frac{\partial R_L}{\partial L_{ij}}$ en el vector $a(c)$, un cuasi-equilibrio afín $((1 : \xi_{11} : \cdots : \xi_{1n_1}), \ldots, (1 : \xi_{r1} : \cdots : \xi_{rn_r}))$ y

$$(L_{11}, L_{12}, \ldots, L_{1n_1}, \ldots, L_{r1}, L_{r2}, \ldots, L_{rn_r}) = (1, 0, \ldots, 0, \ldots, 1, 0, \ldots, 0),$$

obtenemos que

$$0 = W_{i0}(c)(\ell(\xi))\xi_{ij} - W_{ij}(c)(\ell(\xi)),$$

lo cual prueba que V_c puede representarse como en (3.8). □

A continuación presentamos nuestro algoritmo para calcular la resolución geométrica paramétrica de la Proposición 3.5 e inmediatamente después analizamos su complejidad.

Algoritmo 3.6

Input*: El número de jugadores r y las cantidades $n_1 + 1, \ldots, n_r + 1$ de estrategias puras posibles para ellos.*

Output*: La resolución geométrica paramétrica $\{Q, W_{10}, \ldots, W_{rn_r}\} \subset \mathbb{Q}[C][U]$ de un juego genérico con la estructura del* input*, codificada por un* slp*.*

Procedimiento*:*

1. *Calcular un* slp *que codifique la resultante R utilizando una versión adaptada del algoritmo en [JS07, Theorem 5] como se especifica en la Sección 3.5.1.*

2. *Calcular un* slp *que codifique simultáneamente la resultante R y las derivadas parciales*

$$\frac{\partial R}{\partial A_0^{(0)}} \quad y \quad \frac{\partial R}{\partial A_{ij}^{(0)}} \quad \text{para } 1 \leq i \leq r,\ 1 \leq j \leq n_i.$$

3. Agregar al slp *calculado la codificación de la sustitución (3.6).*

Teorema 3.7 *El Algoritmo 3.6 calcula una resolución geométrica paramétrica del conjunto de cuasi-equilibrios de un juego genérico entre r jugadores que disponen de* $n_1 + 1, \ldots, n_r + 1$ *estrategias puras. La complejidad del algoritmo es*

$$O\big(D^2(D + n_1 \ldots n_r\, \delta \log(D) r^2 n^4 (n^3 + rN))\big)$$

y el output *es un* slp *de longitud del mismo orden que la complejidad que codifica simultáneamente a todos los polinomios de la resolución geométrica.*

Demostración: La correctitud del algoritmo se desprende de la Proposición 3.5.

En la Sección 3.5.1 veremos que podemos calcular un *slp* que codifica la resultante R adaptadando el algoritmo en [JS07, Theorem 5] con complejidad $O(D^2(D + n_1 \ldots n_r \delta \log(D) r^2 n^4 (n^3 + rN)))$. A su vez, la longitud del *slp* obtenido es del mismo orden. Luego siguiendo [BS83] podemos calcular un *slp* que codifica simultáneamente a R y a todas sus derivadas parciales con la misma complejidad. Nuevamente, la longitud del *slp* obtenido es del mismo orden. Finalmente el último paso no modifica la complejidad ni el orden de la longitud del *slp* obtenido. ▫

3.3.2. Juegos con máxima cantidad de equilibrios totalmente mixtos

En [MM97] se demuestra la existencia de un conjunto abierto en el espacio (real) de vectores de matrices de pagos tal que, para todo vector c en dicho abierto, el juego asociado tiene la máxima cantidad finita posible de equilibrios de Nash totalmente mixtos para la estructura considerada. Como mencionamos anteriormente, esta cantidad es el número de Bézout δ del sistema de ecuaciones polinomiales (3.3) asociado.

En esta sección daremos un algoritmo para obtener una familia finita de desigualdades polinomiales tales que un juego que satisface estas condiciones tiene δ equilibrios de Nash totalmente mixtos. Más aún, para juegos genéricos, estas condiciones serán equivalentes a la existencia de δ equilibrios de Nash totalmente mixtos.

Este algoritmo está basado en el cálculo de secuencias de subresultantes con signo como en [GVLRR94], adaptando a nuestra situación la construcción clásica de subresultantes a través de determinantes. Otras versiones algorítmicas más sofisticadas

de este enfoque (como por ejemplo, [LR01]) no resultan apropiadas para desarrollar nuestro algoritmo ya que los polinomios con los que trabajamos dependen de parámetros y se encuentran codificados mediante *slps*.

Primeramente, recordemos algunas definiciones y notaciones que utilizaremos (ver por ejemplo [BPR03, Section 2.2.2 y Section 4.2] para más detalles).

Para polinomios $P, Q \in \mathbb{R}[U]$ con $P \not\equiv 0$, la *Sturm query* de Q para P es el número

$$SQ(Q,P) := \#\Big\{u \in \mathbb{R} \mid P(u) = 0,\, Q(u) > 0\Big\} - \#\Big\{u \in \mathbb{R} \mid P(u) = 0,\, Q(u) < 0\Big\}$$

y el *índice de Cauchy* de la función racional Q/P es, informalmente, el número

$$I(Q/P) := \Big(\text{número de ``saltos'' de} - \infty \text{ a } + \infty \text{ de } Q/P\Big) -$$

$$\Big(\text{número de ``saltos'' de} + \infty \text{ a } - \infty \text{ de } Q/P\Big).$$

Para polinomios P y Q sobre cualquier cuerpo de grados $p > q$ respectivamente, para $0 \leq h \leq q$, la h-ésima *matriz de Sylvester-Habitch* de P y Q, $\mathrm{SH}_h(P,Q)$, es la matriz de tamaño $(p+q-2h) \times (p+q-h)$ de los coeficientes de los polinomios $U^{q-h-1}P, \ldots, P, Q, \ldots, U^{p-h-1}Q$ en la base $\{U^{p+q-h-1}, \ldots, U, 1\}$ y la h-ésima *subresultante con signo*, $\mathrm{sr}_h(P,Q)$, es el determinante de la matriz cuadrada $\widehat{\mathrm{SH}}_h(P,Q)$ que se obtiene eliminando las últimas h columnas de $\mathrm{SH}_h(P,Q)$. Además, para P y Q en $\mathbb{R}[U]$, $\mathrm{sr}_p(P,Q)$ es el signo del coeficiente principal de P elevado a la $p-q$.

Antes de dar el algoritmo, probemos el siguiente lema auxiliar.

Lema 3.8 *Sean $Q, W_{10}, \ldots, W_{rn_r} \in \mathbb{Q}[C][U]$ como en la Definición 3.2 y sea $q_\delta \in \mathbb{Q}[C]$ el coeficiente principal de Q. Para $1 \leq i \leq r$, $1 \leq j \leq n_r$, sean*

$$S_{ij}^{(h)} = \mathrm{sr}_h(Q, W_{ij})\,\mathrm{sr}_{h-1}(Q, W_{ij}) \text{ para } 1 \leq h \leq \delta - 1,$$

$$S_{ij}^{(\delta)} = q_\delta\,\mathrm{sr}_{\delta-1}(Q, W_{ij}) \in \mathbb{Q}[C]$$

obtenidos considerando los polinomios Q, W_{ij} como polinomios en la variable U y suponiendo a priori que los polinomios W_{ij} tienen grado $\delta - 1$. Para todo vector c de matrices de pagos tal que $S^{(0)}(c) \neq 0$, las condiciones

$$S_{ij}^{(h)}(c) > 0 \quad \text{para } 1 \leq i \leq r,\, 1 \leq j \leq n_i, 1 \leq h \leq \delta, \tag{3.9}$$

son equivalentes a que el juego asociado tenga exactamente δ equilibrios de Nash totalmente mixtos.

Demostración: Sea c un vector de matrices de pagos tal que $S^{(0)}(c) \neq 0$. Por el Lema 3.3, sabemos que el juego asociado tiene δ cuasi-equilibrios que resultan todos afines y son separados por la forma lineal ℓ. Más aún, por la Proposición 3.5, tenemos que el conjunto de cuasi-equilibrios puede representarse como en (3.8).

Para $1 \leq i \leq r$, sea $S_i = \sum_{0 \leq j \leq n_i} W_{ij} \in \mathbb{Q}[C][U]$. Los equilibrios de Nash totalmente mixtos del juego asociado a c son los puntos $(\xi_1, \ldots, \xi_r) \in \mathbb{R}^{n_1+1} \times \cdots \times \mathbb{R}^{n_r+1}$ de la forma

$$\xi_i = \Big(\frac{W_{i0}(c)(u)}{S_i(c)(u)}, \ldots, \frac{W_{in_i}(c)(u)}{S_i(c)(u)}\Big) \text{ para } 1 \leq i \leq r, \quad \text{con } Q(c)(u) = 0,$$

que tengan todas sus coordenadas reales y positivas. Recordando que para todo $1 \leq i \leq r$, $W_{i0} = Q'$, esto es equivalente a que u pertenezca al conjunto

$$\Big\{u \in \mathbb{R} \mid Q(c)(u) = 0,\, Q'(c)(u) > 0,\, W_{ij}(c)(u) > 0 \ \text{ para } 1 \leq i \leq r,\, 1 \leq j \leq n_i\Big\} \bigcup$$

$$\Big\{u \in \mathbb{R} \mid Q(c)(u) = 0,\, Q'(c)(u) < 0,\, W_{ij}(c)(u) < 0 \ \text{ para } 1 \leq i \leq r,\, 1 \leq j \leq n_i\Big\}.$$

Podemos concluir entonces que el juego asociado a c tendrá δ equilibrios de Nash totalmente mixtos si y solo si

$$\#\Big(\bigcap_{1 \leq i \leq r,\, 1 \leq j \leq n_i} \Big\{u \in \mathbb{R} \mid Q(c)(u) = 0,\, (Q'(c)W_{ij}(c))(u) > 0\Big\}\Big) = \delta. \tag{3.10}$$

Dado que la condición $S^{(0)}(c) \neq 0$ implica que el grado de $Q(c)$ es δ, tenemos que (3.10) es equivalente a que para todo $1 \leq i \leq r$, $1 \leq j \leq n_i$,

$$SQ(Q'(c)W_{ij}(c), Q(c)) = \delta.$$

Por [BPR03, Proposition 2.51], esta igualdad es equivalente a

$$I((Q'(c))^2 W_{ij}(c)/Q(c)) = \delta,$$

y, ya que $Q(c)$ es libre de cuadrados, también es equivalente a

$$I(W_{ij}(c)/Q(c)) = \delta. \tag{3.11}$$

Sea c un vector de matrices de pagos tal que $S^{(0)}(c) \neq 0$ y el juego asociado tiene δ equilibrios de Nash totalmente mixtos. Por [BPR03, Remark 2.49], la igualdad (3.11) implica que $\deg_U(W_{ij}(c)) = \delta - 1$ para todo $1 \leq i \leq r$, $1 \leq j \leq n_i$; luego $\mathrm{sr}_\delta(Q(c), W_{ij}(c))$ coincide con el signo de $q_\delta(c)$. Por [BPR03, Theorem 9.5], la

igualdad (3.11) es a su vez equivalente a que no haya cambios de signo en la secuencia $\mathrm{sr}_\delta(Q(c), W_{ij}(c)), \mathrm{sr}_{\delta-1}(Q(c), W_{ij}(c)), \ldots, \mathrm{sr}_0(Q(c), W_{ij}(c))$ y que ninguno de estos valores sea nulo, lo cual prueba que valen las desigualdades (3.9).

Recíprocamente, si c un vector de matrices de pagos que satisface $S^{(0)}(c) \neq 0$ y las desigualdades (3.9), dado que $\mathrm{sr}_{\delta-1}(Q(c), W_{ij}(c))$ es el coeficiente de grado $\delta - 1$ de $W_{ij}(c)$, la condición $\deg_U(W_{ij}(c)) = \delta - 1$ es consecuencia de que $S_{ij}^{(\delta)}(c)$ sea positivo. En tal caso, nuevamente por [BPR03, Theorem 9.5], las condiciones (3.9) implican la igualdad $I(W_{ij}(c)/Q(c)) = \delta$ y, por lo tanto, el juego asociado a c tiene exactamente δ equilibrios de Nash totalmente mixtos. ▫

Observamos que cada uno de los polinomios $S^{(0)}$ y $\mathrm{sr}_h(Q, W_{ij})$ para $1 \leq i \leq r, 1 \leq j \leq n_i$ y $0 \leq h \leq \delta - 1$ es el determinante de una matriz de tamaño menor o igual a $2\delta - 1$ cuyas entradas son polinomios en $\mathbb{Q}[C]$ de grado total acotado por D y, por lo tanto, sus grados están acotados por $2\delta D$. Consecuentemente, los grados de los polinomios $S_{ij}^{(h)}$ están acotados por $4\delta D$.

Exhibimos a continuación un algoritmo para calcular, a partir del *output* del Algoritmo 3.6, los polinomios definidos en el Lema 3.8 que dan las condiciones para caracterizar los juegos con máxima cantidad finita posible de equilibrios de Nash totalmente mixtos.

Algoritmo 3.9

Input*: Un* slp *de longitud L que codifica simultáneamente los polinomios $Q, W_{10}, \ldots, W_{rn_r} \in \mathbb{Q}[C][U]$ de la Definición 3.2.*

Output*: Los polinomios $S^{(0)}$, $S_{ij}^{(h)} \in \mathbb{Q}[C]$ para $1 \leq i \leq r, 1 \leq j \leq n_r, 1 \leq h \leq \delta$, definidos en el Lema 3.8 codificados por un* slp*.*

Procedimiento*:*

1. *Calcular un* slp *que codifique simultáneamente los polinomios en $\mathbb{Q}[C]$ que definen los coeficientes de Q, Q' y W_{ij} para $1 \leq i \leq r$, $1 \leq j \leq n_i$.*

2. *Calcular un* slp *que codifique simultáneamente los determinantes que dan las subresultantes con signo requeridas aplicando el algoritmo sin divisiones descripto en [Ber84] y agregar la codificación de las multiplicaciones necesarias.*

3. *Calcular un* slp *que codifique el determinante que da la resultante $S^{(0)}$ nuevamente aplicando el algoritmo sin divisiones descripto en [Ber84] y adjuntarlo al* slp *del paso anterior.*

Teorema 3.10 *El Algoritmo 3.9 calcula los polinomios* $S^{(0)}$, $S_{ij}^{(h)} \in \mathbb{Q}[C]$, $1 \leq i \leq r, 1 \leq j \leq n_r, 1 \leq h \leq \delta$, *utilizados para definir un conjunto de desigualdades sobre los valores de las ganancias de un juego genérico con la estructura considerada bajo las cuales el juego asociado tiene la máxima cantidad finita posible de equilibrios de Nash totalmente mixtos. La complejidad del algoritmo es*

$$O(\delta^2(n\delta^2 + L))$$

y el output *es un* slp *de longitud del mismo orden que la complejidad que codifica simultáneamente a todos los polinomios* $S^{(0)}$, $S_{ij}^{(h)}$, $1 \leq i \leq r, 1 \leq j \leq n_r, 1 \leq h \leq \delta$.

Demostración: La complejidad del primer paso es $O(\delta^2 L)$ y la longitud del *slp* obtenido es del mismo orden. Para explicar cómo llevar a cabo el segundo paso, notemos que el algoritmo en [Ber84] calcula, de hecho, todos los coeficientes del polinomio característico de una matriz y procede de manera recursiva, calculando en cada paso el polinomio característico de la matriz que se obtiene borrando una fila y una columna de la matriz considerada en el paso previo. En nuestro caso, para cada $1 \leq i \leq r$, $1 \leq j \leq n_i$, tenemos que para $0 \leq h \leq \delta - 1$, la matriz $\widehat{\mathrm{SH}}_h(Q, W_{ij})$ se obtiene a partir de $\widehat{\mathrm{SH}}_{h-1}(Q, W_{ij})$ borrando la primera y la última fila y las dos últimas columnas. Luego, todas las subresultantes con signo $\mathrm{sr}_h(Q, W_{ij})$ con $1 \leq h \leq \delta - 1$ son calculadas como resultados intermedios en el cálculo de $\mathrm{sr}_0(Q, W_{ij})$ eligiendo convenientemente las filas y columnas a ser eliminadas en cada paso. Procediendo de esta manera, la complejidad total del paso es $O(n\delta^4)$ y la longitud del *slp* obtenido es $O(\delta^2(n\delta^2 + L))$. Finalmente, el tercer paso es llevado a cabo utilizando una vez más este algoritmo con complejidad $O(\delta^4)$ y obteniendo un *slp* de longitud $O(\delta^2(\delta^2 + L))$. ▫

3.4. Equilibrios de Nash totalmente mixtos de un juego arbitrario

En la sección anterior desarrollamos métodos para obtener una resolución geométrica del conjunto de cuasi-equilibrios de un juego tratando a los valores de las ganancias como parámetros. Para juegos genéricos, vimos que esta resolución geométrica puede evaluarse directamente en los valores de las ganancias para describir el conjunto de cuasi-equilibrios del juego particular considerado y, a su vez, especificamos la condición de genericidad bajo la cual esto ocurre. En esta sección adaptaremos los

precedimientos desarrollados para obtener una resolución geométrica del conjunto de cuasi-equilibrios de un juego arbitrario, siempre y cuando dicho conjunto sea finito. Mostraremos además un método para calcular la cantidad de equilibrios de Nash totalmente mixtos en dicha situación.

El Lema 3.1 nos proporciona una condición necesaria y suficiente para caracterizar los vectores de matrices de pagos c tales que el conjunto V_c de cuasi-equilibirios es un conjunto finito. Nuestro primer objetivo en esta sección es dar un método para verificar dicha condición algorítmicamente. Primeramente, probemos el siguiente lema auxiliar.

Lema 3.11 *Sea c un vector de matrices de pagos, t una nueva variable y $\tilde{R} \in \mathbb{Q}[t]$ el polinomio que se obtiene especializando las variables $A^{(0)}$ en $R(A^{(0)}, a(c))$ en potencias sucesivas de t de la siguiente manera:*

$$A_J^{(0)} \mapsto t^{j_1+(n_1+1)j_2+\cdots+(\prod_{0\leq j\leq r-1}(n_j+1))j_r} \quad \begin{array}{l} \text{para } J = j_1 \dots j_r, \\ 0 \leq j_t \leq n_t, 1 \leq t \leq r. \end{array} \tag{3.12}$$

Entonces V_c es finito si y solo si $\tilde{R}(t)$ no es idénticamente nulo.

Demostración: Si V_c no es finito, entonces por el Lema 3.1 sabemos que $R(A^{(0)}, a(c))$ es idénticamente nulo y luego $\tilde{R}(t)$ también es idénticamente nulo. Supongamos ahora que V_c es finito. Para cada cuasi-equilibrio $\xi = ((\xi_{10} : \cdots : \xi_{1n_1}), \dots, (\xi_{r0} : \cdots : \xi_{rn_r}))$ del juego, sea

$$f_\xi(t) = \sum_J \xi_{1j_1} \dots \xi_{rj_r} t^{j_1+(n_1+1)j_2+\cdots+(\prod_{0\leq j\leq r-1}(n_j+1))j_r} \in \mathbb{C}[t],$$

que es un polinomio no idénticamente nulo debido al hecho de que existe al menos una opción de $j_1, \dots, j_r$ para la cual el producto $\xi_{1j_1} \dots \xi_{rj_r}$ no es 0. Observemos que las raíces de $\tilde{R}(t)$ son los valores $t_0 \in \mathbb{C}$ tales que existe un cuasi-equilibrio ξ del juego para el cual $f_\xi(t_0) = 0$. Entonces, como $\tilde{R}(t)$ tiene las mismas raíces que el polinomio no idénticamente nulo $\prod_{\xi\in V_c} f_\xi(t)$, $\tilde{R}(t)$ no es idénticamente nulo. ▫

A continuación exhibimos un algoritmo para verificar la condición de finitud sobre V_c e inmediatamente después calculamos la complejidad del mismo.

Algoritmo 3.12

Input*: El vector de matrices de pagos c.*

Output*: La respuesta a la pregunta si V_c es finito.*

Procedimiento*:*

1. *Calcular un* slp *que codifique la resultante R utilizando una versión adaptada del algoritmo en [JS07, Theorem 5] como especificaremos en la Sección 3.5.1.*

2. *Agregar al* slp *calculado la codificación de la evaluación*

$$\begin{aligned} A_J^{(0)} &\mapsto t^{j_1+(n_1+1)j_2+\cdots+(\prod_{0\le j\le r-1}(n_j+1))j_r} && \text{para } J=j_1\dots j_r,\\ &&& 0\le j_t\le n_t, 1\le t\le r,\\ A_{J_{-i}}^{(ik)} &\mapsto c^{(i)}_{j_1\dots j_{i-1}kj_{i+1}\dots j_r}-c^{(i)}_{j_1\dots j_{i-1}0j_{i+1}\dots j_r} && \text{para } 1\le i\le r, 1\le k\le n_i,\\ &&& J_{-i}=j_1\dots j_{i-1}j_{i+1}\cdots j_r,\\ &&& 0\le j_t\le n_t, 1\le t\le r, t\ne i, \end{aligned}$$

   para calcular el polinomio univariado $\tilde{R}$ del Lema 3.11.

3. *Evaluar $\tilde{R}$ en $(\prod_{1\le i\le r}(n_i+1)-1)\delta+1$ elementos de $\mathbb{Q}$ para decidir si $\tilde{R}$ es idénticamente nulo. En tal caso, responder que V_c no es finito; en caso contrario, responder que V_c es finito.*

Proposición 3.13 *El algoritmo 3.12 determina si el conjunto de cuasi-equilibrios de un juego es finito o no lo es con complejidad*

$$O\big(D^2(n_1\dots n_r)^2\delta(D+n_1\dots n_r\delta\log(D)r^2n^4(n^3+rN))\big).$$

Demostración: La correctitud del algoritmo es consecuencia del Lema 3.11.

El primer paso del algoritmo calcula un *slp* de longitud $O(D^2(D+n_1\dots n_r\delta\log(D)r^2 n^4(n^3+rN)))$ que codifica la resultante multihomogénea R con una complejidad del mismo orden. La especialización para obtener $\tilde{R}$ no suma a la complejidad ni cambia el orden de la longitud del *slp* calculado. Dado que $\deg(\tilde{R})\le(\prod_{1\le i\le r}(n_i+1)-1)\delta$, evaluando $\tilde{R}$ en $(\prod_{1\le i\le r}(n_i+1)-1)\delta+1$ valores distintos de t en $\mathbb{Q}$, podemos decidir si $\tilde{R}$ es idénticamente nulo. La cantidad de operaciones necesarias para realizar estas evaluaciones es la dada en el enunciado de la proposición. ▫

Una vez que sabemos que V_c es un conjunto finito, sabemos que V_c^{af} también lo es. En tal caso, podemos describir el conjunto de cuasi-equilibrios afines del juego mediante técnicas estándar (similares a las que utilizamos en la Proposición 2.16) que describimos a continuación.

Supongamos que $V_c^{\mathrm{af}} = \{\xi^{(1)}, \ldots, \xi^{(p_0)}\}$ donde para $1 \leq k \leq p_0$, $\xi^{(k)} = ((1 : \xi_{11}^{(k)} : \cdots : \xi_{1n_1}^{(k)}), \ldots, (1 : \xi_{r1}^{(k)} : \cdots : \xi_{rn_r}^{(k)}))$ y llamemos nuevamente $\xi^{(k)}$ a $(\xi_{11}^{(k)}, \ldots, \xi_{rn_r}^{(k)}) \in \mathbb{A}^n$. Sea $\tilde{V}_c^{\mathrm{af}} = \{\xi^{(1)}, \ldots, \xi^{(p_0)}\} \subset \mathbb{A}^n$ y sea $\alpha = (\alpha_{11}, \ldots, \alpha_{rn_r}) \in \mathbb{Q}^n$ tal que la forma lineal

$$l(x_{11}, \ldots, x_{rn_r}) := \sum_{1 \leq i \leq r,\, 1 \leq j \leq n_i} \alpha_{ij} x_{ij}$$

separa los puntos de $\tilde{V}_c^{\mathrm{af}}$. Consideremos los polinomios

$$f^{(0)} = A_0^{(0)} + \sum_{1 \leq i \leq r,\, 1 \leq j \leq n_i} A_{ij}^{(0)} x_{ij} \ \in \mathbb{Q}[A^{(0)}, x_1, \ldots, x_r],$$

y

$$Q(A^{(0)}) = \prod_{1 \leq k \leq p_0} f^{(0)}(A^{(0)}, \xi^{(k)}) \in \mathbb{C}[A^{(0)}].$$

Sean q y $w_{ij} \in \mathbb{C}[U]$ para $1 \leq i \leq r$, $1 \leq j \leq n_i$, los polinomios que se obtienen realizando la sustitución

$$\begin{aligned} A_0^{(0)} &\mapsto U, \\ A_{ij}^{(0)} &\mapsto -\alpha_{ij} \quad \text{para } 1 \leq i \leq r, 1 \leq j \leq n_i, \end{aligned}$$

en Q y $\frac{\partial Q}{\partial A_{ij}^{(0)}}$ respectivamente. Entonces $\{q, q', w_{11}, \ldots, w_{rn_r}\} \subset \mathbb{C}[U]$ es una resolución geométrica de $\tilde{V}_c^{\mathrm{af}}$. De hecho, las raíces de q son los valores $l(\xi^{(1)}), \ldots, l(\xi^{(p)})$, los cuales resultan todos distintos, y para $1 \leq k \leq p_0, 1 \leq i \leq r, 1 \leq j \leq n_i$ tenemos que

$$q'(l(\xi^{(k)})) \ = \prod_{\substack{1 \leq k' \leq p_0 \\ k' \neq k}} \big(l(\xi^{(k)}) - l(\xi^{(k')})\big) \neq 0,$$

$$w_{ij}(l(\xi^{(k)})) \ = \ \xi_{ij}^{(k)} \prod_{\substack{1 \leq k' \leq p_0 \\ k' \neq k}} \big(l(\xi^{(k)}) - l(\xi^{(k')})\big) \ = \ \xi_{ij}^{(k)} q'(l(\xi^{(k)})),$$

lo que prueba lo afirmado.

La siguiente observación nos será útil más adelante para calcular el polinomio Q recién introducido.

Observación 3.14 *Sea c un vector de matrices de pagos que define un juego con conjunto de cuasi-equilibrios finito $V_c = \{\xi^{(1)}, \ldots, \xi^{(p)}\}$. Para $1 \leq k \leq p$, elijamos una representación de $\xi^{(k)}$ mediante coordenadas $((\xi_{10}^{(k)}, \ldots, \xi_{1n_1}^{(k)}), \ldots, (\xi_{r0}^{(k)}, \ldots, \xi_{rn_r}^{(k)}))$ tal que si $\xi^{(1)}, \ldots, \xi^{(p_0)}$ son los cuasi-equilibrios afines del juego, entonces $\xi_{i0}^{(k)} = 1$ para $1 \leq k \leq p_0, 1 \leq i \leq r$. Como $R(A^{(0)}, a(c))$ y $\prod_{1 \leq k \leq p} F^{(0)}(A^{(0)}, \xi^{(k)})$ definen la misma variedad en $\mathbb{A}^{(n_1+1)\ldots(n_r+1)}$ y los polinomios $F^{(0)}(A^{(0)}, \xi^{(k)})$ y $F^{(0)}(A^{(0)}, \xi^{(k')})$ son irreducibles y coprimos en $\mathbb{C}[A^{(0)}]$ para $1 \leq k < k' \leq p$, por el Nullstellensatz tenemos que existen una constante $b \in \mathbb{C}$ y $m_1, \ldots, m_p \in \mathbb{N}$ tales que*

$$R(A^{(0)}, a(c)) = b \prod_{1 \leq k \leq p} F^{(0)}(A^{(0)}, \xi^{(k)})^{m_k} \in \mathbb{Q}[A^{(0)}]. \tag{3.13}$$

A continuación damos el esquema del algoritmo para calcular la resolución geométrica buscada. En el teorema que le sigue, detallamos cómo llevar a cabo los sucesivos pasos del algoritmo y analizamos su complejidad.

Algoritmo 3.15

Input*: El vector de matrices de pagos c.*

Output*: Una resolución geométrica $\{q, q', w_{11}, \ldots, w_{rn_r}\}$ del conjunto de cuasi-equilibrios afines del juego asociado a c.*

Procedimiento*:*

1. *Calcular el polinomio $R(A^{(0)}, a(c)) = b \prod_{1 \leq k \leq p} F^{(0)}(A^{(0)}, \xi^{(k)})^{m_k}$.*
2. *Calcular el polinomio $\prod_{1 \leq k \leq p_0} F^{(0)}(A^{(0)}, \xi^{(k)})^{m_k}$.*
3. *Calcular el polinomio $\prod_{1 \leq k \leq p_0} f^{(0)}(A^{(0)}, \xi^{(k)})^{m_k}$.*
4. *Calcular el polinomio $Q = \prod_{1 \leq k \leq p_0} f^{(0)}(A^{(0)}, \xi^{(k)})$ y el vector de coeficientes $\alpha \in \mathbb{Q}^n$ de una forma lineal l que separa los cuasi-equilibrios afines del juego definido por c.*
5. *Calcular los polinomios q, q' y w_{ij} para $1 \leq i \leq r, 1 \leq j \leq n_i$.*

Teorema 3.16 *Dado el vector c de matrices de pagos de un juego entre r jugadores que disponen de $n_1+1,\dots,n_r+1$ estrategias puras y que tiene un conjunto finito de cuasi-equilibrios, el Algoritmo 3.15 calcula una resolución geométrica del conjunto de cuasi-equilibrios afines del juego asociado a c con complejidad*

$$O\big(\delta^9 D^2(D+n_1\dots n_r\delta\log(D)r^2n^5(n^3+rN))\big).$$

Demostración: Detallemos cómo llevar a cabo cada paso y analicemos la complejidad correspondiente.

Paso 1: El polinomio R es obtenido utilizando la versión adaptada del procedimiento en [JS07, Theorem 5] que especificaremos en la Sección 3.5.1. La complejidad de este paso es $O(D^2(D+n_1\dots n_r\delta\log(D)r^2\ n^4(n^3+rN)))$ y la longitud del *slp* obtenido, a la que llamamos L, es del mismo orden. Realizar la evaluación de las variables $A^{(ik)}$ para $1\le i\le r, 1\le k\le n_i$ para obtener $R(A^{(0)},a(c))$ no suma a la complejidad del paso ni modifica la longitud del *slp* obtenido.

Paso 2: Notemos que el polinomio que queremos calcular es mónico en la variable $A_0^{(0)}$ y por otro lado $b\prod_{p_0+1\le k\le p}F^{(0)}(A^{(0)},\xi^{(k)})^{m_k}$ no depende de esta variable. Luego este último polinomio es el coeficiente principal de $R(A^{(0)},a(c))$ en la variable $A_0^{(0)}$. Llamemos d al grado de dicho polinomio en dicha variable.

Primeramente, veamos cómo calcular d. Sea $t_0\in\mathbb{Q}$ tal que el polinomio $\tilde{R}$ del Lema 3.11 no se anula en t_0 (observemos que si ya ejecutamos el Algoritmo 3.12 para verificar que el conjunto de cuasi-equilibrios es finito, conocemos un valor posible para t_0; en caso contrario debemos ejecutar dicho algoritmo y sumar la complejidad correspondiente). Sea $\tilde{r}\in\mathbb{Q}[A_0^{(0)}]$ el polinomio que se obtiene a partir de $R(A^{(0)},a(c))$ especializando las variables $A^{(0)}$ excepto $A_0^{(0)}$ en potencias sucesivas de t_0 como en (3.12). Este polinomio es no nulo pues $\tilde{r}(1)=\tilde{R}(t_0)\neq 0$. Por (3.13), tenemos que $\deg(\tilde{r})=d$ y, por lo tanto, para calcular d es suficiente con calcular los coeficientes de $\tilde{r}$ hasta grado δ, que es una cota para el grado de $\tilde{r}$ en $A_0^{(0)}$. Esto puede ser llevado a cabo con complejidad $O(\delta^2L)$ siguiendo [BCS97, Lema 21.25].

Una vez conocido d, siguiendo nuevamente [BCS97, Lema 21.25] calculamos un *slp* de longitud $O(\delta^2L)$ para $b\prod_{p_0+1\le k\le p}F^{(0)}(A^{(0)},\xi^{(k)})^{m_k}$, que es el coeficiente correspondiente a $(A_0^{(0)})^d$ en $R(A_0^{(0)},a(c))$. Finalmente obtenemos $\prod_{1\le k\le p_0}F^{(0)}(A^{(0)},\xi^{(k)})^{m_k}$ dividiendo $R(A^{(0)},a(c))$ por este coeficiente. Como el divisor no se anula cuando sus variables son especializadas en las sucesivas potencias de t_0, esta división puede realizarse con el algoritmo [Str73] con complejidad $O(\delta^4L)$, lo que produce un *slp* del mismo orden.

Paso 3: Como el polinomio $f^{(0)}$ se obtiene a partir de $F^{(0)}$ especializando en 0 todas las variables $A^{(0)}$ excepto $A_0^{(0)}$ y $A_{ij}^{(0)}$ para $1 \leq i \leq r, 1 \leq j \leq n_i$, este paso se lleva a cabo simplemente realizando esta especialización en el polinomio calculado en el paso anterior. La complejidad correspondiente no suma a la complejidad total del algoritmo.

Paso 4: Sean $P = \prod_{1 \leq k \leq p_0} f^{(0)}(A^{(0)}, \xi^{(k)})^{m_k}$ el polinomio calculado en el paso anterior y G el polinomio $\prod_{1 \leq k \leq p_0} f^{(0)}(A^{(0)}, \xi^{(k)})^{m_k - 1}$; luego $Q = P/G$. Es fácil ver que G es el máximo común divisor entre P y $\frac{\partial P}{\partial A_0^{(0)}}$, luego podemos calcular el polinomio G adaptando el procedimiento basado en el cálculo de subresultantes descripto, por ejemplo, en [BT71].

Sea u una nueva variable. Para todo polinomio F que involucre las variables $A_{ij}^{(0)}$, $1 \leq i \leq r, 1 \leq j \leq n_i$, notaremos F_u al polinomio que se obtiene a partir de F especializando todas estas variables en potencias sucesivas de la variable u.

Para $1 \leq k < k' \leq p_0$, $f_u^{(0)}(A_0^{(0)}, u, \xi^{(k)})$ y $f_u^{(0)}(A_0^{(0)}, u, \xi^{(k')})$ son polinomios irreducibles coprimos en $\mathbb{C}[A_0^{(0)}, u]$; por lo tanto,

$$G_u = \prod_{1 \leq k \leq p_0} f_u^{(0)}(A_0^{(0)}, u, \xi^{(k)})^{m_k - 1} = \gcd\Big(P_u, \frac{\partial P_u}{\partial A_0^{(0)}}\Big) \in \mathbb{C}[A_0^{(0)}, u]$$

y $\tilde{d} := \deg_{A_0^{(0)}}(G) = \deg_{A_0^{(0)}}(G_u)$.

Para calcular $\tilde{d}$, buscamos la primera subresultante entre P_u y $\frac{\partial P_u}{\partial A_0^{(0)}}$ (considerándolos como polinomios en la variable $A_0^{(0)}$) que resulta no nula. Obtenemos primero un *slp* de longitud $O(\delta^4 L)$ para P_u, luego, siguiendo [BCS97, Lema 21.25], un *slp* de longitud $O(\delta^6 L)$ para sus coeficientes en la variable $A_0^{(0)}$ y finalmente, siguiendo [Ber84] un *slp* de longitud $O(\delta^6 L)$ para todas las subresultantes entre P_u y $\frac{\partial P_u}{\partial A_0^{(0)}}$, que son polinomios de grado a lo sumo $2\delta^2 n$ en $\mathbb{Q}[u]$. Para decidir cuál es la primera subresultante no nula, el algoritmo evalúa la variable u en una cantidad suficiente de elementos de $\mathbb{Q}$ con complejidad $O(\delta^8 L n)$.

Utilizando nuevamente los algoritmos [BCS97, Lema 21.25] y [Ber84], una vez conocido $\tilde{d}$ podemos calcular un *slp* de longitud $O(\delta^6 L)$ que codifique los coeficientes del polinomio P en la variable $A^{(0)}$, la $\tilde{d}$-ésima subresultante entre P y $\frac{\partial P}{\partial A_0^{(0)}}$ a la que llamaremos s, y el $\tilde{d}$-ésimo polinomio subresultante (ver [BPR03, Notation 8.52]) entre P y $\frac{\partial P}{\partial A_0^{(0)}}$, que coincide con el polinomio sG.

Finalmente, obtenemos Q dividiendo sP por sG. Notemos que ya conocemos un punto α donde s no se anula (el valor obtenido para calcular $\tilde{d}$). Luego, evaluando el

polinomio no nulo $G(A_0^{(0)}, \alpha) \in \mathbb{Q}[A_0^{(0)}]$ de grado $\tilde{d}$ en a lo sumo $\tilde{d}+1$ elementos de $\mathbb{Q}$, obtenemos un valor $a_0^{(0)} \in \mathbb{Q}$ tal que $(sG)(a_0^{(0)}, \alpha) \neq 0$. Esto nos permite calcular el cociente Q aplicando el algoritmo en [Str73]. La longitud del *slp* obtenido y la complejidad del paso es $O(\delta^8 L)$.

Observemos que la condición $s(\alpha) \neq 0$ implica que el polinomio $(P/G)(A_0^{(0)}, \alpha)$ es libre de cuadrados, y por lo tanto α es el vector de coeficientes de una forma lineal l que separa los puntos de $\tilde{V}_c^{\mathrm{af}}$.

Paso 5: Calculamos un *slp* de longitud $O(\delta^8 L)$ que codifique simultáneamente a Q y todas sus derivadas parciales siguiendo el algoritmo en [BS83], y luego realizamos la especialización de las variables $A_{ij}^{(0)}$ en $-\alpha_{ij}$ para $1 \leq i \leq r, 1 \leq j \leq n_i$. Como los polinomios obtenidos tienen grado acotado por δ, para calcular la codificación densa de ellos interpolamos los valores que toman en $\delta+1$ elementos de $\mathbb{Q}$, siguiendo, por ejemplo, [vzGG99, Chapter 10]. La complejidad del paso es $O(\delta^9 Ln)$. ▫

Usando métodos clásicos (como, por ejemplo, [BOKR86], [Can93]), podemos ahora dar una descripción y calcular la cantidad de equilibrios de Nash totalmente mixtos de un juego con conjunto de cuasi-equilibrios cero-dimensional.

Proposición 3.17 *Es posible calcular la cantidad de equilibrios de Nash totalmente mixtos del juego con r jugadores que disponen de $n_1+1, \ldots, n_r+1$ estrategias puras definido por el vector de matrices de pagos c, si el conjunto de cuasi-equilibrios V_c es finito, con complejidad*

$$O\big(\delta^9 D^2 (D + n_1 \ldots n_r \delta \log(D) r^2 n^5 (n^3 + rN))\big).$$

Demostración: Sean q y w_{ij}, $1 \leq i \leq r, 1 \leq j \leq n_i$, los polinomios que componen la resolución geométrica del conjunto de cuasi-equilibrios afines del juego asociado a c obtenida por el Algoritmo 3.15. El conjunto de equilibrios de Nash totalmente mixtos del juego está formado por los puntos $(\xi_1, \ldots, \xi_r)$ con $\xi_i = (q'(u)/s_i(u), w_{i1}(u)/s_i(u), \ldots, w_{ir}(u)/s_i(u))$, donde $s_i = q' + \sum_{1 \leq j \leq n_i} w_{ij}$ para $1 \leq i \leq r$, y u es una raíz de q, que tienen todas sus coordenadas reales positivas. Luego, la cantidad de equilibrios de Nash totalmente mixtos es el cardinal del conjunto

$$\Big\{u \in \mathbb{R} \mid q(u) = 0,\, q'(u) > 0,\, w_{ij}(u) > 0 \ \text{ para } 1 \leq i \leq r,\, 1 \leq j \leq n_i\Big\} \bigcup$$

$$\Big\{u \in \mathbb{R} \mid q(u) = 0,\, q'(u) < 0,\, w_{ij}(u) < 0 \ \text{ para } 1 \leq i \leq r,\, 1 \leq j \leq n_i\Big\}.$$

Es posible calcular el cardinal de este conjunto usando el algoritmo en [Can93, Section 3] con complejidad $O(n\delta^\omega)$, donde ω es un número real positivo tal que para todo $m \in \mathbb{N}$ es posible invertir matrices en $\mathbb{Q}^{m\times m}$ con $O(m^\omega)$ operaciones en $\mathbb{Q}$, el cual podemos suponer menor o igual a 2,376 (ver [CW90]). ▫

Observación 3.18 *El algoritmo de la Proposición 3.17 puede adaptarse (con la misma complejidad) para calcular la lista de codificaciones de Thom (ver [CR88] para la definición de esta codificación) de las raíces reales del polinomio q en la resolución geométrica del conjunto de cuasi-equilibrios afines del juego que proporcionan equilibrios de Nash totalmente mixtos.*

3.5. Resultantes multihomogéneas

3.5.1. Cálculo de resultantes

El procedimiento en [JS07, Theorem 5] proporciona una manera de calcular resultantes multihomogéneas bajo la suposición de que todas las coordenadas de cada multigrado son números positivos. En esta sección adaptamos dicho procedimiento a nuestro contexto, en el cual esta condición no se cumple.

A tal efecto, utilizaremos la teoría en [Stu94] y [Min03]. Podemos utilizar estos resultados en nuestro caso porque las resultantes multihomogéneas de una familia de polinomios multihomogéneos $G_0, \ldots, G_n$ en r grupos de variables $x_j = (x_{j0}, \ldots, x_{jn_j})$, con $\sum_{1\le j\le r} n_j = n$, coincide con la resultante rala de los polinomios deshomogeneizados $g_0, \ldots, g_n$ obtenidos mediante la evaluación $x_{j0} = 1$ para cada $1 \le j \le r$.

Sean $\mathcal{A}_0, \ldots, \mathcal{A}_n \subset \mathbb{Z}^n$ conjuntos finitos y sean $g_0, \ldots, g_n$ polinomios con soporte $\mathcal{A}_0, \ldots, \mathcal{A}_n$ respectivamente. Para cada subconjunto $J \subseteq \{0, \ldots, n\}$, sea $\mathcal{L}_J$ el reticulado generado por $\sum_{j\in J} \mathcal{A}_j$. Siguiendo [Stu94], para $I \subset \{0, \ldots, n\}$ la colección de soportes $\{\mathcal{A}_i\}_{i\in I}$ se dice *esencial* si $\operatorname{rank} \mathcal{L}_I = \#I - 1$ y $\operatorname{rank} \mathcal{L}_J \ge \#J$ para cada subconjunto propio J de I. Si $\{\mathcal{A}_0, \ldots, \mathcal{A}_n\}$ tiene una única subcolección $\{\mathcal{A}_i\}_{i\in I}$ esencial, la resultante $\operatorname{Res}(g_0, \ldots, g_n)$ no es constante y coincide con la resultante $\operatorname{Res}(g_i; i \in I)$ (ver [Stu94, Corollary 1.1]).

Proposición 3.19 *Sean $n_1, \ldots, n_r \in \mathbb{N}$ tales que $n_i \le \sum_{1\le j\le r, j\ne i} n_j$ para todo $1 \le i \le r$, y sea $n := \sum_{1\le i\le r} n_i$. La resultante de $n+1$ polinomios multihomogéneos genéricos $F^{(0)}, F_1^{(1)}, \ldots, F_{n_1}^{(1)}, \ldots, F_1^{(r)}, \ldots, F_{n_r}^{(r)}$ en r grupos de $n_1 + 1, \ldots, n_r + 1$*

variables, donde $F^{(0)}$ *tiene multigrado* $d_0 = (1, \dots, 1)$ *y, para cada* $1 \leq i \leq r, 1 \leq k \leq n_i$ $F_k^{(i)}$ *tiene multigrado* $d_i = (1, \dots, 0, \dots, 1)$ *donde el* 0 *se encuentra en el* i*-ésimo lugar, es un polinomio no constante y puede ser calculado algorítmicamente con complejidad* $O(D^2(D + n_1 \dots n_r \delta \log(D) r^2 n^4 (n^3 + rN)))$*, donde* D, δ *y* N *son como en la Sección 3.3.1.*

Demostración: Para calcular la resultante R aplicaremos recursivamente la fórmula de Poisson ([Min03, Lemma 13]). Una vez establecida la validez de esta fórmula, todos los cálculos requeridos pueden efectuarse de la misma manera que en [JS07, Theorem 5] y luego la complejidad del algoritmo y la longitud del *slp* obtenido son del mismo orden que los enunciados en dicho teorema. En cada paso de la recursión debemos calcular una resultante multihomogénea en alguna de las siguientes situaciones, donde $m_1, \dots, m_r \in \mathbb{N}$ y $m := \sum_{1 \leq i \leq r} m_i$:

(I) r grupos de $m_1 + 1, \dots, m_r + 1$ variables, un polinomio multihomogéneo de multigrado d_0 y m_i polinomios multihomogéneos de multigrado d_i para cada $1 \leq i \leq r$, donde $m_i \leq \sum_{1 \leq j \leq r, j \neq i} m_j$ para todo i,

(II) r grupos de $m_1 + 1, \dots, m_r + 1$ variables y $m + 1$ polinomios multihomogéneos de multigrado d_0,

(III) r grupos de $m_1, m_2 + 1, \dots, m_r + 1$ variables y m_i polinomios multihomogéneos de multigrado d_i para cada $1 \leq i \leq r$, donde $m_i \leq \sum_{1 \leq j \leq r, j \neq i} m_j$ para todo i.

A continuación definimos la recursión para calcular la resultante buscada. Los polinomios $F^{(0)}, F_1^{(1)}, \dots, F_{n_r}^{(r)}$ con los que comenzamos se encuentran en el caso (I) con $m_i = n_i$ para $1 \leq i \leq r$.

Resolvamos el caso (I) en general: Sean $G_0^{(0)}$ y $G_k^{(i)}$, $1 \leq i \leq r, 1 \leq k \leq m_i$, una familia de polinomios como en el caso (I) y sea $\mathcal{I} := \{(0,0)\} \cup \{(i,k) \mid 1 \leq i \leq r,\ 1 \leq k \leq m_i\}$. Para empezar, notemos que $\operatorname{rank} \mathcal{L}_{\mathcal{I}} = m = \#\mathcal{I} - 1$. Sea J un subconjunto propio de $\mathcal{I}$. Si existen (i,k), (i',k') en J con $i \neq i'$, entonces $\operatorname{rank} \mathcal{L}_J = m \geq \#J$ y lo mismo vale si $(0,0) \in J$. Por otro lado, si $J \subset \{(i,k) : 1 \leq k \leq m_i\}$ para algún $i \neq 0$ fijo, entonces $\operatorname{rank} \mathcal{L}_J = \sum_{1 \leq j \leq r, j \neq i} m_j \geq m_i \geq \#J$. Luego, el conjunto de todos los soportes es el único subconjunto esencial. Por lo tanto, la resultante no es constante y vale la siguiente igualdad:

$$\operatorname{Res}(G_0^{(0)}, (G_k^{(i)})_{1 \leq i \leq r; 1 \leq k \leq m_i}) = \Big(\prod_{\xi \in V} g_0^{(0)}(\xi) \Big) \Big(\prod_{1 \leq j \leq r} \operatorname{Res}((G_{kj}^{(i)})_{1 \leq i \leq r, 1 \leq k \leq m_i}) \Big),$$

donde $g_0^{(0)}$ es la deshomogeneización de $G_0^{(0)}$ mediante la evaluación $x_{\ell\, m_\ell} = 1$ para cada $1 \leq \ell \leq r$, V es el conjunto de ceros comunes en $\mathbb{A}^m$ de los polinomios $g_k^{(i)}$, $1 \leq i \leq r, 1 \leq k \leq m_i$, obtenidos de la misma forma a partir de $G_k^{(i)}$ y, para cada $1 \leq j \leq r$, $G_{kj}^{(i)}$ es el polinomio obtenido a partir de $G_k^{(i)}$ mediante la evaluación $x_{j\, m_j} = 0$. Notemos que este resultado aplicado a los polinomios $F^{(0)}, F_1^{(1)}, \ldots, F_{n_r}^{(r)}$ implica que la resultante R que queremos calcular es un polinomio no nulo.

(I.a) Si $m_i \geq 2$ para todo $1 \leq i \leq r$, renombrando las variables y los polinomios si es necesario, cada una de las resultantes $\mathrm{Res}(G_{kj}^{(i)})$ involucra una familia de polinomios que se encuentra en el caso (III).

(I.b) Sin pérdida de generalidad, supongamos ahora que $m_1 = 1$. Cuando calculamos $\mathrm{Res}((G_{k1}^{(i)})_{1\leq i\leq r, 1\leq k\leq m_i})$ podemos eliminar el primer grupo de variables. Entonces esta resultante involucra m polinomios en $r-1$ grupos de $m_2+1, \ldots, m_r+1$ variables cada uno con m_i polinomios con multigrado $(1, \ldots, 0, \ldots, 1)$, donde el 0 ocupa el $(i-1)$-ésimo lugar para $2 \leq i \leq r$, y uno con multigrado $(1, \ldots, 1)$.

Si, para $2 \leq i \leq r$, $m_i < \sum_{1\leq j\leq r,\, j\neq i} m_j$, dado que $m_1 = 1$ deducimos que $m_i \leq \sum_{2\leq j\leq r,\, j\neq i} m_j$ y por lo tanto, la familia de polinomios obtenida se encuentra en el caso (I) pero con un grupo de variables menos que el original. Por otro lado, si $m_i = 1+\sum_{2\leq j\leq r,\, j\neq i} m_j$ para algún $2 \leq i \leq r$, entonces $m_j < m_i$ para todo $j \neq i$. Luego, el único subconjunto esencial es $\{(i,k) : 1 \leq k \leq m_i\}$ y la resultante que debemos calcular es la resultante de una familia de m_i polinomios de multigrado $(1, \ldots, 1)$ en $r-2$ grupos de $m_2+1, \ldots, m_{i-1}+1, m_{i+1}+1, \ldots, m_r+1$ variables cada uno; esta familia de polinomios se encuentra en el caso (II).

En el caso (II), podemos aplicar directamente el algoritmo en [JS07, Theorem 5] ya que todas las coordenadas de los multigrados son números positivos.

Finalmente, analicemos el caso (III). Consideremos primero el caso en que $r = 2$. En este caso, las hipótesis sobre los números m_i implican que $m_1 = m_2 := M$.

(III.a) Consideramos la resultante de M polinomios con multigrados $(0,1)$ y M polinomios con multigrados $(1,0)$ en dos grupos de M y $M+1$ variables respectivamente. El único conjunto esencial es el correspondiente a los M primeros polinomios y, por lo tanto, la resultante es igual al determinante de su matriz de coeficientes.

Supongamos ahora que $r > 2$. Notemos que la igualdad $m_i = \sum_{1\leq j\leq r, j\neq i} m_j$ puede valer a lo sumo para un único valor de i: si por el contrario, $m_{i_1} = \sum_{1\leq j\leq r, j\neq i_1} m_j$ y $m_{i_2} = \sum_{1\leq j\leq r, j\neq i_2} m_j$ valen para $i_1 \neq i_2$, se sigue que $\sum_{1\leq j\leq r, j\neq i_1, j\neq i_2} m_j = 0$, lo cual implica que $r = 2$. Sea $G_k^{(i)}, 1 \leq i \leq r$, $1 \leq k \leq m_i$, una familia de polinomios que satisface las condiciones (III).

(III.b) Si $m_1 = 1$, esta familia se encuentra en el caso (I.b).

(III.c) Si $m_1 \geq 2$ y $m_i = \sum_{1\leq j\leq r, j\neq i} m_j$ para algún $2 \leq i \leq r$, el conjunto $\{(i,k) : 1 \leq k \leq m_i\}$ es el único subconjunto esencial. Luego la resultante involucra m_i polinomios de multigrado $(1,\ldots,1)$ en $r-1$ grupos de $m_1, m_2+1, \ldots, m_{i-1}+1, m_{i+1}+1 \ldots, m_r+1$ variables respectivamente y, por lo tanto, la familia se encuentra en el caso (II).

(III.d) Si $m_1 \geq 2$ y $m_i < \sum_{1\leq j\leq r, j\neq i} m_j$ para todo $2 \leq i \leq r$, entonces $m_i \leq m_1 - 1 + \sum_{2\leq j\leq r, j\neq i} m_j$ para todo $2 \leq i \leq r$. Luego, el único subconjunto esencial es toda la familia de soportes y aplicando la fórmula de Poisson obtenemos:

$$\mathrm{Res}((G_k^{(i)})_{1\leq i\leq r; 1\leq k\leq m_i}) = (\prod_{\xi\in V} g_1^{(1)}(\xi))(\prod_{2\leq l\leq r} \mathrm{Res}((G_{kl}^{(1)})_{2\leq k\leq m_1}; (G_{kl}^{(i)})_{2\leq i\leq r, 1\leq k\leq m_i}))$$

donde $g_1^{(1)}$ es la deshomogeneización de $G_1^{(1)}$ mediante la evaluación $x_{jm_j} = 1$ para cada $1 \leq j \leq r$, V es el conjunto de ceros comunes en $\mathbb{A}^{m-1}$ de los polinomios $g_k^{(1)}, 2 \leq k \leq m_1$ y $g_k^{(i)}, 2 \leq i \leq r, 1 \leq k \leq m_i$ obtenidos de la misma forma a partir de $G_k^{(i)}$, y $G_{kl}^{(i)}$ es el polinomio obtenido a partir de $G_k^{(i)}$ mediante la evaluación $x_{l\,m_l} = 0$.

Para $2 \leq l \leq r$, tomando $m' := m-1$, $m_1' := m_1 - 1$ y $m_i' := m_i$ para $i \neq 1$, la resultante a calcular involucra m' polinomios en r grupos de $m_1' + 1, \ldots, m_{l-1}' + 1, m_l', m_{l+1}' + 1, \ldots, m_r' + 1$ variables cada uno con m_i' polinomios de multigrado d_i para cada $1 \leq i \leq r$. Tenemos que $m_1' \leq \sum_{2\leq j\leq r} m_j'$ y, para $i \neq 1$, la condición $m_i < \sum_{1\leq j\leq r, j\neq i} m_j$ implica que $m_i' \leq \sum_{1\leq j\leq r, j\neq i} m_j'$; luego, renombrando las variables y los polinomios, estamos nuevamente bajo las condiciones (III).

□

3.5.2. Una cota para el grado de la resultante

Hemos acotado la complejidad de todos los algoritmos desarrollados en el capítulo de manera polinomial en función del número r de jugadores, el número de estrategias

puras $n_1, \ldots, n_r$ de los r jugadores, la máxima cantidad finita δ de equilibrios de Nash totalmente mixtos para un juego con la estructura considerada y el parámetro D, que es el grado total de la resultante R. Como vimos en la Sección 3.3.1, $D = \delta + \sum_{1 \leq i \leq r} n_i \delta_i$, con

$$\delta_i = \mathrm{Bez}_{n_1,\ldots,n_r}(d_0, 1; d_1, n_1; \ldots; d_i, n_i - 1; \ldots; d_r, n_r),$$

donde $d_0, d_1, \ldots, d_r$ son los multigrados de los polinomios $F^{(0)}, F^{(1)}_{j_1}(1 \leq j_1 \leq n_1), \ldots, F^{(r)}_{j_r}(1 \leq j_r \leq n_r)$ respectivamente. El objetivo de esta sección es exhibir una cota para D polinomial en los otros parámetros mencionados anteriormente. De esta manera, obtenemos que la complejidad de todos los algoritmos presentados en este capítulo es polinomial en los parámetros propios de la estructura de juego considerada.

Proposición 3.20 *El grado D de la resultante R puede acotarse de la siguiente manera*

$$D \leq \Big(1 + \sum_{1 \leq i \leq r} n_i(n_i + 1)\Big)\delta \leq n^2\delta.$$

Demostración: Veamos que $\delta_i \leq (n_i + 1)\delta$ para $1 \leq i \leq r$. Sin pérdida de generalidad, supongamos $i = 1$. Como el número de Bézout es aditivo en cada uno de los multigrados involucrados (ver igualdad (2) en la Sección 0.3.2) y $d_0 = d_1 + e_1$ donde $e_1 = (1, 0, \ldots, 0)$, tenemos que δ_1 es igual a

$$\mathrm{Bez}_{n_1,\ldots,n_r}(d_1, n_1; d_2, n_2; \ldots; d_r, n_r) + \mathrm{Bez}_{n_1,\ldots,n_r}(e_1, 1; d_1, n_1 - 1; d_2, n_2; \ldots; d_r, n_r) =$$

$$= \delta + \mathrm{Bez}_{n_1,\ldots,n_r}(e_1, 1; d_1, n_1 - 1; d_2, n_2; \ldots; d_r, n_r).$$

Es fácil ver que $\mathrm{Bez}_{n_1,\ldots,n_r}(e_1, 1; d_1, n_1 - 1; d_2, n_2; \ldots; d_r, n_r) = \#\mathfrak{J}_1$ con

$$\mathfrak{J}_1 := \Big\{(j_{11}, \ldots, j_{rn_r}) \in \{1, \ldots, r\}^n \mid j_{11} = 1,\ j_{ik} \neq i \text{ para } (i,k) \neq (1,1) \text{ y}$$

$$\#\{j_{hk} \,|\, j_{hk} = i\} = n_i \text{ para } 1 \leq i \leq r\Big\}.$$

Recordando que δ es el cardinal del conjunto $\mathfrak{J}_0$ definido en (3.5), para finalizar la demostración, es suficiente con probar que $\#\mathfrak{J}_1 \leq n_1 \#\mathfrak{J}_0$.
Definamos la siguiente función de $\mathfrak{J}_1$ a $\mathfrak{J}_0$: a cada n-upla

$$j = (1, j_{12}, \ldots, j_{1n_1}, \ldots, j_{r1}, \ldots, j_{rn_r}) \in \mathfrak{J}_1$$

le asociamos la n-upla $j' \in \mathfrak{J}_0$ que se obtiene intercambiando la primera coordenada de j (que es un 1) con la primera que es diferente de 1 y se encuentra después de la n_1-ésima coordenada. Tal coordenada existe pues suponemos $n_1 \leq \sum_{2 \leq i \leq r} n_i$ y además se encuentra entre las coordenadas $n_1 + 1$ y $2n_1$ de j. Para probar el lema, veamos que cada elemento de $\mathfrak{J}_0$ es la imagen de a lo sumo n_1 elementos de $\mathfrak{J}_1$. Si j' está en la imagen de esta función, el vector formado por las n_1 coordenadas $n_1 + 1, \ldots, 2n_1$ en j' debe ser de la forma $(1, \ldots, 1, j_{hk}, \ldots)$ y la cantidad de coordenadas iguales a 1 al comienzo del mismo puede variar entre 1 y n_1. Concluimos entonces que hay a lo sumo n_1 n-uplas en la preimagen de j', ya que cada una de ellas puede obtenerse intercambiando la primera coordenada de j' con alguna de estas coordenadas iguales a 1. ▫

Bibliografía

[ABRW96] M.-E. Alonso, E. Becker, M.-F. Roy y T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. En *Algorithms in algebraic geometry and applications (Santander, 1994)*, volumen 143 de *Progr. Math.*, páginas 1–15. Birkhäuser, Basel, 1996.

[ARSED02] P. Aubry, F. Rouillier y M. Safey El Din. Real solving for positive dimensional systems. *J. Symbolic Comput.*, 34(6):543–560, 2002.

[BBP97] D. Bailey, P. Borwein y S. Plouffe. On the rapid computation of various polylogarithmic constants. *Math. Comp.*, 66(218):903–913, 1997.

[BCR98] J. Bochnak, M. Coste y M.-F. Roy. *Real algebraic geometry*, volumen 36 de *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1998.

[BCS97] P. Bürgisser, M. Clausen y M. Shokrollahi. *Algebraic complexity theory*, volumen 315 de *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1997.

[BCSS98] L. Blum, F. Cucker, M. Shub y S. Smale. *Complexity and real computation*. Springer-Verlag, New York, 1998.

[Ber75] D. Bernstein. The number of roots of a system of equations. *Funkcional. Anal. i Priložen.*, 9(3):1–4, 1975.

[Ber84] S. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Inform. Process. Lett.*, 18(3):147–150, 1984.

[BGHM97] B. Bank, M. Giusti, J. Heintz y G. Mbakop. Polar varieties, real equation solving, and data structures: the hypersurface case. *J. Complexity*, 13(1):5–27, 1997.

[BGHM01] B. Bank, M. Giusti, J. Heintz y G. Mbakop. Polar varieties and efficient real elimination. *Math. Z.*, 238(1):115–144, 2001.

[BGHP04] B. Bank, M. Giusti, J. Heintz y L. Pardo. Generalized polar varieties and an efficient real elimination procedure. *Kybernetika (Prague)*, 40(5):519–550, 2004.

[BGHP05] B. Bank, M. Giusti, J. Heintz y L. Pardo. Generalized polar varieties: geometry and algorithms. *J. Complexity*, 21(4):377–412, 2005.

[BOKR86] M. Ben-Or, D. Kozen y J. Reif. The complexity of elementary algebra and geometry. *J. Comput. System Sci.*, 32(2):251–264, 1986. 16th annual ACM-SIGACT symposium on the theory of computing (Washington, D.C., 1984).

[BP94] D. Bini y V. Pan. *Polynomial and matrix computations. Vol. 1. Fundamental algorithms.* Progress in Theoretical Computer Science. Birkhäuser Boston Inc., Boston, MA, 1994.

[BPR96] S. Basu, R. Pollack y M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, 1996.

[BPR03] S. Basu, R. Pollack y M.-F. Roy. *Algorithms in real algebraic geometry*, volumen 10 de *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2003.

[BS83] W. Baur y V. Strassen. The complexity of partial derivatives. *Theoret. Comput. Sci.*, 22(3):317–330, 1983.

[BT71] W. Brown y J. Traub. On Euclid's algorithm and the theory of subresultants. *J. Assoc. Comput. Mach.*, 18:505–514, 1971.

[Can93] J. Canny. Improved algorithms for sign determination and existential quantifier elimination. *Comput. J.*, 36(5):409–418, 1993.

[Col75] G. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. En *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*, páginas 134–183. Lecture Notes in Comput. Sci., Vol. 33. Springer, Berlin, 1975.

[Coo71] S. Cook. The complexity of theorem proving procedures. En *Proceedings Third Annual ACM Symposium on Thoery of Computing*, páginas 151–158. 1971.

[CR88] M. Coste y M.-F. Roy. Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. *J. Symbolic Comput.*, 5(1-2):121–129, 1988.

[CW90] D. Coppersmith y S. Winograd. Matrix multiplication via arithmetic progressions. *J. Symbolic Comput.*, 9(3):251–280, 1990.

[Dat] R. Datta. Finding all Nash equilibria of a finite game using polynomial algebra. Aparecerá en J. Econom. Theory.

[GHH+97] M. Giusti, J. Heintz, K. Hägele, J. Morais, L. Pardo y J. Montaña. Lower bounds for Diophantine approximations. *J. Pure Appl. Algebra*, 117/118:277–317, 1997. Algorithms for algebra (Eindhoven, 1996).

[GHM+98] M. Giusti, J. Heintz, J. Morais, J. Morgenstern y L. Pardo. Straight-line programs in geometric elimination theory. *J. Pure Appl. Algebra*, 124(1-3):101–146, 1998.

[GJ79] M. Garey y D. Johnson. *Computers and intractability. A guide to the theory of NP-completeness*. W. H. Freeman and Co., San Francisco, Calif., 1979.

[GKZ94] I. Gel'fand, M. Kapranov y A. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 1994.

[GLS01] M. Giusti, G. Lecerf y B. Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.

[GV88] D. Grigor'ev y N. Vorobjov Jr. Solving systems of polynomial inequalities in subexponential time. *J. Symbolic Comput.*, 5(1-2):37–64, 1988.

[GVLRR94] L. González-Vega, H. Lombardi, T. Recio y M.-F. Roy. Spécialisation de la suite de Sturm. *RAIRO Inform. Théor. Appl.*, 28(1):1–24, 1994.

[Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3):239–277, 1983.

[HJSS05] J. Heintz, G. Jeronimo, J. Sabia y P. Solernó. Intersection theory and deformation algorithms: the multi-homogeneous case. 2005. Manuscrito.

[HKP+00] J. Heintz, T. Krick, S. Puddu, J. Sabia y A. Waissbein. Deformation techniques for efficient polynomial equation solving. *J. Complexity*, 16(1):70–109, 2000. Real computation and complexity (Schloss Dagstuhl, 1998).

[HP05] P. Herings y R. Peeters. A globally convergent algorithm to compute all Nash equilibria for n-person games. *Ann. Oper. Res.*, 137:349–368, 2005.

[HRS90] J. Heintz, M.-F. Roy y P. Solernó. Sur la complexité du principe de Tarski-Seidenberg. *Bull. Soc. Math. France*, 118(1):101–126, 1990.

[HW79] G. Hardy y E. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[JMSW] G. Jeronimo, G. Matera, P. Solernó y A. Waissbein. Deformation techniques for sparse systems. Aparecerá en *Found. Comput. Math.*

[JS07] G. Jeronimo y J. Sabia. Computing multihomogeneous resultants using straight-line programs. *J. Symbolic Comput.*, 42(1-2):218–235, 2007.

[Kar72] R. Karp. Reducibility among combinatorial problems. En *Complexity of computer computations (Proc. Sympos., IBM Thomas J. Watson Res. Center, Yorktown Heights, N.Y., 1972)*, páginas 85–103. Plenum, New York, 1972.

[KC91] D. Kincaid y W. Cheney. *Numerical analysis*. Brooks/Cole Publishing Co., Pacific Grove, CA, 1991. Mathematics of scientific computing.

[Koe03] J. Koenig. *Einleitung in die allgemeine Theorie der algebraischen Größen.* Leipzig: B. G. Teubner. X u. 552 S. 8° , 1903.

[Kro82] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. Festschrift. 1882.

[Lec03] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *J. Complexity*, 19(4):564–596, 2003.

[LH64] C. Lemke y J. Howson Jr. Equilibrium points of bimatrix games. *J. Soc. Indust. Appl. Math.*, 12:413–423, 1964.

[LM04] R. Lipton y E. Markakis. Nash equilibria via polynomial equations. En *LATIN 2004: Theoretical informatics*, volumen 2976 de *Lecture Notes in Comput. Sci.*, páginas 413–422. Springer, Berlin, 2004.

[LR01] T. Lickteig y M.-F. Roy. Sylvester-Habicht sequences and fast Cauchy index computation. *J. Symbolic Comput.*, 31(3):315–341, 2001.

[LR07] D. Lazard y F. Rouillier. Solving parametric polynomial systems. *J. Symbolic Comput.*, 42(6):636–667, 2007.

[McL99] A. McLennan. The maximum number of real roots of a multihomogeneous system of polynomial equations. *Beiträge Algebra Geom.*, 40(2):343–350, 1999.

[Min03] M. Minimair. Sparse resultant under vanishing coefficients. *J. Algebraic Combin.*, 18(1):53–73, 2003.

[MM96] R. McKelvey y A. McLennan. Computation of equilibria in finite games. En *Handbook of computational economics, Vol. I*, volumen 13 de *Handbooks in Econom.*, páginas 87–142. North-Holland, Amsterdam, 1996.

[MM97] R. McKelvey y A. McLennan. The maximal number of regular totally mixed Nash equilibria. *J. Econom. Theory*, 72(2):411–425, 1997.

[MMT07] R. McKelvey, A. McLennan y T. Turocy. Gambit: Software tools for game theory, version 0.2007.01.30. 2007. Disponible en `http://gambit.sourceforge.net`.

[MSW95] A. Morgan, A. Sommese y C. Wampler. A product-decomposition bound for Bézout numbers. *SIAM J. Numer. Anal.*, 32(4):1308–1325, 1995.

[Nas51] J. Nash. Non-cooperative games. *Ann. of Math. (2)*, 54:286–295, 1951.

[OR94] M. Osborne y A. Rubinstein. *A course in game theory.* MIT Press, Cambridge, MA, 1994.

[Ped04] P. Pedregal. *Introduction to optimization*, volumen 46 de *Texts in Applied Mathematics.* Springer-Verlag, New York, 2004.

[Pla77] D. Plaisted. New NP-hard and NP-complete polynomial and integer divisibility problems. En *18th Annual Symposium on Foundations of Computer Science (Providence, R.I., 1977)*, páginas 241–253. IEEE Comput. Sci., Long Beach, Calif., 1977.

[PS93] P. Pedersen y B. Sturmfels. Product formulas for resultants and Chow forms. *Math. Z.*, 214(3):377–396, 1993.

[Ren92] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. I, II, III. *J. Symbolic Comput.*, 13(3):255–352, 1992.

[RGK02] J. Richter-Gebert y U. Kortenkamp. Complexity issues in dynamic geometry. En *Foundations of computational mathematics (Hong Kong, 2000)*, páginas 355–404. World Sci. Publ., River Edge, NJ, 2002.

[Roj97] J. Rojas. A new approach to counting Nash equilibria. En *Proceedings of the IEEE/IAFE Conference on Computational Intelligence for Financial Engineering, Manhattan, New York, March 23-25*, páginas 130–136. 1997.

[Roj00] J. Rojas. Algebraic geometry over four rings and the frontier to tractability. En *Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999)*, volumen 270 de *Contemp. Math.*, páginas 275–321. Amer. Math. Soc., Providence, RI, 2000.

[Rou99] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):433–461, 1999.

[RRSED00] F. Rouillier, M.-F. Roy y M. Safey El Din. Finding at least one point in each connected component of a real algebraic set defined by a single equation. *J. Complexity*, 16(4):716–750, 2000.

[Sch03] É. Schost. Computing parametric geometric resolutions. *Appl. Algebra Engrg. Comm. Comput.*, 13(5):349–393, 2003.

[SEDS03] M. Safey El Din y É. Schost. Polar varieties and computation of one point in each connected component of a smooth algebraic set. En *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, páginas 224–231 (electronic), New York, 2003. ACM.

[SEDT] M. Safey El Din y P. Trébuchet. Strong bi-homogeneous Bézout theorem and its use in effective real algebraic geometry. INRIA Research Report RR, 2006.

[Sei54] A. Seidenberg. A new decision method for elementary algebra. *Ann. of Math. (2)*, 60:365–374, 1954.

[Sha77] I. Shafarevich. *Basic algebraic geometry*. Springer-Verlag, Berlin, study edition, 1977.

[Str73] V. Strassen. Vermeidung von Divisionen. *J. Reine Angew. Math.*, 264:184–202, 1973.

[Stu94] B. Sturmfels. On the Newton polytope of the resultant. *J. Algebraic Combin.*, 3(2):207–236, 1994.

[Stu02] B. Sturmfels. *Solving systems of polynomial equations*, Amer. Math. Soc., CBMS Regional Conference Series, volumen 97, Providence, Rhode Island, 2002.

[SW05] A. Sommese y C. Wampler. *The numerical solution of systems of polynomials*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.

[Tar51] A. Tarski. *A decision method for elementary algebra and geometry*. University of California Press, Berkeley and Los Angeles, Calif., 1951. 2nd ed.

[vNM07] J. von Neumann y O. Morgenstern. *Theory of games and economic behavior*. Princeton University Press, Princeton, NJ, anniversary edition, 2007.

[Voi03] C. Voisin. *Hodge theory and complex algebraic geometry. II*, volumen 77 de *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2003.

[vS02] B. von Stengel. Computing equilibria for two person games. En *Handbook of Game Theory with Economic Applications*, volumen 3, páginas 1723–1759. North-Holland, 2002.

[vzG86] J. von zur Gathen. Parallel arithmetic computations: a survey. En *Mathematical foundations of computer science (Bratislava, 1986)*, páginas 93-112. *Lecture Notes in Comput. Sci.*, Vol. 233. Springer, Berlin, 1986.

[vzGG99] J. von zur Gathen y Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999.

[Wei92] V. Weispfenning. Comprehensive Gröbner bases. *J. Symbolic Comput.*, 14(1):1–29, 1992.