Tesis de Posgrado

Sobre la complejidad en espacio y tiempo de la eliminación geométrica

Matera, Guillermo

1997

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

UNIVERSIDAD DE BUENOS AIRES
FACULTAD DE CIENCIAS EXACTAS Y NATURALES

Sobre la Complejidad en Espacio y Tiempo de la Eliminación Geométrica

por
Guillermo Matera

DIRECTOR DE TESIS
Dr. Joos Heintz

LUGAR DE TRABAJO
Departamento de Matemática
Facultad de Ciencias Exactas y Naturales

Tesis presentada para optar por el título de:
Doctor de la Universidad de Buenos Aires

1997

On the Space–Time Complexity of Geometric Elimination

Abstract

The space–time complexity of geometric elimination procedures is studied from both the algorithmic and the computational complexity point of view.

From the algorithmic point of view, deterministic algorithms are developed which solve some of the main elimination problems and require small space resources. Afterwards, a class of probabilistic algorithms is developed which has a better time perfomance and is able to distinguish well–conditionated from ill–posed systems.

From the computational complexity point of view, an optimal lower bound for the space–time tradeoff of polynomial evaluation procedures is shown and several natural cases where this bound is reached are exhibited. Finally, all the existent *general purpose* methods on the subject and all their posible variants are proved to requiere exponential time.

Key words: Elimination, algorithms, complexity, tradeoffs, circuits.

Resumen

Se estudia la complejidad en espacio y tiempo de los procedimientos de eliminación geométrica tanto desde el punto de vista algorítmico como del de la complejidad computacional.

Desde el punto de vista algorítmico, se desarrollan algoritmos determinísticos que resuelven algunos de los principales problemas de eliminación y requieren bajo recursos de espacio de memoria. Posteriormente se desarrolla una clase de algoritmos probabiísticos cuyo comportamiento en cuanto al tiempo es superior, que es capaz de distinguir sistemas bien condicionados de sistemas mal condicionados.

Desde el punto de vista de la complejidad computacional, se demuestra una cota inferior para el tradeoff espacio–tiempo de los procedimientos de evaluación de polinomios y se exhiben varios casos naturales donde se alcanza esta cota. Finalmente se demuestra que todos los métodos *generalistas* existentes sobre el tema y todas sus posibles variantes requieren tiempo exponencial.

Palabras clave: Eliminación, algoritmos, complejidad, tradeoffs, circuitos.

Agradecimientos

En primer lugar, debo expresar mi mayor agradecimiento a Joos Heintz, por la dedicación, el apoyo y la paciencia que en todo momento demostró.

En segundo lugar, deseo agradecer a Luis Miguel Pardo Vasallo, cuya influencia es claramente apreciable en varios pasajes de esta tesis.

También quiero reconocer a varias personas que aportaron de una u otra manera a mi trabajo en este tiempo: B. Castaño, K. Hägele, T. Krick, J.L. Montaña, J.E. Morais, P. Solernó, M. Sombra, J.M. Turull, R. Wachenchauzer.

Por último (aunque no necesariamente en este lugar) a mi familia, y especialmente a mi esposa Nancy y mi hija Lucía, a quienes dedico esta tesis.

Contenidos

Introducción

Los procedimientos algorítmicos de eliminación generalmente han sido diseñados desde el punto de vista del álgebra conmutativa. Por ejemplo, consideremos el caso del problema de la consistencia de un sistema de ecuaciones polinomiales $F_1, \ldots, F_s$ en $\mathbb{Z}[X_1, \ldots, X_s]$: se trata de decidir cuando el sistema

$$F_1(X_1, \ldots, X_n) = 0, \ldots, F_s(X_1, \ldots, X_n) = 0$$

tiene una solución, es decir, si la variedad algebraica

$$V := \{(x_1, \ldots, x_n) \in \mathbf{C}^n \ / \ F_1(x_1, \ldots, x_n) = 0, \ldots, F_s(x_1, \ldots, x_n) = 0\}$$

es o no vacía. Por medio de un teorema de Kronecker (el Nullstellensatz erróneamente atribuido a Hilbert), esta cuestión se puede reducir a un problema de naturaleza puramente algebraica:

$V = \emptyset$ si y sólo si existen polinomios $G_1, \ldots, G_s \in \mathbb{Q}[X_1, \ldots, X_n]$ tales que vale la igualdad $1 \in G_1F_1 + \cdots + G_sF_s$

El software existente sobre el tema, basado en la teoría de bases de Gröbner (cf. [36]), se concentra en el estudio del *ideal* polinomial involucrado, es decir, el ideal $\mathcal{I} := (F_1, \ldots, F_s)$ generado por los polinomios $F_1, \ldots, F_s$ en $\mathbb{Q}[X_1, \ldots, X_n]$. En tal sentido, la pregunta del problema de la consistencia de un sistema de ecuaciones polinomiales constituye simplemente un caso particular del problema general de la pertenencia de un polinomio a un ideal dado, cuya formulación precisa es la siguiente:

Dados polinomios $F_1, \ldots, F_s, F$ en $\mathbb{Z}[X_1, \ldots, X_s]$, decidir si F pertenece al ideal generado por $F_1, \ldots, F_s$ en $\mathbb{Q}[X_1, \ldots, X_n]$, es decir, si existen polinomios $G_1, \ldots, G_s \in \mathbb{Q}[X_1, \ldots, X_n]$ tales que se verifica la identidad $F = G_1F_1 + \cdots + G_sF_s$.

Desde la informática teórica la respuesta a esta última pregunta no es alentadora: un trabajo de E. Mayr y A. Meyer [126] (ver también [125]) clasifica este problema como *intratable* desde el punto de vista de los recursos computacionales que éste requiere para su solución. Dado que el software que utiliza los métodos de bases de Gröbner resuelve el problema de la pertenencia, se deduce que éste exige grandes recursos computacionales para su aplicación.

Este fenómeno ocurre con frecuencia en el ámbito del álgebra computacional: dado que los aspectos computacionales no se toman en cuenta, las computadoras se sobrecargan con rutinas (generalmente innecesarias) y en consecuencia el usuario debe ser paciente. Esta ineficiencia práctica crea la demanda de un análisis de los problemas computaciones que puede analizarse por medio de consideraciones de complejidad. El estudio de la complejidad apunta a explicar porque algunos problemas requieren mas espacio de memoria del que la computadora dispone o porque la respuesta a ciertas preguntas no puede esperarse en tiempo razonable.

El objetivo central de esta tesis es estudiar la problemática algorítmica de la eliminación geométrica y algebraica desde el punto de vista de la complejidad. En tal sentido, se prestará atención a los dos aspectos relevantes de la cuestión: el de la optimización y el de las limitaciones. Por tal motivo, la tesis se divididirá en dos partes: en la primera mitad se desarrollarán algoritmos que optimizan el uso de los dos recursos computacionales básicos que consideraremos: el espacio de memoria y el tiempo de cálculo secuenciales. Por su parte, la segunda mitad de la tesis estará dedicada a estudiar los límites de toda posible mejora.

La ineficiencia de los métodos basados en bases de Gröbner crea la necesidad de buscar métodos alternativos para tratar los problemas de eliminación. Retomando nuevamente el problema de la consistencia como ejemplo, una idea natural consiste en acotar los grados de los polinomios G_i que aparecen en la representación de 1 en el ideal generado por $(F_1, \ldots, F_s)$. De este modo, el problema de la consistencia del sistema de ecuaciones polinomiales definido por $F_1, \ldots, F_s$ puede resolverse por comparación de coeficientes y álgebra lineal (la cota para los grados de los polinomios G_i permite estimar el tamaño del sistema lineal). Esta alternativa, propuesta por Hilbert, fue tratada por primera vez por G. Hermann ([96]) en la década del '20 para el caso general de la pertenencia a un ideal. La autora demostró que un polinomio F

pertenece al ideal $(F_1, \ldots, F_s)$ si y solamente si existe una representación:

$$F = G_1 F_1 + \cdots + G_s F_s$$

donde los G_i son polinomios de grado total acotado por $\deg F + 2(1 + d^2 + \cdots + d^{2^{n-1}})$, siendo d el máximo de los grados de los polinomios F_i.

A pesar de diversas mejoras a las que fue objeto el resultado de Hermann, Mayr y Meyer (ver [126]) mostraron que la mejor cota de grado que se puede obtener para un sistema arbitrario es doblemente exponencial en los datos de entrada d y n, por lo que es imposible esperar una estimación mejor.

O.H. Keller y W. Gröbner estudiaron esta idea (de acotar los grados de los polinomios $G_1, \ldots, G_n$) en el Nullstellensatz cuando tenemos $F = 1$ y conjeturaron que en este caso la cota debía ser de tipo $\deg G_i \leq d^n$ (Problema del *Nullstellensatz efectivo*).

La conjetura de Keller y Gröbner fue finalmente demostrada en 1986 por D. Brownawell ([34]) para el caso de los números complejos. El resultado fue extendido poco más tarde al caso general por L. Caniglia, A. Galligo y J. Heintz (ver [38], [39]) y finalmente refinado por J. Kollár ([111]). Se obtuvieron versiones más generales del Nullstellensatz efectivo (ver [5], [15], [35], [41], [64], [65], [143], [164]) y se pudo tratar el problema general de la pertenencia de un polinomio F a un ideal y de la representación para ciertos casos particulares en tiempo simplemente exponencial (ver [56]). Entre estos casos particulares se destacan el de un ideal de dimensión cero y el de un ideal intersección completa. Cabe destacar que los grados de tipo d^n que aparecen en los Nullstellensätze citados son casi optimales (ver [34], donde este hecho se ilustra por medio de un ejemplo debido a T. Mora, D. Lazard, D. Masser y P. Philippon entre otros).

A partir de estos resultados se desarrolló una estrategia general para tratar con problemas geométricos de teoría de eliminación: reducir los problemas a cuestiones de álgebra lineal. De esta manera pudieron resolverse en tiempo simplemente exponencial problemas tales como la eliminación de un bloque de cuantificadores en el caso real y complejo ([66], [67], [91], [92], [93]), la pertenencia al radical ([39]), el cálculo de la dimensión de una variedad ([56]), la descomposición en componentes equidimensionales ([79]), el cálculo de la clausura proyectiva ([40]) y una versión algorítmica del Teorema de Quillen-Suslin ([64], [65]) entre otros. Por otra parte cabe mencionar que la clasificación de la complejidad intrínseca de algunos problemas algorítmicos

fundamentales queda abierta, como por ejemplo el cálculo de generadores para el radical de un ideal polinomial dado (ver [112]).

Una interesante característica común de los algoritmos mencionados anteriormente es el buen comportamiento que todos ellos poseen desde el punto de vista de la computación en *paralelo*. Es decir, en un modelo en el cual se dispone de varios procesadores que trabajan simultáneamente, el tiempo de cálculo se reduce en forma polilogarítmica con respecto a los parámetros de entrada n (la cantidad de variables), s (la cantidad de polinomios) y d (el grado máximo de los polinomios) mediante una adecuada distribución de los procesos (operaciones aritméticas) a realizar.

Surge entonces la cuestión de como puede utilizarse esta característica de los algoritmos considerados en el ámbito de la computación secuencial. Desde la computación booleana, la respuesta viene dada a partir de un resultado de A. Borodin [24] (ver también [69]): bajo ciertas condiciones de *uniformidad*, el tiempo de computación paralela puede transformarse en espacio de memoria secuencial.

En el primer capítulo de la tesis se estudia la manera de aplicar el teorema de Borodin a los problemas de eliminación. Para esto se discute la transformación del teorema de Borodin en una herramienta algorítmica utilizable en este contexto. Se estudia especialmente la forma en la que el teorema de Borodin involucra la uniformidad del algoritmo dado. Posteriormente se desarrollan algoritmos para la resolución de los problemas de álgebra lineal que intervienen en los problemas de eliminación. Los casos centrales desde el punto de vista de las aplicaciones son el cálculo del rango de matrices en $\mathbb{Z}^{n\times m}$ y la resolución de sistemas de ecuaciones lineales sobre $\mathbb{Z}$.

Aquí el espacio de memoria es crítico teniendo en cuenta que los algoritmos comúnmente utilizados (basados en la eliminación gaussiana) requieren una cantidad polinomial de espacio, lo cual los transforma en impracticables para grandes matrices como las que aparecen típicamente en las aplicaciones a la eliminación.

Los algoritmos que se obtienen por medio del teorema de Borodin utilizan espacio de memoria polilogarítmico. Para este propósito se estudian algoritmos *aritméticos* de bajo tiempo paralelo sin divisiones, como los de [19] o [1] para el cálculo del polinomio característico (ver también [52], [150], [30], [72], [137], [75], [20]), los cuales se "traducen" a algoritmos booleanos, a fin de poder aplicar la estrategia del teorema de Borodin.

Si bien parece natural realizar esta traducción de la base de operaciones $\{+,*\}$ en $\mathbb{Z}$ a la base $\{\wedge,\vee,\neg\}$ en $\{0,1\}$, se demuestra que la traducción puede realizarse mas eficientemente a partir de la base $\{+,*,\sum\}$, donde $\sum$ se implementa en tiempo paralelo logarítmico por medio de un circuito Carry Save Adder (ver [23], [181]). Esto permite obtener algoritmos que tienen una perfomance, en cuanto al tiempo paralelo se refiere, comparable con los mejores algoritmos uniformes conocidos hasta el momento, como los de [27], pero con ventajas adicionales importantes desde el punto de vista de la programación.

Posteriormente se muestran reducciones de varios problemas de eliminación en geometría algebraica y semialgebraica a cuestiones de álgebra lineal. A fin de transformar estas reducciones en algoritmos (booleanos) de bajo tiempo paralelo, se controla el tamaño de las matrices involucradas así como también la longitud bit de los números involucrados. De esta manera, se obtienen algoritmos de tiempo paralelo polinomial en n y logarítmico en s, d y h (la longitud binaria máxima de los coeficientes de los polinomios F_i) para resolver algunos problemas fundamentales en teoría de eliminación geométrica (cf. [90], [138]): la representación de 1 en el problema de la consistencia, la pertenencia de un polinomio dado a un ideal cero-dimensional o de intersección completa o a un ideal radical, y la eliminación de un bloque de cuantificadores; como así también algunas cuestiones algorítmicas de importancia: técnicas de preprocesamiento de datos (normalización de Noether), de descripción de la variedad (cálculo de la dimensión, grado, descomposición en componentes irreducibles), de reducción (cálculo de la clausura proyectiva) y otras (versión algorítmica del teorema de Quillen-Suslin).

Estos algoritmos proveen los "buenos" candidatos para la aplicación de la estrategia del teorema de Borodin, y esto nos conduce al tema de la uniformidad. Parece ser un comportamiento éstandar en el ámbito del cálculo simbólico ignorar este aspecto de vital importancia. Por ejemplo, tanto en [19] como en [27] y [125] se anuncian resultados como uniformes sin exhibir ninguna demostración de este hecho. Un punto que es crucial en este tema es que la única forma de probar la uniformidad necesaria para la aplicación del método de Borodin de una familia de circuitos es exhibiendo un algoritmo que, dado el número de circuito como entrada, describe el diseño de dicho circuito en espacio polilogarítmico. Y esto no es trivial, como puede apreciarse en el caso de producto iterado (ver [99]) o de la división de números enteros (ver [108], [152]).

Por lo tanto se discute la cuestión de la uniformidad de los algoritmos antes mencionados y se muestra que ésta puede obtenerse en espacio logarítmico. Finalmente, a partir de la estrategia del teorema de Borodin se consiguen algoritmos que funcionan en espacio de memoria polinomial para todos esos problemas. Cabe destacar que todos estos resultados se encuentran contenidos en los trabajos [86] y [123].

Algunos algoritmos para problemas de teoría de eliminación han sido presentados como algoritmos que utilizan bajos recursos de espacio de memoria. Tal es el caso de los algoritmos en [14], [42], y [153] por ejemplo. Sin embargo, en esos trabajos los autores no analizan las cuestiones de uniformidad de sus algoritmos, de modo que no queda claro que estos posean las características anunciadas.

Es un hecho general de la teoría de complejidad en el ámbito de la computación secuencial, al menos en su modelo mas utilizado, el de la máquina de Turing, que con espacio de memoria S prefijado, el tiempo de cálculo queda acotado en el peor caso en forma exponencial con respecto a S (cf. [7]). Esta estimación aplicada a los algoritmos de eliminación anteriormente mencionados daría cotas no polinomiales (subexponenciales o exponenciales según el contexto) para el tiempo que los mismos requieren. Es por lo tanto interesante estudiar de que manera pueden mejorarse los métodos anteriores a fin de obtener algoritmos con mejor comportamiento con respecto al tiempo de cálculo.

Con esta cuestión como objetivo, el segundo capítulo de la tesis exhibe una nueva clase de algoritmos para problemas de eliminación cuya perfomance en cuanto al tiempo de cálculo es claramente superior, aunque admitiendo la posibilidad de que los mismos produzcan respuestas erróneas (de todas maneras la probabilidad de que esto ocurra es muy baja).

Uno de los ingredientes principales para lograr esta clase de algoritmos es la descripción de una variedad en forma seudo-paramétrica mediante un *elemento primitivo*. La idea original viene del caso de la eliminación cero-dimensional, donde ésta técnica ha sido aplicada con éxito desde bastante tiempo atrás, como por ejemplo en [4], [42], [46], [48], [77], [78], [80], [81], [82], [90], [110], [114], [118], [119], y [128] entre otros. En este caso un elemento primitivo es simplemente una forma lineal γ que separa los (finitos) puntos de la variedad, es decir, que verifica $\gamma(P) \neq \gamma(Q)$ para todo par de puntos distintos $P, Q \in V$.

Mediante una adaptación para el caso de sistemas de ecuaciones polinomiales de dimensión positiva, el elemento primitivo permite una descripción de variedades algebraicas que es útil en varias cuestiones de eliminación y puede calcularse y manipularse con baja complejidad.

El otro ingrediente fundamental es el uso de *correct-test sequences* (cf. [94], ver también [53], [87], [114], [159]). Estas han sido una herramienta de importancia en varios trabajos sobre eliminación (ver [80], [83], [68], [113], [114], [82], [81], [78]), donde se han utilizado para chequear probabilísticamente identidades de polinomios dados por su grafo de computación. Al contrario de los métodos desarrollados en [55], [97], [162] y [186], donde el chequeo depende del polinomio particular que se considera, las correct test sequences brindan un test que es uniforme para todos los polinomios que poseen un grafo de computación del mismo tamaño.

Una de las principales aplicaciones de las correct-test sequences es el caso de sistemas sobredeterminados (es decir, con más ecuaciones que incógnitas). Una técnica común (ver por ejemplo, [16], [17], [34], [38], [39], [42], [48], [60], [68], [80], [83], [111], [113], [114], [118], [144], [154]), es reemplazar las ecuaciones originales por n combinaciones lineales $G_1, \ldots, G_n$ de las mismas de manera de describir la variedad con igual cantidad de ecuaciones que incógnitas. Un punto clave es que los coeficientes que aparecen en esas combinaciones lineales pueden elegirse con la única condición de no satisfacer cierta ecuación polinomial que puede calcularse con bajo tiempo paralelo. Como se demuestra en [114] section 3.1, estos coeficientes pueden generarse aleatoriamente bit a bit con alta probabilidad de obtener una "correct sequence".

En primer lugar se exhibe un algoritmo para calcular elemento primitivo, tomando como base los algoritmos aritméticos desarrollados en [114], [82], [81] y [78], y el teorema de Borodin. Posteriormente se estudian algunas aplicaciones con esta filosofía, como el problema de la representación de la unidad en el caso de la consistencia y la pertenencia de un polinomio a un ideal intersección completa, el cálculo del grado de una variedad y una nueva versión del teorema de Quillen-Suslin en el cual la incidencia del tamaño de la matriz baja de exponencial a polinomial (hecho clave para su "aplicabilidad"). Algunos de estos algoritmos también mejoran sustancialmente las cotas hasta ahora conocidas con respecto a la computación paralela.

Es interesante destacar que esta clase de algoritmos tiene un comportamiento en cuanto al tiempo de cálculo que es al menos tan bueno como

el que poseen los algoritmos que utilizan los métodos de bases de Gröbner, siendo su principal ventaja sobre aquellos que requiere una cantidad razonable de espacio de memoria (en el caso de los métodos de bases de Gröbner, estos son como mínimo de tipo exponencial, lo que ocasiona que frecuentemente su ejecución no pueda completarse por falta de espacio de memoria).

Habiendo estudiado la cuestión de la optimización de la utilización de recursos computacionales en problemas de eliminación, surge claramente la necesidad de estudiar los límites de toda posible mejora. En tal sentido, en el tercer capítulo de la tesis se estudia la forma en que los dos recursos computacionales que hemos estado considerando (espacio de memoria y tiempo de cálculo) se interrelacionan.

El problema de la interrelación (tradeoff) tiempo–espacio en informática teórica ha sido un tópico de interés desde los comienzos de la disciplina. Desde hace tiempo se había observado que frecuentemente la economización de espacio de memoria ocasiona la recomputación de resultados parciales.

Un modelo natural para el estudio de los tradeoffs es el de los *straight-line programs* (cf. [31], [168], [89], [172], [75], [138], [37]). Un straight-line program modela la evaluación de una función representada mediante un grafo de computación (que es un grafo orientado acíclico cuyos nodos son etiquetados según la operación aritmética que realizan) con una cierta cantidad de registros. La evaluación del grafo procede en varias etapas, en cada una de las cuales se calcula el resultado correspondiente a un nodo del grafo (siempre que los resultados correspondientes a sus predecesores estén almacenados en dos registros) y el resultado obtenido se almacena en otro registro. El espacio se mide por la cantidad máxima de registros utilizada durante todo el proceso y la cantidad de etapas necesarias para la evaluación de todo el grafo es lo que se identifica con el tiempo de cálculo.

Literatura sobre tradeoffs tiempo–espacio en este modelo puede hallarse en los surveys de N. Pippenger [149] y J.E. Savage [155]. Los straight-line programs han sido utilizados para mostrar cotas inferiores para varios problemas, incluyendo sorting (ver [173]), reconocimiento de lenguajes ([61]), multiplicación binaria entera [158] problemas de álgebra lineal y multilineal como convolución, producto matriz-vector y transformada de Fourier discreta ([173], [174], [157]), multiplicación, inversión y multiplicación iterada de matrices ([85], [101], [156], [174]), range queries ([183], [175]) y otros ([120],

[140], [148]).

Otro modelo alternativo comúnmente utilizado es el de los *branching programs* (cf. [25]). Este modelo también ha sido lo suficientemente poderoso como para permitir establecer cotas inferiores para problemas algebraicos. En [185] por ejemplo se establecen cotas inferiores para transformada de Fourier discreta y en [2] se muestran tradeoffs tiempo–espacio para una larga lista de problemas algebraicos tales como convolución, multiplicación entera, producto matriz–vector, multiplicación e inversión de matrices, el cálculo del producto de tres matrices y el de PAQ donde P y Q son matrices de permutación. Este modelo puede asimismo aplicarse a otros problemas como sorting (ver [28], [26]), distinción de elementos ([29], [184]) y hallar elementos únicos ([11]).

En esta tesis se estudia la complejidad tiempo–espacio de la evaluación de polinomios bajo el modelo de los straight–line programs. El método para que se utiliza a fin obtener cotas inferiores se basa en una interpretación geométrica de la noción de straight–line program en la que sólo se tienen en cuenta las operaciones *no escalares* (es decir, productos entre polinomios no constantes y divisiones cuyo denominador es un polinomio no constante).

En primer lugar, se observa que el grafo de computación asociado a la regla de Horner para un polinomio univariado $P \in K[X]$ de grado d puede realizarse utilizando exantamente dos registros en tiempo total $2d$ y tiempo no escalar d. Si L y S denotan el tiempo y espacio no escalar del algoritmo de Horner aplicado a la evaluación del polinomio P, se obtiene la siguiente obvia cota superior para el tradeoff tiempo–espacio de evaluar P:

$$L \cdot S^2 = 4 \cdot d.$$

A partir de un simple argumento de dimensión, se mostrará que esta cota es, salvo un orden de magnitud, exacta para casi todos los polinomios univariados de grado d. Como en [171] y [89] se llama a tales polinomios *difíciles de evaluar* en términos de tradeoff.

Luego se desarrolla la estrategia global que permite exhibir polinomios univariados *específicos* que son difíciles de evaluar en el sentido anterior. Esta estrategia incluye un análisis de la altura de puntos en la fibra de un morfismo entre variedades diofánticas y constituye la principal herramienta para establecer tradeoffs tiempo–espacio para polinomios univariados con coeficientes enteros. El caso más simple de los polinomios con coeficientes

algebraicos se trata mediante un método para estimar el grado de una fibra de un morfismo entre variedades diofánticas inspirado en [95] (ver también [94], [90]).

Cabe destacar que estos resultados, contenidos en [3], muestran por primera vez cotas inferiores significantes para el tradeoff tiempo-espacio en circuitos con *una sola salida.*

Finalmente, el cuarto capítulo de la tesis estudia la cuestión de las limitaciones de toda posible optimización de los algoritmos considerados.

Existen ciertos indicios de que la eliminación algorítmica enfrenta serios problemas de complejidad. Por un lado es sabido que la eliminación de cuantificadores general en geometría algebraica y semialgebraica requiere tiempo intrinsecamente doblemente exponencial y espacio de memoria simplemente exponencial ([54], [66], [88]) y que los típicos problemas algebraicos en anillos de polinomios (como el problema de la pertenencia para ideales polinomiales) son completos en espacio exponencial ([125], [126]). Por otro lado una larga lista de problemas geométricos fundamentales son resolubles en espacio polinomial (con la correspondiente complejidad en tiempo simplemente exponencial en la cantidad de variables).

En esta tesis se muestra evidencia que avala la conjetura que la eliminación en geometría tiene una complejidad intrínsecamente exponencial con respecto al tiempo secuencial e intrínsecamente polinomial con respecto al espacio de memoria. Esta evidencia se dará tanto en términos de complejidad *estructural* (relativa) como en términos de complejidad *absoluta* (aunque en modelos de computación restringidos).

Con respecto a complejidad estructural, se demuestra que la suposición de un carácter intrínseco polinomial de la eliminación algorítmica implica que la jerarquía de tiempo aritmética colapsa (lo que implicaría, como es bien conocido y contrario a la creencia general, que P=NP) y que lo mismo ocurre con respecto a modelos no uniformes de computación (por ejemplo, la tesis de Valiant sería incorrecta).

En cuanto a la complejidad absoluta, se demuestra que una clase bien definida de algoritmos, que incluye todos los algoritmos actualmente implementados o posibles variantes de los mismos y los desarrollados en la primera parte de la tesis, requieren espacio de memoria polinomial y tiempo de cálculo simplemente exponencial. Para tal fin se introduce el concepto de *algoritmo algebraicamente robusto*, el cual sintetiza las características de todos los al-

goritmos de eliminación conocidos en cálculo simbólico. Posteriormente, se demuestra que cualquier algoritmo algebraicamente robusto posee el carácter exponencial anteriormente anunciado.

Se deduce que los algoritmos desarrollados en la primera mitad de la tesis no son esencialmente mejorables, al menos utilizando el tipo de técnicas que se han aplicado hasta el momento.

Capítulo 1

Algoritmos determinísticos

El objetivo de esta tesis es estudiar la teoría de eliminación geométrica desde el punto del vista algorítmico. Por lo tanto, uno de los aspectos mas relevantes a tener en cuenta es el del desarrollo de algoritmos "eficientes" para resolver problemas de eliminación.

Este capítulo se dedicará al diseño algoritmos *determinísticos*, es decir, algoritmos que pueden ser aplicados a cualquier instancia del problema considerado, y que producen siempre una solución para tal instancia.

La eficiencia de dichos algoritmos se expresa en términos de los recursos necesarios para ejecutarlos. Dependiendo del modelo de algoritmo que se elige, se considerarán recursos tales como el tiempo de computación, el espacio de memoria requerido o el número de operaciones a realizar.

Las estimaciones de los recursos que requiere un algoritmo para su funcionamiento dependen del aspecto sintáctico del problema. Es por tanto importante acordar de que manera se codificarán los objetos con los cuales se opera. Dado que se piensa en algoritmos que factibles de ser implementados en *computadoras reales*, es necesario que las entradas y los resultados sean sucesiones finitas (*palabras*) de símbolos de un alfabeto finito, como $\{0, 1\}$ por ejemplo.

Un modelo que permite apreciar el comportamiento del software sobre una computadora real es el de las *máquinas de Turing*. Una máquina de Turing *determinística* M es un dispositivo que consiste de un *control finito* y un número fijo k de *cintas* equipadas cada una de ellas con una *cabeza* de lecto-escritura (cf. [7], [71]).

Las cintas se clasifican en tres tipos: hay una cinta de *entrada* que es sólo

de lectura (es decir, no se puede modificar su contenido), una segunda cinta de *salida* que es sólo para escritura y las restantes se denominan cintas de *trabajo* con funciones de lectura y escritura. Estas cintas son semiinfinitas (a derecha) y están divididas en *celdas*. La cabeza de lecto–escritura de cada cinta se puede mover a izquierda o derecha y puede leer los contenidos de una sola celda en cada instante de tiempo.

El control finito consiste de un *alfabeto de cinta* Σ, un conjunto Q de *estados* o *instrucciones* (que posee un elemento distinguido q_0 que se denomina *estado inicial* y un subconjunto especial llamado el conjunto de los *estados finales* $\mathcal{F} \subseteq Q$) y una función (parcial) de transición:

$$\delta : Q \times \Sigma^{k-1} \longrightarrow Q \times \Sigma^{k-1} \times \{L, R, N\}^k$$

(donde L, R, N denotan el movimiento a izquierda, derecha y nulo respectivamente).

A cada instante de tiempo, la máquina M está en un estado $q \in Q$ y las cabezas de las cintas de entrada y de trabajo leen los símbolos $(a_1, \ldots, a_{k-1})$ que contienen las celdas sobre las cuales están posicionadas. Entonces, en un instante de tiempo se puede modificar el contenido de todas las celdas sobre las cuales hay una cabeza de lecto–escritura, imprimir un símbolo sobre la cinta de salida (en la posición actual de la cabeza correspondiente), mover cada cabeza una posición a izquierda o derecha (o dejarla en la misma ubicación) y cambiar el estado $q \in Q$. Todos estos movimientos constituyen un *paso de computación* y se realizan de acuerdo con las especificaciones de la imagen $\delta(q, a_1, \ldots, a_{k-1})$ de la función de transición δ aplicada a la *configuración* definida por $(q, a_1, \ldots, a_{k-1})$.

La máquina M comienza operando con una *palabra de entrada* x sobre la cinta de entrada en estado q_0, todas las demás cintas en blanco y las cabezas situadas sobre la primera celda de cada cinta. Entonces M procede aplicando la función de transición tantas veces como sea posible (hasta que δ resulte indefinida sobre cierta configuración), en cuyo caso la máquina para. Si M se detiene sobre un estado final $q \in \mathcal{F}$ se dice que M *acepta* la entrada x; en caso contrario, M *rechaza* x.

Dada una entrada x que ha sido aceptada por M, se definen el *tiempo de computación* sobre x como la cantidad de pasos de computación que M realiza hasta su detención y el *espacio de memoria* sobre x como la máxima cantidad de celdas de cintas de trabajo utilizadas durante el proceso.

Luego, el *espacio de memoria* S y el *tiempo de computación* T de M se definen como las funciones $S, T : \mathbb{N} \longrightarrow \mathbb{N}$ tales que $S(n)$ es el máximo espacio utilizado en una computación sobre una entrada de longitud n y $T(n)$ el máximo tiempo requerido por una computación sobre entradas de longitud n.

En términos de estos dos recursos los problemas se agrupan en diferentes clases, de las cuales se pueden mencionar la clase P de los problemas resolubles en tiempo polinomial (es decir, de tipo $n^{O(1)}$) y la clase PSPACE de los problemas resolubles en espacio polinomial. En teoría de computación se considera que los problemas que requieren mas que espacio polinomial para su resolución no tienen interés desde el punto de vista práctico.

Existen algunos hechos básicos que relacionan las diferentes clases de complejidad. Entre ellos, se puede citar el siguiente:

Lema 1 ([7], Theorem 2.8) *Sea M una máquina de Turing determinística que funciona en espacio $S(n) \geq \log n$. Entonces M tiene tiempo de computación $T(n)$ acotado por $T(n) \leq 2^{O(S(n))}$.*

Los algoritmos que se presentarán en este capítulo realizan una cuidadosa alocación de data con el fin de optimizar el espacio de memoria disponible. Esto demanda un control permanente del espacio que requiere cada proceso.

Un caso que aparentemente no ofrece complicaciones es el de la composición de dos máquinas de Turing M_1 y M_2. Sin embargo, el esquema obvio de composición no es eficiente desde el punto de vista del espacio de memoria ya que, para realizarlo es necesario alojar en memoria el resultado que calcula M_1 a fin de utilizarlo como entrada de M_2, y éste resultado podría tener una longitud exponencial con respecto al espacio de memoria que usa M_1 (ver lema 1).

No obstante, esta dificultad se evita por medio de un proceso que podría describirse como de recomputación de cada bit de la salida de M_1 a medida que el mismo es requerido por M_2. Más precisamente, el resultado es el siguiente:

Lema 2 ([7], Lemma 3.4) *Sean $f, g : \Sigma^* \to \Sigma^*$ funciones computables por medio de dos máquinas de Turing determinísticas M_1 y M_2 que utilizan espacio $S_1 \geq \log n$ y $S_2 \geq \log n$ respectivamente. Entonces, existe una máquina de Turing determinística M_3 que calcula la composición $g \circ f(x)$ para todo*

$x \in \Sigma^*$ *en espacio* $O\big(S_1(|x|) + S_2(|f(x)|)\big)$, *donde* $|y|$ *denota la longitud de la palabra* $y \in \Sigma^*$.

Mas cercanos al comportamiento del hardware son los *circuitos booleanos* (cf. [23], [108], [181]). Un *circuito booleano* es un grafo dirigido acíclico, cuyos nodos se etiquetan de la siguiente manera: los nodos con in-degree 0 son los nodos de *entrada*, y se etiquetan con una variable o con la constante 0 o 1. Los nodos de in-degree mayor que 0 y out-degree mayor que 0 se dicen nodos *nodos* y se etiquetan con una función booleana ω, que se restringirá al conjunto $\{\wedge, \vee, \neg\}$. Los nodos de out-degree 0 son los nodos de *salida* y se etiquetan también con una operación booleana en $\{\wedge, \vee, \neg\}$.

Los recursos relevantes en el modelo de los circuitos booleanos son la *talla*, que se define como el número total de nodos internos del circuito, y la *profundidad*, que es la longitud (número de nodos internos) del camino mas largo que une un nodo de entrada a un nodo de salida.

Sea $f : \{0,1\}^n \to \{0,1\}$ una función booleana. Entonces, la *talla de circuito* de f, $S(f)$, es el menor número de nodos internos de un circuito que calcula f. Análogamente, la *profundidad de* f, $D(f)$, es la mínima profundidad de un circuito que calcula f.

Obsérvese que el modelo sólo permite instancias de longitud fija. Por lo tanto, si se desean estudiar problemas que tienen instancias de distinta longitud por medio de circuitos booleanos, debe usarse un circuito distinto para cada posible longitud de entrada.

Es por tal motivo que se consideran *familias de circuitos booleanos*: una familia de circuitos booleanos $C = \{c_n\}_{n\geq 1}$ es simplemente un conjunto de circuitos booleanos donde el n–ésimo circuito c_n tiene n entradas.

Se dice que una función booleana $g : \{0,1\}^* \to \{0,1\}$ se calcula con talla h_1 y profundidad h_2, donde $h_1, h_2 : \mathbb{N} \to \mathbb{N}$, si, para todo n, $S(g_n) = h_1(n)$ y $D(g_n) = h_2(n)$, donde g_n es g restringida a $\{0,1\}^n$.

Sea $C = \{c_n\}_{n\geq 1}$ una familia de circuitos booleanos de talla $S(n)$ y profundidad $D(n)$. Supuesto enumerados los nodos de c_n tal que los nodos de entrada están numerados de 1 a n, y la numeración se restringe de modo tal que existe una constante $k > 0$ tal que, para todo $n \in \mathbb{N}$, el mayor número de nodo está acotado por $S(n)^k$, se define la *codificación estándar* del circuito c_n, notada por $\overline{c_n}$, como la lista de 4–uplas $\{(\rho, op, \rho_l, \rho_r)\}_{\rho \leq S(n)^k}$, donde ρ representa el número de nodo, op es la operación booleana que se realiza en

el nodo ρ, ρ_l es el número del nodo cuya salida es la entrada izquierda de ρ y ρ_r es el número del nodo cuyo salida es la entrada derecha de ρ.

Obsérvese que la codificación estándar de una familia arbitraria de circuitos booleanos no necesariamente posee una descripción finita. Sin embargo, la finitud de tal descripción es de vital importancia para la manipulación de dicha familia de circuitos booleanos. Por otro lado, una idea intuitiva aceptada es que cualquier estrategia razonable de resolución de cierto problema no debería cambiar fundamentalmente en función del tamaño de la instancia considerada. Es por estos motivos que en esta tesis se estudiarán especialmente las familias de circuitos que poseen ciertas propiedades de *uniformidad* (cf. [24], [8]):

Definición 1 *Una familia de circuitos* $C = \{c_n\}_{n\geq 1}$ *de tamaño* $S(n)$ *y profundidad* $D(n)$ *se dice uniforme (en espacio logarítmico) si existe una máquina de Turing determinística que calcula la función* $1^n \rightarrow \overline{c_n}$ *en espacio* $O(max\{D(n), \log S(n)\})$.

Esta noción de uniformidad tiene el inconveniente práctico que sólo permite el acceso al código *completo* de cada circuito c_n. Sin embargo, en un proceso de evaluación del circuito c_n, a fin de ahorrar espacio de memoria es más importante obtener información "local", como la que suministra la función

$$1^n \# \rho \rightarrow (\rho, b, \rho_l, \rho_r)$$

la cual, dado el número n de circuito y un número de nodo ρ como entrada, calcula la codificación $(\rho, b, \rho_l, \rho_r)$ del ρ–ésimo nodo del circuito c_n.

Si bien esta función parece requerir más recursos en su cómputo que la función $1^n \rightarrow \overline{c_n}$, esto no es así como se demuestra en el siguiente lema:

Lema 3 *Una familia de circuitos booleanos* $C = \{c_n\}_{n\geq 1}$ *es uniforme si y sólo si existe una máquina de Turing determinística que calcula la función*

$$1^n \# \rho \rightarrow (\rho, b, \rho_l, \rho_r)$$

en espacio $O(max\{D(n), \log S(n)\})$.

Demostración Es claro que el hecho que la función $1^n \# \rho \rightarrow (\rho, b, \rho_l, \rho_r)$ es computable en espacio $O(max\{D(n), \log S(n)\})$ implica la uniformidad, ya

que la máquina de Turing $\tilde{M}$ que atestigua la uniformidad de la familia $C = \{c_n\}_{n\geq 1}$ puede diseñarse de la siguiente manera: por medio de un contador se recorren los índices correspondientes a todos los nodos de c_n y el código de cada nodo se produce por medio de una llamada a la máquina M (obsérvese que el contador requiere $O(\log S(n))$ celdas de espacio de trabajo).

Supóngase ahora que se tiene una máquina de Turing $\tilde{M}$ que demuestra la uniformidad de la familia de circuitos $\{c_n\}_{n\geq 1}$. Se modificará $\tilde{M}$ a fin de obtener una máquina de Turing M la cual, con una entrada $1^n\#\rho$ genera la codificación estandar del ρ-ésimo nodo c_n.

Se supone que $\tilde{M}$ marca el comienzo del código de cada nodo por medio de un símbolo distinguido (que se denominará *separador*). Si se tuviera calculada la posición del ρ-ésimo y el $(\rho+1)$-ésimo separador sobre la cinta de output, se podría modificar el programa de $\tilde{M}$ de modo tal que imprima un símbolo (sobre una cinta de trabajo auxiliar T) si y sólo si previamente éste se iba a imprimir entre las posiciones del ρ-ésimo y el $(\rho+1)$-ésimo separador impreso sobre la cinta de salida de $\tilde{M}$ (esto puede hacerse controlando la posición de la cabeza de la cinta de salida de $\tilde{M}$). De esta manera, la máquina modificada M imprimiría exactamente la codificación del nodo ρ que se desea obtener.

El procedimiento que calcula la posición de los separadores que marcan el comienzo y final del código del nodo ρ funciona en a lo sumo ρ etapas, calculándose en la i-ésima etapa la posición del $(i+1)$-ésimo separador a partir de la posición del i-ésimo separador.

En la primer etapa, se calcula la posición de los dos primeros separadores sobre la cinta de salida. Para este propósito, se simula el funcionamiento de $\tilde{M}$ sin imprimir ningún símbolo sobre la cinta de salida. Luego de guardar en memoria las posiciones de los dos primeros símbolos separadores que imprime $\tilde{M}$ sobre la cinta de salida (obsérvese que $O(\log C(n))$ celdas trabajo serán suficientes para registrar estas ubicaciones), la posición de cada nuevo símbolo separador que imprime $\tilde{M}$ sobre la cinta de salida se compara con las dos posiciones guardadas en memoria, y se conservan las dos posiciones mas bajas. Es claro que de esta manera, al final del proceso se obtiene la ubicación de los primeros separadores impresos por $\tilde{M}$ sobre la cinta de salida.

Posteriormente, se simula $\lceil \frac{\rho-1}{2} \rceil$ veces más el funcionamiento de $\tilde{M}$ de forma similar a la descripta, a fin de obtener las posiciones del ρ-ésimo y el $(\rho+1)$-ésimo separador (sólo se calculan dos posiciones por vez). Desde ya, el espacio de memoria ocupado por las posiciones de separadores anteriormente

calculados se reutiliza cada vez.

El espacio adicional necesario para realizar este procedimiento es de tipo $O(\log S(n))$, lo cual demuestra el enunciado del lema 3. □

Cabe destacar que el resultado del lema 3 también podría haberse obtenido como corolario del lema 2. Sin embargo, debido a la generalidad del enunciado del lema 2, el tiempo de computación que se obtiene de esa manera es netamente superior al del proceso que aquí se describe.

Una de las principales ventajas que resulta de la introducción de las familias de circuitos booleanos como modelo de computación es que es posible apreciar el concepto de *buena paralelizabilidad* en las funciones booleanas. Una función booleana $g : \{0,1\}^* \to \{0,1\}$ se dice bien paralelizable si existe una familia de circuitos booleanos $C_g = \{c_n\}_{n\in\mathbb{N}}$ de talla polinomial $n^{O(1)}$ y profundidad polilogarítmica $O(\log^i n)$ que calcula g (cf. [8], [108], [181]).

El tiempo paralelo queda claramente representado por la profundidad del circuito, sugiriendo la idea de un conjunto de procesadores atravesando el circuito simultáneamente y ejecutando las operaciones definidas por los nodos que encuentran en su camino. Resulta entonces natural relacionar la talla y la profundidad de circuito con el tiempo secuencial y paralelo respectivamente.

En este sentido, las clases NC^i conformadas por las funciones booleanas que pueden calcularse por medio de una familia *uniforme* de circuitos booleanos de talla $n^{O(1)}$ y profundidad $O(\log^i n))$ (cf. [8]) representan las clases de funciones que se pueden beneficiar significativamente con el uso de la computación paralela. De hecho, de acuerdo con la definición dada, el tiempo necesario para calcular cualquier función en NC^i se reduce de polinomial a polilogarítmico cuando se pasa de computación secuencial a paralela.

Una pregunta interesante es si tal propiedad es significativa sólo en el ámbito de la computación paralela, o tiene también repercusiones en el ámbito de la computación secuencial.

En ([24]), A. Borodin halló una respuesta positiva a esta pregunta. La siguiente es una interpretación algorítmica de dicho teorema.

Teorema 1 ([24], Theorem 4) *Sea $f : \{0,1\}^* \to \{0,1\}$ una función booleana en NC^i. Entonces existe una máquina de Turing determinística M que calcula f en espacio $O(\log^i n)$.*

Demostración Sea $C = \{c_n\}_{n\geq 1}$ la familia de circuitos booleanos que calcula f cuya existencia garantiza el enunciado. Dado que la familia C es uni-

forme, aplicando el lema 3 se obtiene una máquina de Turing determinística M_U que, con una entrada $1^n\#\rho$, calcula la codificación del ρ–ésimo nodo de c_n en espacio $O(\log^i n)$.

Se desea construir una máquina de Turing determinística M la cual, para cada número natural n, sobre una entrada dada de n bits evalúa el circuito c_n en espacio $O(\log^i n)$. Esta máquina M simulará la máquina M_U cuando sea necesario y utilizará una pila para su funcionamiento.

Como el objetivo es la evaluación de todos los nodos de salida, el procedimiento general de evaluación de un nodo que realiza M se repetirá sobre cada nodo de salida hasta que todos ellos resulten evaluados.

Comenzando por el nodo de salida cuyo resultado se quiere evaluar, la máquina M recorre el circuito con un esquema estándar de búsqueda en profundidad (ver [141] por ejemplo). La pila (de profundidad máxima $O(\log^i n)$) se utiliza a fin de codificar el camino desde el nodo de salida a evaluar al nodo que está siendo evaluado.

A fin de que cada celda de la pila tenga tamaño constante, se utiliza una codificación especial del camino de forma tal que en cada paso de la computación, la pila se ve como una palabra sobre el alfabeto $\{0, 1, \ell\}$. Esta palabra codifica la *elección* del camino que se sigue en cada nivel (nodo) entre su entrada izquierda y derecha. Al mismo tiempo, el resultado de la evaluación del subcircuito izquierdo se almacena, si el subcircuito derecho está siendo atravesado. Obviamente, siempre se utiliza el orden izquierda–derecho.

Cada vez que se necesita la códificación éstandar de un nodo cuyo número se conoce, M simula la máquina M_U. Por lo tanto, la máquina M, sobre una entrada x de longitud n, necesita las siguientes cantidades de celdas de espacio de memoria:

- $O(\log n)$ celdas para simular M_U.
- $O(\log^i n)$ celdas para la pila.
- $O(\log n)$ celdas para almacenar la codificación de un nodo.
- $O(\log n)$ celdas para almacenar el número de un nodo.

En conclusión, todo el proceso puede ser realizado con $O(\log^i n)$ celdas de trabajo, lo cual demuestra el teorema. □

1.1 Aritmética de baja profundidad

El teorema 1 permite transformar circuitos de baja profundidad en algoritmos que utilizan bajos recursos de memoria. Ahora bien, dado que los problemas a tratar son de naturaleza *aritmética* (fundamentalmente cuestiones algorítmicas de álgebra lineal y manipulaciones algebraicas de polinomios), es natural que los algoritmos que los resuelven se describan por medio de modelos aritméticos. En particular, la propiedad de la buena paralelizabilidad de los algoritmos que se desarrollarán se ven bien reflejadas en los *circuitos aritméticos* (que se definirán posteriormente).

Por lo tanto, la aplicación del teorema 1 exige un proceso de traducción de cada familia de circuitos aritméticos $C = \{c_n\}_{n\in\mathbf{N}}$ en una familia de circuitos booleanos $\tilde{C} = \{\tilde{c}_{n,h}\}_{n,h\in\mathbf{N}}$ de acuerdo con las siguientes pautas:

- por cada nodo de entrada ρ del circuito aritmético c_n se crean h nodos de entrada en el circuito booleano $\tilde{c}_{n,h}$ que contienen la representación binaria del número entero (cuya longitud no supera los h bits) que ingresa como entrada en el nodo ρ.

- por cada nodo ρ de c_n marcado con una operación aritmética $op \in \{+, -, \cdot\}$ se corresponde con un subcircuito booleano que, con la codificación binaria de los dos antecesores ρ_1, ρ_2 de ρ como entrada, produce la representación binaria de $\rho := \rho_1\, op\, \rho_2$ como salida.

Es entonces de suma importancia que los circuitos booleanos que realizan las operaciones aritméticas sean sumamente eficientes, tanto en talla como en profundidad. Esta subsección se dedicará a la descripción de tales circuitos booleanos, que han sido tomados de [108] y [181]. Cabe destacar que todos los circuitos aquí presentados son uniformes.

1.1.1 Suma de números enteros

Un circuito de adición toma dos números enteros de r bits como entrada y produce la representación binaria de la suma de ambos números como salida. Sean $(x_{r-1}, \ldots, x_0)$ e $(y_{r-1}, \ldots, y_0)$ las representaciones binarias de las entradas y sea $(z_r, \ldots, z_0)$ la de la salida.

Nótese por c_j el *bit de acarreo* de la j-ésima posición. Se definen el j-ésimo *bit de acarreo generado* g_j y el j-ésimo *bit de acarreo propagado* por

$g_j = x_j \wedge y_j$ y $p_j = x_j \vee y_j$ respectivamente. Dado que $c_j = g_j \vee (p_j \wedge c_{j-1})$ y $z_j = x_j \oplus y_j \oplus c_{j-1}$ para $j = 0 \ldots r$ (donde $\oplus$ es el "o" *exclusivo* y c_{-1} se define como cero), se deduce que $c_j = \bigvee_{i \leq j} g_i \wedge p_{i+1} \wedge \ldots \wedge p_j$.

Con estas fórmulas es posible obtener el siguiente circuito para la adición de dos números enteros:

- Calcular todos los bits de acarreo generados g_j y todos los bits de acarreo propagados p_j en paralelo.
- Calcular $g_i \wedge p_{i+1} \wedge \ldots \wedge p_j$ en paralelo para $1 \leq i \leq r-1$.
- Calcular c_j para $0 \leq j \leq r-1$ a partir de los resultados de la última etapa.
- Calcular cada z_j a partir de x_j, y_j y c_{j-1} en paralelo para $0 \leq j \leq r$.

Con una implementación directa del proceso descripto resulta un circuito booleano de talla $O(r^2)$ y profundidad $O(\log r)$, mientras que si el cálculo de las expresiones $g_i \wedge p_{i+1} \wedge \ldots \wedge p_j$ se realiza por medio de un algoritmo paralelo para sumas de prefijos ([117]) se obtiene un circuito de talla $O(r)$ y profundidad $O(\log r)$.

1.1.2 Sumatorias de números enteros

Un circuito para la sumatoria de n números enteros de r bits toma como entrada la representación binaria de los n números y produce como salida la de su adición.

A fin de obtener tal circuito, se puede organizar el cálculo en un árbol binario balanceado, donde cada hoja realiza la adición de dos números enteros por medio del circuito anteriormente descripto. Sin embargo, este esquema produce un circuito de profundidad $O(\log n \log r)$, cantidad que es de orden superior al logaritmo del tamaño de la entrada.

En cambio, se utiliza una alternativa que se basa en un truco conocido como *tres-por-dos*, el cual, con talla y profundidad constante reduce el problema de sumar tres números enteros de s bits a la suma de dos números enteros de $s+1$ bits.

Sean $a = (a_{s-1}, \ldots, a_0)$, $b = (b_{s-1}, \ldots, b_0)$ y $c = (c_{s-1}, \ldots, c_0)$ los tres números de s bits a sumar. Si se suman los tres bits a_i, b_i y c_i para cada

$i \in \{0, \ldots, s-1\}$, se obtiene un número de dos bits $a_i + b_i + c_i = 2 \cdot u_i + v_i$, cuyo cálculo requiere talla y profundidad constante. Dado que todos los dígitos u_i y v_i pueden calcularse simultáneamente para $i = 0, \ldots, s-1$, este cómputo se realiza con talla $O(r)$ y profundidad constante. Luego, $a + b + c = u + v$ donde $u = (u_{s-1}, \ldots, u_0, 0)$ y $v = (v_{s-1}, \ldots, v_0)$.

La adición de n números enteros de r bits puede entonces realizarse aplicando $O(\log n)$ iteraciones del truco de tres-por-dos, con lo cual se reduce a dos el número de enteros a sumar, seguido de una adición final de los dos números enteros resultantes. El circuito que resulta de este proceso tiene talla $O\big(n(r + \log n)^2\big)$ y profundidad $O\big(\log(nr)\big)$.

1.1.3 Producto de números enteros

Un circuito de multiplicación toma dos números enteros de r bits como entrada y calcula los $2r$ bits del producto como salida. Sea $(x_{r-1}, \ldots, x_0)$ y $(y_{r-1}, \ldots, y_0)$ la representación binaria de las entradas y sea $(z_{2r-1}, \ldots, z_0)$ la de la salida.

El método escolar produce r números de $O(r)$ bits que se suman para obtener el producto. Denótese por $z^{(i)}$ el i-ésimo número a sumar en la multiplicación. Entonces $z^{(i)} = (x_{r-1} \wedge y_i, \ldots, x_0 \wedge y_i, \underbrace{0, \ldots, 0}_{i \text{ veces}})$ para $i = 0, \ldots, r$. Luego, se aplica $O(\log r)$ veces el truco de tres-por-dos para reducir la suma $z^{(r-1)} + \cdots + z^{(0)}$ a la adición de dos números, los cuales finalmente se suman. De esta manera se tiene un circuito de multiplicación de talla $O(r^2)$ y profundidad $O(\log r)$.

Cabe destacar que existen circuitos *uniformes* de multiplicación mas eficientes que el descripto en esta subsección. El mejor circuito conocido hasta el momento ha sido desarrollado por A. Schönage y V. Strassen ([160]) en base al cálculo de la Transformada de Fourier Discreta sobre ciertos anillos finitos y posee talla $O(r \log r \log\log r)$ y profundidad $O(\log r)$. Sin embargo, dado que el impacto de este circuito sobre las cotas de complejidad es bastante modesto, se ha preferido no reemplazarlo por el descripto a fin de mantener esta exposición autocontenida.

1.2 Algebra lineal

La resolución de los problemas de eliminación que se tratarán se basa en reducciones a cuestiones de álgebra lineal, que generalmente involucran matrices de gran tamaño. Es por lo tanto de suma importancia que los algoritmos de álgebra lineal que se utilizan sean muy eficientes en la utilización de recursos computacionales.

En esta sección se resolverán algunos problemas de álgebra lineal mediante familias uniformes de circuitos booleanos de baja profundidad. De esta manera, en virtud del teorema de Borodin (teorema 1), estas familias de circuitos se pueden convertir en algoritmos que requieren bajos recursos de memoria.

Se describen a continuación las familias de circuitos correspondientes, con la atención puesta en el control de la profundidad de los mismos así como en su uniformidad.

1.2.1 Operaciones matriciales

Producto de matrices

Sean A, B dos matrices de tamaños $n \times l$ y $l \times m$ respectivamente, con coeficientes cuya representación binaria tiene una longitud no mayor que h bits y sea $C := A \cdot B$. Como es bien sabido, los coeficientes c_{ij} de C pueden calcularse por medio de la fórmula:

$$c_{ij} = \sum_{k=1}^{l} a_{ik} b_{kj} \tag{1.1}$$

La evaluación de la fórmula (1.1) para $1 \leq i \leq n$ y $1 \leq j \leq m$ puede llevarse a cabo de la siguiente manera: en primer lugar se calculan todos los productos $a_{ik}b_{kj}$. De acuerdo con los resultados de la subsección 1.1.3, este cálculo requiere $O(nmlh^2)$ operaciones booleanas con profundidad $O(\log h)$.

Posteriormente se calculan todas las adiciones $\sum_k a_{ik}b_{kj}$ siguiendo el esquema detallado en la sección 1.1.2 con talla $O(nmlh^2)$ y profundidad $O(\log(hl))$. De esta manera, se tiene un circuito booleano que realiza el producto de matrices tiene talla $O(nmlh^2)$ y profundidad $O(\log(hl))$.

La uniformidad de la familia de circuitos $\{C_{n,m,l,h}\}_{n,m,l,h \in \mathbf{N}}$ que calcula el producto de 2 matrices de tamaños $n \times l$ y $l \times m$ con coeficientes de h

bits de longitud es una consecuencia directa de la estructura aritmética del procedimiento y la uniformidad de los circuitos booleanos que realizan las operaciones aritméticas.

Se puede construir una máquina de Turing M que genera la codificación estándar del circuito $C_{n,l,m,h}$ descripto en espacio $O(\log(nmlh))$. Esta máquina M organiza las operaciones aritméticas a realizar en función de los índices involucrados: por ejemplo, para ordenar el cálculo de los productos $a_{ik}b_{kj}$ se define un orden sobre las 3-uplas (i,k,j). El orden inducido por la función

$$(i,k,j) \rightarrow k + N \cdot i + N^2 \cdot i$$

donde $N := max\{n,l,m\}$, es particularmente conveniente, ya que los productos $a_{ik}b_{kj}$ se ordenan en la forma en que luego éstos se sumarán. El manejo de esta función y su decodificación puede llevarse a cabo en espacio $O(\log(nmlh))$.

Asimismo, M genera la codificación estándar de los circuitos que realizan las operaciones aritméticas, simulando a tal efecto la máquinas que producen la codificación estándar de los circuitos booleanos que realizan dichas operaciones. Dado que el tamaño de los números enteros involucrados en estas operaciones es polinomial en los parámetros n,m,l,h, se deduce que M requiere espacio de tipo $O(\log(nmlh))$ para realizar estas simulaciones. En conclusión, se puede enunciar el siguiente lema:

Lema 4 *Existe una familia uniforme en espacio $O(\log(nmlh))$ de circuitos booleanos de talla $O(nmlh^2)$ y profundidad $O(\log(hl))$ que realiza el producto de dos matrices de tamaños $n \times l$ y $l \times m$ con coeficientes enteros de a lo sumo h bits.*

Cabe destacar que existen algoritmos mas refinados para el producto de matrices (como los desarrollados en [169], [136] o [50] por ejemplo). Sin embargo, a fin de mantener esta exposición autocontenida, éstos no han sido tomados en cuenta debido al modesto impacto que los mismos producen sobre las cotas de complejidad de los algoritmos desarrollados en esta sección.

Producto iterado de matrices

Sean $A_1,\ldots,A_n$ matrices de tamaños $m_1 \times m_2,\ldots,m_n \times m_{n+1}$ respectivamente, con coeficientes enteros de a lo sumo h bits. Sea $m := max\{m_i : 1 \leq i \leq n+1\}$. El problema es calcular el producto $\prod_{i=1}^{n} A_i$.

Este producto se organiza en un árbol binario balanceado, donde cada nivel de profundidad consiste de los productos, dos a dos, de las matrices calculadas en el nivel anterior.

Dado que el producto de 2 matrices de tamaño $m_i \times m_j$ y $m_j \times m_k$ con coeficientes enteros de h bits es una matriz cuyos coeficientes tienen $2h + \log m$ bits, iterando este razonamiento se deduce que el tamaño bit de los coeficientes de las matrices que se calculan en el l-ésimo nivel de profundidad del árbol de productos está acotado por $2^l h + l \log m$.

Por lo tanto, como se realizan n productos organizados en $\log(n)$ niveles de profundidad, el circuito booleano que calcula el producto $\prod_i A_i$ tiene talla $O(\sum_{l=1}^{\lceil \log n \rceil}(2^l h + l \log m)^2 m^3 \frac{n}{2^l}) = O(n^2 h^2 m^3 \log^2 m \log^2 n)$ y profundidad $O(\log(nhm) \log n)$.

La uniformidad de la familia de circuitos $\{C_{n,m_1,\ldots,m_n,h}\}_{n,m_1,\ldots,m_n,h}$ es consecuencia de la uniformidad del producto de dos matrices (lema 4) y la organización del producto $\prod_i A_i$ en un árbol binario balanceado. Es posible diseñar una máquina de Turing determinística que genera el código del circuito $C_{n,m_1,\ldots,m_n,h}$ en espacio $\log(nmh)$, reutilizando para ello cada vez el espacio necesario para generar el código de un subcircuito que realiza el producto de 2 matrices. Por lo tanto, se tiene el siguiente resultado:

Lema 5 *Existe una familia de circuitos booleanos uniforme en espacio* $O(nmh)$ *de talla* $O(n^2 h^2 m^3 \log^2 m \log^2 n)$ *y profundidad* $O(\log(nhm) \log n)$ *que calcula el producto* $\prod_i A_i$.

Otro caso de producto iterado de matrices de interés es el de la potenciación: dada una matriz A de tamaño $n \times n$ con coeficientes enteros de talla binaria h y un número natural $k \leq n$, el problema es calcular las potencias $A^2, \ldots, A^k$.

En este caso se puede organizar el cálculo de manera de realizar exactamente k productos con profundidad $\log k$. La forma de hacerlo es la siguiente: supónganse construídos los primeros l niveles de de profundidad, donde se calcularon las potencias $A, A^2, \ldots, A^{2^l}$. Entonces, en el $(l+1)$–ésimo nivel se multiplica A^{2^l} por todas las potencias anteriormente calculadas, de modo de obtener las potencias $A^{2^l+1}, \ldots, A^{2^{l+1}}$.

Mediante consideraciones similares a las del lema 5, se obtiene el siguiente resultado:

Lema 6 *Existe una familia de circuitos booleanos uniforme en espacio* $O(\log(nh))$ *de talla* $O(k^2n^3h^2\log^4 n)$ *y profundidad* $O(\log(nh)logn)$ *que calcula las potencias* $A^2,\ldots,A^k$.

1.2.2 Cálculo del polinomio característico

Sea A una matriz $n \times n$ con coeficientes enteros de tamaño bit acotado por h y χ_A su polinomio característico. Se trata ahora de calcular los coeficientes del polinomio característico χ_A (en particular se calculan el determinante y la traza de A).

Escríbase la matriz A en la forma

$$A = \begin{pmatrix} a_{1,1} & R \\ S & M \end{pmatrix}$$

donde R, S y M son matrices enteras de tamaños $1 \times (n-1)$, $(n-1) \times 1$ y $(n-1) \times (n-1)$ respectivamente. Sean

$$\chi_A(\lambda) = \det(M - \lambda \cdot I) = \sum_{i=0}^{n} p_{n-i}\lambda^i$$
$$\chi_M(\lambda) = \det(M - \lambda \cdot I) = \sum_{i=0}^{n-1} q_{n-1-i}\lambda^i$$

Entonces se satisface la siguiente relación [19, Claims 1 and 2]:

$$\chi_A(\lambda) = (a_{1,1} - \lambda)\cdot\det(M - \lambda\cdot I) - R\cdot(\sum_{k=2}^{n}(M^{k-2}\cdot q_0 + \cdots + I\cdot q_{k-2})\cdot\lambda^{n-k})\cdot S$$

A partir de esta ecuación se deduce que existe una relación lineal entre los coeficientes de χ_A y los de χ_M, que puede expresarse fácilmente en la forma:

$$(p_0, p_1, \ldots, p_n)^t = C_1 \cdot (q_0, \ldots, q_{n-1})^t \tag{1.2}$$

donde C_1 es la matriz Toeplitz triangular inferior de tamaño $n \times (n-1)$ definida por:

$$c_{i,j} = \begin{cases} -1 & \text{si} \quad i = j \\ a_{1,1} & \text{si} \quad i = j+1 \\ -R \cdot M^{i-j-2} \cdot S & \text{si} \quad i - j \leq 2 \end{cases}$$

De este modo se reduce el cálculo de los coeficientes del polinomio característico de la matriz A al de los coeficientes del polinomio característico de una submatriz de A. Por lo tanto, iterando este razonamiento se tiene un algoritmo que calcula χ_A *sin divisiones ni ramificaciones.* Mas precisamente, para $1 \leq k \leq n$ se define

$$R_k = (a_{k,k+1}, \ldots, a_{k,n})$$

$$S_k = (a_{k+1,k}, \ldots, a_{n,k})$$

$$M_k = \begin{pmatrix} a_{k,k} & a_{k,n} \\ \vdots & \vdots \\ a_{n,k} & a_{n,n} \end{pmatrix}$$

Se escribe $\chi_{M_k}(\lambda) = \sum_{i=0}^{n-k} q_{n-k-i}^k \lambda^i = \det(M_k - \lambda \cdot I)$ y se define la matriz Toeplitz triangular inferior C_k de $(n-k+1) \times (n-k)$ por:

$$c_{i,j}^k = \begin{cases} -1 & \text{if} \quad i = j \\ a_{k,k} & \text{if} \quad i = j-1 \\ -R_k \cdot M_k^{i-j-2} \cdot S_k & \text{if} \quad i - j \leq 2 \end{cases}$$

La relación (1.2) toma ahora la forma:

$$(q_0^{k-1}, q_1^{k-1}, \ldots, q_{n-k+1}^{k-1})^t = C_k \cdot (q_0^k, \ldots, q_{n-k}^k)^t$$

y aplicándola recursivamente se tiene la identidad:

$$(p_0, p_1, \ldots, p_n)^t = \prod_{k=1}^{n} C_k$$

Las matrices C_k pueden calcularse en forma simultánea, lo que permite reducir la profundidad de los circuitos que calculan χ_A. Asimismo, a fin de reducir la talla de los circuitos, los coeficientes $R_k(M_k)^j S_k$ se calculan de la manera siguiente:
dado que $j < n$, es posible escribir a j en la forma $j = j_1 + j_2\sqrt{n}$, donde $j_1, j_2 < \sqrt{n}$. Por lo tanto, en lugar de calcular la potencia $(M_k)^j$ para luego multiplicarla por R_k y S_k, se calculan las matrices $R_k(M_k)^{j_1}$ y $\left((M_k)^{\sqrt{n}}\right)_2^j S_k$ que multiplicadas dan el producto $R_k(M_k)^j S_k$ buscado. En definitiva, el proceso completo puede describirse de la manera siguiente:

Procedimiento 1: *Algoritmo para el cálculo del polinomio característico.*

1. *Calcular las potencias* $(M_k)^{2^j}$ *para* $j = 1, \ldots, \lceil \log \sqrt{n} \rceil$ *en forma simultánea para* $k = 1, \ldots, n$.

2. *Calcular los productos* $R_k(M_k)^j$ *para* $j = 1, \ldots, \lceil \sqrt{n} \rceil$ *en un árbol binario balanceado de estructura similar al del lema 6, en paralelo para* $k = 1, \ldots, n$.

3. *Calcular la potencia* $(M_k)^{\sqrt{n}}$ *para* $k = 1, \ldots, n$ *en forma simultánea.*

4. *Calcular las potencias* $(M_k)^{2^j\sqrt{n}}$ *para* $j = 1, \ldots, \lceil \log \sqrt{n} \rceil$ *en forma similar al paso 1.*

5. *Calcular los productos* $(M_k)^{j\sqrt{n}} S_k$ *para* $j = 1, \ldots, \lceil \sqrt{n} \rceil$ *en forma similar al paso 2.*

6. *Calcular los productos* $R_k(M_k)^{j_1} \cdot (M_k)^{j_2\sqrt{n}} S_k$ *para* $k = 1, \ldots, n$ *en forma simultánea.*

7. *Calcular el producto* $\prod_{k=1}^{n} C_k$ *en un árbol binario balanceado.*

Teniendo en cuenta que las matrices $(M_k)^j$ tienen coeficientes enteros de tamaño acotado por $O(h + \log n)$, combinando los lemas 4, 5 y 6 se deduce que la familia de circuitos booleanos descripta tiene talla $O(n^6 h^2)$ y profundidad $O(\log(nh) \log n)$, teniendo los coeficientes calculados a lo sumo $O(n(h + \log n))$ bits.

La uniformidad de esta familia depende ahora de la uniformidad de los algoritmos que realizan los diferentes tipos de producto de matrices y la manera en que se ordena el cálculo de las matrices $R_k(M_k)^{j_1}$ y $(M_k)^{j_2\sqrt{n}} S_k$. Dado que los pares (j_1, j_2) se obtienen a partir de la división de j por $\sqrt{n}$, esto sugiere un ordenamiento de los pares (j_1, j_2) según el número $j := j_1 + j_2 \lceil \sqrt{n} \rceil$ que representan.

En conclusión, se ha demostrado el siguiente resultado:

Lema 7 *Existe una familia de circuitos booleanos* $\{C_{n,h}\}_{n,h \in \mathbf{N}}$ *uniforme en espacio* $\log(nh)$, *de tamaño* $O(n^6 h^2)$ *y profundidad* $O(\log(hn) \log n)$ *que calcula los coeficientes del polinomio característico de* A.

1.2.3 Cálculo de la matriz adjunta

Sea A una matriz $n \times n$ no singular con coeficientes enteros de tamaño bit acotado por h. La matriz adjunta de A, $Adj(A)$, se define de la siguiente manera: si $Adj(A) := (b_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$, entonces se tiene la relación:

$$b_{ij} := (-1)^{i+j} det(A(j,i))$$

donde $A(j,i)$ denota la matriz de tamaño $(n-1) \times (n-1)$ que se obtiene a partir de A si se elimina la j-ésima fila y la i-ésima columna de A. La siguiente propiedad de la matriz $Adj(A)$ es bien conocida:

$$A \cdot Adj(A) = Adj(A) \cdot A = det(A) Id_{n \times n}$$

El método para calcular $Adj(A)$ se basa en el cálculo del polinomio característico $\chi_A(T) := T^n + p_{n-1}T^{n-1} + \cdots + p_0$ de A: el teorema de Cayley-Hamilton asegura que

$$\chi_A(A) := A^n + p_{n-1}A^{n-1} + \cdots + p_0 Id_{n \times n} = 0_{n \times n}$$

por lo tanto, multiplicando esta identidad por la matriz $Adj(A)$ se obtiene:

$$\begin{aligned} 0_{n \times n} &= Adj(A) \cdot A^n + p_{n-1} Adj(A) \cdot A^{n-1} + \cdots + p_0 \cdot Adj(A) = \\ &= p_0 A^{n-1} + p_0 p_{n-1} A^{n-2} + \cdots + p_0 \cdot Adj(A) \end{aligned}$$

Luego, dado que $p_0 \neq 0$, diviendo el tercer miembro de la identidad anterior por p_0 se tiene la igualdad:

$$Adj(A) = -A^{n-1} - p_{n-1}A^{n-2} + \cdots - p_1 Id_{n \times n} \tag{1.3}$$

La ecuación (1.3) se puede transformar fácilmente en un algoritmo para el cálculo de $Adj(A)$: se calculan los coeficientes del polinomio característico de A, las potencias sucesivas $A^2, \ldots, A^{n-1}$ y se realiza la combinación lineal de dichas potencias indicada en (1.3). Teniendo en cuenta los resultados del lema 7 se concluye:

Lema 8 *Existe una familia de circuitos booleanos $\{C_{n,h}\}_{n,h \in \mathbf{N}}$ uniforme en espacio $\log(nh)$, de tamaño $O(n^6 h^2)$ y profundidad $O(\log(hn) \log n)$ que calcula la matriz adjunta de A.*

1.2.4 Cálculo del rango

Sea A una matriz de tamaño $n \times m$ con coeficientes enteros de h bits, cuyo rango $rg(A)$ se desea calcular. Dado que $rg(A) = rg(A \cdot A^t)$, se puede calcular el rango de la matriz $B := A \cdot A^t$ en lugar del de A.

Ahora bien, como B es diagonalizable se tiene que $n - rg(B)$ coincide con la multiplicidad de cero como raíz del polinomio característico de B, χ_B. Entonces se puede aplicar el algoritmo descripto en la sección 1.2.2 a fin de calcular los coeficientes de χ_B, y el número $n - rg(B)$ se obtiene por simple inspección de estos coeficientes.

Se describe entonces una familia de circuitos booleanos uniforme que calcula el número $rg(B) = \max\{i; 1 \leq i \leq n \wedge p_i \neq 0\}$ a partir de la codificación binaria de los coeficientes p_i de χ_B.

Para este propósito, se diseñan subcircuitos "$p_i = 0$" y "$p_i \neq 0$" que tienen el mismo valor booleano de verdad que el enunciado con el cual han sido etiquetados.

Sea $p_i = (p_{i_s}, \ldots, p_{i_0})$ la representación binaria de p_i. Entonces $p_i = 0$ si y sólo si todos sus dígitos son nulos, es decir, si $p_{i_s} \vee \cdots \vee p_{i_0} = 0$. Por lo tanto, el operador $\neg(p_{i_s} \vee \cdots \vee p_{i_0})$ tiene el mismo valor de verdad que $p_i = 0$, y esta misma afirmación es cierta para $p_{i_s} \vee \cdots \vee p_{i_0}$ y $p_i \neq 0$ respectivamente. Cada par de subcircuitos "$p_i = 0$" y "$p_i \neq 0$" tiene talla $O(n(h + \log n))$ y profundidad $O(\log(n) \log h)$ (la talla coincide con el número de bits de p_i) y pueden evaluarse en forma independiente para $1 \leq i \leq n$, por lo cual se concluye que todos los pares de subcircuitos requieren talla $O(n^2(h + \log n))$ y profundidad $O(\log h \log n)$.

Luego, para cada $1 \leq i \leq n$ se construye un subcircuito que computa el valor de verdad del enunciado "$p_0 = 0 \wedge p_1 = 0 \wedge \cdots \wedge p_i \neq 0$", por medio de un árbol de conjunciones de las salidas de los subcircuitos previamente construídos. Este árbol tiene talla y profundidad acotadas por n y $\log n$ para cada i, de donde se deduce que las todas las expresiones $p_0 = 0 \wedge p_1 = 0 \wedge \cdots \wedge p_i \neq 0$ pueden calcularse con talla y profundidad adicionales de tipo $O(n^2)$ y $\log n$.

Finalmente, dado un número natural $i \in \{1 \ldots n\}$ con representación binaria $i = (i_s, \ldots, i_0)$, se define $\tilde{i} = (\tilde{i_s}, \ldots, \tilde{i_0})$ por: $\tilde{i_k} := (p_0 = 0 \wedge p_1 = 0 \wedge \cdots \wedge p_i \neq 0) \wedge i_k$, el cual devuelve el k-ésimo dígito de i sii la afirmación $p_0 = 0 \wedge p_1 = 0 \wedge \cdots \wedge p_i \neq 0$ es cierta y 0 en caso contrario.

En consecuencia, la disyunción $\bigvee_{i=1}^{n} \tilde{i}_k$ retorna el k–ésimo dígito del número entero $\max\{i; 1 \leq i \leq n \wedge p_i \neq 0\}$. Dado que talla $O(n^2(h + \log n))$ y profundidad $O(\log n)$ es suficiente para implementar esta última construcción, se tiene talla $O(n^3 h)$ y profundidad $O(\log(n) \log h)$ para todo el circuito.

La uniformidad de esta familia de circuitos es consecuencia directa de su descripción, dado que su construcción sólo se refiere al tamaño bit de los coeficientes del polinomio característico χ_B.

Utilizando los resultados del lema 7, se deduce el siguiente resultado:

Lema 9 *Existe una familia de circuitos booleanos uniforme en espacio* $O(\log(nh))$ *de talla* $O(n^6 h^2)$ *y profundidad* $O(\log(hn) \log n)$ *que calcula el rango de cualquier matriz entera* $n \times m$ *con coeficientes de* h *bits.*

Cabe destacar que si la matriz A pertenece a $R^{n \times m}$, siendo R un dominio efectivo arbitrario ($\mathbb{Z}[X_1, \ldots, X_n]$ por ejemplo), el cálculo de $rg(A)$ puede reducirse al cálculo de un polinomio característico aplicando técnicas debidas a K. Mulmuley [132] (ver también [47]).

En primer lugar, siendo X una nueva indeterminada, se define la forma bilineal simétrica $B := A^t \cdot M \cdot A$ donde M es la matriz diagonal de $n \times n$ cuyo i-ésimo coeficiente M_{ii} tiene la forma $M_{ii} := X^{i-1}$ para $i = 1, \ldots, n$.

En [132, Lemma 1] se demuestra que $rg(A) = rg(B)$. Por lo tanto, el problema se reduce al cálculo del rango de una matriz simétrica B de tamaño $m \times m$.

Posteriormente, se extiende una vez mas el cuerpo de coeficientes por medio de la adición de una nueva indeterminada Y, y se construye una matriz simétrica $C := N \cdot B \cdot N$, donde N es una matriz diagonal de $m \times m$ definida por $N_{ii} := Y^{i-1}$ para $i = 1, \ldots, n$.

Esta nueva matriz C verifica que $rg(C) = rg(B)$ y además se satisface que $rg(C)$ es igual a la multiplicidad de cero como raíz del polinomio característico de C. Por lo tanto, es la reducción buscada.

1.2.5 Resolución de sistemas de ecuaciones lineales

Sea A una matriz entera de $n \times m$, X un vector de tamaño $m \times 1$ cuyos coeficientes son incógnitas y b un vector entero de $n \times 1$. Sea h una cota superior par el tamaño bit de todos los coeficientes de A y b. El problema es resolver el sistema de ecuaciones lineales $A \cdot X = b$.

La idea es chequear en primer lugar que el sistema considerado es compatible. Esta cuestión puede resolverse mediante cálculos de rango: como es bien sabido, el sistema $A \cdot X = b$ es compatible si y sólo si $rg(A) = rg(A, b)$, donde (A, b) denota la matriz cuyas primeras m columnas son las de A y tiene las coordenadas del vector como última columna.

En caso en que el sistema resulte compatible, se reduce su resolución a la de un sistema con matriz cuadrada no singular. Dado que este último sistema puede resolverse mediante la aplicación la regla de Cramer, se tiene la solución al problema original.

La reducción consiste en hallar una submatriz cuadrada no singular de A, que se denotará $\tilde{A}$, de rango máximo, y reexpresar el sistema en términos de $\tilde{A}$. Esto significa que se considera el vector $\tilde{b}$ que se obtiene a partir de b quitando aquellas coordenadas de b que no corresponden a las filas de $\tilde{A}$, y que se fijan como cero todas las coordenadas de X que no corresponden a las columnas de $\tilde{A}$. A partir de cualquier solución del sistema $\tilde{A} \cdot \tilde{X} = \tilde{b}$ se obtiene una solución fácilmente una solución del sistema original $A \cdot X = b$.

Para hallar la submatriz cuadrada $\tilde{A}$ de rango máximo, es necesario evitar una búsqueda exhaustiva, ya que esto resultaría en un crecimiento exponencial de las cotas de complejidad. El proceso que se describirá elige en primer lugar cuales filas de A formarán la matriz $\tilde{A}$, calculando para ello el rango de n matrices. Con un esquema similar se determina que columnas de A se eligen para construir $\tilde{A}$.

Denótese por A_i la i-ésima fila de A. Se calcula en paralelo $rg(A_1, \ldots, A_i)$ para $i = 1, \ldots, n$. Cada vez que $rg(A_1, \ldots, A_{i-1}) < rg(A_1, \ldots, A_i)$ se conserva en memoria el índice i. Estos índices corresponden a las filas que forman $\tilde{A}$. Obsérvese que la matriz formada a partir de las filas elegidas de esta manera tiene el mismo rango que A y todas sus filas son linealmente independientes.

El circuito descripto calcula el rango de $2 + m + n$ matrices de tamaño no mayor que $n \times m + 1$ en 3 etapas sucesivas siguiendo el esquema de la sección 1.2.4. Posteriormente, culmina con el cálculo de a lo sumo n determinantes de matrices de tamaño acotado por n, para lo cual se utiliza el algoritmo de la sección 1.2.2. Su uniformidad se deduce directamente de su descripción y la uniformidad de los circuitos que calculan rango y determinante.

Por lo tanto, a partir de los resultados de los lemas 7 y 9 se puede concluir:

Lema 10 *Existe una familia de circuitos booleanos uniforme en espacio* $O(\log(mnh))$ *de tamaño* $(mnh)^{O(1)}$ *y profundidad* $O(\log(mnh)\log n)$ *tal que chequea si existe una solución del sistema* $A \cdot X = b$*, y, en tal caso, calcula numeradores y denominadores de una solución particular del sistema.*

La talla binaria de la solución calculada puede acotarse por $O(nh \log n)$.

Cabe destacar que mediante una leve modificación del esquema anterior se puede construir un conjunto afinmente independiente maximal de soluciones del sistema de ecuaciones lineales considerado. Para tal propósito, basta notar que la solución particular hallada asigna el valor cero al conjunto de variables $\mathcal{A} := \{X_{r+1}, \ldots, X_n\}$ *a priori*. Esto es posible dado que, por la manera en que se eligieron las filas y columnas que forman $\tilde{A}$, toda asignación de valores $(x_{r+1}, \ldots, x_n) \in \mathbf{C}^n$ a las variables en $\mathcal{A}$ se corresponde con una única solución del sistema que verifica $X_{r+1} = x_{r+1}, \ldots, X_n = x_n$.

En consecuencia, si se asigna el vector de variables $(X_{r+1}, \ldots, X_n)$ todos los posibles valores de un conjunto independiente afín maximal de $\mathbf{Q}^{n-r-1}$, se obtiene un conjunto de soluciones del sistema que forma un conjunto afinmente independiente (dado que su proyección sobre las coordenadas $(X_{r+1}, \ldots, X_n)$ lo es). Mediante un argumento de dimensión se concluye que tal conjunto es maximal con la propiedad de ser afinmente independiente.

1.3 Operaciones con polinomios

Sea R un dominio de característica cero (en esta tesis, R típicamente será $\mathbb{Z}$ o un anillo de polinomios de tipo $\mathbb{Z}[X_1, \ldots, X_n]$ o $\mathbb{Q}[X_1, \ldots, X_n]$), K el cuerpo de cocientes de R y T una indeterminada sobre K.

En esta sección se desarrollarán algoritmos para realizar manipulaciones algebraicas con polinomios univariados en $R[T]$. Todos estos algoritmos serán bien paralelizables y no contendrán divisiones por elementos de R (en el caso $R = \mathbb{Z}[X_1, \ldots, X_n]$ por ejemplo, algoritmos que realizan divisiones por elementos de R pueden producir divisiones por cero al momento de evaluar las variables $X_1, \ldots, X_n$ en valores particulares).

Los algoritmos se describirán en el modelo de los *circuitos aritméticos*, que es el que mejor se adapta a estas cuestiones. Un circuito aritmético tiene una estructura similar a la de un circuito booleano, salvo por el hecho que sus nodos están etiquetados por una operación aritmética $op \in \{+, -, *, \div\}$. La talla y profundidad se definen en forma análoga al caso de los circuitos booleanos.

Aquí se prestará especial atención a las medidas *no escalares*, que son las que se obtienen cuando sólo se consideran las multiplicaciones entre dos polinomios no constantes, y la división cuando el divisor es no constante. En particular, la *profundidad no escalar* permite obtener las estimaciones mas precisas del grado de los polinomios representados de esta manera (cf. [114]) y la talla binaria de los números enteros involucrados, información de vital importancia para el proceso de traducción de circuitos aritméticos a circuitos booleanos en el sentido de la sección 1.1.

También se describirá explícitamente la traducción de estos circuitos aritméticos a circuitos booleanos en el caso en que $R = \mathbb{Z}[X_1, \ldots, X_n]$ y los elementos de R que aparecen en las entradas tienen grado y talla binaria prefijada. La uniformidad de los algoritmos así obtenidos se deducirá directamente de su estructura aritmética y del hecho que los mismos se basan en álgebra lineal que, según lo demostrado en la sección 1.2, es uniforme.

A fin de llevar a cabo estas traducciones, es necesario en primer lugar desarrollar circuitos booleanos que realizen la suma y producto de polinomios multivariados dados en representación densa y operaciones de álgebra lineal tales como el cálculo de los coeficientes del polinomio característico de una matriz cuyos coeficientes son polinomios multivariados.

En lo que sigue se operará con polinomios de $\mathbb{Z}[X_1, \ldots, X_n]$ de grado acotado por D, cuyos coeficientes tienen una talla binaria acotada por h. Asimismo, se fijará un orden monomial de fácil manipulación mediante el cual se ordenan los monomios, como por ejemplo el orden graduado lexicográfico definido por $X_1 > \cdots > X_n$ (ver [51]).

La suma de dos polinomios multivariados no ofrece dificultades: simplemente se suman los coeficientes correspondientes a monomios de las mismas potencias en ambos polinomios. Teniendo en cuenta que existen a lo sumo $O(D^n)$ monomios distintos de grado D en n variables y que la decodificación del orden monomial elegido se realiza en espacio $O\big(\log(nD)\big)$, se concluye que la suma de dos polinomios multivariados se realiza en forma uniforme con talla $O(D^n h^2)$ y profundidad $O(\log h)$.

La sumatoria de N polinomios multivariados se realiza, mediante consideraciones similares a las anteriores y los resultados de la subsección 1.1.2, uniformemente con talla $O\big(D^n N(h + \log N)^2\big)$ y profundidad $O(\log Nh)$.

El cálculo de los coeficientes del producto de dos polinomios multivariados F, G de grado D, cuyos coeficientes tienen talla binaria acotada por h requiere algo mas de reflexión. Sea $\gamma(D, n)$ la cantidad de monomios (distintos) en n variables de grado menor o igual que D. El orden monomial adoptado induce un ordenamiento de las n–uplas $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. Dado que este orden es *graduado*, todo $i \in \{1, \ldots, \gamma(2D, n)\}$ se corresponde con una n-upla no nula $(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})$ tal que $\sum_{k=1}^{n} \alpha_k^{(i)} \leq 2D$ y todo $j \in \{1, \ldots, \gamma(D, n)\}$ se corresponde con una n–upla no nula $(\beta_1^{(j)}, \ldots, \beta_n^{(j)})$.

Se considera entonces la matriz $M(F) \in \mathbb{Z}^{\gamma(2D,n) \times \gamma(D,n)}$ cuya (i, j)–ésima entrada m_{ij} se define de la manera siguiente: si $\alpha_k^{(i)} - \beta_k^{(j)} \geq 0$ para $k = 1, \ldots, n$, entonces m_{ij} es el coeficiente de F correspondiente al monomio

$$(\alpha_1^{(i)} - \beta_1^{(j)}, \ldots, \alpha_n^{(i)} - \beta_n^{(j)})$$

La matriz $M(F)$ fue contruída de forma tal que el vector resultante de multiplicar a $M(F)$ por el vector de los coeficientes de G corresponde a los coeficientes, ordenados según el orden monomial adoptado, del polinomio producto $F \cdot G$. Por lo tanto, los coeficientes del producto $F \cdot G$ se calculan en forma uniforme con talla $O(D^{2n} h^2)$ y profundidad $O\big(n \log(hD)\big)$.

Los resultados obtenidos se resumen en el siguiente lema:

Lema 11 *Sean $F, G, F_1, \ldots, F_n$ polinomios en $\mathbb{Z}[X_1, \ldots, X_n]$ de grado a lo sumo D, cuyos coeficientes tienen talla binaria acotada por h. Entonces, son ciertas las siguientes afirmaciones:*

- *Los coeficientes del polinomio $F + G$ se calculan por medio de una familia uniforme de circuitos booleanos de talla $O(D^n h^2)$ y profundidad $O(\log h)$.*

- *Los coeficientes del polinomio $F_1 + \cdots + F_N$ se calculan por medio de una familia uniforme de circuitos booleanos de talla $O\big(D^n N(h + \log N)^2\big)$ y profundidad $O(\log Nh)$.*

- *Los coeficientes del polinomio $F \cdot G$ se calculan por medio de una familia uniforme de circuitos booleanos de talla $O(D^{2n} h^2)$ y profundidad $O\big(n \log(hD)\big)$.*

Se tienen ahora todos los elementos necesarios para realizar el álgebra lineal con matrices cuyas entradas son polinomios multivariados. El esquema que se utiliza es generalmente el mismo de la sección 1.2 (excepto por el cálculo del rango, donde es necesario aplicar las técnicas descriptas en la subsección 1.2.4), realizándose las operaciones aritméticas entre polinomios multivariados con los métodos del lema 11.

Los resultados que se obtienen de esta manera se resumen en el siguiente lema:

Lema 12 *Sean A, B matrices en $\mathbb{Z}[X_1, \ldots, X_n]^{t \times t}$, tales que los polinomios que aparecen como entradas de A y B tienen grado y talla binaria acotada por D y h respectivamente. Entonces, las siguientes afirmaciones son válidas:*

- *El producto $A \cdot B$ se calcula por medio de una familia uniforme de circuitos booleanos de talla $O(t^3 D^{O(n)} h^2)$ y profundidad $O\big(n \log(Dht)\big)$.*

- *Existen familias uniformes de circuitos booleanos que calculan el determinante de A, su polinomio característico, su rango y la matriz adjunta $Adj(A)$ con talla $O(t^{O(n)} D^{O(n)} h^2)$ y profundidad $O\big(n \log t \log(Dht)\big)$.*

1.3.1 División entera

Sean $f = f_d T^d + \cdots + f_0$ y $g = g_e T^e + \cdots + g_0$ dos polinomios univariados en $R[T]$ de grados d y e respectivamente, tal que se verifica $g|f$ en $K[T]$. El problema es hallar el polinomio $\frac{f}{g} \in K[T]$.

La idea es simple: considerando el polinomio $h := \frac{f}{g}$ con coeficientes indeterminados, la condición $f = gh$ se traduce en un sistema de ecuaciones lineales que se obtiene por medio de la igualación de los coeficientes de f y gh correspondientes a la misma potencia. De esta manera, se tiene un sistema de $d+1$ ecuaciones con $d-e+1$ incógnitas, cuya resolución se reduce al de un sistema con matriz cuadrada no singular siguiendo las ideas de la sección 1.2.5.

Para ello, es necesario hallar una submatriz cuadrada de rango maximal que, en este caso, es fácil de elegir de antemano: es la que se obtiene tomando las primeras $d-e+1$ ecuaciones. En efecto, considerando solamente las ecuaciones correspondientes a las $d-e+1$ mayores potencias de T, el sistema tiene el siguiente aspecto :

$$\begin{pmatrix} f_d \\ \vdots \\ f_0 \end{pmatrix} \begin{pmatrix} g_e & \\ \vdots & \\ g_{d-e} & g_e \end{pmatrix} \begin{pmatrix} h_{d-e} \\ \vdots \\ h_0 \end{pmatrix}$$

donde $h = h_{d-e} T^{d-e} + \cdots + h_0$, de lo cual se deduce que dicha submatriz es de rango maximal $d-e+1$, ya que $g_e \neq 0$.

A fin de evitar divisiones en el cálculo de los coeficientes de h, en lugar de invertir la matriz del sistema se utiliza la matriz adjunta de la misma, por lo que se calcula un múltiplo $g_e^{d-e+1} h$ del polinomio h buscado (ya que g_e^{d-e+1} es el determinante de la matriz del sistema).

En conclusión, se tiene el siguiente resultado:

Lema 13 *Existe un circuito aritmético que calcula el cociente de f por g con talla $d^{O(1)}$ y profundidad no escalar $O(\log d)$.*

Supóngase ahora que los coeficientes $f_d, \ldots, f_0$ y $g_e, \ldots, g_0$ son polinomios en $\mathbb{Z}[X_1, \ldots, X_n]$ de grado acotado por D, cuyos coeficientes tienen talla binaria acotada por h. De los resultados de los lemas 11 y 12 se deduce el siguiente:

Lema 14 *Existe una familia uniforme de circuitos booleanos que calcula el cociente de f por g (salvo un múltiplo uniforme en $\mathbb{Z}[X_1,\ldots,X_n]$) con talla $O(d^{O(n)}D^{O(n)}h^2)$ y profundidad $O\big(n\log d\log(Dhd)\big)$*

1.3.2 Máximo común divisor

Sean f,g polinomios en $R[T]$, con $d := gr(f) \geq gr(g) =: e$. Se desea calcular el máximo común divisor $mcd(f,g)$ de f y g.

El algoritmo que se utilizará determina en primer lugar el grado de $mcd(f,g)$. Para ello, es necesario tener en cuenta que, si f no es un múltiplo constante de g, entonces se satisface la siguiente identidad ([74, Theorem 2.3]):

$$\begin{aligned} gr(mcd(f,g)) =: j = \min\{k \in \mathbb{N}; \exists r,s \in K[T] \\ gr(r) < e-k,\ gr(s) < d-k \text{ y } gr(rf+sg) = k\} \end{aligned} \tag{1.4}$$

Una vez hallado el grado j del polinomio $mcd(f,g)$, la condición (1.4) correspondiente a $k := j$ se utiliza también para calcular los coeficientes de los polinomios r y s que aparecen en (1.4) y los coeficientes de $mcd(f,g)$ a partir de éstos últimos.

El enunciado de (1.4) se puede traducir directamente en un sistema de $d+e-2k$ ecuaciones lineales, que provienen de igualar a cero los coeficientes correspondientes a las potencias $k+1,\ldots,d+e-k$ del polinomio resultante $rf+sg$ en (1.4) e igualar a 1 el coeficiente de grado k de $rf+sg$, considerando los coeficientes de r y s como indeterminadas. La matriz que resulta de tal sistema, $P_k(f,g)$, se conoce como la *k-ésima submatriz principal de Sylvester* de f y g.

Esta matriz se define en términos de la *matriz de Sylvester* $P_0(f,g)$ de f y g: esta matriz $P_0(f,g)$ tiene tamaño $(d+e)\times(d+e)$ y se define por:

$$P_0(f,g) := \left(\begin{array}{ccc|ccc} f_d & & & g_e & & \\ f_{d-1} & f_d & & g_{e-1} & g_e & \\ & f_{d-1} & & & g_{e-1} & \\ f_0 & \vdots & f_d & g_0 & \vdots & g_e \\ & f_0 & f_{d-1} & & g_0 & g_{e-1} \\ & & \vdots & & & \\ & & f_0 & & & g_0 \end{array}\right) \in R^{d+e\times d+e}$$

donde hay e columnas con coeficientes de f y d columnas con coeficientes de g. La *resultante* de f y g es el determinante de $P_0(f,g)$.

La matriz $P_k(f,g)$ se define ahora como la $(d+e-2k)\times(d+e-2k)$-submatriz de $P_0(f,g)$ que consiste de las primeras $e-k$ columnas de coeficientes de f, las primeras $d-k$ columnas de coeficientes de g y las primeras $d+e-2k$ filas de $P_0(f,g)$:

$$P_k(f,g) := \left(\begin{array}{ccc|ccc} f_d & & & g_e & & \\ f_{d-1} & f_d & & g_{e-1} & g_e & \\ \vdots & f_{d-1} & & \vdots & g_{e-1} & \\ f_{d-e+k+1} & \vdots & f_d & g_{e-d+k+1} & \vdots & g_e \\ \vdots & & \vdots & \vdots & & \vdots \\ & & & & & \\ f_{2k-e+1} & & f_k & g_{2j-d+1} & & g_k \end{array}\right)$$

(donde $f_i = 0$, $g_i = 0$ si $i < 0$).

Por lo tanto, se debe determinar cual es el menor índice k tal que $detP_k(f,g) \neq 0$. Posteriormente, si $j = gr(mcd(f,g))$, se resuelve un sistema con matriz $P_j(f,g)$. Dado que $det(P_j)(f,g) \neq 0$, este sistema puede resolverse por la regla de Cramer.

A fin de evitar divisiones por $det(P_j)(f,g)$, si se multiplica ambos lados del sistema por la matriz adjunta de $P_j(f,g)$, $Adj(P_j(f,g))$, se tiene:

$$det(P_j(f,g))(r_{e-j-1},\cdots,r_0,s_{d-j-1},\cdots,s_0)^t = Adj(P_j(f,g))(0,\cdots,0,1)^t$$

Obsérvese que el lado derecho de la última ecuación es la última columna de la matriz $Adj(P_j(f,g))$. De esta manera se calcula un múltiplo $det(P_j(f,g))$ de los coeficientes de $r(T)$ y $s(T)$ en una construcción algorítmica adecuada.

El algoritmo puede resumirse de la siguiente manera:

Procedimiento 2 *Un algoritmo para el cálculo del máximo común divisor.*

- *Calcular* $det(P_i(f,g))$ *en paralelo para* $i = 1,\ldots,\lceil\frac{d+e}{2}\rceil$.
- *Calcular* $j := min\{i; det(P_i(f,g)) \neq 0\}$.

- *Calcular los coeficientes del vector*

$$det(P_j(f,g))(r_{e-i-1}^{(i)},\cdots,r_0^{(i)},s_{d-i-1}^{(i)},\cdots,s_0^{(i)})^t$$

como las coordenadas de la última columna de la matriz $Adj(P_i(f,g))$.

- *Calcular (en paralelo) los coeficientes de los polinomios* $det(P_j(f,g))r\cdot f$ *y* $det(P_j(f,g))s\cdot g$.

- *Calcular* $det(P_j(f,g))\cdot mcd(f,g) = det(P_j(f,g))(r\cdot f + s\cdot g)$.

Durante su ejecución, el algoritmo calcula $O(d+e)$ determinantes organizados en dos niveles de profundidad – las subresultantes principales y la última columna de la matriz $Adj(P_i(f,g))$ – de matrices cuyo tamaño máximo es $(d+e)\times(d+e)$ y realiza $O(d)$ comparaciones (en profundidad $O(\log d)$) y $O(d)$ productos en paralelo. Los determinantes se calculan con los métodos de la sección 7 y las comparaciones con las ideas de la sección 1.2.4. En conclusión se tiene el siguiente resultado:

Lema 15 *Existe un circuito aritmético sin divisiones que calcula un múltiplo escalar de* $mcd(f,g))$ *realizando* $O(d^{O(1)})$ *operaciones aritméticas en profundidad no escalar* $O(\log d)$.

Suponiendo ahora que los coeficientes de f y g son polinomios en son polinomios en $\mathbb{Z}[X_1,\ldots,X_n]$ de grado acotado por D, cuyos coeficientes tienen talla binaria acotada por h, combinando el esquema del procedimiento 2 con los resultados de los lemas 11 y 12 se tiene el siguiente resultado:

Lema 16 *Existe una familia uniforme de circuitos booleanos de talla* $O(d^{O(n)}D^{O(n)}h^2)$ *y profundidad* $O\big(n\log d\log(Dhd)\big)$ *que calcula un múltiplo* $det(P_j(f,g))\in\mathbb{Z}[X_1,\ldots,X_n]$ *del máximo común divisor* $mcd(f,g))$.

Otro caso de interés es el de máximo común divisor de varios polinomios. Sean $F_1,\ldots,F_N$ polinomios en $\mathbb{Z}[X_1,\ldots,X_n][T]$ de grado (total) acotado por d y talla binaria menor o igual que h. El problema es calcular un múltiplo uniforme (en $\mathbb{Z}[X_1,\ldots,X_n][T]$) del máximo común divisor de $F_1,\ldots,F_N$, considerados como polinomios en $\mathbb{Q}(X_1,\ldots,X_n)[T]$.

Una posible manera de calcular este máximo común divisor es iterar el procedimiento 2, organizando el proceso en un árbol binario balanceado. En

lugar de aplicar esta idea, se utilizará una alternativa con la cual se obtienen mejores resultados. Esta se basa en la observación que el máximo común divisor F de $F_1, \ldots, F_N$ es el polinomio de $\mathbb{Q}(X_1, \ldots, X_n)[T]$ mónico en T de grado mínimo que se puede expresar en la forma:

$$F = \sum_{k=1}^{N} H_i F_i \tag{1.5}$$

donde $H_1, \ldots, H_N$ son polinomios en $\mathbb{Q}(X_1, \ldots, X_n)[T]$ de grado en T acotado por $(d-1)N$ y grado en $X_1, \ldots, X_n$ acotado por $d^2(N+1)$.

Con ideas similares a las del lema 15, a partir de la ecuación (1.5) se plantean $d+1$ sistemas de ecuaciones lineales (que corresponden a la condición $gr_T\big(mcd(F_1, \ldots, F_N)\big) = k$ para $k = 0, \ldots, d$) cuyas matrices tienen tamaño $(dN)^{O(n)} \times (dN)^{O(n)}$ y talla binaria acotada por h. De los resultados del lema 10 se deduce entonces el siguiente resultado:

Lema 17 *Existe una familia uniforme de circuitos booleanos que calcula un múltiplo uniforme en $\mathbb{Z}[X_1, \ldots, X_n][T]$ del máximo común divisor de $F_1, \ldots, F_N$ en $\mathbb{Q}(X_1, \ldots, X_n)[T]$ con talla $(dN)^{O(n)}h^2$ y profundidad $O\big(n^2 \log(dN) \log(dNh)\big)$.*

1.3.3 Representación separable

Sea $f = f_d T^d + \cdots + f_0$ un polinomio de $R[T]$. El problema ahora es hallar una *representación separable* de f, es decir, un polinomio $g \in K[T]$ que tiene los mismos ceros que f y es libre de cuadrados.

Dado que K es de característica cero, se observa que el polinomio $g = \frac{f}{mcd(f,f')}$ verifica las propiedades requeridas, donde f' denota el polinomio derivado de f respecto de T. Obsérvese que los coeficientes del polinomio f' se calculan inmediatamente a partir de los coeficientes de f.

Como antes, no se calcula exactamente la representación separable de f sino un múltiplo en $R[T]$ de la misma, a fin de evitar divisiones por elementos de R. Combinando los lemas 15 y 13, se deduce el siguiente resultado:

Lema 18 *Existe un circuito aritmético de talla $d^{O(1)}$ y profundidad no escalar $O(\log d)$ que calcula un múltiplo escalar de la representación separable de f.*

Si los coeficientes de f son polinomios en son polinomios en $\mathbb{Z}[X_1, \ldots, X_n]$ de grado acotado por D, cuyos coeficientes tienen talla binaria acotada por h, se deduce el siguiente resultado como una consecuencia inmediata de los lemas 16 y 14:

Lema 19 *Existe una familia uniforme de circuitos booleanos de talla* $O(d^{O(n)}D^{O(n)}h^2)$ *y profundidad* $O\big(n \log d \log(Dhd)\big)$ *que calcula la representación separable de* f *salvo un múltiplo uniforme en* $\mathbb{Z}[X_1, \ldots, X_n]$.

1.4 Consecuencias para los problemas de eliminación

En esta sección se mostrarán algoritmos que resuelven algunos problemas algorítmicos teoría de eliminación geométrica. Todos los algoritmos requieren recursos de espacio de memoria razonables.

Para comenzar, se fijarán algunas notaciones que se mantendrán durante el resto de la sección:
sean $X_1, \ldots, X_n$ indeterminadas sobre $\mathbb{Q}$. Se considerarán polinomios $F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$ (siendo $n \geq 2$) donde el grado total $gr(F_j)$ para $1 \leq j \leq s$ queda acotado por un entero $d \geq 3$. Se supone que todos los coeficientes de los polinomios F_i tienen talla binaria acotada por h. Se denotará por $(F_1, \ldots, F_s)$ el ideal generado por $F_1, \ldots, F_s$ en $\mathbb{Q}[X_1, \ldots, X_n]$, es decir,

$$(F_1, \ldots, F_s) := \{F \in \mathbb{Q}[X_1, \ldots, X_n];$$

$$\exists P_1, \ldots, P_s \in \mathbb{Q}[X_1, \ldots, X_n] \text{ tales que } F = P_1F_1 + \cdots + P_sF_s\}$$

Además, se notará por V la variedad algebraica de $\mathbf{C}^n$ definida por $F_1, \ldots, F_s$:

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

1.4.1 El problema de la consistencia y la representación

Como ejemplo del método general a aplicar, se considera en primer lugar un problema clásico: el problema de la consistencia de un sistema de ecuaciones polinomiales.

Este problema consiste en decidir si un sistema de ecuaciones polinomiales definido por polinomios $F_1, \ldots, F_s$ en $\mathbb{Z}[X_1, \ldots, X_n]$ posee soluciones comunes en $\mathbf{C}^n$. Como ha sido señalado en la introducción, el teorema de los ceros de Hilbert (el Hilbert Nullstellensatz) demuestra que una respuesta negativa para el problema de la consistencia es equivalente a la *trivialidad* del ideal generado por $F_1, \ldots, F_s$ en $\mathbf{C}[X_1, \ldots, X_n]$. Esta cuestión es a su vez equivalente a la trivialidad del ideal generado por $F_1, \ldots, F_s$ en $\mathbb{Q}[X_1, \ldots, X_n]$, lo cual se verifica si y sólo si $1 \in (F_1, \ldots, F_s)$.

Es común considerar ambos problemas en conjunto: el de la consistencia y la representación de la unidad en el ideal, que se pueden enunciar de la siguiente manera:

Decidir si $V = \emptyset$ y en tal caso, hallar $P_1, \ldots, P_s \in \mathbb{Q}[X_1, .., X_n]$ tales que se satisface la identidad $1 = P_1F_1 + \cdots + P_sF_s$.

La herramienta esencial que se aplicará en la resolución de estos problemas es una versión simplemente exponencial del Nullstellensatz afín en característica 0 demostrada en [34] y sus generalizaciones a cuerpos arbitrarios contenidas en [38], [39], [111] (ver también [15], [16]):

Teorema *El ideal $(F_1, \ldots, F_s)$ es trivial si y sólo si existen polinomios $P_1, \ldots, P_s$ en $\mathbb{Q}[X_1, \ldots, X_n]$ que satisfacen las condiciones*

$$1 = P_1F_1 + \cdots + F_s \qquad \text{y} \qquad \max\{gr(P_jF_j); 1 \leq j \leq s\} \leq d^n \qquad (1.6)$$

Esto transforma la cuestión en un problema de álgebra lineal: dado que se tiene una cota para los grados de los polinomios $P_1, \ldots, P_s$, la condición (1.6) puede reescribirse como un sistema de ecuaciones lineales cuyas indeterminadas son los coeficientes de los polinomios P_i. El sistema se obtiene como resultado de igualar los coeficientes que aparecen en (1.6) monomio por monomio.

Dado que hay $\binom{d^n + n}{n} = O(d^{n^2})$ monomios distintos de grado menor o igual que d^n, se tienen $O(d^{n^2})$ ecuaciones a lo sumo. El número de indeterminadas, $O(sd^{n^2})$, es igual al número de posibles coeficientes de cada polinomio P_i $(1 \leq i \leq s)$. En consecuencia, se obtiene un sistema de ecuaciones lineales de tamaño $O(d^{n^2} \times sd^{n^2})$ cuyos coeficientes se obtienen directamente a partir de los coeficientes de los polinomios $F_1, \ldots, F_s$ y por lo tanto tienen a lo sumo h bits.

Para la construcción uniforme de la matriz del sistema, será necesario fijar un orden monomial de fácil manipulación. Un posible orden es el graduado con orden lexicográfico dado por $X_1 > \cdots > X_n$ (ver [51]). De hecho, la decodificación en ese orden puede hacerse en espacio determinístico de tipo $O(\log(nd))$.

Aplicando los resultados de la sección 1.2.5 a este caso se obtiene una familia de circuitos booleanos de talla $(hsd^{n^2})^{O(1)}$ y profundidad $O(n^4 \log^2(hsd))$, uniforme en espacio de tipo $O(\log(nsdh))$ que decide si el sistema de ecuaciones polinomiales $\{F_1 = 0, \ldots, F_s = 0\}$ es compatible y en tal caso, calcula una solución particular del mismo.

A este punto se aplica la demostración del teorema 1 a fin de evaluar el circuito que ha sido construído. En conclusión, se tiene el siguiente resultado:

Teorema 2 *El problema de la consistencia y de la representación de la unidad puede resolver por medio de una máquina de Turing determinística en espacio* $O(n^4 \log^2(hsd))$.

1.4.2 El problema de la pertenencia y la representación en ideales intersección completa

El problema a considerar es el siguiente: supóngase que $s \leq n$ y $F_1, \ldots, F_s$ forma una sucesión regular de $\mathbb{Q}[X_1, \ldots, X_n]$, es decir, se cumplen las condiciones (cf. [124]):

- Para todo $i \in \{1, \ldots, s\}$, el polinomio F_i no es divisor de cero en el anillo $\mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_{i-1})$.
- El ideal $(F_1, \ldots, F_s)$ no es el ideal trivial de $\mathbb{Q}[X_1, \ldots, X_n]$.

Sea además F un polinomio dado con coeficientes enteros de talla binaria acotada por h. Se quiere decidir si F pertenece al ideal generado por $F_1, \ldots, F_s$ en $\mathbb{Q}[X_1, \ldots, X_n]$ y en tal caso, hallar polinomios $P_1, \ldots, P_s \in \mathbb{Q}[X_1, \ldots, X_n]$ tales que se tiene la siguiente representación de F en el ideal generado por $F_1, \ldots, F_s$:

$$F = P_1 F_1 + \cdots + P_s F_s$$

Como ha sido observado en la introducción, el problema de la pertenencia a ideales arbitrarios requiere espacio exponencial. Sin embargo, las

características particulares del caso en que el ideal es intersección completa permiten un tratamiento efectivo.

Aquí nuevamente los Nullstellensätzse afines efectivos son el punto clave:

Teorema *Supóngase que los polinomios $F_1, \ldots, F_s$ forma una sucesión regular en $\mathbb{Q}[X_1, \ldots, X_n]$. Entonces, F pertenece a $(F_1, \ldots, F_s)$ si y sólo si existen polinomios $P_1, \ldots, P_s \in \mathbb{Q}[X_1, \ldots, X_n]$ tales que*

$$F = \sum_j P_j F_j \qquad \text{y} \qquad \max\{gr(P_j F_j); 1 \leq j \leq s\} \leq gr(F) + d^s \leq gr(F) + d^n$$

Ver [56] por una demostración ([15], [164], [41], [5] contienen versiones algo diferentes de un teorema de cotas de grado para la representación en ideales intersección completa y generalizaciones del mismo).

Se procede entonces de forma similar a la de la sección 1.4.1: se halla un sistema de ecuaciones lineales de tamaño $O(d^{n^2} \times sd^{n^2})$ y coeficientes enteros de talla binaria acotada por h, cuyas soluciones corresponden a los coeficientes de los polinomios $P_1, \ldots, P_s$ requeridos. En consecuencia, se deduce el siguiente teorema:

Teorema 3 *El problema de la pertenencia y la representación en ideales intersección completa puede resolverse por medio de una máquina de Turing determinística en espacio $O(n^4 \log^2(hsd))$.*

1.4.3 El problema de la pertenencia al radical

El ideal radical de $(F_1, \ldots, F_s)$, $\sqrt{(F_1, \ldots, F_s)}$, se define como el ideal de $\mathbb{Q}[X_1, \ldots, X_n]$ que consiste de todos aquellos polinomios que elevados a alguna potencia pertenecen a $(F_1, \ldots, F_s)$, es decir:

$$\sqrt{(F_1, \ldots, F_s)} := \{F \in \mathbb{Q}[X_1, \ldots, X_n]; \exists N \in \mathbb{N} \text{ tal que } F^N \in (F_1, \ldots, F_s)\}$$

El teorema de los ceros de Hilbert fuerte asegura que un polinomio F pertenece al ideal radical de $(F_1, \ldots, F_s)$ si y sólo si F se anula sobre la variedad $V \subseteq \mathbf{C}^n$ definida por $F_1, \ldots, F_s$.

El problema de la pertenencia al radical y la representación consiste en decidir cuando un polinomio F dado se anula sobre V y en tal caso, hallar un número natural $N \in \mathbb{N}$ y polinomios $P_1, \ldots, P_s \in \mathbb{Q}[X_1, \ldots, X_n]$ tales que $F^N = P_1 F_1 + \cdots + P_s F_s$.

La siguiente observación, que se deduce inmediatamente a partir del Nullstellensatz efectivo, permite reducir el problema a la resolución de un sistema de ecuaciones lineales de tamaño simplemente exponencial:

Observación ([56], Remark 1.6) *F se anula sobre V si y sólo si existe una representación $F^{d^n} = P_1F_1 + \cdots + P_sF_s$ con los polinomios $P_1, \ldots, P_s \in \mathbb{Z}[X_1, \ldots, X_n]$ y $\max\{gr(P_jF_j); 1 \leq j \leq s\} \leq d^n(gr(F)+1)$*

En consecuencia se tiene un sistema de ecuaciones lineales de tamaño $O(d^{n^2}(\deg(F)+1)^n)$, cuyas entradas se obtienen directamente a partir de los polinomios $F_1, \ldots, F_s$ y F^{d^n}.

Los coeficientes de F^{d^n} se pueden obtener a partir de los de F en forma uniforme mediante productos matriciales con talla $(d^n gr(F))^{O(n)}h^2$ y profundidad $O(n^2 \log(hd))$, pudiéndose estimar su talla binaria de estos coeficientes por $O(d^{3n}h \log gr(F))$.

Luego, aplicando los algoritmos y los resultados de la sección 1.2.5, se demuestra:

Teorema 4 *Existe una máquina de Turing determinística que resuelve el problema de la pertenencia al radical y la representación en espacio $O\left(n^4 \log^2(dh\, gr(F))\right)$*

1.4.4 El problema de eliminación cero–dimensional

El problema del estudio de variedades de dimensión cero ha sido extensamente estudiado en teoría de eliminación. Una forma de resolución simbólica de esta cuestión se basa en el siguiente problema, que se denomina el problema de la eliminación cero–dimensional (cf. [90]):

Siendo V una variedad cero–dimensional y dada una forma lineal $\ell \in \mathbb{Z}[X_1, \ldots, X_n]$, hallar un polinomio univariado no nulo $Q \in \mathbb{Z}[\ell]$ tal que $Q(\ell)$ se anula sobre V.

A fin de resolver este problema se tiene el siguiente resultado, que se deduce a partir de [56, Proposition 1.12]:

Lema *Existe un polinomio no nulo $F \in \mathbb{Q}[\ell]$ y polinomios $P_1, \ldots, P_s \in \mathbb{Q}[X_1, \ldots, X_n]$ tales que*

$$F = P_1F_1 + \ldots + P_sF_s \text{ y } max\{gr(P_iF_i; 1 \leq i \leq s\} \leq d^n(d^n+1) \qquad (1.7)$$

La condición (1.7) se traduce en un sistema de ecuaciones lineales de tamaño $O(d^{2n} \times sd^{2n})$ y talla binaria $d^{O(n)}h$. Por lo tanto, aplicando los algoritmos desarrollados en la sección 1.2 se deduce el siguiente resultado:

Teorema 5 *El problema de eliminación cero-dimensional puede ser resuelto mediante una máquina de Turing determinística en espacio* $O(n^4 \log^2(hsd))$.

Es de particular interés la situación en la cual la variedad V es localmente intersección completa, es decir, cuando la variedad cero-dimensional V se describe como el conjunto de ceros comunes de n polinomios $F_1, \ldots, F_n$ en $\mathbb{Z}[X_1, \ldots, X_n]$. En este caso, por medio de un esquema mas refinado es posible reducir notablemente las cotas de complejidad para el problema de la eliminación cero-dimensional obtenidas en el teorema 5.

El primer paso consiste en producir una deformación homotópica del sistema, a fin de de reducir la cuestión al caso proyectivo cero-dimensional. Para esto, se introducen nuevas variables X_0 y ε, y se definen los polinomios:

$$G_i := X_0{}^h F_i + \varepsilon X_i^{1+gr(F_i)}$$

donde ${}^hF_i$ denota el polinomio homogeneizado de F_i con variable de homogeinización X_0. Considerados como polinomios en $\overline{\mathbb{Z}[\varepsilon]}[X_0, \ldots, X_n]$, $G_1, \ldots, G_n$ definen una variedad cero-dimensional en $\mathbb{P}^n(\overline{\mathbb{Q}(\varepsilon)})$ ([80], Lemme 3.3.3). La representación densa de $G_1, \ldots, G_n$ se obtiene inmediatamente a partir de la de $F_1, \ldots, F_n$.

Se aplican ahora argumentos sobre la regularidad de la función de Hilbert del anillo graduado

$$A := \overline{\mathbb{Q}(\varepsilon)}[X_0, \ldots, X_n]/(G_1, \ldots, G_n) = A_0 + A_1 + \cdots + A_k + \cdots$$

Se tienen los dos siguientes hechos:

- A_N y A_{N+1} son $\overline{\mathbb{Q}(\varepsilon)}$-espacios vectoriales isomorfos de dimensión finita $D \leq (d+1)^n$, y
- dado que el ideal $(G_1, \ldots, G_n)$ no tiene ceros en el hiperplano $X_0 = 0$, la homotecia $\eta_{X_0} : A_N \longrightarrow A_{N+1}$ es un isomorfismo.

Se considera entonces el endomorfismo:

$$\phi := \eta_{X_0}^{-1} \eta_\ell : A_N \longrightarrow A_N$$

Por el Teorema de Cayley–Hamilton, el polinomio característico $P(T)$ de ϕ verifica $P(\phi) \equiv 0$, por lo que $\eta_{X_0}^D P(\phi)$ también. Como X_0 no es divisor de cero en A, el polinomio no nulo $\tilde{P}(X_0, Z) := X_0^D P\left(\frac{Z}{X_0}\right)$ verifica que $\tilde{P}(X_0, \ell)$ se anula en A.

A fin de evitar divisiones en el cálculo de $\tilde{P}(X_0, Z)$, siguiendo [114] se calcula un múltiplo $\Delta(\varepsilon, X_0, Z) = \sum_{j=1}^{D} p_j(\varepsilon) Z^j X_0^{D-j}$ en $\mathbb{Z}[\varepsilon][X_0, Z]$ del mismo. Para calcular este polinomio, es necesario manipular todos los monomios en $X_0, \ldots, X_n$ de grado menor o igual que $nd+2$ a fin de producir bases monomiales adecuadas para el cálculo de las matrices de las homotecias η_{X_0} y η_ℓ. Esta manipulación se realiza operando con matrices de tamaño $(nd)^{O(n)}$, en lugar de las matrices de tamaño d^{n^2} que hasta ahora consideradas.

Si se divide el polinomio $\Delta(\varepsilon, X_0, Z)$ por la mayor potencia posible de ε, se obtiene un polinomio $\Delta_1(\varepsilon, X_0, Z)$, el cual verifica que $Q(Z) := \Delta_1(0, 1, Z)$ es el polinomio buscado ([80], Proposition 3.3.4).

En conclusión, se tiene el siguiente resultado:

Teorema 6 *El problema de eliminación cero-dimensional para ideales localmente intersección completa puede ser resuelto mediante una máquina de Turing determinística en espacio* $O(n^2 \log^2(hsd))$.

1.4.5 El problema general de eliminación

Varios problemas geométricos y algebraicos interesantes pueden formularse por medio de fórmulas de primer orden sobre $\mathbf{C}$ con cuantificadores existenciales y universales.

A fin de definir que se entiende por una fórmula de primer orden sobre $\mathbf{C}$, se considera en primer lugar el lenguaje de primer orden $\mathcal{L}$ que contiene los siguientes símbolos no lógicos:

- para cada $a \in \mathbb{Q}$, una constante que se denomina también "a",
- los símbolos funcionales $+, -, \cdot$, y
- el símbolo relacional $=$.

Se consideran las variables de $\mathcal{L}$ como indeterminadas $X_1, \ldots, X_n$ sobre $\mathbf{C}$, y se piensan los términos del lenguaje $\mathcal{L}$ representados por polinomios multivariados con coeficientes en $\mathbb{Q}$ (en representación densa).

Por lo tanto, un término típico tiene la forma $F \in \mathbb{Q}[X_1, \ldots, X_n]$, y una fórmula atómica típica tiene la forma $F = 0$. La negación de esta fórmula se notará por $F \neq 0$.

Una *fórmula de primer orden sobre* $\mathbf{C}$ se construye a partir de fórmulas atómicas usando los conectivos lógicos $\vee, \wedge, \neg$ y los cuantificadores de primer orden $\exists, \forall$ variando sobre los elementos de $\mathbf{C}$. Por lo tanto, cada fórmula $\Phi \in \mathcal{L}$ se construye a partir de fórmulas atómicas que involucran polinomios $F_1, \ldots, F_s \in \mathbb{Q}[X_1, \ldots, X_n]$.

Es sabido que toda fórmula Φ de este tipo es equivalente a una fórmula $\tilde{\Phi} \in \mathcal{L}$ libre de cuantificadores. El proceso de hallar la fórmula $\tilde{\Phi} \in \mathcal{L}$ se denomina *eliminación de cuantificadores*, y generalmente se realiza en varias etapas, en cada una de las cuales se elimina el *bloque* de cuantificadores del mismo tipo "mas a la derecha".

Dado que que el cuantificador $\forall$ puede expresarse en la forma $\neg\exists\neg$, se puede asumir que el bloque de cuantificadores a eliminar es existencial, y esto motiva el siguiente problema, conocido como el *problema general de eliminación*:

dada una fórmula $\Phi \in \mathcal{L}$ *de la forma*

$$(\exists X_{m+1}) \cdots (\exists X_n) \Psi(X_1, \ldots, X_n)$$

donde $\Psi(X_1, \ldots, X_n)$ *es una fórmula libre de cuantificadores, hallar una fórmula equivalente a* Φ *libre de cuantificadores.*

Este problema también puede describirse en forma geométrica: notando por V el subconjunto (localmente abierto en la topología de Zariski) de $\mathbf{C}^n$ formado por aquellos elementos que satisfacen la fórmula $\Psi(X_1, \ldots, X_n)$, la fórmula $\Phi(X_1, \ldots, X_n)$ define la *proyección* $\pi(V)$ de V según el morfismo $\pi : \mathbf{C}^n \to \mathbf{C}^m$ definido por $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_m)$.

Todo conjunto expresable por polinomios $F_1, \ldots, F_s$ puede escribirse como una unión de conjuntos de tipo $\{sg(F_1) = \epsilon_1, \ldots, sg(F_s) = \epsilon_s\}$ donde $(\epsilon_1, \ldots, \epsilon_s) \in \{0, 1\}^s$ con la convención que $sg(F_i) = 0$ representa la condición $F_i = 0$ y $sg(F_i) = 1$ equivale a $F_i \neq 0$ (ver [88], [66], [67]). Estos conjuntos se denominan $(F_1, \ldots, F_s)$-*celdas*.

El procedimiento comienza chequeando la consistencia de todas las posibles $(F_1, \ldots, F_s)$-celdas en paralelo. Si bien a primera vista la cantidad total de posibles $(F_1, \ldots, F_s)$-celdas puede estimarse por 2^s, según se demuestra

en [88] esta estimación puede mejorarse a $(d+1)^n$. Siguiendo el esquema descripto en [67] es posible reducir la cantidad de test de consistencia a realizar a $2s(nd)^{2n}$.

Toda $(F_1,\ldots,F_s)$-celda puede expresarse en la forma

$$\left\{ \bigwedge_{j\in\mathcal{M}} F_j = 0 \wedge \left(\prod_{j\notin\mathcal{M}} F_j \right) \neq 0 \right\}$$

donde $\mathcal{M} \subseteq \{1,\ldots,s\}$. Este conjunto es no vacío si y sólo si, siendo Y una nueva indeterminada el siguiente sistema sobre $\mathbf{C}^{n+1}$:

$$\left\{ \bigwedge_{j\in\mathcal{M}} F_j = 0 \wedge 1 - Y\left(\prod_{j\notin\mathcal{M}} F_j \right) = 0 \right\}$$

es compatible. Esta última condición puede chequearse, aplicando los argumentos de la sección 1.4.1, por medio de cálculos de rango de matrices enteras de tamaño $O(d^{n^2})$ y talla binaria $O(s^2hn\log d)$.

Posteriormente la proyección $\pi(V)$ se describe como la unión de la proyección de las $(F_1,\ldots,F_s)$-celdas consistentes. Siendo $\mathcal{M} \subseteq \{1,\ldots,s\}$, considérese la $(F_1,\ldots,F_s)$-celda C definida por:

$$C := \left\{ \bigwedge_{j\in\mathcal{M}} F_j = 0 \wedge \left(\prod_{j\notin\mathcal{M}} F_j \right) \neq 0 \right\}$$

Su proyección $\pi(C)$ puede ser descripta por la fórmula:

$$\pi(C) = (\exists X_{m+1})\cdots(\exists X_n)\left\{ \bigwedge_{j\in\mathcal{M}} F_j = 0 \wedge \left(\prod_{j\notin\mathcal{M}} F_j \right) \neq 0 \right\}$$

A fin de expresar $\pi(C)$ por medio de una fórmula sin cuantificadores existenciales, se considera la cuestión sobre $\mathbf{C}[X_1,\ldots,X_m]$, lo cual transforma el problema, aplicando la estrategia que se utilizó para chequear la consistencia de $(F_1,\ldots,F_s)$-celdas, en un problema de consistencia sobre $\mathbf{C}[X_1,\ldots,X_m]$ en el sentido de la sección 1.4.1 (ver Theorem 2 en [67] o Théorème 3 en [66]).

El problema de la consistencia se reduce a chequear igualdad del rango de dos matrices, para lo cual se utilizan las técnicas descriptas al final de la subsubsección 1.2.4. Para este fin se introducen nuevas variables Z_1, Z_2 y se transforman dichas matrices en dos nuevas matrices cuadradas, cuyos

polinomios característicos se calculan. De la construcción resulta que la multiplicidad de la raíz 0 de esos polinomios característicos indica el rango de las matrices originales.

Entonces se analiza cual es el primer coeficiente no nulo de ambos polinomios característicos. Sean $G_0, \ldots, G_t$ y $H_0, \ldots, H_t$ los polinomios en $\mathbb{Z}[X_1, \ldots, X_m, Z_1, Z_2]$ que aparecen como coeficientes de estos polinomios característicos. Las ecuaciones necesarias para expresar la igualdad de los rangos de las matrices consideradas se pueden describir de la siguiente manera:

$$\bigvee_{k=0}^{t} \left(G_0 = 0 \wedge \ldots \wedge G_{k-1} = 0 \wedge G_k \neq 0 \wedge H_0 = 0 \wedge \ldots \wedge H_{k-1} = 0 \wedge H_k \neq 0\right) \tag{1.8}$$

Considerando a $G_0, \ldots, G_t$ y $H_0, \ldots, H_t$ como polinomios en $\mathbb{Z}[X_1, \ldots, X_m][Z_1, Z_2]$, la condición (1.8) puede reexpresarse en términos de los coeficientes en $\mathbb{Z}[X_1, \ldots, X_m]$ de estos polinomios. Estas ecuaciones son la fórmula libre de cuantificadores buscada.

El cálculo de los polinomios característicos se realiza según la estrategia del lema 12 deduciéndose de éste la existencia de una familia uniforme de circuitos booleanos de de talla $s^{O(1)}d^{O(n^3)}h^2$ y profundidad $O(n^5 \log^2(sdh))$ que resuelve el problema. De aquí se puede concluir el siguiente:

Teorema 7 *El problema general de eliminación puede resolverse por medio de una máquina de Turing determinística en espacio* $O(n^5 \log^2(sdh))$.

1.4.6 Cálculo de la dimensión y normalización de Noether

Un técnica esencial de preprocesamiento de sistemas de ecuaciones polinomiales es la normalización de Noether. Sea $r := dim(V)$. Se dice que las variables $X_1, \ldots, X_n$ están en *posición de Noether* con respecto a V si para cada $r < i \leq n$ existe un polinomio de $\mathbb{Q}[X_1, \ldots, X_r, X_i]$ que es mónico en X_i y se anula sobre V (en este caso se dice que $\{X_{r+1}, \ldots, X_n\}$ son enteras respecto de $X_1, \ldots, X_r$). Dado que siempre es posible extraer r variables del conjunto $\{X_1, \ldots, X_n\}$ que son *libres* con respecto a V (es decir, ningún polinomio en tales variables se anula sobre V), se deduce que las variables $X_1, \ldots, X_r$ son libres con respecto a V.

La *normalización de Noether* consiste en un cambio lineal de coordenadas (que será descripto por medio de una matriz triangular superior $Q \in \mathcal{M}_n(\mathbb{Z})$, salvo un reordenamiento de las variables) de la forma:

$$\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = Q \cdot \begin{pmatrix} X'_1 \\ \vdots \\ X'_n \end{pmatrix}$$

donde las nuevas variables $X'_1, \ldots, X'_n$ satisfacen las siguientes condiciones:

1. $\mathbb{Q}[X'_1, \ldots, X'_r] \cap (F_1, \ldots, F_s) = \{0\}$.
2. Para cada $j \in \{r+1, \ldots, n\}$ existe un polinomio $G_j \in \mathbb{Q}[X'_1, \ldots, X'_r, X'_j]$ mónico en X'_j, tal que $G_j \in (F_1, \ldots, F_s)$.

Obsérvese que el número máximo de variables libres del conjunto $\{X_1, \ldots, X_n\}$ con respecto a V es precisamente la dimensión de V, por lo que un algoritmo que calcula una normalización de Noether calcula necesariamente la dimensión de V.

El primer paso del algoritmo es calcular un sistema de variables independientes con respecto a V. En tal sentido, se tiene el siguiente resultado:

Proposición 1 ([56], Proposition 1.7) *Sea* $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$. *Entonces,* $(F_1, \ldots, F_s) \cap \mathbb{Q}[X_{i_1}, \ldots, X_{i_k}] \neq \{0\}$ *si y sólo si existe un polinomio* $F \in \mathbb{Q}[X_{i_1}, \ldots, X_{i_k}]$ *no nulo y polinomios* $P_1, \ldots, P_s \in \mathbb{Q}[X_1, \ldots, X_n]$ *tales que*

$$F = P_1F_1 + \ldots + P_sF_s \text{ y } max\{gr(P_iF_i; 1 \leq i \leq s\} \leq d^n(d^n + 1)$$

Esta condición es equivalente a la resolubilidad de cierto sistema de ecuaciones lineales de tamaño $O(d^{2n} \times sd^{2n})$ y talla binaria h. Realizando el test para los 2^n subconjuntos de $\{1, \ldots, n\}$, se halla un sistema independiente de variables $\{X_1, \ldots, X_r\}$ maximal (y en particular, la dimensión de V).

Posteriormente, es preciso determinar cuales de las variables $\{X_{r+1}, \ldots, X_n\}$ son enteras con respecto a $\{X_1, \ldots, X_r\}$. Se aplica entonces el siguiente:

Proposición 2 ([56], Proposition 1.11) *Sea* $\{X_1, \ldots, X_r\}$ *un sistema de variables independientes para* $(F_1, \ldots, F_s)$ *y* ℓ *una forma lineal en* $\mathbb{Q}[X_1, \ldots, X_n]$

que es entera respecto de $\{X_1, \ldots, X_r\}$. *Entonces existe un polinomio* $G \in \mathbb{Q}[X_1, \ldots, X_r, T]$ *mónico en* T *de grado acotado por* $d^n(d^n+1)$ *y polinomios* $P_1, \ldots, P_s \in \mathbb{Q}[X_1, \ldots, X_n]$ *tales que*

$$G(X_1, \ldots, X_r, \ell) = P_1F_1 + \ldots + P_sF_s \text{ y } max\{gr(P_iF_i; 1 \leq i \leq s\} \leq d^n(d^n+1)$$

Se chequea entonces la compatibilidad de $n-r$ sistemas de ecuaciones lineales de tamaño $O(d^{2n} \times sd^{2n})$ y talla binaria h (uno por cada variables en $\{X_{r+1}, \ldots, X_n\}$.

Sean $X_{r+1}, \ldots, X_p$ las variables enteras. Un procedimiento recursivo sobre las restantes variables calcula el cambio de variables adecuado. Para esto es necesario el siguiente resultado:

Proposición 3 ([56], Proposition 1.12) *Sea* $\{X_1, \ldots, X_r\}$ *un sistema de variables independientes para* $(F_1, \ldots, F_s)$ *y* ℓ *una forma lineal en* $\mathbb{Q}[X_1, \ldots, X_n]$. *Entonces existe un polinomio* $G \in \mathbb{Q}[X_1, \ldots, X_r, T]$ *no nulo de grado acotado por* $d^n(d^n+1)$ *y polinomios* $P_1, \ldots, P_s \in \mathbb{Q}[X_1, \ldots, X_n]$ *tales que*

$$G(X_1, \ldots, X_r, \ell) = P_1F_1 + \ldots + P_sF_s \text{ y } max\{gr(P_iF_i; 1 \leq i \leq s\} \leq d^n(d^n+1)$$

Tomando $\ell := X_{p+1}$, se hallará un cambio de variables

$$(X_1, \ldots, X_r, X_{p+1}) \longrightarrow (X'_1, \ldots, X'_r, X'_{p+1})$$

de modo tal que el polinomio que se obtiene a partir de G por este cambio de variables (que se notará también por G con un leve abuso de notación) resulte mónico con respecto a X'_{p+1}.

Sea G_1 el polinomio que consiste de los monomios de mayor grado de G (es decir, la componente homogénea de mayor grado de G) y $(\lambda_1, \ldots, \lambda_r) \in \mathbb{Z}^r$ tal que $G_1(\lambda_1, \ldots, \lambda_r, 1) \neq 0$. Se define entonces el cambio de variables:

$$\begin{cases} X_1 &= X'_1 + \lambda_1 X_{p+1} \\ & \\ X_r &= X'_r + \lambda_r X_{p+1} \\ X_{p+1} &= X'_{p+1} \end{cases}$$

Dado que $G_1(X'_1 + \lambda_1 X'_{p+1}, X'_r + \lambda_r X'_{p+1}, X'_{p+1})$ es mónico en X'_{p+1} (ya que el coeficiente correspondiente al monomio X'_{p+1} es $G_1(\lambda_1, \ldots, \lambda_r, 1)$), la

variable X'_{p+1} resulta entera respecto de $X'_1, \ldots, X'_r$. Además, como las variables $X_{r+1}, \ldots, X_p$ son enteras respecto de $X_1, \ldots, X_r, X_{p+1}$ (ya que lo son respecto de $X_1, \ldots, X_r$), y $X_1, \ldots, X_r, X_{p+1}$ son a su vez enteras respecto de $X'_1, \ldots, X'_r, X'_{p+1}$, propiedades estándar de extensiones enteras permiten deducir que $X_{r+1}, \ldots, X_{p+1}$ son enteras respecto de $X_1, \ldots, X_r$.

El problema es entonces hallar una r–upla $(\lambda_1, \ldots, \lambda_r) \in \mathbb{Z}^r$ tal que $G_1(\lambda_1, \ldots, \lambda_r, 1) \neq 0$. Dado que G_1 es un polinomio no nulo tal que $gr(G_1) \leq d^n(d^n+1)$, existe una r–upla $\lambda \in \{0, \ldots, d^n(d^n+1)\}^r$ que verifica la condicíon requerida. Se evalúa G_1 en todas las posibles r–uplas del conjunto $\{0, \ldots, d^n(d^r+1)\}^r$ y se halla una que no anula a G_1.

Mediante $n-p$ pasos recursivos como el descripto, se halla un cambio de variables

$$(X_1, \ldots, X_n) \longrightarrow (X_1, \ldots, X_p, Y_{p+1}, \ldots, Y_n)$$

que constituye una normalización de Noether para V. Utilizando los algoritmos desarrollados en la sección 1.2 y la demostración del teorema 1, se puede concluir:

Teorema 8 *El cálculo de la dimensión y la normalización de Noether puede realizarse por medio de una máquina de Turing determinística en espacio* $O(n^4 \log^2(hsd))$

1.4.7 Descomposición en componentes equidimensionales

Un problema fundamental para la descripción de la variedad V consiste en el cálculo de su descomposición equidimensional. Esto es, a partir de las ecuaciones polinomiales que describen la variedad V, para cada dimensión intermedia i $(0 \leq i \leq dim(V))$ se desea producir un conjunto finito de polinomios que define la unión de las componentes irreducibles de V de dimensión i.

Sea $r := dim(V)$. Para $i = 0, \ldots, r$ se notará por V_i la unión de las componentes irreducibles de V de dimensión i y por W_i la unión de las componentes irreducibles de dimensión estrictamente menor que i. El algoritmo que se aplicará consiste de a lo sumo r etapas recursivas, en cuya i–ésima etapa calcula un sistema de ecuaciones polinomiales que describe V_{r-i+1}.

Una característica fundamental del algoritmo es que los polinomios que se calculan como salida de cada etapa son *intrínsecos*, es decir, no dependen

del algoritmo. Este hecho permite estimar el grado y la talla binaria de estos polinomios en términos de la variedad V, a fin de evitar el crecimiento exponencial de estas cantidades que seguramente ocurriría como consecuencia del proceso recursivo.

Supóngase realizada la $(i-1)$-ésima etapa, en la cual se calcularon los siguientes ítems:

- Ecuaciones para V_{r-i+2}.
- Un sistema de a lo sumo $t := d^{cn^2}$ ecuaciones polinomiales $G_1, \ldots, G_t$ de grado acotado por $gr(V_r \cup \cdots \cup V_{r-i+2})$ y talla binaria no mayor que $d^{c'n}(\log s + h)$ donde c y c' son constantes universales adecuadas que no dependen de s, n, d y h, cuyos ceros comunes constituyen la variedad $V_r \cup \cdots \cup V_{r-i+2}$

La i-ésima etapa comienza calculando las ecuaciones que describen V_{r-i+1}. Esta variedad, supuesta no vacía, consiste de las componentes de mayor dimensión de la variedad $W_{r-i+2} = \overline{V \setminus (V_r \cup \cdots \cup V_{r-i+2})}$. Por lo tanto, es necesario manipular variedades algebraicas del tipo $\overline{V \setminus W}$, donde W está dada como el conjunto de ceros comunes de t' ecuaciones $H_1, \ldots, H_{t'}$ de grado acotado por d^n. Para tal fin, se define el siguiente $\mathbb{Q}$-espacio vectorial de dimensión finita:

$$E(V,W) := \Big\{ F \in \mathbb{Q}[X_1, \ldots, X_n];\ \forall\, j = 1, \ldots, t' \\ \exists\, P_1^{(j)}, \ldots, P_s^{(j)} \in \mathbb{Q}[X_1, \ldots, X_n] \text{ tales que} \\ F H_j^{d^n} = \sum_{k=1}^{s} P_k^{(j)} F_k \text{ y } gr(P_k^{(j)} F_k) \leq d^n(2d^n + 1) \Big\} \qquad (1.9)$$

Se tiene entonces el siguiente resultado:

Proposición 4 ([79], Proposition 4.2.5) *$\overline{V \setminus W}$ es el conjunto de ceros comunes en $\mathbb{C}^n$ de todos los polinomios en $E(V,W)$.*

Si bien es posible calcular con complejidad admisible un sistema de generadores de $E(V, V_r \cup \cdots \cup V_{r-i+2})$, este cálculo no se realizará ya que el operar directamente con tales polinomios haría crecer la complejidad en forma exponencial. En cambio, la información que provee la proposición 4 se utilizará en forma mas indirecta, como se verá posteriormente.

El problema es extraer las componentes de (mayor) dimensión $r-i+1$ de $W_{r-i+2} = \overline{V \setminus (V_r \cup \cdots \cup V_{r-i+2})}$. Para esto se calcula en primer lugar una posición de Noether de las variables con respecto a W_{r-i+2}. En lugar de tomar las ecuaciones que definen W_{r-i+2} para hallar esta posición de Noether, combinando las demostraciones de las proposiciones 1, 2 y 3 con la de la proposición 4 se prueba que la toda información necesaria para calcular una posición de Noether de las variables con respecto a W_{r-i+2} puede obtenerse a partir de sistemas del tipo de (1.9).

Cabe destacar que el cálculo de la posición de Noether implica el de la dimensión de W_{r-i+2}. De esta manera se determina también si V_{r-i+1} es vacía, en cuyo caso se da por finalizada la i–ésima etapa.

Asumiendo que V_{r-i+1} es no vacía, el procedimiento continúa con el cálculo de una *posición general* de las variables con respecto a W_{r-i+2}, lo cual significa que las variables están en posición de Noether con respecto a W_{r-i+2} y el morfismo $\pi : \mathbf{C}^n \longrightarrow \mathbf{C}^{r-i+2}$ definido por $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_{r-i+2})$ separa las componentes irreducibles de W_{r-i+2}, es decir, dadas dos componentes irreducibles C, C' de W_{r-i+2}, se verifica que $\pi(C) \neq \pi(C')$ (cf. [79]).

Para esto, dado $\gamma \in \mathbb{Z}$ se define la forma lineal $X_\gamma := X_1 + \gamma X_2 + \cdots + \gamma^{n-1} X_n$. Entonces, se tiene que existe $\gamma \in \Gamma := \{1, \ldots, nd^{4n^2}\}$ tal que las variables $X_1, \ldots, X_{r-i+1}, X_\gamma, X_{r-i+3}, \ldots, X_n$ están en posición general con respecto a W_{r-i+2} ([79], Lemme 2.3.5). El procedimiento operará con las (posibles) posiciones generales determinadas por todos los elementos $\gamma \in \Gamma$ a la vez (en paralelo).

Para $\gamma \in \Gamma$, se nota por $\pi_\gamma : \mathbf{C}^n \longrightarrow \mathbf{C}^{r-i+2}$ el morfismo definido por $\pi_\gamma(x_1, \ldots, x_n) = (x_1, \ldots, x_{r-i+1}, x_\gamma)$. Como las variables $X_1, \ldots, X_{r-i+1}, X_\gamma, X_{r-i+3}, \ldots, X_n$ están en posición de Noether respecto de W_{r-i+2}, el morfismo π_γ es finito y por lo tanto, dado que V_{r-i+1} es una variedad equidimensional de dimensión $r-i+1$, la imagen $\pi_\gamma(V_{r-i+1})$ es una hipersuperficie de $\mathbf{C}^{r-i+2}$ definible mediante un polinomio H_γ en $X_1, \ldots, X_{r-i+1}, X_\gamma$. A fin de calcular H_γ, se considera el siguiente $\mathbb{Q}$-espacio vectorial de dimensión finita:

$$E_\gamma(V, V_r \cup \cdots \cup V_{r-i+2}) := \Big\{ F \in \mathbb{Q}[X_1, \ldots, X_{r-i+1}, X_\gamma];\ \forall\, j = 1, \ldots, t'$$
$$\exists\, P_1^{(j)}, \ldots, P_s^{(j)} \in \mathbb{Q}[X_1, \ldots, X_n] \text{ tales que}$$
$$F H_j^{d^n} = \sum_{k=1}^{s} P_k^{(j)} F_k \text{ y } gr(P_k^{(j)} F_k) \leq d^n(2d^n + 1) \Big\}$$

Las consideraciones anteriores junto con las ideas de la demostración de la proposición 4 conducen al siguiente resultado:

Teorema 9 ([79], Théorème 4.1.2 y Proposition 4.2.2.) *Para cada $\gamma \in \Gamma$, sea $G_\gamma \in \mathbb{Q}[X_1, \ldots, X_r, X_\gamma]$ el polinomio que resulta de calcular el máximo común divisor con respecto a X_γ de los polinomios que forman una base como $\mathbb{Q}$-espacio vectorial de $E_\gamma(V, V_r \cup \cdots \cup V_{r-i+2})$ y H_γ la representación separable de G_γ. Entonces, $V_{r-i+1} = V(H_\gamma; \gamma \in \Gamma)$.*

El procedimiento que sugiere este teorema se reduce a cálculos de álgebra lineal. De hecho, es necesario hallar una base de soluciones de $O(nd^{4n^2})$ sistemas de ecuaciones lineales homogéneos de tamaño $O(sd^{3n^2} \times d^{3n^2})$ en paralelo, cuyos coeficientes tienen talla binaria de tipo $d^{O(n)}(h + \log s)$. Posteriormente, los polinomios H_γ se calculan en dos etapas: en primer lugar, el máximo común divisor G_γ de la base de soluciones halladas se calcula con la estrategia del lema 17. Luego, de G_γ se extrae una representación separable aplicando para ello el lema 19.

La importancia de los polinomios H_γ radica no sólo en la información que los mismos proveen, sino especialmente en su carácter *intrínseco*. De hecho, como ha sido observado en [79], el grado de cada polinomio H_γ está acotado por $gr(V_{r-i+1})$. Esta observación puede hacerse extensiva también a la talla binaria de los mismos. Combinando el Théorème 3, Proposition 4 y Théorème 6 en [147] (ver también [32]), se deduce una cota de tipo $d^{O(n)}(h + \log s)$ para la talla binaria de los coeficientes del polinomio H_γ (cabe destacar que los trabajos [147] y [32] utilizan métodos no elementales de álgebra y análisis complejo, cuyos resultados pueden reobtenerse en forma elemental a partir de los métodos desarrollados en [114, Section 4]).

Finalmente es necesario calcular un sistema de ecuaciones polinomiales que defina la variedad $V_r \cup \cdots \cup V_{r-i+1}$. En principio, la manera obvia de describir ésta variedad es tomar el ideal generado por todos los productos $G_j \cdot H_\gamma$ para $j = 1, \ldots, t$ y $\gamma = 1, \ldots, nd^{4n^2}$. Ahora bien, como $gr(G_j) \leq gr(V_r \cup \cdots \cup V_{r-i+2})$ y $gr(H_\gamma) \leq gr(V_{r-j})$ teniendo en cuenta que $gr(V_r \cup \cdots \cup V_{r-i+1}) \leq gr(V) \leq d^n$ se obtiene la estimación

$$gr(G_j \cdot H_\gamma) \leq d^n$$

para todo $j = 1, \ldots, t$ y todo $\gamma = 1, \ldots, nd^{4n^2}$ ([79], Proposition 4.2.6). Por lo tanto, dado que el $\mathbb{Q}$-espacio vectorial generado por los polinomios de

grado no mayor que d^n tiene dimensión (cantidad de monomios) acotada por d^{cn^2}, se puede extraer una base formada por a lo sumo d^{cn^2} polinomios de tipo $G_j \cdot H_\gamma$ que definen $V_r \cup \cdots \cup V_{r-i+1}$.

Asimismo, dado que la talla binaria de los coeficientes de cada polinomio G_j está acotada por $d^{c'n}(h + \log s)$ y la talla binaria de los coeficientes de cada polinomio H_γ no supera la cantidad $d^{c''n}(h + \log s)$, se deduce que los coeficientes de los polinomios $G_j \cdot H_\gamma$ elegidos tienen talla binaria acotada por $d^{c'''n}(h + \log s)$.

En conclusión, cada etapa puede llevarse a cabo en forma uniforme con talla $s^{O(n)}d^{O(n^2)}h^2$ y profundidad $O\big(n^4 \log^2(hsd)\big)$. Dado que se efectúan a lo sumo n etapas recursivas, se tiene una talla total $s^{O(n)}d^{O(n^2)}h^2$ y profundidad $O\big(n^5 \log^2(hsd)\big)$. Aplicando entonces la estrategia del teorema 1 se deduce el siguiente resultado:

Teorema 10 *Existe una máquina de Turing determinística que calcula la descomposición equidimensional de V en espacio $n^5 \log^2(hsd)$.*

Capítulo 2

Algoritmos probabilísticos

En el capítulo 1 se estudiaron algoritmos *determínisticos* para resolver los problemas de eliminación geométrica. Estos algoritmos generan siempre la solución exacta de todas las posibles instancias del problema considerado utilizando recursos de espacio y tiempo que dependen de un análisis del *peor caso*.

Sin embargo, en diversas situaciones, esta filosofía impone restricciones que pueden dificultar la aplicabilidad de los algoritmos. A fin de hallar una solución a esta cuestión, dos alternativas han sido estudiadas en el ámbito del cálculo simbólico. La primera de ellas se basa en desarrollar algoritmos que funcionan bien para instancias típicas del problema, los que se conocen como algoritmos para el *caso promedio*.

La otra alternativa, la que se seguirá en este capítulo, consiste en introducir aleatoriedad en el algoritmo por medio de un generador de números aleatorios (cf. [151],[102]). El ejemplo clásico en problemas de eliminación es el de la *verificación de identidades polinomiales*: dado un circuito aritmético sin divisiones que representa un polinomio P, decidir si P es el polinomio nulo.

El método directo de expandir P en una suma de monomios y chequear si todos sus coeficientes son nulos requiere, en general, un número excesivo de operaciones. En cambio se explorará un método alternativo que consiste en evaluar el polinomio en uno o más puntos elegidos aleatoriamente en un conjunto finito I.

Esta idea, que fue considerada por primera vez en un trabajo de R.A. De Millo y R.J. Lipton ([55]), posteriormente en sendos trabajos de J.T.

Schwartz ([162]) y R.E. Zippel ([186]), aparece en varios trabajos (ver [104], [97], [98] por ejemplo; en [159], [97] se han desarrollado métodos similares para chequear probabilísticamente la nulidad de un número calculado por un circuito aritmético). La idea es, dado un circuito aritmético sin divisiones que evalúa un polinomio P en n variables, elegir aleatoriamente un punto $(x_1, \ldots, x_n)$ de $\mathbb{Z}^n$ (que será llamado un *punto testigo* según [165]) en un conjunto $I \subset \mathbb{Z}^n$ adecuado y suficientemente grande de modo que la probabilidad de que P no sea nulo y la evaluación $P(x_1, \ldots, x_n)$ sea igual a 0 es menor que $\frac{1}{2}$. El test (conocido como el test de Schwartz–Zippel) consiste en evaluar $P(x_1, \ldots, x_n)$ y puede repetirse a fin de reducir la probabilidad de error bajo cualquier constante positiva. En resumen, se tiene el siguiente lema:

Lema 20 ([97, Corollary 2.1]) *Sea $P \in \mathbb{Q}[X_1, \ldots, X_n]$ un polinomio no nulo que se evalúa por medio de un circuito aritmético de profundidad no escalar ℓ. Sea $I := \{0, \ldots, 2^{\ell+1}n\}^n \subseteq \mathbb{Z}^n$. Entonces, la probabilidad de elegir aleatoriamente una n-upla $a := (a_1, \ldots, a_n) \in I$ tal que $P(a_1, \ldots, a_n) = 0$ es menor que $\frac{1}{2}$.*

Cabe destacar que el conjunto I elegido depende tanto del tamaño de la entrada (en forma polinomial) como de la instancia que se considera, es decir, cada circuito aritmético requiere de la generación de un nuevo punto testigo si el error quiere mantenerse bajo $\frac{1}{2}$.

En tal sentido, una interesante alternativa surge como consecuencia de un trabajo de Heintz–Schnorr ([94]): el punto testigo se reemplaza por un conjunto de fijo de puntos de $\mathbb{Z}^n$ de cardinalidad polinomial (que será llamado un conjunto *questor* o una *correct test sequence*). La ventaja ahora es que este conjunto de puntos puede utilizarse para todos los circuitos aritméticos de talla y profundidad dada. El test (que se conoce como el test de Heintz–Schnorr) consiste entonces en evaluar el circuito aritmético en estos puntos y da siempre la respuesta correcta si el conjunto questor ha sido correctamente elegido.

Definición 2 *Sea $\mathcal{F}$ un subconjunto de polinomios en $\mathbb{Z}[X_1, \ldots, X_n]$ tal que 0 pertenece a $\mathcal{F}$ y $\mathcal{Q}$ un subconjunto de $\mathbb{Z}^n$. Entonces $\mathcal{Q}$ se dice un conjunto questor para $\mathcal{F}$ si el polinomio 0 es el único polinomio del conjunto $\mathcal{F}$ que se anula sobre todos los puntos x de $\mathcal{Q}$.*

Entonces se tiene el siguiente lema:

Proposición 5 ([94, Theorem 4.4], [114, Corollary 19]) *Sea $\mathcal{F} := W(n, L, \ell)$ el conjunto de todos los polinomios en $\mathbb{Z}[X_1, \ldots, X_n]$ que pueden evaluarse mediante un circuito aritmético de talla (no escalar) L y profundidad (no escalar) ℓ. Sea $\omega := (2^{\ell+1} - 2)(2^\ell + 1)^2$ y $\sigma := 6(\ell L)^2$. Entonces el conjunto $\{1, \ldots, \omega\}^{n\sigma} \subset \mathbb{Z}^{n\sigma}$ contiene al menos $\omega^{n\sigma}(1 - \omega^{\frac{\sigma}{6}})$ conjuntos questores de cardinalidad σ para la clase $\mathcal{F}$.*

Si bien no se conocen algoritmos polinomiales determinísticos que calculen conjuntos questores, es posible generarlos aleatoriamente en forma independiente del input considerado. En tal caso el error que se comete está acotado por $\omega^{\frac{\sigma}{6}} \ll \frac{1}{2}$.

Esta idea ha sido aplicada en varios trabajos, como por ejemplo en [68], [80], [83], [114], [82], [81], [78] (cf. [138]). Recientemente se ha hallado un análogo de este método para el caso de números representados por circuitos aritméticos (ver [87]).

En el presente capítulo ambos tests serán aplicados en diferentes situaciones: el test Schwartz-Zippel será utilizado típicamente cada vez que sea necesario realizar un preprocesamiento de datos. En estos casos es importante generar una única respuesta con la cual se operará posteriormente, y por esto es importante trabajar con un punto testigo.

Por ejemplo, en el caso de sistemas sobredimensionados el número de ecuaciones se puede reducir considerablemente mediante combinaciones lineales de las ecuaciones originales (ver subsección 2.1.1). En este caso se demuestra (Teorema 6) que los coeficientes que intervienen en esas combinaciones lineales pueden elegirse con la condición de no anular un polinomio que se calcula mediante un circuito aritmético de talla y profundidad controladas. Otro caso de aplicación es la normalización de Noether que se realiza en la subsección 2.3.3.

Por otro lado, el test Heintz-Schnorr será aplicado en la subsección 2.3.4 a fin de generar sistemas de ecuaciones polinomiales que sean incompatibles. Dado que se trata con circuitos aritméticos de los cuales solamente su talla y profundidad, es necesario tener un mismo test para todas las posibles instancias, lo que exige la utilización de un conjunto questor.

Un modelo adecuado para describir los algoritmos probabilísticos que se desarrollarán es el de las máquinas de Turing *probabilísticas* (cf. [7]).

Una máquina de Turing probabilística M es un dispositivo de características similares a las del modelo determinístico, excepto por el hecho que la función de transición δ tiene dos imágenes por cada posible configuración.

Luego, en cada paso de computación la máquina M decide aletoriamente cual de las dos posibles imágenes de la función δ considera.

Una entrada x se dice aceptada por M si al menos la mitad de todas las posibles computaciones comenzando con x terminan en un estado de aceptación. El espacio de memoria y el tiempo de computación que requiere M sobre una entrada x se definen ahora como los mínimos entre todas las posibles computaciones aceptantes.

La *probabilidad de error* $e_m(x)$ se define como la proporción entre la cantidad computaciones sobre x que dan una respuesta errónea y la cantidad total de computaciones sobre x.

Un tipo especial de máquinas probabilísticas, las máquinas de *error acotado*, son particularmente interesantes en la práctica ya que, en este caso, el error puede reducirse rápidamente por debajo de cualquier constante positiva, mediante la repetición de la la computación sobre x. Una máquina probabilística de error acotado es una máquinas probabilística M que verifica que existe una constante $\varepsilon < \frac{1}{2}$ tal que el error $e_M(x)$ es inferior a ε para todo $x \in \{0,1\}^*$.

2.1 El caso 0-dimensional: técnicas de elemento primitivo

Los algoritmos que se describirán aprovechan la *semántica* de los problemas que tratan a fin de realizar una utilización mas eficiente de los recursos computacionales. Es por lo tanto importante realizar una reflexión sobre la semántica de las cuestiones que se consideran.

El problema central a considerar es el de *resolver* sistemas de ecuaciones polinomiales. Debido a las restricciones que impone la práctica, resulta natural adoptar como entrada de todos los algoritmos un conjunto finito $F_1, \ldots, F_s$ de polinomios en $\mathbb{Z}[X_1, \ldots, X_n]$.

Claro está, la palabra "resolver" tiene distintos significados en diferentes ámbitos. En esta tesis los problemas que se estudian tienen significado

geométrico, es decir, se refieren a la *variedad* algebraica

$$V := \{(x_1, \ldots, x_n) \in \mathbf{C}^n; F_1(x_1, \ldots, x_n) = \cdots = F_s(x_1, \ldots, x_n) = 0\}$$

mas que al ideal generado por dichas ecuaciones polinomiales $F_1, \ldots, F_s$ en si. En este sentido, se estudia el ideal *radical* $\sqrt{(F_1, \ldots, F_s)}$, ya que este ideal es el que corresponde a la variedad V. Para esto se estudia la $\mathbb{Q}$-álgebra reducida:

$$B := \mathbb{Q}[X_1, \ldots, X_n]/\sqrt{(F_1, \ldots, F_s)}$$

Una estrategia común es reducir las cuestiones al caso *0-dimensional*, dado que en este caso existen técnicas que permiten importantes mejoras de complejidad. Es por lo tanto de suma importancia tener métodos que permitan la descripción efectiva de la $\mathbb{Q}$-álgebra B en el caso cero-dimensional. Este es el objetivo central de esta sección.

2.1.1 Algunas reducciones éstandar

A fin de simplificar un poco la situación, es conveniente realizar algunas reducciones del problema a tratar. En primer lugar se demostrará que toda variedad algebraica de dimensión cero puede describirse por medio de una cantidad $n \leq t \leq n+1$ de ecuaciones $F_1', \ldots, F_t'$ tales que $F_1', \ldots, F_n'$ forman una sucesión regular, las cuales pueden generarse con baja complejidad a partir de cualquier sistema de ecuaciones que defina la variedad V. Este es el contenido del siguiente lema, que es un caso particular de una técnica general de preprocesamiento de sistemas de ecuaciones polinomiales (ver [88], [38], [154], [59], [114]):

Lema 21 *Sean $F_1, \ldots, F_s$ polinomios en $\mathbb{Z}[X_1, \ldots, X_n]$ que definen una variedad algebraica $V \subseteq \mathbf{C}^n$ de dimensión cero. Entonces existe $t \in \{n, n+1\}$ y una matriz genérica $Q \in \mathbb{Z}^{t \times s}$ tales que, si*

$$Q := \begin{pmatrix} \lambda_{11} & \lambda_{1s} \\ \vdots & \vdots \\ \lambda_{t1} & \lambda_{ts} \end{pmatrix}$$

definiendo $F_i' := \lambda_{i1} F_1 + \cdots + \lambda_{is} F_s$ para $i = 1, \ldots, t$, se verifica:

1. $V(F_1', \ldots, F_t') = V(F_1, \ldots, F_s)$

2. *$F'_1, \ldots, F'_n$ forman una sucesión regular*

3. *los coeficientes λ_{ij} verifican $|\lambda_{ij}| \leq d^n$ y se pueden generar aleatoriamente con probabilidad mayor que $\frac{1}{2}$ de obtener una matriz Q que satisfaga las condiciones pedidas.*

Demostración. Se construyen inductivamente polinomios $F'_1, \ldots, F'_n$ que forman una sucesión regular de manera que $\dim(F'_1, \ldots, F'_i) = n - i$ para $i = 1, \ldots, n$. Eventualmente, en el caso en que $V(F'_1, \ldots, F'_n) \neq V$, es necesario construir un polinomio adicional F'_{n+1} tal que $V(F'_1, \ldots, F'_{n+1}) = V(F_1, \ldots, F_s)$.

Para $k = 1$, suponiendo $F_1 \neq 0$ se puede tomar simplemente $F'_1 := F_1$.

En el caso general, sea $1 < i < n$ y $F'_1, \ldots, F'_i$ que verifican las condiciones del enunciado del lema. Sea $\mathcal{C}$ el conjunto de las componentes irreducibles de $V(F'_1, \ldots, F'_i)$. Como V es una variedad de dimensión cero y $V(F'_1, \ldots, F'_i)$ es una variedad equidimensional de dimensión $n - i > 0$, se deduce que ninguna componente $C \in \mathcal{C}$ está contenida en V. Por lo tanto, es posible elegir un punto $x_C \notin V$ en cada componente $C \in \mathcal{C}$ y definir el siguiente polinomio:

$$F^{(i+1)}(T_{i+1\,1}, \ldots, T_{i+1\,s}) := \prod_{C \in \mathcal{C}} (T_{i+1\,1} F_1(x_C) + \cdots + T_{i+1\,s} F_s(x_C))$$

Dado que ningún punto x_C pertenece a V se deduce que, para cada $C \in \mathcal{C}$ existe $j \in \{1, \ldots, s\}$ tal que $F_j(x_C) \neq 0$. Esto asegura que las formas lineales $T_1 F_1(x_C) + \cdots + T_s F_s(x_C))$ son no nulas para todo x_C. Además, el conjunto $\#(\mathcal{C})$ tiene cardinal acotado por d^n (ver [88]). Por lo tanto, el polinomio $F(T_1, \ldots, T_n)$ es un polinomio no nulo de grado menor o igual que d^n, y existen entonces enteros no negativos $\lambda_{i+1\,1}, \ldots, \lambda_{i+1\,s}$ acotados por d^n tales que $F(\lambda_{i+1\,1}, \ldots, \lambda_{i+1\,s}) \neq 0$.

En consecuencia, se define $F'_{i+1} := \lambda_{i+1\,1} F_1 + \cdots + \lambda_{i+1\,s} F_s$. Por construcción, F'_{i+1} no es divisor de cero módulo $(F'_1, \ldots, F'_i)$, ya que $\{F'_{i+1} = 0\}$ corta propiamente todas las componentes irreducibles de $(F'_1, \ldots, F'_i)$: dada una tal componente C, si x_C fue el punto elegido en esa componente para la construcción de F, se tiene que $F'_{i+1}(x_C) = \lambda_{i+1\,1} F_1(x_C) + \cdots + \lambda_{i+1\,s} F_s(x_C) \neq 0$ por la elección de $(\lambda_{i+1\,1}, \ldots, \lambda_{i+1\,s})$, lo que significa que $C \not\subseteq \{F'_{i+1} = 0\}$.

Finalmente, al final del n-ésimo paso se tienen dos posibilidades:

- $V(F'_1, \ldots, F'_n) = V$, en cuyo caso el proceso está concluído.

- $V(F'_1,\ldots,F'_n) \neq V$, en cuyo caso se realiza un paso mas del proceso inductivo.

En el segundo caso se consideran las componentes C de $V(F'_1,\ldots,F'_n)$ que no están contenidas en V. Como estas componentes tienen dimensión cero son los puntos x_C de $\mathbf{C}^n$ que se eligen para la construcción del polinomio F'_{n+1}. De esta manera, los puntos de $V(F'_1,\ldots,F'_n)\setminus V$ se eliminan de $V(F'_1,\ldots,F'_{n+1})$, obteniéndose en consecuencia que $V(F'_1,\ldots,F'_{n+1}) = V$.

Resta demostrar las propiedades que verifican los coeficientes $\lambda_{i\ j}$ que se han elegido para formar la matriz Q. De la demostración se deduce que estos coeficientes pueden elegirse con la única condición de no satisfacer la siguiente ecuación:

$$\prod_{k=2}^{t} F^{(k)}(T_{k1},\ldots,T_{ks}) = 0$$

Los polinomios $F^{(k)}$ tienen grado acotado por d^n. Por lo tanto, el polinomio $\prod F^{(k)}$ tiene grado nd^n, y utilizando el test de Schwartz–Zippel (lema 20) se deduce que los coeficientes λ_{ij} pueden elegirse aleatoriamente en el conjunto $\{0,\ldots,n^2d^n\}^{ts}$ con probabilidad mayor que $\frac{1}{2}$ de obtener una matriz Q que verifica las condiciones del enunciado del lema. □

A los fines que aquí se consideran, es posible trabajar con la variedad $V(F'_1,\ldots,F'_n)$ aún en el caso en que ésta no coincide con la variedad original V. Mediante un nuevo preprocesamiento de las ecuaciones se obtienen generadores para el ideal $(F'_1,\ldots,F'_n)$ que verifican las condiciones anteriores y algunas propiedades adicionales. Esta nueva reducción se realiza aplicando una versión efectiva del Teorema de Bertini (cf. [103]).

Proposición 6 ([114], Proposition 37) *Sean $F_1,\ldots,F_n$ polinomios en $\mathbb{Z}[X_1,\ldots,X_n]$ tales que el ideal $(F_1,\ldots,F_n)$ es de dimensión 0. Entonces existe una matriz $Q \in \mathbb{Z}^{(n-1)\times n}$ con coeficientes acotados por d^n tal que los polinomios definidos por:*

$$\begin{pmatrix} F'_1 \\ \vdots \\ F'_{n-1} \end{pmatrix} = Q \begin{pmatrix} F_1 \\ \vdots \\ F_n \end{pmatrix}$$

verifican las siguientes condiciones:

- $(F'_1, \ldots, F'_{n-1}, F_n) = (F_1, \ldots, F_n)$
- $(F'_1, \ldots, F'_n)$ *es una sucesión regular*
- $(F'_1, \ldots, F'_i)$ *es un ideal radical de* $\mathbb{Q}[X_1, \ldots, X_n]$ *para todo* $i = 1, \ldots, n-1$
- *los coeficientes de* Q *se pueden elegir aleatoriamente en* $\{0, 1, \ldots, d^n\}^n$ *con probabilidad mayor que* $\frac{1}{2}$ *de obtener una matriz* Q *que verifique las condiciones requeridas.*

2.1.2 Soluciones geométricas

Según lo desarrollado en la subsección anterior, se puede suponer que los polinomios de entrada $F_1, \ldots, F_n$ en $\mathbb{Z}[X_1, \ldots, X_n]$ forman una sucesión regular en $\mathbb{Q}[X_1, \ldots, X_n]$ y que el ideal generado por $F_1, \ldots, F_i$ en $\mathbb{Q}[X_1, \ldots, X_n]$ es radical para $i = 1, \ldots, n-1$. Como ha sido dicho anteriormente, el problema es describir la $\mathbb{Q}$-álgebra B definida por:

$$B := \mathbb{Q}[X_1, \ldots, X_n]/\sqrt{(F_1, \ldots, F_n)}$$

Sea $V_i \subset \mathbf{C}^n$ la variedad algebraica definida por $F_1, \ldots, F_i$ y $V := V_n$. Dado que $F_1, \ldots, F_n$ forman una sucesión regular resulta V una variedad cero-dimensional y por lo tanto B es un $\mathbb{Q}$-espacio vectorial de dimensión finita. Asimismo se sabe que $\delta := \dim_{\mathbb{Q}} B = \#(V)$ (ver [83], [88]).

Los procedimientos conocidos para describir la estructura algebraica de B generalmente operan con el conjunto de todos los monomios de $\mathbb{Q}[X_1, \ldots, X_n]$ que verifican cierta condición (este conjunto suele tener cardinalidad al menos de tipo d^n), a fin de obtener una base de B como $\mathbb{Q}$–espacio vectorial.

El método que aquí se propone difiere radicalmente de este tipo de procedimientos, dado que maneja estructuras cuyo tamaño está controlado por parámetros que dependen de la *geometría* del sistema de ecuaciones a considerar.

A fin de hallar una base de B como $\mathbb{Q}$–espacio vectorial, se observa que cualquier forma lineal $U \in \mathbb{Z}[X_1, \ldots, X_n]$ elegida genéricamente *separa* los puntos de la variedad V (es decir, se satisface que $U(x) \neq U(y)$ para todo par de puntos distintos $x, y \in V$). Cada forma lineal U en estas condiciones permite obtener una base de B de la siguiente manera: siendo u la imagen de

U en B, el conjunto de las potencias $\{1, u, \ldots, u^{\delta-1}\}$ forman la base buscada. En tal caso, se llama a u un *elemento primitivo* de B (ver [77], [110] por más detalles).

A partir de un elemento primitivo u se obtiene una representación de B como el cociente de $\mathbb{Q}[T]$ módulo un cierto ideal principal (el generado por el polinomio minimal de u) :

$$B = \mathbb{Q}[X_1, \ldots, X_n]/(P(u), \rho X_1 - v_1(u), \ldots, \rho X_n - v_n(X_n)) = \mathbb{Q}[T]/(P(T))$$

donde ρ es un entero no nulo, $v_1, \ldots, v_n, P \in \mathbb{Z}[T]$, siendo P el polinomio minimal de u en B y el grado de cada polinomio v_i está acotado por $deg(P) - 1 = \delta - 1$.

Obsérvese que la representación de B que se ha elegido consiste solamente de polinomios enteros *univariados* de grado a lo sumo δ y un entero $\rho \in \mathbb{Z}$, lo cual implica que el tamaño de esta estructura de datos es *polinomial* en términos de δ y n. Por último, el tensor de multiplicación en B puede obtenerse fácilmente a partir de esta información : si M es la matriz compañera de $P(T)$, entonces $M_{X_i} := \rho^{-1} v_i(M)$.

Convenientemente traducidas, estas nociones pueden aplicarse al caso mas general de variedades de dimensión positiva: sean $F_1, \ldots, F_r \in \mathbb{Z}[X_1, \ldots, X_n]$ polinomios que forman una sucesión regular en $\mathbb{Q}[X_1, \ldots, X_n]$ tales que el ideal que generan $F_1, \ldots, F_r$ en $\mathbb{Q}[X_1, \ldots, X_n]$ es radical. En primer lugar, es posible realizar un cambio de variables $(X_1, \ldots, X_n) \to (Y_1, \ldots, Y_n)$ tal que las variables $Y_1, \ldots, Y_{n-r}$ son libres respecto de $V := V(F_1, \ldots, F_r)$ (es decir, no existe ningún polinomio en $\mathbb{Q}[Y_1, \ldots, Y_{n-r}]$ que se anule sobre V) y tal que la extensión de anillos conmutativos:

$$R := \mathbb{Q}[Y_1, \ldots, Y_{n-r}] \longrightarrow \mathbb{Q}[Y_1, \ldots, Y_n]/\sqrt{(F_1, \ldots, F_r)} =: B$$

es entera.

En este caso, B resulta reducido (es decir, sin divisores de cero no triviales) y un R-módulo libre de rango finito (cf. [83]). En tal caso, un elemento $u \in B$ se dice un *elemento primitivo* de la extensión de anillos $R \subseteq B$ si el grado del polinomio minimal m_u de u coincide con el rango de B como R-módulo libre.

En lo que sigue, dado $b \in B$ se denota por $\eta_b : B \longrightarrow B$ el endomorfismo R-lineal inducido por la multiplicación de elementos de B por b (un tal endomorfismo será llamado una homotecia). También se denotará la matriz

de la homotecia η_b por M_b, el polinomio característico de η_b por $\chi_b \in R[T]$ y el polinomio minimal primitivo de η_b por m_b. Obsérvese que χ_b y m_b son polinomios mónicos de $R[T]$, que serán llamados el polinomio característico y minimal de b respectivamente.

Sea $k := \mathbb{Q}(Y_1, \ldots, Y_{n-r})$ el cuerpo de cocientes de R y $B' = k \otimes B = \mathbb{Q}(Y_1, \ldots, Y_{n-r})[Y_{n-r+1}, \ldots, Y_n]/k \otimes (F_1, \ldots, F_r)$, donde $k \otimes (F_1, \ldots, F_r)$ es el ideal generado por $(F_1, \ldots, F_r)$ en $k[Y_{n-r+1}, \ldots, Y_n]$. Entonces un elemento $u \in B$ resulta un elemento primitivo B si y sólo si, para $\delta := rango_R B = dim_k B'$ el conjunto $\{1, u, \ldots, u^{\delta-1}\}$ representa una base del k-espacio vectorial B'.

En lugar de describir B, para los fines necesarios será suficiente dar una descripción adecuada de la k-álgebra B'. Y esta álgebra se caracteriza mediante los siguientes ítems:

- una base del k-espacio vectorial B'
- para $n - r + 1 \leq i \leq n$ las matrices M_{X_i} de las homotecias $\eta_{X_i} : B \to B$ con respecto a la base dada (estas matrices describen el tensor de multiplicación de la k-algebra B' y por lo tanto, de la R-álgebra B)

Estos ítems son lo que se define como una *solución geométrica* de la variedad $V(F_1, \ldots, F_r)$. La base de B' se obtiene a partir de un elemento primitivo de B adecuado.

En el contexto de esta tesis, el elemento primitivo $u \in B$ será elegido como la imagen en B de una forma lineal genérica de las variables $X_{n-r+1}, \ldots, X_n$ con coeficientes en $\mathbb{Z}$, es decir, u será la imagen de una forma lineal $U = \lambda_{n-r+1} X_{n-r+1} + \cdots + \lambda_n X_n$, con $\lambda_i \in \mathbb{Z}$ para $n - r + 1 \leq i \leq n$. Siendo T una nueva indeterminada, el polinomio minimal $m_u(T)$ de u como elemento de la R-álgebra B (o equivalentemente como elemento de la k-álgebra B') será un polinomio mónico en $\mathbb{Q}[X_1, \ldots, X_{n-r}, T]$. Este polinomio minimal será elegido como un elemento del anillo $\mathbb{Z}[X_1, \ldots, X_{n-r}, T] = R[T]$ y, en el caso cero-dimensional, será reemplazado por un múltiplo de m_u de manera tal que el polinomio resultante, que será notado q_u, sea primitivo en $\mathbb{Z}[T]$.

Finalmente, como $\{1, u, \ldots, u^{\delta-1}\}$ es una base del k-espacio vectorial B', para $n - r + 1 \leq i \leq n$ existen polinomios $v_i^{(u)} \in R[T]$ y elementos no nulos $\rho_i^{(u)} \in R$ tales que $\rho_i^{(u)} X_i - v_i^{(u)}(U)$ pertenece al ideal generado por $F_1, \ldots, F_r$ en $k[X_{n-r+1}, \ldots, X_n]$. En particular, se tiene la siguiente identidad de ideales de $k[X_{n-r+1}, \ldots, X_n]$:

$$(F_1, \ldots, F_r) = (q_u(U), \rho_1^{(u)} X_{r+1} - v_{r+1}^{(u)}(U), \ldots, \rho_n^{(u)} X_n - v_n^{(u)}(U))$$

Mas aún, si M es la matriz compañera de la homotecia η_u con respecto a la base $\{1, u, \ldots, u^{D-1}\}$, las matrices $M_{X_{n-r+1}}, \ldots, M_{X_n}$ que caracterizan el tensor de multiplicación de la R-álgebra B (o equivalentemente de la k-algebra B') se obtienen a partir de la identidad:

$$\rho_i^{(u)} \cdot M_{X_i} = v_i^{(u)}(M)$$

para $n - r + 1 \leq i \leq n$.

2.1.3 La complejidad del cálculo de un elemento primitivo

En esta subsección se determina la complejidad del cálculo de un elemento primitivo para V y de la solución geométrica que se obtiene a partir del mismo.

Como se ha dicho, la diferencia esencial entre el método aquí aplicado y los métodos anteriormente utilizados es que cantidades algebraicas usualmente utilizadas para estimar la complejidad de los problemas de eliminación geométricos (como el número de Bezout d^n o la regularidad de la función de Hilbert de un ideal homogéneo apropiado) se reemplazan por parámetros que vienen de la geometría. Siguiendo [82], [81], [78] se definen dos invariantes geométricos que controlan el tamaño dél álgebra lineal involucrada y la longitud bit de los números enteros que se manipulan: el *grado (afín)* y la *altura (afín)* de variedades intersección completa.

Sea entonces $V \subset \mathbf{C}^n$ la variedad algebraica definida por polinomios $F_1, \ldots, F_r$ en $\mathbb{Z}[X_1, \ldots, X_n]$ de grado acotado por d ($r \leq n$) que forman una sucesión regular en $\mathbb{Q}[X_1, \ldots, X_n]$ tales que $(F_1, \ldots, F_r)$ es un ideal radical de $\mathbb{Q}[X_1, \ldots, X_n]$. Se considera el conjunto $\mathcal{D}_V$ de todas las variedades lineales H de dimensión $n - i$ tales que $\#(H \cap V) < \infty$ y se tiene la siguiente definición:

Definición 3 *El grado de V, $gr(V)$, se define como la máxima cantidad de puntos que se obtienen al intersecar V con variedades lineales de $\mathcal{D}_V$*

En [88] se demuestra que el grado es siempre un número natural y que el mismo se obtiene cuando la variedad lineal con la que se interseca es genérica. Esta definición de grado es equivalente a la siguiente: si se considera todos los cambios lineales afines de coordenadas

$$(X_1, \ldots, X_n) \to (Y_1, \ldots, Y_n)$$

cada cambio de coordenadas genérico de este tipo induce una extensión de anillos entera:

$$R := \mathbb{Q}[Y_1, \ldots, Y_{n-r}] \to \mathbb{Q}[Y_1, \ldots, Y_n]/(F_1, \ldots, F_r) =: \mathbb{Q}[V].$$

El anillo $\mathbb{Q}[V]$ es un R-módulo de rango finito (cf. [83] por ejemplo). Este rango es el mismo para cualquier cambio de coordenadas lineal genérico y coincide con el grado de la variedad V.

La definición de altura de una variedad diofántica afín se inspira en la noción correspondiente para variedades proyectivas desarrollada en [133], [134], [142], [145], [146], [147] (ver también [33], [18], [62], [113], [114]).

En primer lugar es preciso definir primero que es la altura (logarítmica) de un entero, de un vector de enteros, de una matriz con entradas enteras y de un polinomio con coeficientes enteros.

Sea $a \in \mathbb{Z}$, entonces la altura de a se define como $ht(a) := max\{log|a|, 1\}$. Es claro que la altura mide la longitud binaria de a. Para un vector de números enteros $\alpha := (a_1, \ldots, a_n) \in \mathbb{Z}^n$, se define la altura de α como el máximo entre las alturas de sus coordenadas, y análogamente se define la altura de una matriz $A \in \mathbb{Z}^{n \times m}$ como el máximo entre las alturas de sus entradas. Finalmente la altura de un polinomio $F \in \mathbb{Z}[X_1, \ldots, X_n]$ se define como la altura del vector formado por sus coeficientes.

Se define entonces la noción de altura afín de una variedad diofántica cero-dimensional:

Definición 4 *Dada una variedad algebraica diofántica cero-dimensional $V \subset \mathbb{C}^n$ y una forma lineal $U = \lambda_1 X_1 + \cdots + \lambda_n X_n$ con coeficientes enteros que representa un elemento primitivo u de la extensión de anillos $\mathbb{Q} \to \mathbb{Q}[V]$, se define la altura de V con respecto a U como el máximo de las alturas de los polinomios $q_u(T), \rho_1^{(u)} X_1 - v_1^{(u)}(T), \ldots, \rho_n^{(u)} X_n - v_n^{(u)}(T)$ que corresponden a la solución geométrica de V a partir del elemento primitivo u. Esta altura se notará por $ht(V; U)$.*

Luego, la altura de una variedad algebraica diofántica cero-dimensional V se define como la función $ht_V : \mathbb{N} \to \mathbb{N}$ que asocia a cada número natural $c \in \mathbb{N}$ el valor $ht_V(c) := max\{ht(V,U); ht(U) \leq c\}$ si la extensión de anillos $\mathbb{Q} \to \mathbb{Q}[V]$ tiene un elemento primitivo u que es imagen de una forma lineal U de altura acotada por c y que asocia a c el valor 1 si no existe tal elemento primitivo.

En el caso mas general de una variedad diofántica intersección completa V de dimensión positiva $n-r$, sean $F_1, \ldots, F_r \in \mathbb{Z}[X_1, \ldots, X_n]$ polinomios que forman una sucesión regular en $\mathbb{Q}[X_1, \ldots, X_n]$ que definen V. Sea $\mathcal{N}_V$ la clase de todos los cambios de coordenadas:

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{1n} \\ \vdots & \vdots \\ a_{n1} & a_{nn} \end{pmatrix} \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

tales que la matriz $A := (a_{ij})_{1 \leq i,j \leq n}$ tiene entradas enteras y es no singular y tal que la extensión inducida por el cambio de coordenadas:

$$R := \mathbb{Q}[Y_1, \ldots, Y_{n-r}] \to \mathbb{Q}[Y_1, \ldots, Y_n]/(F_1, \ldots, F_r) := \mathbb{Q}[V] \qquad (2.1)$$

es entera. El cambio de coordenadas dado por la matriz A induce un morfismo *finito* de variedades afines $\pi : V \to \mathbf{C}^{n-i}$. Se considera cualquier forma lineal $U = \lambda_{n-i+1} X_{n-i+1} + \cdots + \lambda_n X_n$ con coeficientes enteros tal que su imagen u en $\mathbb{Q}[V]$ es un elemento primitivo de la extensión de anillos $R \to \mathbb{Q}[V]$, y la clase $\mathcal{F}_u$ de todos los puntos $P \in \mathbb{Z}^{n-i}$ tales que:

- los elementos de $V_P := \pi^{-1}(\{P\})$ son puntos suaves de V,
- el número de elementos $gr(V_P)$ de V_P coincide con el rango del R-módulo libre $\mathbb{Q}[V]$ y
- la forma lineal U genera también un elemento primitivo de la extensión $\mathbb{Q} \to \mathbb{Q}[V_P]$.

Manteniendo estas notaciones se tiene la siguiente noción de altura de variedades algebraicas diofánticas:

Definición 5 *Dada una variedad diofántica intersección completa V como antes, un cambio lineal de coordenadas $A \in \mathcal{N}_V$, una forma lineal $U \in \mathbb{Z}[Y_{n-i+1}, \ldots, Y_n]$ cuya imagen u en $\mathbb{Q}[V]$ es un elemento primitivo de la extensión entera de anillos 2.1 y un punto $P \in \mathcal{F}_u$, se define la altura de V con respecto a (A, U, P) en la forma:*

$$ht(V; (A, U, P)) := ht(V_P; U).$$

Luego, la altura de una variedad algebraica diofántica intersección completa V se define como la función $ht_V : \mathbb{N} \to \mathbb{N}$ que asocia a cada número natural $c \in \mathbb{N}$ el valor $ht_V(c) := max\{ht(V; A, U, P) : ht(A, U, P) \leq c\}$ si existe un triple (A,U,P) que satisface los requerimientos de la definición de altura acotada por c y que asocia a c el valor 1 si no existe tal elemento primitivo.

En [78] se demuestra que $ht(c)$ se acota en forma polinomial en términos del número de Bezout d^n, la altura h de los polinomios F_i y c, pudiendo ser el número $ht(c)$ ostensiblemente menor que esta estimación en casos de interés práctico.

Habiendo definido los parámetros geométricos que controlan la complejidad del proceso, se puede ahora sintetizar el resultado principal de esta sección, cuyo enunciado preciso es el teorema 11:

Sea $V \subset \mathbf{C}^n$ la variedad algebraica intersección completa de dimensión cero definida por polinomios $F_1, \ldots, F_n \in \mathbb{Z}[X_1, \ldots, X_n]$ que verifican:

- *$F_1, \ldots, F_n$ definen una sucesión regular en $\mathbb{Q}[X_1, \ldots, X_n]$,*
- *para todo $i = 1, \ldots, n$, el ideal $(F_1, \ldots, F_i)$ es un ideal radical de $\mathbb{Q}[X_1, \ldots, X_n]$,*
- *los polinomios $F_1, \ldots, F_n$ están dados mediante un circuito aritmético uniforme de talla L y profundidad no escalar ℓ, que utiliza parámetros enteros de talla h.*

Sea $d := max\{gr(F_i) : 1 \leq i \leq n\}$ el máximo grado total de los polinomios input y $\delta := max\{gr(V(F_1, \ldots, F_i)) : 1 \leq i \leq n\}$ el grado geométrico del sistema. Finalmente, se define la altura geométrica del sistema η en la forma

$\eta := max\{ht_{V_i}(c((\log n + \ell)\log\delta) : 1 \leq i \leq n\}$, *donde* $c > 0$ *es una constante universal que no depende del input* $F_1, \ldots, F_n$ *considerado (ni de su tamaño).*

Entonces existe una máquina de Turing probabilística de error acotado que calcula una forma lineal U *que representa un elemento primitivo* u *para* V *y la solución geométrica asociada al elemento primitivo* u *en espacio polinomial con respecto a los parámetros* n, ℓ *y* η *y polilogarítmico con respecto a* d, h, L *y* δ.

2.1.4 El método de Newton–Hensel

Sea $V \subseteq \mathbf{C}^n$ la variedad algebraica intersección completa definida por los polinomios $F_1, \ldots, F_r \in \mathbb{Z}[X_1, \ldots, X_n]$. Según lo desarrollado en la subsección 2.1.2, la idea es hallar una solución geométrica para la variedad V. El objetivo de esta sección es mostrar un método mediante el cual esta cuestión puede reducirse al caso cero-dimensional.

En primer lugar, luego de un preprocesamiento de las variables (la normalización de Noether que se obtiene mediante un cambio de variables lineal), se puede suponer sin pérdida de generalidad que la extensión de anillos

$$R := \mathbb{Q}[X_1, \ldots, X_{n-r}] \to \mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_r) = \mathbb{Q}[V]$$

es inyectiva y entera.

En tal caso, el morfismo $\pi : V \to \mathbf{C}^{n-r}$ inducido por este cambio de variables es finito y la fibra $V_P := \pi^{-1}(\{P\})$ de cualquier punto genérico $P \in \mathbf{C}^{n-r}$ es finita y tiene cardinal $gr(V)$. La intención es aplicar el método de Newton–Hensel en forma simbólica a fin de recuperar la solución geométrica de V a partir de la solución geométrica de la fibra V_P de un punto $P \in \mathbf{C}^{n-r}$ adecuado. Dado que V_P es una variedad cero-dimensional para $P \in \mathbf{C}^{n-r}$ genérico, se deduce que el problema de calcular la solución geométrica de una variedad algebraica intersección completa de dimensión positiva se reduce al caso cero-dimensional.

A fin de preservar la "racionalidad" del algoritmo el punto P será elegido con coordenadas enteras, es decir, $P \in \mathbb{Z}^{n-r}$. Para poder extraer toda la información necesaria de V_P, es preciso que el punto P elegido verifique las siguientes condiciones:

- los elementos de $V_P = \pi^{-1}(P)$ son puntos suaves de V,

- el número de elementos $gr(V_P)$ de V_P coincide con el rango del R-módulo libre $\mathbb{Q}[V]$, y

- la forma lineal U genera también un elemento primitivo de la extensión $\mathbb{Q} \to \mathbb{Q}[V_P]$.

Un punto $P \in \mathbb{Z}^{n-r}$ en estas condiciones se llamará un *punto de levantamiento* y su fibra V_P se llamará la *fibra de levantamiento.*

En lo que sigue se supondrá que se tiene una forma lineal con coeficientes enteros $U = \lambda_{n-r+1}X_{n-r+1} + \cdots + \lambda_n X_n$ tal que su imagen u en $\mathbb{Q}[V_P]$ es un elemento primitivo de la extensión de anillos $\mathbb{Q} \to \mathbb{Q}[V_P]$, polinomios $q^{(P)}(T)$, $v_{n-r+1}^{(P)}(T),\ldots,v_n^{(P)}(T) \in \mathbb{Z}[T]$ y elementos $\rho_{n-r+1}^{(P)}, \ldots, \rho_n^{(P)} \in \mathbb{Z}$ tales que constituyen una solución geométrica para la variedad V_P.

Sea $F := (F_1, \ldots, F_r)$ y sea $D(F) := D(F_1, \ldots, F_r) := \left(\frac{\partial F_i}{\partial X_{n-r+j}}\right)_{1 \le i,j \le r}$ la matriz jacobiana de los polinomios $F_1, \ldots, F_r$. Suponiendo que esta matriz es regular y considerando los polinomios $F_1, \ldots, F_r$ como funciones en $\underline{X} := (X_{n-r+1}, \ldots, X_n)$, se define el siguiente operador de Newton-Hensel:

$$N_F(X_{n-r}, \ldots, X_n) := \begin{pmatrix} X_{n-r} \\ \vdots \\ X_n \end{pmatrix} - D(F)^{-1} \begin{pmatrix} F_1(X_{n-r+1}, \ldots, X_n) \\ \vdots \\ F_r(X_{n-r+1}, \ldots, X_n) \end{pmatrix} \quad (2.2)$$

Se tiene entonces la siguiente versión del conocido lema de Hensel:

Lema 22 *Sea $P = (p_1, \ldots, p_{n-r}) \in \mathbb{Z}^{n-r}$ un punto de levantamiento para V. Entonces, dado un punto $\xi = (\xi_{n-r+1}, \ldots, \xi_n) \in V_P$, existen únicas series de potencias $R_{n-r+1}^{(\xi)}, \ldots, R_n^{(\xi)}$ en $\mathbf{C}[\![X_1 - p_1, \ldots, X_{n-r} - p_{n-r}]\!]$ que verifican las siguientes condiciones*

- *Para $i = 1, \ldots, r$ vale la siguiente identidad en $\mathbf{C}[\![X_1 - p_1, \ldots, X_{n-r} - p_{n-r}]\!]$:*

$$F_i(X_1, \ldots, X_{n-r}, R_{n-r+1}^{(\xi)}, \ldots, R_n^{(\xi)}) = 0$$

- *Para $j = 1, \ldots, r$ vale que $R_{n-r+j}^{(\xi)}(P) = \xi_{n-r+j}$*

Demostración. Se define la siguiente sucesión en $\mathbf{C}[\![X_1 - p_1, \ldots, X_{n-r} - p_{n-r}]\!]^r$:

$$R^{(\xi,0)} = (R^{(\xi,0)}_{n-r+1}, \ldots, R^{(\xi,0)}_n) \ := (\xi_{n-r+1}, \ldots, \xi_n)$$

$$R^{(\xi,N+1)} = (R^{(\xi,N+1)}_{n-r+1}, \ldots, R^{(\xi,N+1)}_n) \ := N_F(R^{(\xi,N)})^t \text{ para } N \geq 0$$

donde A^t denota la matriz traspuesta de A. Obsérvese que de la definición de $R^{(\xi,N)}$, por medio de un argumento inductivo se deduce que cada $R^{(\xi,N)}_{n-r+j}$ representa una función racional de $\mathbf{C}(X_1, \ldots, X_{n-r})$.

Se nota por m el ideal maximal $m := (X_1 - p_1, \ldots, X_{n-r} - p_{n-r})$ generado por $X_1 - p_1, \ldots, X_{n-r} - p_{n-r}$ en $\mathbf{C}[\![X_1 - p_1, \ldots, X_{n-r} - p_{n-r}]\!]$. Entonces las siguientes afirmaciones son válidas para todo $N \in \mathbb{N}$:

1. $F_i(X_1, \ldots, X_{n-r}, R^{(\xi,N)}) \in m^{2^N}$ para $i = 1, \ldots, r$.
2. $det(D(F))(X_1, \ldots, X_{n-r}, R^{(\xi,N)}) \notin m$

Estas afirmaciones se demuestran por inducción en N. En el caso $N = 0$, las afirmaciones 1 y 2 son las hipótesis del lema.

En el caso general, suponiendo ambas afirmaciones ciertas para el caso N, se considera los polinomios $F_1, \ldots, F_r$ como elementos del anillo de polinomios $\mathbf{C}[X_1, \ldots, X_{n-r}][X_{n-r+1}, \ldots, X_n]$. Con un leve abuso de notación se utilizará el mismo símbolo, F_i, para denotar el elemento de $\mathbf{C}[X_1, \ldots, X_n]$ o su imagen en el anillo $\mathbf{C}[X_1, \ldots, X_{n-r}][X_{n-r+1}, \ldots, X_n]$.

Sean $Y_{n-r+1}, \ldots, Y_n$ nuevas indeterminadas. A partir de un desarrollo formal de Taylor de los polinomios $F_1, \ldots, F_r$ en torno a $Y_{n-r+1}, \ldots, Y_n$, se obtiene la siguiente identidad en el $\mathbf{C}[X_1, \ldots, X_{n-r}]$-módulo $\mathbf{C}[X_1, \ldots, X_{n-r}][X_{n-r+1}, \ldots, X_n, Y_{n-r+1}, \ldots, Y_n]$:

$$F_i(X_{n-r+1}, \ldots, X_n) = F_i(Y_{n-r+1}, \ldots, Y_n) +$$

$$+ \sum_{j=1}^{r} \frac{\partial F_i}{\partial X_{n-r+j}}(Y_{n-r+1}, \ldots, Y_n) \cdot (X_{n-r+j} - Y_{n-r+j})$$

$$\text{módulo } (X_{n-r+1} - Y_{n-r+1}, \ldots, X_n - Y_n)^2 \tag{2.3}$$

para $i = 1, \ldots, r$, donde $(X_{n-r+1} - Y_{n-r+1}, \ldots, X_n - Y_n)$ denota el ideal generado por los polinomios $X_{n-r+1} - Y_{n-r+1}, \ldots, X_n - Y_n$ en

$\mathbf{C}[X_1,\ldots,X_{n-r}][X_{n-r+1},\ldots,X_n,Y_{n-r+1},\ldots,Y_n]$.

Utilizando la inclusión

$$\mathbf{C}[X_1,\ldots,X_{n-r}] \hookrightarrow \mathbf{C}[\![X_1-p_1,\ldots,X_{n-r}-p_{n-r}]\!]$$

dada por el desarrollo de Taylor de cada polinomio $F \in \mathbf{C}[X_1,\ldots,X_{n-r}]$ en torno al punto $(p_1,\ldots,p_{n-r})$ y reemplazando en la ecuación (2.3) las variables $X_{n-r+1},\ldots,X_n$ por $R_{n-r+1}^{(\xi,N+1)},\ldots,R_n^{(\xi,N+1)}$ e $Y_{n-r+1},\ldots,Y_n$ por $R_{n-r+1}^{(\xi,N)},\ldots,R_n^{(\xi,N)}$, se obtiene la siguiente identidad en $\mathbf{C}[\![X_1-p_1,\ldots,X_{n-r}-p_{n-r}]\!]$:

$$F_i(R^{(\xi,N+1)}) = F_i(R^{(\xi,N)}) + \sum_{j=1}^{r} \frac{\partial F_i}{\partial X_{n-r+j}}(R^{(\xi,N)}) \cdot (R_{n-r+j}^{(\xi,N+1)} - R_{n-r+j}^{(\xi,N)})$$

$$\text{módulo } (R_{n-r+1}^{(\xi,N+1)} - R_{n-r+1}^{(\xi,N)},\ldots,R_n^{(\xi,N+1)} - R_n^{(\xi,N)})^2 \tag{2.4}$$

De la definición de $R^{(\xi,N)}$ resulta:

$$R^{(\xi,N+1)} - R^{(\xi,N)} = -D(F)^{-1}(R^{(\xi,N)}) \cdot \begin{pmatrix} F_1(R^{(\xi,N)}) \\ \vdots \\ F_r(R^{(\xi,N)}) \end{pmatrix}$$

En consecuencia, multiplicando ambos miembros de esta identidad por el vector $\left(\frac{\partial F_i}{\partial X_{n-r+1}}(R^{(\xi,N)}),\ldots,\frac{\partial F_i}{\partial X_{n-r+1}}(R^{(\xi,N)})\right)$ (que constituye la i-ésima fila de la matriz $D(F)(R^{(\xi,N)})$), se tiene la siguiente ecuación:

$$\left(\frac{\partial F_1}{\partial X_{n-r+1}}(R^{(\xi,N)}),\ldots,\frac{\partial F_r}{\partial X_{n-r+1}}(R^{(\xi,N)})\right)\cdot(R^{(\xi,N+1)}-R^{(\xi,N)})^t =$$

$$\left(\frac{\partial F_1}{\partial X_{n-r+1}}(R^{(\xi,N)}),\ldots,\frac{\partial F_r}{\partial X_{n-r+1}}(R^{(\xi,N)})\right)\cdot\left(-D(F)^{-1}(R^{(\xi,N)})\right)\cdot\begin{pmatrix} F_1(R^{(\xi,N)}) \\ \vdots \\ F_r(R^{(\xi,N)}) \end{pmatrix}$$

$$= -(0,\ldots,\overset{i}{1},0,\ldots,0)\cdot\begin{pmatrix} F_1(R^{(\xi,N)}) \\ \vdots \\ F_r(R^{(\xi,N)}) \end{pmatrix} = -F_i(R^{(\xi,N)})$$

Por lo tanto, reemplazando esta última identidad en (2.4) se obtiene:

$$F_i(R^{(\xi,N+1)}) = F_i(R^{(\xi,N)}) +$$

$$+\Big(\frac{\partial F_1}{\partial X_{n-r+1}}(R^{(\xi,N)}),\ldots,\frac{\partial F_r}{\partial X_{n-r+1}}(R^{(\xi,N)})\Big)\cdot$$

$$\cdot(-D(F)^{-1}(R^{(\xi,N)}))\cdot\begin{pmatrix}F_1(R^{(\xi,N)})\\ \vdots \\ F_r(R^{(\xi,N)})\end{pmatrix} =$$

$$= F_i(R^{(\xi,N)}) - F_i(R^{(\xi,N)}) = 0$$

$$\text{módulo}(R_{n-r+1}^{(\xi,N+1)} - R_{n-r+1}^{(\xi,N)},\ldots,R_n^{(\xi,N+1)} - R_n^{(\xi,N)})^2$$

de donde se deduce que

$$F_i(R^{(\xi,N+1)}) \in (R_{n-r+1}^{(\xi,N+1)} - R_{n-r+1}^{(\xi,N)},\ldots,R_n^{(\xi,N+1)} - R_n^{(\xi,N)})^2$$

para $i = 1,\ldots,r$. Ahora bien, como

$$(R^{(\xi,N+1)} - R^{(\xi,N)})^t = -D(F)^{-1}(R^{(\xi,N)})\cdot\begin{pmatrix}F_1(R^{(\xi,N)})\\ \vdots \\ F_r(R^{(\xi,N)})\end{pmatrix}$$

y $F_i(R^{(\xi,N)}) \in m^{2^N}$ para $i = 1,\ldots,r$ por hipótesis inductiva, resulta entonces que

$$(R_{n-r+1}^{(\xi,N+1)} - R_{n-r+1}^{(\xi,N)},\ldots,R_n^{(\xi,N+1)} - R_n^{(\xi,N)})^2 \subseteq (m^{2^N})^2 = m^{2^{N+1}}$$

lo que demuestra la primera afirmación.

Con respecto a la segunda afirmación, realizando un desarrollo de Taylor formal del polinomio $det(D(F))$ como en (2.3), se tiene la siguiente expresión:

$$det(D(F))(X_{n-r+1},\ldots,X_n) = det(D(F))(Y_{n-r+1},\ldots,Y_n) +$$

$$+\sum_{j=1}^{r}\frac{\partial det(D(F))}{\partial X_{n-r+j}}(Y_{n-r+1},\ldots,Y_n)\cdot(X_{n-r+j} - Y_{n-r+j})$$

$$\text{módulo } (X_{n-r+1} - Y_{n-r+1},\ldots,X_n - Y_n)^2$$

Si se reemplaza en esta ecuación, del mismo modo que en (2.4), las variables $X_{n-r+1},\ldots,X_n$ por $R^{(\xi,N+1)}_{n-r+1},\ldots,R^{(\xi,N+1)}_n$ y las variables $Y_{n-r+1},\ldots,Y_n$ por $R^{(\xi,N)}_{n-r+1},\ldots,R^{(\xi,N)}_n$ se obtiene la siguiente identidad:

$$det(D(F))(R^{(\xi,N+1)}) = det(D(F))(R^{(\xi,N)}) +$$

$$+\sum_{j=1}^{r}\frac{\partial det(D(F))}{\partial X_{n-r+j}}(\xi^{(N)})(R^{(\xi,N+1)}_{n-r+j}) - R^{(\xi,N)}_{n-r+j})$$

$$\text{módulo } (R^{(\xi,N+1)}_{n-r+1} - R^{(\xi,N)}_{n-r+1},\ldots,R^{(\xi,N+1)}_n - R^{(\xi,N)}_n)^2$$

Dado que se verifica que $R^{(\xi,N+1)}_{n-r+j} - R^{(\xi,N)}_{n-r+j} \in m^{2^N} \subseteq m$ para $j = 1,...,r$ y $det(D(F))(R^{(\xi,N)}) \notin m$ por hipótesis, se deduce entonces que $det(D(F))(R^{(\xi,N+1)}) \notin m$.

De las afirmaciones 1 y 2 se desprende que la sucesión $\left\{R^{(\xi,N)}_{n-r+j}\right\}_{N\in\mathbb{N}_0}$ converge en $\mathbf{C}[\![X_1,\ldots,X_{n-r}]\!]$ a una serie de potencias $R^{(\xi)}_{n-r+j}$ para $j = 1,\ldots,r$. Estas son las series de potencias cuya existencia afirma el enunciado del lema.

Denótese por $R^{(\xi)}$ el vector de series de potencias $R^{(\xi)} := (R^{(\xi)}_{n-r+1},\ldots,R^{(\xi)}_n)$. En primer lugar, dado que $R^{(\xi,N+1)}_{n-r+j} - R^{(\xi,N)}_{n-r+j} \in m^{2^N}$ para todo $N \in \mathbb{N}$, se deduce que

$$R^{(\xi)}_{n-r+j} \equiv R^{(\xi,N)}_{n-r+j} \text{ módulo } m^{2^N} \text{ para todo } N \in \mathbb{N} \tag{2.5}$$

Combinando esta observación con la ecuación (2.3), se tiene que

$$F_i(R^{(\xi)}) = F_i(\xi^{(N)}) + D(F)(R^{(\xi,N)})\begin{pmatrix} R^{(\xi)}_{n-r+1} - R^{(\xi,N)}_{n-r+1} \\ \vdots \\ R^{(\xi)}_n - R^{(\xi,N)}_n \end{pmatrix} \text{ módulo } m^{2^N}$$

para $i = 1,\ldots,r$, de donde se deduce que $F_i(R^{(\xi)}) \in m^{2^N}$ para todo $N \in \mathbb{N}$. Luego

$$F_i(R^{(\xi)}) = 0 \text{ en } \mathbf{C}[\![X_1 - p_1,\ldots,X_{n-r} - p_{n-r}]\!]$$

para $i = 1,\ldots,r$, como se quería demostrar.

En cuanto a la unicidad, suponiendo que existieran dos soluciones distintas $R^{(\xi)} := (R^{(\xi)}_{n-r+1},\ldots,R^{(\xi)}_n)$ y $\tilde{R}^{(\xi)} := (\tilde{R}^{(\xi)}_{n-r+1},\ldots,\tilde{R}^{(\xi)}_n)$ en las condiciones

del enunciado, aplicando una vez más la expresión (2.3) se obtiene:

$$F_i(R^{(\xi)}) = F_i(\tilde{R}^{(\xi)}) + D(F)(\tilde{R}^{(\xi)}) \cdot \begin{pmatrix} R^{(\xi)}_{n-r+1} - \tilde{R}^{(\xi)}_{n-r+1} \\ \\ R^{(\xi)}_n - \tilde{R}^{(\xi)}_n \end{pmatrix}$$

$$\text{módulo } (R^{(\xi)}_{n-r+1} - \tilde{R}^{(\xi)}_{n-r+1}, \ldots, R^{(\xi)}_n - \tilde{R}^{(\xi)}_n)^2$$

Como $F_i(R^{(\xi)}) = F_i(\tilde{R}^{(\xi)}) = 0$, se tiene:

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = D(F)(\tilde{R}^{(\xi)}) \cdot \begin{pmatrix} R^{(\xi)}_{n-r+1} - \tilde{R}^{(\xi)}_{n-r+1} \\ \\ R^{(\xi)}_n - \tilde{R}^{(\xi)}_n \end{pmatrix}$$

$$\text{módulo } (R^{(\xi)}_{n-r+1} - \tilde{R}^{(\xi)}_{n-r+1}, \ldots, R^{(\xi)}_n - \tilde{R}^{(\xi)}_n)^2$$

Por hipótesis, $R^{(\xi)}_{n-r+j}$ y $\tilde{R}^{(\xi)}_{n-r+j}$ tienen el mismo término constante, lo que implica que $R^{(\xi)}_{n-r+j} - \tilde{R}^{(\xi)}_{n-r+j} \in m$ para $j = 1, \ldots, r$. Como $det(D(F))(\tilde{R}^{(\xi)}) \notin m$, se deduce entonces que $R^{(\xi)}_{n-r+j} - \tilde{R}^{(\xi)}_{n-r+j} \in m^2$ para $j = 1, \ldots, r$. Iterando este razonamiento se demuestra que $R^{(\xi)}_{n-r+j} - \tilde{R}^{(\xi)}_{n-r+j} \in m^{2^N}$ para todo $N \in \mathbb{N}$ y $j = 1, \ldots, r$, lo que a su vez implica que $R^{(\xi)}_{n-r+j} = \tilde{R}^{(\xi)}_{n-r+j}$ para $j = 1, \ldots, r$, como se quería demostrar. □

Sea $V_P = \{\eta^{(1)}, \ldots, \eta^{(\delta)}\}$ donde cada $\eta^{(k)} \in \mathbb{C}^r$ y $\eta^{(i)} \neq \eta^{(j)}$ si $i \neq j$. Aplicando el lema anterior, mediante la iteración del operador de Newton comenzando con $\eta^{(k)}$ como el primer elemento de la sucesión para $k = 1, \ldots, \delta$, se obtienen δ soluciones distintas $(R^{(k)}_{n-r+1}, \ldots, R^{(k)}_n)$ en forma de series de potencias. Sea $U := \lambda_{n-r+1} X_{n-r+1} + \cdots + \lambda_n X_n$ una forma lineal de $\mathbb{Z}[X_{n-r+1}, \ldots, X_n]$ de modo tal que U representa un elemento primitivo para V y V_P. La idea es recuperar la solución geométrica de V con respecto a U a partir de la solución geométrica de V_P con respecto a U.

La clave para reconstruir la solución geométrica de V es poder calcular proyecciones de V sobre rectas: dada una forma lineal $\ell \in \mathbb{Z}[X_1, \ldots, X_n]$, la cuestión es hallar un polinomio $p_\ell \in \mathbb{Z}[X_1, \ldots, X_{n-r}, T]$, mónico en T, tal que $p_\ell(X_1, \ldots, X_{n-r}, \ell) \in (F_1, \ldots, F_r)$.

El hecho fundamental es que es posible controlar satisfactoriamente el grado del polinomio mínimo $m_\ell \in \mathbb{Z}[X_1, \ldots, X_{n-r}, T]$ que anula la forma lineal ℓ sobre V. En tal sentido, se tiene el siguiente lema:

Lema 23 ([154], Proposition 1) *Con las notaciones anteriores, dada una forma lineal $\ell \in \mathbb{Z}[X_1, \ldots, X_n]$, la ecuación de dependencia entera de grado mínimo $m_\ell \in \mathbb{Q}[X_1, \ldots, X_{n-r}, T]$ que satisface ℓ en la extensión*

$$\mathbb{Q}[X_1, \ldots, X_{n-r}] \to \mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_r)$$

es un polinomio cuyo grado total está acotado por $gr(V)$.

A partir del lema 23 se deduce que es suficiente calcular la $\lceil \log \delta \rceil$-ésima iteración del operador de Newton: dado que el polinomio minimal de cualquier forma lineal ℓ tiene grado total acotado por δ, si se conoce en forma exacta el desarrollo en series de potencias de las soluciones del sistema $(R_{n-r+1}^{(k)}, \ldots, R_n^{(k)})$ hasta grado δ se tiene toda la información necesaria para reconstruir la solución geométrica de la variedad V. Gracias a la identidad (2.5), la expansión en series de potencias de las funciones racionales que se calculan en el paso $\lceil \log(\delta) \rceil$ de iteración del operador de Newton coincide con la expansión de las soluciones exactas hasta el grado δ.

A fin de preservar la racionalidad del algoritmo la estrategia básica es representar los objetos de V_P que se necesitan mediante homotecias en el álgebra $\mathbb{Q}[V_P]$. En tal sentido, en lugar de operar con las coordenadas $\eta_{n-r+1}^{(k)}, \ldots, \eta_n^{(k)}$ de los puntos de V_P, se opera con las homotecias por $X_{n-r+1}, \ldots, X_n$ en $\mathbb{Q}[V_P]$, que se representan mediante las matrices $M_{X_{n-r+1}}^{(P)}, \ldots, M_{X_n}^{(P)}$ que describen el tensor de multiplicación en $\mathbb{Q}[V_P]$.

Sea entonces $\kappa := \lceil \log \delta \rceil$ y $g_{n-i+1}^{(\kappa)}, \ldots, g_n^{(\kappa)}, h_{n-i+1}^{(\kappa)}, \ldots, h_n^{(\kappa)}$ los numeradores y denominadores de las funciones racionales de $\mathbb{Q}[X_1, \ldots, X_n]$ que se obtienen luego de aplicar κ pasos de iteración del operador de Newton al vector $X_{n-r+1}, \ldots, X_n$.

Interpretando a $g_{n-r+1}^{(\kappa)}, \ldots, g_n^{(\kappa)}, h_{n-r+1}^{(\kappa)}, \ldots, h_n^{(\kappa)}$ como funciones de $\mathbb{Q}[X_1, \ldots, X_{n-r}][X_{n-r+1}, \ldots, X_n]$, se definen para $k = 1, \ldots, r$ las siguientes matrices:

$$\mathcal{N}_{n-r+k}^{(\kappa)} := g_{n-r+k}^{(\kappa)}(M_{X_{n-r+1}}^{(P)}, \ldots, M_{X_n}^{(P)}) \cdot h_{n-r+k}^{(\kappa)}(M_{X_{n-r+1}}^{(P)}, \ldots, M_{X_n}^{(P)})^{-1}$$

Las matrices $\mathcal{N}_{n-r+1}, \ldots, \mathcal{N}_n$ contienen toda la información necesaria para llevar a cabo el κ-ésimo paso de iteración de Newton comenzando con cada punto η_k de V_P. Dado que el número κ se ha elegido de forma tal que la aproximación se consigue es suficientemente "cercana" a la solución, a

partir de estas matrices es posible reconstruir la proyección de V en cualquier dirección ℓ. Esto es lo que se demuestra en el siguiente lema, cuya enunciado y demostración se obtiene mediante una combinación de las ideas expuestas en [81] y [78]:

Lema 24 *Sea* $\ell := \lambda_{n-r+1}X_{n-r+1} + \cdots + \lambda_n X_n$ *una forma lineal en* $\mathbb{Z}[X_{n-r+1}, \ldots, X_n]$. *Sea* $\mathcal{M}_\ell \in \mathbb{Q}(X_1, \ldots, X_{n-r})^{\delta \times \delta}$ *la siguiente matriz:*

$$\mathcal{M}_\ell := \ell(\mathcal{N}_{n-r+1}^{(\kappa)}, \ldots, \mathcal{N}_n^{(\kappa)}) = \lambda_{n-r+1}\mathcal{N}_{n-r+1}^{(\kappa)} + \cdots + \lambda_n \mathcal{N}_n^{(\kappa)}$$

y $m_\ell^{(\kappa)} := \sum_{k=1}^{\delta} b_k T^k \in \mathbb{Q}(X_1, \ldots, X_{n-r})[T]$ *el polinomio minimal de la matriz* $\mathcal{M}_\ell$. *Sea* $m_\ell = \sum_{k=1}^{\delta} a_k T^k \in \mathbb{Q}[X_1, \ldots, X_{n-r}, T]$ *el polinomio minimal de* ℓ *sobre* V *(en el sentido del lema 23). Supongamos que el punto de levantamiento* P *verifica que* $gr_T(m_\ell) = gr(m_\ell^{(P)})$. *Entonces, los coeficientes de* m_ℓ *y* $m_\ell^{(\kappa)}$ *satisfacen la siguiente condición en* $\mathbf{C}[\![X_1 - p_1, \ldots, X_{n-r} - p_{n-r}]\!]$

$$a_k \equiv b_k \text{ módulo } (X_1 - p_1, \ldots, X_{n-r} - p_{n-r})^\delta \tag{2.6}$$

para $k = 0, \ldots, \delta$.

Demostración Dado que la imagen de ℓ en $\mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_r)$ es entera respecto de $\mathbb{Q}[X_1, \ldots, X_{n-r}]$ (puesto que las imágenes de las variables $X_{n-r+1}, \ldots, X_n$ lo son y ℓ es combinación lineal de ellas), el polinomio minimal $m_\ell \in \mathbb{Q}[X_1, \ldots, X_{n-r}, T]$ es el único polinomio mónico en T y de grado mínimo en T tal que

$$m_\ell(X_1, \ldots, X_{n-r}, \ell) \in (F_1, \ldots, F_r) \tag{2.7}$$

Sean $R^{(k)} = (R_{n-r+1}^{(k)}, \ldots, R_n^{(k)})$ para $k = 1, \ldots, \delta$ las soluciones en forma de series de potencias cuya existencia se asegura en el lema 22. Reemplazando formalmente las variables $X_{n-r+1}, \ldots, X_n$ por cada $R^{(k)}$ en la identidad (2.7), se deduce que $m_\ell(T)$ tiene a cada $\ell(R^{(k)})$ como raíz para $k = 1, \ldots, \delta$.

Como $\ell(R^{(k)}) \in \mathbf{C}[\![X_1 - p_1, \ldots, X_{n-r} - p_{n-r}]\!]$ verifica para $k = 1, \ldots, \delta$ la identidad $\ell(R^{(k)})(p_1, \ldots, p_{n-r}) = \ell(\eta^{(k)})$, se deduce que el conjunto

$$\mathcal{A} := \{\ell(R^{(1)}), \ldots, \ell(R^{(\delta)})\}$$

tiene al menos tantos elementos distintos como el grado h del minimal $m_\ell^{(P)}$ de la forma lineal ℓ sobre V_P. Dado que el grado del minimal m_ℓ de ℓ sobre

V coincide con el grado de $m_\ell^{(P)}$, se deduce que $\mathcal{A}$ contiene todas las raíces de m_ℓ. Tratándose del polinomio minimal de una homotecia se deduce que éste debe ser libre de cuadrados, lo cual implica que

$$m_\ell = \prod_{k=1}^{h} (T - \ell(R^{(k)})) \tag{2.8}$$

suponiendo que $\ell(R^{(1)}), \ldots, \ell(R^{(h)})$ son los h elementos distintos de $\mathcal{A}$.

Si se nota por $R^{(k,\kappa)} = (R_{n-r+1}^{(k,\kappa)}, \ldots, R_n^{(k,\kappa)})$ el resultado que se obtiene luego de realizar la κ-ésima iteración del operador Newton-Hensel comenzando con $\eta^{(k)}$, se tiene para $k = 1, \ldots, \delta$ que

$$R^{(k)} \equiv R^{(k,\kappa)} \text{ módulo } (X_1 - p_1, \ldots, X_{n-r} - p_{n-r})^\delta$$

en $\mathbf{C}[\![X_1 - p_1, \ldots, X_{n-r} - p_{n-r}]\!]$. Si se aplica esta identidad en (2.8) se obtiene

$$m_\ell \equiv \prod_{k=1}^{h} (T - \ell(R^{(k,\kappa)})) \text{ módulo } (X_1 - p_1, \ldots, X_{n-r} - p_{n-r})^\delta$$

Sea $\sigma_j(Y_1, \ldots, Y_h)$ la j-ésima función simétrica elemental en h variables. Entonces, el j-ésimo coeficiente a_j de m_ℓ verifica que

$$a_j = (-1)^j \sigma_j(\ell(R^{(1)}), \ldots, \ell(R^{(h)}))$$

de donde se deduce que

$$a_j \equiv (-1)^j \sigma_j(\ell(R^{(1,\kappa)}), \ldots, \ell(R^{(h,\kappa)})) \text{ módulo}(X_1 - p_1, \ldots, X_{n-r} - p_{n-r})^\delta$$

en $\mathbf{C}[\![X_1 - p_1, \ldots, X_{n-r} - p_{n-r}]\!]$.

La demostración se completa ahora demostrando que

$$m_\ell^{(\kappa)} = \prod_{k=1}^{h} (T - \ell(R^{(h,\kappa)}))$$

dado que en tal caso los coeficientes b_j de $m_\ell^{(\kappa)}$ satisfarían la igualdad

$$b_j = (-1)^j \sigma_j(\ell(R^{(1,\kappa)}), \ldots, \ell(R^{(h,\kappa)}))$$

Sea U el elemento primitivo de V_P elegido y $m_U^{(P)} \in \mathbb{Q}[T]$ su polinomio minimal. Sea $M_U^{(P)}$ la matriz compañera de $m_U^{(P)}$. Obsérvese que esta matriz

representa la homotecia por U en $\mathbb{Q}[V_P]$ en la base de $\mathbb{Q}[V_P]$ formada por las potencias $\{1,\ldots,U^\delta\}$ de U.

Como U es un elemento primitivo el polinomio $m_U^{(P)}$ tiene grado δ y sus δ raíces (distintas) son $U(\eta^{(1)}),\ldots,U(\eta^{(\delta)})$. Por lo tanto, la matriz $M_U^{(P)}$ es diagonalizable y existe una matriz $P \in \mathbb{C}^{\delta\times\delta}$ inversible tal que la homotecia por U toma la forma diagonal:

$$PM_UP^{-1} = \begin{pmatrix} U(\eta^{(1)}) & 0 & & 0 \\ 0 & U(\eta^{(2)}) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & & 0 & U(\eta^{(\delta)}) \end{pmatrix}$$

Dado que se satisfacen las identidades $\rho_{n-r+k}^{(P)} X_{n-r+k} = v_{n-r+k}^{(P)}(U)$ en V_P, se tiene entonces que $M_{X_{n-r+k}} = \frac{1}{\rho_{n-r+k}}{}^{(P)} v_{n-r+k}^{(P)}(M_U)$. Como los cambios de base aplicados a una matriz conmutan con evaluaciones polinomiales de la misma, resulta entonces:

$$PM_{X_{n-r+k}}P^{-1} = \frac{1}{\rho_{n-r+k}^{(P)}} v_{n-r+k}^{(P)}(PM_UP^{-1}) =$$

$$\begin{pmatrix} \frac{1}{\rho_{n-r+k}^{(P)}} v_{n-r+k}^{(P)}(U(\eta^{(1)})) & 0 & & 0 \\ 0 & \frac{1}{\rho_{n-r+k}^{(P)}} v_{n-r+k}^{(P)}(U(\eta^{(2)})) & & 0 \\ \vdots & & & \vdots \\ 0 & & 0 & \frac{1}{\rho_{n-r+k}^{(P)}} v_{n-r+k}^{(P)}(U(\eta^{(\delta)})) \end{pmatrix}$$

$$= \begin{pmatrix} \eta_{n-r+k}^{(1)} & 0 & & 0 \\ 0 & \eta_{n-r+k}^{(2)} & & 0 \\ \vdots & & & \vdots \\ 0 & & 0 & \eta_{n-r+k}^{(\delta)} \end{pmatrix}$$

Como la matriz $\mathcal{N}_{n-r+k}$ se define en la forma:

$$\mathcal{N}_{n-r+k} = g_{n-r+k}^{(\kappa)}(M_{X_{n-r+1}}^{(P)},\ldots,X_n^{(P)}) \cdot h_{n-r+k}^{(\kappa)}(M_{X_{n-r+k}}^{(P)},\ldots,X_n^{(P)})^{-1}$$

consideraciones similares a las anteriores permiten deducir las siguientes identidades:

$$P\mathcal{N}_{n-r+k}P^{-1} = \frac{g^{(\kappa)}_{n-r+k}}{h^{(\kappa)}_{n-r+k}}(PM_{X_{n-r+1}}P^{-1},\ldots,PM_nP^{-1}) =$$

$$\begin{pmatrix} \frac{g^{(\kappa)}_{n-r+k}}{h^{(\kappa)}_{n-r+k}}(\eta^{(1)}) & 0 & & 0 \\ 0 & \frac{g^{(\kappa)}_{n-r+k}}{h^{(\kappa)}_{n-r+k}}(\eta^{(2)}) & & 0 \\ & & & \\ 0 & & 0 & \frac{g^{(\kappa)}_{n-r+k}}{h^{(\kappa)}_{n-r+k}}(\eta^{(\delta)}) \end{pmatrix} =$$

$$= \begin{pmatrix} R^{(1,\kappa)}_{n-r+k} & \cdot & 0 & 0 \\ 0 & & R^{(2,\kappa)}_{n-r+k} & 0 \\ & & & \vdots \\ 0 & & 0 & R^{(\delta,\kappa)}_{n-r+k} \end{pmatrix}$$

Finalmente, de la definición de la matriz $\mathcal{M}_\ell$ resulta:

$$P\mathcal{M}_\ell P^{-1} = \textstyle\sum_{k=1}^{r} \lambda_{n-r+k} P\mathcal{N}_{n-r+k}P^{-1} =$$

$$\begin{pmatrix} \sum_{k=1}^{r} \lambda_{n-r+k} R^{(1,\kappa)}_{n-r+k} & 0 & & 0 \\ 0 & \sum_{k=1}^{r} \lambda_{n-r+k} R^{(2,\kappa)}_{n-r+k} & & 0 \\ \vdots & & & \\ 0 & & 0 & \sum_{k=1}^{r} \lambda_{n-r+k} R^{(\delta,\kappa)}_{n-r+k} \end{pmatrix}$$

$$= \begin{pmatrix} \ell(R^{(1,\kappa)}) & 0 & & 0 \\ 0 & \ell(R^{(2,\kappa)}) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & & 0 & \ell(R^{(\delta,\kappa)}) \end{pmatrix}$$

Luego, $\mathcal{M}_\ell$ es diagonalizable y por lo tanto su minimal es el polinomio libre de cuadrados que tiene a $\ell(R^{(1,\kappa)}), \ell(R^{(2,\kappa)}), \ldots, \ell(R^{(\delta,\kappa)})$ como raíces. Pero ese polinomio es $m^{(\kappa)}_\ell = \prod_{k=1}^{h} (T - \ell(R^{(k,\kappa)}))$, como se quería demostrar. □

La forma en que se aplicará este lema es la siguiente: dada una forma lineal ℓ de la cual se quiere calcular su polinomio minimal sobre V, la idea es calcular en primer lugar el polinomio $m_\ell^{(\kappa)}$ que se enuncia en el lema. Por el lema 23 el polinomio m_ℓ buscado tiene grado total acotado por δ. Entonces el lema 24 garantiza que la expansión hasta grado δ de $m_\ell^{(\kappa)}$ coincide exactamente con el polinomio m_ℓ buscado.

2.1.5 Sobre los circuitos aritméticos

En la sección 2.1.2 se ha discutido la forma matemática y la codificación sintáctica de la salida del algoritmo para la solución geométrica que se exhibirá. Sin embargo, es también necesario discutir una codificación adecuada de la entrada y los resultados intermedios del algoritmo.

Los objetos matemáticos que se manipulan son polinomios con coeficientes enteros $F \in \mathbb{Z}[X_1, \ldots, X_n]$. Estos polinomios pueden escribirse como una lista de monomios y de esta idea resultan las dos primeras codificaciones posibles para un polinomio: la representación densa y la representación esparsa. Si el polinomio F tiene grado d y coeficientes con talla binaria acotada por h, la longitud de F bajo estas codificaciones queda acotada por $h \cdot \binom{d+n}{n}$, siendo esta cantidad de tipo d^n cuando $d \geq n$. Por lo tanto, la codificación de polinomios multivariados en representación densa o esparsa conlleva un carácter exponencial que se manifiesta negativamente en la complejidad de los procedimientos de eliminación.

Una interesante alternativa es la representación de polinomios mediante circuitos aritméticos. Desde el punto de vista de la geometría, un polinomio es también una función que puede evaluarse y, en tal sentido, las diferentes opciones para evaluar polinomio concretos pueden realizarse mediante circuitos aritméticos.

La idea de representar polinomios mediante algoritmos que realizan su evaluación tiene sus raíces en los inicios de la complejidad algebraica, donde se aplicó como un modelo para algoritmos seminuméricos (cf. [109], [172]). Entre los precursores cabe mencionar a A.M. Ostrowski, quien en 1954 se preguntó sobre la optimalidad de la regla de Horner (cf. [135]). Desde entonces, la teoría de complejidad algebraica tuvo un relevante desarrollo, fundamentalmente relacionado con las cuestiones de la estimación de *cotas inferiores* para la evaluación de polinomios y los problemas de pertenencia a conjuntos construíbles.

A fines de los años setenta se descubrió que los circuitos aritméticos pueden jugar un importante rol en eliminación. Varios autores, entre los cuales se pueden citar a J. von zur Gathen, J. Heintz, O.H. Ibarra, E. Kaltofen, S. Moran, J. Morgenstern, C.P. Schnorr, J.T. Schwartz, M. Sieveking, V. Strassen y R. Zippel entre otros, consideraron la eliminación univariada tratando de obtener el mayor beneficio de la codificación de polinomios

por circuitos aritméticos. Exiten varios trabajos que reflejan esta filosofía, como por ejemplo [76], [94], [95], [97], [98], [104], [162], [186].

A mediados de los años ochenta los circuitos aritméticos fueron aplicados al caso de la eliminación con polinomios multivariados, al influjo de las ideas desarrolladas por M. Giusti, J. Heintz, J. Morgenstern entre otros. Al respecto pueden mencionarse los siguientes trabajos: [79], [80], [65], [66], [67], [83], [114], [82], [81], [78].

Desde ya, entendiendo que la representación de polinomios mediante circuitos aritméticos puede resultar en una importante compresión de datos, la manipulación de polinomios en esta codificación resulta mas difícil de realizar. En lo que resta de la sección se desarrollarán los algoritmos necesarios para operar con polinomios representados por circuitos aritméticos.

Derivadas

Sea $F \in \mathbb{Q}[X_1, \ldots, X_n]$ un polinomio dado mediante un circuito aritmético β de talla L y profundidad no escalar ℓ. El problema consiste en calcular F y sus derivadas parciales primeras $\frac{\partial F}{\partial X_1}, \ldots, \frac{\partial F}{\partial X_n}$.

La idea es realizar el cálculo de cada derivada primera de F "paso a paso" en el circuito aritmético que calcula F. Para ello, por cada nodo ρ del grafo de computación de F se crean n nodos que contienen las derivadas primeras de la función calculada en ρ. A fin de calcular esas derivadas, basta tener en cuenta que en nodos anteriores se tienen calculadas las derivadas primeras de los nodos predecesores de ρ, por lo que el esquema de cálculo de las derivadas de la función calculada en ρ es una consecuencia directa de las reglas de derivación para funciones de tipo $f \, op \, g$ con $op \in \{+, -, \cdot, \div\}$.

Como consecuencia de la estrategia descripta, se puede concluir el siguiente resultado:

Lema 25 *Sea $F \in \mathbb{Q}[X_1, \ldots, X_n]$ un polinomio dado mediante un circuito aritmético β de talla L y profundidad no escalar ℓ. Entonçes, existe un circuito aritmético $\tilde{\beta}$ que evalúa el conjunto de polinomios $\{F, \frac{\partial F}{\partial X_1}, \ldots, \frac{\partial F}{\partial X_n}\}$ con talla $O(nL)$ y profundidad no escalar $O(\ell)$.*

El proceso descripto es lo que se conoce como el "modo directo" (forward mode) en ámbito de diferenciación automática de programas (cf. [6]). Existe un procedimiento alternativo de mejor complejidad para la diferenciación, conocido como el "modo reverso" (backward mode), cuyos orígenes pueden

situarse en un trabajo de W. Baur y V. Strassen ([10]) (ver también [84], [105], [106], [131]). Sin embargo, éste no ha sido tenido en cuenta dado que no es clara la uniformidad del mismo.

Interpolación y cálculo de componentes homogéneas

Sea nuevamente $F \in \mathbb{Q}[X_1, \ldots, X_n]$ un polinomio de grado total acotado por d, representado mediante un circuito aritmético β de talla L y profundidad no escalar ℓ. El problema ahora es hallar la descomposición de F en componentes homogéneas, es decir, se desea calcular los polinomios $F_0, \ldots, F_d \in \mathbb{Q}[X_1, \ldots, X_n]$ que verifican las siguientes propiedades:

- $F = \sum_{k=0}^{d} F_k$
- Para $k = 0, \ldots, d$, el polinomio F_k es el polinomio nulo o es homogéneo de grado k.

Claramente, es necesario evitar el cálculo de la representación densa de las componentes homogéneas de F, ya que esto podría resultar en un crecimiento exponencial de la complejidad debido a la cantidad de monomios distintos de grado d en n variables. Por esto, todas las componentes homogéneas de F se representarán por medio de un circuito aritmético.

Asimismo, a fin de evitar la introducción de parámetros enteros que puedan hacer crecer el tamaño binario de los números con que se opera, el proceso de interpolación que naturalmente aparece en el cálculo de las componentes homogéneas se reemplaza por un cálculo matricial.

La idea es la siguiente: en primer lugar se observa que $F(tX_1, \ldots, tX_n) = \sum_{k=0}^{d} t^k F_k(X_1, \ldots, X_n)$ ya que F_k es homogéneo de grado k. Esto permite reducir el problema del cálculo de las componentes homogéneas a una cuestión de interpolación (escritura) con respecto a la variable t.

Dado que $gr_t(F(tX_1, \ldots, tX_n)) \leq d$, calculando $F(tX_1, \ldots, tX_n)$ módulo t^{d+1} se obtiene nuevamente $F(tX_1, \ldots, tX_n)$. Las componentes homogéneas de F se hallarán como coordenadas de $F(tX_1, \ldots, tX_n)$ respecto de una cierta base de un espacio vectorial de dimensión finita adecuado.

Mas precisamente, se considera el $\mathbb{Q}(X_1, \ldots, X_n)$-espacio vectorial de dimensión finita $\mathbb{Q}(X_1, \ldots, X_n)[t]/(t^{d+1})$ y la base natural de este espacio vectorial dada por las potencias de t: $\mathcal{B} := \{1, t, \ldots, t^d\}$. Obsérvese que las co-

ordenadas de $F(tX_1,\ldots,tX_n)$ en base $\mathcal{B}$ son precisamente las componentes homogéneas que se desea calcular.

Para hallarlas, se considera la homotecia η_F por $F(tX_1,\ldots,tX_n)$. La matriz M_F de esta homotecia en base $\mathcal{B}$ puede hallarse fácilmente teniendo en cuenta que, si M es la matriz de la homotecia por t en base $\mathcal{B}$, entonces $M_F = F(X_1\cdot M,\ldots,X_n\cdot M)$. Finalmente, dado que $\eta_F(\bar{1}) = \overline{F(tX_1,\ldots,tX_n)}$ y $\bar{1}$ tiene coordenadas $(1,0,\ldots,0)$ en base $\mathcal{B}$, se deduce que la primer columna de la matriz M_F contiene las componentes homogéneas a calcular.

En resumen, se realizan los siguientes pasos:

- Se halla un circuito aritmético $\tilde{\beta}$ que calcula $F(tX_1,\ldots,tX_n)$, reemplazando los nodos de entrada $X_1,\ldots,X_n$ por $tX_1,\ldots,tX_n$ (agregándose además el nodo de entrada adicional t).

- Se calcula $M_F = F(X_1\cdot M,\ldots,X_n\cdot M)$ transformando $\tilde{\beta}$ en un circuito aritmético "de matrices" sustituyendo de t por M.

Obsérvese que $M = \begin{pmatrix} 0 & 0 & & 0 \\ 1 & 0 & & 0 \\ & & \ddots & \vdots \\ 0 & \ldots & 1 & 0 \end{pmatrix}$, ya que es la matriz compañera del polinomio t^{d+1}, y por lo tanto las matrices $X_1\cdot M,\ldots,X_n\cdot M$ se obtienen directamente sin realizar ninguna operación aritmética. Dado que cada nodo de $\tilde{\beta}$ se transforma en una operación de matrices de tamaño $d+1$, la talla del circuito resultante puede estimarse por $L(d+1)^3$. En conclusión, se tiene el siguiente resultado:

Lema 26 *Las componentes homogéneas de F se pueden calcular por medio de un circuito aritmético de talla $L(d+1)^3$ y profundidad no escalar ℓ.*

Cabe destacar que el proceso anterior puede aplicarse también en el caso que no se conoce una cota "a priori" del grado de F (en cuyo caso el grado de F queda acotado en forma exponencial con respecto a la profundidad no escalar ℓ) y se sólo se desea calcular las componentes homogéneas de F de grado no mayor que d.

El circuito descripto contiene un esquema de interpolación en una variable que se enuncia separadamente ya que será necesario independientemente de la descomposición en componentes homogéneas:

Lema 27 *La representación densa de F respecto de una variable puede hallarse por medio de un circuito aritmético de talla $L(d+1)^3$ y profundidad no escalar ℓ.*

Elusión de divisiones

Sean $F_0, \ldots, F_m$ polinomios de $\mathbb{Z}[X_1, \ldots, X_n]$ de grado acotado por d que se evalúan por medio de un circuito aritmético β de talla L y profundidad no escalar ℓ. Supóngase además que $F_0 \not\equiv 0$ y que F_0 divide a F_k en $\mathbb{Q}[X_1, \ldots, X_n]$ para $k = 1, \ldots, m$. El problema es calcular los polinomios $\frac{F_1}{F_0}, \ldots, \frac{F_m}{F_0}$ sin divisiones. La idea es aplicar el conocido proceso de Strassen *Vermeidung von divisionen* ([170]) en la versión de [114] a fin de controlar la altura de los parámetros que se utilizan.

Proposición 7 *Con las notaciones anteriores, existe un circuito aritmético sin divisiones $\tilde{\beta}$ de talla $O((L+d+m)d^3)$, profundidad no escalar $O(\ell + \log d)$ y parámetros de altura logarítmica acotada por $O(\log nd)$ que calcula un entero $\theta \in \mathbb{Z}$ no nulo y polinomios $P_1, \ldots, P_m$ tales que $\theta P_k = \frac{F_k}{F_0}$ para $k = 1, \ldots, m$.*

Demostración. Dado que el polinomio F_0 es no nulo y tiene grado d, existe $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}^n$ tal que $|\gamma_i| \leq 2nd$ para $i = 1, \ldots, n$ y $F_0(\gamma) \neq 0$. Por el lema 20, eligiendo las coordenadas γ_i aleatoriamente con la propiedad que $|\gamma_i| \leq 2nd$, con probabilidad mayor que $\frac{1}{2}$ se halla un punto γ de $\mathbb{Z}^n$ tal que $F_0(\gamma) \neq 0$.

Sea $\rho := F_0(\gamma)$ y $G_0, \ldots, G_m$ los polinomios de $\mathbb{Z}[X_1, \ldots, X_n]$ definidos por $G_k(X_1, \ldots, X_n) = F_k(X_1 + \gamma_1, \ldots, X_n + \gamma_n)$. Sea $Q := \rho - G_0$ (obsérvese que $Q(0, \ldots, 0) = \rho - G_0(0, \ldots, 0) = \rho - F_0(\gamma) = 0$). Todos estos polinomios se evalúan por medio de un circuito aritmético de talla $L+n+1$ y profundidad no escalar ℓ. Sea finalmente $\theta := \rho^{d+1}$.

Entonces, se tiene que

$$\frac{\theta G_k}{G_0} = \frac{\theta G_k}{\rho - Q} = \frac{1}{\rho} \frac{\theta G_k}{1 - \frac{Q}{\rho}} = \Big(\sum_{i=0}^{d} \rho^{d-i} Q^i + \sum_{i=d+1}^{\infty} \rho^{d-i} Q^i \Big) G_k \tag{2.9}$$

Dado que

$$\frac{\theta G_k(X_1, \ldots, X_n)}{G_0(X_1, \ldots, X_n)} = \frac{\theta F_k(X_1 + \gamma_1, \ldots, X_n + \gamma_n)}{F_0(X_1 + \gamma_1, \ldots, X_n + \gamma_n)} = \theta P_k$$

y $gr(F_k) \leq d$, se deduce que $gr(\frac{\theta G_k}{G_0}) \leq d$, lo cual implica que $\frac{\theta G_k}{G_0}$ sólo depende de las componentes homogéneas de grado menor o igual que d del último miembro de la identidad (2.9). Dado que $Q(0,\ldots,0) = 0$, todas las componentes homogéneas del segundo sumando del último miembro de la identidad (2.9) tienen grado mayor que d, por lo que $\frac{\theta G_k}{G_0}$ resulta igual a la suma de las componentes homogéneas de $(\sum_{i=0}^{d} \rho^{d-i} Q^i) G_k$ de grado menor o igual que d.

Para concluir, sólo resta observar que

$$P_k = \frac{\theta F_k}{F_0} = \frac{\theta G_k(X_1 - \gamma_1, \ldots, X_n - \gamma_n)}{G_0(X_1 - \gamma_1, \ldots, X_n - \gamma_n)}$$

Por lo tanto, dado que la expresión $(\sum_{i=0}^{d} \rho^{d-i} Q^i) G_k$ cuyas componentes homogéneas de grado a lo sumo d se extraen, se calcula con talla $O(L+d+m)$ y profundidad no escalar $\ell + \log d$ para $k = 1, \ldots, n$, aplicando el lema 26 se demuestra el enunciado de la proposición 7. □

La construcción de un circuito aritmético β que verifica las propiedades del enunciado de la proposición 7 se realiza determinísticamente excepto por la elección del punto $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}^n$ tal que $F_0(\gamma) \neq 0$, como puede inferirse a partir de la demostración de la proposición 7. A fin de hallar un tal punto γ, puede aplicarse el lema 20, que genera probabilísticamente un punto $\gamma \in \mathbb{Z}^n$ con probabilidad mayor que $\frac{1}{2}$ de hallar uno que verifica la condición $F_0(\gamma) \neq 0$. Se concluye que la construcción del circuito aritmético β puede realizarse probabilísticamente con probabilidad mayor que $\frac{1}{2}$ que β cumpla las condiciones requeridas por el enunciado de la proposición 7.

Construcción de un elemento primitivo

La construcción de un elemento primitivo y la solución geométrica asociada al mismo se basa en una versión algorítmica del conocido shape lemma. En esta subsubsección se sigue la estrategia desarrollada en [114] (ver también [80]), cuyos enunciados se redemuestran a fin de analizar la uniformidad de los algoritmos así obtenidos.

Cabe destacar que todos los circuitos que se describirán en esta subsubsección se componen fundamentalmente de rutinas de álgebra lineal. Por esta razón, sus "traducciones" al contexto booleano resultan uniformes.

En primer lugar se trata el caso particular de la solución geométrica de una variedad definida por dos polinomios en dos variables separadas.

Lema 28 ([114], Lemma 26) *Sea R un dominio de característica cero con cuerpo de cocientes k. Sea K la clausura algebraica de k y X, Y indeterminadas sobre K. Sean F, G polinomios en $R[T]$ libres de cuadrados en $k[T]$, $\mathcal{I} := (F(X), G(Y))$ el ideal generado por $F(X)$ y $G(Y)$ en $k[X,Y]$ y $W \subset K^2$ la variedad 0-dimensional definida por $F(X)$ y $G(Y)$. Sea $u := \alpha X + Y$ una forma lineal que constituye un elemento primitivo para W. Se nota $\delta := gr(F) \cdot gr(G)$. Entonces, existe un circuito aritmético sin divisiones de talla $\delta^{O(1)}$ y profundidad no escalar $O(\log \delta)$, consistente principalmente de operaciones de álgebra lineal con matrices de tamaño acotado por δ, que calcula polinomios $q, v_1, v_2 \in R[T]$ y un elemento $\rho \in R$ con las siguientes propiedades:*

- $gr(q) = \delta$ *y* $max\{gr(v_1), gr(v_2)\} < \delta$.
- $(q(u), \rho X - v_1(u), \rho Y - v_2(u)) \subseteq \mathcal{I}$

Demostración. Sea B la k-álgebra $B := k[X,Y]/\mathcal{I}$. Dado $h \in k[X,Y]$, se nota mediante $\overline{h}$ la clase de h en B. Es claro que B es un k-espacio vectorial de dimensión δ y que la imagen en B del conjunto

$$\mathcal{B} := \{X^i Y^j / 0 \leq i \leq gr(F) - 1, 0 \leq j \leq gr(G) - 1\}$$

define una base de B como k-espacio vectorial.

Suponiendo ordenada la base $\mathcal{B}$ por medio del orden lexicográfico con $X < Y$, las matrices $M_X, M_Y \in k^{\delta \times \delta}$ de los endomorfismos η_X y η_Y en base $\mathcal{B}$ pueden obtenerse directamente a partir de los coeficientes de F y G. Obsérvese que, siendo $a, b \in R$ los coeficientes principales de F y G respectivamente, todas las entradas de M_X y M_Y son elementos de R, o bien de la forma $\frac{r}{a}$ o de la forma $\frac{r}{b}$ para algún $r \in R$ respectivamente.

Luego, la matriz de la homotecia η_u en base $\mathcal{B}$ se obtiene directamente a partir de M_X y M_Y gracias a la identidad $M_u = \alpha \cdot M_X + M_Y$. En particular se deduce que los coeficientes que aparecen en $M_{\alpha X + Y}$ son elementos de R o tienen la forma $\frac{r}{ab}$ para algún $r \in R$.

Como u es un elemento primitivo para W, se tiene entonces que el conjunto $\mathcal{B}' := \{1, u, \ldots, u^{\delta - 1}\}$ es una base del k-espacio vectorial B.

Además, por el Teorema de Cayley-Hamilton, el polinomio característico $\chi \in k[T]$ de la matriz M_u verifica que $\chi(\eta_u)$ es el endomorfismo nulo de B. En particular $\chi(\eta_u(\bar{1})) = \chi(u) = 0$ en B, y dado que $gr(\chi) = \delta$, resulta entonces χ la ecuación minimal de u sobre B.

Obsérvese que, debido a la forma especial de la matriz M_u, los coeficientes de χ son de la forma $\frac{r}{a^i b^j}$ con $i, j \in \{0, \ldots, \delta\}$ y $r \in R$. Luego, $a^\delta b^\delta \chi$ es un polinomio en $R[T]$ que anula a la forma lineal u sobre B y tiene grado δ, lo cual implica que es el polinomio q buscado.

A fin de hallar $\rho \in R$ y los polinomios $v_1, v_2 \in R[T]$ que verifican las condiciones del enunciado del lema, dadas las bases $\mathcal{B}' := \{1, u, \ldots, u^{\delta-1}\}$ y $\mathcal{B} := \{X^i Y^j / 0 \leq i \leq gr(F) - 1, 0 \leq j \leq gr(G) - 1\}$, se tiene la relación:

$$\begin{pmatrix} 1 \\ u \\ u^2 \\ \vdots \\ u^{\delta-1} \end{pmatrix} = M_u \cdot \begin{pmatrix} 1 \\ X \\ Y \\ \vdots \\ X^{gr(F)-1} Y^{gr(G)-1} \end{pmatrix}$$

Por lo tanto, multiplicando esta identidad por la matriz adjunta de M_u tenemos:

$$Adj(M_u) \cdot \begin{pmatrix} 1 \\ u \\ u^2 \\ \vdots \\ u^{\delta-1} \end{pmatrix} = det(M_u) \cdot \begin{pmatrix} 1 \\ X \\ Y \\ \vdots \\ X^{gr(F)-1} Y^{gr(G)-1} \end{pmatrix}$$

Dado que cada coeficiente de la matriz adjunta de M_u es (salvo signos) el determinante de una submatriz de M_u de tamaño $(\delta - 1) \times (\delta - 1)$, se deduce que $(ab)^{\delta-1} Adj(M_u) = Adj(abM_u)$ es una matriz con coeficientes en R y $(ab)^\delta \cdot det(M_u)$ pertenece a R. Luego, definiendo $\rho := (ab)^\delta \cdot det(M_u)$ y $v_1(u), v_2(u)$ como los polinomios de $R[T]$ de grado menor que δ cuyo vector de coeficientes se obtiene multiplicando la segunda y tercera fila de $abAdj(abM_u)$ por $(1, u, \ldots, u^{\delta-1})$ respectivamente, se obtienen las siguientes identidades en B:

$$\rho \cdot X = v_1(u)$$
$$\rho \cdot Y = v_2(u)$$

Por último, puede utilizarse la identidad $(ab)^{\delta}\chi_{M_u}(T) = \chi_{abM_u}(abT)$ a fin de evitar divisiones durante el cálculo de $(ab)^{\delta}\chi$.

En resumen, el procedimiento puede describirse algorítmicamente de la siguiente manera:

Procedimiento 3 *Shape lemma para 2 polinomios en 2 variables separadas.*

- *Calcular los coeficientes de* abM_X *y* abM_Y.
- *Calcular los coeficientes de* $abM_{\alpha X+Y} = \alpha abM_X + abM_Y$.
- *Calcular (los coeficientes de) el polinomio característico* $\chi_{abM_{\alpha X+Y}}(T)$.
- *Calcular las potencias sucesivas* $\{1, ab, \ldots, (ab)^{\delta}\}$.
- *Calcular los coeficientes de* $\chi_{abM_{\alpha X+Y}}(abT)$ *a partir de los resultados de los dos pasos anteriores.*
- *Calcular la segunda y tercera fila de* $abAdj(abM_{\alpha X+Y})$.

Utilizando los algoritmos de la sección 1.2, se obtiene un circuito aritmético sin divisiones que calcula la solución geométrica de W con talla $\delta^{O(1)}$ y profundidad no escalar $O(\log \delta)$. □

En lo que resta de la sección se utilizarán las siguientes notaciones:

R denotará un dominio de característica cero con cuerpo de cocientes k y K la clausura algebraica de k. Asimismo, se considerarán polinomios $F_1, \ldots, F_s \in R[X_1, \ldots, X_n]$ que definen una variedad cero-dimensional V de cardinal δ sobre K^n, de modo tal que el ideal $\mathcal{I}$ generado por $F_1, \ldots, F_s$ es radical.

Siendo $T_1, \ldots, T_n$ indeterminadas sobre $K[X_1, \ldots, X_n]$, se notará por Z_j, para $j = 1, \ldots, n$, la forma lineal

$$Z_j := T_1X_1 + \cdots + T_{j-1}X_{j-1} + T_{j+1}X_{j+1} + \cdots + T_nX_n$$

. y por $\mathcal{I}_T$ el ideal generado por $F_1, \ldots, F_s$ en $k(T_1, \ldots, T_n)[X_1, \ldots, X_n]$. Sea finalmente Y una nueva indeterminada.

Lema 29 ([114], Lemma 25) *Supóngase dados los siguientes ítems:*

- *para cada* $j = 1, \ldots, n$, *un polinomio* $G_j \in R[Y]$ *libre de cuadrados en* $k[Y]$ *de grado* $gr(G_j) \leq \delta$ *tal que* $G_j(X_j)$ *pertenece a* I.

- *para cada* $j = 1, \ldots, n$, *un polinomio* $H_j \in R[T_1, \ldots, T_n][Y]$ *libre de cuadrados en* $k(T_1, \ldots, T_n)[Y]$, *mónico en* Y *salvo factores en* R *de grado* $gr_T(H_j) \leq \delta$, *tal que* $H_j(Z_j)$ *pertenece a* $\mathcal{I}_T$

Entonces, existe un circuito aritmético β *de talla* $O(n\delta^{O(1)})$ *y profundidad no escalar* $O(\log(n\delta))$ *que calcula un polinomio* $Q \in \mathbb{Z}[T_1, \ldots, T_n]$ *que verifica la siguiente propiedad: para toda upla* $(\lambda_1, \ldots, \lambda_n) \in R^n$ *tal que* $Q(\lambda_1, \ldots, \lambda_n) \neq 0$, *la forma lineal* $u := \lambda_1 X_1 + \cdots, \lambda_n X_n$ *es un elemento primitivo de* V.

Demostración. Sean $(t_1, \ldots, t_n) \in R^n$ y $x_j^{(1)}, x_j^{(2)}, z_j^{(1)}, z_j^{(2)} \in K$ tales que:

$$\begin{aligned} G_j(x_j^{(1)}) = G_j(x_j^{(2)}) = 0 \\ H_j(t_1, \ldots, t_n, z_j^{(1)}) = H_j(t_1, \ldots, t_n, z_j^{(2)}) = 0 \end{aligned} \tag{2.10}$$

La idea es que $z_j^{(1)}, z_j^{(2)}$ corresponden a valores

$$z_j^{(1)} = t_1 x_1^{(1)} + \cdots + \widehat{t_j x_j^{(1)}} + \cdots + t_n x_n^{(1)}$$

$$z_j^{(2)} = t_1 x_1^{(2)} + \cdots + \widehat{t_j x_j^{(2)}} + \cdots + t_n x_n^{(2)}$$

donde $(x_1^{(1)}, \ldots, x_n^{(1)})$ y $(x_1^{(2)}, \ldots, x_n^{(2)})$ son dos puntos distintos de V. Luego, si se quieren determinar condiciones sobre $(t_1, \ldots, t_n) \in R^n$ para que $u := t_1 X_1 + \cdots + t_n X_n$ sea un elemento primitivo para V, deberá ocurrir que

$$t_1 x_1^{(1)} + \cdots + t_n x_n^{(1)} \neq t_1 x_1^{(2)} + \cdots + t_n x_n^{(2)}$$

y por lo tanto, que

$$t_j x_j^{(1)} + z_j^{(1)} \neq t_j x_j^{(2)} + z_j^{(2)} \tag{2.11}$$

Se hallarán entonces polinomios $Q_1, \ldots, Q_n$ que verifican que, para toda n-upla $(t_1, \ldots, t_n) \in R^n$ tal que $Q_j(t_1, \ldots, t_n) \neq 0$ y pares distintos $(x_j^{(1)}, z_j^{(1)})$ y $(x_j^{(2)}, z_j^{(2)})$ que cumplen la condición (2.10), resulta $t_j x_j^{(1)} + z_j^{(1)} \neq t_j x_j^{(2)} + z_j^{(2)}$. Posteriormente se demostrará que el polinomio $Q := \prod_{j=1}^{n} Q_j$ cumple con los requisitos del enunciado del lema.

Entonces, para cada $j = 1, \ldots, n$ se reemplazan $x_j^{(1)}, x_j^{(2)}, z_j^{(1)}, z_j^{(2)}$ por nuevas indeterminadas $X_j^{(1)}, X_j^{(2)}, Z_j^{(1)}, Z_j^{(2)}$. En términos de estas indeterminadas, la condición (2.11) puede reescribirse como

$$T_j(X_j^{(1)} - X_j^{(2)}) + Z_j^{(1)} - Z_j^{(2)} \neq 0$$

Y ésta última condición se puede reescribir por medio de matrices de homotecias.

Para esto, se consideran las homotecias $\eta_{X_j^{(1)} - X_j^{(2)}}$ por $X_j^{(1)} - X_j^{(2)}$ en $k(T_1, \ldots, T_n)[X_j^{(1)}, X_j^{(2)}]/(G_j(X_j^{(1)}), G_j(X_j^{(2)}))$ y $\eta_{Z_j^{(1)} - Z_j^{(2)}}$ por $Z_j^{(1)} - Z_j^{(2)}$ en $k(T_1, \ldots, T_n)[Z_j^{(1)}, Z_j^{(2)}]/(H_j(Z_j^{(1)}), H_j(Z_j^{(2)}))$.

Del mismo modo que en el lema 28, las matrices de las homotecias $\eta_{X_j^{(1)} - X_j^{(2)}}$ y $\eta_{Z_j^{(1)} - Z_j^{(2)}}$ pueden calcularse directamente (salvo múltiplos en $R[T_1, \ldots, T_n]$) a partir de los coeficientes de G_j y H_j.

Sean $\chi_{X_j^{(1)} - X_j^{(2)}}$ y $\chi_{Z_j^{(1)} - Z_j^{(2)}}$ los polinomios característicos de estas matrices:

$$\chi_{X_j^{(1)} - X_j^{(2)}}(Y) = Y^{D_1} + a_{D_1 - 1} Y^{D_1 - 1} + \cdots + a_{m_1} Y^{m_1}$$

$$\chi_{Z_j^{(1)} - Z_j^{(2)}}(Y) = Y^{D_2} + a_{D_2 - 1} Y^{D_2 - 1} + \cdots + a_{m_2} Y^{m_2}$$

Si $m_1 = D_1$, entonces resulta

$$(X_j^{(1)} - X_j^{(2)})^{D_1} \equiv 0 \text{ módulo } \left(G_j(X_j^{(1)}), G_j(X_j^{(2)})\right)$$

Esto significa que todo par de elementos $x_j^{(1)}, x_j^{(2)} \in K$ tales que $G_j(x_j^{(1)}) = G_j(x_j^{(2)}) = 0$ verifica que $x_j^{(1)} = x_j^{(2)}$. Por lo tanto, definir $Q_j(T_1, \ldots, T_n) := 1$ será suficiente ya que, dados dos pares distintos $(x_j^{(1)}, z_j^{(1)}) \neq (x_j^{(2)}, z_j^{(2)})$ tales que $G_j(x_j^{(1)}) = G_j(x_j^{(2)}) = 0$, resulta $x_j^{(1)} = x_j^{(2)}$. Luego, para que ambos pares sean distintos deberá ocurrir que $z_j^{(1)} \neq z_j^{(2)}$, y por lo tanto, para todo $t_j \in R$ se verifica la condición (2.11).

Análogamente, en el caso $m_2 = D_2$ se tiene que

$$(Z_j^{(1)} - Z_j^{(2)})^{D_2} \equiv 0 \text{ módulo } \left(H_j(Z_j^{(1)}), H_j(Z_j^{(2)})\right)$$

lo cual significa que la condición

$$H_j(t_1, \ldots, t_n, z_j^{(1)}) = H_j(t_1, \ldots, t_n, z_j^{(2)}) = 0 \qquad (2.12)$$

implica $z_j^{(1)} = z_j^{(2)}$. Por lo tanto, dos pares distintos $(x_j^{(1)}, z_j^{(1)})$ y $(x_j^{(2)}, z_j^{(2)})$ en K^2 que cumplen (2.12) tienen su segunda coordenada igual, es decir, $z_j^{(1)} = z_j^{(2)}$, lo cual implica que $x_j^{(1)} \neq x_j^{(2)}$. Por lo tanto, siempre que $t_j \neq 0$ se cumplirá la condición (2.11), de donde se desprende que alcanza con definir $Q_j(T_1, \ldots, T_n) := T_j$.

Se analiza ahora el caso general $D_1 > m_1$ y $D_2 > m_2$. Sean

$$g_j(Y_1) := \frac{\chi_{X_j^{(1)} - X_j^{(2)}}(Y_1)}{Y_1^{m_1}}$$

$$h_j(Y_2) := \frac{\chi_{Z_j^{(1)} - Z_j^{(2)}}(Y_2)}{Y_2^{m_2}}$$

para $j = 1, \ldots, n$. Como antes, la matriz $M_{T_j Y_1 + Y_2}$ de la homotecia $\eta_{T_j Y_1 + Y_2}$ en la base monomial natural de $k(T_1, \ldots, T_n)[Y_1, Y_2]/(g_j(Y_1), h_j(Y_2))$ con el orden lexicográfico se determina directamente a partir de los coeficientes de $g_j(Y_1)$ y $h_j(Y_2)$. La idea es que esta matriz tiene como autovalores todos los posibles valores $T_j(x_j^{(1)} - x_j^{(2)}) + (z_j^{(1)} - z_j^{(2)})$. Dado que es preciso que todos estos valores sean no nulos, debe ocurrir entonces que el polinomio característico de $M_{T_j Y_1 + Y_2}$ no tiene a 0 como raíz, lo cual se traduce en la condición que el término constante del mismo, $det(M_{T_j Y_1 + Y_2})$ sea distinto de cero. Obsérvese que este polinomio no es constante, ya que, en un desarrollo en potencias de T_j del mismo, el término constante corresponde a $det(M_{Y_2})$, que es no nulo puesto que h_j no tiene a cero como raíz.

Por lo tanto, se define Q_j en la forma:

$$Q_j(T_1, \ldots, T_n) := T_j det(M_{T_j Y_1 + Y_2})$$

Se afirma que esta definición verifica lo pedido: sea $(t_1, \ldots, t_n) \in R^n$ tal que $Q_j(t_1, \ldots, t_n) \neq 0$ y dos pares en K^2 distintos $(x_j^{(1)}, z_j^{(1)})$ y $(x_j^{(2)}, z_j^{(2)})$ con las condiciones (2.10).

Si $z_j^{(1)} = z_j^{(2)}$ entonces debe ser $x_j^{(1)} \neq x_j^{(2)}$ y como $t_j \neq 0$ resulta $t_j x_j^{(1)} + z_j^{(1)}) \neq t_j x_j^{(2)} + z_j^{(2)}$. Por otro lado, esta conclusión es evidente si $x_j^{(1)} = x_j^{(2)}$ (en cuyo caso vale que $z_j^{(1)} \neq z_j^{(2)}$). De modo que se puede suponer que $x_j^{(1)} \neq x_j^{(2)}$ y $z_j^{(1)} \neq z_j^{(2)}$.

En este caso se tiene que $g_j(x_j^{(1)} - x_j^{(2)}) = 0$ y $h_j(t_1, \ldots, t_n, z_j^{(1)} - z_j^{(2)}) = 0$. Entonces $t_j(x_j^{(1)} - x_j^{(2)}) + z_j^{(1)} - z_j^{(2)}$ es raíz del polinomio característico de

$M_{t_jY_1+Y_2}$, y dado que $(t_1,\ldots,t_n)$ fue elegida de modo que el término constante de este polinomio resulte no nulo, se deduce que $t_j(x_j^{(1)}-x_j^{(2)})+z_j^{(1)}-z_j^{(2)}\neq 0$.

Resta ahora probar que para toda n-upla $(t_1,\ldots,t_n)\in R^n$ tal que $Q(t_1,\ldots,t_n)\neq 0$, la forma lineal $u := t_1X_1+\cdots+t_nX_n$ es un elemento primitivo de V.

Sean entonces $(t_1,\ldots,t_n)$ una n-upla tal que $Q(t_1,\ldots,t_n)\neq 0$ y $(x_1^{(1)},\ldots,x_n^{(1)})$, $(x_1^{(2)},\ldots,x_n^{(2)})$ dos puntos distintos de V. Luego, existe $j\in\{1,\ldots,n\}$ tal que $x_j^{(1)}\neq x_j^{(2)}$. Si se define

$$z_j^{(i)} := t_1x_1^{(i)}+\cdots+\widehat{t_jx_j^{(i)}}+\cdots+t_nx_n^{(i)}$$

para $i=1,2$, vale que

$$\begin{aligned} G_j(x_j^{(1)}) &= G_j(x_j^{(2)}) = 0\\ H_j(z_j^{(1)}) &= H_j(z_j^{(2)}) = 0\\ (x_j^{(1)},z_j^{(2)}) &\neq (x_j^{(2)},z_j^{(2)}) \end{aligned}$$

Por lo tanto, se cumplen las condiciones de la afirmación anterior, de lo cual se deduce que

$$t_1x_1^{(1)}+\cdots+t_nx_n^{(1)} = t_jx_j+z_j^{(1)} \neq t_jx_j^{(2)}+z_j^{(2)} = t_1x_1^{(2)}+\cdots+t_nx_n^{(2)}$$

Para concluir, se estima la complejidad de este proceso.

En primer lugar, se calculan los coeficientes de los polinomios característicos $\chi_{X_j^{(1)}-X_j^{(2)}}$ y $\chi_{Z_j^{(1)}-Z_j^{(2)}}$ aplicando el lema 7 con talla $O(n\delta^8\log\delta)$ y profundidad no escalar $O(\log\delta)$. Con las ideas del lema 28 en mente, si $a^{(j)}\in\mathbb{Z}$ y $b^{(j)}\in\mathbb{Z}[T_1,\ldots,T_n]$ son los coeficientes principales (en T) de G_j y H_j respectivamente, con el mismo tipo de complejidad se puede calcular $(a^{(j)})^{\delta^2}\chi_{X_j^{(1)}-X_j^{(2)}}(T)$ y $(b^{(j)})^{\delta^2}\chi_{Z_j^{(1)}-Z_j^{(2)}}(T)$ de manera que todo el proceso pueda realizarse sin divisiones.

Luego hay que determinar cual es la potencia de T correspondiente al menor coeficiente no nulo de $(a^{(j)})^{\delta^2}\chi_{X_j^{(1)}-X_j^{(2)}}(T)$ y $(b^{(j)})^{\delta^2}\chi_{Z_j^{(1)}-Z_j^{(2)}}(T)$, a fin de obtener los polinomios g_j y h_j. Para esto se utiliza el lema 20 $O(n\delta^{O(1)})$ operaciones aritméticas adicionales con profundidad no escalar $O(\log\delta)$.

Finalmente, se calculan $(ab)^{\delta^4}det(M_{T,X_j+Z_j})$, siendo M_{T,X_j+Z_j} un matriz de tamaño δ^4, con talla $O(n\delta^{16}\log\delta)$ y profundidad no escalar $O(\log\delta)$, luego

de lo cual se multiplican todos los polinomios F_j obtenidos, lo que implica una talla total de tipo $O(n\delta^{O(1)}\log\delta)$ y una profundidad no escalar $O(\log(n\delta))$, como se había enunciado. □

Este lema reduce el problema de hallar los coeficientes de una forma lineal que representa un elemento primitivo para la variedad V al del la determinación de una n-upla $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$ con la propiedad que $Q(\lambda) \neq 0$, donde Q es el polinomio del enunciado del lema 29. Mediante la aplicación de la proposición 20, esta última cuestión puede resolverse en forma probabilística.

Supuestos dados tales coeficientes, se tiene el siguiente resultado:

Lema 30 ([114], Proposition 27) *En las condiciones del lema 29, dado además un elemento primitivo $u := \lambda_1 X_1 + \cdots + \lambda_n X_n$ para V, existe un circuito aritmético β de talla $n\delta^{O(1)}$ y profundidad no escalar $O(\ell + \log\delta)$ tal que calcula elementos $\rho_1, \ldots, \rho_n \in R$ y polinomios $q, v_1, \ldots, v_n \in R[T]$ con las siguientes propiedades:*

- *$gr_T(q) = \delta$ y q verifica que $q(\lambda_1 X_1 + \cdots + \lambda_n X_n) \in \mathcal{I}$*
- *para todo $i = 1, \ldots, n$ vale que $gr(v_i) \leq \delta$ y $\rho_i X_i - v_i(u) \in \mathcal{I}$*

Demostración : Sea $Z_j := \lambda_1 X_1 + \cdots + \widehat{\lambda_j X_j} + \cdots + \lambda_n X_n$. Reemplazando las variables $(T_1, \ldots, T_n)$ por $(\lambda_1, \ldots, \lambda_n)$ en los polinomios $H_1, \ldots, H_n$ se obtienen polinomios $h_1(T) := H_1(\lambda_1, \ldots, \lambda_n, T), \ldots, h_n(T) := H_n(\lambda_1, \ldots, \lambda_n, T)$ en $R[T]$ que verifican $h_j(Z_j) \in \mathcal{I}$.

Como u es un elemento primitivo de V, en particular separa puntos de $\{G_j(X_j) = 0, h_j(Z_j)\}$. La idea es aplicar el lema 28, para lo cual es necesario previamente hallar una representación separable de los polinomios $h_j(Z_j)$. La representación separable $\tilde{h}_j(Z_j)$ de $h_j(Z_j)$ se calcula utilizando la estrategia descripta en la sección 1.3.3.

Luego se aplica el lema 28 en $k[T]/(G_j(X_j), \tilde{h}_j(Z_j))$ con $u = \lambda_j X_j + Z_j$ como elemento primitivo para $j = 1, \ldots, n$, y se obtiene un elemento $\rho_j \in R$ y polinomios $\tilde{q}_j, v_j \in R[T]$ tales que $\{\rho_j v_j(u), q_j(u)\} \subseteq (G_j(X_j), h_j(z_j)) \subseteq \mathcal{I}$.

De las estimaciones de complejidad de los lemas 18 y 28 se deduce que todo el proceso tiene talla $O(n\delta^4\log\delta)$ y profundidad no escalar $O(\log\delta)$. □

Elusión de divisiones en la iteración del operador de Newton–Hensel

A fin de producir las entradas necesarias para la aplicación de los lemas 29 y 30, se aplicará el lema 24 que reduce al caso cero-dimensional. Para esto, como ha sido dicho en la subsección 2.1.4, es necesario calcular la expansión hasta grado δ de la serie de potencias de cierta función racional.

Esta expansión se calculará mediante el proceso de "elusión de divisiones" descripto en la proposición 7. A fin de poder aplicar esta proposición, es necesario calcular la función racional involucrada con una sola división al final de todo el proceso. Dado que las divisiones provienen de cada paso de iteración con el operador de Newton–Hensel, se redefinirán las funciones racionales que intervienen en el mismo a fin de evitar divisiones en pasos intermedios.

El operador de Newton–Hensel se da como un vector de r funciones racionales de $\mathbb{Q}(X_1,\ldots,X_n)$. Lo mismo es cierto para la κ-ésima iteración de este operador, que se notará por N_F^κ. Escribiendo las r funciones racionales con un denominador común, existen entonces numeradores $(g_{n-r+1}^{(\kappa)},\ldots,g_n^{(\kappa)}) \in \mathbb{Q}[X_1,\ldots,X_n]$ y un denominador $h^{(\kappa)} \in \mathbb{Q}[X_1,\ldots,X_n]$ no nulo tales que N_F^κ puede escribirse como:

$$N_F^\kappa = \left(\frac{g_{n-r+1}^{(\kappa)}}{h^{(\kappa)}},\ldots,\frac{g_n^{(\kappa)}}{h^{(\kappa)}}\right) \in \mathbb{Q}(X_1,\ldots,X_n)^r$$

En el siguiente lema se muestra como pueden calcularse en forma uniforme sin divisiones en $\mathbb{Q}[X_1,\ldots,X_n]$ los numeradores y el denominador de N_F^κ.

Lema 31 ([78], Lemma 27) *Supuesto que $F_1,\ldots,F_r$ se representan mediante un circuito aritmético Γ sin divisiones de talla L y profundidad no escalar ℓ, es posible calcular los numeradores $g_{n-r+1}^{(\kappa)},\ldots,g_n^{(\kappa)}$ y denominador $h^{(\kappa)}$ correspondientes al κ-ésimo paso de iteración del operador de Newton–Hensel N_F^κ sin divisiones en $\mathbb{Q}[X_1,\ldots,X_n]$ por medio de un circuito aritmético de talla $L(\kappa nrd)^{O(1)}$ y profundidad no escalar $O(\kappa(\ell+\log r))$.*

Demostración. Considerando los polinomios $F_1,\ldots,F_r$ como elementos de $\mathbb{Q}[X_1,\ldots,X_{n-r}][X_{n-r+1},\ldots,X_n]$, sea $A(F) = (a_{ij})_{1\le i,j\le n}$ la matriz traspuesta de la matriz adjunta de $D(F)$. Tanto $A(F)$ como el determinante Jacobiano $J(F) := det(D(F))$ pueden evaluarse uniformemente mediante un

circuito aritmético sin divisiones de talla $O(Ln + r^{O(1)})$ y profundidad no escalar $O(\ell + \log r)$, combinando el lema 7 y el lema 25. El operador N_F puede escribirse de la manera siguiente

$$N_F = \frac{J(F)\begin{pmatrix} X_{n-r+1} \\ \vdots \\ X_n \end{pmatrix} - A(F)\begin{pmatrix} F_1(X_{n-r+1},\ldots,X_n) \\ \vdots \\ F_r(X_{n-r+1},\ldots,X_n) \end{pmatrix}}{J(F)} \tag{2.13}$$

Las entradas a_{jk} de la matriz $A(F)$ son polinomios del anillo $\mathbb{Q}[X_1,\ldots,X_n]$ de grado a lo sumo $(n-1)(d-1)$. Asimismo, el determinante Jacobiano $J(F)$ es un polinomio de $\mathbb{Q}[X_1,\ldots,X_n]$ de grado acotado por $n(d-1)$. Para $1 \leq j \leq n$ se considera

$$g_{n-r+j} := J(F)X_{n-r+j} - \sum_{k=1}^{n} a_{jk}F_k$$

Todos los polinomios que aparecen en el miembro derecho de la definición of g_{n-r+j} como sumandos tienen grado acotado por $\nu := nd+1$. Luego, el grado de cada g_{n-r+j} queda acotado por ν. Sean ${}^h g_{n-r+j}(X_0, X_1, \ldots, X_n)$ y ${}^h J(F)(X_0, X_1, \ldots, X_n)$ los polinomios de $\mathbb{Q}[X_0, X_1, \ldots, , X_n]$ que resultan de homogeneizar los polinomios g_{n-r+j} y el determinante Jacobiano $J(F)$ respecto de las variables $X_{n-r+1},\ldots,X_n$ mediante una nueva variable X_0.

Se introducen entonces los siguientes polinomios homogéneos:

- $G_{n-r+j}(X_0,\ldots,X_n) := X_0^{\nu-gr(g_j)}({}^h g_j)$,
- $H(X_0,\ldots,X_n) := X_0^{\nu-gr(J(F))}({}^h J(F))$.

Del lema 26 se deduce que es posible calcular los polinomios G_{n-r+1}, ...,G_n y H con un circuito aritmético sin divisiones en $\mathbb{Q}[X_1,\ldots,X_n]$ de talla $L(nrd)^{O(1)}$ y profundidad no escalar $O(\ell + \log r)$. Finalmente, se definen recursivamente los siguientes polinomios:

- para $k=1$ y $1 \leq j \leq r$ sean $g_{n-r+j}^{(1)} := G_{n-r+j}(1, X_{n-r+1},\ldots,X_n)$,
  $h^{(1)} := H(1, X_{n-r+1},\ldots,X_n)$

- para $k \geq 2$ y $1 \leq j \leq r$ sean $g_{n-r+j}^{(k)} := G_{n-r+j}(h^{(k-1)}, g_{n-r+1}^{(k-1)}, .., g_n^{(k-1)})$

$$h^{(k)} := H(h^{(k-1)}, g_{n-r+1}^{(k-1)}, \ldots, g_n^{(k-1)})$$

Por inducción en k se demuestra que los polinomios $g_{n-r+1}^{(k)}, \ldots, g_n^{(k)}$ son los numeradores y $h^{(k)}$ es el denominador de la k-ésima iteración del operador de Newton–Hensel N_F^k.

El circuito aritmético que evalúa $g_{n-r+1}^{(k)}, \ldots, g_n^{(k)}$ se obtiene iterando k veces el circuito aritmético (sin divisiones) que calcula $G_{n-r+1}, \ldots, G_n$ y H, resultando su talla $O(Lk(nrd)^{O(1)})$ y su profundidad no escalar $O(k(\ell + \log r))$. Dado que no se introducen nuevos parámetros por este procedimiento, poniendo $k := \kappa$ se tiene el enunciado del lema. □

Cabe destacar que el circuito aritmético descripto se compone fundamentalmente de operaciones de álgebra lineal con matrices de tamaño $r \times r$, lo cual implica que su traducción booleana puede realizarse en forma uniforme.

2.1.6 El algoritmo para el cálculo de un elemento primitivo

En esta sección se desarrollará un algoritmo que calcula un elemento primitivo para V y la solución geométrica asociado al mismo. Este algoritmo se aplica recursivamente a las variedades $V_i := V(F_1, \ldots, F_i)$ para $1 \leq i \leq n$, por lo que se describirá el i-ésimo paso de esta recursión.

Según lo desarrollado en la sección 2.1.1, se puede suponer que los polinomios input $F_1, \ldots, F_n$ forman una sucesión regular en $\mathbb{Q}[X_1, \ldots, X_n]$ y los ideales $\mathcal{I}_i$ generados por $F_1, \ldots, F_i$ en $\mathbb{Q}[X_1, \ldots, X_n]$ son radicales para todo $i = 1, \ldots, n-1$. Se asume asimismo que $(F_1, \ldots, F_n)$ es radical.

Los polinomios $F_1, \ldots, F_n \in \mathbb{Z}[X_1, \ldots, X_n]$ se representan mediante un circuito aritmético Γ en $\mathbb{Z}[X_1, \ldots, X_n]$ de talla L y profundidad no escalar ℓ con parámetros enteros de altura máxima h que evalúa $F_1, \ldots, F_n$. A fin de estimar la complejidad del i-ésimo paso recursivo del algoritmo, será necesario introducir los siguientes parámetros:

- $\delta_i := gr(V_i)$
- $\delta := max\{\delta_i : 1 \leq i \leq n\}$
- $\eta_i := ht_{V_i}(C)$, donde C es un número natural de orden $O((\log n + \ell) \log \delta)$ elegido de modo tal que $\mathbb{Q}[V_i]$ tiene un elemento primitivo de altura C con respecto a una posición de Noether adecuada para V_i
- $\eta := max\{\eta_i : 1 \leq i \leq n\}$

Sea $i \in \{1, \ldots, n\}$ fijo. A fin de simplificar las notaciones se supone que las variables $X_1, \ldots, X_n$ están en posición de Noether con respecto a la variedad V_i, siendo las variables $X_1, \ldots, X_{n-i}$ libres. También se supone dada la representación binaria de las coordenadas enteras de un punto de levantamiento P_i, de los coeficientes enteros de una forma lineal U_i que representa un elemento primitivo para V_{P_i} y de los coeficientes de los polinomios primitivos que constituyen la solución geométrica para V_{P_i} correspondiente al elemento primitivo definido por U_i. La siguiente proposición, que sigue las líneas generales de [78, Proposition 30] con la diferencia que realiza todo el proceso sin necesidad de pasar al espacio proyectivo, se describe el circuito aritmético Γ_i que realiza el i-ésimo paso recursivo del algoritmo:

Proposición 8 ([78], Theorem 28) *Existe un circuito aritmético* Γ_i *en* $\mathbb{Z}[X_1, \ldots, X_n]$ *sin divisiones de talla* $(id\delta_i L)^{O(1)}$ *y profundidad no escalar* $O((\log i + \ell)\log \delta_i)$ *que utiliza parámetros de altura logarítmica acotada por* $max\{h, \eta_i, O((\log i + \ell)\log \delta_i)\}$ *el cual, teniendo como entrada*

- *una normalización de Noether para la variedad* V_i,
- *un punto de levantamiento* P_i *para* V_i *y*
- *la solución geométrica de la fibra de levantamiento* V_{P_i}

produce como salida

- *un cambio lineal de variables* $(X_1, \ldots, X_n) \longrightarrow (Y_1, \ldots, Y_n)$ *tal que las nuevas variables* $Y_1, \ldots, Y_n$ *están en posición de Noether con respecto a* V_{i+1},
- *un punto de levantamiento* P_{i+1} *para* V_{i+1} *y*
- *una solución geométrica para la fibra de levantamiento* $V_{P_{i+1}}$.

Este circuito aritmético consiste fundamentalmente de operaciones de álgebra lineal con matrices cuyo tamaño máximo está acotado por $\delta^4 \times \delta^4$.

Demostración. El circuito aritmético Γ_i consta de dos etapas. En la primer etapa obtiene la solución geométrica de V_i a partir de la de V_{P_i}, es decir, se calculan los siguientes ítems:

- el polinomio minimal primitivo $q_i \in \mathbb{Z}[X_1, \ldots, X_{n-i}, U_i]$ del elemento primitivo u_i de la extensión de anillos:
  $R_i := \mathbb{Q}[X_1, \ldots, X_{n-i}] \longrightarrow \mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_i) =: \mathbb{Q}[V_i]$ y
- polinomios $\rho_{n-i+1}^{(i)}, \ldots, \rho_n^{(i)} \in \mathbb{Z}[X_1, \ldots, X_{n-i}]$, $\rho^{(i)} := \prod_{k=n-i+1}^{n} \rho_k^{(i)}$ y polinomios $v_{r+1}^{(i)}, \ldots, v_n^{(i)} \in \mathbb{Z}[X_1, \ldots, X_{n-i}, U_i]$ con las siguientes propiedades:
  - $max\{gr_{U_i} v_j^{(i)} \; ; \; r < j \leq n\} < \delta_i$,
  - para $k = 1, \ldots, n-i$ el polinomio $\rho_{n-i+k} X_{n-i+k} - v_{b-i+k}^{(i)}$ es primitivo, y

– se satisface la identidad:

$$(F_1,\ldots,F_i)_{\rho^{(i)}} = (q_i(U_i), \rho_{r+1}^{(i)} X_{r+1} - v_{r+1}^{(i)}(U_i), \ldots, \rho_n^{(i)} X_n - v_n^{(i)}(U_i))_{\rho^{(i)}}$$

(donde $\mathcal{I}_\rho$ denota la localización del ideal $\mathcal{I}$ por el conjunto $\{1, \rho, \ldots, \rho^k, \ldots\}$ de todas las potencias de ρ).

En la segunda etapa se interseca algorítmicamente la variedad V_i con la hipersurperficie $V(F_{i+1})$ a fin de producir:

- una normalización de Noether de las variables con respecto a la variedad $V_{i+1} = V_i \cap V(F_{i+1})$,
- un punto de levantamiento P_{i+1} para la variedad V_{i+1} y
- una forma lineal U_{i+1} que representa un elemento primitivo tanto de la extensión $R_{i+1} := \mathbb{Q}[X_1,\ldots,X_{n-i}] \longrightarrow \mathbb{Q}[X_1,\ldots,X_n]/(F_1,\ldots,F_{i+1}) =: \mathbb{Q}[V_{i+1}]$ como de la extensión $\mathbb{Q} \longrightarrow \mathbb{Q}[V_{P_{i+1}}]$, y
- la solución geométrica de $V_{P_{i+1}}$ asociada a elemento primitivo u_i inducido por U_{i+1} en $\mathbb{Q}[V_{P_{i+1}}]$.

1er. etapa:
Dado que las variables $X_1,\ldots,X_n$ están en posición de Noether con respecto a la variedad V_i, siendo las variables $X_1,\ldots,X_{n-i}$ libres, se tiene que la extensión $R_i \longrightarrow \mathbb{Q}[V_i]$ es entera.

Sea $P_i = (p_1,\ldots,p_{n-i}) \in \mathbb{Z}^{n-i}$ el punto de levantamiento dado y $V_{P_i} = \pi_i^{-1}(P_i)$ la fibra de levantamiento. Entonces se tiene que $D_i := gr(V_{P_i}) = rango_{R_i}\mathbb{Q}[V_i] \leq gr(V_i) = \delta_i$. Sea

$$U_i = \lambda_{n-i+1} X_{n-i+1} + \cdots + \lambda_n X_n \in \mathbb{Z}[X_{n-i+1},\ldots,X_n]$$

la forma lineal dada que genera un elemento primitivo de la extensión de anillos $\mathbb{Q} \longrightarrow \mathbb{Q}[V_{P_i}]$ (es decir, U_i separa los puntos de V_{P_i}).

El polinomio minimal de la imagen u_i de U_i en $\mathbb{Q}[V_i]$ tiene grado mayor o igual que la cardinalidad del conjunto $U_i(V_{P_i})$. Como U_i separa los puntos de V_{P_i}, esta cardinalidad es $gr(V_{P_i}) = rango_{R_i}\mathbb{Q}[V_i]$. Por lo tanto, el polinomio minimal m_{u_i} tiene grado D_i, lo cual significa que U_i genera también un elemento primitivo de la extensión de anillos $R_i \longrightarrow \mathbb{Q}[V_i]$.

En lo que sigue se notará indistintamente por u_i al elemento primitivo generado por U_i en las extensiones de anillos $\mathbb{Q} \longrightarrow \mathbb{Q}[V_{P_i}]$ y $R_i \longrightarrow \mathbb{Q}[V_i]$.

Por hipótesis, los siguientes ítems están dados como input:

- la ecuación minimal primitiva $\tilde{q} \in \mathbb{Z}[T]$ del elemento primitivo u_i de $\mathbb{Q}[V_{P_i}]$,

- la parametrización de V_{P_i} por los ceros de $\tilde{q}$, dada por las ecuaciones

$$X_1 - p_1 = 0, \ldots, X_{n-i} - p_{n-i} = 0, \tilde{q}(T) = 0,$$

$$\tilde{\rho}_{n-i+1} X_{n-i+1} - \tilde{v}_{n-i+1}(T) = 0, \ldots, \tilde{\rho}_n X_n - \tilde{v}_n(T) = 0,$$

donde $\tilde{v}_{n-i+1}, \ldots, \tilde{v}_n$ son polinomios de $\mathbb{Z}[T]$ de grado menor que D_i y $\tilde{\rho}_{n-i+1}, \ldots, \tilde{\rho}_n$ son números enteros no nulos tales que los polinomios $\tilde{\rho}_{n-i+1} X_{n-i+1} - \tilde{v}_{n-i+1}(T), \ldots, \tilde{\rho}_n X_n - \tilde{v}_n(T)$ son primitivos.

Sea $a \in \mathbb{Z}$ el coeficiente principal de $\tilde{q}$.

Considerando $F_1, \ldots, F_i$ como polinomios en las variables $X_{n-i+1}, \ldots, X_n$, es decir, como elementos del anillo de polinomios $R_i[X_{n-i+1}, \ldots, X_n]$, se tiene el operador de Newton-Hensel N_F para $F := (F_1, \ldots, F_i)$ introducido en la sección 2.1.4. Este operador fue definido en la forma

$$N_F = \begin{pmatrix} X_{n-i+1} \\ \vdots \\ X_n \end{pmatrix} - D(F)^{-1} \begin{pmatrix} F_1 \\ \vdots \\ F_i \end{pmatrix}.$$

donde $D(F)$ es la matriz Jacobiana de F con respecto a las variables $X_{n-i+1}, \ldots, X_n$, es decir:

$$D(F) := \left(\frac{\partial F_k}{\partial X_j} \right)_{\substack{1 \le k \le i \\ n-i+1 \le j \le n}}$$

Del lema 31 se deduce la existencia de numeradores $g_{n-i+1}^{(\kappa)}, \ldots, g_n^{(\kappa)}$ y un denominador no nulo $h^{(\kappa)}$ en el anillo de polinomios $R_i[X_{n-i+1}, \ldots, X_n]$ tal que la κ-ésima iteración del operador de Newton-Hensel es de la forma:

$$N_F^{\kappa} = \begin{pmatrix} \frac{g_{n-i+1}^{(\kappa)}}{h} \\ \vdots \\ \frac{g_n^{(\kappa)}}{h^{(\kappa)}} \end{pmatrix}$$

Sean $M_{X_{n-i+1}}, \ldots, M_{X_n}$ las matrices que describen el tensor de multiplicación de la $\mathbb{Q}$-álgebra $\mathbb{Q}[V_{P_i}]$. Siendo M la matriz compañera del polinomio $a^{-1}q(T) \in \mathbb{Q}[T]$, para $1 \leq j \leq i$ la siguiente identidad es inmediata:

$$\tilde{\rho}_{n-i+j} M_{X_{n-i+j}} = \tilde{v}_{n-i+j}(M)$$

Dado que $\tilde{v}_{n-i+j}$ es un polinomio de grado menor o igual que $D_i - 1$, se deduce que las matrices $\tilde{\rho}_{n-i+j} a^{D_i-1} M_{X_{n-i+j}}$ tienen coeficientes enteros. Siguiendo la estrategia del lema 24, sea $\kappa := 1 + log_2 \delta_i$ (nótese que $\kappa \geq 1 + log_2 D_i$). El circuito aritmético Γ_i ejecuta κ iteraciones del operador de Newton–Hensel en forma simbólica de la siguiente manera: Γ_i calcula numeradores y denominadores de las matrices $N_{n-i+1}, \ldots, N_n$ con entradas en $\mathbb{Q}(X_1, \ldots, X_{n-i})$ definidas por:

$$N_{n-i+k} := \frac{g^{(\kappa)}_{n-i+k}(X_1, \ldots, X_{n-i}, \underline{M})}{h^{(\kappa)}(X_1, \ldots, X_{n-i}, \underline{M})}$$

donde $\underline{M} = (M_{X_{n-i+1}}, \ldots, M_{X_n})$ y $g^{(\kappa)}_{n-i+1}, \ldots, g^{(\kappa)}_n$ son los numeradores y $h^{(\kappa)}$ el denominador del lema 31 (es decir, $N_{n-i+1}, \ldots, N_n$ son las matrices que resultan de aplicar κ pasos de iteración del operador de Newton a las matrices $M_{X_{n-i+1}}, \ldots, M_{X_n}$).

A partir de éstas, se obtiene la matriz

$$\mathcal{M} := U_i(N_{n-i+1}, \ldots, N_n) = \lambda_{n-i+1} N_{n-i+1} + \cdots + \lambda_n N_n$$

con coeficientes en $\mathbb{Q}(X_1, \ldots, X_{n-i})$ cuyo polinomio característico χ permite hallar una ecuación que anula a u_i en $\mathbb{Q}[V_i]$ (ver lema 24).

A fin de evaluar los coeficientes del polinomio característico χ de $\mathcal{M}$ *sin divisiones* por polinomios de $\mathbb{Q}[X_1, \ldots, X_n]$ en pasos intermedios, es necesario retomar la demostración del lema 31: los polinomios $g^{(\kappa)}_{n-i+1}, \ldots, g^{(\kappa)}_n, h^{(\kappa)}$ se definen a partir de polinomios homogéneos

$$G_{n-i+1}(X_0, \ldots, X_n), \ldots, G_n(X_0, \ldots, X_n), H(X_0, \ldots, X_n)$$

del mismo grado, siguiendo las siguientes reglas:

- para $k = 1$ y $1 \leq j \leq i$, $g^{(1)}_{n-i+j} := G_{n-i+j}(1, X_{n-i+1}, \ldots, X_n)$,
  $h^{(1)} := H(1, X_{n-i+1}, \ldots, X_n)$

- para $k \geq 2$ y $1 \leq j \leq i$, $g_{n-i+j}^{(k)} := G_{n-i+j}(h^{(k-1)}, g_{n-i+j}^{(k-1)}, \ldots, g_n^{(k-1)})$,
$$h^{(k)} := H(h^{(k-1)}, g_{n-i+j}^{(k-1)}, \ldots, g_n^{(k-1)})$$

Dado que los polinomios G_{n-i+j} y H son homogéneos del mismo grado, la fracción $\frac{G_{n-i+j}}{H}(X_0, X_{n-i+1}, \ldots, X_n)$ no varía si se reemplaza el vector $(X_0, X_{n-i+1}, \ldots, X_n)$ por cualquier múltiplo escalar del mismo. Entonces, si se define $\tilde{\rho}^{(i)} := \prod_{j=1}^{i} \tilde{\rho}_{n-i+j}$, comenzando el primer paso con las funciones:

para $1 \leq j \leq i$, $g_{n-i+j}^{(1)} := G_{n-i+j}(a^{D_i-1}\tilde{\rho}^{(i)}, a^{D_i-1}\tilde{\rho}^{(i)}X_{n-i+1}, \ldots, a^{D_i-1}\tilde{\rho}^{(i)}X_n)$

$$h^{(1)} := H(a^{D_i-1}\tilde{\rho}^{(i)}, a^{D_i-1}\tilde{\rho}^{(i)}X_{n-i+1}, \ldots, a^{D_i-1}\tilde{\rho}^{(i)}X_n)$$

la sucesión de funciones racionales $\frac{g_{n-i+1}^{(k)}}{h^{(k)}}$ coincide con la definida anteriormente. Esta nueva sucesión tiene la ventaja de estar en términos de los polinomios $\tilde{\rho}^{(i)}X_{n-i+j}$, cuyo tensor de multiplicación en $\mathbb{Q}[V_{P_i}]$ se tiene sin divisiones por polinomios de $\mathbb{Q}[X_1, \ldots, X_n]$ y con coeficientes enteros.

Por lo tanto, si se calcula la siguiente sucesión

- para $k = 1$ y $1 \leq j \leq i$ sean $g_{n-i+j}^{(1)} := G_{n-i+j}(a^{D_i-1}\tilde{\rho}^{(i)}, Y_{n-i+1}, \ldots, Y_n)$,
$$h^{(1)} := H(a^{D_i-1}\tilde{\rho}^{(i)}, Y_{n-i+1}, \ldots, Y_n)$$

- para $k \geq 2$ y $1 \leq j \leq i$ sean $g_{n-i+j}^{(k)} := G_{n-i+j}(h^{(k-1)}, g_{n-i+j}^{(k-1)}, \ldots, g_n^{(k-1)})$,
$$h^{(k)} := H(h^{(k-1)}, g_{n-i+j}^{(k-1)}, \ldots, g_n^{(k-1)})$$

las funciones resultantes del κ-ésimo paso verifican:

$$\begin{pmatrix} \frac{g_{n-i+1}^{(\kappa)}}{h^{(\kappa)}}(a^{D_i-1}\tilde{\rho}^{(i)}X_{n-i+1}, \ldots, a^{D_i-1}\tilde{\rho}^{(i)}X_n) \\ \vdots \\ \frac{g_n^{(\kappa)}}{h^{(\kappa)}}(a^{D_i-1}\tilde{\rho}^{(i)}X_{n-i+1}, \ldots, a^{D_i-1}\tilde{\rho}^{(i)}X_n) \end{pmatrix} = N_F^{\kappa} \begin{pmatrix} X_{n-i+1} \\ \vdots \\ X_n \end{pmatrix}$$

De aquí se deduce que las matrices que las matrices $g_{n-i+k}^{(\kappa)}(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M})$ para $k = 1, \ldots, i$ y $h^{(\kappa)}(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M})$ pueden utilizarse a fin de expresar las matrices $N_{n-i+1}, \ldots, N_n$ sin divisiones. En consecuencia, la matriz $\mathcal{M}$ se puede escribir en la forma:

$$\mathcal{M} = \left(\lambda_{n-i+1} g_{n-i+1}^{(\kappa)}(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M}) + \cdots + \lambda_n g_n^{(\kappa)}(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M})\right) \cdot h(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M})^{-1}$$

Para evitar las divisiones en el cálculo de los coeficientes de χ que se producirían si $\mathcal{M}$ se calcula mediante el esquema de la identidad anterior, sea $\theta := det(h(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M})) \in R_i$ y $\mathcal{M}_1$ la matriz con coordenadas en R_i definida por $\mathcal{M}_1 := \theta\mathcal{M}$. Entonces, se tienen las siguientes identidades:

$$det(T \cdot Id_{D_i} - \mathcal{M}) = det(T \cdot Id_{D_i} - \theta^{-1}\mathcal{M}_1) = \theta^{-D_i} det((\theta T)Id_{D_i} - \mathcal{M}_1).$$

Sea $\phi(T) = T^{D_i} + \phi_{D_i-1}T^{D_i-1} + \cdots + \phi_0 \in R_i[T]$ el polinomio característico de $\mathcal{M}_1$. De las identidades anteriores se deduce que para $0 \leq k \leq D_i - 1$ el k-ésimo coeficiente de χ puede escribirse como

$$a_k = \frac{\theta^k \phi_k}{\theta^{D_i}} \tag{2.14}$$

Por lo tanto, en lugar de calcular los coeficientes a_k se calculan los coeficientes ϕ_k, los cuales poseen toda la información necesaria para recuperar los a_k mediante la identidad (2.14).

Sea ahora $m_{u_i} := T^{D_i} + b_{D_i-1}T^{D_i-1} + \cdots + b_0$. A partir de las relaciones de congruencia (2.6) se concluye que los coeficientes a_k del polinomio χ verifican la siguiente propiedad:

$$a_k \equiv b_k \text{ módulo } (X_1 - p_1, \ldots, X_{n-i} - p_{n-i})^{\delta_i}$$

Asimismo, el lema 23 asegura que los grados de los coeficientes b_k del polinomio minimal $m_{u_i} \in R_i[T]$ están acotados por δ_i. Por lo tanto, el desarrollo hasta grado δ_i del polinomio a_k es precisamente el polinomio b_k buscado para $k = 0, \ldots, D_i - 1$. Dado que a_k se tiene como cociente de dos polinomios con coeficientes enteros, la escritura de a_k se recupera por medio de la proposición 7.

Resta estimar la complejidad de este proceso. En primer lugar, es necesario tener los numeradores y el denominador correspondiente al $\kappa = 1 + log_2\delta_i$ paso de iteración del operador de iteración de Newton-Hensel, que se calculan según el esquema descripto en el lema 2.1.6, con talla $Ldi^{O(1)}\log\delta_i$ y profundidad no escalar $O(\log\delta_i(\ell + \log i))$. Asimismo, la matriz aM y las matrices $a^{D_i-1}\tilde{\rho}^{(i)}M_{X_{n-i+1}}, \ldots, a^{D_i-1}\tilde{\rho}^{(i)}M_{X_n}$ se obtienen de la manera siguiente: siendo $V_{n-i+j}(X_0, T)$ la homogeinización de $\tilde{v}_{n-i+j}$ con variable X_0, entonces se tiene

$$\Big(\prod_{k\neq j}\tilde{\rho}_{n-i+k}\Big)a^{D_i-1-gr(\tilde{v}_{n-i+j})}V_{n-i+j}(a, aM) = a^{D_i-1}\tilde{\rho}^{(i)}M_{X_{n-i+j}}$$

Por lo tanto, aM, $a^{D_i-1}\tilde{\rho}^{(i)}M_{X_{n-i+1}},\ldots,a^{D_i-1}\tilde{\rho}^{(i)}M_{X_n}$ se calculan con talla $O(i\delta_i^3)$ y profundidad no escalar $O(\log i+\log\delta_i)$.

A partir de estos datos se calculan las matrices $g_{n-i+1}^{(\kappa)}(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M}),\ldots,$ $g_n^{(\kappa)}(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M})$ y $h^{(\kappa)}(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M})$ evaluando el circuito aritmético que calcula $g_{n-i+1}^{(\kappa)},\ldots,g_n^{(\kappa)}$ y $h^{(\kappa)}$ en $a^{D_i-1}\tilde{\rho}^{(i)}M_{X_{n-i+1}},\ldots,a^{D_i-1}\tilde{\rho}^{(i)}M_{X_n}$, y se calcula también $\theta=det(h(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M}))$. Esto requiere $Ld(i\delta_i)^{O(1)}$ operaciones aritméticas con profundidad no escalar $O(\log\delta_i(\ell+\log i))$.

Luego, la matriz $\mathcal{M}_1$ se calcula por medio de la identidad:

$$\mathcal{M}_1=\theta\mathcal{M}=$$
$$=(\lambda_{n-i+1}g_{n-i+1}^{(\kappa)}+\cdots+\lambda_n g_n^{(\kappa)})(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M})\cdot Adj(h(a^{D_i-1}\tilde{\rho}^{(i)}\underline{M}))$$

y los coeficientes ϕ_k del polinomio característico de $\mathcal{M}_1$ se calculan sin divisiones vía el lema 7, con talla $Ld(i\delta_i)^{O(1)}$ y profundidad no escalar $O(\log\delta_i(\ell+\log i))$.

Finalmente se utiliza la proposición 7 a fin de evitar divisiones en el cálculo de $\frac{\theta^k\phi_k}{\theta^{D_i-1}}$ y se calcula el máximo común divisor del contenido de $g_0,\ldots,g_{D_i-1}$, para luego dividir por éste número a $g_0,\ldots,g_{D_i-1}$ y obtener así el polinomio minimal primitivo $q_i\in\mathbb{Z}[X_1,\ldots,X_{n-i},T]$ buscado.

Dado que los cálculos de máximo común divisor entero exigen ramificaciones, se tiene una red aritmética sin divisiones Γ_i' en $\mathbb{Z}[X_1,\ldots,X_{n-i}]$ de talla $Ld(i\delta_i)^{O(1)}$ y profundidad no escalar $O((\log i+\ell)\log\delta_i)$ que utiliza como parámetros las coordenadas $p_1,\ldots,p_{n-i}$ de P_i, los coeficientes del cambio de coordenadas de la normalización de Noether para V_i, los números enteros que aparecen como coeficientes en la solución geométrica de la fibra de levantamiento V_{P_i} y los parámetros de Γ.

El cálculo de las parametrizaciones $v_{n-i+1}^{(i)},\ldots,v_n^{(i)}\in\mathbb{Q}[X_1,\ldots,X_{n-i},T]$, se realiza combinando el esquema del circuito Γ_i' y la estrategia del lema 30. Para aplicar el lema 30 es necesario calcular el polinomio minimal $m_{X_{n-i+k}}$ de las imágenes de las variables X_{n-i+k} en $\mathbb{Q}[V_i]$ y el polinomio minimal $m_{Z_{n-i+k}}$ de las imágenes de las formas lineales $Z_{n-i+k}:=T_{n-i+1}X_{n-i+1}+\cdots+T_{n-i+k}\widehat{X}_{n-i+k}+\cdots+T_nX_n$ en $\mathbb{Q}[V_i]\otimes\mathbb{Q}(T_{n-i+1},\ldots,T_n)$ para $k=1,\ldots,i$.

Dado que los endomorfismos que se consideran son homotecias, sus polinomios minimales se obtienen mediante una representación separable de su polinomio característico. A fin de calcular tales ecuaciones se utilizan los polinomios característicos de las matrices N_{n-i+k} anteriormente definidas y

los polinomios característicos de las matrices

$$N_{n-i+k}^{(Z)} := Z_{n-i+k}(N_{n-i+k}, \ldots, N_n)$$

El cálculo de estos polinomios característicos sigue los lineamientos del cálculo de polinomio característico χ de la matriz $\mathcal{M}$: en lugar de calcularlos directamente, a fin de evitar divisiones se calcula el polinomio característico de un múltiplo adecuado de las matrices a considerar.

Posteriormente, la representación separable de estos polinomios característicos se calcula utilizando la estrategia de la sección 1.3.3 a fin de evitar divisiones. De esta manera los coeficientes de los polinomio minimales buscados se obtienen por un circuito aritmético que tiene solamente una división al final del proceso. Por lo tanto, la proposición 7 permite calcular la expansión exacta de los coeficientes de los polinomios minimales hasta grado δ_i, que por el lema 23 resultan los coeficientes buscados.

Finalmente, operando como en el lema 30 se obtienen las parametrizaciones asociadas a las variables X_{n-i+k} y se completa la primera etapa. Obsérvese que el circuito aritmético en cuestión tiene talla $(id\delta_i L)^{O(1)}$ y profundidad no escalar $O(log(d\delta_i) + \ell)$ con parámetros of altura logarítmica acotada por $O(log(d\delta_i) + \ell)$.

2da. etapa:
La segunda etapa se comienza con el cálculo de una normalización de Noether de las variables respecto de V_{i+1}. Esta posición consiste de un cambio lineal de las variables $X_1, \ldots, X_n$ (que se suponen normalizadas respecto de V_i) en nuevas variables $Y_1, \ldots, Y_n$ de forma tal que se cumplen los siguientes requisitos:

- $Y_1, \ldots, Y_{n-i-1}$ son libres respecto de V_{i+1}
- la siguiente extensión de anillos es entera

$$R_{i+1} := \mathbb{Q}[Y_1, \ldots, Y_{n-i-1}] \longrightarrow \mathbb{Q}[Y_1, \ldots, Y_n]/(F_1, \ldots, F_{i+1})$$

- las coordenadas del cambio de coordenadas son enteras

Para tal fin, se considera la imagen de F_{i+1} en $\mathbb{Q}[V_i]$, y la homotecia que éste elemento define. El polinomio minimal $m_{F_{i+1}}$ de esta homotecia tiene su término constante no nulo, ya que F_{i+1} no es divisor de cero en $\mathbb{Q}[V_{i+1}]$. Y este

término constante $a_0(X_1,\ldots,X_{n-i})$ constituye una relación de dependencia de las variables $X_1,\ldots,X_{n-i}$ en $\mathbb{Q}[V_{i+1}]$: dado que $m_{F_{i+1}}(F_{i+1}) \equiv 0$ en $\mathbb{Q}[V_i]$, se tiene que

$$F_{i+1}^{D_i} + a_{D_i-1}F_{i+1}^{D_i-1} + \cdots + a_0 \equiv 0$$

en $\mathbb{Q}[V_i]$. Por lo tanto, $a_0 \equiv 0$ en $\mathbb{Q}[V_{i+1}]$.

Si se realiza un cambio de variables

$$(X_1,\ldots,X_{n-i}) \to (Y_1,\ldots,Y_{n-i})$$

de modo tal que a_0 resulte mónico en Y_{n-i}, se tendrá entonces que Y_{n-i} es entera respecto de $Y_1,\ldots,Y_{n-i-1}$. Dado que las variables $X_{n-i+1},\ldots,X_n$ eran enteras respecto de $X_1,\ldots,X_{n-i}$ en $\mathbb{Q}[V_i]$ también lo son en $\mathbb{Q}[V_{i+1}]$, y por lo tanto $X_{n-i+1},\ldots,X_n$ son enteras respecto de $Y_1,\ldots,Y_{n-i}$ en $\mathbb{Q}[V_{i+1}]$. Pero además Y_{n-i} es entera respecto de $Y_1,\ldots,Y_{n-i+1}$, de donde se deduce que las variables $Y_{n-i}, X_{n-i+1},\ldots,X_n$ son enteras respecto de $Y_1,\ldots,Y_{n-i-1}$ en $\mathbb{Q}[V_{i+1}]$, lo cual implica que las variables $Y_1,\ldots,Y_{n-i},X_{n-i+1},\ldots,X_n$ están en posición de Noether respecto de V_{i+1}.

Entonces, para obtener el cambio de variables buscado es necesario calcular el término constante a_0 del polinomio minimal $m_{F_{i+1}}$ de F_{i+1} respecto de $\mathbb{Q}[V_i]$.

Como la extensión $R_i \longrightarrow \mathbb{Q}[V_i]$ es entera y R_i es un anillo íntegramente cerrado, el minimal de F_{i+1} sobre $\mathbb{Q}[V_i]$ es igual al minimal de F_{i+1} como elemento de $\mathbb{Q}(X_1,\ldots,X_{n-i})[X_{n-i+1},\ldots,X_n]/(F_1,\ldots,F_i)$. Este espacio vectorial tiene una base $\mathcal{B} := \{1, u_i,\ldots,u_i^{D_i-1}\}$, siendo u_i el elemento primitivo hallado, en la cual el tensor de multiplicación es conocido. Esto es el hecho fundamental que permite calcular los coeficientes el polinomio minimal $m_{F_{i+1}}$.

Sea ahora $A_0 \in \mathbb{Q}[X_1,\ldots,X_{n-i}]$ la componente homogénea de mayor grado de a_0, y $\gamma := (\gamma_1,\ldots,\gamma_{n-i})$ una $(n-i)$-upla que verifica que $A_0(\gamma_1,\ldots,\gamma_{n-i-1},\gamma_{n-i}) \neq 0$. Se introduce entonces el cambio de variables:

$$\begin{aligned} X_1 &= Y_1 + \gamma_1 Y_{n-i} \\ X_{n-i+1} &= Y_{n-i+1} + \gamma_1 Y_{n-i} \\ X_{n-i} &= Y_{n-i} \\ X_n &= Y_n \end{aligned}$$

Dado que el coeficiente de a_0 en el monomio $Y_{n-i}^{gr(a_0)}$ es $A_0(\gamma_1, \ldots, \gamma_{n-i}, 1)$, se deduce que el polinomio a_0 es mónico en Y_{n-i}. Por lo tanto, este cambio de variables es una normalización de Noether respecto de V_{i+1}.

A fin de calcular la componente de mayor grado A_0 de a_0, es importante observar que a_0 tiene grado acotado por $d\delta_i$:

sea Φ el morfismo de variedades algebraicas definido por:

$$\begin{array}{rcl} \Phi : V_i & \longrightarrow & \mathbb{Q}^{n-i+1} \\ (x_1, \ldots, x_n) & \longmapsto & (x_1, \ldots, x_{n-i}, F_{i+1}(x_1, \ldots, x_n)) \end{array}$$

Dado que ningún polinomio en $X_1, \ldots, X_{n-i}$ se anula sobre V_i, se deduce que $\overline{\Phi(V_i)} = V(m_{F_{i+1}})$. Por lo tanto, $gr(m_{F_{i+1}}) = gr(\overline{\Phi(V_i)}) = gr(\Phi(V_i))$ (cf. [88]).

Siendo $\overline{\Phi(V_i)}$ una hipersuperficie de $\mathbb{C}^{n-i+1}$, existe un hiperplano afín $H := \{c_1X_1 + \cdots + c_{n-i+1}X_{n-i+1} = c_0\}$ de $\mathbb{C}^{n-i+1}$ tal que el conjunto $\Phi(V_i) \cap H$ es finito y verifica: $\#\overline{\Phi(V_i)} \cap H = \#\Phi(V_i) \cap H = gr(\Phi(V_i))$.

Entonces, se tiene que

$$\Phi^{-1}(H) = \Phi^{-1}(\Phi(V_i) \cap H) =$$

$$= \{c_1X_1 + \cdots c_{n-i}X_{n-i} + c_{n-i+1}F_{i+1}(X_1, \ldots, X_n) = 0\} \cap V_i$$

Por lo tanto, aplicando la desigualdad de Bézout (ver por ejemplo [88], Theorem 1 o [70], Example 8.4.6) resulta

$$gr(\Phi^{-1}(H)) \leq gr(V_i) \cdot gr(F_{i+1})$$

Pero además se verifica que

$$gr(\Phi(V_i)) = \#(\Phi(V_i) \cap H) \leq gr(\Phi^{-1}(H))$$

ya que, siendo $\Phi^{-1}(H) = \cup_{C \in \mathcal{C}} C$ la descomposición de $\Phi^{-1}(H)$ en componentes irreducibles, como la imagen $\Phi(\Phi^{-1}(H)) = \Phi(V_i) \cap H$ es cero-dimensional, se tiene que la imagen por Φ de cada componente $C \in \mathcal{C}$ es un punto.

Se deduce entonces la siguiente cadena de desigualdades:

$$gr(\Phi(V_i)) = \#(\Phi(V_i) \cap H) \leq \#\mathcal{C} \leq \sum_{C \in \mathcal{C}} gr(C) =$$

$$= gr\Big(\phi^{-1}(\phi(V_i) \cap H)\Big) \leq gr(V_i) \cdot gr(F_{i+1})$$

En consecuencia, se tiene que

$$gr(m_{F_{i+1}}) \leq gr(\Phi(V_i)) \leq d\delta_i$$

como se había afirmado.

Luego, la descomposición en componentes homogéneas de a_0 se halla con cotas de complejidad admisible gracias a la cota de grado de a_0 y posteriormente se genera aleatoriamente la $(n-i)$-upla γ que no anula A_0 por medio del lema 20.

Desde el punto de vista algorítmico, el procedimiento que realiza el primer paso de la segunda etapa calcula en primer lugar el polinomio característico $\chi_{F_{i+1}}$. A fin de evitar divisiones por elementos de $\mathbb{Z}[X_1, \ldots, X_{n-i}]$, en lugar de utilizar el polinomio característico de la homotecia por F_{i+1}, se opera con el de la homotecia por $(a^{D_i-1}\rho^{(i)})^d F_{i+1}$, cuyo cálculo puede realizarse sin divisiones de la manera siguiente:
si $F_{i+1} = \sum_{k=0}^{d} F_{i+1}^{(k)}$ es la descomposición de F_{i+1} en componentes homogéneas con respecto a las variables $X_{n-i+1}, \ldots, X_n$ (cf. sección 2.1.5), entonces

$$(a^{D_i-1}\rho^{(i)})^d F_{i+1} =$$

$$= \sum_{k=1}^{d} (a^{D_i-1}\rho^{(i)})^{d-k} F_{i+1}^{(k)}(X_1, \ldots, X_{n-i}, a^{D_i-1}\rho^{(i)} X_{n-i+1}, \ldots, a^{D_i-1}\rho^{(i)} X_n)$$

Luego, la matriz de la homotecia por $(a^{D_i-1}\rho^{(i)})^d F_{i+1}$ en la base $\mathcal{B}$ de $\mathbb{Q}[V_i]$ formada por las potencias de u_i, $\mathcal{B} := \{1, u_i, \ldots, u_i^{D_i-1}\}$, es la siguiente:

$$M_{(a^{D_i-1}\rho^{(i)})^d F_{i+1}} =$$

$$\sum_{k=1}^{d} (a^{D_i-1}\rho^{(i)})^{d-k} F_{i+1}^{(k)}(X_1, \ldots, X_{n-i}, a^{D_i-1}\rho^{(i)} M_{X_{n-i+1}}, \ldots, a^{D_i-1}\rho^{(i)} M_{X_n})$$

Para calcular esta matriz, se escribe en primer lugar la matriz aM, siendo $M \in \mathbb{Q}[X_1, \ldots, X_{n-i}]^{D_i \times D_i}$ la matriz compañera de $a^{-1}q_i$, cuyas entradas pueden obtenerse directamente a partir de los coeficientes de $a^{-1}q_i$. Posteriormente, se hallan las matrices $a^{D_i-1}\rho^{(i)} M_{X_{n-i+k}}$ de la manera siguiente: si $V_{n-i+j}^{(i)}(X_0, T)$ es la homogeinización respecto de T de $v_{n-i+j}^{(i)}$ con variable X_0, entonces se tiene la identidad:

$$a^{D_i-1}\rho^{(i)} M_{X_{n-i+k}} = \Big(\prod_{j \neq k} \rho_{n-i+k}^{(i)}\Big) a^{D_i-1-gr(v_{n-i+j})} V_{n-i+k}^{(i)}(a, aM)$$

la cual sugiere un esquema de cálculo que puede llevarse a cabo con talla $O(i\delta_i^3)$ y profundidad no escalar $O(\log(i\delta_i))$. Por otro lado, los polinomios $F_{i+1}^{(k)}$ se calculan por medio del circuito aritmético desarrollado en el lema 26 con talla $O(Ld^3)$ y profundidad no escalar $O(\ell)$. Luego, la matriz $M_{a^{D_i-1}(\rho^{(i)})^d F_{i+1}}$ se obtiene simplemente reemplazando en el circuito aritmético para la evaluación de $F_{i+1}^{(0)}, \ldots, F_{i+1}^{(d)}$ las variables $X_{n-i+1}, \ldots, X_n$ por las matrices
$a^{D_i-1}\rho^{(i)} M_{X_{n-i+1}}, \ldots, a^{D_i-1}\rho^{(i)} M_{X_n}$ y realizando algunas multiplicaciones adicionales, lo cual conlleva $O(Ld^3\delta_i^3)$ operaciones aritméticas adicionales con profundidad no escalar $O(\ell + \log(i\delta_i))$.

Luego, se aplica el lema 7 a fin de calcular los coeficientes del polinomio característico de la homotecia por $(a^{D_i-1}\rho^{(i)})^d F_{i+1}$ con talla $O(\delta_i^4)$ y profundidad no escalar $O(\log \delta_i)$. Dado que $M_{(a^{D_i-1}\rho^{(i)})^d F_{i+1}} = (a^{D_i-1}\rho^{(i)})^d M_{F_{i+1}}$, se deduce que $\chi_{(a^{D_i-1}\rho^{(i)})^d F_{i+1}}((a^{D_i-1}\rho^{(i)})^d T) = (a^{D_i-1}\rho^{(i)})^{dD_i}\chi_{F_{i+1}}(T)$, de donde se desprende que el coeficiente correspondiente al monomio T^k del polinomio $\chi_{(a^{D_i-1}\rho^{(i)})^d F_{i+1}}(T)$ tiene la forma $(a^{D_i-1}\rho^{(i)})^{d(D_i-k)} b_k$, siendo b_k el k–ésimo coeficiente de $\chi_{F_{i+1}}$. Por lo tanto, multiplicando el k–ésimo coeficiente de $\chi_{(a^{D_i-1}\rho^{(i)})^d F_{i+1}}$ por $(a^{D_i-1}\rho^{(i)})^{dk}$, se obtienen los coeficientes del polinomio $(a^{D_i-1}\rho^{(i)})^{dD_i}\chi_{F_{i+1}}$.

Finalmente, a fin de obtener los coeficientes del polinomio $m_{F_{i+1}}$, siguiendo el esquema de la sección 1.3.3 se calcula sin divisiones un polinomio $\theta \in R_i$ y una representación separable del polinomio $(a^{D_i-1}\rho^{(i)})^{dD_i}\chi_{F_{i+1}}$ respecto de T multiplicada por θ con $O(\delta_i^4)$ operaciones aritméticas y profundidad no escalar $O(\log \delta_i)$.

En definitiva, siendo $m_{F_{i+1}} := T^D + a_{D-1}T^{D-1} + \cdots + a_0$, se calculan sin divisiones los polinomios $\theta(a^{D_i-1}\rho^{(i)})^{dD_i} a_k \in R_i$ los cuales, divididos por $\theta(a^{D_i-1}\rho^{(i)})^{dD_i}$ dan los coeficientes $a_D, \ldots, a_0$ buscados. Aquí se aplica entonces la proposición 7 a fin de evitar divisiones, con lo cual se tiene una talla total de tipo $Li(d\delta_i)^{O(1)}$ con profundidad no escalar $O(\ell + \log(i\delta_i))$.

En particular, se obtiene un circuito aritmético con parámetros enteros sin divisiones en $\mathbb{Q}[X_1, \ldots, X_{n-i}]$ de talla $Li(d\delta_i)^{O(1)}$ y profundidad no escalar $O(\log(i\delta_i) + \ell)$ que calcula el coeficiente constante $a_0 \in \mathbb{Q}[X_1, \ldots, X_{n-i}]$, de $m_{F_{i+1}}$.

Como $gr(a_0) \leq d\delta_i$, con $Li(d\delta_i)^{O(1)}$ operaciones aritméticas en profundidad no escalar $O(\log(i\delta_i) + \ell)$ es posible calcular todas las componentes homogéneas del polinomio a_0. Del lema 20 se desprende que eligiendo aleato-

riamente una $(n-i)$-upla γ cuyas coordenadas tengan talla binaria acotada por $O(\log(i\delta_i)+\ell)$, con probabilidad mayor que $\frac{1}{2}$ se obtiene una tal que $A_0(\gamma) \neq 0$. Esta $(n-i)$-upla es la que se utiliza para definir el cambio de variables que realiza la normalización de Noether respecto de V_{i+1}.

El siguiente paso en la segunda etapa consiste en obtener un punto de levantamiento $P_{i+1} \in \mathbb{Z}^{n-i-1}$.

Para tal propósito, se considera el polinomio

$$J(F_1 \ldots, F_{i+1}) := det\left(\frac{\partial F_k}{\partial X_j}\right)_{\substack{1\leq k\leq i+1 \\ n-i\leq j\leq n}}$$

el cual no es divisor de cero en $\mathbb{Q}[V_{i+1}]$, dado que el ideal $(F_1, \ldots, F_{i+1})$ es radical.

Sea $\mu \in \mathbb{Q}[X_1, \ldots, X_{n-i-1}]$ el término constante del polinomio característico de la homotecia definida por $J := J(F_1 \ldots, F_{i+1})$ en $\mathbb{Q}[V_{i+1}]$. Dado que J representa un elemento que no es divisor de cero en $\mathbb{Q}[V_{i+1}]$, se concluye que μ no es el polinomio nulo. La importancia de este polinomio μ radica en el hecho que, siendo π_{i+1} el morfismo de variedades algebraicas $\pi_{i+1} \quad V_{i+1} \longrightarrow \mathbb{C}^{n-i-1}$ que proyecta las primeras $n-i$ coordenadas de los puntos de V_{i+1}, un punto de levantamiento $P_{i+1} \in \mathbb{Z}^{n-i+1}$ tiene fibra $\pi_{i+1}^{-1}(\{P_{i+1}\})$ suave si y sólo si $\mu(P_{i+1}) \neq 0$:
siendo u_{i+1} un elemento primitivo para $\mathbb{Q}[V_{P_{i+1}}]$, cada raíz del polinomio característico χ_J corresponde a la evaluación de $J(F_1 \ldots, F_{i+1})$ en un punto de $\mathbb{Q}[V_{P_{i+1}}]$. Por lo tanto, una condición suficiente para que la evaluación de $J(F_1, \ldots, F_{i+1})$ en cada punto de $V_{P_{i+1}}$ resulte distinta de cero es que χ_J no contenga a cero entre sus raíces, siendo esta última afirmación equivalente a que el término constante de χ_J, es decir μ, verifique $\mu(P_{i+1}) \neq 0$.

Por otro lado, la suavidad de la fibra $V_{P_{i+1}}$ asegura también que el cardinal de la misma es igual al rango de $\mathbb{Q}[V_{i+1}]$ como R_{i+1}-módulo:

como $\mathbb{Q}[V_{i+1}]$ es un R_{i+1}-módulo libre de tipo finito (ver por ejemplo [83]) de rango D_{i+1}, se tiene que $\mathbb{Q}[V_{i+1}]$ es isomorfo como R_i-módulo a $(R_{i+1})^{D_i}$. Luego, para cualquier punto $(p_1, \ldots, p_{n-i-1}) \in \mathbb{Q}^{n-i-1}$, se tiene que $\mathbb{Q}[V_{i+1}]/(Y_1 - p_1, \ldots, Y_{n-i-1} - p_{n-i-1})$ es un $\mathbb{Q}$-espacio vectorial de dimensión finita isomorfo a $(R_{i+1}/(Y_1 - p_1, \ldots, Y_{n-i-1} - p_{n-i-1}))^{D_i} \simeq \mathbb{Q}^{D_i}$, y por lo tanto, de dimensión D_i.

Ahora bien, si el punto P_{i+1} de coordenadas $(p_1, \ldots, p_{n-i-1})$ tiene fibra suave, se tiene entonces que

$$\mathbb{Q}[V_{i+1}]/(Y_1 - p_1, \ldots, Y_{n-i-1} - p_{n-i-1}) =$$

$$= \mathbb{Q}[Y_1, \ldots, Y_n]/(F_1, \ldots, F_{i+1}, Y_1 - p_1, \ldots, Y_{n-i-1} - p_{n-i-1}) \simeq$$

$$\simeq \mathbb{Q}[Y_{n-i}, \ldots, Y_n]/(F_1(P_{i+1}, Y_{n-i}, \ldots, Y_n), \ldots, F_{i+1}(P_{i+1}, Y_{n-i}, \ldots, Y_n))$$

Siendo P_{i+1} un punto de fibra suave, se tiene que $\mu(P_{i+1}) \neq 0$ de lo cual se deduce, gracias al criterio del jacobiano, que el anillo

$$\mathbb{Q}[Y_1, \ldots, Y_n]/(F_1, \ldots, F_{i+1}, Y_1 - p_1, \ldots, Y_{n-i-1} - p_{n-i-1})$$

es reducido. En consecuencia, el ideal $(F_1, \ldots, F_{i+1}, Y_1 - p_1, \ldots, Y_{n-i-1} - p_{n-i-1})$ es radical y define la variedad cero–dimensional $V_{P_{i+1}}$. Por lo tanto, el cardinal de la fibra $V_{P_{i+1}}$ es igual a la dimensión del $\mathbb{Q}$–espacio vectorial $\mathbb{Q}[Y_1, \ldots, Y_n]/(F_1, \ldots, F_{i+1}, Y_1 - p_1, \ldots, Y_{n-i-1} - p_{n-i-1})$, y es entonces D_i como se había afirmado.

Se observa entonces que cualquier punto $P_{i+1} \in \mathbb{Z}^{n-i-1}$ que verifica $\mu(P_{i+1}) \neq 0$ cumple los requerimientos necesarios para ser un punto de levantamiento para V_{i+1}. Luego, un tal punto puede conseguirse aplicando el lema 20, para lo cual es preciso estimar la complejidad aritmética de la evaluación del polinomio μ. Obsérvese que μ es el coeficiente de un polinomio característico de una homotecia en $\mathbb{Q}[V_{i+1}]$, cuyo tensor de multiplicación todavía no ha sido calculado.

El esquema que se aplicará en la resolución de esta cuestión se utilizará reiteradamente en lo que sigue. Si bien no se tiene el polinomio característico de la homotecia por $J(F_1, \ldots, F_{i+1})$ en $\mathbb{Q}[V_{i+1}]$, es posible calcular sin divisiones los coeficientes del polinomio característico de la homotecia por este mismo polinomio en $\mathbb{Q}[V_i]$ con las mismas ideas con que se ha calculado el polinomio característico $\chi_{F_{i+1}}$ (para estimar la complejidad de este proceso es importante observar que $gr\, J(F_1, \ldots, F_{i+1}) \leq (d-1)(i+1)$). La idea es "eliminar" la variable Y_{n-i} de χ_J, para lo cual se utiliza la relación de dependencia $a_0(Y_1, \ldots, Y_{n-i})$ que verifican las variables $Y_1, \ldots, Y_{n-i}$ en V_{i+1}.

En primer lugar, los coeficientes de $a_0(Y_1, \ldots, Y_{n-i})$ respecto de su escritura en la variable Y_{n-i} puede conseguirse siguiendo el esquema de la sección 2.1.5. A partir de estos coeficientes se escribe la matriz compañera $M_{Y_{n-i}}$ del

polinomio $a_0(Y_1,\ldots,Y_{n-i})$ (como polinomio en Y_{n-i}) y se calcula la matriz $\mathcal{M}_J := \chi_J(Y_1,\ldots,Y_{n-i+1},M_{Y_{n-i}},T)$. Se afirma que el determinante $det(\mathcal{M}_J)$ de la matriz $\mathcal{M}_J$ es una ecuación que anula a $J(F_1,\ldots,F_{i+1})$ en $\mathbb{Q}[V_{i+1}]$:
de su definición, se tiene que el polinomio $\chi_J \in \mathbb{Q}[Y_1,\ldots,Y_{n-i}][T]$ verifica $\chi_J(J(F_1,\ldots,F_{i+1})) \equiv 0$ módulo $(F_1,\ldots,F_i)$. Para eliminar la variable Y_{n-i} de esta ecuación, se calcula el polinomio $det(\mathcal{M}_J) \in \mathbb{Q}[Y_1,\ldots,Y_{n-i-1}][T]$. Este polinomio satisface que $det(\mathcal{M}_J)(T) \equiv 0$ módulo el ideal generado por a_0:
la matriz $\mathcal{M}_J$ describe la homotecia por χ_J en $\mathbb{Q}(Y_1,\ldots,Y_{n-i+1},T)[Y_{n-i}]/(a_0)$ en la base natural formada por las potencias de Y_{n-i}. Si se aplica esta homotecia al polinomio cuyas coordenadas son las de la primer columna de la matriz adjunta de $\mathcal{M}_J$ se obtienen las coordenadas de un múltiplo de χ_J módulo a_0. De la definición de $Adj(\mathcal{M}_J)$ se deduce que estas coordenadas son nulas salvo por la coordenada correspondiente al término de grado cero en Y_{n-i}, la cual da el polinomio $det(\mathcal{M}_J)$. Por lo tanto, este polinomio es un múltiplo de χ_J módulo (a_0) que tiene grado cero en Y_{n-i}. Se deduce entonces que

$$det(\mathcal{M}_J)(Y_1,\ldots,Y_{n-i-1},J(F_1,\ldots,F_{i+1})) \in (F_1,\ldots,F_i,a_0) \subseteq (F_1,\ldots,F_{i+1})$$

y es, por tanto, una ecuación que anula J en V_{i+1}. En particular, el coeficiente constante $\tilde{\mu}$ (respecto de T) de esta ecuación es múltiplo del polinomio μ y por lo tanto la condición $\mu(P_{i+1}) \neq 0$ puede reemplazarse por $\tilde{\mu}(P_{i+1}) \neq 0$.

El proceso descripto opera con la solución geométrica de V_i, que sólo tiene validez en un abierto Zariski de $\mathbb{C}^n$ (el definido por $\rho^{(i)} \neq 0$). Esto podría introducir divisiones por cero en pasos posteriores del algoritmo que deben evitarse. Este inconveniente se soluciona si se impone la condición adicional que el punto P_{i+1} a hallar no anule el polinomio $\rho^{(i)}$.

A fin de estimar la complejidad aritmética del polinomio $\tilde{\mu} \cdot \rho^{(i)}$, se observa que en primer lugar que el polinomio $J(F_1,\ldots,F_{i+1})$ puede evaluarse mediante un circuito aritmético sin divisiones de talla $((i+1)^5 + L)$ y profundidad no escalar $O(\log i + \ell)$, combinando los lemas 7 y 25. Además, $J(F_1,\ldots,F_{i+1})$ tiene grado acotado por $(i+1)(d-1)$.

Luego, mediante consideraciones similares a las realizadas para el cálculo del polinomio minimal de F_{i+1} se obtiene un circuito aritmético sin divisiones en $\mathbb{Q}[X_1,\ldots,X_{n-i-1}]$ que calcula $\tilde{\mu}$ con talla $L(id\delta_i)^{O(1)}$ y profundidad no escalar $O(\ell + \log i\delta_i)$, y esto mismo es cierto para el producto $\rho^{(i)} \cdot \tilde{\mu}$.

Aplicando el lema 20, se generan aleatoriamente números enteros $p_1, \ldots, p_{n-i-1}$ de altura logarítmica $O(\ell + \log n + \log i\delta_i)$ tales que el punto $P_{i+1} := (p_1, \ldots, p_{n-i-1}) \in \mathbb{Z}^{n-i-1}$ satisface la condición $(\rho \cdot \tilde{\mu})(P_{i+1}) \neq 0$ con probabilidad mayor que $\frac{1}{2}$. Claramente, P_{i+1} resulta un punto de levantamiento para la variedad V_{i+1}.

La segunda etapa se completa con el cálculo de una solución geométrica de $V_{P_{i+1}}$. Para esto, se generarán las entradas necesarias para la aplicación de los lemas 29 y 30. En la demostración del lema 29 se calcula un polinomio $F(T_{n-i}, \ldots, T_n)$ de talla $O(i\delta_i^{O(1)})$ y profundidad no escalar $O(\log(i\delta_i))$ con la propiedad siguiente:
cualquier vector de coeficientes $(\lambda_{n-i}, \ldots, \lambda_n) \in \mathbb{Z}^{i+1}$ que verifica la condición $F(\lambda_{n-i}, \ldots, \lambda_n) \neq 0$ define una forma lineal $U_{i+1} := \lambda_{n-i}Y_{n-i} + \cdots + \lambda_n Y_n$ que induce un elemento primitivo u_{i+1} de $V_{P_{i+1}}$. Por lo tanto, aplicando el lema 20 se obtienen los coeficientes $(\lambda_{n-i}, \ldots, \lambda_n)$ de U_{i+1} buscados.

Luego se utiliza el lema 30, a fin de calcular la solución geométrica de $V_{P_{i+1}}$ asociada al elemento primitivo u_{i+1}.

Resta entonces resolver la cuestión de generar las entradas necesarias para la aplicación de los lemas 29 y 30. Especializando $(Y_1, \ldots, Y_{n-i-1})$ en P_{i+1} en los polinomios obtenidos como resultado de la aplicación del método de Newton–Hensel (primera etapa) y el polinomio $a_0(Y_1, \ldots, Y_{n-i})$ resultante de la normalización de Noether respecto de V_{i+1} (primera parte de la segunda etapa), se tienen los siguientes ítems:

- Para cada $j = n - i + 1, \ldots, n$, un polinomio $g_j \in \mathbb{Z}[Y_{n-i}][T]$ tal que $g_j(Y_j)$ pertenece a $\mathcal{I}^{(P_{i+1})}$, donde $\mathcal{I}^{(P_{i+1})}$ es el ideal definido por los polinomios $F_1(P_{i+1}, Y_{n-i}, \ldots, Y_n), \ldots, F_{i+1}(P_{i+1}, Y_{n-i}, \ldots, Y_n)$.

- Para cada $j = n - i + 1, \ldots, n$, un polinomio

  $h_j \in \mathbb{Z}[T_{n-i+1}, \ldots, T_n, Y_{n-i}, \ldots, Y_n][T]$ tal que $h_j(T_{n-i+1}Y_{n-i+1} + \cdots + \widehat{T_jX_j} + \cdots T_nY_n)$ pertenece al ideal $\mathcal{I}^{(P_{i+1})} \otimes \mathbb{Q}(T_{n-i+1}, \ldots, T_n)$.

- Un polinomio $h_{n-i} \in \mathbb{Z}[T_{n-i+1}, \ldots, T_n, Y_{n-i}, \ldots, Y_n][T]$ tal que

  $h_j(T_{n-i+1}Y_{n-i+1} + \cdots T_nY_n)$ pertenece al ideal $\mathcal{I}^{(P_{i+1})} \otimes \mathbb{Q}(T_{n-i+1}, \ldots, T_n)$.

- Un polinomio $A_0 \in \mathbb{Z}[T]$ tal que $A_0(Y_{n-i})$ pertenece a $\mathcal{I}^{(P_{i+1})}$.

A fin de calcular los polinomios minimales de las variables $Y_{n-i},\ldots,Y_n$ en $\mathbb{Q}[V_{P_{i+1}}]$, se realiza un proceso similar al aplicado para hallar una ecuación para $J(F_1,\ldots,F_{i+1})$ en $V_{P_{i+1}}$, utilizando el polinomio A_0 como forma "eliminante" de la variable Y_{n-i}. Así, operando con A_0 y g_j se obtiene un polinomio $G_j\mathbb{Z}[T]$ tal que $G_j(X_j)\in\mathcal{I}^{(P_{i+1})}$ para $j=n-i+1,\ldots,n$. La representación separable de los polinomios obtenidos de esta manera y A_0 da un múltiplo entero del polinomio minimal de las variables $X_{n-i},\ldots,X_n$ que se quieren hallar. De la misma forma se calcula el polinomio minimal de $T_{n-i+1}Y_{n-i+1}+\cdots+T_nY_n$ a partir de h_{n-i} y A_0.

Finalmente, los polinomios minimales en $\mathbb{Q}[V_{P_{i+1}}]\otimes\mathbb{Q}(T_{n-i},\ldots,T_n)$ de las formas $T_{n-i}Y_{n-i}+\cdots+\widehat{T_jY_j}+\cdots+T_nY_n$ para $j=n-i+2,\ldots,n$ se calculan por medio del lema 28 aplicado a los polinomios h_j y a_0, utilizando el elemento primitivo $T_{n-i}Y_{n-i}+\cdots+T_nY_n$.

Podría ocurrir que la altura de los coeficientes de estos polinomios minimales fuera excesiva. En tal caso, dividiendo por sus contenidos se los hace primitivos, lo cual requiere cálculos de máximo común divisor entero que no modifican el comportamiento asintótico de la complejidad del algoritmo.

De las estimaciones de complejidad de los lemas 28 y 30 se concluye que este proceso puede realizarse con talla $L(id\delta_i)^{O(1)}$ y profundidad no escalar $O(\ell+\log i\delta_i)$. Por lo tanto, el i-ésimo paso recursivo se realiza mediante un circuito aritmético de talla total $L(id\delta_i)^{O(1)}$ y profundidad no escalar $O(\log\delta_i(\ell+\log i))$. □

Habiendo descripto el circuito que realiza el i-ésimo paso recursivo del algoritmo, es posible enunciar el resultado principal de esta sección:

Teorema 11 *Sea $\mathcal{F}:=\{\mathcal{F}_{(n,L,\ell,d,h,\delta,\eta)}\}$ una familia de subconjuntos finitos de polinomios con las siguientes propiedades:*

- $\mathcal{F}_{(n,L,\ell,d,h,\delta,\eta)}:=\{F_1,\ldots,F_n\}\subseteq\mathbb{Z}[X_1,\ldots,X_n]$
- $d=max\{gr(F_i):1\le i\le n\}$ *es el máximo grado total de los polinomios* $F_1,\ldots,F_n$.
- $\delta=max\{gr(V(F_1,\ldots,F_i)):1\le i\le n\}$ *es el grado geométrico del sistema definido por* $F_1,\ldots,F_n$.
- $\eta:=max\{ht_{V(F_1,\ldots,F_i)}(c((\log n+\ell)\log\delta):1\le i\le n\}$ *es la altura geométrica del sistema definido por* $F_1,\ldots,F_n$, *donde* $c>0$ *es una*

constante universal que no depende del input $F_1, \ldots, F_n$ considerado (ni de su tamaño).

- *Los polinomios $F_1, \ldots, F_n$ están dados mediante un circuito aritmético $\Gamma_{(n,L,\ell,d,h,\delta,\eta)}$ de talla L y profundidad no escalar ℓ, que utiliza parámetros enteros de talla h.*
- *La familia de circuitos $\{\Gamma_{(n,L,\ell,d,h,\delta,\eta)}\}$ es uniforme en espacio $\log(nLh)$.*
- *$F_1, \ldots, F_n$ definen una sucesión regular en $\mathbb{Q}[X_1, \ldots, X_n]$*
- *para todo $i = 1, \ldots, n$, el ideal $(F_1, \ldots, F_i)$ es un ideal radical de $\mathbb{Q}[X_1, \ldots, X_n]$*

Sea $V := V_{(n,L,\ell,d,h,\delta,\eta)} \subset \mathbf{C}^n$ la variedad algebraica intersección completa de dimensión cero definida por $\mathcal{F}_{(n,L,\ell,d,h,\delta,\eta)}$. Entonces existe una máquina de Turing probabilística de error acotado que calcula una forma lineal U que representa un elemento primitivo u para V y la solución geométrica asociada al elemento primitivo u en espacio $O\big(n\log(n\delta)(\ell + \log(\eta n h \delta))\big)$ y tiempo $L(\ell n d h \delta)^{O(n\log\delta+\ell)}$.

Demostración. La idea es utilizar el circuito descripto en la proposición 8, para luego aplicar el teorema 1. Este circuito contiene entradas que se determinan aleatoriamente, las cuales se generan en el momento necesario y se alojan en memoria.

Por tal motivo, es necesario "expandir" el circuito de la proposición 8 a un circuito booleano y demostrar la uniformidad del mismo.

La estimación de la profundidad no escalar del subcircuito que realiza i–ésimo paso recursivo permite deducir que el circuito global opera con números enteros cuya altura logarítmica está acotada por $O(nh\eta\delta 2^{\ell}))$. Asimismo, todas las matrices que se utilizan tienen tamaño de tipo $n\delta^{O(1)}$. Por lo tanto, el álgebra lineal puede llevarse a cabo con profundidad (booleana) máxima de tipo $O\big(\log(n\delta)\log(n\delta(nh\eta\delta 2^{\ell}))\big)$. Dado que el algoritmo funciona en n etapas recursivas, es necesario componer n máquinas de Turing, lo cual puede realizarse en el espacio correspondiente a la suma de las mismas y tiempo correspondiente al producto del tiempo que utiliza cada una (lema 2).

La uniformidad de las familias de circuitos consideradas depende fundamentalmente de la uniformidad del circuito que evalúa $F_1, \ldots, F_n$ y del

álgebra lineal. Las cotas para el tamaño del álgebra lineal considerada y la longitud binaria de los números enteros involucrados permiten concluir que el código del circuito puede generarse en espacio de tipo $O(\log(Lnh\ell\eta\delta))$.

Aplicando el teorema 1 se deducen las cotas de espacio y tiempo enunciadas. □

Cabe destacar que en el peor caso (es decir, cuando el grado geométrico δ del sistema es de la misma magnitud que el número de Bézout $gr(F_1)\cdots gr(F_n) \leq d^n$), el espacio (y por ende el tiempo) utilizado puede mejorarse a cantidades de tipo $n^2\log(hL\ell\delta\eta)$, aplicando las técnicas basadas en deformaciones homotópicas del sistema descriptas en 1.4.4. Desafortunadamente estas técnicas tienen la desventaja de no distinguir los sistemas bien condicionados de los mal condicionados, por lo que la complejidad de la resolución de *cualquier* sistema cuyas ecuaciones tienen grado y cantidad de variables prefijados corresponde a la del peor caso y queda en función de parámetros "sintácticos" (como la regularidad de la función de Hilbert de cierto ideal o el número de Bezout) que no tienen relación con la geometría del conjunto de soluciones.

Por otro lado, el control del tamaño del álgebra lineal involucrada que se realiza en el algoritmo que se ha descripto es una puerta abierta a la posibilidad de mejoras la complejidad espacio-tiempo de la resolución de sistemas de ecuaciones polinomiales: una mayor eficiencia (en el sentido de tradeoff espacio-tiempo) para la resolución de problemas de álgebra lineal tendría consecuencias inmediatas importantes sobre la complejidad espacio-tiempo del algoritmo descripto.

2.2 La división módulo un ideal intersección completa reducido

En esta sección se trata un problema crucial para las aplicaciones que involucran cuestiones de representación: el problema del calcular el cociente de una división en un anillo que es intersección completa reducido.

El ingrediente principal para el teorema de división es una técnica de dualidad basada en la existencia de trazas para álgebras de Gorenstein.

2.2.1 Traza y dualidad

Fórmulas de traza aparecen en varios trabajos recientes que tratan problemas algorítmicos en teoría de eliminación. En algunos de estos trabajos se utilizan fórmulas de traza a fin de calcular un cociente como el resultado de la división de dos polinomios dados módulo un ideal intersección completa (ver [68], [114]). En otros trabajos se usan fórmulas de traza o de residuos para diseñar algoritmos para la resolución geométrica o algebraica de álgebras de Gorenstein cero-dimensionales dadas por ideales intersección completa ([4], [12], [43], [44], [57], [58]). En [154] se aplica una fórmula de traza para obtener una cota superior para los grados en el Nullstellensatz (ver también [15], [16], [17] por aspectos aritméticos).

Sin embargo, todas estas aplicaciones de fórmulas de traza requieren el uso de una familia de monomios de grado acotado que genera el álgebra de Gorenstein como un espacio vectorial sobre un cuerpo adecuado. En consecuencia, tales fórmulas no proveen cotas de complejidad intrínseca. En esta sección, siguiendo el desarrollo realizado en [78], se utiliza una fórmula de traza alternativa que permite obtener cotas de complejidad polinomiales para álgebras de Gorenstein geométricamente bien condicionadas.

Se comienza recordando los hechos básicos de teoría de traza que se necesitan. Para sus demostraciones se refiere al lector a [116], Apéndices E y F.

Teoría general de traza

Sea R un anillo de polinomios sobre $\mathbb{Q}$. Sea K el cuerpo de cocientes de R y $R[X_1, \ldots, X_n]$ el anillo de polinomios en n variables con coeficientes en R. Sea $F_1, \ldots, F_n$ una sucesión regular suave de polinomios en $R[X_1, \ldots, X_n]$ de

grado en las variables $X_1, \ldots, X_n$ acotado por d, que genera un ideal radical $(F_1, \ldots, F_n)$.

Se considera R-álgebra B dada como el cociente de $R[X_1, \ldots, X_n]$ por este ideal:

$$B := R[X_1, \ldots, X_n]/(F_1, \ldots, F_n)$$

Se supone además que la extensión de anillos entera $R \to B$ representa una normalización de Noether de la variedad $V(F_1, \ldots, F_n)$ definida por los polinomios $F_1, \ldots, F_n$ en un espacio afín adecuado. Por lo tanto, B es un R-módulo libre de rango acotado por el grado de la variedad $V(F_1, \ldots, F_n)$. Mas aún, la R-álgebra B es Gorenstein y los siguientes enunciados se basan en este hecho.

Se considera $B^* := Hom_R(B, R)$ con la estructura de B-módulo definida a partir del producto escalar

$$B \times B^* \longrightarrow B^*$$

que asocia a cada (b, τ) en $B \times B^*$ el morfismo R-lineal $b \cdot \tau : B \longrightarrow R$ definido por $(b \cdot \tau)(x) := \tau(bx)$ para cada elemento x de B.

Dado que la R-álgebra B es Gorenstein, su dual B^* es un B-módulo libre de rango 1. Cada elemento σ de B^* que genera B^* como B-módulo se dice una *traza* de B. Existen dos elementos relevantes de B^* que se denotan por Tr y σ. El primero, Tr, se llama la *traza estándar* de B y se define de la siguiente manera: dado $b \in B$, sea $\eta_b : B \longrightarrow B$ la homotecia por b. La imagen $Tr(b)$ por Tr se define como la traza ordinaria del endomorfismo η_b de B (nótese que esta definición tiene sentido ya que B es un R-módulo libre).

Para introducir σ (que será llamado una traza de B), se necesitan algunas notaciones adicionales. Para cualquier elemento $G \in R[X_1, \ldots, X_n]$ se denota por $\bar{G}$ su imagen en B, es decir la clase residual de G módulo el ideal $(F_1, \ldots, F_n)$. Sean $Y_1, \ldots, Y_n$ nuevas variables e $Y := (Y_1, \ldots, Y_n)$. Sea $1 \leq j \leq n$ y $F_j^{(Y)} := F_j(Y_1, \ldots, Y_n)$ el polinomio de $R[Y_1, \ldots, Y_n]$ obtenido sustituyendo en F_j las variables $X_1, \ldots, X_n$ por $Y_1, \ldots, Y_n$. Se considera el polinomio

$$F_j^{(Y)} - F_j = \sum_{k=1}^{n} l_{jk}(Y_k - X_k) \in R[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$$

donde los l_{jk} son polinomios que pertenecen a $R[X_1,\ldots,X_n,Y_1,\ldots,Y_n]$ de grado total acotado por $(d-1)$ (obsérvese que los l_{jk} no están unívocamente determinados por la sucesión $F_1,\ldots,F_n$). Se considera ahora el determinante Δ de la matriz $(l_{jk})_{1\leq j,k\leq n}$ el cual puede escribirse en la forma

$$\Delta = \sum_m a_m(X_1,\ldots,X_n)b_m(Y_1,\ldots,Y_n) \in R[X_1,\ldots,X_n,Y_1,\ldots,Y_n],$$

siendo los a_m elementos de $R[X_1,\ldots,X_n]$ y los b_m elementos of $R[Y_1,\ldots,Y_n]$. (cabe destacar que no será necesario hallar los polinomios a_m y b_m, sólo es necesaria su existencia para la argumentación). El polinomio Δ se llama el determinante seudo-jacobiano de la sucesión regular $F_1,\ldots,F_n$. Obsérvese que los polinomios a_m y b_m pueden elegirse con grados acotados por $n(d-1)$ en las variables $X_1,\ldots,X_n$ e $Y_1,\ldots,Y_n$ respectivamente.

Sea $c_m \in R[X_1,\ldots,X_n]$ el polinomio que se obtiene sustituyendo las variables $Y_1,\ldots,Y_n$ por $X_1,\ldots,X_n$ en b_m. Si $\bar{J}$ es la clase del determinante jacobiano $J(F_1,\ldots,F_n)$ en B se tiene la siguiente identidad

$$\bar{J} = \sum_m \bar{a}_m \cdot \bar{c}_m$$

Mas aún, la imagen del polinomio Δ en el anillo de clases de residuos $R[X_1,\ldots,X_n,Y_1,\ldots,Y_n]$ módulo el ideal $(F_1,\ldots,F_n,F_1^{(Y)},\ldots,F_n^{(Y)})$ es independiente de la elección particular de la matriz $(l_{kj})_{1\leq k,j\leq n}$. Esto justifica el nombre "seudo-jacobiano" para el polinomio Δ. Con estas notaciones existe una única traza $\sigma \in B^*$ tal que la siguiente identidad vale en B:

$$\bar{1} = \sum_m \sigma(\bar{a}_m) \cdot \bar{c}_m$$

La principal propiedad de la traza σ, conocida como la "fórmula de traza" ("fórmula de traza de Tate" [116, Appendix F], siendo [100] un caso especial de la misma) es el siguiente enunciado: para cada $G \in R[X_1,\ldots,X_n]$ se verifica la siguiente identidad en B:

$$\bar{G} = \sum_m \sigma(\bar{G} \cdot \bar{a}_m) \cdot \bar{c}_m \tag{2.15}$$

Obsérvese que el polinomio $\sum_m \sigma(\bar{G} \cdot \bar{a}_m) \cdot c_m \in R[X_1,\ldots,X_n]$ de la identidad (2.15) tiene grado en las variables $X_1,\ldots,X_n$ acotado por $n(d-1)$.

Esta fórmula de traza se utilizará para resolver el problema del "levantamiento" de una clase residual:
dado un polinomio $G \in R[X_1, \ldots, X_n]$ de grado arbitrario en $X_1, \ldots, X_n$, se quiere hallar un polinomio $G_1 \in R[X_1, \ldots, X_n]$ de grado en las variables $X_1, \ldots, X_n$ acotado por $n(d-1)$, tal que vale $\bar{G}_1 = \bar{G}$ en B.

Como ya se ha visto, la fórmula de traza (2.15) resuelve este problema dado que se puede elegir para G_1 el polinomio

$$G_1 := \sum_m \sigma(\bar{G} \cdot \bar{a}_m) \cdot c_m. \tag{2.16}$$

Sin embargo, la definición del polinomio G_1 mediante la fórmula (2.16) tiene la desventaja que es necesario calcular los polinomios a_m y c_m, para lo cual hay que operar con todos los monomios de grado acotado por $n(d-1)$. En consecuencia, se reemplazará la fórmula (2.15) por medio de la siguiente alternativa:

Proposición 9 ([78], Proposition 31) *Con las notaciones anteriores, se considera el $R[X_1, \ldots, X_n]$-módulo libre $B[X_1, \ldots, X_n]$ y el polinomio $\Delta_1 \in R[X_1, \ldots, X_n]$ definido por:*

$$\Delta_1 := \sum_m \bar{a}_m \cdot c_m \in B[X_1, \ldots, X_n]$$

Entonces, para cada $G \in R[X_1, \ldots, X_n]$ se satisface la siguiente identidad en $R[X_1, \ldots, X_n]$:

$$\sum_m \sigma(\bar{G} \cdot \bar{a}_m) \cdot c_m = \tilde{\mathrm{Tr}}(\bar{J}^{-1}\bar{G} \cdot \Delta_1)$$

(donde $\tilde{\mathrm{Tr}} := \mathrm{Tr} \otimes Id_{R[X_1,\ldots,X_n]} : B[X_1, \ldots, X_n] \longrightarrow R[X_1, \ldots, X_n]$ es la traza estándar que se obtiene a partir de la traza estándar $\mathrm{Tr} : B \longrightarrow R$ por extensión de escalares).

Claramente se ve que, para $H \in R[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, $\tilde{\mathrm{Tr}}(\bar{H})$ es la traza estándar de la imagen $\bar{H}$ de H en el $R[Y_1, \ldots, Y_n]$-módulo $B[Y_1, \ldots, Y_n]$. Esta observación en conjunto con la proposición 9 representa la herramienta básica para la evaluación de la fórmula (2.16) y por lo tanto para la solución del problema del cálculo de una clase residual. Este es el contenido de las siguientes observaciones.

Sea $B' = K \otimes_R B$ la K-álgebra obtenida localizando B en los elementos no nulos de R. Dada una base fija del K-espacio vectorial de dimensión finita B', sean $M_{X_1}, \ldots, M_{X_n}$ las matrices de las homotecias $\eta_{X_i} : B' \longrightarrow B'$ con respecto a la base dada de B' y sea Tr la función que asocia a la matriz dada su traza usual. Con estas convenciones, el polinomio G_1 de 2.16 se puede hallar de la siguiente manera:

$$\begin{aligned} G_1 &= Tr(J(F_1, \ldots, F_n)(M_{X_1}, \ldots, M_{X_n})^{-1} \cdot G(M_{X_1}, \ldots, M_{X_n}) \cdot \\ &\quad \cdot \Delta(M_{X_1}, \ldots, M_{X_n}, X_1, \ldots, X_n)) \end{aligned} \tag{2.17}$$

Se ve entonces que G_1 pertenece a $R[X_1, \ldots, X_n]$ y que se satisface la igualdad $\bar{G}_1 = \bar{G}$ en B.

2.2.2 Un paso de división

El proceso de levantamiento descripto en la subsección anterior se utilizará a fin de calcular el cociente de dos polinomios módulo un ideal intersección completa reducida. Mas precisamente, sea $F \in R[X_1, \ldots, X_n]$ un polinomio que no es divisor de cero en B y $G \in R[X_1, \ldots, X_n]$ un polinomio tal que la clase residual $\bar{F}$ divide a la clase residual $\bar{G}$ en B. En la siguiente proposición se demuestra como se puede calcular un cociente de levantamiento $Q \in R[X_1, \ldots, X_n]$ para la división de $\bar{G}$ por $\bar{F}$ en B.

Proposición 10 (Paso de división) *Con las notaciones y suposiciones de la subsección previa, sea D el rango de B como R-módulo libre. Sean dados los siguientes ítems como entrada:*

- *un circuito aritmético Γ' de talla L y profundidad no escalar ℓ que evalúa los polinomios $F, G, F_1, \ldots, F_n$, y*
- *las matrices $M_{X_1}, \ldots, M_{X_n}$ que describen el tensor de multiplicación de B con respecto a la base dada de $B' = K \otimes_R B$.*

Supóngase que $\bar{F}$ no es un divisor de cero de $\bar{B}$ y que $\bar{F}$ divide $\bar{G}$ en B. Entonces, existe un circuito aritmético Γ sin divisiones en $K[X_1, \ldots, X_n]$ de talla $L(nD)^{O(1)}$ y profundidad no escalar $O(\ell + log_2 D + log_2 n)$ que calcula, a partir de las entradas de las matrices $M_{X_1}, \ldots, M_{X_n}$ y los parámetros de Γ' un elemento no nulo θ de R, y un polinomio Q de $R[X_1, \ldots, X_n]$ tal que θ divide Q en $R[X_1, \ldots, X_n]$ y tal que se satisface la identidad $\bar{Q}\bar{F} = \bar{\theta}\bar{G}$ en B.

Demostración. Obsérvese en primer lugar que cualquier base de B como R-módulo libre induce una base de $B[Y_1,\ldots,Y_n]$ como $R[Y_1,\ldots,Y_n]$-módulo libre. Mas aún, si M_{X_i} es la matriz que representa la homotecia por $\bar{X}_i$ en B con respecto a la base dada, M_{X_i} representa también la homotecia por $\bar{X}_i$ en $B[Y_1,\ldots,Y_n]$ con respecto a la misma base. Además, dado que los polinomios F y $J(F_1,\ldots,F_n)$ no son divisores de cero módulo $(F_1,\ldots,F_n)$, las siguientes matrices son no singulares:

$$\mathcal{F} := F(M_{X_1},\ldots,M_{X_n})$$
$$J_1 := J(F_1,\ldots,F_n)(M_{X_1},\ldots,M_{X_n})$$

Finalmente, se nota por G_1 y Δ_1 las siguientes matrices:

$$G_1 := G(M_{X_1},\ldots,M_{X_n})$$
$$\Delta_1 := \Delta(M_{X_1},\ldots,M_{X_n},X_1,\ldots,X_n)$$

donde Δ es el determinante seudo-jacobiano de $F_1,\ldots,F_n$. Obsérvese que las matrices $\mathcal{F}, J_1$ y G_1 tienen entradas en K mientras que Δ_1 tiene entradas en $K[Y_1,\ldots,Y_n]$. A partir de la fórmula (2.17) de la sección anterior se deduce que $Q_1 := Tr(J_1^{-1}\cdot\mathcal{F}^{-1}\cdot G_1\cdot\Delta_1(X_1,\ldots,X_n))$ es un polinomio de $R[X_1,\ldots,X_n]$ que satisface en B la identidad $\bar{Q}_1\bar{F} = \bar{G}$ en B (donde Tr denota ahora la traza usual de matrices).

Por último, se traspone la matriz adjunta de $\mathcal{F}$ y J_1:

$$\tilde{\mathcal{F}} := {}^tAdj(\mathcal{F}),\ \text{and}\ J_2 := {}^tAdj(J_1)$$

El cociente $Q \in R[X_1,\ldots,X_n]$ y la constante no nula $\theta \in R$ que se buscan están dadas por:

- $Q := Tr(\tilde{\mathcal{F}}\cdot J_2\cdot G_1\cdot\Delta_1)$
- $\theta := det(\tilde{\mathcal{F}})\cdot det(J_2)$

Claramente, el polinomio Q_1 es el cociente de $\frac{Q}{\theta}$, y además $\bar{Q}\bar{F} = \bar{\theta}\bar{G}$ se satisface en B. Mas aún, Q puede calcularse por medio de un circuito aritmético Γ sin divisiones en $K[X_1,\ldots,X_n]$ a partir de las entradas de $M_{X_1},\ldots,M_{X_n}$ y los parámetros de Γ' (nótese que para el cálculo de Q_1 se necesitan divisiones). La cota de complejidad en el enunciado de la proposición sigue de la reconstrucción del circuito aritmético que evalúa $F, G, J(F_1,\ldots,F_n), \Delta$ y los determinantes involucrados. □

2.3 Aplicaciones a la eliminación

En esta sección se aplican las técnicas desarrolladas a problemas de eliminación. Se estudiarán el problema de la consistencia de un sistema de ecuaciones polinomiales y la identidad de Bézout en caso que el sistema no posee soluciones comunes, la pertenencia de un polinomio y su representación en el caso de ideales intersección completa, se calculará el grado de una variedad algebraica y finalmente se dará una versión algorítmica del teorema de Quillen-Suslin.

2.3.1 El problema de la consistencia y la representación

Sean $F_1, \ldots, F_{t+1}$ polinomios en $\mathbb{Z}[X_1, \ldots, X_n]$, siendo $t \leq n$, tales que $F_1, \ldots, F_t$ forman una sucesión regular en $\mathbb{Q}[X_1, \ldots, X_n]$ y los ideales generados por $F_1, \ldots, F_i$ sobre $\mathbb{Q}[X_1, \ldots, X_n]$ son radicales para $i = 1, \ldots, t$ (de la sección 2.1.1 se deduce que pueden suponerse tales hipótesis). Supóngase además que los polinomios $F_1, \ldots, F_{t+1}$ tienen grado acotado por d, coeficientes de talla binaria no mayor que h y se evalúan por medio de un circuito aritmético de talla L y profundidad no escalar ℓ, cuya codificación puede generarse en espacio determinístico de tipo $O(\ell L h)$. Sean finalmente δ y η el grado geométrico y la altura geométrica del sistema definido por $F_1, \ldots, F_t$.

El problema a tratar es el siguiente:

1. Decidir si el sistema definido por $F_1, \ldots, F_{t+1}$ es consistente, es decir, si la variedad algebraica $V(F_1, \ldots, F_{t+1})$ constituída por los ceros comunes de $F_1, \ldots, F_{t+1}$ en $\mathbf{C}^n$ es vacía.

2. En caso de respuesta afirmativa en 1, hallar una identidad de Bézout:

$$1 = P_1 F_1 + \cdots + P_{t+1} F_{t+1}$$

donde los polinomios $P_1, \ldots, P_{t+1}$ pertenecen a $\mathbb{Q}[X_1, \ldots, X_n]$.

A efectos de resolver ambas cuestiones, supóngase calculada una solución geométrica de la variedad $V_t := V(F_1, \ldots, F_t)$ (lo cual implica que se ha calculado una solución geométrica para las variedades $V_i := V(F_1, \ldots, F_i)$ para $i = 1, \ldots, t-1$, que se supone alojada en memoria).

Sean $X_1, \ldots, X_{n-t}$ las variables libres respecto de V_t y $M^{(t)}_{X_{n-t+1}}, \ldots, M^{(t)}_{X_n}$ las matrices que describen el tensor de multiplicación en $\mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_t)$ con respecto a la base definida por el elemento primitivo u_t que resulta de la solución geométrica de V_t. Se define la matriz $M_{F_{t+1}}$ por:

$$M_{F_{t+1}} = F_{t+1}(X_1, \ldots, X_{n-t}, M^{(t)}_{X_{n-t+1}}, \ldots, M^{(t)}_{X_n})$$

Entonces, se tiene que la siguiente observación: $V(F_1, \ldots, F_{t+1})$ es vacía si y sólo si $det(M_{F_{t+1}}) \in \mathbb{Q} \setminus \{0\}$.

En primer lugar se supone que $V(F_1, \ldots, F_{t+1})$ es vacía. Dado que las variables $X_1, \ldots, X_n$ están en posición de Noether con respecto a a $F_1, \ldots, F_t$, se deduce que estos polinomios, considerados en $\mathbb{Q}(X_1, \ldots, X_{n-t})[X_{n-t+1}, \ldots, X_n]$, definen una variedad cero-dimensional $V_t = \{\eta^{(1)}, \ldots, \eta^{(\delta)}\}$ en $\overline{\mathbb{Q}(X_1, \ldots, X_{n-t})}^t$.

Con respecto a una base adecuada de $\mathbb{Q}[X_1, \ldots, X_n]/(F_1, \ldots, F_t)$, la matriz $M_{F_{t+1}}$ toma la forma:

$$\begin{pmatrix} F_{t+1}(\eta^{(1)}) & & \\ & F_{t+1}(\eta^{(2)}) & \\ & & F_{t+1}(\eta^{(\delta)}) \end{pmatrix}$$

Por lo tanto $det(M_{F_{t+1}}) = \prod_{k=1}^{\delta} F_{t+1}(\eta^{(k)})$. Si $det(M_{F_{t+1}}) \notin \mathbb{Q} \setminus \{0\}$, existe un punto $\alpha := (\alpha_1, \ldots, \alpha_{n-t}) \in \mathbb{C}^{n-t}$ tal que $det(M_{F_{t+1}})(\alpha_1, \ldots, \alpha_{n-t})$ está definido y es igual a 0.

Dado que el morfismo $\pi \quad V_t \to \mathbb{C}^{n-t}$ definido por $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_{n-t})$ es finito de rango δ, la fibra de α tiene a lo sumo δ puntos $\eta^{(1,\alpha)}, \ldots, \eta^{(\delta,alpha)}$.

Considérese ahora un elemento $\tilde{u}_t$ de modo tal que la solución geométrica asociada al mismo está definida en α. Dado que esta solución geométrica describe ahora la π-fibra de α se deduce que la matriz $\tilde{M}_{F_{t+1}}$ que representa la homotecia por F_{i+1} en la base inducida por la potencias de $\tilde{u}_t$ verifica la siguiente identidad:

$$det(\tilde{M}_{F_{t+1}})(\alpha) = \prod_{k=1}^{\delta} F_{t+1}(\eta^{(k,\alpha)})$$

Debido a la invariancia de $det(M_{F_{t+1}})$ por cambios de base, se tiene que

$$det(M_{F_{t+1}}) = det(\tilde{M}_{F_{t+1}})$$

En consecuencia, como $det(M_{F_{t+1}})(\alpha) = det(\tilde{M}_{F_{t+1}}) = 0$ existe $1 \leq k \leq \delta$ tal que $F_{t+1}(\eta^{(k,\alpha)}) = 0$. Este punto $\eta^{(k,\alpha)}$ es un cero común de $F_1, \ldots, F_{t+1}$ contrariamente a lo supuesto. De aquí se deduce que $det(M_{F_{t+1}}) \in \mathbb{Q} \setminus \{0\}$.

Recíprocamente, si $det(M_{F_{t+1}}) \in \mathbb{Q} \setminus \{0\}$ entonces la inversa de $M_{F_{t+1}}$ tiene coeficientes en $\mathbb{Q}[X_1, \ldots, X_{n-t}]$. Por lo tanto, las coordenadas de la primer columna de $M_{F_{t+1}}^{-1}$ representan un polinomio $P_{t+1} \in \mathbb{Q}[X_1, \ldots, X_{n-t}]$ que verifica $\bar{1} = \bar{P}_{t+1}\bar{F}_{t+1}$, lo cual implica que $V(F_1, \ldots, F_{t+1})$ es vacía.

En consecuencia, es suficiente con calcular el determinante $det(M_{F_{t+1}})$ y chequear si es un número racional no nulo. Para esto, se calcula $det(M_{F_{t+1}})$ evaluado en un punto $(p_1, \ldots, p_{n-t})$ de $\mathbb{Z}^{n-t}$ adecuado y se determina si el polinomio $det(M_{F_{t+1}})$ es el polinomio constante $det(M_{F_{t+1}})(p_1, \ldots, p_{n-t})$ por medio del test de Schwartz–Zippel (lema 20). Estos procesos de realizan sin divisiones por números enteros y polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$ empleando el mismo tipo de técnicas de la demostración del teorema 11. En conclusión, se tiene el siguiente resultado:

Teorema 12 *El problema de la consistencia puede resolverse mediante una máquina de Turing probabilística de error acotado en espacio* $O\big(n \log \delta(\ell + \log(\eta n h)\delta)\big)$ *y tiempo* $L(\ell n d h \delta)^{O(n \log \delta + \ell)}$

Supóngase ahora que $V(F_1, \ldots, F_{t+1})$ es vacía. El problema de la representación de la unidad en el ideal generado por $F_1, \ldots, F_{t+1}$ se resolverá por medio de la aplicación de la proposición 10 a fin de realizar divisiones módulo ciertos ideales intersección completa.

La idea es la siguiente: como $\bar{F}_{t+1} | \bar{1}$ módulo $(F_1, \ldots, F_t)$, por medio de la proposición 10 es posible calcular un elemento $\theta_{t+1} \in R_t := \mathbb{Q}[X_1, \ldots, X_{n-t}]$ y un polinomio $Q_{t+1} \in \mathbb{Q}[X_1, \ldots, X_n]$ de grado acotado por nd tal que $\theta_{t+1} | Q_{t+1}$ y se satisface la condición

$$\overline{\theta_{t+1} \cdot 1} = \overline{Q_{t+1} F_{t+1}} \text{ módulo } (F_1, \ldots, F_t)$$

Esto significa que $\theta_{t+1}(1 - F_{t+1}\frac{Q_{t+1}}{\theta_{t+1}})$ pertenece a $(F_1, \ldots, F_t)$ que es un ideal equidimensional de dimensión $n - t$ (lo cual implica que θ_t no es divisor

de cero módulo $(F_1,\ldots,F_t)$). Por lo tanto, se tiene que $1-F_{t+1}\frac{Q_{t+1}}{\theta_{t+1}}$ pertenece a $(F_1,\ldots,F_t)$, de donde se deduce que $F_t|1-F_{t+1}\frac{Q_{t+1}}{\theta_{t+1}}$ en $(F_1,\ldots,F_{t-1})$, lo cual implica a su vez que $\theta_{t+1}F_t|\theta_{t+1}\cdot 1-Q_{t+1}F_{t+1}\in(F_1,\ldots,F_{t-1})$.

Posteriormente se divide el polinomio $\theta_{t+1}\cdot 1-Q_{t+1}F_{t+1}$ por $\theta_{t+1}F_t$ módulo $(F_1,\ldots,F_{t-1})$, consiguiéndose de esta manera un elemento $\theta_t\in R_{t-1}:=\mathbb{Q}[X_1,\ldots,X_{n-t+1}]$ y un polinomio $Q_t\in\mathbb{Q}[X_1,\ldots,X_n]$ de grado no mayor que nd tal que $\theta_t|Q_t$ en R_{t-1} y

$$\theta_t\theta_{t+1}\cdot 1-\theta_tQ_{t+1}F_{t+1}-Q_t\theta_{t+1}F_t\in(F_1,\ldots,F_{t-1})$$

Prosiguiendo con este esquema en forma recursiva, se calculan polinomios $\theta_1,\ldots,\theta_{t+1},Q_1,\ldots,Q_{t+1}\in\mathbb{Q}[X_1,\ldots,X_n]$, tales que se verifican las siguientes propiedades:

- $\theta_i\in R_{i-1}:=\mathbb{Q}[X_1,\ldots,X_{n-i-1}]$ para $i=1,\ldots,t+1$.
- $Q_i\in\mathbb{Q}[X_1,\ldots,X_n]$ y tiene grado acotado por nd para todo $i=1,\ldots,t+1$.
- $\theta_i|Q_i$ en R_{i-1}.
- $\theta_{t-i}\cdots\theta_{t+1}\cdot 1-Q_{t-i}\cdots\theta_{t+1}F_{t-i}-\cdots-\theta_{t-i}\cdots\theta_tQ_{t+1}F_{t+1}\in(F_1,\ldots,F_{t-i-1})$

En consecuencia, al final del último paso recursivo se tiene la identidad:

$$\theta_1\cdots\theta_{t+1}\cdot 1=Q_1\theta_2\cdots\theta_{t+1}F_1+\theta_1Q_2\theta_3\cdots\theta_{t+1}F_1+\cdots+\theta_1\cdots\theta_tQ_{t+1}F_{t+1} \tag{2.18}$$

donde cada $\theta_i|Q_i$ en R_{i-1}. Por lo tanto, aplicando la proposición 7, se calcula sin divisiones un entero no nulo $a\in\mathbb{Z}^*$ y polinomios $P_1,\ldots,P_{t+1}\in\mathbb{Z}[X_1,\ldots,X_n]$ tales que $P_i=a\frac{Q_i}{\theta_i}$ para $i=1,\ldots,t+1$.

Reemplazando esta identidad en (2.18) se obtiene la representación:

$$a=P_1F_1+\cdots+P_{t+1}F_{t+1}$$

Para estimar la complejidad de este proceso, se estudia el i-ésimo paso recursivo. En este paso, se calculan polinomios $\theta_{t-i+2}\in R_{t-i+1}$ y $Q_{t-i+2}\in\mathbb{Q}[X_1,\ldots,X_n]$ a partir de θ_{t-i+3} y Q_{t-i+3} de la siguiente manera:
si $M_{X_{n-t+i-1}},\ldots,M_{X_n}$ son las matrices con coeficientes en $\mathbb{Q}(X_1,\ldots,X_{n-t+i-1})$ que describen el tensor de multiplicación en $\mathbb{Q}[X_1,\ldots,X_n]/(F_1,\ldots,F_{t-i+1})$,

se calculan el determinante jacobiano $J(X_1,\ldots,X_n)$ y el determinante seudo-jacobiano $\Delta(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$ del ideal $(F_1,\ldots,F_{t-i+1})$ definidos en la proposición 10 y se reemplazan las variables $X_{n-t+i-1},\ldots,X_n$ por las matrices $M_{X_{n-t+i-1}},\ldots,M_{X_n}$ en los polinomios J,Δ y Q_{t-i+3} (no es necesario realizar este reemplazo en θ_{t-i+3}, ya que este polinomio no depende de $X_{n-t+i-1},\ldots,X_n$).

Los polinomios $J = J^{(i)},\Delta = \Delta^{(i)}$ correspondientes a la i-ésima etapa recursiva pueden calcularse simultáneamente para todo $i = 1,\ldots,n$. En consecuencia, el reemplazo matricial en éstos no produce un incremento de la complejidad asintótica del proceso. No ocurre lo mismo con Q_{t-i+3}.

Sin embargo, observando que:

- $Q_{t-i+3} = Tr(\tilde{Q}\cdot\tilde{J}\cdot\tilde{P}\cdot\tilde{\Delta}) = Tr(\tilde{Q}\cdot\tilde{J}\cdot\tilde{P})\cdot Tr(\tilde{\Delta})$,

- sólo $Tr(\tilde{\Delta})$ depende de las variables $X_{n-t+i-1},\ldots,X_n$, y

- $\tilde{\Delta} = \tilde{\Delta}$ se calcula simultáneamente para todo $i = 1,\ldots,n$,

se deduce que la talla del circuito que resulta del proceso recursivo crece de manera *aditiva*, lo cual implica una talla total aritmética de tipo $L(nd\delta)^{O(1)}$ (que a su vez implica una talla booleana de tipo $L(dh\eta\delta)^{O(1)}$).

La profundidad no escalar es de tipo $O\Big(n^2\log(n\delta)(\ell+\log(n\delta))\Big)$, ya que, una vez calculada la solución geométrica de las variedades $V(F_1,\ldots,F_i)$ para $i = 1,\ldots,n$, se tiene un proceso recursivo que en cada etapa opera con matrices de tamaño no superior a $\delta^{O(1)}$ y manipulaciones algebraicas similares a las realizadas en la construcción del circuito que calcula la solución geométrica de $V(F_1,\ldots,F_t)$. Asimismo, debido a la talla binaria de los números con que se opera, se tiene una profundidad booleana de tipo $O\Big(n^2\log(n\delta)(\ell+\log(nh\eta\delta))\Big)$.

Aplicando la demostración del teorema 1, se deduce el siguiente teorema:

Teorema 13 *El problema de la representación de 1 en el caso de un sistema no consistente puede resolverse por medio de una máquina de Turing probabilística de error acotado en espacio* $O\Big(n^2\log(n\delta)(\ell+\log(nh\eta\delta))\Big)$.

2.3.2 El problema de la pertenencia y la representación en el caso de ideales intersección completa

Sean $F, F_1, \ldots, F_t$ polinomios en $\mathbb{Z}[X_1, \ldots, X_n]$ tales que $F_1, \ldots, F_t$ forman una sucesión regular en $\mathbb{Q}[X_1, \ldots, X_n]$ y los ideales generados por $F_1, \ldots, F_i$ sobre $\mathbb{Q}[X_1, \ldots, X_n]$ son radicales para $i = 1, \ldots, t$. Se supone que los polinomios $F, F_1, \ldots, F_t$ tiene grados acotado por d, coeficientes de talla binaria no mayor que h y se evalúan por medio de un circuito aritmético de talla L y profundidad no escalar ℓ, cuya codificación puede generarse en espacio determinístico de tipo $O(\ell L h)$. Sean finalmente δ y η el grado geométrico y la altura geométrica del sistema definido por $F_1, \ldots, F_t$.

El problema a tratar es la pertenencia de F al ideal generado por $F_1, \ldots, F_t$ y su representación en este ideal. Es decir, se desea determinar si F pertenece al ideal generado por $F_1, \ldots, F_t$ en $\mathbb{Q}[X_1, \ldots, X_n]$, y en tal caso, hallar polinomios $P_1, \ldots, P_t \in \mathbb{Z}[X_1, \ldots, X_n]$ tales que se verifica la siguiente identidad:

$$F = P_1 F_1 + \cdots + P_t F_t$$

En primer lugar se estudia el problema de la pertenencia. Se observa que $F \in (F_1, \ldots, F_t)$ si y sólo si la homotecia definida por F en $\mathbb{Q}[X_1, \ldots, X_n]$ es nula. Para calcular la matriz de esta homotecia, se utiliza la base definida por un elemento primitivo u de la variedad $V(F_1, \ldots, F_t)$. Si $M_{X_{n-t+1}}, \ldots, M_{X_n}$ son las matrices que representan el tensor de multiplicación con respecto a esta base, se tiene entonces que la matriz de la homotecia por F en esta base es $F(X_1, \ldots, X_{n-t}, M_{X_{n-t+1}}, \ldots, M_{X_n})$.

Finalmente, para chequear que esta matriz tiene todas sus entradas nulas, será necesario utilizar δ^2 puntos elegidos aleatoriamente en cierto conjunto de acuerdo con la estrategia del lema 20.

Una vez establecida la pertenencia de F a $(F_1, \ldots, F_t)$, la representación de F en el ideal se realiza con la técnica descripta en la sección anterior, comenzando con F en lugar del polinomio 1.

De acuerdo con los teoremas 11 y 13, se deduce el siguiente resultado:

Teorema 14 *El problema de la pertenencia y la representación para ideales intersección completa puede resolverse por medio de una máquina de Turing probabilística de error acotado en espacio* $O\big(n^2 \log(n\delta)(\ell + \log(nh\eta\delta))\big)$.

2.3.3 Cálculo del grado de una variedad

Sea r la dimensión de V y $V = V_r \cup \cdots \cup V_0$ la descomposición de V en componentes equidimensionales donde V_i tiene dimensión i para $i = 1, \ldots, r$ (ver sección 1.4.7). Para cada componente V_i, se define el grado de V_i como usualmente (ver sección 2.1.2) y se nota esta cantidad por $gr(V_i)$. Siguiendo [88], se define el grado de una variedad algebraica arbitraria V como la suma de los grados de sus componentes equidimensionales, es decir, $gr(V) := gr(V_r) + \cdots + gr(V_0)$.

Según se demuestra en [88], si se eligen i hiperplanos genéricos $H_1^{(i)}, \ldots, H_i^{(i)}$ se verifican las siguientes condiciones:

1. $V_i \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)}$ es una variedad cero-dimensional de cardinal $gr(V_i)$.

2. $V_j \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)} = \emptyset$ si $j < i$.

3. $V_j \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)}$ es una variedad equidimensional de dimensión $j - i$ si $j > i$.

En consecuencia, los puntos aislados de $V \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)}$ (es decir, las componentes irreducibles de dimensión cero) son los puntos de $V_i \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)}$. Por lo tanto, calculando esta cantidad se obtiene $gr(V_i)$.

A fin de realizar el proceso descripto en forma algorítmica, es necesario estimar el grado de los polinomios que representan la condición genérica requerida para los coeficientes de los hiperplanos $H_1^{(i)}, \ldots, H_i^{(i)}$.

De los resultados de la sección 1.4.7 se deduce que cada componente V_i se puede describir por medio de polinomios $G_1^{(i)}, \ldots, G_{i_i}^{(i)}$ en $\mathbb{Z}[X_1, \ldots, X_n]$ de grado acotado por d^n. Se introducen nuevas variables A_{jk}, B_j para $1 \leq j \leq i$ y $1 \leq k \leq n$ y los hiperplanos $H_k^{(i)}$ definidos por:

$$H_j^{(i)} := \sum_{k=1}^{n} A_{jk} X_k + B_j$$

para $k = 1, \ldots, j$.

El hecho que la condición 1 vale genéricamente significa que reemplazando las variables A_{jk}, B_j por puntos de un abierto Zariski de $\mathbf{C}^{ni+1}$, los hiperplanos así construídos intersecan a V_i en $gr(V_i)$ puntos (ver [88]). Por lo tanto, la

variedad W que consiste de las soluciones en $\overline{\mathbf{C}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n]}^n$ del siguiente sistema:

$$W := \{G_1^{(i)} = 0, \ldots, G_{i_1}^{(i)} = 0, H_1^{(i)} = 0, \ldots, H_i^{(i)} = 0\}$$

es cero-dimensional y consiste de $gr(V_i)$ puntos. De [114, Section 4], se deduce que existe un circuito aritmético bien paralelizable de profundidad no escalar $O(n^2 \log d)$ que calcula los coeficientes en $\mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n]$ de los siguientes polinomios:

- una forma lineal $u \in \mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n][X_1, \ldots, X_n]$, y
- un polinomio $p \in \mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n][T]$ de grado $gr(V_i)$

tales que u separa los puntos de W y $\frac{1}{\alpha}p$ es el polinomio minimal que anula a u sobre W, donde $\alpha \in \mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n]$ es el coeficiente principal de p.

Sea γ un vector de $\mathbb{Z}^{ni+1}$ tal que si se reemplaza en p las variables A_{jk}, B_j por γ el polinomio resultante de $\mathbb{Z}[T]$ tiene grado $gr(V_i)$ y es libre de cuadrados. Entonces los hiperplanos que se obtienen a partir de γ cortan a V_i en exactamente $gr(V_i)$. Por lo tanto, la condición genérica que deben cumplir los coeficientes de los hiperplanos a elegir es no anular al coeficiente principal α de p y al discriminante $\Delta \in \mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n]$ de p. Y el producto de ambos polinomios puede calcularse en profundidad no escalar $O(n^2 \log d)$ (para el cálculo de Δ se utilizan las ideas de la sección 1.3.2).

Ahora es necesario introducir una condición genérica sobre los coeficientes de los hiperplanos $H_1^{(i)}, \ldots, H_i^{(i)}$ que asegure que se cumple la condición 2. Para esto, es necesario apelar a una versión diofántica del Nullstellensatz efectivo. Dado que genéricamente ocurre que $(V_{i-1} \cup \cdots \cup V_0) \cap (H_1^{(i)} \cup \ldots \cup H_i^{(i)})$ es vacía, esto mismo ocurre cuando se considera la situación en $\overline{\mathbf{C}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n]}^n$. Aplicando el Nullstellensatz efectivo en la versión de [114], se deduce la existencia de un polinomio no nulo $a \in \mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n]$, calculable por un circuito aritmético de profundidad no escalar $O(n^2 \log d)$, que pertenece al ideal generado por los polinomios que definen $V_{i-1} \cup \cdots \cup V_0$ (ver sección 1.4.7) y $H_1^{(i)}, \ldots, H_i^{(i)}$.

Cualquier evaluación de las variables A_{jk}, B_j en un vector $\gamma \in \mathbb{Z}^{ni+1}$ tal que $a(\gamma) \neq 0$ asegura que la variedad lineal definida por los hiperplanos

$H_1^{(i)}(\gamma), \ldots, H_i^{(i)}(\gamma)$ no corta a $V_{i-1} \cup \cdots \cup V_0$. Por lo tanto, el polinomio a es la condición genérica que se busca.

Finalmente, resta imponer la tercera condición, es decir, que $W_j := V_j \cap H_1^{(i)} \cap \ldots \cap H_i^{(i)}$ no tenga puntos aislados si $j > i$. Con los mismos argumentos de antes, se considera la situación en $\overline{\mathbf{C}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n]}^n$. Aplicando [114] nuevamente, con profundidad no escalar $O(n^2 \log d)$ se obtiene la solución geométrica de una variedad cero-dimensional $\tilde{W}_j$ que contiene los puntos aislados de W_j. Sea $u \in \mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n][X_1, \ldots, X_n]$ la forma lineal que se calcula y $p \in \mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n][T]$ el polinomio minimal de la misma. Dado que la variedad W_j no posee puntos aislados, la intersección entre la variedad calculada $\tilde{W}_j$ y W_j debe ser vacía. Para constatar esta condición será suficiente con reemplazar las variables $X_1, \ldots, X_n$ en los polinomios que definen W_j por las parametrizaciones obtenidas en la solución geométrica de $\tilde{W}_j$ (que de esta manera se transforman en polinomios de $\mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n][u]$) y chequear que el máximo común divisor de los mismos y $p(u)$ sea 1.

Según la estrategia desarrollada en la subsección 1.3.2, se halla un polinomio $b \in \mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n]$ que se escribe como una combinación polinomial de los polinomios involucrados. La no anulación de este polinomio asegura que la intersección $W_j \cap \tilde{W}_j$ es vacía, por lo cual b constituye la condición genérica restante.

En conclusión, multiplicando las $O(n)$ condiciones obtenidas se obtiene un polinomio $P_i \in \mathbb{Z}[A_{jk}, B_j; 1 \leq j \leq i, 1 \leq k \leq n]$, calculable con profundidad $O(n^2 \log n \log d)$, que verifica que cualquier vector $\gamma \in \mathbb{Z}^{ni+1}$ tal que $P_i(\gamma) \neq 0$ provee los coeficientes de i hiperplanos con todas las condiciones requeridas. Aplicando el lema 20, se obtiene un tal vector aleatoriamente con talla binaria $O(n^2 \log n \log d)$.

Luego, es necesario calcular los puntos aislados de $V \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)}$ para $i = 1, \ldots, n$. Se sigue entonces esencialmente el procedimiento descripto en la sección 1.4.4. En primer lugar, se genera aleatoriamente una n-upla en $\mathbb{Z}^n$ a partir de la cual se hallan los coeficientes de n polinomios que definen una variedad W que difiere de $V \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)}$ sólo en finitos puntos. Por medio de una deformación homotópica posterior se pasa al caso cero-dimensional proyectivo. Dada una forma lineal ℓ, según se demuestra en [80], el polinomio $p \in \mathbb{Z}[T]$ que se calcula verifica que $p(\ell)$ se anula sobre los puntos aislados de $V \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)}$.

Una vez que se tiene un mecanismo para calcular proyecciones sobre rectas, éste se utiliza a fin de calcular las proyecciones necesarias para la aplicación de los lemas 29 y 30. De esta manera, se halla la solución geométrica de los puntos aislados de W (que contienen a los puntos aislados de $V \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)}$). Finalmente, reemplazando las parametrizaciones obtenidas por la solución geométrica de W en las ecuaciones que definen la variedad $V \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)}$, se obtienen ciertos polinomios univariados cuyo máximo común divisor tiene grado igual a la cantidad de puntos aislados de $V \cap H_1^{(i)} \cap \cdots \cap H_i^{(i)}$.

Teniendo en cuenta que el procedimiento opera con matrices de tamaño $(nd)^{O}(n)$ cuyas entradas tienen talla binaria de tipo shd^n, se deduce el siguiente teorema:

Teorema 15 *Existe una máquina de Turing probabilística de error acotado que calcula el grado de V en espacio $O\big(n^2 \log^2(hsd)\big)$.*

2.3.4 Una versión efectiva del Teorema de Quillen-Suslin

Una matriz F en $\mathbb{Z}[X_1, \ldots, X_n]^{r \times s}$ con $s \geq r$ se dice *unimodular* si y sólo si el ideal generado en $\mathbb{Q}[X_1, \ldots, X_n]$ por todos sus menores de tamaño $r \times r$ es el ideal trivial.

Sea F una matriz unimodular en $\mathbb{Z}[X_1, \ldots, X_n]^{r \times s}$. Denótese por $gr(F)$ el máximo de los grados de las entradas de F y sea $d = 1 + deg(F)$. Del teorema de Quillen-Suslin se deduce la existencia de una matriz M unimodular de tamaño $s \times s$ tal que $FM = [I_r, 0]$, donde $[I_r, 0]$ denota la matriz de $r \times s$ que se obtiene agregando a la matriz identidad I_r de $r \times r$, $s - r$ columnas nulas.

El problema es hallar algorítmicamente la matriz M. El proceso que se realiza para tal fin consta de n etapas, en las que se construyen matrices $M_1, \ldots, M_n$ unimodulares de tamaño $s \times s$ que verifican la siguiente propiedad:

$$F \cdot M_n \cdots M_{i+1} = \big(F_{ij}(X_1, \ldots, X_i, 0, \ldots, 0)\big)_{1 \leq i \leq r, 1 \leq j \leq s}$$

donde $F := \big(F_{ij}(X_1, \ldots, X_n)\big)_{1 \leq i \leq r, 1 \leq j \leq s}$.

Dado que la matriz $F \cdot M_1 \cdots M_n$ es unimodular y tiene entradas en $\mathbb{Q}$, mediante un proceso estándar de triangulación ésta puede reducirse a la forma $[I_r, 0]$. Si M_0 es la matriz (unimodular) que realiza esta triangulación, $M := M_n \cdots M_0$ es la matriz buscada.

Obsérvese que las matrices $\big(F_{ij}(X_1, \ldots, X_i, 0, \ldots, 0)\big)_{1 \le i \le r, 1 \le j \le s}$ pueden producirse simultáneamente, por lo que el cálculo de las matrices $M_0, \ldots, M_n$ puede realizarse en paralelo.

Siguiendo el esquema propuesto en [64] (ver también [65]), el proceso del cálculo de cada matriz M_i se divide en cuatro etapas. A fin de simplificar la notación, se describirá solamente el cálculo de M_n.

En la primera etapa, se construye una sucesión $c_1, \ldots, c_N$ de polinomios de grado acotado por $(rd)^2$ (donde N se determinará posteriormente) tales que:

- $1 \in (c_1, \ldots, c_N)$
- Para todo $k \in \{1, \ldots, N\}$, existe una matriz no singular $\Lambda_k \in GL_s(\mathbb{Q})$ tal que:

$$c_k = Res\Big(det[F_1^{(k)}, \ldots, F_r^{(k)}], det[F_1^{(k)}, \ldots, F_{r-1}^{(k)}, F_{r+1}^{(k)}]\Big)$$

donde $F_1^{(k)}, \ldots, F_{r+1}^{(k)}$ denota las columnas de la matriz $F^{(k)} := F \cdot \Lambda_k$.

Se elegirán matrices Λ_k con el siguiente aspecto:

$$\Lambda_k = \begin{pmatrix} 1 & & & & & & \\ \alpha_1 & 1 & & & & & \\ \alpha_1\beta_1 & \alpha_2 & & & & & \\ \alpha_1\beta_1^2 & \alpha_2\beta_2 & & & & & \\ \vdots & \vdots & 1 & & & & \\ & & \alpha_{r-1} & 1 & & & \\ & & \alpha_{r-1}\beta_{r-1} & 0 & 1 & & \\ & & \vdots & & \alpha_r & & \\ & & & & & & \\ \alpha_1\beta_1^{s-2} & \alpha_2\beta_2^{s-3} & \alpha_{r-1}\beta_{r-1}^{s-r} & 0 & \alpha_r^{s-r-1} & & 1 \end{pmatrix} \tag{2.19}$$

donde $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_{r-1}$ son números enteros.

Se trata entonces de hallar enteros $\alpha_1^{(k)}, \ldots, \alpha_r^{(k)}, \beta_1^{(k)}, \ldots, \beta_{r-1}^{(k)}$ para $k = 1, \ldots, N$ de talla binaria controlada y en la menor cantidad posible de manera que la variedad definida por $c_1, \ldots, c_N$ sea vacía.

Se consideran indeterminadas $S_1, \ldots, S_r, T_1, \ldots, T_{r-1}$ y la matriz $\Lambda \in \mathbb{Z}[S_i, T_j; 1 \leq i \leq r, 1 \leq j \leq r-1]$ que se obtiene si se reemplaza en la matriz Λ_k de (2.19) cada α_i por S_i y cada β_j por T_j. Asimismo, se definen:

- $F' := [F'_1, \ldots, F'_{r+1}] = F \cdot \Lambda$
- $D'_1 := det[F'_1, \ldots, F'_r]$
- $D'_2 := det[F'_1, \ldots, F'_{r-1}, F'_{r+1}]$
- $c := Res_{X_n}(D'_1, D'_2)$

El punto clave es que, para cada $x \in \mathbf{C}^n$, existe un vector $(\alpha, \beta) \in \mathbb{N}^{2r-1}$ tal que $c(x, \alpha, \beta) \neq 0$ ([64, Proposition 5.6]). Por lo tanto, se tiene que $c(x, S_1, \ldots, S_r, T_1, \ldots, T_{r-1})$ es un polinomio de $\mathbb{Z}[S_i, T_j; 1 \leq i \leq r, 1 \leq j \leq r-1]$ no nulo para cada $x \in \mathbf{C}^n$. Además, $c(x, S_1, \ldots, S_r, T_1, \ldots, T_{r-1})$ se calcula con talla (aritmética) de tipo $O(s^3 r^4 (rd)^{2n})$ y profundidad no escalar $O(n \log(sd))$. Por la proposición 5 existe un conjunto questor de $N := O(s^7 (rd)^{5n})$ elementos $(\alpha^{(k)}, \beta^{(k)}) \in \{1, \ldots, u\}^{2r-1}$ para $k = 1, \ldots, t$, donde $u := (sd)^{O(n)}$, tal que para todo $x \in \mathbf{C}^n$ existe $k \in \{1, \ldots, N\}$ que verifica $c(x, \alpha^{(k)}, \beta^{(k)}) \neq 0$. Mas aún, un tal conjunto questor puede ser hallado aleatoriamente con probabilidad mayor que $1 - u^{\frac{N}{6}} \gg \frac{1}{2}$.

Entonces se define $c_k := c(X_1, \ldots, X_n, \alpha^{(k)}, \beta^{(k)})$ para $k = 1, \ldots, N$. Obsérvese que los polinomios $c_1, \ldots, c_N$ tienen grado acotado por $(rd)^2$ y su cómputo involucra el cálculo del determinante de $O(s^7 (rd)^{5n})$ matrices polinomiales de $r \times r$.

En la segunda etapa se halla una representación:

$$X_n = a_1 c_1 + \cdots + a_N c_N$$

de la variable X_i en el ideal generado por los polinomios $c_1, \ldots, c_N$ generados en la primera etapa.

En la tercer etapa se construyen N matrices unimodulares $M_n^{(1)}, \ldots, M_n^{(N)}$ en $\mathbb{Q}[X_1, \ldots, X_n]^{s \times s}$ de modo tal que, definiendo $b_k := \sum_{h=1}^{k} a_h c_h$ para $k = 1, \ldots, N$, se tiene la identidad:

$$F^{(k)}(b_k) M_n^{(k)} = F^{(k)}(b_{k-1}) \tag{2.20}$$

donde $F^{(k)} = F \cdot \Lambda_k$ y $F^{(k)}(b_k)$ denota la matriz que se obtiene a partir de $F^{(k)}$ cuando se evalúa la variable X_n de las entradas de $F^{(k)}$ en b_k.

A partir de la identidad (2.20) se deduce que la matriz $E_k := \Lambda_k \cdot M_k \cdot \Lambda_k^{-1}$ verifica la propiedad:

$$F(b_k)E_k = F(b_{k-1}) \tag{2.21}$$

Como $c_k = Res_{X_n}(D_1^{(k)}, D_2^{(k)})$, existen polinomios $g, h \in \mathbb{Q}[X_1, \ldots, X_n]$ tales que

$$c_k = g \cdot D_1^{(k)} + h \cdot D_2^{(k)}$$

Dado que c_k no depende de X_k, se deduce que:

$$c_k = g(b_k) \cdot D_1^{(k)}(b_k) + h(b_k) \cdot D_2^{(k)}(b_k) \tag{2.22}$$

Siguiendo la demostración del Lemma 4.5 en [64], si $F_j^{(k)}$ denota la j-ésima columna de $F^{(k)}$, dado que $b_k \equiv b_{k-1}$ módulo $c_k \cdot \mathbb{Q}[X_1, \ldots, X_n]$, mediante un desarrollo en series de Taylor de los coeficientes de $F_j^{(k)}$ se demuestra la existencia de un vector columna $G_j^{(k)} \in \mathbb{Q}[X_1, \ldots, X_n]^{r \times 1}$ que verifica

$$F_j^{(k)}(b_k) - F_j^{(k)}(b_{k-1}) = c_k G_j^{(k)} \tag{2.23}$$

Combinando (2.22) y (2.23) se obtiene la identidad:

$$F_j^{(k)}(b_k) - F_j^{(k)}(b_{k-1}) = D_1^{(k)}\left(g(b_k)G_j^{(k)}\right) + D_2^{(k)}\left(h(b_k)G_j^{(k)}\right) \tag{2.24}$$

Sean B_1 y B_2 las siguientes matrices:

$$B_1^{(k)} := Adj[F_1^{(k)}(b), \ldots, F_r^{(k)}(b_k)]$$

$$B_2^{(k)} := Adj[F_1^{(k)}(b), \ldots, F_{r-1}^{(k)}(b_k), F_{r+1}^{(k)}(b_k)]$$

Entonces, se tienen las identidades:

$$D_1^{(k)}(b_k)g(b_k)G_j^{(k)} = [F_1^{(k)}(b_k), \ldots, F_r^{(k)}(b_k)]B_1^{(k)}g(b_k)G_j^{(k)} := \sum_{j=1}^{r} \eta_j F_j^{(k)}(b_k)$$

$$D_2^{(k)}(b_k)h(b_k)G_j^{(k)} = [F_1^{(k)}(b_k), \ldots, F_{r-1}^{(k)}(b_k), F_{r+1}^{(k)}(b_k)]B_2^{(k)}h(b_k)G_j^{(k)}$$
$$:= \textstyle\sum_{j \neq r} \tilde{\eta}_j F_j^{(k)}(b_k)$$

donde $(\eta_1, \ldots, \eta_r)^t := B_1^{(k)} g(b_k) G_j^{(k)}$ y $(\tilde{\eta}_1, \ldots, \tilde{\eta}_{r-1}, \tilde{\eta}_{r+1})^t := B_2^{(k)} h(b_k) G_j^{(k)}$. Estas identidades, aplicadas en (2.24), dan la siguiente igualdad:

$$F_j^{(k)}(b_k) - F_j^{(k)}(b_{k-1}) = (\eta_1 + \tilde{\eta}_1) F_1^{(k)}(b_k) + \cdots + \eta_r F_r^{(k)}(b_k) + \tilde{\eta}_{r+1} F_{r+1}^{(k)}(b_k)$$

Utilizando esta ecuación para $j = r+2, \ldots, s$ se construye una matriz unimodular $\tilde{M}^{(k)}$ que verifica:

$$F^{(k)}(b_k)\tilde{M}^{(k)} = [F_1^{(k)}(b_k), \ldots, F_{r+1}^{(k)}(b_k), F_{r+2}^{(k)}(b_{k-1}), \ldots, F_s^{(k)}(b_{k-1})]$$

Para concluir la construcción de la matriz $M^{(k)}$, se define la siguiente matriz unimodular $T^{(k)}$ de tamaño $(r+1) \times (r+1)$:

$$T^{(k)} := \frac{1}{c_k} Adj \begin{pmatrix} F_1^{(k)}(b_k) & \cdots & F_r^{(k)}(b_k) & F_{r+1}^{(k)}(b_k) \\ 0 & \cdots & -h(b_k) & g(b_k) \end{pmatrix} \cdot \begin{pmatrix} F_1^{(k)}(b_{k-1}) & \cdots & F_r^{(k)}(b_{k-1}) & F_{r+1}^{(k)}(b_{k-1}) \\ 0 & \cdots & -h(b_{k-1}) & g(b_{k-1}) \end{pmatrix}$$

Luego, $M^{(k)} := \tilde{M}^{(k)} \cdot (T^{(k)} \oplus I_{s-r-1})$ es la matriz buscada.

Finalmente, en la cuarta etapa se calcula el producto $M_n := \prod_{k=1}^{N} E_k = \prod_{k=1}^{N} \Lambda_k M^{(k)} \Lambda_k^{-1}$. Dado que se tienen las identidades:

$$\begin{aligned} F = F(X_n) &= F(b_N) \\ F(b_N) E_n &= F(b_{N-1}) \\ &\vdots \\ F(b_1) E_1 &= F(b_0) = F(0) \end{aligned}$$

se tiene que la matriz M_n verifica las condiciones requeridas.

Luego de n procesos paralelos como el descripto, se obtiene una familia uniforme de circuitos booleanos que satisface las condiciones requeridas por el teorema 1. Entonces, se puede aplicar la estrategia de la sección 1.2 y concluir:

Teorema 16 *El Teorema de Quillen-Suslin puede realizarse en forma algorítmica por medio de una máquina de Turing probabilística de error acotado en espacio* $O(n^4 \log^2(shd))$.

Capítulo 3

Tradeoffs espacio–tiempo

Las medidas mas naturales de complejidad computacional son el espacio y el tiempo, donde el tiempo se mide -generalmente hablando- por el número de pasos discretos en una computación y el espacio por el tamaño de las distintas locaciones de memoria que se acceden durante la computación.

Lo que se intenta es clasificar la complejidad *intrínseca* de un problema dado, pero un problema puede ser resuelto de muchas maneras diferentes. ¿Cual debería ser *la* solución óptima para un problema? El deseo natural es elegir aquella que posea las *menores* complejidades posibles, las cuales se identificarían como las inherentes al problema.

Dado que se consideran dos medidas de complejidad, las cuales se representan mediante funciones y no mediante números naturales, es posible que no existan soluciones que puedan identificarse como óptimas para la resolución de un problema dado. Podrían existir relaciones o *tradeoffs* entre el espacio y el tiempo requerido por cualquier solución (algoritmo) de determinado problema que hagan imposible la tarea de elegir una medida de espacio o tiempo como inherente al problema.

A fin de entender mejor las posibilidades y las dificultades que se aparecen en la búsqueda de las mejores soluciones de cada problema, es necesario estudiar el tradeoff espacio-tiempo del mismo. De esta manera, se podrá identificar una clase de soluciones que son óptimas en cierto sentido, de las cuales puede elegirse aquella que mejor se adapta a las facilidades disponibles.

En este capítulo se estudiarán tradeoffs espacio–tiempo en teoría de complejidad algebraica. Mas precisamente, se estudiarán tradeoffs para los procedimientos de evaluación de polinomios, caso que es central ya que los poli-

nomios representan los objetos básicos del lenguaje de la teoría de complejidad algebraica.

En particular, el análisis de los tradeoffs espacio-tiempo brindará la posibilidad de obtener cotas inferiores para la complejidad de espacio de los procedimientos de álgebra computacional, cuyo estudio parece estar relegado en el ámbito de la computación algebraica.

Es claro que todo polinomio puede evaluarse con un número constante de registros por medio de la regla de Horner, y observaciones similares pueden realizarse en otros modelos de complejidad algebraica (ver [13], [127] por ejemplo). Esto aparentemente indicaría que el espacio no es un recurso significativo en el estudio de la complejidad de la evaluación de polinomios, lo cual constituye al mismo tiempo una paradoja.

En este capítulo se tratará de arrojar alguna luz en esta dirección, mostrando cotas inferiores de complejidad para el espacio requerido en procesos de evaluación polinomial. Por ejemplo, se concluirá que la "mayoría" de los polinomios univariados de grado d requiere $\Omega(d^{\frac{1}{4}})$ registros de memoria para realizar una estrategia de evaluación óptima en términos de complejidad no escalar (como la de [139]).

3.1 Espacio y tiempo para circuitos aritméticos

En primer lugar, se discutirá como las medidas de complejidad de espacio y tiempo pueden representarse adecuadamente en el modelo básico de computación, es decir, el de los circuitos aritméticos. Intuitivamente se podría decir que espacio y tiempo computacionales de un circuito aritmético tienen una representación natural en cualquier pebble game realizado sobre el grafo de computación (ver por ejemplo [25]).

Sin embargo, esta definición combinatoria del espacio y el tiempo no es conveniente para la aplicación de los métodos geométricos que se utilizarán a fin de demostrar cotas inferiores de complejidad -el principal objetivo de este capítulo. Por este motivo, se transformará el modelo de complejidad basado en los pebble games primero en un modelo de locación de registros, y posteriormente éste último en un modelo geométrico de computación.

3.1.1 Del modelo de pebble games al de locación de registros

Sea K un cuerpo infinito y $X_1, \ldots, X_n$ indeterminadas sobre K. Por $K[X_1, \ldots, X_n]$ se denota el anillos de polinomios en n variables sobre K y por $K(X_1, \ldots, X_n)$ su cuerpo de cocientes.

Sea F un elemento de $K(X_1, \ldots, X_n)$, es decir, una función racional sobre K en las variables $X_1, \ldots, X_n$. Se recuerdan las siguientes nociones estándar de teoría de complejidad algebraica (ver [31], [172], [168], [89], [72], [75], [138], [37]).

Definición 6 *Un* straight-line program *en $K(X_1, \ldots, X_n)$ que calcula una función racional F es una sucesión $\beta = (Q_1, \ldots, Q_r)$ de elementos del cuerpo $K(X_1, \ldots, X_n)$ con las siguientes propiedades:*

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

Las funciones racionales $Q_1, \ldots, Q_r$ se llaman los *resultados intermedios* del straight-line program β y la función racional $F = Q_r$ es el resultado final o *salida* de β. En lo sucesivo, se asumirá sin pérdida de generalidad que todos los resultados intermedios $Q_1, \ldots, Q_r$ de β son no nulos.

A un straight-line program $\beta = (Q_1, \ldots, Q_r)$ dado en $K(X_1, \ldots, X_n)$ se le asocia como usualmente un *grafo dirigido acíclico* que se notará por $\Gamma(\beta)$ y será llamado el *grafo de computación* del straight-line program β. El grafo de computación $\Gamma(\beta)$ tiene r vértices llamados nodos. Cada nodo de $\Gamma(\beta)$ tiene indegree 0 o 2 y está etiquetado por un elemento de $K \cup \{X_1, \ldots, X_n\}$ en el primer caso y por una operación aritmética en el segundo caso. Los nodos de indegree 0 se llaman los nodos fuente de $\Gamma(\beta)$. Los nodos fuente marcados con una variable $X_1, \ldots, X_n$ se llaman *nodos de entrada* y los marcados con un elemento de K se llaman *nodos parámetros*. Los elementos de K que aparecen de esta manera de llaman *parámetros* del grafo de computación $\Gamma(\beta)$ (o del straight-line program β).

Los nodos de $\Gamma(\beta)$ se numeran por $1 \leq \rho \leq r$. Si para un nodo ρ de $\Gamma(\beta)$ existen nodos $1 \leq \rho_1,\ \rho_2 < \rho$ y una operación aritmética op_ρ tal que vale

$Q_\rho = Q_{\rho_1}\ op_\rho\ Q_{\rho_2}$, entonces el nodo ρ se marca con op_ρ, su indegree es 2 y $\Gamma(\beta)$ contiene dos ejes dirigidos de los vértices ρ_1 y ρ_2 al vértice ρ (los nodos ρ_1 y ρ_2 se llaman los *nodos predecesores* de ρ). Los nodos que no son fuente se dicen *nodos internos* de $\Gamma(\beta)$. El nodo r se denomina *nodo de salida* del grafo de computación $\Gamma(\beta)$.

A cada nodo ρ de $\Gamma(\beta)$ se asocia la función racional Q_ρ que aparece en la sucesión β como resultado intermedio. Esta función racional se calcula recursivamente por el grafo $\Gamma(\beta)$ comenzando por los nodos fuente. En particular, la función racional que corresponde al nodo de salida r es $Q_r = F$.

Un nodo ρ de $\Gamma(\beta)$ es *no escalar* si tiene la siguiente propiedad: el nodo ρ tiene indegree 2, la operación aritmética op_ρ es una multiplicación o división y los resultados intermediatos Q_{ρ_1}, Q_{ρ_2} de β asociados a los nodos predecesores ρ_1, ρ_2 de ρ satisfacen la condicioń $Q_{\rho_1}, Q_{\rho_2} \notin K$ si op_ρ es una multiplicación y $Q_{\rho_2} \notin K$ si op_ρ es una división. .

Sobre el grafo dirigido acíclico $\Gamma(\beta)$ se puede jugar un pebble game de acuerdo con las siguientes reglas (ver [25]):

P1 cualquier nodo fuente puede recibir un pebble,

P2 si los nodos predecesores de un nodo ρ de $\Gamma(\beta)$ tienen ambos un pebble, entonces ρ puede recibir un nuevo pebble o uno de los pebbles de alguno de sus predecesores,

P3 todo pebble puede ser removido de un nodo de $\Gamma(\beta)$.

El pebble game finaliza cuando el nodo de salida de$\Gamma(\beta)$ recibe un pebble. En general es posible jugar varios pebble games distintos sobre un grafo de computación dado $\Gamma(\beta)$. Esto significa que el grafo de computación $\Gamma(\beta)$ típicamente admite más de un pebble game, o en otras palabras: los pebble games no están únicamente determinados por el grafo de computación.

Para un pebble game particular sobre un grafo de computación $\Gamma(\beta)$ se tienen las siguientes medidas de complejidad:

C1 una medida de *espacio* dada por el máximo número de pebbles utilizado en cualquier momento del juego,

C2 una medida de *tiempo total* dada por el número de ubicaciones de pebbles realizados durante el juego según las reglas P1 y P2,

C3 una medida de *tiempo no escalar* dada por la cantidad de ubicaciones de pebbles sobre los nodos no escalares de $\Gamma(\beta)$ realizadas durante el juego siguiendo la regla P2.

Se extiende esta noción de straight-line program en la forma siguiente: *a partir de ahora, un straight-line program será un un circuito aritmético β en el sentido de la Definición 6 junto con un pebble game fijo jugado sobre su grafo de computación $\Gamma(\beta)$. Se utilizará la misma notación, es decir β, para el nuevo objeto matemático: el straight-line program junto con el pebble game fijado.*

Se introduce el siguiente modelo de complejidad combinatorio que refleja tiempo secuencial y espacio en el contexto aritmético:

Definición 7 *Sea $F \in K(X_1, \ldots, X_n)$ una función racional. Un straight-line program en el cuerpo de las funciones racionales $K(X_1, \ldots, X_n)$ que evalúa F en tiempo total T, tiempo no escalar L y espacio S es un straight-line program β para F en el sentido de la Definicion 6 junto con un pebble game realizado sobre $\Gamma(\beta)$ en tiempo total T, tiempo no escalar L y espacio S, donde estas medidas de complejidad están determinadas en términos de las condiciones C2, C3 y C1.*

De esta manera se obtiene un modelo de complejidad puramente combinatorio que mide tiempo total y no escalar utilizado por un pebble game realizado sobre un grafo de computación. Se construirá ahora un modelo de locación de registros a fin de derivar cotas inferiores sobre el tradeoff espacio-tiempo de la evaluación de polinomios.

Supóngase dado un straight-line program β como antes junto con su grafo de computación $\Gamma(\beta)$. Supóngase además que se tiene un pebble game sobre $\Gamma(\beta)$ que usa S pebbles $1, \ldots, S$ y se juega en tiempo total T sobre el grafo de $\Gamma(\beta)$. En lo que sigue se piensa el pebble game dado como una sucesión de T instrucciones de locación de registros en las cuales las nuevas variables $R_1, \ldots, R_S$ aparecen como nombres de registros. Las instrucciones de locación de registros se marcan con los símbolos $(1), \ldots, (T)$. Se las define de la manera siguiente:

1. Si un nodo fuente ρ de $\Gamma(\beta)$ recibe el pebble $1 \leq j \leq S$ en el instante de tiempo $1 \leq t \leq T$ del juego siguiendo la regla P1 entonces la instrucción (t) tiene la forma

$$\text{“}R_j := X_i\text{”}$$

en caso en que el nodo ρ esté marcado por la variable de entrada X_i. Si el nodo ρ está marcado por el parámetro $\alpha \in K$ la instrucción de locación de registros (t) toma la forma

$$\text{“}R_j := \alpha\text{”}$$

2. Si el nodo interno ρ de $\Gamma(\beta)$ recibe el pebble $1 \leq j \leq S$ en el instante $1 \leq t \leq T$ del juego siguiendo la regla P2, entonces la instrucción de locación de registros (t) tendrá la forma

$$\text{“}R_j := R_k \; op_\rho \; R_l\text{”}$$

donde op_ρ es la operación aritmética asociada con el nodo ρ y $1 \leq k$, $l \leq S$ son los pebbles ubicados sobre los nodos predecesores ρ_1, ρ_2 de ρ.

De acuerdo con las reglas de locación de registros introducida se puede redefinir la noción de un straight-line program de tiempo total T (resp. tiempo no escalar L) y espacio S de la siguiente manera:

Definición 8 *Un straight-line program β en $K(X_1, \ldots, X_n)$ que utiliza tiempo total T y espacio S es una sucesión de instrucciones de locación de registros $(1), \ldots, (T)$ tales que para $1 \leq t \leq T$ la instrucción (t) es de uno de los siguientes dos tipos:*

(i) “$R_j := a$” *con* $a \in K \cup \{X_1, \ldots, X_n\}$ *y* $1 \leq j \leq S$

(ii) “$R_j := R_k \; op \; R_l$” *con* $op \in \{+, -, \cdot, \div\}$ *y* $1 \leq k, l < j \leq S$.

Aquí $R_1, \ldots, R_S$ son las (distintas) variables que denotan los registros que usa el straight-line program β.

El *tiempo total* utilizado por un straight-line program β es en consecuencia el número T de instrucciones de locación de registros que contiene. El *tiempo no escalar* utilizado por β (o su *longitud no escalar*) es el número de intrucciones de locación de registros de la forma (ii) que aparecen en β sujetas a las siguientes restricciones: la operación aritmética *op* es una multiplicación o división, los contenidos de los registros R_k, R_l -noción que se introducirá mas adelante- no pertenece al dominio K de los parámetros en caso en que

op es una multiplicación y el contenido del registro R_l no pertenece a K si *op* es una división. En lo que sigue se notará $L(\beta)$ el *tiempo no escalar* y por $S(\beta)$ el *espacio* utilizado por el straight-line program β.

Dado un straight-line program β en el sentido de la Definición 8 se puede definir de la manera más obvia para cada instante de tiempo $1 \leq t \leq T$ y cada registro R_j con $1 \leq j \leq S$ su *contenido* R_j^t como la función racional de $K(X_1, \ldots, X_n)$ que se obtiene aplicando paso a paso las intrucciones de locación de registros $(1), \ldots, (T)$. En el caso en que el registro j permanece sin especificar de esta manera al instante t se define su contenido como el valor constante 1 del cuerpo K. Por lo tanto en cualquier instante el contenido de cualquier registro es el valor constante $1 \in K$ o una función racional de $K(X_1, \ldots, X_n)$ que aparece como resultado intermedio del circuito aritmético β correspondiente en el sentido de la Definición 6. Se denomina $(R_j^t)_{1 \leq j \leq S, 1 \leq t \leq T}$ la *matriz de computación* del straight-line program β.

3.1.2 Del modelo de locación de registros al modelo de complejidad geométrico

En esta subsección se introduce un modelo geométrico para la evaluación de polinomios que refleja el espacio y el tiempo computacional cuando las operaciones aritméticas se cuentan con costo uno. El modelo es algo grosero con respecto a cotas superiores de complejidad pero es conveniente para inferir cotas inferiores para la complejidad intrínseca de la función de tradeoff espacio-tiempo de una serie de polinomios explícitos los cuales -al menos al conocimiento del autor- se estudian por primera vez bajo el aspecto de espacio versus tiempo.

El método para obtener cotas inferiores para el tradeoff espacio-tiempo de procesos de evaluación de polinomios se basa en una interpretación geométrica de la noción de un straight-line program que utiliza tiempo no escalar y espacio no superior a cantidades prefijadas L y S respectivamente. En lo que sigue se restringirá el estudio al caso $n := 1$. Esto significa que se tratará con polinomios y funciones racionales univariadas definidas sobre el cuerpo K. Se denota por $X := X_1$ la única variable de los polinomios y funciones racionales que aparecen como resultados intermedios en los straight-line programs que se considerarán a partir de ahora.

En primer lugar, obsérvese que, sobre el grafo de computación asociado

a la regla de Horner para un polinomio univariado $F \in K[X]$ de grado d, puede jugarse un pebble game en tiempo total time $2d$ y tiempo no escalar d usando exactamente dos pebbles. Sean L y S el tiempo no escalar y el espacio utilizado por el algoritmo de Horner que evalúa el polinomio F. Entonces L y S satisfacen la relación de tradeoff $LS^2 = 4d$.

Esta consideración conduce a la siguiente pregunta: dado *cualquier* polinomio $F \in K[X]$ de grado no mayor que d, ¿existe un straight-line program β in $K(X)$ que utiliza tiempo no escalar $L(\beta)$ y espacio $S(\beta)$ tal que el *tradeoff espacio-tiempo* $LS^2(\beta) := L(\beta)S^2(\beta)$ es considerablemente menor que d? Por medio de un simple argumento de dimensión se demostrará que la respuesta a esta cuestión es negativa. Esto significa que existe una constante universal $c > 0$ tal que (en un sentido preciso) *casi todos* los polinomios $F \in K[X]$ de grado acotado por d tienen la propiedad que *cualquier* straight-line program β en $K(X)$ que evalúa F tiene un tradeoff espacio-tiempo $LS^2(\beta)$ que satisface la desigualdad $LS^2(\beta) \geq cd$ (ver Teorema 17). En lo sucesivo se abreviará un tal enunciado como $LS^2(F) \geq cd$.

De forma similar a [171] y [89], se dirá que una familia de polinomios univariados $(F_d)_{d\in\mathbb{N}}$ tal que F_d tiene grado d es *difícil de evaluar* en términos de tradeoff si existe una constante $c' > 0$ tal que cualquier familia de circuitos aritméticos $(\beta_d)_{d\in\mathbb{N}}$ en $K[X]$ tal que β_d evalúa el polinomio F_d satisface la siguiente desigualdad de tradeoff espacio-tiempo:

$$LS^2(\beta_d) \geq d^{c'}.$$

En lo sucesivo tal enunciado se abreviará en la forma:

$$LS^2(F_d) = d^{\Omega(1)}.$$

El método geométrico que se desarrollará permitirá exhibir familias de polinomios univariados *específicas* que son difíciles de evaluar en este sentido.

Sean L y S números naturales fijos y sea β un straight-line program que calcula la función racional $F \in K(X)$ en tiempo no escalar $L(\beta) \leq L$ y espacio $S(\beta) \leq S$.

A fin de homogeneizar notaciones se comienza el cálculo formalmente en el instante cero fijando para $1 \leq j \leq S$ el contenido R_j^0 de cada registro R_j como $R_j^0 := 0$. Además del espacio se tendrá en cuenta solamente el tiempo *no escalar* como medida de complejidad. El tiempo no escalar será indicado por el nuevo parámetro l que varía de 1 a L. Mas aún, se utilizarán

dos registros adicionales R_{-1} y R_0 cuyos contenidos en cualquier instante de tiempo $0 \leq l \leq L$ se fija como $R_{-1}^l := 1$ y $R_0^l := X$. Dado que en el modelo no escalar operaciones $K-$lineales son libres y que sólo se toman en cuenta operaciones no escalares en el straight-line program β, se puede describir β por una sucesión recursiva de instrucciones de locación de registros (I_j^l) del tipo siguiente:
para $1 \leq j \leq S$ y $1 \leq l \leq L$ la instrucción (I_j^l) tiene la forma

$$R_j^l := \left(\sum_{-1 \leq k \leq S} a_k^{(j,l)} R_k^{l-1} \right) op \left(\sum_{-1 \leq k \leq S} b_k^{(j,l)} R_k^{l-1} \right),$$

donde op es una multiplicación o división y los $a_k^{(j,l)}$ y $b_k^{(j,l)}$ son elementos adecuados de K.

La salida F de β se da por la siguiente instrucción final de locación de registros (I):

$$F := \sum_{-1 \leq k \leq S} c_k R_k^L$$

donde los c_k son ciertos elementos de K.

Los elementos $a_k^{(j,l)}$, $b_k^{(j,l)}$, c_k de K que aparecen en estas instrucciones de locación de registros se llaman los *parámetros* del straight-line program β. Mas aún, los resultados intermedios de β se representan por medio de la *matriz de computación*

$$M(\beta) := (R_j^l)_{-1 \leq j \leq S, 0 \leq l \leq L}$$

El circuito β queda determinado por sus parámetros y la indicación sobre cual operación aritmética, multiplicación o división, se aplica en cada instrucción de locación de registros (I_j^l).

Obsérvese que la intrucción de locación de registros (I_j^l) no refleja exactamente un pebble game sobre el grafo de computación $\Gamma(\beta)$ dado que en este modelo se supone que todos los registros cambian sus contenidos simultáneamente. Por el contrario, un pebble game en cada instante de tiempo afecta sólo un registro y no todos simultáneamente.

En consecuencia, el modelo de computación en $K(X)$ definido por las reglas de locación de registros de tipos (I_j^l) e (I) para $1 \leq j \leq S$ y $1 \leq l \leq L$ es algo mas grosero que el modelo dado por las Definiciones 7 y 8. Esto significa que de esta manera pueden aparecer funciones racionales

como el resultado de computaciones que no pueden ser efectuadas por medio de un straight-line program que utiliza solamente tiempo no escalar L y espacio S. Dado que el propósito final es demostrar cotas *inferiores* para el tradeoff entre espacio y tiempo no escalar requerido para calcular ciertos polinomios univariados, esta falta de precisión del modelo de complejidad no afectará la correctitud de los resultados que enunciaremos en el sentido de las Definiciones 7 y 8.

Sean L y S cantidades fijas. Supóngase que los parámetros $a_k^{(j,l)}$, $b_k^{(j,l)}$, c_k que aparecen para $-1 \leq k \leq S$, $1 \leq j \leq S$ y $1 \leq l \leq L$ en las instrucciones de locación de registros (I_j^l) y (I) se consideran como variables, es decir, se reemplazan estos parámetros por nuevas indeterminadas. Entonces las entradas de la matriz de computación $M(\beta)$ y la función racional F que representa los resultados intermedios y la salida del straight-line program β se transforman en expresiones racionales en los parámetros del circuito β (y por supuesto en la variable X).

De esta manera el straight-line program β se transforma en un *esquema de computación genérico de tiempo no escalar L y espacio S* el cual queda únivocamente determinado por las cantidades L y S y la elección de la operación aritmética realizada (multiplicación o división) para cada $1 \leq j \leq S$ y $1 \leq l \leq L$ en la instrucción de locación de registros (I_j^l).

Se simplificará algo mas el esquema de computación de tiempo no escalar L y espacio S. Para este propsito se introduce para cada $1 \leq j \leq S$ y $1 \leq l \leq L$ un nuevo parámetro $d^{(j,l)}$ el cual se interpretará de la manera siguiente: el valor asignado al parámetro $d^{(j,l)}$ es 1 si la operación aritmética *op* de la instrucción (I_j^l) es una multiplicación y el valor es 0 si esta operación aritmética es una división.

Ahora se reemplaza para cada $1 \leq j \leq S$, $1 \leq l \leq L$ la instrucción de locación de registros (I_j^l) por la siguiente que se denotará (J_j^l) :

$$R_j^l = \left(\sum_{-1 \leq k \leq S} a_k^{(j,l)} R_k^{l-1} \right) \cdot \left(d^{(j,l)} \left(\sum_{-1 \leq k \leq S} b_k^{(j,l)} R_k^{l-1} \right) + \right.$$

$$\left. + (1 - d^{(j,l)}) \left(\sum_{-1 \leq k \leq S} b_k^{(j,l)} R_k^{l-1} \right)^{-1} \right)$$

(obsérvese que tomar en la instrucción de locación de registros (J_j^l) la inversa de la subexpresión $\sum_{-1 \leq k \leq S} b_k^{j,l} R_k^{l-1}$ es consistente con la suposición general

que las computaciones que se consideran no contienen la función racional cero como resultado intermedio). Como siempre, cada parámetro $d^{(j,l)}$ se representa por medio de una nueva indeterminada.

3.1.3 Una descripción geométrica del conjunto de los polinomios evaluables con recursos prefijados

En la subsección anterior se obtuvo un esquema de computación genérico que sólo depende del tiempo no escalar L y el espacio S. Los parámetros de este esquema de computación son $a_k^{(j,l)}$, $b_k^{(j,l)}$, $d^{(j,l)}$ y c_k con $-1 \leq k \leq S$, $1 \leq j \leq S$ y $1 \leq l \leq L$.

Se analizará ahora como la salida F depende de estos parámetros si F es un polinomio que pertenece a $K[X]$. Para este fin se aplica una idea cuyo origen puede situarse en el trabajo [171] (ver también [161]).

A fin de enunciar el siguiente resultado técnico se recuerda que el *peso* de un polinomio con coeficientes enteros es la suma de los valores absolutos de estos coeficientes.

Lema 32 *Sean d, L, S números naturales dados, sea $N := 8LS^2$ y sean $Z_1, \ldots, Z_N$ nuevas indeterminadas. Entonces existen polinomios $P_d, \ldots, P_0 \in \mathbb{Z}[Z_1, \ldots, Z_N]$ de grado y peso acotados por $2(Ld+1)$ y $(4(S+1))^{(d+1)^{L+1}}$ respectivamente, tales que el morfimo de espacios afines*

$$\Phi_{d,L,S} : K^N \to K^{d+1}$$

definido por estos polinomios tiene la siguiente propiedad:
para cada polinomio $F \in K[X]$ de grado acotado por d que puede evaluarse por medio de un straight-line program en $K(X)$ que utiliza tiempo no escalar L y espacio S, existe un subconjunto cofinito (no vacío) U_F de K tal que para cada elemento $\eta \in U_F$ el punto $(f_d(\eta), \ldots, f_0(\eta)) \in K^{d+1}$ dado por la representación

$$F = \sum_{0 \leq i \leq d} f_i(\eta)(X - \eta)^i$$

pertenece a la imagen del morfismo $\Phi_{d,L,S}$.

Demostración. Sea β un straight-line program arbitrario en $K(X)$ que calcula un polinomio dado $F \in K[X]$ de grado acotado por d en tiempo

no escalar L y espacio S. Se supone que β está dado como antes por una sucesión de instrucciones locación de registros (J_j^l) con $1 \leq j \leq S$ y $1 \leq l \leq L$ y una instrucción final (I). Por lo tanto, los resultados intermedios de β son funciones racionales $R_k^l \in K(X)$ con $-1 \leq k \leq S$ y $0 \leq l \leq L$ que satisfacen las siguientes relaciones recursivas:

$$R_{-1}^l = 1 \text{ para cada } 0 \leq l \leq L$$

$$R_0^l = X \text{ para cada } 0 \leq l \leq L$$

$$R_j^0 = 0 \text{ para cada } 1 \leq j \leq S$$

y

$$R_j^l = \left(\sum_{-1 \leq k \leq S} a_k^{(j,l)} R_k^{l-1} \right) \cdot \left(.d^{(j,l)} (\sum_{-1 \leq k \leq S} b_k^{(j,l)} R_k^{l-1}) + \right.$$

$$\left. + (1 - d^{(j,l)}) (\sum_{-1 \leq k \leq S} b_k^{(j,l)} R_k^{l-1})^{-1} \right) \quad (3.1)$$

para cada $1 \leq j \leq S$ y cada $1 \leq l \leq L$.

Finalmente, el polinomio de salida $F \in K[X]$ se representa como

$$F = \sum_{-1 \leq k \leq S} c_k R_k^L \quad (3.2)$$

Aquí $a_k^{(j,l)}$, $b_k^{(j,l)}$, $d^{(j,l)}$, c_k son elementos adecuados de K with $-1 \leq k \leq S$, $1 \leq j \leq S$ y $1 \leq l \leq L$, los parámetros del straight-line program β.

Cada una de las funciones racionales $\sum_{-1 \leq k \leq S} a_k^{(j,l)} R_k^{l-1}$ y $\sum_{-1 \leq k \leq S} b_k^{(j,l)} R_k^{l-1}$ que aparecen como subexpresiones en la ecuación (3.1) están bien definidas y son diferentes de cero en todos los puntos de algún subconjunto cofinito U_F de K. Dado que K es infinito el conjunto U_F es no vacío. Sea η un punto arbitrario de U_F y j y l números naturales con $1 \leq j \leq S$ y $1 \leq l \leq L$. Entonces las funciones racionales $R_{-1}^{l-1}, \ldots, R_S^{l-1}$, $\sum_{-1 \leq k \leq S} a_k^{(j,l)} R_k^{l-1}$ y $\sum_{-1 \leq k \leq S} b_k^{(j,l)} R_k^{l-1}$ están definidas en η y son diferentes de cero en η. Por medio de un cambio adecuado de los parámetros $a_j^{(j,l)}, b_j^{(j,l)}$ y c_k en las ecuaciones (3.1) y (3.2) se puede suponer sin pérdida de generalidad que vale $\sum_{-1 \leq k \leq S} a_k^{(j,l)} R_k^{l-1}(\eta) = 1$ y $\sum_{-1 \leq k \leq S} b_k^{(j,l)} R_k^{l-1}(\eta) = 1$. El parámetro $d^{(j,l)}$

toma por hipótesis solamente los valores 0 o 1. Esto implica que la función racional R_j^l está definida en η y que se satisface la condición $R_j^l(\eta) = 1$. Esto permite representar R_j^l como una serie de potencias formal en $X - \eta$ con coeficientes en K. Más precisamente, se puede escribir la función racional R_j^l unívocamente como la serie de potencias

$$R_j^l = 1 + \sum_{i \geq 1} R_{j,i}^l (X - \eta)^i$$

con coeficientes $R_{j,i}^l$ pertenecientes al cuerpo K. Obsérvese que $R_0^l = X$ tiene también una representación en series de potencias de la forma $R_0^l = \eta + (X - \eta) = \eta + \sum_{i \leq 1} R_{0,i}^l (X - \eta)^i$ con $R_{0,1}^l = 1$ y $R_{0,i}^l = 0$ para $i > 1$. De las hipótesis realizadas se deduce:

$$\begin{aligned} \sum_{-1 \leq k \leq S} a_k^{(j,l)} R_k^{l-1} &= \sum_{-1 \leq k \leq S} a_k^{(j,l)} R_{k,i}^{l-1}(\eta) + \sum_{0 \leq k \leq S} a_k^{(j,l)} \sum_{i \geq 1} R_{k,i}^{l-1} (X - \eta)^i = \\ &= 1 + \sum_{0 \leq k \leq S} a_k^{(j,l)} \sum_{i \geq 1} R_{k,i}^{l-1} (X - \eta)^i \end{aligned} \tag{3.3}$$

y similarmente

$$\sum_{-1 \leq k \leq S} b_k^{(j,l)} R_k^{l-1} = 1 + \sum_{0 \leq k \leq S} b_k^{(j,l)} \sum_{i \geq 1} R_{k,i}^{l-1} (X - \eta)^i \tag{3.4}$$

La ecuación (3.4) implica la siguiente:

$$\left(\sum_{-1 \leq k \leq S} b_k^{(j,l)} R_k^{l-1} \right)^{-1} = 1 + \sum_{v \geq 1} \left(- \sum_{0 \leq k \leq S} b_k^{(j,l)} \sum_{i \geq 1} R_{k,i}^{l-1} (X - \eta)^i \right)^v$$

Esto permite expresar la ecuación (3.1) en términos de series de potencias. Para $1 \leq j \leq S$ y $1 \leq l \leq L$ se tiene

$$\begin{aligned} &1 + \textstyle\sum_{i \geq 1} R_{j,i}^l (X - \eta)^i = \\ &= \left(1 + \textstyle\sum_{0 \leq k \leq S} a_k^{(j,l)} \sum_{i \geq 1} R_{k,i}^{l-1} (X - \eta)^i \right) \cdot \\ &\quad \cdot \left(d^{(j,l)} \left(1 + \textstyle\sum_{0 \leq k \leq S} b_k^{(j,l)} \sum_{i \geq 1} R_{k,i}^{l-1} (X - \eta)^i \right) + \right. \\ &\quad \left. + (1 - d^{(j,l)}) \left(1 + \sum_{v \geq 1} \left(- \sum_{0 \leq k \leq S} b_k^{(j,l)} \sum_{i \geq 1} R_{k,i}^{l-1} (X - \eta)^i \right)^v \right) \right) \end{aligned} \tag{3.5}$$

De la ecuación (3.5) se deduce inductivamente que los coeficientes $R^l_{j,i}$ son expresiones polinomiales con coeficientes enteros en los parámetros $a_k^{(j',l')}$, $b_k^{(j',l')}, d^{(j',l')}$ del straight-line program β donde k, j' y l' varían en $0 \leq k \leq S$, $1 \leq j' \leq S$ y $1 \leq l' \leq l$. Estas expresiones polinomiales dependen solamente de L y S y son independientes de la elección particular de η y del straight-line program particular β.

Dado que no puede aparecer ninguna ambigüedad, se denotará tal expresión polinomial con el mismo símbolo que el coeficiente de la serie de potencias que representa, es decir $R^l_{j,i}$.

Comparando coeficientes en la ecuación (3.5) se ve que cada coeficiente $R^l_{j,i}$ es, salvo signos, una suma de expresiones monomiales de uno de los dos tipos siguientes:

$$(d^{(j,l)})^\epsilon \prod_{1 \leq v \leq \mu} b_{k_v}^{(j,l)} R^{l-1}_{k_v,i_v} \tag{3.6}$$

$$a_{k_\mu}^{(j,l)} R^{l-1}_{k_\mu,i_\mu} (d^{(j,l)})^\epsilon \prod_{1 \leq v < \mu} b_{k_v}^{(j,l)} R^{l-1}_{k_v,i_v} \tag{3.7}$$

con $\sum_{1 \leq v \leq \mu} i_v = i$, $1 \leq i_v \leq i$, $1 \leq \mu \leq i$, $0 \leq k_v \leq S$ y $\epsilon \in \{0,1\}$.

A partir de esta observación se deduce la siguiente cota de grados recursiva:
$gr(R^l_{j,i}) \leq \max\{\mu + 1 + \sum_{1 \leq v \leq \mu} gr(R^{l-1}_{k_v,i_v}) :$

$$\sum_{1 \leq v \leq \mu} i_v = i,\ 1 \leq i_v \leq i,\ 1 \leq \mu \leq i,\ 0 \leq k_v \leq S\} \tag{3.8}$$

De la construcción realizada se deduce inmediatamente que para cada $0 \leq k \leq S$ y cada $i \geq 1$ se satisface la siguiente estimación:

$$gr(R^0_{k,i}) \leq 0 \tag{3.9}$$

Si se resuelven las relaciones de recurrencia (3.8) tomando en cuenta las condiciones iniciales (3.9) se obtiene:

$$gr(R^l_{j,i}) \leq i(2l-1) + 1 \tag{3.10}$$

para cada $1 \leq j \leq S$, $1 \leq l \leq L$ y $i \geq 1$.

Se estima ahora el peso de los polinomios $R^l_{j,i}$. Para tal propósito se observa que el número de expresiones monomiales (3.6) y (3.7) que aparecen en $R^l_{j,i}$ no excede $2^{i+1}(S+1)^i$. Por lo tanto, se deduce la siguiente cota recursiva para el peso:

$$peso(R^l_{j,i}) \leq 2^{i+1}(S+1)^i \max\{\textstyle\prod_{1\leq v\leq \mu} peso(R^{l-1}_{k_v,i_v}) : \\ \sum_{1\leq v\leq \mu} i_v = i,\ 1\leq i_v\leq i,\ 1\leq \mu\leq i,\ 0\leq k_v\leq S\} \quad (3.11)$$

Por inspección directa se verifica fácilmente que para cada $1 \leq l \leq L$ y cada $0 \leq k \leq S$ vale la estimación:

$$peso(R^l_{k,1}) \leq 4^l(S+1)^l \quad (3.12)$$

Tomando en cuenta las condiciones iniciales (3.12), la resolución de las relaciones de recurrencia (3.11) da:

$$peso(R^l_{j,i}) \leq 2^{(i+1)((i+1)^l-1)}(S+1)^{i(i+1)^l-1)} \quad (3.13)$$

Los coeficientes $R^l_{j,i}$ de la serie de potencias que aparece en la ecuación (3.5) son expresiones polinomiales sobre $\mathbb{Z}$ en los $2LS^2+3LS$ parámetros $a_k^{(j,l)}$, $b_k^{(j,l)}$, $d^{(j,l)}$ con $0 \leq k \leq S$, $1 \leq j \leq S$ y $1 \leq l \leq L$. En consecuencia, se los considerará como polinomios en $(2LS^2+3LS)$ variables sobre $\mathbb{Z}$.

El polinomio $F \in K[X]$ tiene grado no mayor que d y por lo tanto posee una expansión finita en series de Taylor en $(X-\eta)$ del tipo:

$$F = \sum_{0\leq i\leq d} f_i(\eta)(X-\eta)^i$$

con coeficientes $f_i(\eta)$ pertenecientes al cuerpo K.

De la ecuación (3.2) se deduce:

$$\begin{aligned} F &= \sum_{0\leq i\leq d} f_i(\eta)(X-\eta)^i = \sum_{-1\leq k\leq S} c_k R^L_k = \\ &= \left(c_{-1} + c_0\eta + \sum_{1\leq k\leq S} c_k\right) + \sum_{0\leq k\leq S} c_k \left(\sum_{i\geq 1} R^L_{k,i}(X-\eta)^i\right) = \\ &= \left(c_{-1} + c_0\eta + \sum_{1\leq k\leq S} c_k\right) + \sum_{i\geq 1}\left(\sum_{0\leq k\leq S} c_k R^L_{k,i}\right)(X-\eta)^i. \end{aligned}$$

Esto implica

$$f_i(\eta) = \sum_{0 \le k \le S} c_k R^L_{k,i} \tag{3.14}$$

para $1 \le i \le d$ y

$$f_0(\eta) = c_{-1} + c_0\eta + \sum_{1 \le k \le S} c_k \tag{3.15}$$

para $i = 0$.

Obsérvese que la ecuación (3.14) es independiente del parámetro c_{-1}. Esto permite considerar $c_{-1} + c_0\eta$ como un nuevo parámetro c del cual depende el straight-line program β que reemplaza al viejo parámetro c_{-1}. En este sentido se puede reescribir la ecuación (3.15) como

$$f_0(\eta) = c + \sum_{1 \le k \le S} c_k. \tag{3.16}$$

El lado derecho de las ecuaciones (3.14) y (3.16) son expresiones polinomiales en los $2LS^2 + 3LS + S + 2 \le 8LS^2$ parámetros c, c_k, $a_k^{(j,l)}$, $b_k^{(j,l)}$, $d^{(j,l)}$ con $0 \le k \le S$, $1 \le j \le S$ y $1 \le l \le L$. Estas expresiones polinomiales dependen solamente de L y S y son independientes de la elección del punto $\eta \in U_F$.

Sea $N := 8LS^2$ y let $Z_1, \ldots, Z_N$ nuevas indeterminadas. De las ecuaciones (3.10), (3.13), (3.14) y (3.16) se deduce que existen polinomios $P_0, \ldots, P_d \in \mathbb{Z}[Z_1, \ldots, Z_N]$ tales que para cada $0 \le i \le d$ el grado y el peso de P_i puede estimarse por

$$gr(P_i) \le i(2L-1) + 2 \le 2(Ld+1)$$
$$peso(P_i) \le (4(S+1))^{(d+1)^{L+1}}$$

tales que se satisface la siguiente afirmación: para cada polinomio $F \in K[X]$ de grado a lo sumo d que puede evaluarse por medio de un straight-line program en tiempo no escalar L y espacio S existe un conjunto cofinito (no vacío) U_F en K tal que para cada valor $\eta \in U_F$ hay un punto $z \in K^N$ con

$$F = \sum_{0 \le i \le d} f_i(\eta)(X-\eta)^i = \sum_{0 \le i \le d} P_i(z)(X-\eta)^i$$

Sea ahora

$$\Phi_{d,L,S} : K^N \longrightarrow K^{d+1}$$

el morfismo de espacios afines definido por $\Phi_{d,L,S}(z) := (P_d(z), \ldots, P_0(z))$ para $z \in K^N$ arbitrario. Este morfismo tiene todas las propiedades anunciadas en el enunciado del lema 32. □

En las aplicaciones se necesitará una formulación mas comprensible del lema 32 en la cual el valor genérico η y el conjunto cofinito U_F al cual η pertenece no aparezcan explícitamente. Tal formulación puede obtenerse fácilmente incluyendo el valor genérico η en la lista de parámetros del straight-line program β hipotético analizado en la demostración del lema 32. De esta observación se deduce el próximo resultado.

Lema 33 *Sean d, L, S números naturales dados, $N := 8LS^2 + 1$ y sean $Z_1 \ldots, Z_N$ nuevas indeterminadas. Entonces existen polinomios $P_d, \ldots, P_0 \in \mathbb{Z}[Z_1, \ldots, Z_N]$ de grado y peso acotados por*

$$2(Ld + 1)$$

y

$$(d+1)!(4(S+1))^{(d+1)^{L+1}}$$

respectivamente tales que el morfismo espacios afines

$$\Phi_{d,L,S} : K^N \longrightarrow K^{d+1}$$

definido por estos polinomios tiene la siguiente propiedad:
para cada polinomio $F \in K[X]$ de grado menor o igual que d que puede evaluarse por medio de un straight-line program en tiempo no escalar L y espacio S, el punto $(f_d, \ldots, f_0) \in K^{d+1}$ dado por la representación $F = \sum_{0 \leq i \leq d} f_i X^i$ pertenece a la imagen de $\Phi_{d,L,S}$.

En lo sucesivo se identificará cada polinomio $F = \sum_{0 \leq i \leq d} f_i X^i \in K[X]$ de grado a lo sumo d con su vector de coeficientes $(f_d, \ldots, f_0)$ que se considerará como un punto del espacio afín K^{d+1}. En este sentido una afirmación como "$F \in K^{d+1}$" deberá entenderse como "$(f_d, \ldots, f_0) \in K^{d+1}$".

Del lema 32 se deducen las siguientes consecuencias geométricas que representan la principal herramienta para derivar cotas inferiores sobre el tradeoff espacio-tiempo intrínseco de polinomios univariados (comparar con [95]).

Lema 34 *Sean d, L, S números naturales dados. Existe un Subconjunto cerrado Zariski irreducible $\mathbb{Q}$-definible $W_{d,L,S}$ de K^{d+1} tal que se satisfacen las siguientes afirmaciones:*

(i) $\dim(W_{d,L,S}) \leq 8LS^2$.

(ii) $gr(W_{d,L,S}) \leq (2(Ld+1))^{8LS^2}$.

(iii) *el vector de coeficientes de todo polinomio* $F \in K[X]$ *de grado no mayor que* d *que puede evaluarse por medio de un straight-line program en* $K(X)$ *de tiempo no escalar* L *y espacio* S *pertenece a la variedad algebraica* $W_{d,L,S}$.

Demostración Sea $W := W_{d,L,S}$ la clausura Zariski en K^{d+1} de la imagen del morfismo $\Phi := \Phi_{d,L,S}$ del lema 32. Se ve inmediatamente que W es un conjunto cerrado Zariski irreducible del espacio afín K^{d+1}. Este subconjunto es también $\mathbb{Q}$-definible dado que el morfismo Φ está dado por polinomios $P_d, \ldots, P_0$ que tienen coeficientes enteros. Durante el resto de la demostración se interpretará Φ como un morfismo de variedades afines K^N en W. En esta interpretación Φ es dominante. y por lo tanto esto implica $\dim(W) \leq N = 8LS^2$. En consecuencia, la variedad algebraica $W = W_{d,L,S}$ satisface la condición (i).

Se verifica ahora la condición (ii). Sea $r := \dim W$. Dado que el morfismo Φ es dominante existe un subconjunto Zariski abierto no vacío de W que está contenido en $Im\,\Phi$, la imagen de Φ. Por lo tanto, se deduce de [88] que existen r hiperplanos afines $H_1, \ldots, H_r$ de K^{d+1} que intersecan $Im\,\Phi$ en $gr(W)$ puntos. Sea $M := H_1 \cap \ldots \cap H_r \cap Im\,\Phi$. Entonces se tiene $\#M = gr(W)$. Del lema 32 se deduce inmediatamente que $\Phi^{-1}(H_1), \ldots, \Phi^{-1}(H_r)$ son hipersurperficies de K^N de grado a lo sumo $2(Ld+1)$. Sea

$$\mathcal{C} := \{C : C \text{ es una componente irreducible de } \Phi^{-1}(H_1) \cap \ldots \cap \Phi^{-1}(H_r)\}$$

Por la desigualdad de Bézout (ver [88], o [70]) se tiene

$$\#\,\mathcal{C} \leq \sum_{C \in \mathcal{C}} gr(C) \leq ((2(Ld+1))^r \leq ((2(Ld+1))^{8LS^2}$$

donde $gr(C)$ denota el grado (geométrico) del cerrado irreducible C de K^N.

Para cada $C \in \mathcal{C}$ la clausura Zariski de la imagen $\Phi(C)$ es un subconjunto irreducible de K^{d+1} contenido en M, y por lo tanto un punto de M. Dado que el conjunto M está contenido en $Im\,\Phi$ se concluye que

$$gr(W_{d,L,S}) = gr(W) = \#M \leq \#\mathcal{C} \leq (2(Ld+1))^{8LS^2}$$

Finalmente, resta verificar la condición (iii). Sea $F = \sum_{0 \leq i \leq d} f_i X^i \in K[X]$ un polinomio de grado acotado por d que puede evaluarse por un

straight-line program en $K(X)$ en tiempo no escalar L y espacio S. Para cada $\eta \in K$ sea $F = \sum_{0 \leq i \leq d} f_i(\eta)(X-\eta)^i$ la expansión de Taylor de F en $X-\eta$. El vector $(f_d(\eta), \ldots, f_0(\eta))$ depende en forma polinomial del parámetro η. Sea $U := U_F$ el subconjunto cofinito no vacío introducido en el lema 32. Para cada $\eta \in U$ se tiene:

$$(f_d(\eta), \ldots, f_0(\eta)) \in Im\, \Phi_{d,L,S} = Im\, \Phi \subset W,$$

por este lema. Dado que U es infinito y W es un cerrado Zariski de K^{d+1} se concluye que $(f_d, \ldots, f_0) = (f_d(0), \ldots, f_0(0))$ pertenece a la variedad algebraica $W = W_{d,L,S}$. □

3.1.4 Algunas consecuencias en términos de tradeoffs

A partir del lema 34 se deducirán cotas inferiores para el tradeoff espacio-tiempo. El primer resultado que se obtendrá caracteriza la complejidad intrínseca del tradeoff espacio–tiempo de "casi todos" los polinomios univariados de grado acotado por d generalizando en consecuencia el resultado principal de [139] y mostrando que la regla de Horner es asintóticamente optimal en términos de tradeoff espacio–tiempo.

Teorema 17 *Sea d un número natural dado. Existe subconjunto abierto Zariski no vacío U de K^{d+1} tal que para cada polinomio $F \in K[X]$ de grado a lo sumo d con $F \in U$ vale la estimación de tradeoff*

$$LS^2(F) \geq \frac{d}{8}$$

Demostración Sea d fijo. Para cada número racional positivo $t \leq d$ se considera el suconjunto cerrado Zariski $W_{d,t}$ de K^{d+1} definido por

$$W_{d,t} := \bigcup_{L,S \in \mathbb{N},\, LS^2 \leq t} W_{d,L,S}$$

Del lema 34 (i) se deduce:

$$\dim(W_{d,t}) \leq \max\{\dim(W_{d,L,S}) :\ L, S \in \mathbb{N},\ LS^2 \leq t\} \leq 8t$$

Por lo tanto, para $t := \frac{d}{8}$ se tiene

$$\dim(W_{d,\frac{d}{8}}) \leq d$$

Esto implica que el subconjunto abierto Zariski $U := K^{d+1} \setminus W_{d,\frac{d}{8}}$ es no vacío. Del lema 34 (*iii*) se deduce finalmente que para polinomio F de $K[X]$ cuyo grado no excede d que pertenece al conjunto U satisface la estimación de tradeoff $LS^2(F) \geq \frac{d}{8}$. □

Siguiendo [139] existe una constante $c > 0$ tal que cualquier polinomio $F \in K[X]$ de grado arbitrario d puede evaluarse con un straight-line program en $K[X]$ en tiempo no escalar no superior $c\sqrt{d}$. Combinando este resultado con el teorema 17 se obtiene la siguiente conclusión:

Corolario 1 *Existe una constante $c' > 0$ con las siguientes propiedades: sea d un número natural dado y sea U el subconjunto abierto Zariski de K^{d+1} introducido en el teorema 17. Entonces para cada polinomio $F \in K[X]$ de grado no mayor que d que satisface la condición $F \in U$ y para cada straight-line program β en $K(X)$ que evalúa F en tiempo no escalar óptimo, el espacio $S(\beta)$ requerido por el procedimiento β se acota inferiormente por*

$$S(\beta) \geq c'\sqrt[4]{d}$$

Se puede reenunciar el contenido del corolario 1 de la siguiente manera: casi todos los polinomios de $K[X]$ de grado a lo sumo d requieren espacio $c'\sqrt[4]{d}$ si se evalúan optimalmente con respecto al tiempo no escalar. Por otro lado, siguiendo [139] existe una constante $c'' > 0$ tal que casi todos los polinomios de $K[X]$ de grado no superior a d necesitan tiempo no escalar $c''\sqrt{d}$ para su evaluación. Esto explica en que sentido el teorema 17 contiene el mejor resultado de tradeoff espacio-tiempo *genérico* posible.

3.2 Herramientas de eliminación geométrica y teoría de intersección

En este capítulo frecuentemente se enfrentarán situaciones como la siguiente: supóngase dado un polinomio $F \in K[X]$ de grado d. Solamente a partir del conocimiento de los coeficientes de F se debe deducir una cota inferior para la cantidad LS^2 donde L y S son números naturales arbitrarios que satisfacen la condición $F \in W_{d,L,S}$ o $F \in Im\Phi_{d,L,S}$ con $W_{d,L,S}$ y $\Phi_{d,L,S}$ definidos como en el lema 34 y el lema 33 respectivamente. Estos dos lemas establecen una relación entre el tamaño de los parámetros de complejidad L y S y el grado o la altura de la variedad algebraica $W_{d,L,S}$ o el morfismo algebraico $\Phi_{d,L,S}$. Por lo tanto, se necesitan herramientas que permitan estimar estos invariantes geométricos: el grado y la altura de $W_{d,L,S}$ y $\Phi_{d,L,S}$ respectivamente a partir de los coeficientes de un sólo punto específico que pertenece a la variedad algebraica $W_{d,L,S}$ o la imagen del morfismo $\Phi_{d,L,S}$. Tales herramientas se desarrollarán por medio del uso de un Nullstellensätz adecuado y una Desigualdad de Bézout de teoría de eliminación geométrica y aritmética (comparar con [139], [171], [161], [95], [76], [94], [89], [90], [167], [168], [121], [129], [130], [9], por un punto de vista similar).

En esta sección técnica se explicarán los resultados de eliminación y teoría de intersección que se aplicarán. En primer lugar, recuérdese que la *altura* de un polinomio con coeficientes enteros es el máximo valor absoluto de sus coeficientes. Similarmente, la *altura logarítmica* de un polinomio es la máxima longitud bit de sus coeficientes.

El principal resultado de esta sección es el siguiente:

Proposición 11 *Sean N, d, D y η números naturales y sea*

$$\Phi := (P_d, \ldots, P_0) : \mathbf{C}^N \longrightarrow \mathbf{C}^{d+1}$$

un morfismo de espacios afines donde $P_0, \ldots, P_d$ son polinomios que pertenecen a $\mathbb{Z}[Z_1, \ldots, Z_N]$. Sea F un punto dado de $\mathbb{Z}^{d+1}$. Considérese la Φ-fibra $V := \Phi^{-1}(F)$ del punto F como una subvariedad cerrada Zariski $\mathbb{Q}$-definible de $\mathbf{C}^N$. Supóngase que V es no vacía. Sean $h_1, \ldots, h_s \in \mathbb{Z}[Z_1, \ldots, Z_N]$ polinomios que satisfacen las siguientes condiciones:

1. $V := \{z \in \mathbf{C}^N : h_1(z) = 0, \ldots, h_s(z) = 0\}$

2. $\max\{gr(h_i) : 1 \leq i \leq s\} \leq D$ *y*

3. $\max\{\log_2 height(h_i) : 1 \leq i \leq s\} \leq \eta$

Entonces, existe un punto $\theta = (\theta_1, \ldots, \theta_N)$ *de la fibra* V *que satisface la estimación*

$$\log_2 \max\{|\ \theta_i\ | : 1 \leq i \leq N\} \leq D^{cN}(\log_2 s + \eta),$$

donde $c > 0$ *es una constante universal adecuada.*

El resto de esta sección se dedicará a la demostración de este resultado. Para este propósito se necesitan una serie de resultados intermedios técnicos de teoría de eliminación geométrica. El primero de ellos es una forma adecuada de un Nullstellensatz efectivo, el cual se vuelve a enunciar para comodidad del lector.

Teorema 18 (Nullstellensatz efectivo) *Sean* $D \geq 3$ *y* $N \geq 3$ *números naturales y* $h_1, \ldots, h_s \in \mathbb{Z}[Z_1, \ldots, Z_N]$ *polinomios de grado a lo sumo* D. *Considérese el ideal* $\mathcal{I} = (h_1, \ldots, h_s)$ *generado por estos polinomios en* $\mathbb{Q}[Z_1, \ldots, Z_N]$. *Entonces, el ideal* $\mathcal{I}$ *es trivial si y sólo si existen polinomios* $g_1, \ldots, g_s \in \mathbb{Z}[Z_1, \ldots, Z_N]$ *que satisfacen la cota de grados*

$$\max\{gr(g_i) : 1 \leq i \leq s\} \leq D^N - D$$

tales que vale la siguiente identidad de Bézout:

$$1 = \sum_{1 \leq i \leq s} g_i h_i \tag{3.17}$$

Cabe destacar que recientes Nullstellensätze "intrínsecos" como los demostrados en [115] y [166] permitirían establecer leves mejoras en las cotas de tradeoff.

La cota sobre el grado de los polinomios $g_1, \ldots, g_s$ en el teorema 18 permite reducir la cuestión de la vacuidad de la variedad algebraica V definida por los polinomios $h_1, \ldots, h_s$ al problema de la compatibilidad de un sistema inhomogéneo de ecuaciones lineales de tamaño $D^{N^2} \times sD^{N^2}$ con entradas racionales, las cuales están dadas por los coeficientes de los polinomios $h_1, \ldots, h_s$. Este sistema de ecuaciones lineales permite calcular un polinomio adecuado de grado acotado que expresa una cierta propiedad de eliminación de la variedad V. Esta observación conduce al siguiente resultado:

Lema 35 *Sean $D \geq 3$ y $N \geq 3$ números naturales dados y sea V un subconjunto cerrado Zariski de $\mathbf{C}^N$ que es $\mathbb{Q}$-definible y tiene dimensión positiva r. Supóngase que V está dado como el conjunto de ceros comunes de finitos polinomios en $\mathbb{Z}[Z_1, \ldots, Z_N]$ de grado a lo sumo D. Se introducen para $1 \leq i \leq r$ y $1 \leq j \leq N+1$ nuevas indeterminadas $T_{i,j}$ y polinomios*

$$L_i := T_{i,1}Z_1 + \cdots + T_{i,N}Z_N + T_{i,N+1}$$

Bajo estas condiciones existe un polinomio no nulo $E \in \mathbb{Z}[T_{i,j};\ 1 \leq i \leq r,\ 1 \leq j \leq N+1]$ de grado a lo sumo D^{N^2} con la siguiente propiedad: cualquier matriz $t = (t_{i,j})_{\{1 \leq i \leq r,\ 1 \leq j \leq N+1\}}$ de $\mathbf{C}^{r \times (N+1)}$ que define r polinomios lineales afines

$$L_1(t, Z_1, \ldots, Z_N) = t_{1,1}Z_1 + \cdots + t_{1,N}Z_N + t_{1,N+1},$$

$$L_r(t, Z_1, \ldots, Z_N) = t_{r,1}Z_1 + \cdots + t_{r,N}Z_N + t_{r,N+1}$$

verifica que la intersección de V con el subespacio lineal afín de $\mathbf{C}^N$ dado por estos polinomios

$$V \cap \{z \in \mathbf{C}^N \ :\ L_1(t,z) = 0, \ldots, L_r(t,z) = 0\},$$

es no vacío si se satisface la condición Zariski abierta (consistente) $E(t) \neq 0$.

Notación 1 *Por el resto de esta sección se fijan las siguientes notaciones:*

$$T := (T_{i,j})_{1 \leq i \leq r, 1 \leq j \leq N+1} \quad y \quad Z := (Z_1, \ldots, Z_N).$$

Demostración del lema 35 Por hipótesis existen finitos polinomios $h_1, \ldots, h_s \in \mathbb{Z}[Z_1, \ldots, Z_N]$ de grado no mayor que D que definen la variedad V. Dado que r es la dimensión (positiva) de V existe un subconjunto abierto Zariski no vacío U de $\mathbf{C}^{r \times (N+1)}$ tal que para cada $t \in U$ la intersección

$$V \cap \{z \in \mathbf{C}^N \ :\ L_1(t,z) = 0, \ldots, L_r(t,z) = 0\},$$

contiene al menos un punto (ver por ejemplo [88], Lemma 1). Esto implica que el ideal $\mathcal{J}$ generado por los polinomios $h_1, \ldots, h_s, L_1, \ldots, L_r$ en el anillos de polinomios $\mathbb{Q}(T)[Z]$ es propio. Del teorema 18 se deduce entonces que

no pueden existir polinomios $g_1, \ldots, g_{r+s} \in \mathbb{Q}(T)[Z]$ tales que para cada $1 \leq k \leq r+s$ el polinomio g_k tiene la forma

$$g_k(Z) := \sum_{\nu_1+\cdots+\nu_N \leq D^N - D} Y^{(k)}_{\nu_1,\ldots,\nu_N} Z_1^{\nu_1} \ldots Z_N^{\nu_N}$$

con coeficientes $Y^{(k)}_{\nu_1,\ldots,\nu_N}$ en el cuerpo $\mathbb{Q}(T)$ y tal que se satisface la identidad de Bézout:

$$\begin{aligned} 1 = g_1(Z)h_1(Z) + \cdots + g_s(Z)h_s(Z) + \\ + g_{s+1}(Z)L_1(T,Z) + \cdots + g_{r+s}(Z)L_r(T,Z) \end{aligned} \quad (3.18)$$

en $\mathbb{Q}(T)[Z]$.

La identidad polinomial (inconsistente) (3.18) puede interpretarse como un sistema inhomogéneo de ecuaciones lineales en las indeterminadas $Y^{(k)}_{\nu_1,\ldots,\nu_N}$ que aparecen como coeficientes de los polinomios "potenciales" $g_1, \ldots, g_{r+s}$ en las variables $Z_1, \ldots, Z_N$. Este sistema de ecuaciones tiene tamaño de tipo $D^{N^2} \times sD^{N^2}$ y su matriz, que se denota por A, contiene como entradas los coeficientes de los polinomios $h_1, \ldots, h_s$ y $L_1, \ldots L_r$ con respecto a las variables $Z_1, \ldots, Z_N$.

En consecuencia, la matriz A se construye con enteros e indeterminadas $T_{i,j}$. Nótese por

$$AY = B \quad (3.19)$$

el sistema inhomogéneo de ecuaciones lineales que representa la identidad polinomial (3.18). Aquí B e Y son vectores columna de longitud a lo sumo D^{N^2} y sD^{N^2} respectivamente, todas las entradas de B son 0 excepto una que es 1, e Y es el vector columna de indeterminadas del sistema. Estas indeterminadas pueden escribirse como $Y^{(k)}_{\nu_1,\ldots,\nu_N}$ con $1 \leq k \leq r+s$ y $\nu_1 + \cdots + \nu_n \leq D^N$. La inconsistencia de la identidad polinomial (3.18) implica la inconsistencia del sistema de ecuaciones lineales (3.19). Por lo tanto, el rango de la matriz A es estrictamente inferior al rango, m, de la matriz A^* que se obtiene agregando a la matriz A el vector columna B. Esto significa que A^* contiene un menor regular $m \times m$ con determinante no nulo $E \in \mathbb{Z}[T]$ mientras que todos los menores de $m \times m$ de A son singulares. Este determinante $E(T)$ expresa un propiedad de eliminación adecuada de la variedad algebraica definida en $\mathbb{C}^{r \times (N+1)} \times \mathbb{C}^N$ por los polinomios $h_1(Z), \ldots, h_s(Z), L_1(T,Z), \ldots, L_r(T,Z)$ si se proyecta esta variedad en el espacio afín $\mathbb{C}^{r \times (N+1)}$. El siguiente argumento contiene el sentido preciso de este enunciado y su justificación:

para cada $t \in \mathbf{C}^{r\times(N+1)}$ tal que vale $E(t) \neq 0$ el sistema de ecuaciones lineales que se obtiene a partir de (3.19) especializando la matriz genérica T en t es inconsistente. En virtud del teorema 18 esto significa que el ideal generado por los polinomios $h_1(Z), \ldots, h_s(Z), L_1(t,Z), \ldots, L_r(t,Z)$ en el anillo de polinomios $\mathbf{C}[Z]$ es propio. Por lo tanto, la variedad

$$V \cap \{z \in \mathbf{C}^N : L_1(t,z) = 0, \ldots, L_r(t,z) = 0\} =$$
$$= \{z \in \mathbf{C}^N : h_1(z) = 0, \ldots, h_s(z) = 0, L_1(t,z) = 0, \ldots, L_r(t,z) = 0\}$$

es no vacía.

Obsérvese que las entradas de la matriz A^* son constantes o polinomios lineales de $\mathbb{Z}[T]$ y que A^* tiene a lo sumo D^{N^2} filas lo que implica $m \leq D^{N^2}$. En consecuencia, el grado del polinomio $E(T)$ está acotado por D^{N^2}. □

El lema 35 representa el principal paso en la demostración del próximo resultado.

Lema 36 *Sean $D \geq 3$ y $N \geq 3$ números naturales y sea V un subconjunto de $\mathbf{C}^N$ cerrado Zariski $\mathbb{Q}$-definible de dimensión positiva r. Supóngase que V está dada como el conjunto de ceros de finitos polinomios de $\mathbb{Z}[Z_1, \ldots, Z_N]$ de grado a lo sumo D. Entonces existen r polinomios lineales afines $L_1, \ldots, L_r \in \mathbb{Z}[Z_1, \ldots, Z_N]$ de altura logarítmica acotada por $N(N+1)\log_2 D$, tal que para cada $1 \leq k \leq r$ la variedad algebraica*

$$V \cap \{z \in \mathbf{C}^N : L_1(z) = 0, \ldots, L_k(z) = 0\}$$

es no vacía de dimensión $r - k$.

Obsérvese aquí que los resultados de [114], Subsection 4.8 implican una mejora de la estimación para la altura logarítmica de los polinomios lineales afines $L_1, \ldots, L_r$ en el lema 36 a $cN \log_2 D$ donde $c > 0$ es una constante universal adecuada. Sin embargo se trabajará con la cota de altura del enunciado del lema 36, dado que el impacto de la mejora mencionada sobre los resultados de complejidad que se obtendrán es bastante modesto y la cota hallada es mucho mas fácil de demostrar.

En la siguiente demostración se utilizará nuevamente la matriz

$$T := (T_{i,j})_{1\leq i\leq r, 1\leq j\leq N+1}$$

de indeterminadas $T_{i,j}$ introducida anteriormente.

Demostración del lema 36 Aplicando el lema 35 se construyen en forma recursiva con respecto a la dimensión r de la variedad V polinomios lineales afines $L_1, \ldots, L_r \in \mathbb{Z}[Z]$ que satisfacen los requirimientos del lema a demostrar.

Antes de comenzar esta construcción recursiva obsérvese que la hipótesis que V se define por medio de polinomios en N variables de grado acotado por D y la Desigualdad de Bézout (ver por ejemplo, [88], Theorem 1 o [70], Example 8.4.6) implican en conjunto que el grado de V está acotado por D^N.

Se considera en primer lugar el caso $r := 1$.

Dado que $gr(V) \leq D^N$ es posible elegir un conjunto Γ de a lo sumo D^N puntos de V tales que para cada componente irreducible de máxima dimensión $r = 1$ de V existe al menos un punto en esta componente que pertenece a Γ. Sea

$$Q := \prod_{(\gamma_1,\ldots,\gamma_N)\in\Gamma} (\gamma_1 T_{1,1} + \cdots + \gamma_N T_{1,N} + T_{1,N+1}) \in \mathbb{C}[T_{1,1}, \ldots, T_{1,N+1}]$$

y sea $E_1 \in \mathbb{Z}[T_{1,1}, \ldots, T_{1,N}]$ el polinomio de eliminación del lema 35. Entonces QE_1 es un polinomio no nulo de $\mathbb{C}[T_{1,1}, \ldots, T_{1,N+1}]$ de grado no mayor que $D^{N^2} + D^N < D^{N(N+1)}$. Por lo tanto, existe en el conjunto

$$\left\{(t_{1,1}, \ldots, t_{1,N+1}) \in \mathbb{Z}^{N+1} : \max\{|\, t_{1,j} \,|\colon\ 1 \leq j \leq N+1\} \leq D^{N(N+1)}\right\}$$

un punto $(t_{1,1}, \ldots, t_{1,N+1})$ tal que se satisface la condición

$$QE_1(t_{1,1}, \ldots, t_{1,N+1}) \neq 0$$

Sea $L_1 := t_{1,1}Z_1 + \cdots + t_{1,N}Z_N + t_{1,N+1}$.

Dado que $Q(t_{1,1}, \ldots, t_{1,N+1}) \neq 0$ se deduce que el hiperplano afín $\{z \in \mathbb{C}^N : L_1(z) = 0\}$ corta propiamente todas las componentes irreducibles de V de dimensión maximal $r = 1$ y $E_1(t_{1,1}, \ldots, t_{1,N+1}) \neq 0$ implica que $V \cap \{z \in \mathbb{C}^N : L_1(z) = 0\}$ es no vacía. En consecuencia, por el Teorema de la Dimensión (ver por ejemplo [163]) la dimensión de la variedad algebraica $V \cap \{z \in \mathbb{C}^N : L_1(z) = 0\}$ es $r - 1 = 0$. Mas aún, la altura logarítmica del polinomio lineal afín L_1 satisface los requerimientos en la conclusión del lema 36.

En el caso general $r > 1$ se procede similarmente. Se asume inductivamente que para cada subvariedad cerrada de $\mathbb{C}^N$ de dimensión $r - 1$ que

es definible por polinomios de $\mathbb{Z}[Z_1,\ldots,Z_N]$ de grado a lo sumo D se ha hallado un conjunto de $r-1$ polinomios lineales afines de $\mathbb{Z}[Z_1,\ldots,Z_N]$ que satisfacen los requirimientos en la conclusión del lema 36.

Nuevamente se elige un conjunto Γ de a lo sumo D^N puntos de V tal que para cada componente de dimensión maximal r de V existe al menos un punto en esta componente que pertenece a Γ.

Sea

$$Q := \prod_{(\gamma_1,\ldots,\gamma_N)\in\Gamma} (\gamma_1 T_{1,1} + \cdots + \gamma_N T_{1,N} + T_{1,N+1}) \in \mathbb{C}[T_{1,1},\ldots,T_{1,N+1}]$$

y sea $E_r \in \mathbb{Z}[T]$ el polinomio de eliminación del lema 35. Entonces QE_r es nuevamente un polinomio no nulo de $\mathbb{C}[T]$ de grado estrictamente menor que $D^{N(N+1)}$. Por lo tanto, existe en el conjunto

$$\{(t_{i,j})_{1\le i\le r,\, 1\le j\le N+1} \in \mathbb{Z}^{r\times(N+1)} : \\ : \max\{|\, t_{i,j}\,|\colon\ 1\le i\le r,\ 1\le j\le N+1\} \le D^{N(N+1)}\}$$

un punto $t = (t_{i,j})_{1\le i\le r,\, 1\le j\le N+1}$ tal que $QE_r(t) \neq 0$. Sea $L_1 := t_{1,1}Z_1 + \cdots + t_{1,N}Z_N + t_{1,N+1}$.

Dado que $Q(t) = Q(t_{1,1},\ldots,t_{1,N+1}) \neq 0$ se deduce que el hiperplano afín $\{z \in \mathbf{C}^N :\ L_1(z) = 0\}$ corta propiamente todas las componentes de V de dimensión maximal r. Por otro lado, si se nota por T^* la matriz obtenida a partir de T reemplazando el primer vector fila $(T_{1,1},\ldots,T_{1,N+1})$ en T by $(t_{1,1},\ldots,t_{1,N+1})$ puede inferirse de $E_r(t) \neq 0$ que el polinomio $(r-1)(N+1)$-variado $E_r(T^*)$ es no nulo. Del lema 35 se deduce fácilmente que cada selección de $r-1$ polinomios lineales afines de $\mathbb{C}[Z_1,\ldots,Z_n]$ cuyos coeficientes satisfacen la condición abierta Zariski $E_r(T^*) \neq 0$ define una intersección no vacía con la variedad algebraica $W := V \cap \{z \in \mathbf{C}^N :\ L_1(z) = 0\}$. Esto implica que W es no vacía y que $\dim W = r-1$. Por otro lado, W es definible por polinomios de $\mathbb{Z}[Z_1,\ldots,Z_N]$ de grado a lo sumo D. En consecuencia, aplicando la hipótesis inductiva a la variedad W se hallan polinomios lineales afines $L_2,\ldots,L_r \in \mathbb{Z}[Z_1,\ldots,Z_N]$ de altura logarítmica acotada por $N(N+1)\log_2 D$ tales que para cada $2 \le k \le r$ el subconjunto cerrado Zariski

$$W \cap \{z \in \mathbf{C}^N :\ L_2(z) = 0,\ldots,L_k(z) = 0\} = \\ = V \cap \{z \in \mathbf{C}^N :\ L_1(z) = 0,\ldots,L_k(z) = 0\}$$

es no vacío de dimensión $\dim(W) - (k-1) = (r-1) - (k-1) = r - k$. Juntando toda esta información se ve que los polinomios lineales afines $L_1, \ldots, L_r$ satisfacen los requirimientos en la conclusión del lema 36. □

A fin de finalizar la demostración de la proposición 11 se necesario el siguiente resultado que estima los valores absolutos de las coordenadas de los coordenadas de los puntos aislados de un subconjunto del espacio afín $\mathbf{C}^N$ cerrado Zariski $\mathbb{Q}$-definible.

Proposición 12 *Sean N, D, η y s números naturales dados con $D \geq N$ y sean $h_1, \ldots, h_s$ polinomios de grado a lo sumo D y altura logarítmica acotada por η, que pertenecen a $\mathbb{Z}[Z_1, \ldots, Z_N]$. Sea V el subconjunto de $\mathbf{C}^N$ cerrado Zariski definido por estos polinomios, es decir:*

$$V := \{z \in \mathbf{C}^N :. h_1(z) = 0, \ldots, h_s(z) = 0\}$$

Entonces cualquier punto aislado $\theta := (\theta_1, \ldots, \theta_N)$ de V satisface la estimación

$$\max\{\log_2 | \theta_i | :\ 1 \leq j \leq N\} \leq D^{c'N}(\log_2 s + \eta),$$

donde $c' > 0$ es una constante universal adecuada.

Por una demostración de este resultado ver [114], Corollary 7.

Ahora se puede demostrar la Proposición 11:

Demostración de la proposición 11 Sea $r := \dim V$. Dado que V es no vacía por hipótesis se tiene que $0 \leq r \leq N$. En caso en que $r = 0$ todos los puntos de V son puntos aislados y se puede aplicar directamente la proposición 12 a fin de obtener un punto θ de V que satisface la estimación requerida.

Supóngase ahora que $r > 0$. Del lema 36 se deduce que existen r polinomios lineales afines en $\mathbb{Z}[Z_1, \ldots, Z_N]$, $L_1, \ldots, L_r$, de altura logarítmica no mayor que $N(N+1)\log_2 D$ tales que

$$\begin{aligned} W := V \cap \{z \in \mathbf{C}^N :\ & L_1(z) = 0, \ldots, L_r(z) = 0\} = \\ & = \{z \in \mathbf{C}^N : h_1(z) = 0, \ldots, h_s(z) = 0, L_1(z) = 0, \ldots, L_r(z) = 0\} \end{aligned}$$

es una subvariedad algebraica de $\mathbf{C}^N$ cero-dimensional. En particular W es no vacía. La variedad W se define por $s + r \leq s + N$ polinomios que

pertenecen a $\mathbb{Z}[Z_1, \ldots, Z_N]$ y que tienen grado acotado por D y altura logarítmica no mayor que $\max\{\eta, N(N+1)\log_2 D\}$. Sea $\theta = (\theta_1, \ldots, \theta_N)$ un punto cualquiera de W. Aplicando la proposición 12 a la variedad W se deduce la estimación

$$\max\{\log_2 \mid \theta_i \mid : \ 1 \leq j \leq N\} \leq D^{c'N}(\log_2(s+N)+\max\{\eta,\ N(N+1)\log_2 D\})$$

$$\leq D^{cN}(\log_2 s + \eta)$$

donde $c > 0$ es una constante universal adecuada (aquí se usa la hipótesis $D \geq N$). Dado que W está contenida en V el punto θ pertenece a la variedad V. Mas aún, los valores absolutos de las coordenadas de θ satisfacen los requirimientos en la conclusión de la proposición 11. □

3.3 Polinomios difíciles de evaluar

En esta última sección de este capítulo se exhibirán algunos ejemplos de familias de polinomios univariados *específicas* que son difíciles de evaluar desde el punto de vista del tradeoff espacio-tiempo. En estos ejemplos se exhibirán cotas inferiores significativas para los requerimientos de espacio de cualquier procedimiento óptimo con respecto al tiempo no escalar que evalúa estos polinomios. Se pueden dividir los ejemplos en dos grupos principales según la forma en que están dados los polinomios en consideración: por sus coeficientes o por sus raíces. El interés del último grupo de ejemplos está motivado por la búsqueda de cotas inferiores de complejidad en teoría de eliminación geométrica donde la representación de los polinomios por sus raíces aparece naturalmente (ver [90], [165]). Se puede realizar una segunda división de los ejemplos en dos clases que agrupan a los polinomios que tienen coeficientes algebraicos o racionales. Se ha tratado de hallar una presentación casi unificada para estas clases de ejemplos.

3.3.1 Polinomios dados por sus coeficientes

En esta subsección se presenta una serie de técnicas para mostrar cotas inferiores para el tradeoff espacio-tiempo y aplicarlas a familias específicas de polinomios con coeficientes enteros y algebraicos. Se comenzará con dos familias de polinomios particulares con *coeficientes enteros* y se demostrará que

estas familias son difíciles de evaluar en términos de tradeoff espacio-tiempo. Luego, se obtendrá el mismo tipo de resultados para familias de polinomios específicos con *coeficientes algebraicos*. Finalmente se demostrará que existen muchas familias de polinomios con *coeficientes* $\{0,1\}$ que son difíciles de evaluar en términos de tradeoff espacio-tiempo.

Polinomios con coeficientes enteros

En [171] se presentan varias familias explícitas de polinomios con coeficientes enteros que son difíciles de evaluar en el sentido de complejidad de tiempo secuencial. Este tipo de resultados se extiende y se mejora en [161] y [168]. Se aplicará la proposición 11 a fin de obtener resultados de tradeoff espacio-tiempo en el espíritu de las referencias citadas.

Ejemplo 1 *Sea* $\mathcal{F}_1 := (F_d)_{d\in\mathbf{N}}$ *la familia de los polinomios* $F_d \in \mathbb{Z}[X]$ *de grado* d *definida por*

$$F_d := \sum_{0\le j\le d} 2^{j!} X^j.$$

Entonces esta familia $\mathcal{F}_1$ *es difícil de evaluar en el sentido del tradeoff espacio-tiempo. Más precisamente, se tiene*

$$LS^2(F_d) = \Omega(d)$$

Demostración Sea d fijo y sea $F := F_d$. Sean además L y S números naturales arbitrarios tales que el polinomio F puede evaluarse por medio de un straight-line program en $\mathbb{Q}(X)$, que utiliza tiempo no escalar L y espacio S. Entonces el polinomio F pertenece a la imagen del morfismo

$$\Phi := \Phi_{d,L,S} := (P_d, \ldots, P_0) : \mathbf{C}^N \longrightarrow \mathbf{C}^{d+1}$$

introducido en el lema 33, con $N := 8LS^2 + 1$ y $P_0, \ldots, P_d \in \mathbb{Z}[Z_1, \ldots, Z_N]$ (recuérdese que se identifica el polinomio $F \in \mathbb{Z}[X]$ con el punto $(f_j)_{0\le j\le d} := (2^{j!})_{0\le j\le d}$ de $\mathbf{C}^{d+1}$ dado por el vector de coeficientes de F). Se observa que $(f_j)_{0\le j\le d}$ es el único punto de $\mathbf{C}^{d+1}$ contenido en la variedad algebraica

$$\{(f_d, \ldots, f_0) \in \mathbf{C}^{d+1} : \ f_0 - 2 = 0, f_1 - f_0 = 0, \ldots, f_d - f_{d-1}^d = 0\}.$$

Sea $Z = (Z_1, \ldots, Z_N)$ y considérense los polinomios $Q_0, \ldots, Q_d \in \mathbb{Z}[Z]$ definidos $Q_0 := P_0(Z) - 2$ y $Q_j(Z) := P_j(Z) - P_{j-1}^j(Z)$ con $1 \leq j \leq d$. Nótese que la Φ-fibra $V := \Phi^{-1}(F)$ del punto $F \in \mathbb{C}^{d+1}$ es el conjunto algebraico

$$V = \{z \in \mathbb{C}^N : \ Q_0(z) = 0, \ldots, Q_d(z) = 0\}$$

Sea

$$D := \max\{gr(Q_i) : \ 0 \leq j \leq d\}$$

y

$$\eta := \max\{\log_2 height(Q_j) : \ 0 \leq j \leq d\}$$

Del lema 33 se deduce que vale

$$gr(Q_j) \leq j gr(P_j) \leq 2j(Ld+1) \leq 2d(Ld+1)$$

para $0 \leq j \leq d$.

Esto implica

$$D \leq 2d(Ld+1) \tag{3.20}$$

Además, del lema 33 se concluye

$$\begin{aligned} \log_2(height(Q_0)) &\leq 1 + \log_2(peso(P_0)) \leq \\ &\leq 1 + (d+1)\log_2(d+1) + (d+1)^{L+1}(2 + \log_2(S+1)), \end{aligned}$$

y

$$\begin{aligned} \log_2(height(Q_j)) &\leq \log_2(peso(P_j)) + \log_2(peso(P_{j-1}))^j \leq \\ &\leq (d+1)\log_2(d+1) + (d+1)^{L+1}(2 + \log_2(S+1)) + \\ &+ d((d+1)\log_2(d+1) + (d+1)^{L+1}(2 + \log_2(S+1))) \leq \\ &\leq (d+1)^2 \log_2(d+1) + (d+1)^{L+2}(2 + \log_2(S+1)) \end{aligned}$$

para $1 \leq j \leq d$. Esto implica la cota de altura

$$\eta \leq (d+1)^2 \log_2(d+1) + (d+1)^{L+2}(2 + \log_2(S+1)) + 1 \tag{3.21}$$

Aplicando la proposición 11 a la variedad algebraica V definida y tomando en cuenta las estimaciones de profundidad y altura (3.20) y (3.21), se concluye que V contiene un punto $\theta = (\theta_1, \ldots, \theta_N)$ que satisface la estimación:

$$\log_2 \max\{|\, \theta_i \,|\colon\ 1 \le i \le N\} \le D^{cN}(\log_2(d+1)+\eta)\},$$

donde $c > 0$ es una constante universal adecuada. Sea $|\ \theta\ | := max\{|\ \theta_i\ |\colon 1 \le i \le N\}$. A fin de terminar la demostración se considera para $0 \le j \le d$ el j-ésimo coeficiente f_j del polinomio F. Dado que la imagen del punto θ bajo el morfismo Φ es F, se tiene que $f_j = P_j(\theta)$ para $0 \le j \le d$. Por lo tanto, por el lema 33, el valor absoluto de f_j está acotado como sigue:

$$\begin{aligned}\log_2 |\, f_j \,| &\le \log_2 peso(P_j) + gr(P_j)\cdot \log_2 |\, \theta \,| \le \\ &\le (d+1)\log_2(d+1) + (d+1)^{L+1}(2+\log_2(S+1)) + \\ &\quad + 2(Ld+1)D^{cN}(\eta + \log_2(d+1)).\end{aligned}$$

Por la regla de Horner se puede asumir sin pérdida de generalidad que $LS^2 \le c_1 d$, donde c_1 es una constante universal adecuada. Combinando esta observación con las estimaciones (3.20) y (3.21) para D y η, se concluye que el valor absoluto de las coordenadas $f_0, \ldots, f_d$ del polinomio F satisfacen la desigualdad

$$d! \le \max\{\log_2 |\, f_j \,| \colon\ 0 \le j \le d\} \le d^{c_2 N}$$

donde $c_2 > 0$ es una constante universal adecuada. En consecuencia, se obtiene por un lado que $d! \le d^{c_2 N}$ y por el otro que $N = 8LS^2 + 1$. Esto implica $c_3 d \le LS^2$ para una constante universal adecuada $c_3 > 0$. Dado que L y S son los requerimientos de tiempo y espacio de un straight-line program arbitrario que evalúa el polinomio $F = F_d$ se obtiene finalmente $LS^2(F_d) = \Omega(d)$. □

Ejemplo 2 *Sea $\mathcal{F}_2 := (F_d)_{d\in\mathbb{N}}$ la familia de polinomios $F_d \in \mathbb{Z}[X]$ de grado d definida por*

$$F_d := \sum_{0\le j\le d} 2^{2^j} X^j$$

Entonces, esta familia $\mathcal{F}_2$ es difícil de evaluar en el sentido del tradeoff espacio-tiempo. Más precisamente, se tiene

$$LS^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right)$$

La demostración de esta cota puede establecerse en la misma forma que en el ejemplo 1. Para $d, L, S \in \mathbb{N}$ dados se considera la variedad algebraica

$$\{(f_d, \ldots, f_0) \in \mathbf{C}^{d+1} : f_0 - 2 = 0,\ f_1 - f_0^2 = 0, \ldots,\ f_d - f_{d-1}^2 = 0\}$$

cuyos único punto es el vector de coeficientes del polinomio F_d. La $\Phi_{d,L,S}$-fibra de esta variedad se define por $P_0(Z) - 2$ y los polinomios $P_j(Z) - P_{j-1}^2(Z)$ con $1 \leq j \leq d$. Los restantes argumentos son los mismos que en la demostración de la cota inferior del ejemplo 1.

Cabe destacar que el ejemplo 2 se analiza en [171] donde se demuestra la cota inferior de tiempo secuencial $L(F_d) = \Omega\left(\sqrt[3]{\frac{d}{\log_2 d}}\right)$.

Polinomios con coeficientes algebraicos

En esta subsubsección se adaptan dos métodos generales para demostrar cotas inferiores de complejidad para polinomios con coeficientes no racionales al contexto del tradeoff espacio-tiempo. El primer método que se presenta fue recientemente introducido por W. Baur [9]. La descripción de una idea similar puede hallarse en [37], Chapter 9, Exercise 9.11.

Proposición 13 *Existe una constante universal $c > 0$ con la siguiente propiedad: sea D un número natural dado y sea*

$$F := \sum_{0 \leq j \leq d} f_j X^j$$

un polinomio de grado a lo sumo d con coeficientes complejos. Supóngase que existen polinomios $g_1, \ldots, g_m \in \mathbb{Q}[Y_d, \ldots, Y_0]$ de grado a lo sumo D, y que los números complejos $g_1(f_d, \ldots, f_0), \ldots, g_m(f_d, \ldots, f_0)$ son $\mathbb{Q}$-linealmente independientes. Bajo estas hipótesis se tiene

$$LS^2(F) \geq c \cdot \frac{\log_2 m}{\log_2 d + \log_2 D}$$

Demostración Sea dado un straight-line program arbitrario β en $\mathbf{C}(X)$ que evalúa el polinomio F en tiempo no escalar L y espacio S. Como antes, en virtud de la regla de Horner se puede asumir sin pérdida de generalidad que vale $L \leq d$. Sea $N := 8LS^2 + 1$ y $\delta := (2Ld + 1)$. Sean

$Z_1, \ldots, Z_N$ nuevas indeterminadas. Entonces por el lema 33 existen polinomios $P_d, \ldots, P_0 \in \mathbb{Z}[Z_1, \ldots, Z_N]$ de grado a lo sumo δ tales que el vector de coeficientes $(f_d, \ldots, f_0)$ de F está en la imagen del morfismo de espacios afines $\Phi_{d,L,S} : \mathbf{C}^N \longrightarrow \mathbf{C}^{d+1}$ dado por $(P_d, \ldots, P_0)$.

Dado que los números complejos $g_1(f_d, \ldots, f_0), \ldots, g_m(f_d, \ldots, f_0)$ son $\mathbb{Q}$-linealmente independientes por hipótesis y existe un punto $\theta \in \mathbf{C}^N$ tal que vale

$$(f_d, \ldots, f_0) = (P_d(\theta), \ldots, P_0(\theta))$$

se concluye que los polinomios $g_1(P_d \ldots, P_0), \ldots, g_m(P_d, \ldots, P_0)$ también deben ser $\mathbb{Q}$-linealmente independientes. Nótese que estos polinomios tienen grado acotado por δD. Esto implica que el $\mathbb{Q}$-espacio vectorial:

$$\mathcal{P} := \{G \in \mathbb{Q}[Z_1, \ldots, Z_N] : \ gr(G) \leq \delta D\}$$

tiene dimensión al menos m. Por otro lado, se tiene

$$dim(\mathcal{P}) = \binom{N + \delta D}{N} \leq (\delta D)^N$$

Teniendo en cuenta que $L \leq d$ se deduce de ésta la estimación

$$m \leq (\delta D)^N = (2(Ld + 1)D)^{8LS^2+1} \leq (2(d^2 + 1)D)^{8LS^2+1}$$

Tomando logaritmos, se concluye que existe una constante universal $c > 0$ tal que vale $LS^2 \geq c\frac{\log_2 m}{\log_2 d + \log_2 D}$. Dado que β era un straight-line program arbitrario en $\mathbb{Q}(X)$ calculando el polinomio F en tiempo no escalar L y espacio S sigue la proposición 13. □

El segundo método para demostrar cotas inferiores del tradeoff espacio-tiempo del polinomios con coeficientes racionales tiene su origen en [95].

Proposición 14 *Existe una constante universal $c > 0$ con la siguiente propiedad: sea D un número natural y sea*

$$F := \sum_{0 \leq j \leq d} f_j X^j$$

un polinomio de grado a lo sumo d con coeficientes complejos algebraicos. Sea ρ el cardinal de la órbita del punto $(f_d, \ldots, f_0) \in \mathbf{C}^{d+1}$ bajo la acción

del grupo de automorfismos de $\mathbf{C}$ *over* $\mathbb{Q}$. *Supóngase que existen polinomios* $g_1, \ldots, g_m \in \mathbb{Q}[Y_d, \ldots, Y_0]$ *de grado a lo sumo* D, *tales que el conjunto de ceros comunes de esos polinomios en* $\mathbf{C}^{d+1}$ *es finito y contiene el punto* $(f_d, \ldots, f_0)$. *Bajo estas hipótesis se tiene*

$$LS^2(F) \geq c \cdot \frac{\log_2 \rho}{\log_2 d + log_2 D}$$

Demostración Sea β un straight-line program arbitrario en $\mathbf{C}(X)$ que evalúa el polinomio F en tiempo no escalar L y espacio S. Obsérvese que el vector de coeficientes $(f_d, \ldots, f_0)$ del polinomio F pertenece a la subvariedad algebraica $W := W_{d,L,S}$ de $\mathbf{C}^{d+1}$ introducida en el lema 34. Sea $r := \dim(W)$ y obsérvese que vale $r \leq 8LS^2$ por el mismo lema. Se eligen ahora r combinaciones $\mathbb{Q}$-lineales genéricas

$$B_k := \beta_1^{(k)} g_1 + \ldots + \beta_m^{(k)} g_m \in \mathbb{Q}[Y_d, \ldots, Y_0]$$

de los polinomios $g_1, \ldots, g_m$ para $1 \leq k \leq r$ con coeficientes $\beta_1^{(k)}, \ldots, \beta_m^{(k)} \in \mathbb{Q}$. La genericidad de esta elección y el hecho que los polinomios $g_1, \ldots, g_m$ definen un subconjunto no vacío finito (es decir una subvariedad cero-dimensional) de $\mathbf{C}^{d+1}$ implican, junto con el hecho que $r = \dim(W)$, que el conjunto

$$V := W \cap \{(y_d, \ldots, y_0) \in \mathbf{C}^{d+1} : B_1(y_d, \ldots, y_0) = 0, \ldots, B_r(y_d, \ldots, y_0) = 0\}$$

es finito. Obsérvese que vale que $(f_d, \ldots, f_0) \in V$ y que $B_1, \ldots, B_r$ son polinomios de $\mathbb{Q}[Y_d, \ldots, Y_0]$ de grado acotado por D.

En consecuencia V es una subvariedad de $\mathbf{C}^{d+1}$ cero-dimensional $\mathbb{Q}$-definible que contiene a la órbita del punto $(f_d, \ldots, f_0)$ bajo la acción del grupo de automorfismos de $\mathbf{C}$ sobre $\mathbb{Q}$. Esto implica $\rho \leq \#V = gr(V)$.

De la Desigualdad de Bézout y el lema 34 (ii) se infiere

$$gr(V) \leq gr(W) \cdot D^r \leq gr(W) \cdot D^{8LS^2} \leq (2(Ld+1)D)^{8LS^2}$$

Como antes se puede asumir sin pérdida de generalidad que vale $L \leq d$. Juntando toda esta información se obtiene la estimación

$$\rho \leq (2(d^2+1)D)^{8LS^2}$$

Tomando logaritmos, se concluye que existe una constante universal $c > 0$ tal que se satisface la condición $LS^2 \geq c \cdot \frac{\log_2 \rho}{\log_2 d + \log_2 D}$.

Dado que β es un straight-line program arbitrario en $\mathbf{C}(X)$ que calcula el polinomio F en tiempo no escalar L y espacio S sigue la proposición 14. □

Usando las proposiciones 13 y 14 se exhibirán dos familias de polinomios con coeficientes algebraicos que son difíciles de evaluar en el sentido del tradeoff espacio-tiempo. Estas familias han sido analizadas en [95] y [76], Application 2 desde el punto de vista de la complejidad de tiempo secuencial.

Ejemplo 3 *1. Sea $\mathcal{F}_3 := (F_d)_{d \in \mathbf{N}}$ la familia de polinomios $F_d \in \mathbb{R}[X]$ de grado d definida por*

$$F_d := \sum_{1 \leq j \leq d} \sqrt{p_j} X^{j-1}$$

donde p_j denota el j-ésimo número primo. Entonces esta familia $\mathcal{F}_3$ es difícil de evaluar en el sentido del tradeoff espacio-tiempo. Más precisamente, se tiene

$$LS^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right)$$

2. Sea $\mathcal{F}_4 := (F_d)_{d \in \mathbf{N}}$ la familia de polynomios $F_d \in \mathbf{C}[X]$ de grado d definida por

$$F_d := \sum_{1 \leq j \leq d} e^{\frac{2\pi i}{j}} X^{j-1}$$

donde $e^{\frac{2\pi i}{j}}$ denota la j-ésima raíz de la unidad (canónica) contenida en $\mathbf{C}$. Entonces esta familia $\mathcal{F}_4$ es difícil de evaluar en el sentido del tradeoff espacio-tiempo. Más precisamente, se tiene

$$LS^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right)$$

Demostración Sean $Y_d, \ldots, Y_0$ nuevas indeterminadas.

Se discute en primer lugar la cota inferior asintótica para la familia $\mathcal{F}_3$. Para ello, se aplicará la proposición 13.

Para cada $S \subseteq \{1, \ldots, d\}$ se considera el polinomio

$$g_S := \prod_{j \in S} Y_j \in \mathbb{Q}[Y_d, \ldots, Y_0]$$

Obsérvese que el grado de g_S está acotado por d.

De [76] se deduce fácilmente que la familia de valores complejos

$$\left\{ g_S(\sqrt{p_1}, \ldots, \sqrt{p_d}) \ : \ S \subseteq \{1, \ldots, d\} \right\}$$

es $\mathbb{Q}$-linealmente independiente. La cota inferior para el tradeoff espacio-tiempo de la familia $\mathcal{F}_3$ se deduce ahora fácilmente de la proposición 13 tomando $m := 2^d$ y $D := d$.

Con respecto a la familia $\mathcal{F}_4$, se aplicará la proposición 14. Considérense los polinomios

$$g_1 := Y_0, \ g_2 := Y_1 - 1, g_3 := Y_2^2 - 1, \ldots, \ g_{d+1} := Y_d^d - 1$$

Obsérvese que estos polinomios se anulan en el punto $\theta := (0, e^{\frac{2\pi i}{1}}, \ldots, e^{\frac{2\pi i}{d}})$ de $\mathbb{C}^{d+1}$ que representa los coeficientes del d-ésimo miembro de la familia $\mathcal{F}_4$, es decir, el polinomio $F_d = \sum_{1 \leq j \leq d} e^{\frac{2\pi i}{j}} X^{j-1}$. Más áun, los polinomios $g_1, \ldots, g_{d+1}$ pertenecen a $\mathbb{Q}[Y_d, \ldots, Y_0]$, tienen grado a lo sumo d y definen un subconjunto finito de $\mathbb{C}^{d+1}$.

Sea ρ el cardinal de la órbita del punto θ bajo la acción del grupo de automorfismos de $\mathbb{C}$ sobre $\mathbb{Q}$. Denótese por φ la función de Euler y por $[1, 2, \ldots, d]$ el mínimo común múltiplo de los $1, 2, \ldots, d$. Con estas notaciones se deduce fácilmente la siguiente identidad

$$\rho = [\mathbb{Q}(e^{\frac{2\pi i}{1}}, \ldots, e^{\frac{2\pi i}{d}}) : \mathbb{Q}] = \varphi([1, 2, \ldots, d])$$

Del Teorema de los Números Primos (ver por ejemplo [45] se infiere que

$$log_2 \rho = \log_2 \varphi([1, 2, \ldots, d]) = \Omega(d)$$

La cota inferior para el tradeoff espacio-tiempo de la familia $\mathcal{F}_4$ es una consecuencia inmediata de la proposición 14 tomando $D := d$. □

Polinomios con coeficientes $\{0,1\}$

En esta subsubsección se demuestra que casi todos los polinomios con coeficientes $\{0,1\}$ son difíciles de evaluar en el sentido del tradeoff espacio-tiempo. El método que se utilizará en la demostración de este resultado fue aplicado en una forma levemente diferente en [94] a fin de demostrar cotas inferiores para la complejidad en tiempo no escalar de estos polinomios. Se introduce la siguiente notación:
para cada número natural d sea

$$LS^2_{\{0,1\}}(d) := \max\Big\{LS^2\big(\sum_{0\le j\le d} f_j X^j\big) : (f_d,\ldots,f_0)\in\{0,1\}^{d+1}\Big\}$$

Teorema 19 *Sean $d\ge 2$ y k números naturales con $d > k\log_2 d$. Entonces se tiene:*

(i) $\#\{(f_d,\ldots,f_0)\in\{0,1\}^{d+1} : LS^2(\sum_{0\le j\le d} f_j X^j)\le \frac{1}{16}(\frac{d}{\log_2 d}-k)\}\le \frac{2^d}{d^k}$,

(ii) $LS^2_{\{0,1\}}(d)\ge \frac{1}{16}\frac{d}{\log_2 d}$.

Demostración Sean d,k,L,S números naturales dados sujetos a las condiciones $d\ge 2$, $d > k\log_2 d$ y $LS^2\le \frac{1}{16}(\frac{d}{\log_2 d}-k)$. Obsérvese que el conjunto $\{0,1\}^{d+1}$ puede ser definido como la intersección de $d+1$ hipersuperficies de $\mathbf{C}^{d+1}$ de grado 2, es decir como

$$\{0,1\}^{d+1} = \{(f_d,\ldots,f_0)\in\mathbf{C}^{d+1} : f_d^2-f_d=0,\ldots,f_0^2-f_0=0\}$$

Aplicando [94], Proposition 2.3 y el lema 34 de la subsección 3.1.3 se deduce de la Desigualdad de Bézout las siguientes estimaciones:

$$\begin{aligned}\#(W_{d,L,S}\cap\{0,1\}^{d+1}) &\le gr(W_{d,L,S})\cdot 2^{\dim(W_{d,L,S})}\le\\ \le (4(Ld+1))^{8LS^2} &\le (8Ld)^{8LS^2}\le\\ &\le (8LS^2d)^{8LS^2}.\end{aligned}$$

Tomando logaritmos y usando la hipótesis $LS^2\le\frac{1}{16}(\frac{d}{\log_2 d}-k)$, se concluye

$$\begin{aligned}
\log_2(\#(W_{d,L,S} \cap \{0,1\}^{d+1})) &\leq 8LS^2 \log_2(8LS^2 d) \leq \\
&\leq \frac{1}{2}\left(\frac{d}{\log_2 d} - k\right) \log_2 \left(\frac{1}{2}\left(\frac{d}{\log_2 d} - k\right) d\right) \leq \\
&\leq \frac{1}{2}\left(\frac{d}{\log_2 d} - k\right) \log_2 \left(\frac{1}{2} d^2 \left(\frac{1}{\log_2 d} - \frac{k}{d}\right)\right) \leq \\
&\leq \frac{1}{2}\left(\frac{d}{\log_2 d} - k\right) \left(2\log_2 d + \log_2 \left(\frac{1}{2}\left(\frac{1}{\log_2 d} - \frac{k}{d}\right)\right)\right).
\end{aligned}$$

De la suposición que $d > k \log_2 d$ se deduce $0 < \frac{1}{2}(\frac{1}{\log_2 d} - \frac{k}{d}) \leq 1$. Esto implica

$$\log_2(\#(W_{d,L,S} \cap \{0,1\}^{d+1})) \leq d - k \log_2 d$$

Del lema 2.6 (iii) se infiere que

$$\#\{(f_d, \ldots, f_0) \in \{0,1\}^{d+1} : LS^2(\sum_{0 \leq j \leq d} f_j X^j) \leq \frac{1}{16}(\frac{d}{\log_2 d} - k)\} \leq \frac{2^d}{d^k}$$

lo cual constituye la aserción (i) del teorema. (ii) sigue de (i) tomando $k := 1$ y observando que el conjunto $\{0,1\}^{d+1}$ tiene $2^{d+1} > \frac{2^d}{d}$ elementos. □

3.3.2 Polinomios dados por sus raíces

El estudio de las cotas inferiores de complejidad para la evaluación de familias polinomios dados por sus raíces está motivada por su relación con la complejidad intrínseca de los procedimientos de eliminación de cuantificadores. Puede hallarse evidencia de esta relación en [90], [138] y [165]. En esta subsección se exhiben dos ejemplos de familias de polinomios dados por sus raíces que son difíciles de evaluar en términos del tradeoff espacio-tiempo.

Sean $Y_{d-1}, \ldots, Y_0$ nuevas indeterminadas y sea $G := X^d + Y_{d-1}X^{d-1} + \cdots + Y_0$ el polinomio genérico mónico en la variable X con coeficientes $Y_{d-1}, \ldots, Y_0$.

Sea además $D(Y_{d-1},\ldots,Y_0)$ el discriminante del polinomio G con respecto a la variable X.

Lema 37 *Sea $\mathcal{F}_5 := (F_d)_{d\in\mathbb{N}}$ la familia de polinomios $F_d \in \mathbb{Z}[X]$ de grado d definida por*

$$F_d := \prod_{1\le j\le d} (X - 2^{2^j}).$$

Entonces F_d es el único polinomio mónico $F = X^d + f_{d-1}X^{d-1} + \cdots + f_0$ de grado d con coeficientes reales que satisface las siguientes cuatro condiciones:

1. $F(0) \neq 0, F(1) \neq 0, F(-1) \neq 0$
2. $D(f_{d-1},\ldots,f_0) \neq 0$ *(esto significa que F tiene solamente raíces simples)*
3. *el polinomio F tiene solamente ceros reales*
4. *existe un número real t_0 con $t_0^2 \neq 4$ tal que vale*

$$(-1)^d 4 f_0 = t_0^2$$

$$y\ (-1)^d F(X)F(-X)(X^2-4) = (X^2 - t_o^2)F(X^2)$$

Demostración Tomando $t_0 := 2^{2^d}$ se puede chequear fácilmente que el polinomio F_d satisface las cuatro condiciones del lema. En consecuencia es suficiente demostrar que existe al menos un polinomio mónico $F = X^d + f_{d-1}X^{d-1} + \cdots + f_0 \in \mathbb{R}[X]$ de grado d que satisface las condiciones.

Supóngase ahora que tal polinomio F está dado y fíjese un número real t_0 que satisface la cuarta condición con respecto a este F. Esta condición implica que para cada raíz x de F, o bien $x^2 = t_0^2$ o $F(x^2) = 0$ se satisface. Por lo tanto, para cada raíz x de F ocurre uno de los dos siguientes casos:

(i) existe un número natural k con $x^{2^k} = t_0^2$, o

(ii) cualquier elemento del conjunto $S(x) := \{x^{2^m} : m \in \mathbb{N}\}$ es una raíz de F.

En el caso (ii) las hipótesis sobre F implican que el conjunto $S(x)$ es infinito. Esto elimina este caso ya que F es mónico. En consecuencia cualquier raíz x de F satisface (i).

Se ve fácilmente que $F(4) = 0$. Sea r un entero no negativo maximal tal que $2^2, 2^{2^2}, \ldots, 2^{2^r}$ son raíces de F. Dado que $F(4) = 0$ y $gr(F) = d$ se concluye que $1 \leq r \leq d$. La maximalidad de r implica que $F(2^{2^{r+1}}) \neq 0$ de donde $2^{2^{r+1}} = t_0^2 = (-1)^d 4 f_0$. En consecuencia se tiene $\mid t_0 \mid > 1$.

Ahora se demostrará que $r = d$. Supóngase que este no es el caso. De la hipótesis que F tiene solamente raíces simples que son todas reales se deduce que deben existir $d - r$ ceros reales distintos $x_{r+1}, \ldots, x_d$ de F no contenidos en el conjunto $\{2^2, 2^{2^2}, \ldots, 2^{2^r}\}$. Por lo tanto, las raíces de F son los números reales $2^2, 2^{2^2}, \ldots, 2^{2^r}, x_{r+1}, \ldots, x_d$. Esto implica

$$2^{2^{r+1}} = (-1)^d 4 f_0 = 4 \cdot 2^2 \cdot 2^{2^2} \cdots 2^{2^r} \cdot x_{r+1} \cdots x_d$$

y consecuentemente $x_{r+1} \cdots x_d = 1$.

Sea $r < m \leq d$. Dado que la raíz x_m de F satisface (i) existe un número natural k_m tal que $x_m^{2^{k_m}} = t_0^2$. Por lo tanto, como $\mid t_0 \mid > 1$ se tiene que $\mid x_m \mid > 1$ para cada $r < m \leq d$. Pero esto contradice la conclusión $x_{r+1} \cdots x_d = 1$.

La demostración de la aserción $r = d$ se concluye observando que $2^2, 2^{2^2}, \ldots, 2^{2^d}$ son todas las raíces del polinomio mónico F de grado d. En otras palabras, se tiene

$$F = \prod_{1 \leq j \leq d} (X - 2^{2^j}) = F_d$$

□

Sea n un número natural y sean $X_1, \ldots, X_n$ indeterminadas sobre $\mathbb{Z}$. Un subconjunto S de $\mathbb{R}^n$ se dice *semialgebraico* si existe un conjunto finito de polinomios $\mathcal{G} \in \mathbb{Z}[X_1, \ldots, X_n]$ tales que S es definible como una expresión booleana contruída a partir de fórmulas atómicas de tipo $G = 0$ o $G > 0$ con $G \in \mathcal{G}$. En este caso se dirá también que S es un conjunto semialgebraico $\mathcal{G}$-*definible*. Un conjunto semialgebraico tiene sólo finitas componentes conexas que son a su vez conjuntos semialgebraicos (por más detalles ver [22]).

En lo sucesivo se utilizará la siguiente estimación que puede hallarse en [179] (comparar con [93], Theorem 4):

Proposición 15 *Existe una constante universal $c_0 > 0$ con la siguiente propiedad:*
sean n, D, s, h números naturales y sea $\mathcal{G}$ un conjuto de s polinomios de $\mathbb{Z}[X_1, \ldots, X_n]$ de grado acotado por D y altura logarítmica acotada por h, que define un conjunto semialgebraico S de $\mathbb{R}^n$. Entonces la bola de $\mathbb{R}^n$ de radio $2^{(sD)^{c_0 n} \cdot h}$ centrada en el origen interseca cada componente conexa de S en al menos un punto.

Ahora se tienen todas las herramientas necesarias para demostrar que la familia $\mathcal{F}_5$ es difícil de evaluar en el sentido del tradeoff espacio-tiempo si se restringe el cuerpo de parámetros a $K := \mathbb{R}$ (ver subsección 3.1.2):

Proposición 16 *Existe una constante universal $c > 0$ con la siguiente propiedad:*
sean d, L, S números naturales y sea

$$F := \prod_{1 \leq j \leq d} (X - 2^{2^j})$$

Sea γ un straight-line program en $\mathbb{R}(X)$ que evalúa el polinomio F en tiempo no escalar L y espacio S. Entonces se tiene

$$LS^2 \geq c \frac{d}{\log_2 d}$$

Demostración Sea $F = f_d X^d + f_{d-1} X^{d-1} + \cdots + f_0$ con $(f_d, \ldots, f_0) \in \mathbb{Z}^{d+1}$ y $f_d = 1$. Obsérvese que F y $(f_{d-1}, \ldots, f_0)$ satisfacen las cuatro condiciones del lema 37. Se aplica ahora el lema 33 con $K := \mathbb{R}$. Siguiendo la demostración de este resultado se ve que existen para $N := 8LS^2 + 1$ polinomios $P_d, \ldots, P_0 \in \mathbb{Z}[Z_1, \ldots, Z_N]$ de grado a lo sumo $2(Ld + 1)$ y peso acotado por $(d+1)!(4(S+1))^{(d+1)^{L+1}}$ tales que el morfismo de espacios afines $\Phi_{d,L,S} : \mathbb{R}^N \to \mathbb{R}^{d+1}$ introducido en este lema manda los parámetros del straight-line program γ en $(f_d, \ldots, f_0) \in \mathbb{Z}^{d+1}$.

Sea $(\zeta_1, \ldots, \zeta_N)$ el punto de $\mathbb{R}^N$ que representa los parámetros de γ, sea $\Phi := \Phi_{d,L,S}$ y sea $V := \Phi^{-1}((f_d, \ldots, f_0))$ la Φ-fibra del punto entero $(f_d, \ldots, f_0)$. Dado que $(\zeta_1, \ldots, \zeta_N)$ está contenido en V, se concluye que V es no vacío.

Se verifica inmediatamente que V es un subconjunto semialgebraico de $\mathbb{R}^N$. Sean $T, U_1, U_2, U_3, U_4, U_5$ nuevas indeterminadas. Usando la notación del lema 37 se considera el siguiente sistema de ecuaciones polinomiales:

$$\begin{aligned}
&P_d - 1 = 0\\
&P_0U_1 - 1 = 0\\
&(\textstyle\sum_{0\le j\le d} P_j)U_2 - 1 = 0\\
&(\textstyle\sum_{0\le j\le d} P_j(-1)^j)U_3 - 1 = 0\\
&D(P_{d-1},\ldots,P_0)U_4 - 1 = 0\\
&(T^2-4)U_5 - 1 = 0\\
&(-1)^d 4P_0 - T^2 = 0\\
&(-1)^d R(k)R(-k)(k^2-4) = (k^2-T^2)R(k^2)
\end{aligned}$$

para $0 \le k \le 2d$ con $R := P_dX^d + \cdots + P_0$. Obsérvese que los polinomios que aparecen en este sistema pertenecen al anillo $\mathbb{Z}[Z_1,\ldots,Z_N,T,U_1,U_2,U_3,U_4,U_5]$ y tienen grado acotado por $D := c'Ld^3$ y altura logarítmica acotada por $h := c'(d+1)^{L+2}(2+\log S)$ para una constante universal $c' > 0$ adecuada. Además hay a lo sumo $s := c'd$ de estos polinomios.

Estos polinomios codifican las cuatro condiciones del lema 37 y definen un subconjunto semialgebraico W de $\mathbb{R}^N \times \mathbb{R}^6$. Sea $\pi : \mathbb{R}^N \times \mathbb{R}^6 \to \mathbb{R}^N$ la proyección canónica que manda cada punto de $\mathbb{R}^N \times \mathbb{R}^6$ en sus primeras N componentes.

De los lemas 37 y 33 se deduce fácilmente que $\pi(W) = V$. En particular W es no vacía. Aplicando la proposición 15 se ve que W contiene un punto $\omega := (\theta_1,\ldots,\theta_N,t,u_1,u_2,u_3,u_4,u_5) \in \mathbb{R}^N \times \mathbb{R}^6$ con

$$\| \omega \| := (\theta_1^2 + \cdots + \theta_N^2 + t^2 + u_1^2 + u_2^2 + u_3^2 + u_4^2 + u_5^2)^{\frac{1}{2}} \le 2^{(sD)^{c_0(N+6)\cdot h}}$$

donde $c_0 > 0$ es la constante universal de dicha proposición. Esto implica que el conjunto semialgebraico contiene un punto $\theta := ((\theta_1,\ldots,\theta_N) \in \mathbb{R}^N$, que se nota por $\theta = \pi(\omega)$, el cual satisface

$$\log_2 | \theta | = \log_2 max\{| \theta_i | : 1 \le i \le N\} \le (sD)^{c_0(N+6)\cdot h}$$

Sin pérdida de generalidad se puede suponer $L \le d$. En consecuencia, tomando en consideración que $N = 8LS^2 + 1, s = c'd, D = c'Ld^3$ y $h = c'(d+1)^{(L+2)}(2+\log S)$ se concluye que existe una constante universal $c'' > 0$

tal que vale la estimación $\log_2 \mid \theta \mid \leq d^{c''LS^2}$. Dado que el punto θ pertenece a la Φ-fibra V de $(f_d, \ldots, f_0)$ se tiene

$$(-1)^d 2^{2^{d+1}-2} = (-1)^d \prod_{1 \leq j \leq d} 2^{2^j} = f_0 = P_0(\theta)$$

Razonando como en la demostración de la cota inferior de tradeoff del ejemplo 1 se obtienen las siguientes desigualdades:

$$2^{d+1} - 2 = \log_2 \mid f_0 \mid \leq \log_2 \text{peso}(P_0) + gr(P_0) \cdot \log_2 \mid \theta \mid \leq$$

$$(d+1)\log_2(d+1) + (d+1)^{L+1}(2 + \log_2(S+1)) + 2(Ld+1)d^{c''LS^2}$$

Tomando logaritmos en estas desigualdades se deduce de $L \leq d$ que existe una constante universal $c > 0$ tal que

$$LS^2 \geq c\frac{d}{\log_2 d}$$

□

Ejemplo 4 *Sea como antes* $\mathcal{F}_5 := (F_d)_{d \in \mathbb{N}}$ *la familia de polinomios* $F_d \in \mathbb{Z}[X]$ *de grado* d *definida por*

$$F_d := \prod_{1 \leq j \leq d} (X - 2^{2^j})$$

Entonces esta familia $\mathcal{F}_5$ *es difícil de evaluar en el sentido del tradeoff espacio-tiempo. Más precisamente se tiene*

$$LS^2(F_d) = \Omega(\frac{d}{\log_2 d})$$

Demostración La cota inferior anunciada en este ejemplo se refiere a straight-line programs en $\mathbf{C}(X)$ y no en $\mathbb{R}(X)$ como en la proposición 16. Sin embargo, esta cota inferior se deduce fácilmente a partir de esa proposición: es suficiente observar que cualquier straight-line program β en $\mathbf{C}(X)$ que calcula el polinomio F_d, puede transformarse en un straight-line program γ que evalúa F_d en tiempo no escalar $5L(\beta)$ y espacio $4S(\beta)$ usando solamente parámetros *reales*.

Este straight-line program γ se obtiene calculando la parte real e imaginaria de cada resultado intermedio de β separadamente (nótese que, en virtud de [122], estas estimaciones de tiempo y espacio para γ son incluso bastante groseras).

El enunciado sigue entonces fácilmente de la proposición 16. □

Se considera ahora un segundo ejemplo de una familia de polinomios dados por su raíces que es difícil de evaluar en el sentido del tradeoff espacio-tiempo. Los polinomios de esta segunda familiar tienen coeficientes algebraicos. Un ejemplo similar fue analizado en [90] desde el punto de vista de la complejidad en tiempo secuencial.

Ejemplo 5 *Sea* $\mathcal{F}_6 := (F_d)_{d\in\mathbb{N}}$ *la familia de polinomios* $F_d \in \mathbb{Z}[X]$ *de grado* d *definido por*

$$F_d := \prod_{1\leq j\leq d} (X - \sqrt{p_j}),$$

donde p_j *denota el* j*-ésimo número primo. Entonces, esta familia* $\mathcal{F}_6$ *es difícil de evaluar en el sentido del tradeoff espacio-tiempo. Más precisamente, se tiene*

$$LS^2(F_d) = \Omega(\frac{d}{\log_2 d})$$

Demostración La cota inferior anunciada sigue de una adaptación de un argumento introducido en [9] al contexto de los tradeoffs espacio-tiempo. Sea $d \in \mathbb{N}$ dado y sea $F := F_d$. Para $1 \leq j \leq d$ se nota por σ_j la j-ésima función simétrica elemental en d argumentos y $f_j := \sigma_j(\sqrt{p_1}, \ldots, \sqrt{p_d})$ por su valor en el punto $(\sqrt{p_1}, \ldots, \sqrt{p_d}) \in \mathbb{R}^d$. Se tiene entonces

$$F = \prod_{1\leq j\leq d} (X - \sqrt{p_j}) = X^d - f_1 X^{d-1} + \cdots + (-1)^d f_d$$

para ciertos números reales algebraicos $f_1, \ldots, f_d$. Sean $X_1, \ldots, X_d$ e $Y_1, \ldots, Y_d$ nuevas indeterminadas y sea $1 \leq j \leq d$. El polinomio $N_j := X_1^{2j+1} + \cdots + X_d^{2j+1}$ es simétrico y por lo tanto existe un (único) polinomio $Q_j \in \mathbb{Z}[Y_1, \ldots, Y_d]$ de grado a lo sumo $2j+1$ tal que

$$N_j(X_1, \ldots, X_d) = Q_j\big(\sigma_1(X_1, \ldots, X_d), \ldots, \sigma_d(X_1, \ldots, X_d)\big)$$

(ver por ejemplo [180]). Sea b_j el número real

$$b_j := Q_j(f_1, \ldots, f_d)$$

Se verifica inmediatamente que

$$b_j = N_j(\sqrt{p_1}, \ldots, \sqrt{p_d}) = p_1^j\sqrt{p_1} + \cdots + p_d^j\sqrt{p_d}$$

Por lo tanto, los valores $b_1, \ldots, b_d$ pueden escribirse como combinaciones $\mathbb{Z}$-lineales de los valores $\sqrt{p_1}, \ldots, \sqrt{p_d}$. La matriz correspondiente es una matriz de Vandermonde no singular $(p_k^j)_{1\leq j,k\leq d}$. Esto implica que existen formas $\mathbb{Q}$-lineales $H_1, \ldots, H_d$ en d argumentos tales que vale $\sqrt{p_j} = H_j(b_1, \ldots, b_d)$ para $1 \leq j \leq d$.

Para cada subconjunto $S \subset \{1, \ldots, d\}$ se considera el polinomio

$$g_S := \prod_{j\in S} H_j(Q_1(Y_1, \ldots, Y_d), \ldots, Q_d(Y_1, \ldots, Y_d))$$

Obsérvese que $gr(g_S) \leq d(2d+1)$ y

$$g_S(f_1, \ldots, f_d) = \prod_{j\in S} \sqrt{p_j}$$

Por lo tanto,

$$\left\{g_S(f_1, \ldots, f_d) : S \subset \{1, \ldots, d\}\right\}$$

forma una familia de 2^d valores reales que son $\mathbb{Q}$-linealmente independientes. La cota inferior para el tradeoff espacio-tiempo de la familia $\mathcal{F}_6$ sigue ahora de la proposición 13 tomando $m := 2^d$ and $D := d(2d+1)$. □

3.3.3 Cotas inferiores de espacio para una evaluación óptima en tiempo

De la regla de Horner se deduce que cualquier polinomio univariado puede evaluarse en espacio constante (ver en este contexto también [13]). En consecuencia, el espacio puede reducirse arbitrariamente en la evaluación de polinomios si no se considera el tiempo.

Sin embargo, restringiéndose a procedimientos óptimos en tiempo se obtiene como consecuencia inmediata de los resultados de tradeoff demostrados en este capítulo el siguiente enunciado concerniente a cotas inferiores de espacio (comparar con el corolario 1):

Proposición 17 *Sean* $1 \leq i \leq 6$ *y* $\mathcal{F}_i := (F_d^{(i)})_{d \in \mathbf{N}}$ *cualquiera de las familias de polinomios* $F_d^{(i)} \in \mathbf{C}[X]$ *introducidas en los ejemplos 1, 2, 3, 4, 5. Entonces, existe una constante universal* $c > 0$ *con la siguiente propiedad: para cada sucesión* $(\beta_d)_{d \in \mathbf{N}}$ *de circuitos aritméticos en* $\mathbf{C}(X)$ *tal que* β_d *evalúa el polinomio* $F_d^{(i)}$ *en tiempo no escalar* $L(\beta_d) \leq \sqrt{d}$*, el espacio* $S(\beta_d)$ *utilizado por* β_d *satisface la cota inferior*

$$S(\beta_d) \geq c \cdot \frac{\sqrt[4]{d}}{\sqrt{\log_2 d}}.$$

Para el caso de la familia $\mathcal{F}_1$ *esta cota puede incluso mejorarse a*

$$S(\beta_d) \geq c \cdot \sqrt[4]{d}.$$

Capítulo 4

La complejidad intrínseca de la eliminación

La clasificación de un problema de acuerdo a la dificultad computacional de su resolución involucra dos disciplinas de carácter diferente. Una de ellas, la teoría de algoritmos, se ocupa de dar cotas *superiores* sobre la cantidad de recursos necesarios para resolver un problema dado.

La otra disciplina, conocida como teoría de la complejidad computacional, intenta demostrar que ciertos problemas no pueden ser resueltos eficientemente estableciendo para ello cotas *inferiores* sobre su complejidad computacional inherente.

En este capítulo se analizará la complejidad computacional de los problemas de eliminación desde el punto de vista del *tiempo secuencial*. Combinando este estudio con los resultados sobre el tradeoff espacio-tiempo obtenidos en el capítulo 3 se obtiene información sobre la complejidad computacional desde el punto de vista del espacio.

Usualmente los enunciados de cotas inferiores se entienden como resultados sobre cotas inferiores para un problema. Sin embargo, esto no es completamente cierto, ya que las cotas inferiores para un problema también dependen del aspecto sintáctico del mismo.

Esto se hace patente en el caso de los problemas de eliminación. Si se consideran los problemas de representación en un ideal polinomial con la codificación densa de los polinomios se tienen respuestas definitivas: no existen algoritmos polinomiales para los problemas de representación:

Teorema 20 *([126]) Dados $k, d \in \mathbb{N}, d \geq 5, n := 10k$, existen $n+1$ polinomios $P_1, \ldots, P_{n+1}$ en $\mathbb{Z}[X_1, \ldots, X_n]$ de grado acotado por d (en realidad, los polinomios P_i se construyen como la diferencia entre dos monomios), tales que $X_1 - X_n$ pertenece al ideal generado por $P_1, \ldots, P_{n+1}$ en $\mathbb{Q}[X_1, \ldots, X_n]$ y se verifica la siguiente condición:*

$$\text{si } X_1 - X_n := \sum_{i=1}^{n+1} g_i P_i \text{ entonces } max\{gr(g_i); 1 \leq i \leq n+1\} \geq (d-2)^{2^{k-1}}$$

La cota inferior se basa entonces en una estimación de la longitud de la salida: la cota de grado del enunciado del teorema 20 determina la longitud de un polinomio de salida en representación densa.

Este teorema dice que la codificación densa de polinomios hace que el problema de la representación en el caso de ideales arbitrarios resulte fuera del alcance de cualquier clase de complejidad tratable. Pueden hallarse cotas inferiores de orden similar con la representación densa de las salidas para el problema de la eliminación de cuantificadores sobre cuerpos algebraicamente cerrados o real cerrados de característica dada (ver [54], [66], [88], [182]) y la decisión en la teoría de los cuerpos algebraicamente cerrados ([63]).

Incluso si se considera el problema de la representación en el Nullstellensatz en representación densa, se tienen cotas inferiores exponenciales en tiempo. Varios autores (D. Lazard, T. Mora, W. Masser, P. Philippon entre otros) han encontrado el siguiente ejemplo :

Proposición 18 *Considérese el siguiente sistema de ecuaciones polinomiales sobre $\mathbb{Q}[X_1, \ldots, X_n]$:*

$$f_1 = X_1^d, \; f_2 = X_1 - X_2^d, \ldots, \; f_{n-1} = X_{n-2} - X_{n-1}^d, \; f_n = 1 - X_{n-1} X_n^{d-1} \tag{4.1}$$

Entonces son ciertas las siguientes afirmaciones:

- *el sistema definido en (4.1) no posee soluciones comunes en $\mathbf{C}^n$.*
- *toda representación $1 := \sum_{i=1}^n g_i f_i$ verifica que $gr(g_1) \geq d^n - d^{n-1}$.*

Dado que la cantidad de monomios del polinomio g_1 es de tipo exponencial $d^{O(n^2)} = (d^{O(n)})^n$ con respecto a la cantidad $d^{O(n)}$ de monomios de grado d en n variables, se concluye la cota inferior anunciada.

Cabe destacar que este resultado implica la optimalidad (salvo factores logarítmicos) de la versión probabilística del algoritmo desarrollado en la sección 1.4.4 con respecto al espacio y al tiempo secuencial.

A fin de evitar la notable simplificación de la cuestión de la complejidad computacional de los problemas de eliminación que se introduce cuando se consideran modelos con una fuerte estructura involucrada, se considerará la cuestión sobre un modelo más general: se codificarán los polinomios por medio de *programas* (=circuitos) aritméticos que los evalúen.

Es claro que cualquier cota inferior en este modelo se traslada inmediatamente a una cota inferior en representación densa (así como también en representación rala (sparse)), ya que la codificación de cualquier polinomio por medio de un programa es más económica que la representación densa del mismo (si bien en el caso genérico ambas representaciones poseen aproximadamente el mismo tamaño, en ciertos casos especiales -que eventualmente podrían ser los casos de los polinomios que aparecen como resultado de un proceso de eliminación- la diferencia puede ser importante).

4.1 Resultados de complejidad estructural

Un primer intento de clasificar la complejidad computacional de la resolución de un problema consiste en relacionarlo con clases de complejidad. De la existencia de teoremas de jerarquía de espacio y tiempo (cf. [7]) se deducen cotas inferiores para el problema considerado.

En tal sentido, la tarea de la *complejidad estructural* es establecer relaciones en términos de clases de complejidad. Para esto es necesario tener una herramienta que permita comparar la dificultad de dos problemas dados, la cual viene dada con el concepto de *reducibilidad.*

Una vez que se ha fijado algún tipo de reducción, se pueden definir los conceptos de dureza y completitud para miembros de una clase de complejidad: siendo $\mathcal{A}$ una clase de complejidad, se dice que un problema o lenguaje $\mathcal{P}$ es *$\mathcal{A}$-duro* si todo problema de la clase $\mathcal{A}$ es *reducible* $\mathcal{P}$, y $\mathcal{P}$ se dice *$\mathcal{A}$-completo* si es $\mathcal{A}$-duro y además pertenece a la clase $\mathcal{A}$.

En forma intuitiva se puede decir que los problemas $\mathcal{A}$-completos son aquellos miembros de la clase $\mathcal{A}$ de *máxima dificultad*, y que la resolución de un problema $\mathcal{A}$-duro ofrece al menos tanta dificultad como la de cualquier

otro problema de la clase $\mathcal{A}$. Si bien no es clara la existencia de problemas $\mathcal{A}$-completos para una clase $\mathcal{A}$ arbitraria, en el caso de las principales clases de complejidad ésta ha sido establecida por medio de la exhibición de ejemplos concretos.

Una observación obvia es la siguiente: dado un problema $\mathcal{P}$, si existe un problema $\tilde{\mathcal{P}}$ que es $\mathcal{A}$-duro o $\mathcal{A}$-completo y reducible a $\mathcal{P}$, entonces $\mathcal{P}$ es $\mathcal{A}$-duro. Por lo tanto, a fin de demostrar que la resolución de cierto problema ofrece tanta dificultad como la de cualquier miembro de una clase de complejidad $\mathcal{A}$ dada, es suficiente con demostrar que existe una problema $\mathcal{A}$-duro o $\mathcal{A}$-completo que es reducible a éste.

En lo que sigue se estudiarán distintos modelos de complejidad desde el punto de vista de la complejidad estructural. Se demostrará que los problemas de eliminación son "duros" en ciertas clases, reduciendo para ello problemas completos en esas clases a cuestiones de eliminación.

De esta manera, se aportarán indicios a la conjetura que la complejidad de los problemas de eliminación tiene un comportamiento inherente simplemente exponencial si la entrada se mide mediante parámetros sintácticos (como el grado o la talla de circuito de los polinomios de entrada, la altura de sus coeficientes o el número de variables).

4.1.1 Cotas inferiores relativas sobre modelos binarios

Para el primer indicio sobre la intratabilidad de los problemas de eliminación que se han considerado se utilizarán las herramientas que provee la teoría de la NP-completitud. La idea es demostrar que los problemas de eliminación son "al menos tan duros" como una larga lista de problemas de diferentes ámbitos, los cuales son ampliamente reconocidos como problemas probablemente intratables: los problemas NP-completos (cf. [71]).

Todos estos problemas poseen una característica común: pueden resolverse en forma polinomial, si se considera una variante mas "poderosa" que las máquinas de Turing determinísticas: las *máquinas de Turing no determinísticas.*

Una máquina de Turing no determinística M es un dispositivo de características similares a una máquina determinística excepto por el hecho que cada paso de computación puede elegirse entre varias posibilidades codifi-

cadas en la función de transición δ.

Por lo tanto, sobre cada entrada x no existe una sola computación sino un conjunto de posibles computaciones. En tal sentido, se dice que una entrada x es *aceptada* por M si y sólo si existe una computación de M sobre x que finaliza en un estado de aceptación.

El *tiempo* requerido por M sobre una entrada x se define como el mínimo, sobre todas las posibles computaciones aceptantes sobre x, del número de pasos de computación realizados. En estos términos se define la clase NP, como la clase de los problemas que pueden ser resueltos por una máquina de Turing no determinística en tiempo *polinomial*.

Dados dos lenguajes $L_1, L_2 \subseteq \Sigma^*$, se dice que L_1 es reducible (o polinomialmente reducible) a L_2 si existe una máquina de Turing de determinística que calcula en tiempo polinomial una función $f : \Sigma^* \to \Sigma^*$ con siguiente propiedad:

$$f(x) \in L_2 \text{ si y sólo si } x \in L_1$$

La clase de los problemas NP-completos se define en términos de esta reducción. El mérito de haber descubierto el concepto de la NP-completitud se debe a S. Cook, quien demostró que el siguiente problema, conocido como SAT, es NP-completo [49]:

Problema 1 *Dada una fórmula booleana Φ en las variables $X_1, \ldots, X_n$ libre de cuantificadores, decidir si Φ es satisfactible, es decir, si existe una asignación de valores booleanos*

$$\alpha : \{X_1, \ldots, X_n\} \longrightarrow \{0, 1\}$$

tal que $\Phi(\alpha(X_1), \ldots, \alpha(X_n)) = 1$.

Aquí se utilizará una variante de este problema, conocida como 3SAT, más fácil de manipular, cuya completitud en NP es conocida (ver [107]):

Problema 2 *Sea Φ una fórmula booleana en las variables $X_1, \ldots, X_n$ dada en forma 3-conjuntiva normal, es decir:*

$$\Phi = c_1 \wedge \cdots \wedge c_s$$

donde cada cláusula c_i es de la forma

$$c_i = u_{i_1} \vee u_{i_2} \vee u_{i_3}$$

siendo u_{i_j} una variable X_k o su negación $\overline{X_k}$. Decidir si Φ es satisfactible.

Se tienen ahora todas las herramientas necesarias para demostrar el primer resultado concerniente a la complejidad relativa de los procedimientos de eliminación. Se enuncia en primer lugar el problema de eliminación que se estudiará:

Problema 3 : El Problema de la Consistencia (PC) *Dada una sucesión finita de polinomios $F_1, \ldots, F_s$ en $\mathbb{Z}[X_1, \ldots, X_n]$, decidir si el siguiente sistema de ecuaciones polinomiales tiene una solución en $\mathbf{C}^n$:*

$$F_1(X_1, \ldots, X_n) = 0\,, \ \ldots\ , \ F_s(X_1, \ldots, X_n) = 0$$

La NP-dureza del problema PC es bien conocida en el ámbito de teoría de eliminación (ver [90], [138] por ejemplo). La demostración de este hecho se reproduce aquí por motivos didácticos:

Teorema 21 *PC es NP-duro.*

Demostración Siguiendo el esquema estándar de demostración de este tipo de enunciados, se exhibirá una reducción polinomial de 3SAT a PC. Para ello, sea $\Phi = c_1 \wedge \cdots \wedge c_s$ una fórmula booleana sin cuantificadores sobre las variables $\mathcal{U} := \{U_1, \ldots, U_n\}$.

A fin de definir la función f que realizará la reducción de 3SAT a PC, a cada variable $U_i \in \mathcal{U}$ se le asigna una indeterminada X_i sobre $\mathbf{C}$. A fin de simular un comportamiento "discreto" de las variables "continuas" $X_1, \ldots, X_n$, estas variables estarán sujetas a las condiciones:

$$(X_1)^2 - X_1 = 0, \ldots, (X_n)^2 - X_n = 0$$

que asegura que todos los posibles valores que toman $X_1, \ldots, X_n$ son los enteros 0 o 1.

Se construirá ahora un polinomio F_Φ en $\mathbb{Z}[X_1, \ldots, X_n]$ de forma tal que F_Φ posee una solución en $\{0,1\}^n$ si y sólo si la fórmula Φ es satisfactible. Cada cláusula c_i que aparece en Φ es de alguno de los siguientes tipos:

$$\begin{array}{c} X \vee Y \vee Z \\ X \vee Y \vee \overline{Z} \\ X \vee \overline{Y} \vee \overline{Z} \\ \overline{X} \vee \overline{Y} \vee \overline{Z} \end{array}$$

Para cada una de estas clásulas, se definen los siguientes polinomios:

$$\begin{gathered} X+Y+Z-XY-XZ-YZ+XYZ \\ 1-Z+XZ-XYZ \\ 1-YZ+XYZ \\ 1-XYZ \end{gathered} \tag{4.2}$$

Es fácil corroborar que los polinomios así definidos toman solamente los valores 0 o 1 sobre cada upla en el conjunto $\{0,1\}^3$, y toman el valor 1 sobre una tal upla si y sólo ésta corresponde a una asignación de valores booleanos a las variables X, Y, Z que satisface la cláusula en consideración. Por lo tanto, por cada cláusula c_i que aparece en Φ existe un polinomio $p_i(X_{i_1}, X_{i_2}, X_{i_3})$ de alguno de los tipos definidos en 4.2 que verifica las propiedades mencionadas.

En consecuencia, la compatibilidad del siguiente sistema de ecuaciones polinomiales con coeficientes enteros:

$$\begin{gathered} (X_1)^2 - X_1 = 0, \ldots, (X_n)^2 - X_n = 0 \\ F_\Phi := \prod_{i=1}^{s} p_i(X_{i_1}, X_{i_2}, X_{i_3}) - 1 = 0 \end{gathered} \tag{4.3}$$

es equivalente a la satisfactibilidad de la fórmula Φ. Nótese que los polinomios que definen el sistema (4.3) pueden calcularse por medio de $O(s)$ operaciones aritméticas.

Debido a la forma especial del sistema definido en (4.3) es claro que éste puede ser generado en tiempo polinomial a partir de la fórmula Φ. Dado que 3SAT es un problema NP-completo, se ha demostrado el enunciado del teorema. □

El siguiente resultado constituye una mejora con respecto a la NP-dureza de los problemas de eliminación: se demostrará que la hipótesis de la polinomialidad de los problemas de eliminación implica no sólo que P=NP, como se deduce del teorema 21, sino también que la clase #P, de complejidad presumiblemente superior a NP, también colapsa a P.

La clase #P, introducida por L. Valiant en [177], se describe en términos de las máquinas de Turing *contadoras*. Una máquina de Turing contadora es una máquina no determinística estándar que posee un dispositivo auxiliar que (mágicamente) imprime en notación binaria sobre una cinta especial

el número de computaciones aceptantes inducidas por la entrada. Una tal máquina tiene complejidad en tiempo $f(n)$ si la más larga computación aceptante inducida por el conjunto de todas las entradas de tamaño n toma $f(n)$ pasos de computación (cuando la máquina se mira como una máquina no determinística estándar sin dispositivo auxiliar).

La clase #P consiste de todas las funciones que pueden computarse por medio de máquinas de Turing contadoras en tiempo polinomial.

Se define una noción de reducción por medio de *oráculos*, en un sentido similar a la noción en [49]. Una *máquina de Turing con oráculo* es una que posee dos cintas especiales: una de consulta y una de respuesta. Para consultar al oráculo la máquina imprime una palabra sobre la cinta de consulta y, yendo a un estado especial de consulta, retorna una respuesta en una unidad de tiempo sobre la cinta de respuesta.

Con esta terminología, un problema L se dice #P–duro si todo problema #P puede calcularse en tiempo polinomial con una maáquina con oráculo L. Por supuesto, un problema #P–completo es uno que es #P–duro y pertenece a #P.

En [177] se demostró que el problema de calcular el *permanente* de una matriz $A \in \mathbb{Z}^{n\times n}$ es $\#P$–completo. El permanente de una matriz A en $\mathbb{Z}^{n\times n}$ se define en la forma

$$\text{Perm } A := \sum_{\sigma\in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

donde $a_{i,j}$ denota el coeficiente (i,j) de la matriz A y S_n denota el conjunto de todas las permutaciones de $(1,2,\ldots,n)$.

Se relacionará la dificultad de la resolución de los problemas de eliminación con la de los problemas #P–completos mediante una reducción al cálculo del permanente. El problema de eliminación que se utilizará a tal efecto es el siguiente:

Problema 4 : El problema general de eliminación (PGE) *Dados polinomios $F_1,\ldots,F_s$ en $\mathbb{Z}[X_1,\ldots,X_n]$, hallar una fórmula sin cuantificadores en el lenguaje de cuerpos algebraicamente cerrados que describa la siguiente proyección sobre $\mathbf{C}^r$ $(r \le n)$:*

$$(\exists X_{r+1})\cdots(\exists X_n)\{F_1(X_1,\ldots,X_n)=0,\ldots,F_s(X_1,\ldots,X_n)=0\}$$

Se tiene entonces el siguiente resultado, el cual es una versión mejorada de [90, Proposition 13]:

Teorema 22 *Si PGE es resoluble en tiempo polinomial entonces P=#P.*

Demostración La idea es mostrar que a partir de una instancia de PGE se obtiene el permanente de cualquier matriz $A \in \mathbb{Z}^{n\times n}$. Dado que el problema del cálculo del permanente de matrices enteras es #P-duro, se deducirá el enunciado del teorema.

Para esto, se considera la siguiente fórmula definida sobre las variables $X_{11},\ldots,X_{nn},Z_{11},\ldots,Z_{nn},T,Y$:

$$\begin{aligned}(\exists X_{11})\cdots(\exists X_{nn})\Big\{ & \bigwedge_{1\le i,j\le n}(X_{ij})^2 - X_{ij} = 0 \\ & \bigwedge_{i=1}^{n}\Big(\sum_{j=1}^{n} X_{ij} = 1\Big) \\ & \bigwedge_{j=1}^{n}\Big(\sum_{i=1}^{n} X_{ij} = 1\Big) \\ & Y = T\prod_{i=1}^{n}\Big(\sum_{j=1}^{n} X_{ij}Z_{ij}\Big)\Big\}\end{aligned} \tag{4.4}$$

En primer lugar, obsérvese que si las variables $X_{11},\ldots,X_{nn}$ se piensan como coordenadas de una matriz X de $n\times n$, las condiciones

$$\bigwedge_{1\le i,j\le n}(X_{ij})^2 - X_{ij} = 0\,,\ \bigwedge_{i=1}^{n}\Big(\sum_{j=1}^{n} X_{ij} = 1\Big)\,,\ \bigwedge_{j=1}^{n}\Big(\sum_{i=1}^{n} X_{ij} = 1\Big) \tag{4.5}$$

implican que la matriz X es una matriz de *permutación*: X sólo tiene 0 o 1 como entradas, y existe una permutación σ en S_n tal que $X_{ij} = 1$ si y sólo si $\sigma(i) = j$. Más aún, todas las posibles matrices definidas por las condiciones (4.5) corresponden exactamente a todas las permutaciones σ en S_n.

A fin de determinar que conjunto resulta de la proyección definida en (4.4), se reemplaza el polinomio:

$$Y = T\prod_{i=1}^{n}\Big(\sum_{j=1}^{n} X_{ij}Z_{ij}\Big)$$

(que es el único polinomio que aparece en (4.4) que no depende exclusivamente de $X_{11}, \ldots, X_{nn}$) por todos los posibles valores que pueden tomar las variables $X_{11}, \ldots, X_{nn}$ de acuerdo con las restricciones impuestas por la fórmula (4.4).

Así se obtienen $n!$ conjuntos, cuya unión constituye la proyección definida en (4.4):

$$\bigcup_{\sigma \in S_n} \left(Y - T \prod_{i=1}^{n} Z_{i,\sigma(i)} \right)$$

Esta unión se puede expresar en forma mas compacta por medio de los ceros del siguiente polinomio "eliminante":

$$G_n := \prod_{\sigma \in S_n} \left(Y - T \prod_{i=1}^{n} Z_{i,\sigma(i)} \right)$$

Se demostrará que el permanente de cualquier matriz $n \times n$ puede calcularse con un oráculo que resuelve la instancia del problema PGE definida por la fórmula (4.4). Por lo tanto, dado que esta fórmula tiene longitud $O(n^2)$ (y se calcula por medio de $O(n^2)$ operaciones aritméticas) se tienen las dos alternativas siguientes: o bien la instancia del problema PGE definida por la fórmula (4.4) no es resoluble en tiempo polinomial; o ésta si es resoluble en tiempo polinomial, lo cual implicará que el problema PGE es #P–duro, ya que se demostrará que la respuesta a la fórmula (4.4) puede utilizarse como oráculo para el cálculo del permanente. En ambos casos se deduce el enunciado del teorema.

A fin de demostrar como puede calcularse el permanente a partir del polinomio eliminante G_n, se observa qùe la escritura de G_n como polinomio en $\mathbb{Q}[T, Z_{11}, \ldots, Z_{nn}][Y]$ está dada por la siguiente expresión:

$$G_n = Y^{n!} + a_1 T Y^{n!-1} + a_2 T^2 Y_{+}^{n!-2} \cdots + a_0 T^{n!}$$

donde el coeficiente a_1 toma la forma:

$$a_1 = \sum_{\sigma \in S_n} \left(\prod_{i=1}^{n} Z_{i,\sigma(i)} \right) = Perm(Z_{ij})$$

Supóngase que G_n viene representado por un circuito aritmético sin divisiones β_n de talla L_n. Si no existe ningún circuito aritmético β_n que evalúe G_n en tiempo L_n polinomial, entonces se habrá demostrado que PGE es

intrínsecamente exponencial en cuyo caso el enunciado del teorema es cierto. En consecuencia, se puede suponer que L_n está acotado por un polinomio en n.

Aplicando el teorema de Baur-Strasen [10] (ver también [131]), es posible transformar en tiempo polinomial en n el circuito β_n en uno $\tilde{\beta}_n$ que calcula la derivada $\frac{\partial G_n}{\partial T}$. Dado que este polinomio tiene la forma:

$$\frac{\partial G_n}{\partial T} = a_1 Y^{n!-1} + 2a_2 T Y_+^{n!-2} \cdots + n! a_0 T^{n!}$$

especializando Y en 1 y T en 0, se obtiene el coeficiente a_1, es decir, el permanente $\mathrm{Perm}\big((Z_{ij})_{1\leq i,j\leq n}\big)$. Por lo tanto, PGE es #P-duro, de donde se deduce que un algoritmo polinomial para su resolución implica uno polinomial para la resolución de cualquier problema #P. En consecuencia, se tiene que P=#P. □

4.1.2 Cotas inferiores relativas sobre modelos aritméticos

En esta subsección se considerarán los problemas de eliminación sobre el modelo aritmético introducido por L. Valiant en [176] (ver también [178], [73]), el cual constituye un análogo aritmético de la teoría booleana de P versus NP, que se pone en términos de las clases de familias de polinomios p-computables versus p-definibles.

En la teoría de Valiant, los polinomios se evalúan (y representan) por medio de circuitos aritméticos, de los cuales sólo se considera su talla de circuito como medida de complejidad. Dado que los circuitos aceptan solamente un número fijo de entradas, es natural considerar *familias* de circuitos como modelo de computación.

El objeto de estudio son las *familias* $\mathcal{F} = (F_n)_{n\in\mathbb{N}}$ de polinomios de *grado polinomial en n* con coeficientes en un cuerpo (que aquí se restringirá a $\mathbb{Q}$), en una *cantidad polinomial de variables.* Es decir, cada polinomio F_n de la familia $\mathcal{F}$ pertenece a $\mathbb{Q}[X_1, \ldots, X_{v(n)}]$, donde $v(n)$ es una función acotada en forma polinomial con respecto a n y tiene grado total polinomial en n.

Se dice que una función $t : \mathbb{N} \to \mathbb{N}$ es p-acotada ("polinomialmente acotada") si existen constantes c_1, c_2 tales que $t(n) \leq c_1 n^{c_2}$ y qp-acotada ("cuasi-polinomialmente acotada") si existen constantes c_1, c_2 tales que $t(n) \leq c_1 2^{(\log n)^{c_2}}$.

Las clases centrales –los análogos aritméticos de P y NP– son las formadas por las familias de polinomios *p–computables* y *p–definibles.*

Una familia $\mathcal{F} = (F_n)_{n\in\mathbb{N}}$ de polinomios con $F_n \in \mathbb{Q}[X_1, \ldots, X_{v(n)}]$ es p–computable si $v(n)$ y $gr(F_n)$ son funciones p–acotadas y la función $L(F_n)$ que mide la talla del polinomio F_n es p–acotada. Estas familias son consideradas "factibles", es decir, el análogo aritmético de la clase P.

La definición de la clase de las familias p–definibles involucra algunos conceptos técnicos previos. En primer lugar, una familia $\mathcal{F} = (F_n)_{n\in\mathbb{N}}$ se dice p–expresable si $v(n)$ y $gr(F_n)$ son funciones p–acotadas y la función $E(F_n)$ que mide el *tamaño de fórmula* de F_n es también p–acotada.

Las reducciones se establecen por medio de las *p–proyecciones.* Un polinomio $F \in \mathbb{Q}[X_1, \ldots, X_n]$ es una *proyección* de $G \in \mathbb{Q}[X_1, \ldots, X_m]$, si existen $a_1, \ldots, a_m \in \mathbb{Q} \cup \{X_1, \ldots, X_n\}$ tales que

$$F = G(a_1, \ldots, a_m)$$

Dadas dos familias $\mathcal{F} = (F_n)_{n\in\mathbb{N}}$ y $\mathcal{G} = (G_n)_{n\in\mathbb{N}}$ de polinomios sobre $\mathbb{Q}$, con $F_n \in \mathbb{Q}[X_1, \ldots, X_{v(n)}]$ y $G_m \in \mathbb{Q}[X_1, \ldots, X_{w(m)}]$, y una función $t : \mathbb{N} \to \mathbb{N}$, se dice $\mathcal{F}$ es una t–proyección de $\mathcal{G}$ si, para todo $n \in \mathbb{N}$, existe $m \leq t(n)$ tal que tal que $v(n), w(m) \leq t(n)$ y F_n es una proyección de G_m.

Finalmente, siendo $\mathcal{F}$ y $\mathcal{G}$ familias como antes, se dice que $\mathcal{F}$ es una p–proyección de $\mathcal{G}$ si $\mathcal{F}$ es una t–proyección de $\mathcal{G}$ para alguna función t que es p–acotada.

En estos términos se puede definir el concepto de p–definabilidad: si $\mathcal{G} = (G_n)_{n\in\mathbb{N}}$ y $\mathcal{H} = (H_n)_{n\in\mathbb{N}}$ son dos familias de polinomios sobre $\mathbb{Q}$, entonces $\mathcal{G}$ *define* a $\mathcal{H}$ si para todo $n \in \mathbb{N}$ se tiene

$$H_n = \sum_{e\in\{0,1\}^n} G_n(e)X^e$$

donde X^e denota el monomio $X_1^{e_1} \cdots X_n^{e_n}$. Una familia $\mathcal{F}$ de polinomios sobre $\mathbb{Q}$ es p–definible si existe una familia p–expresable $\mathcal{G}$ sobre $\mathbb{Q}$ tal que $\mathcal{F}$ es una p–proyección de la familia $\mathcal{H}$ definida por $\mathcal{G}$.

Las familias p–definibles son el análogo aritmético de NP. Los miembros mas difíciles de esta clase, bajo el concepto de p–proyección, se denominan las familias *p–completas.* La *Hipótesis de Valiant* afirma que existen familias de polinomios p–definibles sobre $\mathbb{Q}$ que no son p–computables. Claro está, la hipótesis de Valiant es cierta si y sólo si existe una familia p–completa que no es p–computable.

A fin de aportar mas evidencia sobre la intratabilidad de los problemas de eliminación, se demostrará que cualquier familia de polinomios p-completa es la p-proyección del resultado de un proceso de eliminación del tipo PGE:

Teorema 23 *El problema de eliminación PGE es resoluble en tiempo (=cantidad de operaciones aritméticas) polinomial si y sólo si la hipótesis de Valiant es falsa.*

Demostración La prueba del enunciado del teorema se basa en demostrar que es posible obtener cualquier polinomio de la forma

$$H = \sum_{e \in \{0,1\}^n} G(e) X^e$$

donde G es un polinomio cualquiera, como el resultado de un proceso de eliminación del tipo PGE aplicadó a un sistema de ecuaciones polinomiales que se calcula con $O\big(n + L(G)\big)$ operaciones aritméticas, donde $L(G)$ denota la talla de circuito del polinomio G.

Para esto, siendo G un polinomio computable por medio de un circuito aritmético de talla L, se considera la siguiente fórmula Φ_G:

$$(\exists X_1)\cdots(\exists X_n)\Big\{ \bigwedge_{i=1}^{n}(X_i)^2 - X_i = 0, Y = TG(X_1,\ldots,X_n)\prod_{i=1}^{n}\big(1 + X_i(Z_i - 1)\big)\Big\} \tag{4.6}$$

Obsérvese que todos los polinomios que forman la fórmula Φ_G pueden calcularse por medio de un circuito aritmético de talla $O(n + L)$. A fin de hallar un polinomio eliminante para Φ_G, se utilizará la técnica aplicada en el teorema 22.

En primer lugar, se observa que las condiciones

$$\bigwedge_{i=1}^{n}(X_i)^2 - X_i = 0$$

implican que el vector de variables $(X_1,\ldots,X_n)$ toma exactamente todos los posibles valores del conjunto $\{0,1\}^n$. Reemplazando cada uno de estos valores en el polinomio

$$Y = TG(X_1,\ldots,X_n)\prod_{i=1}^{n}\big(1 + X_i(Z_i - 1)\big)$$

se obtienen 2^n conjuntos, cuya unión constituye el conjunto resultante del proceso de eliminación PGE aplicado a la fórmula (4.6). Esta unión puede expresarse como el conjunto de ceros del siguiente polinomio:

$$Q := \prod_{(\varepsilon_1,\ldots,\varepsilon_n)\in\{0,1\}^n} \left(Y - TG(\varepsilon_1,\ldots,\varepsilon_n)Z_1^{\varepsilon_1}\cdots Z_n^{\varepsilon_n}\right)$$

La escritura del polinomio Q con respecto a la variable Y tiene la siguiente forma:

$$Q = Y^{n!} + a_1 TY^{n!-1} + a_2 T^2 Y^{n!-2} + \cdots + a_0 T^{n!}$$

donde el coeficiente a_1 viene dado por la expresión:

$$a_1 = \sum_{(\varepsilon_1,\ldots,\varepsilon_n)\in\{0,1\}^n} G(\varepsilon_1,\ldots,\varepsilon_n)Z_1^{\varepsilon_1}\cdots Z_n^{\varepsilon_n}$$

Si no existe ningún circuito aritmético que evalúe Q en tiempo L polinomial en n, entonces se deduce que no existen algoritmos polinomiales para PGE, lo cual implica el enunciado del teorema. En consecuencia, se puede suponer que la evaluación del polinomio Q puede realizarse por medio de un circuito aritmético β de talla polinomial en n y L.

Aplicando nuevamente el teorema de Baur-Strasen [10] se transforma el circuito β en uno $\tilde{\beta}$ que calcula el polinomio $\frac{\partial Q}{\partial T}$. Dado que este polinomio tiene la forma:

$$\frac{\partial Q}{\partial T} = a_1 Y^{n!-1} + 2a_2 TY_+^{n!-2}\cdots + n!a_0 T^{n!}$$

se concluye que, especializando Y en 1 y T en 0, se obtiene el coeficiente a_1, es decir, el polinomio

$$\sum_{(\varepsilon_1,\ldots,\varepsilon_n)\in\{0,1\}^n} G(\varepsilon_1,\ldots,\varepsilon_n)Z_1^{\varepsilon_1}\cdots Z_n^{\varepsilon_n}$$

Considérese entonces una familia $\mathcal{F} := (F_n)_{n\in\mathbf{N}}$ de polinomios sobre $\mathbb{Q}$ p-completa. Sin pérdida de generalidad, puede suponerse directamente que la familia $\mathcal{F}$ está p-definida por medio de una familia $\mathcal{G} := (G_n)_{n\in\mathbf{N}}$ que es p-expresable (y por lo tanto, p-computable).

En consecuencia, en virtud de la hipótesis de la polinomialidad del problema PGE, dado que la familia de polinomios que conforman la familia de

fórmulas $\{\Phi_{G_n}\}$ definidas según (4.6) es p–computables, se concluye que la familia de polinomios eliminantes

$$F_n = \sum_{(\epsilon_1,\ldots,\epsilon_n)\in\{0,1\}^n} G_n(\epsilon_1,\ldots,\epsilon_n) Z_1^{\epsilon_1}\cdots Z_n^{\epsilon_n}$$

es p–computable.

Luego, dado que la familia $\mathcal{F}$ es p–completa, se tiene que la hipótesis de Valiant es falsa, lo que concluye la demostración del teorema. □

Cabe destacar el modelo aritmético de las máquinas *reales* introducido por L. Blum, M. Shub y S. Smale ([21]), el cual realiza un desarrollo análogo de la teoría booleana P versus NP por medio de las clases $\mathrm{P}_{\mathbf{C}}$ y $\mathrm{NP}_{\mathbf{C}}$. En [21] se demuestra que PC es un problema $\mathrm{NP}_{\mathbf{C}}$–completo, lo cual avala la conjetura sobre la intratabilidad de los problemas de eliminación (ver también [165]).

4.2 Resultados de complejidad absoluta

En esta sección se darán argumentos *absolutos* a favor de la hipótesis de la intratabilidad de los problemas de eliminación, es decir, argumentos que *no dependen de la supuesta intratabilidad de alguna clase de complejidad.*

Desafortunadamente, estos argumentos requieren ciertas hipótesis sobre el tipo de algoritmos que se utilizan en la resolución de los problemas de eliminación. Sin embargo, los resultados que se demostrarán en esta sección tendrán un gran impacto desde el punto de vista práctico –al menos en la opinión del autor– ya que las hipótesis necesarias son aplicables a *todos los algoritmos hasta ahora conocidos y posibles variantes de los mismos.*

Como se puede apreciar del contenido de la sección anterior, existen varias propuestas diferentes para modelar el concepto de algoritmo. Cada modelo posee clases de problemas "probablemente intratables" de gran interés práctico, cuya conjeturada intratabilidad no ha sido demostrada en forma concluyente.

Es posible que este fenómeno se deba a la generalidad con que se aborda la palabra "algoritmo". De esta manera, se incluyen en esta categoría procedimientos que muy probablemente no serán jamás implementados (o siquiera imaginados!).

La intención de esta sección es *pragmática*: no se pretende dar un cota inferior para la cantidad de operaciones que realiza cualquier posible algoritmo de eliminación, sino mas bien sobre el tipo de algoritmos que se ha desarrollado hasta ahora. La conclusión que debería extraerse es: "no es posible desarrollar algoritmos polinomiales generalistas para resolver los problemas de eliminación con este tipo de técnicas".

Es por tanto necesario encontrar un modelo general de algoritmo que incluya a todos los hasta ahora desarrollados y todas las posibles variantes de los mismos. Para este fin, se introduce el concepto de *robustez algebraica*. Informalmente, un procedimiento general de eliminación se dice algebraicamente robusto si, para familias *playas* de instancias de problemas, produce soluciones *continuas* o *estables* (en un cierto sentido a precisar).

Por supuesto, esta noción de robustez algebraica depende del contexto (algebraico o geométrico). Si bien no se dará una definición general de este concepto, la idea se explicará en la siguiente subsección en un ejemplo típico.

4.2.1 Familias playas de problemas de eliminación

Sean $T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n, Y$ indeterminadas sobre $\mathbf{C}$ y sean $G_1, \ldots, G_n, F$ polinomios que pertenecen a $\mathbb{Q}[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n]$. Supóngase que los polinomios $G_1, \ldots, G_n$ forman una sucesión regular en $\mathbb{Q}[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n]$, y definen una variedad (equidimensional)

$$V := \{G_1 = 0, \ldots, G_n = 0\}$$

de $\mathbf{C}^{m+r+n}$ de dimensión $m + r$, cuyo grado (afín) se nota por δ. Supóngase asimismo que las variables $T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n$ están en posición de Noether con respecto a V, y denótese por $\pi : V \longrightarrow \mathbf{C}^{m+r}$ el morfismo de variedades algebraicas definido por

$$\pi(t_1, \ldots, t_m, u_1, \ldots, u_r, x_1, \ldots, x_n) := (t_1, \ldots, t_m, u_1, \ldots, u_r)$$

para todo $(t_1, \ldots, t_m, u_1, \ldots, u_r, x_1, \ldots, x_n) \in V$. Este morfismo π es finito y genéricamente no ramificado, lo cual implica, en particular, que π es *playo*.

Sea $\tilde{\pi} : V \longrightarrow \mathbf{C}^{m+r+1}$ el morfismo definido por

$$\tilde{\pi}(z) := \big(\pi(z), F(z)\big)$$

para todo $z \in V$. La imagen de $\tilde{\pi}$ es una hipersuperficie de $\mathbf{C}^{m+r+1}$ cuya ecuación minimal es un polinomio $P \in \mathbb{Q}[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$. Obsérvese que P es mónico en Y y que $gr_Y(P) \leq \delta$. Más aún, $gr_Y(P)$ es el cardinal de la imagen de la restricción de F al conjunto $\{w\} \times \pi^{-1}\{w\}$ definido por un punto $w \in \mathbf{C}^{m+r}$ genérico.

Considérese un punto arbitrario $t = (t_1, \ldots, t_m)$ de $\mathbf{C}^m$. Para polinomios $B \in \mathbb{Q}[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n]$ y $C \in \mathbb{Q}[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$ arbitrarios se nota:

$$B^{(t)} := B(t_1, \ldots, t_m, U_1, \ldots, U_r, X_1, \ldots, X_n)$$

y

$$C^{(t)} := C(t_1, \ldots, t_m, U_1, \ldots, U_r, Y)$$

Los polinomios $G_1^{(t)}, \ldots, G_n^{(t)}$ forman una sucesión regular en $\mathbb{Q}(t_1, \ldots, t_m)[U_1, \ldots, U_r, X_1, \ldots, X_n]$ y definen una variedad equidimensional

$$V^{(t)} := \{G_1^{(t)} = 0, \ldots, G_n^{(t)} = 0\}$$

de $\mathbf{C}^{r+n}$ cuyo grado está acotado por δ. Sean

$$\pi^{(t)} : V^{(t)} \longrightarrow \mathbf{C}^{r+n}$$

$$\tilde{\pi}^{(t)} : V^{(t)} \longrightarrow \mathbf{C}^{r+n+1}$$

los morfismos inducidos por π y $\tilde{\pi}$ sobre la variedad $V^{(t)}$. Entonces el morfismo $\pi^{(t)}$ es finito y playo pero no necesariamente genéricamente no ramificado. Mas aún, la imagen de $\tilde{\pi}^{(t)}$ es una hipersuperficie de $\mathbf{C}^{r+1}$ sobre la cual se anula el polinomio $P^{(t)}$ (sin ser necesariamente la ecuación minimal de esta superficie).

Definición 9 *El sistema de ecuaciones $G_1 = 0, \ldots, G_n = 0$ y el polinomio F se llaman (la instancia general de)* **una familia playa** *del problema de eliminación m-dimensional dependiente de los parámetros $T_1, \ldots, T_m$. El polinomio P se dice la* **solución general** *del problema de eliminación dado.*

Cada elemento t de $\mathbf{C}^m$ se considera como un punto paramétrico que determina una instancia particular del problema de eliminación dado. Esta instancia está entonces definida por los siguientes ítems:

- las ecuaciones $G_1^{(t)} = 0, \ldots, G_n^{(t)} = 0$
- el polinomio $F^{(t)}$

y su solución (particular) es $P^{(t)}$.

Dos puntos paramétricos $t, t' \in \mathbf{C}^m$ se dicen *equivalentes* (y se nota $t \sim t'$) si satisfacen las identidades:

$$G_1^{(t)} = G_1^{(t')}, \ldots, G_n^{(t)} = G_n^{(t')}, F^{(t)} = F^{(t')}$$

Obsérvese que $t \sim t'$ implica que $P^{(t)} = P^{(t')}$.

Asimismo, polinomios $A \in \mathbb{Q}[T_1, \ldots, T_m]$, $B \in \mathbb{Q}[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_m]$ y $C \in \mathbb{Q}[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$ se denominan *invariantes* (con respecto a $\sim$) si para todo par de puntos paramétricos $t, t' \in \mathbf{C}^m$ tales que $t \sim t'$, se satisfacen las identidades $A(t) = A(t')$, $B^{(t)} = B^{(t')}$ y $C^{(t)} = C^{(t')}$.

Sean β y β' circuitos aritméticos en $\mathbb{Q}[T_1, \ldots, T_m, U_1, \ldots, U_r, X_1, \ldots, X_n]$ y $\mathbb{Q}[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$ respectivamente, con parámetros pertenecientes al anillos de polinomios $\mathbb{Q}[T_1, \ldots, T_m]$. Los circuitos aritméticos β y β' se dicen *invariantes* (con respecto a $\sim$) si todos sus parámetros son elementos invariantes de $\mathbb{Q}[T_1, \ldots, T_m]$. Obsérvese que los resultados intermedios de un circuito aritmético invariante son polinomios invariantes.

Se tienen ahora todos los elementos necesarios para caracterizar, en la situación dada, el significado de un procedimiento de eliminación algebraicamente robusto.

Definición 10 *Supóngase que los polinomios $G_1, \ldots, G_n, F$ se dan por medio de un circuito aritmético (típicamente invariante) β en $\mathbb{Q}[T_1, \ldots, T_m][U_1, \ldots, U_r, X_1, \ldots, X_n]$. Un procedimiento de eliminación se dice* **algebraicamente robusto** *si produce, a partir del circuito aritmético β como entrada, un circuito aritmético Γ* **invariante** *en $\mathbb{Q}[T_1, \ldots, T_m, U_1, \ldots, U_r, Y]$ como salida tal que Γ representa el polinomio P.*

El requerimiento de invariancia en esta definición de robustez algebraica tiene el siguiente significado: sea $t = (t_1, \ldots, t_m)$ un punto paramétrico de $\mathbf{C}^m$ y sea $\Gamma^{(t)}$ el circuito aritmético en $\mathbb{Q}(t_1, \ldots, t_m)[U_1, \ldots, U_r, Y]$ obtenido a partir de Γ por medio de la evaluación en t de los elementos de $\mathbb{Q}[T_1, \ldots, T_m]$ que aparecen como parámetros de Γ. Entonces el circuito $\Gamma^{(t)}$ depende solamente de la instancia particular del problema determinado por el punto paramétrico t y no de t en sí mismo. Dicho de otra manera, un procedimiento

de eliminación algebraicamente robusto produce la solución de una instancia particular del problema de forma independiente de los posibles diferentes puntos paramétricos que definen la misma instancia del problema dado.

Obsérvese que por definición un procedimiento de eliminación algebraicamente robusto produce siempre la solución general del problema de eliminación en consideración.

Habiendo definido el concepto de robustez algebraica, se demostrará que cualquier procedimiento general de eliminación algebraicamente robusto tiene una complejidad intrínsecamente no polinomial con respecto al tamaño de la entrada, si ésta se mide solamente por medio de parámetros sintácticos. Para esto, se considera la siguiente familia playa de problemas de eliminación 1-dimensional.

Ejemplo 6 *Sean $S, T, U, X_1, \ldots, X_n, Y$ indeterminadas sobre $\mathbb{Q}$. Sea $\mathcal{F}$ la familia playa de problemas de eliminación 1-dimensional dependiente de los parámetros S y T, definida por los siguientes polinomios:*

$$G_1 := (X_1)^2 - X_1, \ldots, G_n := (X_n)^2 - X_n$$

$$F := \left(1 + S \prod_{i=1}^{n} \left(T^{2^{i-1}} + \left(\sum_{j=1}^{n} 2^{j-1} X_j\right)^{2^{i-1}}\right)\right) \prod_{k=1}^{n} \left((U^{2^{k-1}} - 1)X_k + 1\right)$$

Estos polinomios se consideran como elementos de anillo de polinomios $\mathbb{Q}[S,T][U, X_1, \ldots, X_n]$. En consecuencia, se tiene que $m = 2$ y $r = 1$ en esta situación.

Es claro a partir de su representación que los polinomios $G_1, \ldots, G_n, F$ pueden evaluarse por medio de un circuito aritmético β en $\mathbb{Q}[S, T, U, X_1, \ldots, X_n]$ de longitud $O(n)$. La variedad $V := \{G_1 = 0, \ldots, G_n = 0\}$ es la unión de 2^n subespacios afines lineales de $\mathbf{C}^{n+3}$: $V = \mathbf{C}^3 \times \{0,1\}^n$. El morfismo $\pi : V \longrightarrow \mathbf{C}^3$ es la proyección canónica de $\mathbf{C}^4 \times \{0,1\}^n$ en $\mathbf{C}^4$. Obviamente el morfismo π es finito y genéricamente no ramificado. Más aún, todas las fibras de π tienen cardinal 2^n.

Con estas notaciones se tiene el siguiente resultado:

Teorema 24 *Todo procedimiento general de eliminación algebraicamente robusto aplicado a la familia $\mathcal{F}$ de problemas del ejemplo 6 produce un circuito invariante solución cuya talla es de tipo $2^{\Omega(n)}$.*

Demostración. Sea $(\ell_1, \ldots, \ell_n)$ un punto de $\{0,1\}^n$ y sea $\ell := \sum_{j=1}^{n} 2^{j-1}\ell_j$ el número entero con representación binaria $\ell_n \ell_{n-1} \ldots \ell_1$. Se verifica inmediatamente que vale la siguiente identidad:

$$F(S,T,U,\ell_1,\ldots,\ell_n) := \Big(1 + S\sum_{k=0}^{2^n-1} T^k \ell^{2^n-1-k}\Big)U^\ell$$

En consecuencia, para cualquier punto $(s,t,u,\ell_1,\ldots,\ell_n) \in V$ con $\ell := \sum_{j=1}^{n} 2^{j-1}\ell_j$ se tiene:

$$F(s,t,u,\ell_1,\ldots,\ell_n) := \Big(1 + s\sum_{k=0}^{2^n-1} t^k \ell^{2^n-1-k}\Big)u^\ell$$

A partir de esta consideración se deduce fácilmente que el polinomio de eliminación $P \in \mathbb{Q}[S,T,U,Y]$ requerido es

$$P := \prod_{\ell=0}^{2^n-1} \Big(Y - \Big(1 + S\sum_{k=0}^{2^n-1} T^k \ell^{2^n-1-k}\Big)U^\ell\Big)$$

Este polinomio puede expresarse en la forma:

$$P := Y^{2^n} + a_1(S,T,U)Y^{2^n-1} + \cdots + a_{2^n}(S,T,U)$$

donde cada $a_i \in \mathbb{Q}[S,T,U]$ y a_1 es el siguiente polinomio:

$$a_1 := -\sum_{\ell=0}^{2^n-1} \Big(1 + S\sum_{k=0}^{2^n-1} T^k \ell^{2^n-1-k}\Big)U^\ell$$

Supóngase dado un procedimiento de eliminación algebraicamente robusto, el cual produce a partir del circuito aritmético de entrada β un circuito aritmético invariante Γ en $\mathbb{Q}[S,T,U,Y]$ que evalúa el polinomio P. Recuérdese que la invariancia de Γ significa que los parámetros de Γ son polinomios invariantes $A_1, \ldots, A_N$ de $\mathbb{Q}[S,T]$.

Sea $\mathcal{L}(\Gamma)$ la talla de Γ y $L(\Gamma)$ la talla no escalar de Γ con respecto a $\mathbb{Q}[S,T]$. Se tiene entonces que $L(\Gamma) \leq \mathcal{L}(\Gamma)$ y $N \leq \big(L(\Gamma)+3\big)^2$ (ver [171] o [161] por ejemplo). Sean $\Omega_1, \ldots, \Omega_N$ nuevas indeterminadas. De la estructura del grafo del circuito Γ se deduce que, para cada $0 \leq \ell < 2^n$, existe un

polinomio $Q_\ell \in \mathbb{Z}[\Omega_1, \ldots, \Omega_N]$ tal que $Q(A_1, \ldots, A_N)$ es el coeficiente del monomio $U^\ell Y^{2^n-1}$ de P, es decir:

$$Q_\ell(A_1, \ldots, A_N) = 1 + S \sum_{k=0}^{2^n-1} T^k \ell^{2^n-1-k}$$

para $\ell = 0, \ldots, 2^n - 1$.

Obsérvese que para todo par de puntos $t \sim t'$ se verifica la relación $(0, t) \sim (0, t')$. A partir de la invariancia de $A_1, \ldots, A_N$ se deduce que

$$A_1(0,t) = A_1(0,t'), \ldots, A_N(0,t) = A_N(0,t')$$

Esto significa que los elementos

$$\alpha_1 := A_1(0,T), \ldots, \alpha_N := A_N(0,T) \tag{4.7}$$

son valores constantes de $\mathbb{Q}$.

Se consideran los siguientes morfismos de espacios afines:

$$\begin{array}{rcl} \psi : \mathbf{C}^N & \longrightarrow & \mathbf{C}^{2^n} \\ (\Omega_1, \ldots, \Omega_n) & \longmapsto & \Big(Q_\ell(\Omega_1, \ldots, \Omega_n)\Big)_{0 \le \ell \le 2^n-1} \end{array}$$

$$\begin{array}{rcl} \mu : \mathbf{C}^2 & \longrightarrow & \mathbf{C}^N \\ (S,T) & \longmapsto & \Big(A_1(S,T), \ldots, A_N(S,T)\Big) \end{array}$$

Obsérvese que

$$\begin{array}{rcl} \psi \circ \mu(S,T) & = & \Big(Q_\ell\Big(A_1(S,T), \ldots, A_N(S,T)\Big)\Big)_{0 \le \ell \le 2^n-1} = \\ & = & (1 + S \sum_{k=0}^{2^n-1} T^k \ell^{2^n-1-k})_{0 \le \ell \le 2^n-1} \end{array}$$

Sea $\alpha := (\alpha_1, \ldots, \alpha_N)$ el punto de CC^N cuyas coordenadas son las definidas en 4.7 y $\varepsilon := (1, \ldots, 1) \in \mathbf{C}^{2^n}$. A partir de la argumentación previamente desarrollada se deducen las identidades:

$$\begin{array}{rcl} (\psi \circ \mu)(0,T) & = & \Big(Q_\ell\Big(A_1(0,T), \ldots, A_N(0,T)\Big)\Big)_{0 \le \ell \le 2^n-1} = \\ & = & \Big(Q_\ell(\alpha_1, \ldots, \alpha_N)\Big)_{0 \le \ell \le 2^n-1} = \\ & = & \Big(Q_\ell(\alpha)\Big)_{0 \le \ell \le 2^n-1} = (1, \ldots, 1) = \varepsilon \end{array}$$

En particular se tiene que $\psi(\alpha) = \epsilon$.

Se analiza ahora el morfismo ψ localmente en el punto $\alpha \in \mathbf{C}^N$. Sean $\mathcal{T}_\alpha$ y $\mathcal{T}_\epsilon$ los espacios tangentes de los puntos α y ε de los espacios afines $\mathbf{C}^N$ y $\mathbf{C}^2$ respectivamente. Se denota por $(\mathcal{D}_\psi)_\alpha : \mathcal{T}_\alpha \longrightarrow \mathcal{T}_\epsilon$ el diferencial del morfismo ϕ en el punto α. Tomando las proyecciones canónicas de $\mathbf{C}^N$ y $\mathbf{C}^{2^n}$ como coordenadas locales en los puntos α y ε respectivamente, se identifica $\mathcal{T}_\alpha$ con $\mathbf{C}^N$ y $\mathcal{T}_\epsilon$ con $\mathbf{C}^{2^n}$. Para todo $t \in \mathbf{C}^1$, se consideran las siguientes curvas paramétricas:

$$\begin{aligned} \gamma_t : \mathbf{C} &\longrightarrow \mathbf{C}^N \\ S &\longmapsto \big(A_1(S,t), \ldots, A_N(S,t)\big) \end{aligned}$$

$$\begin{aligned} \delta_t : \mathbf{C} &\longrightarrow \mathbf{C}^{2^n} \\ S &\longmapsto (1 + S\textstyle\sum_{k=0}^{2^n-1} t^k \ell^{2^n-1-k})_{0\le \ell 2^n-1} \end{aligned}$$

Obsérvese que $\psi \circ \gamma_t = \delta_t$ y vale que —independientemente del valor de t— $\gamma_t(0) = \alpha$ y $\delta_t(0) = \varepsilon$.

Para $t \in \mathbf{C}$ fijo, los vectores tangentes a las curvas γ_t y δ_t en $S = 0$ tienen la forma:

$$\gamma_t'(0) = \big(\frac{\partial A_1}{\partial S}(0,t), \ldots, \frac{\partial A_N}{\partial S}(0,t)\big)$$

$$\delta_t'(0) = (\sum_{k=0}^{2^n-1} t^k \ell^{2^n-1-k})_{0\le \ell \le 2^n-1}$$

Es claro que $\gamma_t'(0) \in \mathcal{T}_\alpha$ y $\delta_t'(0) \in \mathcal{T}_\epsilon$. Más aún, dado que $\psi \circ \gamma_t = \delta_t$ se tiene que

$$(\mathcal{D}_\psi)_\alpha\big(\gamma_t'(0)\big) = \delta_t'(0) = (\sum_{k=0}^{2^n-1} t^k \ell^{2^n-1-k})_{0\le \ell \le 2^n-1}$$

Eligiendo 2^n puntos diferentes $t_0, \ldots, t_{2^n-1}$ de $\mathbf{C}$ se obtienen 2^n vectores tangentes de $\mathcal{T}_\alpha$:

$$\omega_0 := \gamma_{t_0}'(0), \ldots, \omega_{2^n-1} := \gamma_{t_{2^n-1}}'(0)$$

Obsérvese que la matriz M de tamaño $2^n \times 2^n$ cuyas filas son los vectores

$$(\mathcal{D}_\psi)_\alpha(\omega_0), \ldots, (\mathcal{D}_\psi)_\alpha(\omega_{2^n-1})$$

tiene la forma

$$M = (t_h^{2^n-1-p})_{0\leq h,p\leq 2^n-1} \cdot (\ell^q)_{0\leq \ell,q\leq 2^n-1}$$

Luego, M es no singular ya que es el producto de dos matrices Vandermonde no singulares. Esto significa que los vectores tangentes $(\mathcal{D}_\psi)_\alpha(\omega_0), \ldots, (\mathcal{D}_\psi)_\alpha(\omega_{2^n-1})$ de $\mathcal{T}_\epsilon$ son linealmente independientes sobre $\mathbf{C}$. Por lo tanto, los vectores tangentes $\omega_0, \ldots, \omega_{2^n-1}$ de $\mathcal{T}_\alpha$ deben ser también $\mathbf{C}$-linealmente independientes. En consecuencia, se tiene que $2^n \leq dim\, \mathcal{T}_\alpha = N$, lo cual implica que $2^n \leq N \leq (L+3)^2$, de donde se deduce la estimación $2^{\frac{n}{2}} - 4 \leq L(\Gamma) \leq \mathcal{L}(\Gamma)$.

De esta manera se ha demostrado que cualquier procedimiento de eliminación algebraicamente robusto aplicado a la familias de problemas del ejemplo 6 (que tiene talla de entrada $O(n)$ o $O(n^2)$ según el contexto) produce un circuito solución de talla al menos $2^{\frac{n}{2}} - 4$, es decir, un circuito de talla no polinomial con respecto a la longitud de la entrada. □

Cabe destacar que las hipótesis del teorema 24 son aplicables a todos los procedimientos de eliminación conocidos, es decir, todos los procedimientos de eliminación conocidos (tanto los basados en álgebra lineal como en técnicas de bases de Gröbner) son algebraicamente robustos sobre familias playas de problemas de eliminación si la solución general del problema dado se requiere como salida. La propiedad de invariancia de estos algoritmos se verifica fácilmente en la situación de una familia playa de problemas de eliminación m-dimensionales anteriormente considerados. Para ésto, es suficienten observar que todos los algoritmos de eliminación conocidos aceptan los polinomios de entrada $G_1, \ldots, G_n, F$ en su representación densa o esparsa o por evaluación "black box" con respecto a las variables $U_1, \ldots, U_m, X_1, \ldots, X_n$.

En consecuencia, ninguno de los métodos de eliminación conocido puede mejorarse a fin de obtener un procedimiento de tiempo polinomial para eliminación geométrica (o algebraica).

Si bien la noción de procedimientos de eliminación algebraicamente robustos excluye ramificaciones en el programa de salida, la familia de polinomios del ejemplo exhibido parece indicar que un algoritmo de eliminación de tiempo polinomial (si existe) debe tener una gran complejidad topológica incluso si se aplica solamente a familias playas de problemas de eliminación. Por lo tanto, la eficiencia implicaría una muy complicada casuística en eliminación geométrica.

También se podría analizar si la admisión de divisiones en los circuitos de salida permitiría mejorar su talla minimal. Si bien ciertas divisiones son compatibles con el método exhibido en la demostración del teorema 24, en el caso general es necesario garantizar que las funciones parámetricas están racionalmente definidas para cualquier instancia del problema.

Finalmente, cabe destacar que el método de demostración aquí desarrollado no contribuye en absoluto a la cuestión fundamental de la teoría de complejidad algebraica sobre la no polinomialidad de la eliminación geométrica en el modelo no uniforme de complejidad o a la cuestión $\mathrm{P}_{\mathbf{C}} \neq \mathrm{NP}_{\mathbf{C}}$ en el modelo de las máquinas reales. De hecho, sólo se señala que todos los procedimientos de eliminación conocidos poseen una propiedad de uniformidad muy limitante (llamada robustez algebraica) y que esta propiedad implica la imposibilidad de transformar esto procedimientos en algoritmos de tiempo polinomial.

4.2.2 La complejidad de eliminación de un sistema de ecuaciones polinomiales

En esta subsección se analizará desde un punto de vista no uniforme el funcionamiento de los algoritmos desarrollados en el capítulo 2 sobre una familia playa de problemas de eliminación cero-dimensional. Como consecuencias de dicho análisis se propondrá un nuevo parámetro de complejidad, la *complejidad de eliminación* de un sistema de ecuaciones polinomiales, con el cual se intenta medir la dificultad intrínseca de la resolución de un sistema de ecuaciones polinomiales dado.

Sean $T_1, \ldots, T_m, X_1, \ldots, X_n, Y$ indeterminadas sobre $\mathbb{Q}$ y sean $G_1, \ldots, G_n$, y F polinomios de $\mathbb{Q}[T_1, \ldots, T_m, X_1, \ldots, X_n]$. Sea d el máximo de los grados de los polinomios $G_1, \ldots, G_n$. Supóngase que $G_1, \ldots, G_n$ y F están dados por medio de dos circuitos aritméticos en $\mathbb{Q}[T_1, \ldots, T_m, X_1, \ldots, X_n]$ de talla L y K respectivamente. Se asume además que $G_1, \ldots, G_n$ forman una sucesión regular en $\mathbb{Q}[T_1, \ldots, T_m, X_1, \ldots, X_n]$ y definen una variedad equidimensional

$$V := \{G_1 = 0, \ldots, G_n = 0\}$$

de $\mathbf{C}^{m+n}$ de dimensión m y grado afín δ. Finalmente, se supone que el morfismo $\pi : V \longrightarrow \mathbf{C}^m$ inducido por la proyección canónica de $\mathbf{C}^{n+m}$ en $\mathbf{C}^m$ es finito, genéricamente no ramificado y tiene grado δ.

Sea $\pi' : V \longrightarrow \mathbf{C}^{m+n}$ el morfismo de variedades afines definido por $\pi'(z) = \big(\pi(z), F(z)\big)$ para todo $z \in V$ y sea $P \in \mathbb{Q}[T_1, \ldots, T_m, Y]$ el polinomio minimal de la imagen de π'. El polinomio P es mónico en Y y se ve inmediatamente que $gr(P) \leq \delta gr(F)$ y $gr_Y(P) \leq \delta$. El método básico desarrollado en el capítulo 2 requiere $K\delta^{O(1)} + L(nd\Lambda)^{O(1)}$ operaciones aritméticas, donde Λ es el grado del sistema de ecuaciones $G_1 = 0, \ldots, G_n = 0$ (obsérvese que siempre se verifica $\Lambda \leq gr(G_1) \cdots gr(G_n)$). La salida es un circuito aritmético Γ_1 en $\mathbb{Q}[T_1, \ldots, T_m, Y]$ de longitud $(K + L)(n\delta)^{O(1)}$ que representa el polinomio P. Se analizará si una complejidad (cantidad de operaciones) de tipo $K\delta^{O(1)}$ es intrínseca para los problemas de eliminación en consideración.

Para tal fin, se exhibirá un ejemplo de un problema de eliminación cerodimensional para el cual la cantidad $K\delta$ representa una cota inferior para la complejidad no escalar de la salida polinomial en el modelo *no uniforme* de complejidad.

Ejemplo 7 *Sean $S, T_1, \ldots, T_\delta, X, Y$ indeterminadas sobre $\mathbb{Q}$. Sea $\mathcal{G}$ la familia de problemas de eliminación definida por los siguientes polinomios:*

$$G := \prod_{j=1}^{\delta} (X - T_j)\,,\ F := SX^{2^K}$$

Sea $V := \{G = 0\}$ la hipersuperficie de $\mathbf{C}^{\delta+2}$ definida por el polinomio G y sea $\pi : V \longrightarrow \mathbf{C}^{\delta+1}$ el morfismo finito y genéricamente no ramificado inducido por la proyección canónica de $\mathbf{C}^{\delta+2}$ en $\mathbf{C}^{\delta+1}$. Obsérvese que δ es el grado de la hipersuperficie V de $\mathbf{C}^{\delta+2}$ y del morfismo π (de hecho, V es la unión de δ hiperplanos distintos de $\mathbf{C}^{\delta+2}$).

Los polinomios G y F tienen complejidad (talla de circuito) no escalar intrínseca δ y K respectivamente, y constituyen una familia playa de problemas de eliminación con $m := \delta + 1$ y $n := 1$. La longitud de la entrada es $\delta + K$. La solución general de este problema de eliminación se representa por medio del polinomio

$$P := \prod_{\ell=1}^{\delta} (Y - ST_i^{2^K}) = Y^\delta - Y^{\delta-1} S \sum_{\ell=1}^{\delta} T_\ell^{2^k} + O(S^2)$$

que pertenece a $\mathbb{Q}[T_1, \ldots, T_\delta, Y]$.

Sea Γ el circuito aritmético en $\mathbb{Q}[T_1, \ldots, T_\delta, S, Y]$ de talla no escalar $L(\Gamma)$ que calcula el polinomio P. Derivando este circuito con respecto a S y especializando S en 0 e Y en 1 se obtiene un circuito aritmético Γ^* de talla $L(\Gamma^*) \leq 3L(\Gamma)$ que calcula el polinomio

$$R := \sum_{\ell=1}^{\delta} T_\ell^{2^k}$$

Analizando la complejidad del polinomio R por medio del método del grado de Strassen [171], en el estilo de [10], se concluye que $L(\Gamma^*) \geq K\delta$. Esto implica que $L(\Gamma) \geq \frac{1}{3}K\delta$.

Desafortunadamente el carácter del parámetro δ es ambiguo, ya que éste es el grado de la variedad V y del morfismo π así como también la complejidad no escalar del polinomio G.

En consecuencia, cualquier procedimiento de eliminación optimal (incluso no uniforme) que produce la solución general de una familia playa dada de problemas de eliminación cero-dimensional tiene una complejidad inherente que depende linealmente de la complejidad no escalar del polinomio que define la proyección que se considera. El factor de proporcionalidad de esta dependencia lineal aparece como un invariante de la parte ecuacional del problema de eliminación. Por el momento, el autor no es capaz de interpretar sin ambigüedad este factor de proporción. El mismo está siempre acotado superiormente por una función polinomial en el tamaño del circuito aritmético, el número de variables eliminadas y el grado de la variedad de entrada, y en algunos casos aparece acotado inferiormente por una cantidad que puede ser interpretada alternativamente como el grado del sistema de entrada o su complejidad no escalar.

La discusión realizada en torno a los ejemplos 6 y 7 justifica la necesidad de introducir parámetros significativos a fin de estimar la complejidad computacional de cada problema de eliminación. En tal sentido se propondrá el concepto de *complejidad de eliminación.*

Sean $T_1, \ldots, T_m, X_1, \ldots, X_n, Y$ indeterminadas sobre $\mathbb{Q}$ y sean $G_1, \ldots, G_n$ polinomios de $\mathbb{Q}[T_1, \ldots, T_m, X_1, \ldots, X_n]$ que forman una sucesión regular en $\mathbb{Q}[T_1, \ldots, T_m, X_1, \ldots, X_n]$ y definen una variedad equidimensional $V := \{G_1 = 0, \ldots, G_n = 0\}$ de $\mathbb{C}^{m+n}$ de dimensión m y grado afín, y sea $\pi : V \longrightarrow$

$\mathbf{C}^m$ el morfismo de variedades afines inducido por la proyección canónica de $\mathbf{C}^{m+n}$ en $\mathbf{C}^m$. Supóngase que π es finito y genéricamente no ramificado.

Para cada polinomio $F \in \mathbb{Q}[T_1, \ldots, T_m, X_1, \ldots, X_n]$ se considera la familia playa de problemas de eliminación cero-dimensional definida por las ecuaciones $G_1 = 0, \ldots, G_n = 0$ y el polinomio F. La solución general de este problema se representa por medio de un polinomio de $\mathbb{Q}[T_1, \ldots, T_m, X_1, \ldots, X_n]$ que se denota por P_F. Sean $L(F)$ y $L(P_F)$ la complejidad no escalar de los polinomios F y P_F respectivamente. En esta situación, se observa que el conjunto:

$$N_{G_1,\ldots,G_n} := \left\{ \frac{L(P_F)}{L(F)}; F \in \mathbb{Q}[T_1, \ldots, T_m, X_1, \ldots, X_n] \right\}$$

está acotado (por una cantidad que depende en forma polinomial de la talla no escalar del circuito aritmético que evalúa $G_1, \ldots, G_n$ y $gr(V)$).

Definición 11 *Se define la* **complejidad de eliminación** *del sistema de ecuaciones*

$$G_1 = 0, \ldots, G_n = 0$$

como la cantidad

$$r(G_1, \ldots, G_n) := \sup N_{G_1,\ldots,G_n}$$

Del contenido del capítulo 2 se deduce que la complejidad de eliminación del sistema $G_1 = 0, \ldots, G_n = 0$ está acotada superiormente por una función polinomial en el grado del sistema, el grado y la complejidad de $G_1, \ldots, G_n$ y la cantidad de variables. Asimismo, el ejemplo 7 muestra una cota inferior para la complejidad de eliminación del sistema que, como ya ha sido señalado, puede interpretarse tanto como la complejidad o el grado (del sistema) de $G_1, \ldots, G_n$.

Conclusiones

Retomando la discusión del capítulo 4, se deduce que existen graves obstáculos (probablemente insalvables) para el desarrollo de algoritmos *generalistas* polinomiales que resuelvan los problemas de eliminación geométrica. Es entonces necesario reorientar el estudio hacia algoritmos y el software específicos para problemas particulares.

Las técnicas desarrolladas en el capítulo 2 constituyen un paso en tal dirección. En lugar de cantidades algebraicas como número de Bézout o la regularidad de la función de Hilbert de un ideal homogéneo apropiado, se han introducido invariantes *geométricos* que permiten, en casos geométricamente bien condicionados, reducir considerablemente el tamaño de las matrices en los algoritmos (y por lo tanto, la complejidad de los procedimientos).

Otra importante característica de los algoritmos desarrollados radica en la selección de la estructura de datos que se utiliza. La representación de polinomios por medio de circuitos aritméticos es indispensable para evitar el crecimiento exponencial de la complejidad de los algoritmos que ocurre cuando se codifican polinomios multivariados por su escritura densa.

Desde ya, quedan varios problemas por resolver: el primero de ellos es hallar familias infinitas de ejemplos de interés *práctico* en los cuales el grado y la altura geométrica del sistema son bajos. Esto demostraría concluyentemente la utilidad de las técnicas aquí desarrolladas.

Una segunda cuestión se refiere a la búsqueda de nuevos invariantes que permitan reducir la complejidad de los procedimientos en casos particulares. En particular, sería interesante hallar invariantes *continuos* que introduzcan mejoras de la complejidad.

Asimismo, permanece sin respuesta la cuestión de la (conjeturada) intratabilidad de los problemas de eliminación geométrica.

Bibliografía

[1] J. ABDELJOUED: *Sur l'algorithm de Berkowitz pour le calcul du déterminant dans un anneau commutatif arbitraire.* Preprint Université de Franche Compté, Besançon (1995).

[2] K.R. ABRAHAMSON: *Time-space tradeoffs for algebraic problems on general sequential machines.* Journal of Computer and System Sciences **43** (1991) 269–289.

[3] M. ALDAZ, J. HEINTZ, J.L. MONTAÑA, G. MATERA, L.M. PARDO: *Time-space trade-offs in algebraic complexity theory.* Sometido a Computational Complexity (1997).

[4] M.E. ALONSO, E. BECKER, M.-F. ROY, T. WÖRMAN: *Zeroes, multiplicities and idempotents for zerodimensional systems.* Algorithms in Algebraic Geometry and Applications, Proceedings MEGA'94 (L. Gonzalez Vega, T. Recio, Eds.), Progress in Mathematics **143**, Birkhäusser Verlag (1996).

[5] F. AMOROSO: *Test d'appartenance d'après un théorème de Kollár.* Comptes Rendus de l'Académie des Sciences de Paris **309**, Série I (1989) 691–694.

[6] *Automatic differentiation of algorithms: theory, implementation and application* Proceedings of the first SIAM Workshop on Automatic Differentiation, held in Breckenridge, Colorado (1991).

[7] J. BALCÁZAR, J. DÍAZ, J. GABARRÓ: *Structural complexity I.* EATCS Monographs on Theoretical Computer Science **11**, Springer-Verlag (1988).

[8] J. BALCÁZAR, J. DÍAZ, J. GABARRÓ: *Structural complexity II.* EATCS Monographs on Theoretical Computer Science **22**, Springer-Verlag (1990).

[9] W. BAUR: *Simplified lower bounds for polynomials with algebraic coefficients.* Aparecerá en Journal of Complexity (1996).

[10] W. BAUR, V. STRASSEN: *The complexity of partial derivatives.* Theoretical Computer Science **22** (1982) 317–330.

[11] P. BEAME: *A general sequential time-space tradeoff for finding unique elements.* Proceedings 21st Annual ACM Symposium on Theory of Computing (1989) 197–203.

[12] E. BECKER, J.P. CARDINAL, M.-F. ROY, Z. SZAFRANIEC: *Multivariate Bezoutians, Kronecker symbol and Eisenbud-Levine formula.* Algorithms in Algebraic Geometry and Applications, Proceedings MEGA'94 (L. Gonzalez Vega, T. Recio, Eds.), Progress in Mathematics **143**, Birkhäusser Verlag (1996).

[13] M. BEN-OR, R. CLEVE: *Computing algebraic formulas using a constant number of registers.* Proceedings 20th Annual ACM Symposium on Theory of Computing (1988) 254–257. También en SIAM Journal of Computing **21**(1) (1992) 54–58.

[14] M. BEN-OR, M. KOZEN, J. REIF: *The complexity of elementary algebra and geometry.* Journal of Computer and System Sciences **32** (1986) 251–264.

[15] C. BERENSTEIN, A. YGER: *Bounds for the degrees in the division problem.* The Michigan Mathematical Journal **37** (1990) 25–43.

[16] C. BERENSTEIN, A. YGER: *Effective Bézout identities in* $\mathbf{C}[z_1, \ldots, z_n]$. Acta Mathematica **166** (1991) 69–120.

[17] C. BERENSTEIN, A. YGER: *Une formule de Jacobi et ses conséquences.* Ann. Sci. E.N.S., $4^{\text{ième}}$ série, **24** (1991) 363–377.

[18] C. BERENSTEIN, A. YGER: *Green currents and analytic continuation.* Preprint, University of Maryland, 1995.

[19] S.J. BERKOWITZ: *On computing the determinant in small parallel time using a small number of processors.* Information Processing Letters **18** (1984) 147–150.

[20] D. BINI, V.Y. PAN: *Polynomial and matrix computations, Volume 1: Fundamentals algorithms.* Progress in Theoretical Computer Science, Birkhaüser, Boston (1994).

[21] L. BLUM, M. SHUB, S. SMALE: *On a theory of computation and complexity over the real numbers: NP–completeness, recursive functions and universal machines.* Bulletin of the American Mathematical Society **21**(1) (1989) 1–46.

[22] J. BOCHNAK, M. COSTE, M.–F. ROY: *Géométrie algébrique réelle.* Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 12, Springer Verlag (1987).

[23] R.B. BOPPANA, M. SIPSER: *The complexity of finite functions.* Handbook of theoretical computer science (J. Van Leeuwen, Ed.), Volumen A: Algorithms and Complexity. North–Holland, Amsterdam (1990) 759–804.

[24] A. BORODIN: *On relating time and space to size and depth.* SIAM Journal of Computing **6** (1977) 733–744.

[25] A. BORODIN: *Time–space tradeoffs (getting closer to the barriers?).* Proceedings 4th ACM-SIGSAM International Symposium on Symbolic and Algebraic Computation (1993) (K.W. Ny *et al.*, Eds.), Lecture Notes in Computer Science **762**, Springer–Verlag (1993) 209–220.

[26] A. BORODIN, S. COOK: *A time–space tradeoff for sorting on a general sequential model of computation.* SIAM Journal of Computing **11** (1982) 287–297.

[27] A. BORODIN, S. COOK, N. PIPPENGER: *Parallel computation for well-endowed rings and space-bounded probabilistic machines.* Information and Control **58** (1983) 113–136.

[28] A. BORODIN, M. J. FISCHER, D. J. KIRKPATRICK, N. A. LYNCH, M. TOMPA: *A time-space tradeoff for sorting on non-oblivious machines.* Journal of Computer and System Sciences **22**(3) (1981) 351–364.

[29] A. BORODIN, M. J. FISCHER, F. MEYER AUF DER HEIDE, E. UPFAL, A. WIGDERSON: *A time-space tradeoff for element distinctness.* SIAM Journal of Computing **16**(1) (1987) 97–99.

[30] A. BORODIN, J. VON ZUR GATHEN, J. HOPCROFT: *Fast parallel matrix and GCD computations.* Information and Control **52** (1982) 241–256.

[31] A. BORODIN, I. MUNRO: *The computational complexity of algebraic and numeric problems.* American Elsevier, New York (1975).

[32] J.-B. BOST, H. GILLET, C. SOULÉ: *Un analogue arithmétique du théorème de Bézout.* Comptes Rendus de l'Académie des Sciences de Paris **312**, Série I (1991) 845–848.

[33] J.-B. BOST, H. GILLET, C. SOULÉ: *Heights of projective varieties and positive Green forms.* Manuscript I.H.E.S. (1993).

[34] D. BROWNAWELL: *Bounds for the degrees in the Nullstellensatz.* Annals of Mathematics, Second Series, **126**(3) (1987) 577–591.

[35] D. BROWNAWELL: *A prime power version of the Nullstellensatz.* Manuscrito Penn State University (1989).

[36] B. BUCHBERGER: *Gröbner bases: an algorithmic method in polynomial ideal theory.* Multidimensional System Theory (N.K. Bose, Ed.), Reidel, Dordrecht (1985) 374–383.

[37] P. BÜRGISSER, M. CLAUSEN, A. SHOKROLLAHI: *Algebraic complexity theory.* A Series of Comprehensive Studies in Mathematics **315**, Springer-Verlag (1996).

[38] L. CANIGLIA, A. GALLIGO, J. HEINTZ: *Borne simple exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque.* Comptes Rendus de l'Académie des Sciences de Paris **307**, Série I (1988) 255–258.

[39] L. CANIGLIA, A. GALLIGO, J. HEINTZ: *Some new effectivity bounds in computational geometry.* Proceedings 6th International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer Lectures Notes in Computer Science **357** (1989) 131–151.

[40] L. CANIGLIA, A. GALLIGO, J. HEINTZ: *Equations for the projective closure and effective Nullstellensatz.* Discrete and Applied Mathematics **33** (1991) 11–23.

[41] L. CANIGLIA, J.A. GUCCIONE, J.J. GUCCIONE: *Local membership problems for polynomial ideals.* Effective Methods in Algebraic Geometry (T. Mora, C. Traverso, Eds.), Progress in Mathematics **94**, Birkhäuser (1991) 31–45.

[42] J. CANNY: *Some algebraic and geometric computations in PSPACE.* Proceedings 20th Annual ACM Symposium on Theory of Computing (1988) 460-467.

[43] J.P. CARDINAL: *Dualité et algorithmes itératives pour la solution des systémes polynomiaux.* Thése, Université de Rennes I (1993).

[44] E. CATTANI, A. DICKENSTEIN, B. STURMFELS: *Computing multidimensional residues.* Algorithms in Algebraic Geometry and Applications, Proceedings MEGA'94 (L. Gonzalez Vega, T. Recio, Eds.), Progress in Mathematics **143**, Birkhäusser Verlag (1996) 135–164.

[45] K. CHANDRASEKHARAN: *Introduction to analytic number theory.* Grundlehren der Math. Wissenschaften, Springer Verlag (1968).

[46] A.L. CHISTOV: *Polynomial-time computation of the dimension of the components of algebraic varieties in zero-characteristic.* Preprint Université Paris Val de Marne.

[47] A.L. CHISTOV: *Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic.* Lecture Notes in Computer Science **199** (1985) 63–69.

[48] A.L. CHISTOV, D.YU. GRIGOR'EV: *Subexponential time solving systems of algebraic equations.* LOMI Preprints E-9-83, E-10-83, Leningrad (1983).

[49] S. COOK: *The complexity of theorem proving procedures.* Proceedings 3rd. Annual Symposium on Theory of Computing (1971) 151–158.

[50] D. COPPERSMITH, S. WINOGRAD: *Matrix multiplication via arithmetic progression.* Proceedings 19th. Annual ACM Symposium on Theory of Computing (1987) 1–16.

[51] D. COX, J. LITTLE, D. O'SHEA: *Ideals, varieties and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Springer–Verlag (1992).

[52] L. CSANKY: *Fast parallel matrix inversion algorithms.* SIAM Journal of Computing **5**(4) (1976) 618–623.

[53] F. CUCKER, M. KARPINSKI, P. KOIRAN, T. LICKTEIG, K. WERTHER : *On real Turing machines that toss coins.* Manuscrito University Bonn (1995).

[54] J. DAVENPORT, J. HEINTZ: *Real quantifier elimination is doubly exponential.* Journal of Symbolic Computation **5** (1988) 29–35.

[55] R.A. DE MILLO, R.J. LIPTON: *A probabilistic remark on algebraic program testing.* Information Processing Letters **7**(4) (1978) 193–195.

[56] A. DICKENSTEIN, M. GIUSTI, N. FITCHAS, C. SESSA: *The membership problem for unmixed polynomial ideals is solvable in single exponential time.* Discrete and Applied Mathematics **33** (1991) 73–94.

[57] A. DICKENSTEIN, C. SESSA: *An effective residual criterion for the membership problem in* $\mathbf{C}[Z_1, \ldots, Z_n]$. Journal of Pure and Applied Algebra **74** (1991) 149–158.

[58] A. DICKENSTEIN, C. SESSA: *Duality methods for the membership problem.* Effective Methods in Algebraic Geometry (T. Mora, C. Traverso, Eds.), Progress in Mathematics **94**, Birkhäuser (1991) 89–103..

[59] A. DICKENSTEIN, C. SESSA: *Résidus de formes méromorphes et cohomologie modérée.* Géométrie Complexe, Prépublication Université Paris 7 (1994).

[60] T.W. DUBÉ: *A combinatorial proof of Effective Nullstellensatz.* Journal of Symbolic Computation **15** (1993) 277–296.

[61] P. DURIS, Z. GALIL: *A time-space tradeoff for language recognition.* Proceedings 22nd. Annual IEEE Symposium on Foundations of Computer Science (1981) 53–57.

[62] G. FALTINGS: *Diophantine approximation on abelian varieties.* Ann. of Math. **133** (1991) 549–576.

[63] M.J. FISCHER, M.D. RABIN: *Super-exponential complexity of Presburger arithmetic.* Complexity of Computation (R.M. Karp, Ed.), American Mathematical Society , Providence, RI (1974) 27–41.

[64] N. FITCHAS: *Algorithmic aspects of Suslin's solution of Serre's Conjecture.* Computational Complexity **3** (1993) 31–55.

[65] N. FITCHAS, A. GALLIGO: *Nullstellensatz effectif et conjecture de Serre (théorème de Quillen-Suslin) pour le Calcul Formel.* Math. Nachrichten **149** (1990) 231-253.

[66] N. FITCHAS, A. GALLIGO, J. MORGENSTERN: *Algorithmes rapides en séquentiel et parallèle pour l'élimination des quantificateurs en géométrie élémentaire.* Sélection d'exposes 1986-1987, Vol. I (F. Delon, M. Dickman, D. Gondard, Eds.), Publications Mathematiques de L'Universite Paris 7 **32** 103–145.

[67] N. FITCHAS, A. GALLIGO, J. MORGENSTERN: *Precise sequential and parallel complexity bounds for the quantifier elimination over algebraically closed fields.* Journal of Pure and Applied Algebra **67** (1990) 1-14.

[68] N. FITCHAS, M. GIUSTI, G. SMIETANSKI: *Sur la complexité du théoreme des zéros.* Approximation and Optimization **8** (J. Guddat *et al.*, Eds.), Peter Lange Verlag, Frankfurt am Main (1995) 274–329.

[69] S. FORTUNE, J. WYLLIS: *Parallelism in random access machines.* Proceedings 10th. ACM Symposium on Theory of Computing (1978) 114–118.

[70] W. FULTON: *Intersection theory.* Ergebnisse der Mathematik, 3 Folge Band 2, Springer Verlag (1984).

[71] M. GAREY, D. JOHNSON: *Computers and intractability : a guide to the theory of NP-completeness.* Freeman, San Francisco (1979).

[72] J. VON ZUR GATHEN: *Parallel arithmetic computations: a survey.* Proceedings 12th International Symposium on Mathematical Foundations on Computer Science, Bratislava, Springer Lecture Notes in Computer Science **233** (1986) 93–112.

[73] J. VON ZUR GATHEN: *Feasible arithmetic computations: Valiant's Hypothesis* Journal of Symbolic Computation **4** (1987) 137–172.

[74] J. VON ZUR GATHEN: *Parallel algorithms for algebraic problems.* Proceedings 13th Conference on Mathematical Foundations of Computer Science, Springer Lecture Notes in Computer Science **356** (1989) 269–300.

[75] J. VON ZUR GATHEN: *Parallel linear algebra.* Synthesis of Parallel Algorithms, chapter 8, Morgan Kauffmann Publishers (1993) 573–617.

[76] J. VON ZUR GATHEN, V. STRASSEN: Some polynomials that are hard to compute. Theoretical Computer Science **11**(3) (1981) 159–171.

[77] P. GIANNI, T. MORA: *Algebraic solution of systems of polynomial equations using Gröbner bases.* Proceedings 5th International Conference on Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, Springer Lectures Notes in Computer Science **356** (1989) 247–257.

[78] M. GIUSTI, K. HÄGELE, J. HEINTZ, J.L. MONTAÑA, J.E. MORAIS, L.M. PARDO: *Lower bounds for diophantine approximation.* Aparecerá en Journal of Pure and Applied Algebra (1997).

[79] M. GIUSTI, J. HEINTZ: *Algorithmes -disons rapides- pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles.* Effective Methods in Algebraic Geometry (T. Mora, C. Traverso, Eds.), Progress in Mathematics **94**, Birkhäuser (1991) 169–193.

[80] M. GIUSTI, J. HEINTZ: *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial.* Computational Algebraic Geometry and Commutative Algebra, Proceedings of the Cortona Conference on Computational Algebraic Geometry and Commutative Algebra (D. Eisenbud, L. Robbiano, Eds.), Symposia Matematica, vol. XXXIV, Istituto Nazionale di Alta Matematica, Cambridge University Press (1993) 216–256.

[81] M. GIUSTI, J. HEINTZ, J.E. MORAIS, J. MORGENSTERN, L.M. PARDO: *Straight-line programs in geometric elimination theory.* Aparecerá en Journal of Pure and Applied Algebra (1996).

[82] M. GIUSTI, J. HEINTZ, J.E. MORAIS, L.M. PARDO: *When polynomial equation systems can be 'solved' fast?* Proceedings 11th. International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer Lectures Notes in Computer Science **948** (1995) 205–231.

[83] M. GIUSTI, J. HEINTZ, J. SABIA: *On the efficiency of the effective Nullstellensätze.* Computational Complexity **3** (1993) 56–95.

[84] A. GRIEWANK: *Achieving logarithmic growth of temporal and spatial complexity in reverse automatic differentiation.* Preprint MCS-P228-0491, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, III (1991).

[85] D. GRIGORIEV: *An application of separability and independence notions for proving lower bounds of circuit complexity.* Notes of Scientific Seminars **60** Leningrad Departament, Steklov Mathematical Institute (1976) 36–48 (in Russian).

[86] A. GROSSO, N. HERRERA, G. MATERA, M.E. STEFANONI, J.M. TURULL: *Un algoritmo para el cálculo del rango de matrices enteras en espacio polilogarítmico.* Procedimientos 25° Jornadas Argentinas de Informática e Investigación Operativa (1996) 29–48.

[87] K. HAEGELE, J.L. MONTAÑA: *Polynomial random test for the equivalence problem of integers given by arithmetic circuits.* Publicación Universidad de Cantabria (1995).

[88] J. HEINTZ: *Definability and fast quantifier elimination in algebraically closed fields.* Theoretical Computer Science **24** (1983) 239–277.

[89] J. HEINTZ: *On the computational complexity of polynomials and bilinear mappings.* Proceedings 5th. International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer Lectures Notes in Computer Science **356** (1989) 269–300.

[90] J. HEINTZ, J. MORGENSTERN: *On the intrinsic complexity of elimination theory.* Journal of Complexity **9** (1993) 471–498.

[91] J. HEINTZ, M.-F. ROY, P. SOLERNÓ: *On the complexity of semialgebraic sets.* Proceedings Information Processing 89 (IFIP 89) San Francisco 1989 (G.X.Ritter, Ed.), North-Holland (1989) 293–298.

[92] J. HEINTZ, M.-F. ROY, P. SOLERNÓ: *Complexité du principe de Tarski-Seidenberg.* Comptes Rendus de l'Académie des Sciences de Paris **309**, Série I (1989) 825–830.

[93] J. HEINTZ, M.-F. ROY, P. SOLERNÓ: *Sur la complexité du principe de Tarski-Seidenberg.* Bulletin de la Societé Mathematique de France **118** (1990) 101–126.

[94] J. HEINTZ, C.P. SCHNORR: *Testing polynomials which are easy to compute.* Logic and Algorithmic. An International Symposium held in honour of Ernst Specker. Monographie **30** de L'Enseignement Mathématique, Genève (1982) 237–254. También publicado en Proceedings 12th Annual ACM Symposium on Theory of Computing (1980) 262–280.

[95] J. HEINTZ, M. SIEVEKING: *Lower bounds for polynomials with algebraic coefficients.* Theoretical Computer Science **11** (1980) 321–330.

[96] G. HERMANN: *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.* Math. Ann. **95** (1926) 736–788.

[97] O.H. IBARRA, S. MORAN: *Probabilistic algorithms for deciding equivalence of straight-line programs.* Journal of the Association for Computing Machinery **30**(1) (1983) 217–228.

[98] O.H. IBARRA, S. MORAN, E. ROSIER: *Probabilistic algorithms and straight-line programs for some rank decision problems.* Information Processing Letters **12**(5) (1981) 227–232.

[99] N. IMMERMAN, S. LANDAU: *The complexity of iterated multiplication.* Preprint (1991).

[100] B. IVERSEN: *Generic local structures of the morphisms in commutative algebra.* Springer Lecture Notes in Mathematics **310** (1973).

[101] J. JA'JA': *Time-space tradeoffs for some algebraic problems.* Journal of the Association for Computing Machinery **30**(3) (1983) 657–667.

[102] J. JA'JA': *An introduction to parallel algorithms.* Addison-Wesley (1992).

[103] J.P. JOUANOLOU: *Théorèmes de Bertini et applications.* Progress in Mathematics **42**, Birkhäuser (1983).

[104] E. KALTOFEN: *Greatest common divisors of polynomials given by straight line programs.* Journal of the Association for Computing Machinery **35**(1) (1988) 234–264.

[105] E. KALTOFEN, V. PAN: *Processor efficient parallel solution of linear systems over an abstract field.* Proceedings 3rd. Annual ACM Symposium on Parallel Algorithms and Architectures (1991) 180–191.

[106] E. KALTOFEN, M. SINGER: *Size efficient parallel algebraic circuits for partial derivatives.* Technical Report 90–32, Computer Science Department RPI, Troy, New York (1990).

[107] R.M. KARP: *Reducibility among combinatorial problems.* Complexity of Computer Computations (R.E. Miller, J.W. Tatcher, Eds.), Plenum Press, New York (1972) 85–103.

[108] R.M. KARP, V. RAMACHANDRAN: *Parallel algorithms for shared-memory machines.* Handbook of theoretical computer science (J. Van Leeuwen, Ed.), Volumen A: Algorithms and Complexity. North-Holland, Amsterdam (1990) 871–941.

[109] D.E. KNUTH: *The Art of Programming (vol. 2) : semi-numerical algorithms.* Addison-Wesley (1981).

[110] H. KOBAYASHI, T. FUJISE, A. FURUKAWA: *Solving systems of algebraic equations equations by general elimination method.* Journal of Symbolic Computation **5** (1988) 303-320.

[111] J. KOLLÁR: *Sharp effective Nullstellensatz.* Journal of American Mathematical Society **1** (1988) 963-975.

[112] T. KRICK, A. LOGAR: *Memberships problems, representation problems and the computation of the radical for one-dimensional ideals.* Effective Methods in Algebraic Geometry (T. Mora, C. Traverso, Eds.), Progress in Mathematics **94**, Birkhäuser (1991) 203-216.

[113] T. KRICK, L.M. PARDO: *Une approche informatique pour l'approximation diophantienne.* Comptes Rendus de l'Académie des Sciences de Paris **318**, Série I, No. 5 (1994) 407-412.

[114] T. KRICK, L.M. PARDO: *A computational method for diophantine approximation.* Algorithms in Algebraic Geometry and Applications, Proceedings MEGA'94 (L. Gonzalez Vega, T. Recio, Eds.), Progress in Mathematics **143**, Birkhäusser Verlag (1996) 193-254.

[115] T. KRICK, J. SABIA, P. SOLERNÓ: *On intrinsic bounds in the Nullstellensatz.* Aparecerá en Applicable Algebra in Engineering, Communication and Computer Science (1996).

[116] E. KUNZ: *Kähler differentials.* Advanced Lectures in Mathematics, Vieweg Verlag, Braunschweig/Wiesbaden (1986).

[117] R.E. LADNER, M.J. FISCHER: *Parallel prefix computation.* Journal of the Association for Computing Machinery **27** (1980) 831-838.

[118] Y.N. LAKSHMAN, D. LAZARD: *On the complexity of zero-dimensional algebraic systems.* Effective Methods in Algebraic Geometry (T. Mora, C. Traverso, Eds.), Progress in Mathematics **94**, Birkhäuser (1991) 217-225.

[119] D. LAZARD: *Résolution des systèmes d'équations algébriques.* Theoretical Computer Science **15** (1981) 77–110.

[120] T. LENGUAGER, R.E. TARJAN: *Upper and lower bounds on time-space tradeoffs.* Proceedings 11th. Annual ACM Symposium on Theory of Computing (1979) 262–277.

[121] T. LICKTEIG: *Semi-algebraic decision complexity.* Technical Report TR-90-052 Int. Comp. Science Inst., Berkeley, (1990) and Univ. Tübingen, Habilitatiosschrift.

[122] T. LICKTEIG, K. WERTHER: *How to compute a complex square root optimally?.* Computational Complexity (1996).

[123] G. MATERA, J.M. TURULL: *The space complexity of elimination theory: upper bounds.* Foundations of Computational Mathematics, Springer-Verlag (1997) 267–276.

[124] H. MATSUMURA: *Commutative ring theory.* Cambridge University Press (1986).

[125] E. MAYR: *Membership in polynomial ideals over $\mathbb{Q}$ is exponential space complete.* Proceedings 6th. Annual Symposium on Theoretical Aspects of Computer Science, Springer Lectures Notes in Computer Science **349** (1989) 400–406.

[126] E. MAYR, A. MEYER: *The complexity of the word problem for commutative semi-groups and polynomial ideals.* Advances in Math. **46**(3) (1982) 305–329.

[127] C. MICHAUX: *Une remarque à propos des machines sur $\mathbb{R}$ introduites par Blum, Shub et Smale.* Comptes Rendus de l'Académie des Sciences de Paris **309**, Série I (1989) 435–437.

[128] M. MOELLER: *Systems of algebraic equations solved by means of endomorphisms.* Proceedings 10th. International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer Lectures Notes in Computer Science (1993).

[129] J.L. MONTAÑA, L.M. PARDO: *Lower bounds for arithmetic networks.* Applicable Algebra in Engineering, Communication and Computer Science **4**(1) (1993) 1–24.

[130] J.L. MONTAÑA, J.E. MORAIS, L.M. PARDO: *Lower Bounds for Arithmetic Networks II: Sum of Betti numbers.* Applicable Algebra in Engineering, Communication and Computer Science **7**(1) (1996) 41–51.

[131] J. MORGENSTERN: *How to compute fast a function and all its derivatives.* Prépublication **49**, Université de Nice (1984).

[132] MULMULEY K.: *A fast parallel algorithm to compute the rank of a matrix over an arbitrary field.* Proceedings 18th Annual Symposium on Theory of Computing (1986) 338–339.

[133] JU. V. NESTERENKO: *Estimates for the order of zero o functions of a certain class and applications in the theory of transcendental numbers.* Math. USSR Izvestija **11**(2) (1977) 239–270.

[134] YU. V. NESTERENKO: *On a measure of the algebraic independence of the values of certain functions.* Math. USSR Sbornik **56** (1987) 545–567.

[135] A.M. OSTROWSKI: *On two problems in abstract algebra connected with Horner's rule.* Studies in Mathematics and Mechanics presented to Richard von Mises, Academic Press (1954) 40–48.

[136] V.Y. PAN: *New combinations of methods for the acceleration of matrix multiplication.* Comput. Math. Appl. **7** (1981) 73–125.

[137] V.Y. PAN: *Complexity of parallel matrix computations.* Theoretical Computer Science **54**(1) (1987) 65–85.

[138] L.M. PARDO: *How lower and upper complexity bounds meet in elimination theory.* Proceedings 11th. International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer Lectures Notes in Computer Science **948** (1995) 33–69.

[139] M.S. PATERSON, L.J. STOCKMEYER: *On the number of non-scalar multiplications necessary to evaluate polynomials.* SIAM Journal of Computing **2** (1973) 80–96.

[140] W.J. PAUL, R.E. TARJAN: *Time-space tradeoffs in a pebble game.* Acta Informatica **10** (1978) 509–515.

[141] PFALTZ J.L.: *Computer data structures.* McGraw-Hill (1977).

[142] P. PHILIPPON: *Critères pour l'independence algébrique.* Pub. Math. de l'IHFS **64** (1987) 5–52.

[143] P. PHILIPPON: *Théorème des zéros effective, d'après J. Kollar.* Publications Mathematiques de l'Univ. P. et M. Curie, Paris VI **88**, Groupe d'étude sur les Problémes diophantiens 1988–1989, exposé 6.

[144] P. PHILIPPON : *Dénominateurs dans le théorème des zéros de Hilbert.* Acta Arithmetica **58** (1991) 1–25.

[145] P. PHILIPPON: *Sur des hauteurs alternatives I* Math. Ann. **289** (1991) 255–283.

[146] P. PHILIPPON: *Sur des hauteurs alternatives II.* Ann. Inst. Fourier, Grenoble **44**(2) (1994) 1043–1065.

[147] P. PHILIPPON: *Sur des hauteurs alternatives III.* Journal de Mathématiques Pures et Appliquées **75** (1995) 345–365.

[148] N. PIPPENGER: *A time-space tradeoff.* Journal of the Association for Computing Machinery **25** (1978) 509–515.

[149] N. PIPPENGER: *Pebbling.* Proceedings 5th. IBM Symposium on Mathematical Foundations of Computer Science (1980).

[150] F.P. PREPARATA, D.V. SARWATE: *An improved parallel processor bound in fast matrix inversion.* Information Processing Letters **7**(2) (1978) 148–150.

[151] M.O. RABIN: *Probabilistic algorithms.* Algorithms and Complexity, Recent Results and New Directions (J.F. Traub, Ed.), Academic Press, Cambridge, MA (1976).

[152] J. REIF: *Logarithmic depth circuits for algebraic functions.* SIAM Journal of Computing **15** (1986) 231–242.

[153] J. RENEGAR: *On the computational complexity and geometry of the first order theory of the reals.* Journal of Symbolic Computation **13**(3) (1992) 255–352.

[154] J. SABIA, P. SOLERNÓ: *Bounds for traces in complete intersections and degrees in the Nullstellensatz.* Applicable Algebra in Engineering, Communication and Computer Science **6** (1996) 353–376.

[155] J.E. SAVAGE: *Space-time tradeoffs - A survey.* Proceedings 3rd. Hungarian Computer Science Conference (1981).

[156] J.E. SAVAGE: *Space-time tradeoffs for banded matrix problems.* Journal of the Association for Computing Machinery **31**(4) (1984) 422-437.

[157] J.E. SAVAGE, S. SWAMY: *Space-time tradeoffs on the FFT algorithm.* IEEE Transactions on Information Theory **24** (1978) 563–568.

[158] J.E. SAVAGE, S. SWAMY, Space-time tradeoffs for oblivious integer multiplication. Springer Lecture Notes in Computer Science **71** (1979) 240–251.

[159] A. SCHÖNHAGE: *On the power of random access machines.* Proceedings Sixth Colloquium on Automata, Languages and Programming ICALP (1977) 520–529, también en Springer Lectures Notes in Computer Science **71** (1979).

[160] A. SCHÖNHAGE, V. STRASSEN: *Schnelle multiplikation grosser zahlen.* Comput. **7** (1971) 281–292.

[161] C.P. SCHNORR: *Improved lower bounds on the number of multiplications/divisions which are necessary to evaluate polynomials.* Theoretical Computer Science **7** (1978) 251–261.

[162] J.T. SCHWARTZ: *Fast probabilistic algorithms for verification of polynomial identities.* Journal of the Association for Computing Machinery **27** (1980) 701–717.

[163] I.R. SHAFAREVICH: *Basic algebraic geometry: varieties in projective space.* Springer Verlag (1994).

[164] B. SHIFFMAN: *Degree bounds for the division problem in polynomial ideals.* Michigan Mathematical Journal **36** (1989) 163–171.

[165] M. SHUB, S. SMALE: *On the Intractability of Hilbert's Nullstellensatz and an algebraic version of "NP=P ?.* Duke Journal of Mathematics **81**(1) (1996) 47–54.

[166] M. SOMBRA: *Bounds for the Hilbert function of polynomial ideals and for the degrees in the Nulstellensatz.* Aparecerá en Journal of Pure and Applied Algebra (1997).

[167] H.J. STOSS: Lower bounds for the complexity of polynomials. Theoretical Computer Science **64** (1989) 15–23.

[168] H. J. STOSS: *On the representation of rational functions of bounded complexity.* Theoretical Computer Science **64** (1989) 1–13.

[169] V. STRASSEN: *Gaussian elimination is not optimal.* Num. Math. **13** (1969) 354–356.

[170] V. STRASSEN: *Vermeidung von Divisionen.* Crelles Journal für die Reine und Angewandte Mathematik **264** (1973) 184–202.

[171] V. STRASSEN: *Polynomials with rational coefficients which are hard to compute.* SIAM Journal of Computing **3** (1974) 128–149.

[172] V. STRASSEN: *Algebraic complexity theory.* Handbook of theoretical computer science (J. Van Leeuwen, Ed.), Volumen A: Algorithms and Complexity. North-Holland, Amsterdam (1990) 634–671.

[173] M. TOMPA: *Time-space tradeoffs for computing functions, using conectivity properties of their circuits.* Journal of Computer and System Sciences **20** (1980) 118–132.

[174] M. TOMPA: *Two Familiar Transitive Closure Algorithms which Admit no Polynomial Time, Sublinear Space Implementations.* SIAM Journal of Computing **11**(1) (1982) 130–137.

[175] P.M. VAIDYA: *Space-time tradeoff for orthogonal range queries.* Proceedings 17th. Annual ACM Symposium on Theory of Computing (1985) 169–174.

[176] L. VALIANT: *Completeness classes in algebra.* Proceedings 11th. Annual ACM Symposium on Theory of Computing (1979) 249–261.

[177] L. VALIANT: *The complexity of computing the permanent.* Theoretical Computer Science **8** (1979) 189–201.

[178] L. VALIANT: *Reducibility by algebraic projections.* Logic and Algorithmic. An International Symposium held in honour of Ernst Specker. Monographie **30** de L'Enseignement Mathématique, Genève (1982) 365–380.

[179] N. VOROBJOV: *Bounds of real roots of a system of algebraic equations.* Notes of Scientific Seminars **137**, Leningrad Departament, Steklov Mathematical Institute (1984) 7–19.

[180] B.L. VAN DER WAERDEN: *Algebra I*, 5. Auflage der Modernen Algebra, Springer Verlag (1960).

[181] I. WEGENER: *The complexity of boolean functions.* Wiley-Teubner Series in Computer Science (1987).

[182] V. WEISPFENNING: *The complexity of linear problems in fields.* Journal of Symbolic Computation **5** (1988) 3–28.

[183] A.C.C. YAO: *Space–time tradeoff for answering range queries.* Proceedings 14th Annual ACM Symposium on Theory of Computing (1982) 128–136.

[184] A.C.C. YAO: *Near optimal time–space tradeoff for element distinctness.* Proceedings 29th Annual IEEE Symposium on Foundations of Computer Science (1988) 91–97.

[185] Y. YESHA: *Time–space tradeoffs for matrix multiplication and the discrete Fourier transformation on any general sequential random acces computer.* Journal of Computer and System Sciences **29** (1984) 183–197.

[186] R.E. ZIPPEL: *Probabilistic algorithms for sparse polynomials.* Springer Lectures Notes in Computer Science **72** (1979) 216–226.