Un Problema de Eliminación Geométrica en Sistemas de Pham–Brieskorn

Agustín Bompadre

Diciembre 1999

Agustín Bompadre
Departamento de Matemáticas,
Facultad de Ciencias Exactas y Naturales,
Universidad de Buenos Aires,
Pabellón 1, Ciudad Universitaria,
Buenos Aires, Argentina.

Título Original: "Un problema de Eliminación Geométrica en sistemas de Pham–Brieskorn"

Tesis de Licenciatura en Matemáticas. Universidad de Buenos Aires. Diciembre de 1999.

Director de Tesis: Joos U. Heintz.

Co–director de Tesis: Guillermo Matera.

Contenidos

Resumen

En [GHM+98], [GHH+97], [HKP+98] y [Mor97] se desarrollan algoritmos que resuelven el siguiente problema: dados como input n polinomios en n variables con coeficientes en $\mathbb{Q}$ que definen una variedad algebraica cero–dimensional en $\mathbb{C}^n$, dar como output una descripción adecuada (la *solución geométrica*) de esta variedad. En estos algoritmos es necesario poder resolver el problema de hallar la ecuación minimal que verifica un polinomio dado H en el anillo de coordenadas definido por una variedad m–dimensional V incluída en un espacio n–dimensional. Para ello, se trabaja con un vector en $\mathbb{Q}^(n-m)$, llamado *punto de levantamiento*. El punto de levantamiento es un punto no ramificado; esta restricción se traduce en que un cierto polinomio no se anule en este punto. Es decir que genéricamente un elemento de $\mathbb{Q}^(n-m)$ es un punto de levantamiento. En [HKP+98] se refinan las cotas de complejidad, pasando a depender de la elección del punto de levantamiento. Es decir, se mejora la complejidad para puntos de levantamiento "especiales". Hay que tener en cuenta que un punto genérico implica una complejidad del peor caso. Por esta razón es interesante poder debilitar las restricciones que pesan sobre el punto de levantamiento; en esta tesis se eliminan estas restricciones para variedades 1–dimensionales definidas por un sistema de Pham–Brieskorn.

1 Introducción

1.1 Definiciones y notación

En lo que sigue, notaremos $\mathbb{Q}$al cuerpo de los números racionales, $\mathbb{C}$al de los números complejos. Más adelante necesitaremos más generalidad, por lo que notamos $\mathbf{k}$ a un cuerpo de característica cero. $\mathbb{A}^n$ denotará al espacio n–dimensional afín $\mathbb{C}^n$ provisto de la topología Zariski. Sean $\varepsilon, X_1, \ldots, X_n, T$ indeterminadas sobre $\mathbb{Q}$. Sean $f_1, \ldots, f_s$ polinomios en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$, sea $(f_1, \ldots, f_s)$ el ideal que generan en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ y sea $V := V(f_1, \ldots, f_s) \subseteq \mathbb{A}^{n+1}$ la variedad algebraica afín definida por $(f_1, \ldots, f_s)$.
El anillo de coordenadas de V es $\mathbb{Q}[V]$.
log() nota a la función logaritmo en base 2. Dado f un polinomio, $\deg(f)$ denota el grado total de f. Finalmente, $\mathbb{Z}$ y $\mathbb{N}$ denotan al anillo de los números enteros y al conjunto de los enteros positivos respectivamente.
En esta tesis seguimos la terminología y notaciones estándar del álgebra conmutativa y de la geometría algebraica tal como se encuentran en libros como [AM69], [Eis95] (álgebra conmutativa), [Wal78] y [Sha84] (geometría algebraica).

1.2 Comentario breve

En esta tesis estudiamos una instancia del problema de Eliminación en Geometría Algebraica que llamamos el **Problema de Proyección** (ver [HKP$^+$98]). El Problema de Proyección es el siguiente:

Sea $V \subseteq \mathbb{A}^p$ una variedad algebraica equidimensional de dimensión $m = \dim V$ definida por un sistema de $p-m$ ecuaciones polinomiales sobre $\mathbb{Q}$. Sea $\pi : V \to \mathbb{A}^m$ el morfismo inducido por la proyección en las primeras coordenadas pensando a $V \subset \mathbb{A}^p = \mathbb{A}^m \times \mathbb{A}^{p-m}$, y supongamos que π es un epimorfismo finito de variedades. Sea $h \in \mathbb{Q}[V]$ un elemento en el anillo de coordenadas de V dado por un polinomio p–variado H sobre $\mathbb{Q}$. Consideramos al morfismo $\tilde{\pi} : V \to \mathbb{A}^{m+1}$ definido por la regla $\tilde{\pi}(x) := (\pi(x), h(x))$ para x en V. Por construcción $\tilde{\pi}$ resulta un morfismo finito, y dado que $\mathbb{A}^m$ es normal , se sigue que la imagen de $\tilde{\pi}$ es una subvariedad equidimensional de codimensión 1 de $\mathbb{A}^{m+1}$, i.e. una hipersuperficie. Supongamos además que es conocido un punto $t \in \mathbb{A}^m$ tal que su fibra por π, o sea $\pi^{-1}(t)$, es no ramificada, y que de hecho π es genéricamente playo y genéricamente no ramificado. Sean $T_1, \ldots, T_m, Y$ indeterminadas sobre $\mathbb{Q}$.
Entonces existe una única ecuación minimal $m_H \in \mathbb{Q}[T_1, \ldots, T_m][Y]$ que define, la imagen de $\tilde{\pi}$. Llamamos **problema de proyección** al de, dados polinomios con coeficientes en $\mathbb{Q}$ que definen a la variedad algebraica V, la función regular h, y una descripción de la variedad $\pi^{-1}(t)$, encontrar un polinomio $(m+1)$–variado sobre $\mathbb{Q}$

que represente a la ecuación de dependencia entera minimal que satisface la función regular h en la extensión $\mathbb{Q}[T_1, \ldots, T_m] \to \mathbb{Q}[V]$. Diremos que el polinomio m_H que resuelve este problema es la proyección de h en V.

Este es un problema fundamental para los procedimientos de eliminación geométrica y fue considerado por varios autores (ver por ejemplo [GH93], [KP96], [GHMP95], [GHM$^+$98], [GHH$^+$97], [Mor97]). Más precisamente, se utilizan algoritmos que resuelven instancias particulares de este problema como pasos intermedios en el problema de hallar una solución geométrica de una variedad cero–dimensional (una definición de solución geométrica está establecida en 11). En [HMW99] y [GLS99] se plantean variantes para resolver este último problema donde es necesario la proyección de formas lineales en variedades 1–dimensionales. En esta tesis estudiamos el problema de proyección en una curva definida por un sistema de Pham–Brieskorn (ver Subsección siguiente).

Una tarea paralela al desarrollo de un algoritmo es estudiar su complejidad en espacio y tiempo. Para ello, se definen medidas del espacio y tiempo utilizado y se obtienen cotas en función del "tamaño" del input. La razón es clara, dada una instancia particular de un problema nos interesa saber de antemano si se puede resolver con los recursos que disponemos. Las medidas de espacio y tiempo se definen en la Subsección 2.1.

Un aspecto al que hay que prestar atención es al de las estructuras de datos utilizadas para representar polinomios multivariados. Típicamente, los polinomios se representan por su escritura densa. Sin embargo, un ejemplo debido a D. Lazard, T. Mora, W. Masser y P. Philippon (ver [Bor93]) muestra que un comportamiento super–exponencial en tiempo es inevitable utilizando esta representación.

Una alternativa es codificar los polinomios por circuitos aritméticos y sus esquemas de evaluación asociados, los straight–line programs. Un ejemplo de straight–line program es la conocida regla de Horner. La filosofía detrás de esta representación es la de recordar que los polinomios son funciones. El input del algoritmo es dado entonces por straight–line programs y los polinomios intermedios y el polinomio que será el output también estarán codificados por straight–line programs. En esta tesis utilizaremos esta codificación; las definiciones de circuito aritmético y straight–line program se encuentran en la Subsección 2.1.

1.3 Establecimiento del resultado principal

Sean $G_1, \ldots, G_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$, sea d en $\mathbb{N}$ tal que $d > \deg(G_i)$ para $1 \leq i \leq n$. Consideramos el sistema de Pham–Brieskorn en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$:

$$\left\{\begin{array}{c} F_1(\varepsilon, X_1, \ldots, X_n) := X_1^d - \varepsilon G_1(X_1, \ldots, X_n) \\ \vdots \\ F_n(\varepsilon, X_1, \ldots, X_n) := X_n^d - \varepsilon G_n(X_1, \ldots, X_n) \end{array}\right. \tag{1}$$

Supongamos que para cada $1 \leq i \leq n$, $\alpha_i := G_i(0, \ldots, 0)$ es no nulo. Sea I el ideal generado por $F_1, \ldots, F_n$ en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$, sea B el ágebra $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]/I$ y sea V la variedad algebraica definida por I:

$$V := \{F_1 = 0, \ldots, F_n = 0\} := \{(\tau, \xi) \in \mathbb{A}^1 \times \mathbb{A}^n; F_1(\tau, \xi) = \ldots = F_n(\tau, \xi) = 0\}.$$

Sea $V' \subseteq \mathbb{A}^n$ la variedad algebraica cero–dimensional definida por los ceros comunes de $X_1^d - \alpha_1, \ldots, X_n^d - \alpha_n$. Sea $\pi : V \longrightarrow \mathbb{A}^1$ el morfismo de variedades algebraicas inducido por la proyección canónica de $\mathbb{A}^1 \times \mathbb{A}^n$ en $\mathbb{A}^1$. Este morfismo resulta finito, en particular implica que el morfismo de anillos

$$\mathbb{Q}[\varepsilon] \longrightarrow B$$

es entero, es decir que para todo polinomio H en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ existe un polinomio q_H en $\mathbb{Q}[\varepsilon][T]$, mónico en T, tal que $q_H(H) = 0$ en B. La indeterminada ε juega entonces el rol de variable libre, mientras que las indeterminadas $X_1, \ldots, X_n$ dependen de ε. La variedad V definida por los polinomios $F_1, \ldots, F_n$ en $\mathbb{C}^{n+1}$ resulta una curva, y para todo número complejo z existen a lo sumo d^n elementos de $\mathbb{C}^n$, que numeraremos $\xi(z)_1, \ldots, \xi(z)_{K_z}$ tal que los puntos $(z, \xi(z)_1), \ldots, (z, \xi(z)_{K_z})$ pertenecen a la variedad V. Dado un complejo z, el cardinal del conjunto $\pi^{-1}(z) = \{(z, \xi) \in \mathbb{A}^{n+1} : (z, \xi) \in V\}$ es menor o igual que d^n,y la igualdad vale para todo complejo salvo un número finito de ellos. Un complejo z tal que $\#\pi^{-1}(z) = d^n$ es llamado un *punto de levantamiento* y el conjunto $\pi^{-1}(z)$ es llamado la *fibra de levantamiento* de z. Se observa que el origen $0 \in \mathbb{A}$ no es un punto de levantamiento pues su fibra $\pi^{-1}(0)$ está compuesta por un único punto, el vector $(0, 0, \ldots, 0) \in \mathbb{A}^{n+1}$. Dada $\pi^{-1}(z)$ una fibra de levantamiento con $z \in \mathbb{Q}$, se denomina una *solución geométrica de* $\pi^{-1}(z)$ al conjunto formado por una forma lineal $U \in \mathbb{Q}[X_1, \ldots, X_n]$, y polinomios $q, v_1, \ldots, v_n \in \mathbb{Q}[T]$ tal que se tiene el isomorfismo de álgebras inducido por la forma U

$$\mathbb{Q}[\pi^{-1}(z)] \simeq \mathbb{Q}[T]/(q(T)) \simeq \mathbb{Q}[X_1, \ldots, X_n]/(q(U), X_1 - v_1(U), \ldots, X_n - v_n(U)).$$

Dado un polinomio H en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$, se quiere un algoritmo que encuentre el polinomio mónico en T, de grado mínimo en T (de hecho, de grado total mínimo),

m_H tal que $m_H(H) \in I$. En [GHM+98], [GHH+97] y [Mor97], en un contexto más general, se obtiene el polinomio buscado a partir de la información que se tiene de una fibra de levantamiento. Para ello, se utiliza una versión simbólica del operador de Newton en varias variables, que obtiene las series formales, en las variables libres, de las variables dependientes (que se anulan en V) si se conoce una solución geométrica de la fibra de levantamiento. El algoritmo opera sobre la matriz compañera de q, siendo esta matriz en nuestro contexto de tamaño $d^n \times d^n$. Por último, en ([HMW99, Theorem 11] y [Wai99]) se refinan las cotas de complejidad en espacio y tiempo de los dos trabajos anteriormente citados.

Un punto de levantamiento z de V es un punto no ramificado: esto significa que el ideal especializado $(F_1(z, X_1, \ldots, X_n), \ldots, F_n(z, X_1, \ldots, X_n))$ es radical en $\mathbb{Q}[X_1, \ldots, X_n]$. Esto implica que la fibra $\pi^{-1}(z)$ sólo contiene puntos lisos. Esto es equivalente a pedir que la matriz jacobiana $(\frac{\partial F_i}{\partial X_j})_{1 \leq i,j \leq n}$, evaluada en cualquier punto de la fibra $\pi^{-1}(z)$, sea inversible. En esta tesis se busca eliminar esta restricción: el algoritmo desarrollado obtiene el polinomio buscado m_H a partir de la fibra correspondiente al origen, que **no** es un punto de levantamiento. Para ello, se calculan los primeros términos de las series de Puiseux (una generalización de las series formales) de las variables dependientes $X_1, \ldots, X_n$ respecto de la variable libre ε. A partir de esta información y mediante una transformación del sistema de polinomios $F_1, \ldots, F_n$ se está en condiciones de aplicar el operador de Newton. El rol que juega la fibra de levantamiento en los algoritmos citados es jugado ahora por la variedad cero–dimensional V' donde V' son los ceros comunes de los polinomios $X_1^d - \alpha_1, \ldots, X_n^d - \alpha_n$. Recordamos que $G_i \in \mathbb{Q}[X_1, \ldots, X_n]$ son los polinomios que definen el sistema de Pham–Brieskorn y $\alpha_i = G_i(0, \ldots, 0) \neq 0$ para todo $1 \leq i \leq n$.

Una idea desarrollada en ([HKP+98], ver también [Wai99]) es la siguiente: supongamos que el polinomio q de la solución geométrica de la fibra de levantamiento se factoriza en s factores no constantes en $\mathbb{Q}[T], q = q_1 \ldots q_s$. En lugar de trabajar con la matriz compañera de q, se trabaja con una matriz semejante, la matriz por bloques formada por las matrices compañeras de $q_1, \ldots, q_s$. Esto produce una mejora en la complejidad en espacio y en tiempo del algoritmo.

Sea $(U, q, v_1, \ldots, v_n)$ una solución geométrica correspondiente a la variedad V', supongamos que q se factoriza en s factores no constantes en $\mathbb{Q}[T]$, $q = q_1 \ldots q_s$, $q_i \in \mathbb{Q}[T]$ y sean $D_i = \deg(q_i)$. Sin pérdida de generalidad suponemos $D_1 \leq D_2 \leq \ldots \leq D_s$. Sea β un straight–line program (sin divisiones esenciales) que computa en espacio $\mathcal{S}$ y tiempo $\mathcal{T}$ a los polinomios $F_1, \ldots, F_n$ del sistema de Pham–Brieskorn (1), a un polinomio $H \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ y a los polinomios $U, q_1, \ldots, q_s, v_1, \ldots, v_n$. El algoritmo desarrollado en esta tesis (ver Teorema 45) es un straight–line program (sin divisiones esenciales) que computa al polinomio minimal m_H con complejidad

asintótica en espacio lineal respecto de $\mathcal{S}$, $D_1^2 + \ldots + D_s^2$ y $\deg(H)^2$ y en tiempo lineal respecto de $\mathcal{T}$, $\max(sD_s^3; s^2D_s^2)$, $\deg(H)^2$ y n^5. En las cotas de complejidad enunciadas se omiten factores logarítmicos.

2 Preliminares

2.1 Modelo computacional

Consideraremos la representación de polinomios multivariados mediante *circuitos aritméticos*.
Sea $\mathbb{Q}(\varepsilon, X_1, \ldots, X_n)$ el cuerpo de las funciones racionales sobre $\mathbb{Q}$ en las variables $\varepsilon, X_1, \ldots, X_n$. Un circuito aritmético β en $\mathbb{Q}(\varepsilon, X_1, \ldots, X_n)$ es un *grafo orientado acíclico* cuyos nodos tienen grado de entrada igual a 0 o 2. Los nodos de grado 0 están etiquetados por elementos de $\mathbb{Q} \cup \{\varepsilon, X_1, \ldots, X_n\}$ y los nodos de grado 2 (llamados *nodos internos*) están etiquetados con alguna de las siguientes operaciones aritméticas: adición, substracción, multiplicación o división. Los nodos de grado cero etiquetados con elementos de $\varepsilon, X_1, \ldots, X_n$ son *nodos input*. Los nodos de grado cero etiquetados con elementos de $\mathbb{Q}$ son *nodos de parámetros*. Finalmente, algunos nodos de β están etiquetados como *nodos output*. Se denota el grafo de computación de β por $\Gamma(\beta)$.

A cada nodo ρ le corresponde una función racional Q_ρ que es el resultado de los pasos anteriores. Dadas s funciones racionales distintas $F_1, \ldots, F_s \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ y β un circuito aritmético en $\mathbb{Q}(\varepsilon, X_1, \ldots, X_n)$ con s nodos output, $F_1, \ldots, F_s$ son *representadas* por β si $F_1, \ldots, F_s$ son las funciones racionales asociadas a los nodos output de β.

En adelante trabajaremos con circuitos aritméticos en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ no conteniendo divisiones esenciales (es decir, sólo divisiones por elementos no nulos de $\mathbb{Q}$).

Se introduce la noción de *pebble game* para modelizar la computación en un circuito aritmético. Un pebble game convierte un circuito aritmético dado en un algoritmo secuencial (llamado también *straight line program*) y se definen medidas de espacio y tiempo asociadas. En el grafo de computación $\Gamma(\beta)$ de un circuito aritmético es posible jugar un pebble game sujeto a las siguientes reglas (ver [Bor93]):

P1 se puede ocupar con una piedra cualquier nodo de grado cero.

P2 si los nodos anteriores a un dado nodo ρ se encuentran ocupados, entonces ρ puede ser ocupado con una piedra nueva o moviendo una piedra de un nodo predecesor.

P3 siempre se puede remover una piedra de un nodo ocupado.

Un pebble game finaliza cuando han sido ocupados todos los nodos output. Observamos que un grafo de computación $\Gamma(\beta)$ no determina un único pebble game.

Asociamos a un dado pebble game las siguientes medidas de complejidad:

C1 una medida del espacio utilizado dada por el máximo número de piedras utilizadas durante el juego.

C2 una medida del tiempo dada por el número de ubicación de piedras durante el juego siguiendo las reglas P1 y P2.

Un pebble game fijo en un grafo de computación $\Gamma(\beta)$ define un algoritmo que llamamos un *straight line program*. Un straight line program en $\mathbb{Q}(\varepsilon, X_1, \ldots, X_n)$ que computa funciones racionales $F_1, \ldots, F_s$ es una secuencia $\beta = (Q_1, \ldots, Q_r)$ de elementos en el cuerpo $\mathbb{Q}(X_1, \ldots, X_n)$ con las siguientes propiedades:

- $\{F_1, \ldots, F_s\} \subseteq \{Q_1, \ldots, Q_r\}$,
- para todo $1 \leq \rho < r$, la función racional Q_ρ pertenece a $Q \cup \{\varepsilon, X_1, \ldots, X_n\}$ o existen $1 \leq \rho_1, \rho_2 < \rho$ y una operación aritmética op_ρ en $\{+, -, \times, \div\}$ tal que vale $Q_\rho = Q_{\rho_1} op_\rho Q_{\rho_2}$.

En adelante trabajaremos con circuitos aritméticos en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ conteniendo divisiones no esenciales (es decir, sólo divisiones por elementos no nulos de $\mathbb{Q}$).

Algunos resultados útiles:

Lema 1 *([HMW99]) Sea R un anillo de polinomios y sea K su cuerpo de cocientes. Sea Y una indeterminada sobre R, sean $q(Y), f(Y)$ y $g(Y)$ polinomios de $R[Y]$. Supongamos que $q(Y)$ es separable y mónico respecto de Y y sea $D := \deg_Y q(Y)$. Supongamos además que $q(Y)$ y $g(Y)$ son coprimos en $K[Y]$ y sea β un straight-line program sin divisiones en R que computa los coeficientes del polinomio $q(Y)$ respecto de la variable Y y evalúa a los polinomios $f(Y)$ y $g(Y)$ respecto de todas las variables (incluída Y) en espacio $\mathcal{S}$ y tiempo $\mathcal{T}$. Entonces existe un straight-line program sin divisiones en R, de espacio $O(\mathcal{S}D)$ y tiempo $O(\mathcal{T}D^2 \log D \log\log D)$, que computa un elemento α distinto de cero en R y los coeficientes de un polinomio $h(Y)$ de $R[Y]$ de grado $\deg_Y h \leq D - 1$ tal que se verifica $g(Y)h(Y) \equiv \alpha f(Y)$ módulo $q(Y)$ en $R[Y]$.*

Para encontrar el polinomio buscado haremos nuestras computaciones en $R[Y]/(q(Y))$, i.e. trabajaremos siempre con los restos módulo $q(Y)$ de los polinomios que aparezcan en cada nodo del straight–line program que encuentra la solución. De esta manera todo polinomio con el que trabajemos tendrá grado (en Y) acotado por

D, podrá ser representado por un straight–line program en R que calcule sus coeficientes, y así mantendremos la complejidad del straight–line program output acotada. Esta técnica, que conocemos como aritmética modular, suele ser útil cuando se quiere mantener acotada la complejidad (o la altura) de las entradas que maneja el algoritmo (ver [BS98]). Notamos también, que para sistemas especiales (e.g. si sabemos que $\deg_Y f \ll D$ y $\deg_Y g \ll D$) podremos agilizar este procedimiento no haciendo todas las computaciones módulo $q(Y)$, sino sólo las necesarias (ver [BS98]).

Demostración.– Calculemos primero a los restos de dividir a $f(Y)$ y a $g(Y)$ por el polinomio $q(Y)$. Llamamos a estos restos $\tilde{f}(Y)$ y $\tilde{g}(Y)$ respectivamente. Computacionalmente lo que hacemos es simular al straight–line program β, que calcula a $f(Y)$ y a $g(Y)$, reemplazando cada nodo (que representa un polinomio en $R[Y]$) por el resto de dividir a este polinomio por $q(Y)$, y guardándolo como un vector de R^D.

De esta manera, los nodos suma son reemplazados de manera obvia: la salida módulo $q(Y)$. Hace falta tener algo más de cuidado con las multiplicaciones. Sean dados dos polinomios $e_1(Y), e_2(Y)$ ya reducidos módulo $q(Y)$, y supongamos que β calcula su producto $(e_1 \cdot e_2)(Y)$. Utilizamos primero un algoritmo basado en FFT para la multiplicación (transformadas rápidas de Fourier, ver [BP94]), y luego el algortimo de Sieveking–Kung basado en inversión de series de potencias formales (ver [Sie72], [BM72] o [BP94]) para la reducción módulo $q(Y)$ obteniendo así un vector en R^D que representa a los coeficientes en la variable principal Y de un polinomio en $R[Y]$ congruente a $(e_1 \cdot e_2)(Y)$ módulo $q(Y)$. Este nuevo straight–line program con el nodo de multiplicación reemplazado usa espacio $O(D)$ y tiempo $O(D^2 \log D \log\log D)$.

Al recorrer todo β haciendo los reemplazos recién expuestos obtenemos un nuevo circuito aritmético sin divisiones que calcula a los coeficentes de $\tilde{f}(Y)$ y $\tilde{g}(Y)$ en espacio a los más $O(\mathcal{S}D)$ y tiempo $O(\mathcal{T}D^2 \log D \log\log D)$.

Como segundo paso calculamos un elemento α de R, y un polinomio $\tilde{h}(Y)$ en $R[Y]$ tales que $\tilde{g}\tilde{h} \equiv \alpha$ módulo $q(Y)$ usando un algoritmo para matrices de tipo Hankel (ver [Sen90] y [SL92]). Obtenemos así un circuito aritmético sin divisiones en R que calcula al elemento α y los coeficientes del polinomio $\tilde{h}(Y)$ en espacio adicional $O(D)$ y tiempo $O(D^2 \log D \log\log D)$.

El elemento α de R de la tesis es aquel ya calculado. Para obtener a $h(Y)$ calculamos al polinomio $(f \cdot \tilde{h})(Y)$ que resulta de multiplicar a los polinomios $f(Y)$ y $\tilde{h}(Y)$ entre si por el método de aritmética modular desarrollado a principios de la demostración. Finalmente notamos que esta computación no altera la complejidad asintótica ya calculada terminando entonces la demostración del Lema.

□

Lema 2 *([HMW99]) Con las notaciones e hipótesis del Lema (1), sea M la matriz compañera del polinomio $q(Y)$. Entonces $g(M)$ es una matriz de $R^{D\times D}$, inversible en el anillo $K^{D\times D}$. Sea N la matriz $N := f(M)g(M)^{-1}$. Entonces existe un straight-line program en R que computa en espacio $O(\mathcal{S}D)$ y tiempo $O((\mathcal{T}+D)D\log D\log\log D)$ los α^D-múltiplos de los coeficientes del polinomio característico $\chi_N(Y)$ de N. En particular, estos α^D-múltiplos de los coeficientes de $\chi_N(Y)$ son elementos de R.*

Supongamos calculado el polinomio característico $\chi_{\alpha N}(Y)$ de la matriz N. Entonces notamos que haciendo la especialización αY en Y obtenemos al polinomio

$$\chi_{\alpha N}(\alpha Y) = \alpha^D \chi_N(Y) \qquad ,$$

terminando el algoritmo.

Para encontrar al polinomio característico $\chi_{\alpha N}(Y)$ de la matriz αN calcularemos primero las trazas $tr(\alpha N), \ldots, tr((\alpha N)^D)$ de las primeras D potencias de la matriz αN y después usamos las relaciones de Newton para obtener los coeficientes de $\chi_{\alpha N}(Y)$, su polinomio característico.

Consideramos en $\mathbb{C}[Z]$ la descomposición del polinomio $q(Z)$ en factores lineales, digamos para establecer la notación

$$q(Z) = \prod_{\ell=1}^{D}(Z - z_\ell) \qquad ,$$

donde $z_1, \ldots, z_D$ son elementos de $\mathbb{C}$. Consideremos además a la derivada formal $q'(Z)$ de $q(Z)$ en la variable Z. Con la notación recién establecida se tiene la identidad

$$q'(Z) = \sum_{\ell=1}^{D}\prod_{\ell\neq k}(Z - z_k) \qquad .$$

Y notamos que $\deg_Z q' = D - 1$.

A partir de estas dos identidades deduciremos congruencias que nos permitirán calcular las trazas de las primeras D potencias de αN efectivamente. Sea $1 \leq \ell \leq D$ fijo, luego se verifica la congruencia

$$Z\prod_{k\neq\ell}(Z - z_k) \equiv z_\ell \prod_{k\neq\ell}(Z - z_k) \quad \text{módulo } q(Z)$$

en $\mathbb{C}[Z]$. Sumando ahora esta congruencia para cada $1 \leq \ell \leq D$ se tiene que

$$Z\sum_{\ell=1}^{D}\prod_{k\neq\ell}(Z - z_k) \equiv \sum_{\ell=1}^{D} z_\ell \prod_{k\neq\ell}(Z - z_k) \quad \text{módulo } q(Z) \quad .$$

Notamos que las dos identidades anteriores son también válidas en $\overline{K}[Z]$. Sea ahora $p(Z)$ un polinomio arbitrario en $R[Z]$. Entonces se sigue la congruencia

$$\begin{aligned} p(Z)q'(Z) &= p(Z)\sum_{\ell=1}^{D}\prod_{k\neq\ell}(Z-z_k) \\ &\equiv \sum_{\ell=1}^{D} p(z_\ell)\prod_{k\neq\ell}(Z-z_k) \quad \text{módulo } q(Z) \end{aligned} \tag{2}$$

en $R[Y]$. De (2) deducimos que la traza $tr(p(M)) = \sum_{\ell=1}^{D} p(z_\ell)$ de la matriz $p(M)$ no es más que el coeficiente principal del resto de dividir a $(p \cdot q')(Z)$ por $q(Z)$.

Para obtener la traza $tr((\alpha N)^\ell) = tr(h(M)^\ell)$ para $1 \leq \ell \leq D$ observamos que esta es exactamente el coeficiente $(D-1)$–ésimo del polinomio obtenido al dividir a $(q' \cdot h^\ell)(Z)$ por el polinomio $q(Z)$.

Enunciemos ahora la forma computacional que generamos a partir de las deducciones en los párrafos precedentes de esta demostración, y los correspondientes cálculos de complejidad. Como primer paso utilizamos el Lema 1 para calcular al elemento α de R y al polinomio $h(Y)$ en $R[Z]$ usando el espacio y el tiempo del enunciado. Recordamos que $q(Z)$ es un polinomio de grado $\deg_Z q(Z) = D$ con coeficientes racionales, luego su derivada $q'(Z)$ puede calcularse sin alterar la complejidad asintótica del procedimiento. Notamos además que el elemento α y los coeficientes de $q(Y)$ y $q'(Y)$ módulo $q(Y)$, que guardaremos durante todo este procedimiento, y los coeficientes de $h(Y)$ que guardamos temporalmente, pueden guardarse en memoria usando espacio $O(D)$.

Calcularemos las distintas trazas recurrentemente. Con la misma táctica usada en la demostración del Lema 1 calculamos al resto de dividir al polinomio $(q' \cdot h)(Y)$ por $q(Y)$. Y guardamos al resultado en la memoria temporalmente, salvo el coeficiente $(D-1)$–ésimo que es la traza $tr(\alpha N)$ que guardamos y no será borrado hasta el final del procedimiento.

En el k–ésimo paso, para $1 \leq k < D$ calculamos, a partir de los coeficientes de $q(Y)$, $q'(Y)$ módulo $q(Y)$ y $(h^k \cdot q')(Y)$, a los coeficientes de $(h^{k+1} \cdot q')(Y)$ módulo $q(Y)$ guardandolos temporariamente y despejando de la memoria temporal los coeficientes de $(h^k \cdot q')(Y)$ (recordemos que el $(D-1)$–ésimo ya fue almacenado como $tr((\alpha N)^k)$). De esta manera encontramos a las trazas $tr(\alpha N), \ldots, tr((\alpha N)^D)$ usando espacio adicional $O(D)$ y en tiempo $O(D^2 \log D \log\log D)$.

Finalmente utilizamos las relaciones de Newton para calcular los coeficientes del polinomio característico $\chi_{\alpha N}(Y)$ de αN sin aumentar la complejidad asintótica del procedimiento. Y luego multiplicamos estos coeficientes por potencias adecuadas de α obteniendo así a los coeficientes del polinomio $\alpha^D \chi_{\alpha N}(Y) = \chi_{\alpha N}(\alpha Y)$, nuevamente sin aumentar la complejidad asintótica del procedimiento. Sumando las

complejidades de la subrutina descrita deducimos que existe un straight–line program que calcula a los coeficientes del polinomio $\alpha^D \chi_N(Y)$ en espacio $O(\mathcal{S}D)$ y tiempo $O(\mathcal{T}D \log D \log\log D + D^2 \log D \log\log D) = O(\mathcal{T}D^2 \log D \log\log D)$.

□

Por otro lado, aplicando las reglas de derivación *(forward mode)* se concluye un resultado del tipo:

Lema 3 *Sea R un dominio y sea β un esquema de evaluación en $R[X_1, \ldots, X_n]$ en espacio $\mathcal{S}$ y tiempo $\mathcal{T}$ que representa la familia de polinomios $\{f_1, \ldots, f_s\} \subset R[X_1, \ldots, X_n]$. En estas condiciones, existe un esquema de evaluación en $R[X_1, \ldots, X_n]$ en espacio $\mathcal{S}+1$ y tiempo $(2n+1)\mathcal{T}$ con los mismos parámetros de β que evalúa $f_1, \ldots, f_s$ y todas sus derivadas parciales de primer orden:*

$$\{\frac{\partial f_i}{\partial X_j} : 1 \leq i \leq s, 1 \leq j \leq n\}.$$

Una técnica importante es la conocida como "Vermeidung von Divisionen" debida a V. Strassen ([Str73]) y permite calcular el cociente de dos polinomios cuando el resultado también es un polinomio. En la proposición es necesario la computación de las componentes homogéneas de un polinomio dado por un esquema de evaluación. Este es el contenido del siguiente Lema:

Lema 4 *Sea $F(X_1, \ldots, X_m)$ un polinomio con coeficientes racionales en las variables $X_1, \ldots, X_m$ de grado $\deg F = D$ que es calculado por un circuito aritmético sin divisiones β en $\mathbb{Q}[X_1, \ldots, X_m]$ en espacio $\mathcal{S}$ y en tiempo $\mathcal{T}$. Entonces existe un circuito aritmético sin divisiones que calcula las componentes homogéneas de $F(X_1, \ldots, X_m)$ en espacio $O(\mathcal{S}D)$ y tiempo $O(\mathcal{T}D \log D \log\log D)$.*

Demostración.– Seguimos la demostración de [Mat97]. Sea Z una nueva indeterminada que consideramos auxiliarmente para la demostración de este Lema. Para encontrar la descomposición de $F(X_1, \ldots, X_m)$ en componentes homogéneas trabajamos en el $\mathbb{Q}(X_1, \ldots, X_m)$–espacio vectorial $\mathbb{Q}(X_1, \ldots, X_m)[Z]/(Z^{D+1})$. Dado un elemento $G \in \mathbb{Q}[X_1, \ldots, X_m][Z]$ denotamos por $\overline{G}$ a la clase de este polinomio en $\mathbb{Q}(X_1, \ldots, X_m)[Z]/(Z^{D+1})$. Notamos que $\mathcal{B} := \{1, Z, \ldots, Z^D\}$ es una base del espacio vectorial en la cual las coordenadas del vector que representa a $\overline{F(ZT_1, \ldots, ZT_m)}$ son exactamente las componentes homogéneas de $F(X_1, \ldots, X_m)$.

Para obtenerlas definimos a η_F la transformación $\mathbb{Q}(X_1, \ldots, X_m)$–lineal inducida por la homotecia por la función regular $\overline{F(ZT_1, , \ldots, ZT_m)}$ en $\mathbb{Q}(X_1, \ldots, X_m)[Z]/(Z^{D+1})$ y consideramos a M_F la matriz de η_F en la base $\mathcal{B}$. Teniendo en cuenta que $\eta_F\left(\overline{1}\right) = F$ deducimos, dado que $\overline{1}$ se escribe como $(1, 0, \ldots, 0) \in \mathbb{Q}(X_1, \ldots, X_m)^{(D+1)\times(D+1)}$,

que las componentes homogéneas de $F(X_1, \ldots, X_m)$ son las entradas que aparecen en la primera columna de la matriz $M_F = F(MT_1, \ldots, MT_m)$.

Para calcular las distintas entradas de la matriz M_F introducimos un nuevo nodo de entrada, y reemplazamos en β las entradas $Y_1, \ldots, Y_m$ por las entradas $ZT_1, \ldots, ZT_m$ obteniendo un nuevo circuito aritmético. Sea M la matriz que representa la homotecia por $\overline{Z}$

$$M = \begin{pmatrix} 0 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \\ & \ddots & \ddots & \vdots \\ 0 & \ldots & 1 & 0 \end{pmatrix} \quad ,$$

luego reemplazamos al nodo de entrada Z por M obteniendo así un circuito aritmético que calcula a la matriz $F(MT_1, \ldots, MT_m)$ de $\mathbb{Q}[X_1, \ldots, X_m]^{(D+1)\times(D+1)}$. En definitiva las únicas operaciones que hace el nuevo circuito aritmético son las que resultan de reemplazar cada nodo de β por una operación de matrices de tamaño $(D+1) \times (D+1)$, que usando técnicas de multiplicación basados en FFT ([BP94]), resultan en los recursos estimados.

□

Lema 5 *([Str73], [HMW99]) Sea $\mathcal{F} := \{F_0, \ldots, F_m\}$ un conjunto finito de polinomios de $\mathbb{Q}[Y_1, \ldots, Y_n]$ de grado a lo sumo δ, computados por un straight-line program β en espacio $\mathcal{S}$ y tiempo $\mathcal{T}$. Supongamos que $F_0 \neq 0$ y tal que F_0 divide a F_i en $\mathbb{Q}[Y_1, \ldots, Y_n]$ para $1 \leq i \leq m$. Entonces existe un straight-line program que calcula los polinomios*

$$P_1 := \frac{F_1}{F_0}, \ldots, P_m := \frac{F_m}{F_0}$$

en espacio $O(\mathcal{S}\delta)$ y tiempo $O((\mathcal{T} + \log\delta)\delta \log\delta \log\log\delta) = O(\mathcal{T}\delta \log^2 \delta \log\log\delta)$.

Demostración.– Sean $g_i(Y_1, \ldots, Y_n) = F_i(Y_1 + t_1, \ldots, Y_n + t_n)$ para $0 \leq i \leq m$ los polinomios que resultan de trasladar a $F_0, \ldots, F_m$ en el punto $t = (t_1, \ldots, t_n)$. Luego, para cada $1 \leq i \leq m$, el polinomio $\frac{F_i}{F_0}(Y_1+t_1, \ldots, Y_n+t_n)$ puede ser calculado como la suma de las primeras $\delta+1$ componentes homogéneas del polinomio $\dfrac{g_i}{\rho} \displaystyle\sum_{k=0}^{\delta} \left(\frac{\rho - g_0}{\rho}\right)^k$.

Este último polinomio puede calcularse usando espacio $O(\mathcal{S})$ y tiempo $O(\mathcal{T} + \log\delta)$. Usando el Lema anterior calculamos sus primeras $\delta + 1$ componentes homogéneas con la complejidad enunciada.

□

Una observación que será útil más adelante es la siguiente:

Observación 6 *Bajo las hipótesis y notación de la proposición anterior con $n = 1$, es decir si*
$F_0, \ldots, F_m$ son polinomios de $\mathbb{Q}[Y_1]$, el straight–line program β anterior calcula la representación densa de los polinomios

$$P_1 := \frac{F_1}{F_0}, \ldots, P_m := \frac{F_m}{F_0}.$$

Lema 7 *([HMW99]) Sea R un anillo de polinomios y sea K su cuerpo de cocientes. Sea β un straight-line program en R que computa los coeficientes de dos polinomios univariados $r(Y)$ y $s(Y) \in R[Y]$ con $s(Y) \neq 0$, en espacio $\mathcal{S}$ y tiempo $\mathcal{T}$. Sean $u(Y), v(Y)$ dos polinomios coprimos de $K[Y]$ que verifican que $\frac{r}{s} = \frac{u}{v}$, $\deg_Y u = D$ y $\deg_Y v \leq D$. Supongamos además que $u(Y)$ es mónico en Y. Entonces existe un straight-line program en R que computa un elemento no nulo $\gamma \in R$ y un γ-múltiplo de los coeficientes de u en espacio $O(\mathcal{S} + D)$ y tiempo $O(\mathcal{T} + D^2 \log D \log\log D)$. En particular, los coeficientes de γu pertenecen a R.*

Demostración.– Sin pérdida de generalidad podemos asumir $r(Y) \neq 0$, sino el resultado es trivial.

Sea dado un elemento $y \in \mathbb{Q}$ tal que $S(y) \neq 0$ (notamos que un tal y puede ser encontrado mediante un test aleatorio de Zippel–Schwartz (ver [Zip79], [Sch80] o [Zip93], también [HS80] y [HS82]), e.g. en el hipercubo $[1, 2D] \cap \mathbb{Z}$ en espacio $\mathcal{S}$ y tiempo $2\mathcal{T}$).

Sea $u(Y) = Y^D + u_{D-1}Y^{D-1} + \cdots + u_0$ donde $u_{D-1}, \ldots, u_0$ son elementos de K. Y sea

$$\frac{v\Big((Y-y)^{-1}\Big)}{(Y-y)u\Big((Y-y)^{-1}\Big)} = \frac{s\Big((Y-y)^{-1}\Big)}{(Y-y)r\Big((Y-y)^{-1}\Big)} = \sum_{i=0}^{+\infty} h_i (Y-y)^i. \tag{3}$$

la representación en serie de potencias formal de la función racional $\frac{v\left((Y-y)^{-1}\right)}{(Y-y)u\left((Y-y)^{-1}\right)}$. Entonces por [BP94, Proposition 2.9.1] se sigue la identidad

$$\begin{pmatrix} h_0 & h_1 & \ldots & h_{\delta-1} \\ h_1 & h_2 & \ldots & h_{\delta} \\ \vdots & \vdots & & \vdots \\ h_{\delta-1} & h_{\delta} & \ldots & h_{2\delta-2} \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{\delta-1} \end{pmatrix} = - \begin{pmatrix} h_{\delta} \\ h_{\delta+1} \\ \vdots \\ h_{2\delta-1} \end{pmatrix} \tag{4}$$

Dado que $r(Y)$ es no nulo, deducimos que los primeros D coeficientes del desarrollo en series de potencias (3) es no nulo, i.e. $(h_0, \ldots, h_{D-1}) \neq 0$. De esta manera aplicamos el algoritmo de Sieveking–Kung para encontrar un elemento ρ de R y

a los elementos $\rho^D h_0, \ldots, \rho^D h_{D-1}$ de R que representan múltiplos por ρ^D de los primeros D coeficientes del desarrollo en series de potencias (3). Notamos que esto puede hacerse en espacio $O(D)$ y en tiempo $O(D \log^2 D \log\log D)$.

Sea $\gamma := \rho^D$, y notemos que el sistema (4) tiene la misma solución que el nuevo sistema que obtenemos al reemplazar las entradas $h_0, \ldots, h_{D-1}$ por sus múltiplos $\gamma h_0, \ldots, \gamma h_{D-1}$, ergo encontremos una solución del nuevo sistema. Dado que la matriz que queda definida es de tipo Hankel, resolvemos al nuevo sistema (o equivalentemente a (4)) usando una ligera variación del procedimiento descripto en [SL92] usando espacio adicional $O(D)$ y en tiempo adicional $O(D^2 \log D \log\log D)$. Aclaramos que mediante dicha variación encontraremos no a la solución exacta, sino al múltiplo $(\gamma u_0, \ldots, \gamma u_{D-1})$ con las mismas cotas asintóticas de complejidad.

□

2.2 Definiciones y resultados geométricos

Sea $V \in \mathbb{A}^n$ una variedad algebraica equidimensional. Si V es cero dimensional se define el *grado geométrico de V* como el número de puntos en V . Supongamos que la dimensión de V es positiva e igual a $r \leq n$. En este caso consideramos la clase $\mathcal{D}$ de subespacios afines de dimensión r.

Definición 8 *Sea $\mathcal{D}_\mathcal{V}$ la subclase de $\mathcal{D}$ de todos los subespacios afines $H \in \mathcal{D}$ tales que $H \cap \mathcal{D}$ es una variedad cero dimensional. Definimos el grado de V como el máximo de los grados de las intersecciones de V con los subespacios afines de la clase $\mathcal{D}_\mathcal{V}$.*

En el caso general, si V es una variedad algebraica y $V = \cup_i C_i$ es una descomposición irredundante de la variedad en componentes irreducibles, se define el grado de V como

$$\deg(V) := \sum_i \deg(C_i).$$

El grado así definido es siempre un número natural positivo. Además verifica la siguiente propiedad conocida como desigualdad de Bézout:

Teorema 9 (Desigualdad de Bézout) *Sean V y W dos variedades algebraicas. Se tiene*

$$\deg(V \cap W) \leq \deg(V).\deg(W).$$

El grado geométrico de una variedad y la desigualdad de Bézout son conceptos desarrollados en [Hei83] (ver también [Ful84]).

Proposición 10 *([GHS93]) Sea k un cuerpo de característica cero, sea $f_1, \ldots, f_r$ una sucesión regular de polinomios en $\mathbf{k}[X_1, \ldots, X_m]$ y supongamos que las variables están en posición de Noether con respecto al ideal $\mathcal{F} = (f_1, \ldots, f_r)$. Supongamos además que $\mathcal{F}$ es un ideal radical. Sea $A := \mathbf{k}[X_1, \ldots, X_r]$ y $\mathcal{B} := \mathbf{k}[X_1, \ldots, X_m]/\mathcal{F}$. Entonces, $\mathcal{B}$ es un A–módulo libre de rango acotado por el grado de la variedad definida por $\mathcal{F}$.*

Finalmente definimos el concepto de solución geométrica de una variedad cero–dimensional.

Definición 11 ([HKP$^+$98]) *Sea k un cuerpo de característica cero, y sea $\bar{k}$ un cuerpo algebraicamente cerrado que contiene al cuerpo k. Sea $n \in \mathbb{N}$. Y sean $X_1, \ldots, X_n, Y$ indeterminadas sobre k. Sean dados polinomios $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ que definen una subvariedad cero–dimensional de $\mathbb{A}^n(\bar{k})$. Una* **solución geométrica** *de la subvariedad cero–dimensional V (o de la extensión $k \to k[V]$) está dada por una forma k–lineal $U = \lambda_1 X_1 + \cdots + \lambda_n X_n \in k[X_1, \ldots, X_n]$ y por $n+1$ polinomios univariados $q, v_1, \ldots, v_n \in k[Y]$ tales que las siguientes condiciones algebraicas y geométricas se cumplen:*

- *el polinomio q es mónico, separable y tiene grado la cardinalidad de V y los grados de $v_1, \ldots, v_n$ son estrictamente menores que la cardinalidad de V, i.e.*

$$\deg q = \#V \qquad y \qquad \deg v_i < \#V \qquad ,$$

- $\{\eta \in \bar{k} : q(\eta) = 0\} = \{U(\xi) : \xi \in V\}$ *y* $V = \{(v_1(\eta), \ldots, v_n(\eta)) : \eta \in \bar{k}$ *y* $q(\eta) = 0\}$.

2.3 Bases de Gröbner

En lo que sigue, F denotará a un anillo de polinomios $\mathbf{k}[Z_1, \ldots, Z_m]$ sobre un cuerpo $\mathbf{k}$. Un *monomio* m de F es un elemento que se puede escribir $m = Z_1^{a_1} \ldots Z_m^{a_m}$ para alguna m–upla $(a_1, \ldots, a_m) \in \mathbb{N}^m$, un *término* de F es un monomio multiplicado por un escalar.

Un ideal $I \subseteq F$ generado por un conjunto de monomios es llamado un *ideal monomial*.
Sean m_1, m_2 dos monomios en F, $m_1 = Z_1^{a_1} \ldots Z_m^{a_m}, m_2 = Z_1^{b_1} \ldots Z_m^{b_m}$, el máximo común divisor entre m_1 y m_2 es el monomio

$$MCD(m_1; m_2) := Z_1^{\min\{a_1; b_1\}} \ldots Z_m^{\min\{a_m; b_m\}}.$$

Definición 12 *Un orden monomial en F es un orden total $>$ en los monomios de F tal que si m_1, m_2 son monomios de F y $n \neq 1$ es un monomio de F, entonces*

$$m_1 > m_2 \text{ implica } nm_1 > nm_2 > m_2.$$

Si $>$ es un orden monomial, entonces para todo $f \in F$ definimos el *término inicial de f*, y lo notamos $M(f)$, al término de f de mayor orden respecto de $>$, y si $I \subseteq F$ es un ideal, definimos $M(I)$ al ideal de F generado por $\{M(f) : f \in I\}$.
Sean m_1, m_2 en F, $m_1 = Z_1^{a_1} \dots Z_m^{a_m}$, $m_2 = Z_1^{b_1} \dots Z_m^{b_m}$, se tienen los siguientes órdenes monomiales:

Orden lexicográfico. $m_1 >_{lex} m_2$ si y sólo si $a_i > b_i$ donde i es el primer índice tal que $a_i \neq b_i$.

Orden lexicográfico homogéneo. $m_1 >_{hlex} m_2$ si y sólo si $\deg(m_1) > \deg(m_2)$ ó $\deg(m_1) = \deg(m_2)$ y $a_i > b_i$ donde i es el primer índice tal que $a_i \neq b_i$.

Si tenemos una secuencia de órdenes parciales $>_1, >_2, \dots$, se define el orden parcial, llamado *producto lexicográfico*, como el orden en el cual $m_1 > m_2$ si existe $i \in \mathbb{N}$ tal que $m_1 >_i m_2$, y para todo $j < i$, m_1 y m_2 no son comparables respecto del orden $>_j$.
Si $I \subseteq F$ es un ideal generado por monomios $m_1, \dots, m_t$, es trivial decidir cuándo un monomio m pertenece a I: esto ocurre si y sólo si m es divisible por algún m_i. Más generalmente, un polinomio $f \in F$ pertenece a un ideal monomial I si y sólo si cada uno de sus monomios pertenece a I.
Un resultado importante es el siguiente:

Teorema 13 *(Macaulay) Sea I un ideal de F, sea $>$ un orden monomial en F, el conjunto B de todos los monomios que no están en M(I) es una base del* $\mathbf{k}$*-espacio vectorial F/I ([Eis95, pages 329]).*

Definición 14 *Sea I un ideal de F. Una base de Gröbner de I respecto de un orden monomial $>$ es un conjunto de polinomios $g_1, \dots, g_t$ tal que:*

i) $\{g_1, \dots, g_t\}$ *genera a I.*

ii) $\{M(g_1), \dots, M(g_t)\}$ *genera a M(I).*

Una base de Gröbner $g_1, \dots, g_t$ tal que $M(g_i)$ no divide a ningún monomio de g_j para todo $i \neq j$ es llamada una base *reducida*.
Más resultados útiles:

Lema 15 *Todo orden monomial en F es Artiniano (todo subconjunto tiene primer elemento)([Eis95, pages 328]).*

Lema 16 *Sea $I = (g_1, \ldots, g_t)$ un ideal de F y $>$ un orden monomial dado. Si $M(g_1), \ldots, M(g_t)$ son coprimos dos a dos, entonces $g_1, \ldots, g_t$ es una base de Gröbner ([Eis95, pages 372]).*

Lema 17 *(Algoritmo de división à la Hironaka) Sea $>$ un orden monomial dado en F, y sean $f, g_1, \ldots, g_t$ polinomios en F. Existen $f', f_1, \ldots, f_t$ en F tal que*

$$f = \sum_{i=1}^{t} f_i g_i + f'$$

donde ninguno de los monomios de f' pertenece al ideal $(M(f_1), \ldots, M(f_t))$. Más aún, $M(f) \geq M(f_i g_i)$ para todo i ([Eis95, pages 334]).

2.4 Teoría de Eliminación

Dadas $Y_1, \ldots, Y_r, Z_1, \ldots, Z_m$ indeterminadas sobre un cuerpo $\mathbf{k}$,
sea $F := \mathbf{k}[Z_1, \ldots, Z_m]$, dado un ideal $I \subseteq F[Y_1, \ldots, Y_r] = \mathbf{k}[Z_1, \ldots, Z_m, Y_1, \ldots, Y_r]$ se quiere calcular $J = I \cap F$.
El significado geométrico de la eliminación es la proyección: dada la variedad algebraica $V \subseteq \mathbf{k}^{m+r}$ definida por los ceros de I, la proyección de V en $\mathbf{k}^m$ es un conjunto cuya clausura (en la topología Zariski) es la variedad definida por los ceros de J.
Para eliminar variables usando bases de Gröbner se trabaja con un orden en $T = \mathbf{k}[Z_1, \ldots, Z_m, Y_1, \ldots, Y_r]$ que verifique:

$$\text{Si } f \in T \text{ y } M(f) \in F, \text{ entonces } f \in F.$$

Un orden con esta propiedad es llamado un *orden de eliminación (respecto de $Y_1, \ldots, Y_r$)*.
Se tiene el siguiente resultado:

Lema 18 *Sea $>$ un orden monomial en $T = F[Y_1, \ldots, Y_r]$, y supongamos que $>$ es un orden de eliminación respecto de las variables $Y_1, \ldots, Y_r$. Si $I \subseteq T$ es un ideal, entonces respecto al orden monomial de F resultante de restringir $>$, tenemos*

$$M(I \cap F) = M(I) \cap F$$

Más aún, si $g_1, \ldots, g_t$ es una base de Gröbner de I, y $g_1, \ldots, g_u$ son los g_i que no contienen variables Y_j, entonces $g_1, \ldots, g_u$ es una base de Gröbner en F de $I \cap F$ ([Eis95, pages 361]).

2.5 Series de Puiseux

El dominio y el cuerpo de las series formales de potencias. Un polinomio sobre un dominio D se define como una suma formal finita, $a_0 + a_1X + \ldots + a_nX^n$, donde los coeficientes a_i pertenecen al dominio D y X es una indeterminada sobre D. Si se permiten sumas infinitas de este tipo, $a_0+a_1X+\ldots+a_nX^n+\ldots$ se obtiene un conjunto llamado las series formales de potencias sobre D y se nota $D[|X|]$. Dos series se suman y multiplican de la misma manera que dos polinomios, y $D[|X|]$ resulta un dominio.
Sea $\mathbf{k}$ un cuerpo, sea $\mathbf{k}((X))$ el cuerpo de fracciones de $\mathbf{k}[|X|]$. Se prueba que los elementos de $\mathbf{k}((X))$ son series formales de potencias con un finito número de términos con exponente negativo.

El cuerpo $\mathbf{k}(X)^*$ de las series de potencia fraccionarias. Consideramos para cada $n \in \mathbb{N}$ el cuerpo $\mathbf{k}((X^{1/n}))$. Sea $\mathbf{k}(X)^* := \bigcup_{n\in\mathbb{N}} \mathbf{k}((X^{1/n}))$ el conjunto formado por la unión de los cuerpos $\mathbf{k}((X^{1/n}))$. Si $\bar{x}, \bar{y}$ son dos elementos de $\mathbf{k}(X)^*$, entonces existen $n, m \in N$ tal que $\bar{x} \in \mathbf{k}((X^{1/n})), \bar{y} \in \mathbf{k}((X^{1/m}))$. Por lo tanto, $\bar{x}, \bar{y} \in \mathbf{k}((X^{1/nm}))$ y también su suma, producto y cociente (si $\bar{y} \neq 0$). Se sigue que $\mathbf{k}(X)^*$ es un cuerpo. Los elementos de $\mathbf{k}(X)^*$ se llaman *series de Puiseux* de X en $\mathbf{k}$.
Un elemento $\bar{r}$ de $\mathbf{k}(X)^*$ tiene una única escritura de tipo $\sum_{j=z_0}^{\infty} a_j X^{j/n}$ donde $z_0 \in \mathbb{Z}, n \in \mathbb{N}, \mathrm{a_j} \in \mathbf{k}$ y $a_{z_0} \neq 0$. Se define el *orden* de $\bar{r}$ como el número z_0/n y se lo nota $O(\bar{r})$.

Sea $\mathbb{C}(\varepsilon)^*$ el cuerpo de las series de Puiseux de ε en $\mathbb{C}$, sea d en $\mathbb{N}$, sea $\mathbb{C}[|\varepsilon^{1/d}|] \subset \mathbb{C}(\varepsilon)^*$ el anillo de las series formales en $\varepsilon^{1/d}$. Este anillo es completo respecto de $\mathcal{M} = (\varepsilon^{1/d})$, su único ideal maximal. Se tiene la siguiente versión del Lema de Hensel ([Eis95, pages 210]):

Proposición 19 *Sean $f_1, \ldots, f_n \in \mathbb{C}[|\varepsilon^{1/d}|][X_1, \ldots, X_n]$, sea $J(x)$ la matriz jacobiana*

$$J(x) = (\partial f_i / \partial X_j),$$

sea $\bar{a} = (\bar{a}_1, \ldots, \bar{a}_n) \in \mathbb{C}[|\varepsilon^{1/d}|]^n$ y supongamos que $\det(J(\bar{a}))$ es una unidad en $\mathbb{C}[|\varepsilon^{1/d}|]$. Si

$$f_i(\bar{a}) \in \mathcal{M} \text{ para } 1 \leq i \leq n,$$

entonces existe un único elemento $\bar{b} = (\bar{b}_1, \ldots, \bar{b}_n) \in \mathbb{C}[|\varepsilon^{1/d}|]^n$ tal que $f_i(\bar{b}) = 0$ para $1 \leq i \leq n$ y $\bar{b}_i - \bar{a}_i \in \mathcal{M}$ para $1 \leq i \leq n$.

Para mayor información sobre series de Puiseux, ver ([Wal78]).

3 Un algoritmo para el cálculo de un polinomio minimal

Sean $G_1, \ldots, G_n$ polinomios en $\mathbb{Q}[X_1, \ldots, X_n]$, sea d en $\mathbb{N}$ tal que $d > \deg(G_i)$ para $1 \leq i \leq n$. Consideramos el sistema de Pham–Brieskorn en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$:

$$\begin{cases} F_1(\varepsilon, X_1, \ldots, X_n) = X_1^d - \varepsilon G_1(X_1, \ldots, X_n) \\ \vdots \\ F_n(\varepsilon, X_1, \ldots, X_n) = X_n^d - \varepsilon G_n(X_1, \ldots, X_n) \end{cases} \tag{5}$$

Supongamos que para cada $1 \leq i \leq n$, $\alpha_i := G_i(0, \ldots, 0)$ es no nulo.

Notación 20 *Para $i = 1, \ldots, n, k = 1, \ldots, d$ enumeramos con $a_i^{(k)}$ a las raíces d–ésimas de α_i en $\mathbb{C}$.*

Consideramos $F_1, \ldots, F_n$ como polinomios de $\mathbb{C}(\varepsilon)^*[X_1, \ldots, X_n]$. Las siguientes dos proposiciones caracterizan a las series de Puiseux en ε que se anulan en los polinomios $F_1, \ldots, F_n$.

Proposición 21 *Sean $\bar{r}_1, \ldots, \bar{r}_n \in \mathbb{C}(\varepsilon)^*$ tales que para $i = 1, \ldots, n$ se verifica la siguiente identidad en $\mathbb{C}(\varepsilon)^*$:*

$$F_i(\bar{r}_1, \ldots, \bar{r}_n) = 0$$

Entonces existe una n–upla $a_1^{(k_1)}, \ldots, a_n^{(k_n)}$ de raíces d–ésimas de $\alpha_1, \ldots, \alpha_n$ respectivamente tal que $O(\bar{r}_i) = 1/d$ y $O(\bar{r}_i - a_i^{(k_i)}\varepsilon^{1/d}) > 1/d$.

Demostración.– Dado que para $1 \leq i \leq n$ vale
$0 = F_i(\bar{r}_1, \ldots, \bar{r}_n) = \bar{r}_i^d - \varepsilon G_i(\bar{r}_1, \ldots, \bar{r}_n)$,
se tiene que $\bar{r}_i^d = \varepsilon G_i(\bar{r}_1, \ldots, \bar{r}_n)$ para $1 \leq i \leq n$.
Queremos ver que $O(\bar{r}_i) \geq 0$:

Supongamos que no. Sea i_0 tal que $O(\bar{r}_{i_0}) = \min\{O(\bar{r}_i)\} < 0$. Dado que por hipótesis, $d > \deg(G_{i_0})$ y que estamos suponiendo $O(\bar{r}_{i_0})$ negativo se tienen las desigualdades

$$O(\bar{r}_{i_0}^d) = dO(\bar{r}_{i_0}) < \deg(G_{i_0})O(\bar{r}_{i_0}) < \deg(G_{i_0})O(\bar{r}_{i_0}) + 1 \leq O(\varepsilon G_{i_0}(\bar{r}_1, \ldots, \bar{r}_n)).$$

Pero esto es absurdo pues $O(\bar{r}_{i_0}^d) = O(\varepsilon G_{i_0}(\bar{r}_1, \ldots, \bar{r}_n))$.
Como $O(\bar{r}_i) \geq 0$ para todo i, se tiene que $O(\varepsilon G_i(\bar{r}_1, \ldots, \bar{r}_n)) \geq 1$ y por lo tanto $O(\bar{r}_i^d) = d.O(\bar{r}_i) = O(\varepsilon G_i(\bar{r}_1, \ldots, \bar{r}_n)) \geq 1$. Es decir que $O(\bar{r}_i) \geq 1/d$ para todo i.

Ahora bien, si $O(\bar{r}_i) \geq 1/d > 0$ para todo i, el orden de $\varepsilon G_i(\bar{r}_1, \ldots, \bar{r}_n)$ es igual a 1 pues $G_i(0, \ldots, 0) = \alpha_i \neq 0$ por hipótesis. El término de menor orden de $\varepsilon G_i(\bar{r}_1, \ldots, \bar{r}_n)$ resulta entonces ser $\alpha_i \varepsilon$. Puesto que $0 = \bar{r}_i^d - \varepsilon G_i(\bar{r}_1, \ldots, \bar{r}_n)$, el orden de $\bar{r}_i^d$ es 1 y su término de menor orden es igual a $\alpha_i \varepsilon$, y por lo tanto el término de menor orden de $\bar{r}_i$ es igual a $a_i^{(k_i)} \varepsilon^{1/d}$ para alguna raíz d–ésima $a_i^{(k_i)}$ de α_i, que era lo que se quería probar.

□

Proposición 22 *Dada una n–upla $a_1^{(k_1)}, \ldots, a_n^{(k_n)}$ de raíces d–ésimas de $\alpha_1, \ldots, \alpha_n$ respectivamente existen únicas $\bar{r}_1, \ldots, \bar{r}_n$ en $\mathbb{C}(\varepsilon)^*$ que verifican las siguientes condiciones:*

- $O(\bar{r}_i) = 1/d$ *para* $1 \leq i \leq n$.
- $O(\bar{r}_i - a_i^{(k_i)} \varepsilon^{1/d}) > 1/d$ *para* $1 \leq i \leq n$.
- $F_i(\bar{r}_1, \ldots, \bar{r}_n) = 0$.

Además, $\bar{r}_1, \ldots, \bar{r}_n$ pertenecen a $\mathbb{C}[|\varepsilon^{1/d}|]$.

Demostración.– Dada una n–upla $a_1^{(k_1)}, \ldots, a_n^{(k_n)}$ se definen los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n} \in \mathbb{C}(\varepsilon)^*[X_1, \ldots, X_n]$ de la siguiente manera:

$$\begin{cases} \widetilde{F_1}(X_1, \ldots, X_n) = (F_1((X_1 + a_1^{(k_1)})\varepsilon^{1/d}, \ldots, (X_n + a_n^{(k_n)})\varepsilon^{1/d}))\varepsilon^{-1} \\ \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ \widetilde{F_n}(X_1, \ldots, X_n) = (F_n((X_1 + a_1^{(k_1)})\varepsilon^{1/d}, \ldots, (X_n + a_n^{(k_n)})\varepsilon^{1/d}))\varepsilon^{-1} \end{cases}$$

Estos polinomios pertenecen a $\mathbb{C}[\varepsilon^{1/d}][X_1, \ldots, X_n]$ pues $\widetilde{F_i} = (F_i((X_1 + a_1^{(k_1)})\varepsilon^{1/d}, \ldots, (X_n + a_n^{(k_n)})\varepsilon^{1/d}))\varepsilon^{-1} = (((X_i + a_i^{(k_i)})\varepsilon^{1/d})^d - \varepsilon G_i((X_1 + a_1^{(k_1)})\varepsilon^{1/d}, \ldots, (X_n + a_n^{(k_n)})\varepsilon^{1/d})))\varepsilon^{-1} = (X_i + a_i^{(k_i)})^d - G_i((X_1 + a_1^{(k_1)})\varepsilon^{1/d}, \ldots, (X_n + a_n^{(k_n)})\varepsilon^{1/d}))$.

Afirmación: Evaluando los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$ en el origen $0 = (0, \ldots, 0) \in \mathbb{C}[|\varepsilon^{1/d}|]^n$ se tiene que :

i) $O(\widetilde{F_i}(0)) \geq 1/d$ para $1 \leq i \leq n$.

ii) $\det(D\widetilde{F})(0)$ es inversible en $\mathbb{C}[|\varepsilon^{1/d}|]$.

El polinomio $\widetilde{F_i}$, evaluado en $(0,\ldots,0)$ resulta:

$$\widetilde{F_i}(0,\ldots,0) = (F_i((0+a_1^{(k_1)})\varepsilon^{1/d},\ldots,(0+a_n^{(k_n)})\varepsilon^{1/d}))\varepsilon^{-1} =$$

$$= (((0+a_i^{(k_i)})\varepsilon^{1/d})^d - \varepsilon G_i((0+a_1^{(k_1)})\varepsilon^{1/d},\ldots,(0+a_n^{(k_n)})\varepsilon^{1/d}))\varepsilon^{-1} =$$

$$= (a_i^{(k_i)})^d - G_i(a_1^{(k_1)}\varepsilon^{1/d},\ldots,a_n^{(k_n)}\varepsilon^{1/d})$$

Dado que $(a_i^{(k_i)})^d = \alpha_i$ y que $O(G_i(a_1^{(k_1)}\varepsilon^{1/d},\ldots,a_n^{(k_n)}\varepsilon^{1/d}) - \alpha_i) \geq 1/d$, se tiene la primer afirmación.
La derivada parcial de $\widetilde{F_i}$ respecto de X_j es

$$\frac{\partial}{\partial X_j}\widetilde{F_i} = \frac{\partial}{\partial X_j}(X_i + a_i^{(k_i)})^d - \frac{\partial}{\partial X_j}G_i((X_1+a_1^{(k_1)})\varepsilon^{1/d},\ldots,(X_n+a_n^{(k_n)})\varepsilon^{1/d}) =$$

$$= \delta_{i,j}d(X_i+a_i^{(k_i)})^{d-1} - \frac{\partial}{\partial X_j}G_i(a_1^{(k_1)}\varepsilon^{1/d},\ldots,a_n^{(k_n)}\varepsilon^{1/d})\varepsilon^{1/d}$$

Donde $\delta_{i,j}$ vale 1 si $i=j$ y 0 en otro caso. Evaluada en $0=(0,\ldots,0)$ resulta

$$\frac{\partial}{\partial X_j}\widetilde{F_i}(0) = \delta_{i,j}d(a_i^{(k_i)})^{d-1} - \frac{\partial}{\partial X_j}G_i(a_1^{(k_1)},\ldots,a_n^{(k_n)})\varepsilon^{1/d}$$

En particular se tiene que $O(\frac{\partial}{\partial X_j}\widetilde{F_i}(0)) = 0$ si $i=j$ y $O(\frac{\partial}{\partial X_j}\widetilde{F_i}(0)) \geq 1/d$ si $i \neq j$. Por lo tanto, $O(\det(D\widetilde{F})(0) - d^n\prod_{i=1}^n(a_i^{(k_i)})^{d-1}) \geq 1/d$. Dado que $d^n\prod_{i=1}^n(a_i^{(k_i)})^{d-1}$ es distinto de cero, se sigue que $\det(D\widetilde{F})(0)$ es inversible en $\mathbb{C}[|\varepsilon^{1/d}|]$, que es lo que queríamos demostrar.

De acuerdo a la Proposición 19, existe un único elemento $\widetilde{r} = (\widetilde{r_1},\ldots,\widetilde{r_n}) \in \mathbb{C}[|\varepsilon^{1/d}|]^n$ tal que

$$O(\widetilde{r_i}) \geq 1/d \text{ y } \widetilde{F}_i(\widetilde{r_1},\ldots,\widetilde{r_n}) = 0 \text{ para } 1 \leq i \leq n.$$

Definimos $\bar{r} = (\bar{r}_1,\ldots,\bar{r}_n) := ((a_1^{(k_1)}+\widetilde{r_1})\varepsilon^{1/d},\ldots,(a_n^{(k_n)}+\widetilde{r_n})\varepsilon^{1/d}) \in \mathbb{C}[|\varepsilon^{1/d}|]^n$. $\bar{r}$ es el único elemento de $\mathbb{C}[|\varepsilon^{1/d}|]^n$ que verifica las condiciones enunciadas, es decir:

- $O(\bar{r}_i) = 1/d$ para $1 \leq i \leq n$.
- $O(\bar{r}_i - a_i^{(k_i)}\varepsilon^{1/d}) > 1/d$ para $1 \leq i \leq n$.
- $F_i(\bar{r}_1,\ldots,\bar{r}_n) = 0$.

Resta probar la unicidad de la solución en $(\mathbb{C}(\varepsilon)^*)^n$. Sea $\bar{y} = (\bar{y}_1, \ldots, \bar{y}_n) \in (\mathbb{C}(\varepsilon)^*)^n$ una serie que verifica lo pedido. Existe $m \in \mathbb{N}$ tal que $\bar{y} \in \mathbb{C}[|\varepsilon^{1/m}|]^n$ y por lo tanto $\bar{y}, \bar{r} \in \mathbb{C}[|\varepsilon^{1/md}|]^n$. Ahora bien, los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$ pertenecen a $\mathbb{C}[\varepsilon^{1/md}][X_1, \ldots, X_n]$ y el origen $(0, \ldots, 0) \in \mathbb{C}[|\varepsilon^{1/md}|]^n$ sigue verificando las hipótesis de la Proposición 19, esta vez en el anillo $\mathbb{C}[|\varepsilon^{1/md}|]^n$. Puesto que esta Proposición garantiza unicidad de la solución, se sigue entonces que $\bar{y} = \bar{r}$.

□

Como consecuencia de las dos proposiciones anteriores se tiene que hay en total d^n raíces $\bar{r}^{(i)} = (\bar{r}_1^{(i)}, \ldots, \bar{r}_n^{(i)})$ en $\mathbb{C}[|\varepsilon^{1/d}|]^n$ del ideal $(F_1, \ldots, F_n)$ y quedan unívocamente determinadas por su primer n–upla: la coordenada j–ésima de $\bar{r}^{(i)}$ se escribe $\bar{r}_j^{(i)} = a_j^{(k_i)}\varepsilon^{1/d} +$ términos de orden superior a $1/d$, donde $a_j^{(k_i)}$ es una raíz d–ésima de α_j. La proposición siguiente será necesaria para probar la radicalidad del ideal generado por $F_1, \ldots, F_n$ en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$.

Proposición 23 *Sea D un dominio, $d \in \mathbb{N}$, p un polinomio en $D[X_1, \ldots, X_n]$ tal que para $1 \leq i \leq n$, $\deg_{X_i} p < d$ y sean, para $1 \leq i \leq n, 1 \leq k \leq d$, elementos $\xi_i^{(k)} \in D$ tales que $\xi_i^{(k)} \neq \xi_i^{(k')}$ para $k \neq k'$ y $p(\xi_1^{(k_1)}, \ldots, \xi_n^{(k_n)}) = 0$ para toda n–upla $(\xi_1^{(k_1)}, \ldots, \xi_n^{(k_n)})$. Entonces p es el polinomio nulo.*

Demostración.– Se prueba por inducción en la cantidad de variables n. Si $n = 1$, se tiene que p es un polinomio en $D[X_1]$ de grado menor que d y con d raíces, por lo que $p = 0$.
Supongamos que vale para $n = h$, sea $n = h + 1$:
Sea $p = \sum_{i=0}^{d-1} a_i X_{h+1}^i, a_i \in D[X_1, \ldots, X_h]$ su escritura respecto de la variable $Xh + 1$. Evaluando las primeras h variables en una h–upla $(\xi_1^{(k_1)}, \ldots, \xi_h^{(k_h)})$ se tiene un polinomio en $D[X_{h+1}]$, de grado menor que d y con d raíces, por lo que $a_i(\xi_1^{(k_1)}, \ldots, \xi_h^{(k_h)}) = 0$ para $0 \leq i < d$. Aplicando la hipótesis inductiva en los polinomios a_i se sigue que p es el polinomio nulo.

□

Definición 24 *Sea $>$ el orden monomial en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ que es producto lexicográfico del orden parcial definido por el grado total en $X_1, \ldots, X_n$ y el orden lexicográfico donde $X_1 > \ldots > X_n > \varepsilon$.*

Con este orden, para cada $1 \leq i \leq n$, el término inicial de F_i es $M(F_i) = X_i^d$.

Proposición 25 *El ideal $I = (F_1, \ldots, F_n)$ generado por los polinomios del sistema de Pham–Brieskorn en (1) es radical en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$.*

Demostración.– Supongamos al contrario que exista $f \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n], m \in \mathbb{N}$ tal que $f \notin I$ y $f^m \in I$. Sea $>$ el orden monomial en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ dado en la Definición 24. Por el algoritmo de división de Hironaka (ver Lema 17), existen $g_1, \ldots, g_n, r \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ tal que $f - \sum_{i=1}^n g_i F_i = r$ y ningún término de r pertenece al ideal $(M(F_1), \ldots, M(F_n)) = (X_1^d, \ldots, X_n^d)$. Es decir que todo término $aX_1^{w_1}, \ldots, X_1^{w_1}\varepsilon^w$ de r verifica que $w_i < d$ para $1 \leq i \leq n$. Por otra parte, dado que $r \equiv f$ módulo I, y $f^m \equiv 0$ módulo I, se tiene que $r^m \equiv 0$ módulo I.
Sea $\bar{r}^{(i)} \in \mathbb{C}[|\varepsilon^{1/d}|]^n$ una n–upla de series de Puiseux que anula a los polinomios de I (ver Proposiciones 21 y 22), se tiene entonces que $r^m(\bar{r}^{(i)}) = 0$ en $\mathbb{C}[|\varepsilon^{1/d}|]$ y, dado que $\mathbb{C}[|\varepsilon^{1/d}|]$ es un dominio, se tiene que $r(\bar{r}^{(i)}) = 0$ en $\mathbb{C}[|\varepsilon^{1/d}|]$.
Escribimos $r = \sum_j p_j$, donde los términos $m = a_m X_1^{m_1} \ldots X_n^{m_n}\varepsilon^{\widetilde{m}}$ de p_j verifican $\frac{1}{d}\sum_{i=1}^n m_i + \widetilde{m} = j$. Sea $j_0 := \min\{j : p_j \neq 0\}$.

Afirmación: Pensamos al polinomio p_{j_0} en el anillo $\mathbb{C}[|\varepsilon^{1/d}|][X_1, \ldots, X_n]$; dada una n–upla $a_1^{(k_1)}, \ldots, a_n^{(k_n)}$ de raíces d–ésimas de $\alpha_1, \ldots, \alpha_n$ se tiene que
$p_{j_0}(a_1^{(k_1)}\varepsilon^{1/d}, \ldots, a_n^{(k_n)}\varepsilon^{1/d}) = 0$ en $\mathbb{C}[|\varepsilon^{1/d}|]$.

El polinomio p_{j_0}, evaluado en $a_1^{(k_1)}\varepsilon^{1/d}, \ldots, a_n^{(k_n)}\varepsilon^{1/d}$, ó bien es un elemento de $\mathbb{C}[|\varepsilon^{1/d}|]$ de orden j_0, ó bien es el elemento nulo. Sabemos de la Proposición 22 que, dada una n–upla $a_1^{(k_1)}, \ldots, a_n^{(k_n)}$ existen $\bar{r}_1, \ldots, \bar{r}_n$ en $\mathbb{C}[|\varepsilon^{1/d}|]$ tales que $r(\bar{r}_1, \ldots, \bar{r}_n) = 0$ y $\bar{r}_i = a_i^{(k_i)}\varepsilon^{1/d} +$ términos de orden superior. Dado que $O(r - p_{j_0})(\bar{r}_1, \ldots, \bar{r}_n) > j_0$ y $O(p_{j_0}(\bar{r}_1, \ldots, \bar{r}_n) - p_{j_0}(a_1^{(k_1)}\varepsilon^{1/d}, \ldots, a_n^{(k_n)}\varepsilon^{1/d})) > j_0$ se concluye de $r(\bar{r}_1, \ldots, \bar{r}_n) = 0$ que vale
$p_{j_0}(a_1^{(k_1)}\varepsilon^{1/d}, \ldots, a_n^{(k_n)}\varepsilon^{1/d}) = 0$ en $\mathbb{C}[|\varepsilon^{1/d}|]$.
Ahora bien, el polinomio $p_{j_0} \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ verifica que $\deg_{X_i}(p_{j_0}) < d$ para $1 \leq i \leq n$ y se anula en las n–uplas $a_1^{(k_1)}\varepsilon^{1/d}, \ldots, a_n^{(k_n)}\varepsilon^{1/d}$. Pensando al polinomio p_{j_0} en el anillo de polinomios $\mathbb{C}[|\varepsilon^{1/d}|][X_1, \ldots, X_n]$, la Proposición 23 nos permite concluir que p_{j_0} es el polinomio nulo, pero esto es absurdo pues $j_0 = \min\{j : p_j \neq 0\}$.
□

Sea $V \in \mathbb{A}^{n+1}$ la variedad algebraica afín definida por los ceros de $I = (F_1, \ldots, F_n)$, el sistema de Pham definido en (1). Observamos que V es no vacía pues el origen pertenece a V. Sea B el ágebra $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]/I$. De la Proposición 25 el ideal I es radical, y B resulta el anillo de coordenadas de V.
Recordamos la definición de orden monomial dada en 24:
Sea $>$ el orden monomial en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ que es producto lexicográfico del orden parcial definido por el grado total en $X_1, \ldots, X_n$ y el orden lexicográfico donde $X_1 > \ldots > X_n > \varepsilon$.
Notar que este orden verifica que si $f \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ y $M(f) \in \mathbb{Q}[\varepsilon]$, entonces $f \in \mathbb{Q}[\varepsilon]$, por lo tanto es un orden de eliminación respecto de $X_1, \ldots, X_n$.
Con este orden, para cada $1 \leq i \leq n$, el término inicial de F_i es $M(F_i) = X_i^d$.

Proposición 26 *Bajo las hipótesis y notación anteriores se verifica:*

i) El conjunto $G = \{F_1, \ldots, F_n\}$ *es una base de Gröbner reducida de* I *para el orden monomial definido anteriormente y* $M(I) = (X_1^d, \ldots, X_n^d)$.

ii) El morfismo

$$\pi : V \longrightarrow \mathbb{A}^1$$
$$\pi(\tau, \xi_1, \ldots, \xi_n) = \tau$$

es finito, es decir que las variables están en posición de Noether respecto de V.

iii) V *es una curva.*

iv) $F_1, \ldots, F_n$ *es una sucesión regular en* $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$.

v) $\deg(V) = d^n$.

Demostración.– i) Los polinomios $F_1, \ldots, F_n$ generan I y los monomios $M(F_i) = X_i^d$ son coprimos dos a dos; del Lema 16 se sigue que G es una base de Gröbner de I. Dado que G es una base de Gröbner, $M(I) = (M(F_1), \ldots, M(F_n)) = (X_1^d, \ldots, X_n^d)$. Puesto que $X_i^d > M(F_j - X_j^d)$ y X_i^d, X_j^d son coprimos dos a dos para $i \neq j$, se tiene que X_i^d no divide a ningún monomio de F_j, y por lo tanto G es una base de Gröbner reducida.

ii) Por definición, el morfismo π es finito si $\pi(V)$ es denso en $\mathbb{A}^1$ y el morfismo de anillos asociado

$$\pi^* : \mathbb{Q}[\varepsilon] \longrightarrow B$$

es entero. La clausura de $\pi(V)$ es igual a la variedad V_ε definida por el ideal $J_\varepsilon = I \cap \mathbb{Q}[\varepsilon]$ en $\mathbb{Q}[\varepsilon]$. Queremos ver entonces que V_ε es $\mathbb{A}^1$:

Sea $F = \mathbb{Q}[\varepsilon], T = \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$. $>$ es un orden de eliminación respecto de $X_1, \ldots, X_n$ y $G = \{F_1, \ldots, F_n\}$ es una base de Gröbner de $(F_1, \ldots, F_n)$. Por el Lema 18, tenemos que $M(J_\varepsilon) = (X_1^d, \ldots, X_n^d) \cap \mathbb{Q}[\varepsilon]$. Ahora bien, $(X_1^d, \ldots, X_n^d) \cap \mathbb{Q}[\varepsilon] = \{0\}$ por lo que $J_\varepsilon = \{0\}$ y entonces la variedad $V_\varepsilon = V(J_\varepsilon) = \mathbb{A}^1$.

Dado que B es una $\mathbb{Q}[\varepsilon]-$ ágebra finitamente generada, B es entero sobre $\pi^*(\mathbb{Q}[\varepsilon]) \simeq \mathbb{Q}[\varepsilon]$ si y sólo si B es finito como $\mathbb{Q}[\varepsilon]-$ módulo ([AM69]). De acuerdo al Teorema 13, el conjunto E formado por los monomios de $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ que no pertenecen al ideal monomial $M(I)$ es una base del $\mathbb{Q}-$ espacio vectorial

$\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]/I$. Ahora bien, un monomio m pertenece a $M(I)$ si y sólo si es divisible por algún X_i^d. Es decir que E se escribe

$$E = \{m \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n] : m = X_1^{a_1} \ldots X_n^{a_n}.\varepsilon^b, a_i < d\}.$$

Por lo tanto, el conjunto $D = \{m \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n] : m = X_1^{a_1} \ldots X_n^{a_n}, a_i < d\}$ es una base de $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]/I$ como $\mathbb{Q}[\varepsilon]-$ módulo y además es un conjunto finito.

iii) Dado que $\pi : V \longrightarrow \mathbb{A}^1$ es un morfismo entero, tenemos que $\dim(V) = \dim(\mathbb{A}^1) = 1$. Ahora bien, no hay componentes de dimensión menor pues V es una variedad en $(n+1)$ variables generada por n polinomios, por lo que toda componente tiene dimensión $\geq (n+1) - n = 1$. Concluímos entonces que todas las componentes tienen dimensión 1.

iv) Para $1 \leq k < n$, sean $I_k = (F_1, \ldots, F_k)$. Igual que en *i)* se prueba que $F_1, \ldots, F_k$ es una base de Gröbner reducida de I_k, y entonces $M(I_k) = (M(F_1), \ldots, M(F_k)) = = (X_1^d, \ldots, X_k^d)$. Por definición, $F_1, \ldots, F_n$ es sucesión regular en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ si para $1 \leq k < n$, el polinomio F_{k+1} no es divisor de cero de $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]/I_k$. Sea $C := \{g \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n] : g.F_{k+1} \in I_k \text{ y } g \notin I_k\}$. El conjunto C es vacío si y sólo si el polinomio F_{k+1} no es divisor de cero del álgebra $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]/I_k$. Supongamos por el contrario que $C \neq \emptyset$:

Sea g_0 un elemento de C, de orden mínimo entre todos los elementos de C, respecto del orden monomial definido en 24, es decir que $M(g_0) = \min\{M(g) : g \in C\}$. Existe un tal g_0 pues todo subconjunto de $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ tiene primer elemento respecto de un orden monomial $>$ fijo (ver Lema 15). Se tiene que
$M(g_0.F_{k+1}) = M(g_0)M(F_{k+1}) = X_{k+1}^d M(g_0) \in M(I_k)$. Al ser $M(I_k)$ un ideal generado por monomios, un monomio pertenece al mismo si y sólo si es divisible por algún monomio generador. Calculamos el máximo común divisor entre los términos iniciales de F_i y F_{k+1}:
$MCD(M(F_{k+1}); M(F_i)) = MCD(X_{k+1}^d; X_i^d) = 1$ para $1 \leq i \leq k$ resulta entonces que $M(g_0.F_{k+1}) \in I_k$ implica que $M(g_0) \in M(I_k)$. Sea $h \in I_k$ tal que $M(g_0) = M(h)$. Se tiene que $(g_0 - h)F_{k+1} \in I_k$ y $M(g_0 - h) < M(g_0) = \min\{M(g) : g \in C\}$. Si $g_0 - h \in I_k$, entonces $g_0 \in I_k$, lo cual es falso, y si $g_0 - h \notin I_k$, entonces $g_0 - h \in C$, pero esto es absurdo pues $M(g_0 - h) < M(g_0)$.

v) De la desigualdad de Bézout y de la observación de que el grado de una hipersuperficie es igual al grado del polinomio que la define, se deduce que, al ser V una variedad definida por la sucesión regular $F_1, \ldots, F_n$ de grado d, se tiene que $\deg(V) \leq d^n$. La otra desigualdad se deduce de la Proposición 10:
En nuestro caso, $F_1, \ldots, F_n$ es una sucesión regular en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$, $A = \mathbb{Q}[\varepsilon]$, $\mathcal{B} = B$, el ideal $(F_1, \ldots, F_n)$ es radical en $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ (ver Proposición 25) y

las variables se encuentran en posición de Noether, así que tenemos la desigualdad $\deg(V) \geq \#D = d^n$ donde D es la base obtenida en $ii)$.

□

Observación 27 *El punto $0 \in \mathbb{A}^{n+1}$ es un punto singular de la variedad V y es el único elemento de la fibra $\pi^{-1}(0)$.*

Sea H un polinomio perteneciente a $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$. Dado que el morfismo de anillos $\mathbb{Q}[\varepsilon] \longrightarrow B$ es entero, existe un único polinomio m_H en $\mathbb{Q}[\varepsilon][T]$, mónico en T y de grado mínimo en T, tal que $m_H(H) = 0$ en B.

Tenemos la siguiente cota para el grado total de m_H :

Proposición 28 *([SS96]) Sea $\mathcal{F}$ en $\mathbf{k}[X_1, \ldots, X_m]$ un ideal radical, V:=V($\mathcal{F}$) y supongamos que la dimensión de V es r y que las variables están en posición de Noether. Sea $A := \mathbf{k}[X_1, \ldots, X_r]$ y $B := \mathbf{k}[X_1, \ldots, X_m]/\mathcal{F}$ y sea $f \in \mathbf{k}[X_1, \ldots, X_m]$. Entonces, existe un polinomio mónico $F \in A[T]$ que verifica que $F(f) = 0$ en B y cuyo grado total está acotado por* $\deg(V).\deg(f)$.

En nuestro caso, $\mathbf{k} = \mathbb{Q}$, $\mathcal{F} = I$, la variedad V tiene dimensión 1 y $A = \mathbb{Q}[\varepsilon]$. Entonces, dado $H \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$, el polinomio $m_H \in \mathbb{Q}[\varepsilon][T]$ tiene grado total acotado por $d^n.\deg(H)$.

Observación 29 *El grado en la variable T de m_H está acotado por el grado de V.*

Esto se debe a que B es un $\mathbb{Q}[\varepsilon]$ - módulo de rango igual al grado geométrico de V.

Recordamos que a partir de las Proposiciones 21 y 22 se tienen exactamente d^n n–uplas $\bar{r}^{(i)}$ en $\mathbb{C}[|\varepsilon^{1/d}|]^n$ que se anulan en los polinomios $F_1, \ldots, F_n$. Cada coordenada $r_j^{(i)}$ de la n–upla $\bar{r}^{(i)} = (r_1^{(i)}, \ldots, r_n^{(i)})$ se escribe $r_j^{(i)} = a_j^{(k_i)}\varepsilon^{1/d} + R_{i,j}$ donde $a_j^{(k_i)}$ es una raíz d–ésima de α_j y $O(R_{i,j}) > 1/d$.
Dado que hay una cantidad finita de n–uplas que se anulan en los polinomios $F_1, \ldots, F_n$, existe $U = \sum_{k=1}^n \lambda_k X_k \in \mathbb{Q}[X_1, \ldots, X_n]$ una forma lineal tal que $U(\bar{r}^{(i)}) \neq U(\bar{r}^{(j)})$ para n–uplas distintas $\bar{r}^{(i)}, \bar{r}^{(j)}$. Existe una tal forma lineal, una manera de probarlo es utilizando la siguiente afirmación:
Afirmación: Dado $m \in \mathbb{N}$, sean $P_1, \ldots, P_m$ elementos distintos de $\mathbb{C}^n$. Existe una forma lineal $U = \sum_{k=1}^n \lambda_k X_k \in \mathbb{Q}[X_1, \ldots, X_n]$ tal que $U(P_i) \neq U(P_j)$ para $P_i \neq P_j$.

Dada una forma lineal $U = \sum_{k=1}^n \lambda_k X_k \in \mathbb{Q}[X_1, \ldots, X_n]$, evaluar U en un elemento $P \in \mathbb{C}^n$ es igual a hacer el producto interno usual de $\mathbb{C}^n$ entre P y $\lambda = (\lambda_1, \ldots, \lambda_n)$. Pedir que $U(P_i) \neq U(P_j)$ para $P_i \neq P_j$ es equivalente a pedir que $U(P_i) - U(P_j) \neq 0$ para $P_i \neq P_j$ y puesto que $U(P_i) - U(P_j) = U(P_i - P_j)$ es el producto interno entre

los vectores $\lambda = (\lambda_1, \ldots, \lambda_n)$ y $P_i - P_j$, esto es equivalente a pedir que el vector $(\lambda_1, \ldots, \lambda_n)$ no sea perpendicular a los vectores $P_i - P_j$ para todo par i, j distintos. Fijando $i \neq j$, el conjunto $W_{i,j} := \{w \in \mathbb{C}^n :< w; (P_i - P_j) >= 0\}$ de vectores perpendiculares al vector $P_i - P_j$ es un subespacio lineal cerrado de dimensión $n-1$, y su complemento es un abierto denso de $\mathbb{C}^n$. La unión finita de subespacios de dimensión $n-1$ es un cerrado incluído estrictamente en $\mathbb{C}^n$, y su complemento es un abierto denso de $\mathbb{C}^n$. Puesto que $\mathbb{Q}^n$ también es un conjunto denso en $\mathbb{C}^n$, existe $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Q}^n$ que no pertenece a $W_{i,j}$ para todo par $i \neq j$ y por lo tanto la forma lineal $U = \sum_{k=1}^n \lambda_k X_k \in \mathbb{Q}[X_1, \ldots, X_n]$ verifica que $U(P_i) \neq U(P_j)$ para $P_i \neq P_j$.

Sean $P_1, \ldots, P_{d^n} \in \mathbb{C}^n$ todas las n–uplas tales que sus coordenadas son raíces d–ésimas de $\alpha_1, \ldots, \alpha_n$ respectivamente. Sea $U = \sum_{k=1}^n \lambda_k X_k \in \mathbb{Q}[X_1, \ldots, X_n]$ una forma lineal tal que $U(P_i) \neq U(P_j)$ para $P_i \neq P_j$, entonces $U(\bar{r}^{(i)}) \neq U(\bar{r}^{(j)})$ para n–uplas distintas $\bar{r}^{(i)}, \bar{r}^{(j)}$.

Sea $m_u \in \mathbb{Q}[\varepsilon][T]$ el polinomio mónico en T y de grado mínimo en T tal que $m_u(U) \in I$. Este polinomio existe y tiene grado en T acotado por d^n; esto es consecuencia de la Proposición 26. Existen $g_1, \ldots, g_n \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ tal que

$$m_u(U) = \sum_{i=1}^n g_i F_i \text{ en } \mathbb{Q}[\varepsilon, X_1, \ldots, X_n].$$

Evaluando esta igualdad en las n–uplas $\bar{r}^{(i)}$ para $1 \leq i \leq d^n$ se tiene

$$m_u(U)(\bar{r}^{(i)}) = m_u(U((\bar{r}^{(i)}))) = 0 \text{ en } \mathbb{C}[|\varepsilon^{1/d}|].$$

Dado que $U((\bar{r}^{(i)})) \neq U((\bar{r}^{(i)}))$ para n–uplas distintas se tienen d^n raíces de m_u en $\mathbb{C}[|\varepsilon^{1/d}|]$ y son todas por la cota de grado de m_u. Puesto que $\mathbb{C}[|\varepsilon^{1/d}|][T]$ es un dominio de factorización única, m_u se factoriza

$$m_u = \prod_{k=1}^{d^n} (T - U((\bar{r}^{(k)}))) \text{ en } \mathbb{C}[|\varepsilon^{1/d}|][T].$$

La forma lineal U permite obtener una base del $\mathbb{Q}(\varepsilon)$ - espacio vectorial $B' :=$
$= \mathbb{Q}(\varepsilon) \otimes_{\mathbb{Q}[\varepsilon]} B$ de la siguiente manera: siendo u la imagen de U en B', el conjunto de las potencias $P := \{1, u, \ldots, u^{d^n-1}\}$ es una base. Sean $v_1, \ldots, v_n \in \mathbb{Q}[\varepsilon][T]$ tal que $X_i - v_i(u) \in B$. El grado de cada polinomio v_i está acotado por $d^n - 1$.
Consideramos la homotecia $\mathbb{Q}[\varepsilon]$ - lineal η en B correspondiente a multiplicar por u. Se sigue que la matriz M de η en la base P es la matriz compañera del polinomio m_u. Los autovalores de esta matriz son las raíces del polinomio m_u. Por lo tanto, existe una base P' de la $\mathbb{C}(\varepsilon)^*$ - álgebra $\mathbb{C}(\varepsilon)^*[X_1, \ldots, X_n]/(F_1, \ldots, F_n)$ tal que la matriz M' de la homotecia η tiene la forma

$$M' = \begin{pmatrix} u(\bar{r}^{(1)}) & 0 & \dots & 0 \\ 0 & u(\bar{r}^{(2)}) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & u(\bar{r}^{(d^n)}) \end{pmatrix}$$

Para $1 \leq i \leq n$ consideramos las homotecias η_{X_i} inducidas por la multiplicación por la clase de X_i en B. Sean $M_{X_i} \in \mathbb{Q}(\varepsilon)^{d^n \times d^n}$ las matrices correspondientes a estas homotecias en la base P. Dado un polinomio $H \in \mathbb{Q}[\varepsilon, X_1, \dots, X_n]$, sea η_H la homotecia asociada y M_H la matriz de η_H en la base P. Puesto que B es un álgebra conmutativa, se sigue que las homotecias $\eta_{X_1}, \dots, \eta_{X_n}$ y por lo tanto las matrices $M_{X_1}, \dots, M_{X_n}$ conmutan entre sí. Esto implica que $\eta_H = H(\eta_{X_1}, \dots, \eta_{X_n})$, $M_H = H(M_{X_1}, \dots, M_{X_n})$.
La igualdad de ideales $I = (m_u(U), X_1 - v_1(U), \dots, X_n - v_n(U))$ en $\mathbb{Q}(\varepsilon)[X_1, \dots, X_n]$ implica las siguientes identidades:

$$\eta_{X_1} = v_1(\eta), \dots, \eta_{X_n} = v_n(\eta),$$
$$M_{X_1} = v_1(M), \dots, M_{X_n} = v_n(M).$$

Entonces, para cualquier polinomio H de $\mathbb{Q}[\varepsilon, X_1, \dots, X_n]$ vale que:

$$\eta_H = H(v_1(\eta), \dots, v_n(\eta)),$$

$$M_H = H(v_1(M), \dots, v_n(M)).$$

Por lo tanto, la matriz M_H es semejante a la matriz

$$M'_H = \begin{pmatrix} H(v_1(u(\bar{r}^{(1)})), \dots, v_n(u(\bar{r}^{(1)}))) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & H(v_1(u(\bar{r}^{(d^n)})), \dots, v_n(u(\bar{r}^{(d^n)}))) \end{pmatrix}$$
$$= \begin{pmatrix} H(\bar{r}^{(1)}) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & H(\bar{r}^{(d^n)}) \end{pmatrix}$$

Sea $q \in \mathbb{Q}(\varepsilon)[T]$ el polinomio característico de M_H y $\mu \in \mathbb{Q}(\varepsilon)[T]$ su polinomio minimal. Se tiene la siguiente observación:

Observación 30 *Los polinomios q y μ pertenecen a $\mathbb{Q}[\varepsilon][T]$.*

Demostración.– Sea $m_H \in \mathbb{Q}[\varepsilon][T]$ el polinomio mónico en T y de grado mínimo en T tal que $m_H(H) \in I$. Notamos que $m_H(M_H) = M_{m_H(H)} = 0$ y por lo tanto μ divide a m_H. Puesto que los polinomios m_H y μ son mónicos deducimos del Lema de Gauss que μ pertenece a $\mathbb{Q}[\varepsilon][T]$ y también q.

□

Sea $q \in \mathbb{Q}[\varepsilon][T]$ el polinomio característico de M_H. Por el teorema de Cayley-Hamilton se tiene que la matriz $q(M_H) = M_{q(H)}$ es la matriz nula y, puesto que la matriz $M_{q(H)}$ es la matriz de la homotecia $\eta_{q(H)}$ en la base P, se deduce que el polinomio $q(H)$ pertenece a I. Dado que B es un álgebra reducida, el polinomio minimal de M_H es el polinomio minimal de H en B. Hemos probado entonces la siguiente proposición:

Proposición 31 *Con la notación anterior, sea* $q := \prod_{k=1}^{d^n}(T - H(\bar{r}^{(k)}))$ *en* $\mathbb{C}(\varepsilon)^*[T]$. *Entonces,* q *pertenece a* $\mathbb{Q}[\varepsilon][T]$ *y* $q(H) = 0$ *en* B. *Más aun, el polinomio* $m_H := q/MCD(q; q')$ *es el polinomio minimal buscado.*

Idea de lo que sigue : Queremos encontrar las series de Puiseux de las variables $(X_1, \ldots, X_n)$ respecto de ε. Dado que la fibra correspondiente al cero está compuesta por un punto singular, debemos hacer algunas cuentas a mano. Más concretamente, encontraremos el primer término de cada serie, y después de un cambio de variables, estaremos en condiciones de aplicar el operador de Newton.

Sean $B_1, \ldots, B_n$ indeterminadas sobre $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$,
sean $\widetilde{F_1}, \ldots, \widetilde{F_n} \in \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)(\varepsilon^{1/d})[X_1, \ldots, X_n]$ definidos de la siguiente manera:

$$\begin{cases} \widetilde{F_1} = (F_1((X_1 + B_1)\varepsilon^{1/d}, \ldots, (X_n + B_n)\varepsilon^{1/d}))\varepsilon^{-1} \\ \qquad\qquad \vdots \\ \widetilde{F_n} = (F_n((X_1 + B_1)\varepsilon^{1/d}, \ldots, (X_n + B_n)\varepsilon^{1/d}))\varepsilon^{-1} \end{cases} \tag{6}$$

Los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n} \in \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)(\varepsilon^{1/d})[X_1, \ldots, X_n]$ "representan", de alguna manera, a los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n} \in \mathbb{C}[\varepsilon^{1/d}][X_1, \ldots, X_n]$ definidos en la Proposición 22 pues las indeterminadas $B_1, \ldots, B_n$ son raíces d–ésimas de $\alpha_1, \ldots, \alpha_n$ en el anillo $\mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)$.

Observación 32 *Los polinomios* $\widetilde{F_1}, \ldots, \widetilde{F_n}$ *pertenecen a* $\mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)[\varepsilon^{1/d}][X_1, \ldots, X_n]$.

Demostración.– Los polinomios están en
$\mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)[\varepsilon^{1/d}][X_1, \ldots, X_n]$ pues
$\widetilde{F_i} = (F_i((X_1 + B_1)\varepsilon^{1/d}, \ldots, (X_n + B_n)\varepsilon^{1/d}))\varepsilon^{-1} = (((X_i + B_i)\varepsilon^{1/d})^d - \varepsilon G_i((X_1 + B_1)\varepsilon^{1/d}, \ldots, (X_n + B_n)\varepsilon^{1/d})))\varepsilon^{-1} = (X_i + B_i)^d - G_i((X_1 + B_1)\varepsilon^{1/d}, \ldots, (X_n + B_n)\varepsilon^{1/d}))$.

Definición 33 *Sea $\mathcal{R}$ el anillo semilocal $\mathbb{Q}[B_1,\ldots,B_n]/(B_1^d-\alpha_1,\ldots,B_n^d-\alpha_n)[|\varepsilon^{1/d}|]$.*

Un elemento f de $\mathcal{R}$ es una serie formal en $\varepsilon^{1/d}$, con coeficientes en $\mathbb{Q}[B_1,\ldots,B_n]/(B_1^d-\alpha_1,\ldots,B_n^d-\alpha_n)$. f se escribe entonces $\sum_{k=k_0}^{\infty} a_k\varepsilon^{k/d}$ donde $k_0\geq 0$ y $a_{k_0}\neq 0$. Se define el *orden de f* como el número racional k_0/d.
Via la inclusión $\mathbb{Q}[B_1,\ldots,B_n]/(B_1^d-\alpha_1,\ldots,B_n^d-\alpha_n)[\varepsilon^{1/d}]\hookrightarrow\mathcal{R}$ se puede pensar a los polinomios $\widetilde{F_i}$ en $\mathcal{R}[X_1,\ldots,X_n]$.

Observación 34 *Sea $g\in\mathcal{R}$ inversible, sea $f\in\mathcal{R}$ tal que $O(f-g)>0$, entonces f es inversible en $\mathcal{R}$.*

Demostración.– f tiene una escritura de tipo $\sum_{k=0}^{\infty} a_k\varepsilon^{k/d}$ donde $a_k\in\mathbb{Q}[B_1,\ldots,B_n]/(B_1^d-\alpha_1,\ldots,B_n^d-\alpha_n)$. Dado que $O(f-g)>0$, resulta a_0 el término constante de la escritura de g como serie de potencias de $\varepsilon^{1/d}$. Puesto que g es inversible en $\mathcal{R}$, a_0 es inversible en $\mathbb{Q}[B_1,\ldots,B_n]/(B_1^d-\alpha_1,\ldots,B_n^d-\alpha_n)$. Definimos b_k recursivamente:
$b_0=a_0^{-1}$
$b_k=-a_0^{-1}\sum_{j=0}^{k-1} a_{k-j}b_j$ si $k\geq 1$
Se prueba inductivamente que $b_k\in\mathbb{Q}[B_1,\ldots,B_n]/(B_1^d-\alpha_1,\ldots,B_n^d-\alpha_n)$ y que $\sum_{k=0}^{\infty} b_k\varepsilon^{k/d}$ es el inverso de f.

Observación 35 *El vector $0=(0,\ldots,0)\in\mathcal{R}^n$ verifica:*

i) $O(\widetilde{F_i}(0))\geq 1/d$ *para* $1\leq i\leq n$.

ii) $\det(D\widetilde{F})(0)$ *es inversible en $\mathcal{R}$ y por lo tanto $D(\widetilde{F})(0)$ es inversible en $\mathcal{R}^{n\times n}$.*

Demostración.– El polinomio $\widetilde{F_i}$, evaluado en 0 resulta:

$$\widetilde{F_i}(0)=(F_i((0+B_1)\varepsilon^{1/d},\ldots,(0+B_n)\varepsilon^{1/d}))\varepsilon^{-1}=$$

$$=(((0+B_i)\varepsilon^{1/d})^d-\varepsilon G_i((0+B_1)\varepsilon^{1/d},\ldots,(0+B_n)\varepsilon^{1/d}))\varepsilon^{-1}=$$

$$=(B_i)^d-G_i((B_1)\varepsilon^{1/d},\ldots,(B_n)\varepsilon^{1/d})$$

Dado que $B_i^d=\alpha_i$ y que $O(G_i((B_1)\varepsilon^{1/d},\ldots,(B_n)\varepsilon^{1/d})-\alpha_i)\geq 1/d$, se tiene la primer afirmación.
La derivada parcial de $\widetilde{F_i}$ respecto de X_j es

$$\frac{\partial}{\partial X_j}\widetilde{F_i}=\frac{\partial}{\partial X_j}(X_i+B_i)^d-\frac{\partial}{\partial X_j}G_i((X_1+B_1)\varepsilon^{1/d},\ldots,(X_n+B_n)\varepsilon^{1/d})=$$

$$= \delta_{i,j} d(X_i + B_i)^{d-1} - \frac{\partial}{\partial X_j} G_i(B_1\varepsilon^{1/d}, \ldots, B_n\varepsilon^{1/d})\varepsilon^{1/d},$$

donde $\delta_{i,j}$ vale 1 si $i = j$ y 0 en otro caso. Evaluada en 0 resulta

$$\frac{\partial}{\partial X_j}\widetilde{F_i}(0) = \delta_{i,j} d B_i^{d-1} - \frac{\partial}{\partial X_j} G_i(B_1, \ldots, B_n)\varepsilon^{1/d}$$

En particular se tiene que $O(\frac{\partial}{\partial X_j}\widetilde{F_i}(0)) = 0$ si $i = j$ y $O(\frac{\partial}{\partial X_j}\widetilde{F_i}(0)) \geq 1/d$ si $i \neq j$ y por lo tanto

$$O(\det(D\widetilde{F})(0) - d^n \prod_{i=1}^{n} B_i^{d-1}) \geq 1/d. \tag{7}$$

$d^n \prod_{i=1}^n B_i^{d-1}$ es inversible en $\mathcal{R}$ pues B_i es inversible en $\mathcal{R}$ para todo i, y se sigue de la Observación 34 que $\det(D\widetilde{F})(0)$ es inversible en $\mathcal{R}$. Esto implica que $D(\widetilde{F})(0)$ es inversible en $\mathcal{R}^{n\times n}$ y su inversa es la matriz

$$(\det(D\widetilde{F}))(0))^{-1} Adj(D(\widetilde{F}))(0).$$

□

4 Operador de Newton sin divisiones

Recordamos la definición de los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$ $\in \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)[\varepsilon^{1/d}][X_1, \ldots, X_n]$ dada en la sección anterior,

$$\begin{cases} \widetilde{F_1} = (F_1((X_1 + B_1)\varepsilon^{1/d}, \ldots, (X_n + B_n)\varepsilon^{1/d}))\varepsilon^{-1} \\ \qquad\qquad \vdots \\ \widetilde{F_n} = (F_n((X_1 + B_1)\varepsilon^{1/d}, \ldots, (X_n + B_n)\varepsilon^{1/d}))\varepsilon^{-1} \end{cases}$$

Recordamos también que definimos el anillo $\mathcal{R} := \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)[[\varepsilon^{1/d}]]$ y que podemos pensar a los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$ en $\mathcal{R}[X_1, \ldots, X_n]$. Sea $\widetilde{F} := (\widetilde{F_1}, \ldots, \widetilde{F_n})$ y sea $D(\widetilde{F}) := (\frac{\partial \widetilde{F_i}}{\partial X_j})_{1\leq i,j\leq n}$ la matriz jacobiana de los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$. Suponiendo que esta matriz es regular y considerando los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$ como funciones racionales en $(X_1, \ldots, X_n)$, se define el siguiente operador de Newton–Hensel:

$$N_{\widetilde{F}}(X_1, \ldots, X_n) := \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} - D(\widetilde{F})^{-1} \begin{pmatrix} \widetilde{F_1}(X_1, \ldots, X_n) \\ \vdots \\ \widetilde{F_n}(X_1, \ldots, X_n) \end{pmatrix}.$$

Se tiene la siguiente versión del Lema de Hensel ([Mat97]):

Lema 36 *Existen únicas series de potencias $R_1, \ldots, R_n$ en $\mathcal{R}$ que verifican las siguientes condiciones:*

- *Para $i = 1, \ldots, n$ vale la siguiente identidad en $\mathcal{R}$:*

$$\widetilde{F_i}(R_1, \ldots, R_n) = 0.$$

- *Para $i = 1, \ldots, n$ vale que $O(R_i) \geq 1/d$.*

Demostración.– Se define la siguiente sucesión en $\mathcal{R}^n$:

$$R^{(0)} := (0, \ldots, 0)$$

$$R^{(N+1)} := N_{\widetilde{F}}(R^{(N)})^t \text{ para } N \geq 0$$

donde A^t denota la matriz transpuesta de A. Obsérvese que de la definición de $R^{(N)}$, por medio de un argumento inductivo se deduce que cada $R_j^{(N)}$ representa una función racional de $\mathbb{Q}(\varepsilon^{1/d}, X_1, \ldots, X_n)$.
Se nota por $\mathcal{M}$ el ideal $\mathcal{M} := (\varepsilon^{1/d})$ generado por $\varepsilon^{1/d}$ en $\mathcal{R}$. Entonces las siguientes afirmaciones son válidas para todo $N \in \mathbb{N}$:

i) $\widetilde{F_i}(R^{(N)})) \in \mathcal{M}^{2^N}$ para $1 \leq i \leq n$.

ii) $\det(D(\widetilde{F}))(R^{(N)})$ es un elemento inversible de $\mathcal{R}$ y por lo tanto $R^{(N+1)}$ está bien definido.

Estas afirmaciones se demuestran por inducción en N. En el caso $N = 0$, las afirmaciones i) e ii) se probaron en la Observación 35.
En el caso general, suponiendo ambas afirmaciones ciertas para el caso N, veamos que se verifican para el caso $N+1$. Sean $Y_1, \ldots, Y_n$ nuevas indeterminadas. A partir de un desarrollo formal de Taylor de los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$ en torno a $Y_1, \ldots, Y_n$ se obtiene la siguiente identidad en $\mathcal{R}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$:

$$\begin{gathered}\widetilde{F_i}(X_1, \ldots, X_n) = \widetilde{F_i}(Y_1, \ldots, Y_n) + \textstyle\sum_{j=1}^n \frac{\partial \widetilde{F_i}}{\partial X_j}(Y_1, \ldots, Y_n).(X_j - Y_j) \\ \text{módulo } (X_1 - Y_1, \ldots, X_n - Y_n)^2\end{gathered} \tag{8}$$

para $i = 1, \ldots, n$, donde $(X_1 - Y_1, \ldots, X_n - Y_n)$ denota el ideal generado por los polinomios $X_1 - Y_1, \ldots, X_n - Y_n$ en $\mathcal{R}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$.
Reemplazando en la ecuación (8) las variables $X_1, \ldots, X_n$ por $R_1^{(N+1)}, \ldots, R_n^{(N+1)}$ e $Y_1, \ldots, Y_n$ por $R_1^{(N)}, \ldots, R_n^{(N)}$, se obtiene la siguiente identidad en $\mathcal{R}$:

$$\begin{array}{c}\widetilde{F_i}(R^{(N+1)}) = \widetilde{F_i}(R^{(N)}) + \sum_{j=1}^{n} \frac{\partial \widetilde{F_i}}{\partial X_j}(R^{(N)}).(R_j^{(N+1)} - R_j^{(N)}) \\ \text{módulo } (R_1^{(N+1)} - R_1^{(N)}, \ldots, R_n^{(N+1)} - R_n^{(N)})^2\end{array} \tag{9}$$

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

$$R^{(N+1)} - R^{(N)} = -D(\widetilde{F})^{-1}(R^{(N)}). \begin{pmatrix} \widetilde{F}_1(R^{(N)}) \\ \vdots \\ \widetilde{F}_n(R^{(N)}) \end{pmatrix}$$

En consecuencia, multiplicando ambos miembros de esta identidad por el vector $(\frac{\partial \widetilde{F_i}}{\partial X_1}(R^{(N)}), \ldots, \frac{\partial \widetilde{F_i}}{\partial X_n}(R^{(N)}))$, que constituye la i–ésima fila de la matriz $D(\widetilde{F})(R^{(N)})$, se tiene la siguiente ecuación:

$$(\frac{\partial \widetilde{F_i}}{\partial X_1}(R^{(N)}), \ldots, \frac{\partial \widetilde{F_i}}{\partial X_n}(R^{(N)})).(R^{(N+1)} - R^{(N)})^t =$$

$$(\frac{\partial \widetilde{F_i}}{\partial X_1}(R^{(N)}), \ldots, \frac{\partial \widetilde{F_i}}{\partial X_n}(R^{(N)})).(-D(\widetilde{F})^{-1}(R^{(N)})). \begin{pmatrix} \widetilde{F}_1(R^{(N)}) \\ \vdots \\ \widetilde{F}_n(R^{(N)}) \end{pmatrix} =$$

$$= -(0, \ldots, \overbrace{1}^{i}, 0, \ldots, 0). \begin{pmatrix} \widetilde{F}_1(R^{(N)}) \\ \vdots \\ \widetilde{F}_n(R^{(N)}) \end{pmatrix} = -\widetilde{F}_i(R^{(N)})$$

Por lo tanto, reemplazando esta última identidad en (9) se obtiene:

$$\widetilde{F}_i(R^{(N+1)}) = \widetilde{F}_i(R^{(N)}) +$$

$$+(\frac{\partial \widetilde{F_i}}{\partial X_1}(R^{(N)}), \ldots, \frac{\partial \widetilde{F_i}}{\partial X_n}(R^{(N)})).(-D(\widetilde{F})^{-1}(R^{(N)})). \begin{pmatrix} \widetilde{F}_1(R^{(N)}) \\ \vdots \\ \widetilde{F}_n(R^{(N)}) \end{pmatrix} =$$

$$= \widetilde{F}_i(R^{(N)}) - \widetilde{F}_i(R^{(N)}) = 0$$

$$\text{módulo } (R_1^{(N+1)} - R_1^{(N)}, \ldots, R_n^{(N+1)} - R_n^{(N)})^2$$

de donde se deduce que

$$\widetilde{F}_i(R^{(N+1)}) \in (R_1^{(N+1)} - R_1^{(N)}, \ldots, R_n^{(N+1)} - R_n^{(N)})^2$$

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

$$(R^{(N+1)} - R^{(N)}))^t = -D(\widetilde{F})^{-1}(R^{(N)}).\begin{pmatrix} \widetilde{F}_1(R^{(N)}) \\ \vdots \\ \widetilde{F}_n(R^{(N)}) \end{pmatrix}$$

y $\widetilde{F}_i(R^{(N)}) \in \mathcal{M}^{2^N}$ para $i = 1, \ldots, n$ por hipótesis inductiva, resulta entonces que

$$(R_1^{(N+1)} - R_1^{(N)}, \ldots, R_n^{(N+1)} - R_n^{(N)})^2 \subseteq (\mathcal{M}^{2^N})^2 = \mathcal{M}^{2^{N+1}}$$

lo que demuestra i).
Con respecto a la segunda afirmación, realizando un desarrollo de Taylor formal del polinomio $\det(D(\widetilde{F}))$ como en (8), se obtiene la siguiente expresión:

$$\det(D(\widetilde{F}))(X_1, \ldots, X_n) = \det(D(\widetilde{F}))(Y_1, \ldots, Y_n) +$$

$$+\sum_{j=1}^{n} \frac{\partial \det(D(\widetilde{F}))}{\partial X_j}(Y_1, \ldots, Y_n).(X_j - Y_j) \text{ módulo } (X_1 - Y_1, \ldots, X_n - Y_n)^2 \quad (10)$$

Si se reemplaza en esta ecuación, del mismo modo que en (9), las variables $X_1, \ldots, X_n$ por $R_1^{(N+1)}, \ldots, R_n^{(N+1)}$ y las variables $Y_1, \ldots, Y_n$ por $R_1^{(N)}, \ldots, R_n^{(N)}$ se obtiene la siguiente identidad:

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

$$+\sum_{j=1}^{n} \frac{\partial \det(D(\widetilde{F}))}{\partial X_j}(R^{(N)}).(R_j^{(N+1)} - R_j^{(N)})$$

$$\text{módulo } (R_1^{(N+1)} - R_1^{(N)}, \ldots, R_n^{(N+1)} - R_n^{(N)})^2$$

Dado que se verifica que $R_j^{(N+1)} - R_j^{(N)} \in \mathcal{M}^{2^N} \subseteq \mathcal{M}$ para $j = 1, \ldots, n$ y $\det(D(\widetilde{F}))(R^{(N)})$ es inversible en $\mathcal{R}$ por hipótesis, se deduce de la observación (34) que $\det(D(\widetilde{F}))(R^{(N+1)})$ también es inversible en $\mathcal{R}$.
De las afirmaciones i) e ii) se desprende que la sucesión $\{R_j^{(N)}\}_{N \in \mathbb{N}}$ converge en $\mathcal{R}$ a una serie de potencias R_j para $j = 1, \ldots, n$. Estas son las series de potencias cuya existencia afirma el enunciado del Lema.
Denótese por R el vector de series de potencias $R := (R_1, \ldots, R_n)$. En primer lugar, dado que $R_j^{(N+1)} - R_j^{(N)} \in \mathcal{M}^{2^N}$ para todo $N \in \mathbb{N}$, se deduce que

$$R_j \equiv R_j^{(N)} \text{ módulo } \mathcal{M}^{2^N} \text{ para todo } N \in \mathbb{N} \quad (11)$$

Combinando esta observación con la ecuación (8), se tiene que

$$\widetilde{F}_i(R) = \widetilde{F}_i(R^{(N)}) + D(\widetilde{F})(R^{(N)}).\begin{pmatrix} R_1 - R_1^{(N)} \\ \vdots \\ R_n - R_n^{(N)} \end{pmatrix} \text{ módulo } \mathcal{M}^{2^N}$$

para $i = 1, \ldots, n$, de donde se deduce que $\widetilde{F}_i(R) \in \mathcal{M}^{2^N}$ para todo $N \in \mathbb{N}$. Luego

$$\widetilde{F}_i(R) = 0 \text{ en } R$$

para $i = 1, \ldots, n$, que era lo que se quería demostrar.
Por otra parte, de (11) y de que $(R_1^{(0)}, \ldots, R_n^{(0)}) = (0, \ldots, 0)$ se sigue que $O(R) \geq 1/d$.
En cuanto a la unicidad, suponiendo que existiera otra solución distinta $\widetilde{R} = (\widetilde{R}_1, \ldots, \widetilde{R}_n)$ en las condiciones del enunciado, es decir que se anula en $\widetilde{F}$ y para $i = 1, \ldots, n$ vale que $O(\widetilde{R_i}) \geq 1/d$, aplicando una vez más la expresión (8) se obtiene:

$$\widetilde{F}_i(R) = \widetilde{F}_i(\widetilde{R}) + D(\widetilde{F})(\widetilde{R}).\begin{pmatrix} R_1 - \widetilde{R}_1 \\ \vdots \\ R_n - \widetilde{R}_n \end{pmatrix}$$

$$\text{módulo } (R_1 - \widetilde{R}_1, \ldots, R_n - \widetilde{R}_n)^2$$

Como $\widetilde{F}_i(R) = \widetilde{F}_i(\widetilde{R}) = 0$, se tiene:

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = D(\widetilde{F})(\widetilde{R}).\begin{pmatrix} R_1 - \widetilde{R}_1 \\ \vdots \\ R_n - \widetilde{R}_n \end{pmatrix}$$

$$\text{módulo } (R_1 - \widetilde{R}_1, \ldots, R_n - \widetilde{R}_n)^2 \tag{12}$$

Puesto que para $i = 1, \ldots, n$ vale que $O(R_i) \geq 1/d, O(\widetilde{R_i}) \geq 1/d$, se sigue que $R_i - \widetilde{R}_i \in \mathcal{M}$ para $i = 1, \ldots, n$. Reemplazando en la ecuación (10) las variables $X_1, \ldots, X_n$ por $R_1, \ldots, R_n$ y las variables $Y_1, \ldots, Y_n$ por $\widetilde{R}_1, \ldots, \widetilde{R}_n$ se obtiene la siguiente identidad:

$$\det(D(\widetilde{F}))(R) = \det(D(\widetilde{F}))(\widetilde{R}) +$$

$$+ \sum_{j=1}^{n} \frac{\partial \det(D(\widetilde{F}))}{\partial X_j}(\widetilde{R}).(R_j - \widetilde{R}_j)$$

$$\text{módulo } (R_1 - \widetilde{R}_1, \ldots, R_n - \widetilde{R}_n)^2$$

Puesto que hemos probado que $\det(D(\widetilde{F}))(R) \notin \mathcal{M}$, se sigue de esta última ecuación y del hecho que $R_i - \widetilde{R}_i \in \mathcal{M}$ para $i = 1, \ldots, n$ que $\det(D(\widetilde{F}))(\widetilde{R}) \notin \mathcal{M}$. De ésto y de la ecuación (12) se deduce entonces que $R_i - \widetilde{R}_i \in \mathcal{M}^2$ para $i = 1, \ldots, n$. Utilizando la ecuación (12) se demuestra inductivamente que $R_i - \widetilde{R}_i \in \mathcal{M}^{2^N}$ para todo $N \in \mathbb{N}$, $i = 1, \ldots, n$, lo que a su vez implica que $R_i = \widetilde{R}_i$ para $i = 1, \ldots, n$, como se quería demostrar.

□

Gracias a la cota del grado total de m_H obtenida en la Proposición 28 y al "orden" de convergencia de la sucesión R^N que se obtiene de la ecuación (11), será suficiente calcular hasta la $\lceil \log(\deg(H)) + (n+1)\log(d) \rceil$– ésima iteración del operador de Newton.
Sea $A = \mathbb{Q}[B_1, \ldots, B_n, \varepsilon^{1/d}]$, sea K su cuerpo de fracciones. Se puede pensar al operador de Newton definido para funciones de $K(X_1, \ldots, X_n)$. Por lo tanto, para cualquier número natural $k \in \mathbb{N}$, existen polinomios $g_1^{(k)}, \ldots, g_n^{(k)}$,
$h^{(k)} \in A[X_1, \ldots, X_n]$ tales que

$$N_{\widetilde{F}}^{(k)} = \left(\frac{g_1^{(k)}}{h^{(k)}}, \ldots, \frac{g_n^{(k)}}{h^{(k)}} \right) \qquad .$$

El Lema siguiente muestra la existencia de un esquema de evaluación que calcula tales polinomios sin utilizar divisiones.

Lema 37 *Supongamos que los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$ vienen dados por un circuito aritmético β en espacio $\mathcal{S}$ y tiempo $\mathcal{T}$. Entonces, existe un circuito aritmético en espacio $O(\mathcal{S}n)$ y tiempo $O((\mathcal{T}n + n^4)k)$ que, utilizando los mismos parámetros que β, computa los numeradores $g_1^{(k)}, \ldots, g_n^{(k)}$ y un denominador (distinto de cero) $h^{(k)}$ para $N_{\widetilde{F}}^{(k)}$.*
Más aún, el denominador $h^{(k)}$ evaluado en $0, \ldots, 0$ es un elemento inversible del anillo $\mathcal{R} = \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)[|\varepsilon^{1/d}|]$.

Demostración.– Calculamos las n^2 entradas de la matriz Jacobiana $D(\widetilde{F})$ espacio $\mathcal{S} + 1$ y tiempo $(2n+1)\mathcal{T}$ según el Lema (3).
Sea $Adj(D(\widetilde{F})) = (a_{i,j})_{1 \le i,j \le n}$ la matriz adjunta de $D(\widetilde{F})$. Tanto $Adj(D(\widetilde{F}))$ como el determinante de la matriz jacobiana $D(\widetilde{F})$ se evalúan mediante una adaptación del algoritmo de Samuelson para el cálculo de determinantes (ver [FF63] o [Abd97]) en espacio $O(\log n + \mathcal{S})$ y tiempo $O(n^5 + n\mathcal{T})$.

Puesto que $D(\widetilde{F})^{-1} = \det(D\widetilde{F}))^{-1} Adj(D(\widetilde{F}))$, el operador $N_{\widetilde{F}}$ se puede escribir como

$$N_{\widetilde{F}} = \frac{\det(D\widetilde{F})) \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} - Adj(D(\widetilde{F})) \begin{pmatrix} \widetilde{F}_1(X_1, \ldots, X_n) \\ \vdots \\ \widetilde{F}_n(X_1, \ldots, X_n) \end{pmatrix}}{\det(D\widetilde{F})} \tag{13}$$

Los coeficientes $a_{i,j}$ de la matriz $Adj(D(\widetilde{F}))$ son polinomios en $A[X_1, \ldots, X_n]$ con grado acotado por $(n-1)(d-1)$. Por otro lado, es evidente que el determinante de la matriz jacobiana $\det(D\widetilde{F})$ es un polinomio en $A[X_1, \ldots, X_n]$ cuyo grado está acotado superiormente por $n(d-1)$.
Definimos ahora, para $1 \leq i \leq n$, los siguientes polinomios de $A[X_1, \ldots, X_n]$

$$g_i := \det(D\widetilde{F})X_i - \sum_{j=1}^{n} a_{i,j}\widetilde{F}_j.$$

Veamos, en primer lugar, que el grado total de g_i está acotado por $v := n(d-1)+1$. Para ello, basta escribir el desarrollo de $\det(D\widetilde{F})$ por los elementos de la columna i–ésima de $D\widetilde{F}$, es decir, $\det(D\widetilde{F}) = \sum_{j=1}^{n} a_{i,j}\frac{\partial \widetilde{F}_j}{\partial X_i}$. Así,

$$g_i = \sum_{j=1}^{n} a_{i,j}(\frac{\partial \widetilde{F}_j}{\partial X_i}.X_i - \widetilde{F}_j).$$

Esta identidad demuestra que, efectivamente, el grado de g_i es menor o igual que v. Introducimos una nueva variable X_0 y sean $({}^h g_i)(X_0, X_1, \ldots, X_n) \in A[X_0, \ldots, X_n]$ y $({}^h\det(D\widetilde{F}))(X_0, \ldots, X_n) \in A[X_0, \ldots, X_n]$ los polinomios homogeneizados de g_i y del determinante jacobiano, $\det(D\widetilde{F})$, con respecto a la variable X_0.

Sean ahora:

- $\widetilde{g}_i(X_0, \ldots, X_n) := X_0^{v-\deg(g_i)}.({}^h g_i)$,
- $\widetilde{h}(X_0, \ldots, X_n) := X_0^{v-\deg(\det(D\widetilde{F}))}.({}^h\det(D\widetilde{F}))$.

Estos polinomios pertenecen a $A[X_0, \ldots, X_n]$. De acuerdo al Lema (4), existe un esquema de evaluación sin divisiones en espacio $O(\log n + \mathcal{S})$ y tiempo $O(d^2(n^7 + n^3\mathcal{T}))$ que representa a los polinomios $\widetilde{g}_1, \ldots, \widetilde{g}_n, \widetilde{h}$. Por otro lado, definimos, de manera recursiva, los polinomios siguientes:

- para $k = 1$ y $1 \leq i \leq n$, sea
  $g_i^{(1)} := \widetilde{g}_i(1, X_1, \ldots, X_n)$ y
  $h^{(1)} := \widetilde{h}(1, X_1, \ldots, X_n)$,

- para $k \geq 2$ y $1 \leq i \leq n$, sea
  $g_i^{(k)} := \widetilde{g}_i(\widetilde{h}^{(k-1)}, \widetilde{g}_1^{(k-1)}, \ldots, \widetilde{g}_n^{(k-1)})$ y
  $h^{(k)} := \widetilde{h}(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)})$.

Probaremos por inducción en k que $h^{(k)}(0, \ldots, 0)$ es inversible en $\mathcal{R}$ y que $g_1^{(k)}, \ldots, g_n^{(k)}, h^{(k)}$ son los numeradores y el denominador de $N_{\widetilde{F}}^{(k)}$.
Claramente $g_1^{(1)}, \ldots, g_n^{(1)}, h^{(1)}$ son los numeradores y el denominador de $N_{\widetilde{F}}^{(1)}$. De acuerdo a la ecuación (7) de la Observación 35, el polinomio $h^{(1)}$ evaluado en $(0, \ldots, 0)$ verifica la siguiente relación de congruencia:

$$h^{(1)}(0, \ldots, 0) \equiv d^n \prod_{i=1}^{n} B_i^{d-1} \text{ módulo } \varepsilon^{1/d}$$

y puesto que B_i es inversible en $\mathcal{R}$ para $1 \leq i \leq n$, $h^{(1)}(0, \ldots, 0)$ resulta inversible en $\mathcal{R}$.
Es claro que los polinomios $g_1^{(k)}, \ldots, g_n^{(k)}, h^{(k)}$ pertenecen a $A[X_1, \ldots, X_n] = \mathbb{Q}[B_1, \ldots, B_n, \varepsilon^{1/d}, X_1, \ldots, X_n]$. Además los polinomios $g_1^{(k)}, \ldots, g_n^{(k)}$ y el polinomio $h^{(k)}$ son, respectivamente, numeradores y denominador del operador de Newton–Hensel iterado k veces:

$$\frac{g_i^{(k)}}{h^{(k)}} = \frac{g_i(\frac{g_1^{(k-1)}}{h^{(k-1)}}, \ldots, \frac{g_n^{(k-1)}}{h^{(k-1)}})}{\det(D\widetilde{F})(\frac{g_1^{(k-1)}}{h^{(k-1)}}, \ldots, \frac{g_n^{(k-1)}}{h^{(k-1)}})} = \frac{(h^{(k-1)})^{(v)}}{(h^{(k-1)})^{(v)}} \cdot \frac{g_i(\frac{g_1^{(k-1)}}{h^{(k-1)}}, \ldots, \frac{g_n^{(k-1)}}{h^{(k-1)}})}{\det(D\widetilde{F})(\frac{g_1^{(k-1)}}{h^{(k-1)}}, \ldots, \frac{g_n^{(k-1)}}{h^{(k-1)}})} =$$

$$= \frac{(h^{(k-1)})^{(v-\deg(g_i))} \cdot ({}^h g_i)(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)})}{(h^{(k-1)})^{(v-\deg(\det(D\widetilde{F})))} \cdot ({}^h\det(D\widetilde{F}))(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)})} =$$

$$= \frac{\widetilde{g}_i(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)})}{\widetilde{h}(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)})}.$$

Por otra parte, supongamos que el polinomio $h^{(k-1)}$ evaluado en $(0, \ldots, 0)$ es inversible en $\mathcal{R}$. El polinomio $h^{(k)}$ se define

$$h^{(k)} := \widetilde{h}(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)}) =$$
$$= (h^{(k-1)})^{v-\deg(\det(D\widetilde{F}))} \cdot ({}^h\det(D\widetilde{F}))(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)}).$$

Notamos 0 al vector $(0, \ldots, 0)$. Puesto que $h^{(k-1)}(0)$ es inversible en $\mathcal{R}$ se tienen las siguientes igualdades en $\mathcal{R}$:

$$h^{(k)}(0) = (h^{(k-1)})^{v-\deg(\det(D\widetilde{F}))}(0).(^h\det(D\widetilde{F})(h^{(k-1)}(0), g_1^{(k-1)}(0), \ldots, g_n^{(k-1)}(0))) =$$

$$= (h^{(k-1)})^v(0)\det(D\widetilde{F})(\frac{g_1^{(k-1)}(0)}{h^{(k-1)}(0)}, \ldots, \frac{g_n^{(k-1)}(0)}{h^{(k-1)}(0)}) \quad (14)$$

Resta demostrar que $\det(D\widetilde{F})(\frac{g_1^{(k-1)}(0)}{h^{(k-1)}(0)}, \ldots, \frac{g_n^{(k-1)}(0)}{h^{(k-1)}(0)})$ es inversible en $\mathcal{R}^n$. Ahora bien, por hipótesis inductiva la n–upla $(\frac{g_1^{(k-1)}(0)}{h^{(k-1)}(0)}, \ldots, \frac{g_n^{(k-1)}(0)}{h^{(k-1)}(0)}) \in \mathcal{R}^n$ es igual a $R^{(k-1)}$, donde $R^{(N)} \in \mathcal{R}^n$ se definía en el Lema 36 de la siguiente manera :

$$R^{(0)} := (0, \ldots, 0)$$

$$R^{(N+1)} := N_{\widetilde{F}}(R^{(N)})^t \text{ para } N \geq 0.$$

En ese Lema se prueba que

$$\det(D(\widetilde{F}))(R^{(k)}) = \det(D(\widetilde{F}))(R^{(k-1)}) +$$

$$+ \sum_{j=1}^{n} \frac{\partial \det(D(\widetilde{F}))}{\partial X_j}(R^{(k-1)}).(R_j^{(k)} - R_j^{(k-1)})$$

$$\text{módulo } (R_1^{(k)} - R_1^{(k-1)}, \ldots, R_n^{(k)} - R_n^{(k-1)})^2$$

Puesto que $R_j^{N+1} \equiv R_j^{(N)}$ módulo $\varepsilon^{1/d}$ para $1 \leq N, 1 \leq j \leq n$ según la ecuación (11) del Lema 36, se deduce que

$$\det(D(\widetilde{F}))(R^{(k)}) \equiv \det(D(\widetilde{F}))(R^{(1)}) \text{ módulo } \varepsilon^{1/d}$$

en $\mathcal{R}$. Dado que $\det(D(\widetilde{F}))(R^{(1)})$ es inversible en $\mathcal{R}$, se tiene que $\det(D(\widetilde{F}))(R^{(k)})$ también lo es. Retomando la ecuación (14), se prueba la inversibilidad de $h^{(k)}(0)$ en $\mathcal{R}$ que es lo que se quería demostrar.

Para evaluar tales polinomios, no es preciso más que iterar k veces el esquema de evaluación anteriormente descrito. De tal forma, se obtienen las complejidades que se establecen en el enunciado del Lema.

□

El operador de Newton definido en el Lema anterior es aplicable a w-múltiplos de los polinomios $\widetilde{F}_1, \ldots, \widetilde{F}_n$ donde $w \in \mathbb{Q}[\varepsilon^{1/d}]$ es un polinomio no nulo. En nuestro algoritmo nos será útil poder aplicar el circuito aritmético anterior a los polinomios $\varepsilon\widetilde{F}_1, \ldots, \varepsilon\widetilde{F}_n$. Para ello necesitamos la siguiente observación:

Observación 38 *Bajo las hipótesis y notación anteriores, sean* $g_1^{(k)}, \ldots, g_n^{(k)}, h^{(k)}$ *los polinomios que se obtienen en el circuito aritmético descripto en el Lema anterior. Sea* $w \in \mathbb{Q}[\varepsilon^{1/d}]$ *un polinomio no nulo, y supongamos que los polinomios* $w, \widetilde{F}_1, \ldots, \widetilde{F}_n$ *vienen dados por un circuito aritmético* β *en espacio* $\mathcal{S}$ *y tiempo* $\mathcal{T}$*. Entonces, el circuito aritmético descripto en el Lema anterior es aplicable a los polinomios* $w\widetilde{F}_1, \ldots, w\widetilde{F}_n$ *y los numeradores* $g_1^{(w,k)}, \ldots, g_n^{(w,k)}$ *y el denominador* $h^{(w,k)}$ *obtenidos son* $\widetilde{w}_k$*-múltiplos de los polinomios* $g_1^{(k)}, \ldots, g_n^{(k)}, h^{(k)}$*, donde* $\widetilde{w}_k$ *es una potencia de* w*. En particular, se tiene la siguiente igualdad en* $\mathbb{Q}(B_1, \ldots, B_n, \varepsilon^{1/d}, X_1, \ldots, X_n)$ *:*

$$N_{\widetilde{F}}^{(k)} = (\frac{g_1^{(k)}}{h^{(k)}}, \ldots, \frac{g_n^{(k)}}{h^{(k)}}) = (\frac{\widetilde{w}_k g_1^{(k)}}{\widetilde{w}_k h^{(k)}}, \ldots, \frac{\widetilde{w}_k g_n^{(k)}}{\widetilde{w}_k h^{(k)}}) = (\frac{g_1^{(w,k)}}{h^{(w,k)}}, \ldots, \frac{g_n^{(w,k)}}{h^{(w,k)}}) = N_{\widehat{F}}^{(k)}.$$

El nuevo circuito aritmético utiliza espacio $O(\mathcal{S}n)$ *y tiempo* $O((\mathcal{T}n + n^4)k)$*.*

Demostración.– Se prueba por inducción en k, el número de iteraciones del operador de Newton que realiza el circuito aritmético.
Notamos $D(w\widetilde{F}) \in A[X_1, \ldots, X_n]^{n\times n}$ a la matriz jacobiana correspondiente a los polinomios $w\widetilde{F}_1, \ldots, w\widetilde{F}_n$, sea $Adj(D(w\widetilde{F})) = (a_{i,j}^{(w)})_{1\leq i,j\leq n}$ la matriz adjunta de $D(w\widetilde{F})$.
Recordamos que $Adj(D(\widetilde{F})) = (a_{i,j})_{1\leq i,j\leq n}$ es la matriz adjunta de $D(\widetilde{F})$. Puesto que vale la siguiente igualdad entre las matrices jacobianas $D(w\widetilde{F}) = wD(\widetilde{F})$, por propiedad del determinante se tienen las siguientes igualdades:

i) $(a_{i,j}^{(w)})_{1\leq i,j\leq n} = Adj(D(w\widetilde{F})) = w^{n-1}Adj(D(\widetilde{F})) = w^{n-1}(a_{i,j})_{1\leq i,j\leq n}$.
ii) $\det(D(w\widetilde{F})) = w^n \det(D\widetilde{F})$.

Recordamos la definición de los siguientes polinomios de $A[X_1, \ldots, X_n]$, para $1 \leq i \leq n$:

$$g_i := \det(D\widetilde{F})X_i - \sum_{j=1}^{n} a_{i,j}\widetilde{F}_j.$$

Notamos $g_i^{(w)}$ a estos polinomios calculados a partir de $w\widetilde{F}$, es decir
$g_i^{(w)} := \det(D(w\widetilde{F}))X_i - \sum_{j=1}^{n} a_{i,j}^{(w)} w\widetilde{F}_j$.

A partir de las igualdades i) e ii) se tienen las siguientes igualdades:
$g_i^{(w)} := \det(D(w\widetilde{F}))X_i - \sum_{j=1}^{n} a_{i,j}^{(w)} w\widetilde{F}_j = w^n \det(D\widetilde{F})X_i - w^{n-1}w\sum_{j=1}^{n} a_{i,j}\widetilde{F}_j =$
$w^n(\det(D\widetilde{F})X_i - \sum_{j=1}^{n} a_{i,j}\widetilde{F}_j) = w^n g_i$.
Recordamos que $v := n(d-1)+1$ es una cota superior de los grados de los polinomios g_i y por lo tanto también de $g_i^{(w)}$.
Introduciendo una nueva variable X_0, recordamos que

$({}^h g_i)(X_0, X_1, \ldots, X_n) \in A[X_0, \ldots, X_n]$ y $({}^h\det)(D\widetilde{F})(X_0, \ldots, X_n) \in A[X_0, \ldots, X_n]$ son los polinomios homogeneizados de g_i y del determinante jacobiano, $\det(D\widetilde{F})$, con respecto a la variable X_0.

Recordamos la definición de los polinomios $\widetilde{g}_i, \widetilde{h}$:

- $\widetilde{g}_i(X_0, \ldots, X_n) := X_0^{v-\deg(g_i)}.({}^h g_i)$,
- $\widetilde{h}(X_0, \ldots, X_n) := X_0^{v-\deg(\det(D\widetilde{F}))}.({}^h\det(D\widetilde{F}))$.

Estos polinomios, calculados a partir de $w\widetilde{F}$, resultan:

- $\widetilde{g}_i^{(w)}(X_0, \ldots, X_n) := X_0^{v-\deg(g_i)}.({}^h g_i^{(w)})$,
- $\widetilde{h}^{(w)}(X_0, \ldots, X_n) := X_0^{v-\deg(\det(D\widetilde{F}))}.({}^h\det(D(w\widetilde{F})))$.

De las igualdades demostradas anteriormente se tienen las siguientes identidades:

$\widetilde{g}_i^{(w)} = X_0^{v-\deg(g_i)}.w^n.({}^h g_i)$,
$\widetilde{h}^{(w)} = X_0^{v-\deg(\det(D\widetilde{F}))}.w^n.({}^h\det(D\widetilde{F}))$.
Por último en el Lema anterior se definían de manera recursiva los polinomios siguientes:

- para $k = 1$ y $1 \leq i \leq n$:
  $g_i^{(1)} := \widetilde{g}_i(1, X_1, \ldots, X_n)$ y
  $h^{(1)} := \widetilde{h}(1, X_1, \ldots, X_n)$,
- para $k \geq 2$ y $1 \leq i \leq n$:
  $g_i^{(k)} := \widetilde{g}_i(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)})$ y
  $h^{(k)} := \widetilde{h}(h^{(k-1)}, g_1^{(k-1)}, \ldots, g_n^{(k-1)})$.

Recordamos que los polinomios $g_1^{(k)}, \ldots, g_n^{(k)}$ y que el polinomio $h^{(k)}$ son, respectivamente, numeradores y denominador del operador de Newton–Hensel iterado k veces, aplicado a los polinomios $\widetilde{F}_1, \ldots, \widetilde{F}_n$.
Los polinomios $g_i^{(k)}, h^{(k)}$, calculados a partir de $w\widetilde{F}$, resultan:

Para $k = 1$ y $1 \leq i \leq n$:

$g_i^{(w,1)} := \widetilde{g}_i^{(w)}(1, X_1, \ldots, X_n) = w^n \widetilde{g}_i(1, X_1, \ldots, X_n) = w^n g_i^{(1)}$ y
$h^{(w,1)} := \widetilde{h}^{(w)}(1, X_1, \ldots, X_n) = w^n \widetilde{h}(1, X_1, \ldots, X_n) = w^n h^{(1)}$.

Entonces la observación es cierta para el caso $k = 1$, donde $\widetilde{w}_1$ resulta igual a w^n.

Para $k \geq 2$ y $1 \leq i \leq n$:

$g_i^{(w,k)} := \widetilde{g}_i^{(w)}(h^{(w,k-1)}, g_1^{(w,k-1)}, \ldots, g_n^{(w,k-1)})$ y
$h^{(w,k)} := \widetilde{h}^{(w)}(h^{(w,k-1)}, g_1^{(w,k-1)}, \ldots, g_n^{(w,k-1)})$.

Supongamos cierta la observación para el caso $k = k_0 - 1$, veamos que es cierta para $k = k_0$. Por hipótesis inductiva, existe $\widetilde{w}_{k_0-1}$ potencia de w tal que valen las igualdades:

$g_i^{(w,k_0-1)} = \widetilde{w}_{k_0-1}.g_i^{(k_0-1)}$,
$h^{(w,k_0-1)} = \widetilde{w}_{k_0-1}.h^{(k_0-1)}$.
De la definición recursiva de $g_i^{(w,k_0)}$ se tienen las igualdades:

$g_i^{(w,k_0)} := \widetilde{g}_i^{(w)}(h^{(w,k_0-1)}, g_1^{(w,k_0-1)}, \ldots, g_n^{(w,k_0-1)}) =$
$= (h^{(w,k_0-1)})^{v-\deg(g_i)}.({}^h g_i^{(w)}(h^{(w,k_0-1)}, g_1^{(w,k_0-1)}, \ldots, g_n^{(w,k_0-1)})) =$
$= \widetilde{w}_{k_0-1}^v.(h^{(k_0-1)})^{v-\deg(g_i)}.w^n.({}^h g_i(h^{(k_0-1)}, g_1^{(k_0-1)}, \ldots, g_n^{(k_0-1)})) = \widetilde{w}_{k_0-1}^v.w^n.g_i^{(k_0)}$.

Análogamente se sigue que $h^{(w,k_0)} = \widetilde{w}_{k_0-1}^v.w^n.h^{(k_0)}$. Puesto que $\widetilde{w}_{k_0-1}$ es potencia de w, se sigue que $\widetilde{w}_{k_0-1}^v.w^n$ también lo es, lo que prueba la hipótesis inductiva.

□

5 Las cuentas y su complejidad

5.1 Solución geométrica de V'

Sea ahora el álgebra

$$A' := \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n).$$

Recordamos que $\alpha_i = G_i(0, \ldots, 0)$ para $1 \leq i \leq n$, donde los polinomios G_i son los del sistema de Pham (1). Sean $I' := (B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n) \subseteq \mathbb{Q}[B_1, \ldots, B_n], V' := V(I') \subseteq \mathbb{A}^n$. Claramente se tiene que $V' = \{(\xi_1, \ldots, \xi_n) \in \mathbb{A}^n : \xi_i^d = \alpha_i\}$, es decir que los elementos de V' son todas las n - uplas $a_1^{(k_1)}, \ldots, a_n^{(k_n)}$ de raíces d–ésimas de $\alpha_1, \ldots, \alpha_n$ y por lo tanto $\#(V') = d^n$. Fijamos un orden en los elementos de $V' = \{\xi^{(k)} : 1 \leq k \leq d^n\}$.

Proposición 39 *Bajo las hipótesis y notación anteriores se verifica:*

i) $B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n$ *es una sucesión regular en* $\mathbb{Q}[B_1, \ldots, B_n]$.

ii) I' es un ideal radical y por lo tanto A' es un álgebra reducida.

iii) A' es un $\mathbb{Q}$ - espacio vectorial de dimensión finita, y $dim_{\mathbb{Q}} A' = \#(V') = d^n$.

Demostración.– *i)* Para $1 \leq k < n$ fijo, sea el ideal $I'_k := (B_1^d - \alpha_1, \ldots, B_k^d - \alpha_k)$ en $\mathbb{Q}[B_1, \ldots, B_n]$. Sea $>$ el orden monomial lexicográfico en $\mathbb{Q}[B_1, \ldots, B_n]$. Con este orden se tiene que el término inicial del polinomio $B_i^d - \alpha_i$ es $M(B_i^d - \alpha_i) = B_i^d$. Como B_i^d, B_j^d son coprimos para $i \neq j$, del Lema 16 se sigue que $B_1^d - \alpha_1, \ldots, B_k^d - \alpha_k$ es una base de Gröbner de I'_k.
Sea $C := \{g \in \mathbb{Q}[B_1, \ldots, B_n] : g.(B_{k+1}^d - \alpha_{k+1}) \in I'_k \text{ y } g \notin I'_k\}$. Por definición, $B_{k+1}^d - \alpha_{k+1}$ no es divisor de cero en $\mathbb{Q}[B_1, \ldots, B_n]/I'_k$ si y sólo si el conjunto C es vacío. Supongamos por el contrario que $C \neq \emptyset$:
Sea g_0 tal que $M(g_0) = \min\{M(g) : g \in C\}$. Existe un tal g_0 pues todo subconjunto de $\mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ tiene primer elemento respecto de un orden monomial $>$ fijo (ver Lema 15). Se tiene que
$M(g_0.(B_{k+1}^d - \alpha_{k+1})) = M(g_0)M(B_{k+1}^d - \alpha_{k+1}) = B_{k+1}^d M(g_0) \in M(I'_k)$. Al ser $M(I'_k)$ un ideal generado por monomios, un monomio pertenece al mismo si y sólo si es divisible por algún monomio generador. Calculamos el máximo común divisor entre los términos iniciales de $B_{k+1}^d - \alpha_{k+1}$ y $B_i^d - \alpha_i$:
$MCD(M(B_{k+1}^d - \alpha_{k+1}); M(B_i^d - \alpha_i)) = MCD(B_{k+1}^d; B_i^d) = 1$ para $1 \leq i \leq k$, resulta entonces que $M(g_0.(B_{k+1}^d - \alpha_{k+1})) \in I'_k$ implica que $M(g_0) \in M(I'_k)$. Sea $h \in I'_k$ tal que $M(g_0) = M(h)$. Se tiene que $(g_0 - h)(B_{k+1}^d - \alpha_{k+1}) \in I'_k$ y $M(g_0 - h) < M(g_0) = \min\{M(g) : g \in C\}$. Si $g_0 - h \in I'_k$, entonces $g_0 \in I'_k$, lo cual es falso, y si $g_0 - h \notin I'_k$, entonces $g_0 - h \in C$, pero esto es absurdo pues $M(g_0 - h) < M(g_0)$. Por lo tanto, el polinomio $B_{k+1}^d - \alpha_{k+1}$ no es divisor de cero en $\mathbb{Q}[B_1, \ldots, B_n]/I'_k$. Dado que este razonamiento se hace para todo $1 \leq k < n$, se sigue que $B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n$ es una sucesión regular en $\mathbb{Q}[B_1, \ldots, B_n]$.

ii) Sea $f \in \mathbb{Q}[B_1, \ldots, B_n]$ y $m \in \mathbb{N}$ tal que $f^m \in I'$. Sea $>$ el orden monomial definido en el ítem *i)*. De acuerdo al algoritmo de división, existen $h_1, \ldots, h_n, r \in \mathbb{Q}[B_1, \ldots, B_n]$ tal que $f = \sum_{i=1}^n h_i(B_i^d - \alpha_i) + r$ donde ningún monomio de r pertenece al ideal $(B_1^d, \ldots, B_n^d)$, lo cual implica que $\deg_{B_i}(r) < d$ para $1 \leq i \leq n$. Por otra parte, como $f^m \in I'$ se tiene que $r^m \in I'$. Dado que los polinomios de I' se anulan en V', se sigue que r^m (y por lo tanto r) se anula en V'. De acuerdo a la Proposición 23, se sigue que r es el polinomio nulo y por lo tanto $f \in I'$.

iii) Dado que I' es un ideal radical se tiene que $A' = \mathbb{Q}[V']$. Puesto que $\#(V') = d^n$ se sigue que A' es un $\mathbb{Q}$–espacio vectorial de dimensión d^n.

□

Sea $U \in \mathbb{Z}[B_1, \ldots, B_n]$ una forma lineal que separa los puntos de la variedad V' (es decir, se satisface que $U(\xi^{(k)}) \neq U(\xi^{(j)})$ para todo par de puntos distintos $\xi^{(k)}, \xi^{(j)} \in$

V'). Existe una tal forma lineal pues V' es un conjunto finito. Una forma lineal en estas condiciones permite obtener una base de A' como $\mathbb{Q}$ - espacio vectorial de la siguiente manera: siendo u la imagen de U en A', el conjunto de las potencias $P := \{1, u, u^2, \ldots, u^{d^n-1}\}$ es una base. En tal caso, se llama a u un *elemento primitivo* de A'. Sean $v_1, \ldots, v_n \in \mathbb{Q}[T]$ tales que $B_i - v_i(u) \in A'$. El grado de cada polinomio v_i está acotado por $d^n - 1$.
Sea $q \in \mathbb{Q}[T]$ el polinomio minimal de u en A'. El polinomio q es mónico y tiene grado $\deg q = \#V' = d^n$. Puesto que U separa puntos de V', se tiene que $q(T)$ tiene como raíces a las imágenes de V' bajo U, es decir que $q(T) = \prod_{i=1}^{d^n}(T - U(\xi^{(i)}))$. Consideramos la homotecia $\mathbb{Q}$ - lineal η en A' correspondiente a multiplicar por u. Se sigue que la matriz M de η en la base P es la matriz compañera del polinomio q. Los autovalores de esta matriz son las raíces del polinomio q. Por lo tanto, existe una base P' (y una matriz de cambio de base $C \in \mathbb{C}^{d^n \times d^n}$) de la $\mathbb{C}$ - álgebra $\mathbb{C}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)$ tal que la matriz M' de la homotecia η tiene la forma

$$CMC^{-1} = M' = \begin{pmatrix} u(\xi^{(1)}) & 0 & \ldots & 0 \\ 0 & u(\xi^{(2)}) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & u(\xi^{(d^n)}) \end{pmatrix}$$

Para $1 \leq i \leq n$ consideramos las homotecias η_{B_i} inducidas por la multiplicación por la clase de B_i en la $\mathbb{Q}$ - álgebra A'. Sean M_{B_i} las matrices correspondientes a estas homotecias en la base P. Sea S un polinomio en $\mathbb{Q}[B_1, \ldots, B_n]$, η_S la homotecia asociada y M_S la matriz de η_S en la base P. Puesto que A' es un álgebra conmutativa, se sigue que las homotecias $\eta_{B_1}, \ldots, \eta_{B_n}$ y por lo tanto las matrices $M_{B_1}, \ldots, M_{B_n}$ conmutan entre sí. Esto implica que para cualquier polinomio $S \in \mathbb{Q}[B_1, \ldots, B_n]$ se tiene que $\eta_S = S(\eta_{B_1}, \ldots, \eta_{B_n})$, $M_S = S(M_{B_1}, \ldots, M_{B_n})$.
La igualdad de ideales $I' = (q(U), B_1 - v_1(U), \ldots, B_n - v_n(U))$ en $\mathbb{Q}[B_1, \ldots, B_n]$ implica las siguientes identidades:

$$\eta_{B_1} = v_1(\eta), \ldots, \eta_{B_n} = v_n(\eta),$$
$$M_{B_1} = v_1(M), \ldots, M_{B_n} = v_n(M).$$

En particular se tiene que, para $1 \leq i \leq n$ la matriz de η_{B_i} en la base P' tiene la forma

$$CM_{B_i}C^{-1} = v_i(CMC^{-1}) = \begin{pmatrix} a_i^{(1)} & 0 & \ldots & 0 \\ 0 & a_i^{(2)} & \ldots & 0 \\ \vdots & \ldots & \ddots & \vdots \\ 0 & 0 & \ldots & a_i^{(d^n)} \end{pmatrix} \tag{15}$$

Entonces, para cualquier polinomio S de $\mathbb{Q}[B_1, \ldots, B_n]$ vale que:

$$\eta_S = S(v_1(\eta), \ldots, v_n(\eta)),$$
$$M_S = S(v_1(M), \ldots, v_n(M)). \tag{16}$$

Supongamos que el polinomio minimal q del elemento primitivo u sea reducible en $\mathbb{Q}[T]$. Sea $q = q_1 \ldots q_s$ su descomposición en factores irreducibles no constantes en $\mathbb{Q}[T]$. Sean $D_i = \deg q_i$, se tiene que $D_1 + \ldots + D_s = d^n$. Los polinomios q_i son coprimos pues q es un polinomio separable. Sea la siguiente matriz:

$$M^* := \begin{pmatrix} M_1 & 0 & \ldots & 0 \\ 0 & M_2 & \ldots & 0 \\ \vdots & \ldots & \ddots & \vdots \\ 0 & 0 & \ldots & M_s \end{pmatrix}$$

donde, para cada $1 \leq i \leq s$, la matriz M_i es la matriz compañera de q_i. Del hecho que los polinomios son coprimos dos a dos y del Teorema Chino del Resto se deduce que M^* es similar a la matriz M. Trabajar con la matriz M^* en lugar de M produce una reducción en la complejidad del algoritmo formulado anteriormente, ya que el algoritmo trabaja con las matrices $M_{B_i} = v_i(M)$; a partir de M^*, tenemos las matrices $M^*_{B_i} = v_i(M^*)$.
Recordamos que en el Lema 37 se construye un circuito aritmético que teniendo como entrada a los polinomios $\widetilde{F}_1, \ldots, \widetilde{F}_n$ computa numeradores $g_1^{(\kappa)}, \ldots, g_n^{(\kappa)} \in \mathbb{Q}[B_1, \ldots, B_n, \varepsilon^{1/d}, X_1, \ldots, X_n]$ y un denominador (distinto de cero)
$h^{(\kappa)} \in \mathbb{Q}[B_1, \ldots, B_n, \varepsilon^{1/d}, X_1, \ldots, X_n]$ correspondientes a aplicar κ pasos de iteración del operador de Newton $N^{(\kappa)}_{\widetilde{F}}$. La cantidad de iteraciones del operador de Newton necesarias en nuestro algoritmo es $\kappa := \lceil \log(\deg(H)) + (n+1)\log(d) \rceil$.
Reemplazamos formalmente las indeterminadas B_i por las matrices M_{B_i} y las indeterminadas X_j por 0 en $g_1^{(\kappa)}, \ldots, g_n^{(\kappa)}, h^{(\kappa)}$ y definimos para $i = 1, \ldots, n$ las siguientes matrices en $\mathbb{Q}[|\varepsilon^{1/d}|]^{d^n \times d^n}$:

$$\mathcal{N}_i^{(\kappa)} := (M_{B_i} + g_i^{(\kappa)}(M_{B_1}, \ldots, M_{B_n}, 0, \ldots, 0).h^{(\kappa)}(M_{B_1}, \ldots, M_{B_n}, 0, \ldots, 0)^{-1})\varepsilon^{1/d}. \tag{17}$$

Para la buena definición de las matrices $\mathcal{N}_i^{(\kappa)}$ necesitamos que la matriz $h^{(\kappa)}(M_{B_1}, \ldots, M_{B_n}, 0, \ldots, 0)$ sea inversible en $\mathbb{Q}[|\varepsilon^{1/d}|]^{d^n \times d^n}$. Para ello probamos la siguiente observación:

Sea $J \subseteq \mathbb{Q}^{d^n \times d^n}$ la $\mathbb{Q}$- álgebra generada por las matrices $I, M_{B_1}, \ldots, M_{B_n}$. Es un álgebra conmutativa pues las matrices que la generan conmutan entre sí. Se tiene el siguiente isomorfismo de álgebras:

Observación 40 *La función*

$$\hat{i} : J \longrightarrow A' = \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)$$

$$M_{B_i} \longrightarrow B_i$$

está bien definida y es un isomorfismo de $\mathbb{Q}$ *- álgebras.*

Demostración.– Debemos probar que es un morfismo de $\mathbb{Q}$ - álgebras, para lo cual basta ver que dado $P \in \mathbb{Q}[X_1, \ldots, X_n]$ un polinomio tal que $P(M_{B_1}, \ldots, M_{B_n}) = 0$ en J entonces $P(B_1, \ldots, B_n) = 0$ en A'. Recordamos (ver ecuación (15)) que existe $C \in \mathbb{C}^{d^n \times d^n}$ inversible tal que para $1 \leq i \leq n$ vale:

$$CM_{B_i}C^{-1} = \begin{pmatrix} a_i^{(1)} & 0 & \ldots & 0 \\ 0 & a_i^{(2)} & \ldots & 0 \\ \vdots & \ldots & \ddots & \vdots \\ 0 & 0 & \ldots & a_i^{(d^n)} \end{pmatrix}$$

Entonces se tienen las igualdades
$0 = CP(M_{B_1}, \ldots, M_{B_n})C^{-1} = P(CM_{B_1}C^{-1}, \ldots, CM_{B_n}C^{-1}) =$

$$= \begin{pmatrix} P(a_1^{(1)}, \ldots, a_n^{(1)}) & 0 & \ldots & 0 \\ 0 & P(a_1^{(2)}, \ldots, a_n^{(2)}) & \ldots & 0 \\ \vdots & \ldots & \ddots & \vdots \\ 0 & 0 & \ldots & P(a_1^{(d^n)}, \ldots, a_n^{(d^n)}) \end{pmatrix}.$$

Puesto que $V' = \{\xi_1^{(1)}, \ldots, \xi_1^{(d^n)}\}$, P se anula en la variedad V', lo cual dado que el ideal $(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)$ es radical se sigue que $P(B_1, \ldots, B_n) = 0$ en A', que es lo que se quería demostrar. La inyectividad de $\hat{i}$ se prueba de manera análoga y dado que es un morfismo sobreyectivo se tiene el isomorfismo probado.

□

Observación 41 $h^{(\kappa)}(M_{B_1}, \ldots, M_{B_n}, 0, \ldots, 0)$ *es inversible en* $\mathbb{Q}[|\varepsilon^{1/d}|]^{d^n \times d^n}$.

Demostración.– Recordamos que se probó en el Lema 37 que para todo $k \in \mathbb{N}$, el denominador
$h^{(k)} \in \mathbb{Q}[B_1, \ldots, B_n, \varepsilon^{1/d}][X_1, \ldots, X_n]$, evaluado en $0, \ldots, 0$ es un elemento inversible de $\mathcal{R} = \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)[|\varepsilon^{1/d}|]$.
De acuerdo a la Observación 40 el álgebra generada por las matrices $M_{B_1}, \ldots, M_{B_n}$ es isomorfa al álgebra $A' = \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)$. Por lo tanto $h^{(\kappa)}(M_{B_1}, \ldots, M_{B_n}, 0, \ldots, 0)$ es inversible en $\mathbb{Q}[|\varepsilon^{1/d}|]^{d^n \times d^n}$.

□

Recordamos la observación hecha en esta Subsección sobre la conveniencia de trabajar con la matriz por bloques M^* en lugar de la matriz compañera de $q(T)$, M. Para $1 \leq i \leq s, 1 \leq j \leq n$ definimos las matrices $M_{(B_j,i)} := v_j(M_i)$ donde M_i es la matriz compañera de q_i.
Definimos para $1 \leq i \leq s, 1 \leq j \leq n$ las matrices de $\mathbb{Q}[|\varepsilon^{1/d}|]^{D_i \times D_i}$:

$$\mathcal{N}_{(j,i)}^{(\kappa)} :=$$

$$:= (M_{(B_j,i)} + \frac{g_j^{(\kappa)}}{h^{(\kappa)}}(M_{(B_1,i)}, \ldots, M_{(B_n,i)}, 0, \ldots, 0))\varepsilon^{1/d}. \tag{18}$$

Para todo $1 \leq j \leq n$, la matriz $\mathcal{N}_j^{(\kappa)}$ es semejante a la matriz por bloques:

$$\begin{pmatrix} \mathcal{N}_{(j,1)}^{(\kappa)} & 0 & \ldots & 0 \\ 0 & \mathcal{N}_{(j,2)}^{(\kappa)} & \ldots & 0 \\ \vdots & \ldots & \ddots & \vdots \\ 0 & 0 & \ldots & \mathcal{N}_{(j,s)}^{(\kappa)} \end{pmatrix}.$$

Esto se deduce de que la matriz M es semejante a la matriz por bloques M^* y de la ecuación (16).

Sea $H \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ un polinomio, sea $M_H \in \mathbb{Q}(\varepsilon)^{d^n \times d^n}$ la matriz correspondiente a la homotecia "multiplicar por H" en el álgebra B, en alguna base. Sea $q_H = \sum_{k=1}^{d^n} a_k T^k \in \mathbb{Q}[|\varepsilon|][T]$ su polinomio característico . Reemplazando las indeterminadas X_i por las matrices $\mathcal{N}_i^{(\kappa)}$, sea $\mathcal{M}_H := H(\mathcal{N}_1^{(\kappa)}, \ldots, \mathcal{N}_n^{(\kappa)}) \in \mathbb{Q}[|\varepsilon^{1/d}|]^{d^n \times d^n}$, sea $\chi_{\mathcal{M}} = \sum_{k=1}^{d^n} b_k T^k \in \mathbb{Q}[|\varepsilon^{1/d}|][T]$ su polinomio característico. El siguiente Lema muestra que $\chi_{\mathcal{M}}$ aproxima, en un sentido a precisar por el mismo Lema, al polinomio característico q_H.

Lema 42 *Bajo las hipótesis y notación anteriores, los coeficientes de $\chi_{\mathcal{M}}$ y q_H verifican la siguiente condición en $\mathbb{C}[|\varepsilon^{1/d}|]$:*

$$a_k \equiv b_k \text{ módulo } (\varepsilon)^{\deg(H)d^n}$$

para $k = 1, \ldots, d^n$.

Demostración.– De la Proposición 31 sabemos que $q_H := \prod_{k=1}^{d^n}(T - H(\bar{r}^{(k)}))$ en $\mathbb{C}[|\varepsilon^{1/d}|][T]$ donde $\bar{r}^{(k)} = (\bar{r}_1^{(k)}, \ldots, \bar{r}_n^{(k)})$ para $1 \leq k \leq d^n$ son las series de Puiseux de $X_1, \ldots, X_n$ respecto de ε.

Abreviamos $(\xi^{(j)},0)$ por $(a_1^{(j)},\ldots,a_n^{(j)},0,\ldots,0)\in \mathbb{A}^{2n}$ para $1\leq j\leq d^n$. Recordamos que $a_i^{(j)}\in\mathbb{C}$ son raíces d–ésimas de α_i y que el conjunto $\{\xi^{(j)}: 1\leq j\leq d^n\}$ es la variedad V' definida al comienzo de esta sección. A partir de las identidades (15) y (16) se deduce que cada matriz $\mathcal{N}_i^{(\kappa)}$ es semejante a

$$C\mathcal{N}_i^{(\kappa)}C^{-1}=\begin{pmatrix} (a_i^{(1)}+\frac{g_i^{(\kappa)}(\xi^{(1)},0)}{h^{(\kappa)}(\xi^{(1)},0)})\varepsilon^{1/d} & \ldots & 0\\ \vdots & \ddots & \vdots\\ 0 & \ldots & (a_i^{(d^n)}+\frac{g_i^{(\kappa)}(\xi^{(d^n)},0)}{h^{(\kappa)}(\xi^{(d^n)},0)})\varepsilon^{1/d}\end{pmatrix} \tag{19}$$

Abreviamos $\widetilde{g}^{(\kappa)}(\xi^{(j)},0)$ por
$((a_1^{(j)}+g_1^{(\kappa)}(\xi^{(j)},0).h^{(\kappa)}(\xi^{(j)},0)^{-1})\varepsilon^{1/d},\ldots,(a_n^{(j)}+g_n^{(\kappa)}(\xi^{(j)},0).h^{(\kappa)}(\xi^{(j)},0)^{-1})\varepsilon^{1/d})$. Se tiene entonces que la matriz $\mathcal{M}_H$ es semejante a

$$C\mathcal{M}_HC^{-1}=\begin{pmatrix} H(\widetilde{g}^{(\kappa)}(\xi^{(1)},0)) & \ldots & 0\\ \vdots & \ddots & \vdots\\ 0 & \ldots & H(\widetilde{g}^{(\kappa)}(\xi^{(d^n)},0))\end{pmatrix}$$

Y por lo tanto su polinomio característico se factoriza:

$$\chi_{\mathcal{M}}=\sum_{k=1}^{d^n}b_kT^k=\prod_{k=1}^{d^n}(T-H(\widetilde{g}^{(\kappa)}(\xi^{(k)},0)))\text{ en }\mathbb{C}[|\varepsilon^{1/d}|][T]. \tag{20}$$

Recordamos la definición de $\kappa=\lceil\log(\deg(H))+(n+1)\log(d)\rceil$. De acuerdo a la ecuación (11) de la demostración del Lema 36 se tiene que

$$R^{(\kappa)}\equiv R\text{ módulo }(\varepsilon)^{\deg(H)d^n}$$

en $(\mathbb{Q}[B_1,\ldots,B_n]/(B_1^d-\alpha_1,\ldots,B_n^d-\alpha_n)[|\varepsilon^{1/d}|])^n$. Es decir que para todo $1\leq i\leq n$ se tiene la relación de congruencia $R_i^{(\kappa)}\equiv R_i$ módulo $(\varepsilon)^{\deg(H)d^n}$. De estas equaciones se deduce que $(B_i+R_i^{(\kappa)})\varepsilon^{1/d}\equiv(B_i+R_i)\varepsilon^{1/d}$ módulo $(\varepsilon)^{\deg(H)d^n}$ para todo $1\leq i\leq n$. Evaluando las indeterminadas $B_1,\ldots,B_n$ en las matrices $M_{B_1},\ldots,M_{B_n}$ en esta última relación de congruencia (recordar la Observación 40) se tiene:

$$(M_{B_i}+R_i^{(\kappa)}(M_{B_1},\ldots,M_{B_n}))\varepsilon^{1/d}\equiv(M_{B_i}+R_i(M_{B_1},\ldots,M_{B_n}))\varepsilon^{1/d}\text{ módulo }(\varepsilon)^{\deg(H)d^n}$$

en $\mathbb{Q}[|\varepsilon^{1/d}|]^{d^n\times d^n}$. Notar que la matriz de la izquierda es la matriz $\mathcal{N}_i^{(\kappa)}$. Multiplicamos a izquierda por la matriz C y a derecha por C^{-1} y tenemos:

$$C\mathcal{N}_i^{(\kappa)}C^{-1}\equiv(CM_{B_i}C^{-1}+R_i(CM_{B_1}C^{-1},\ldots,CM_{B_n}C^{-1}))\varepsilon^{1/d}\text{ módulo }(\varepsilon)^{\deg(H)d^n}$$

La matriz de la izquierda es semejante a la matriz $\mathcal{N}_i^{(\kappa)}$ de acuerdo a la ecuación (19). La matriz de la derecha es la matriz

$$\begin{pmatrix} \bar{r}_i^{(1)} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \bar{r}_i^{(d^n)} \end{pmatrix}.$$

Vale decir que para todo $1 \leq i \leq n, 1 \leq j \leq d^n$ se tiene la relación de congruencia $(a_i^{(j)} + \frac{g_i^{(\kappa)}(\xi^{(j)},0)}{h^{(\kappa)}(\xi^{(j)},0)})\varepsilon^{1/d} \equiv r_i^{(j)}$ módulo $(\varepsilon)^{\deg(H)d^n}$.
Sea σ_j la j–ésima función simétrica elemental en d^n variables. Entonces, los j–ésimos coeficientes de q_H y $\chi_{\mathcal{M}}$ verifican

$$a_j = (-1)^j \sigma_j(H(\bar{r}^{(1)}), \dots, H(\bar{r}^{(d^n)})),$$

$$b_j = (-1)^j \sigma_j(H(\widetilde{g}^{(\kappa)}(\xi^{(1)}, 0)), \dots, H(\widetilde{g}^{(\kappa)}(\xi^{(d^n)}, 0)).$$

De donde se deduce que

$$a_k \equiv b_k \text{ módulo } (\varepsilon)^{\deg(H)d^n}.$$

□

Sea $H_1 \in \mathbb{Q}[X_1, \dots, X_n]$ la forma lineal correspondiente al desarrollo de Taylor de H en el origen $(0, \dots, 0) \in \mathbb{A}^n$, respecto de las variables $X_1, \dots, X_n$. Sea $m_H \in \mathbb{Q}[\varepsilon, X_1, \dots, X_n]$ el polinomio minimal de H y supongamos que $\#\{H_1(V')\} = \deg_T(m_H)$.

El Lema siguiente es una variante del Lema 29 de [GHH$^+$97].

Lema 43 *([GHH$^+$97, Lemma 29]) Bajo las hipótesis y notación anteriores, sea $m_H \in \mathbb{Q}[\varepsilon, X_1, \dots, X_n]$ el polinomio minimal de H, sea $\widetilde{m}_H \in \mathbb{Q}[|\varepsilon^{1/d}|][X_1, \dots, X_n]$ el polinomio minimal de la matriz $\mathcal{M}_H$. Supongamos que vale la igualdad $\deg_T(\widetilde{m}_H) = \deg_T(m_H)$. Entonces se tiene la relación de congruencia:*

$$m_H \equiv \widetilde{m}_H \text{ módulo } \varepsilon^{d^n \deg(H)} \text{ en } \mathbb{Q}[|\varepsilon^{1/d}|][T].$$

5.2 El resultado principal

Recordamos la definición del álgebra A' :

$$A' = \mathbb{Q}[B_1, \dots, B_n]/(B_1^d - \alpha_1, \dots, B_n^d - \alpha_n),$$

y la variedad $V' = V(B_1^d - \alpha_1, \dots, B_n^d - \alpha_n) \subset \mathbb{A}^n$. La forma lineal $U \in \mathbb{Q}[B_1, \dots, B_n]$ es un elemento primitivo de A' y los polinomios $q = q_1 \dots q_s, v_1, \dots, v_n \in \mathbb{Q}[T] - \{0\}$

corresponden a la solución geométrica de V', es decir que se tiene el isomorfismo de álgebras

$$A' \simeq \mathbb{Q}[B_1, \ldots, B_n]/(q(U), B_1 - v_1(U), \ldots, B_n - v_n(U)).$$

Sea $D_i = \deg(q_i)$. Sin pérdida de generalidad suponemos $D_1 \leq D_2 \leq \ldots \leq D_s$.

El input del algoritmo del Teorema 45 es un straight–line program β que computa en espacio $\mathcal{S}$ y tiempo $\mathcal{T}$ los siguientes polinomios:

- Los polinomios $F_1, \ldots, F_n \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$ que definen el sistema de Pham–Brieskorn (1),
- un polinomio $H \in \mathbb{Q}[\varepsilon, X_1, \ldots, X_n]$,
- Una forma lineal $U \in \mathbb{Q}[B_1, \ldots, B_n]$ y los polinomios $q_1, \ldots, q_s, v_1, \ldots, v_n \in \mathbb{Q}[T]$ correspondientes a la solución geométrica del álgebra V'.

El output del algoritmo es un straight–line program que computa al (único) polinomio $m_H \in \mathbb{Q}[\varepsilon, T]$, mónico en T y de grado mínimo en T tal que $m_H(\varepsilon, H) \in (F_1, \ldots, F_n)$.

Definimos los siguientes polinomios en $\mathbb{Q}[\varepsilon^{1/d}, B_1, \ldots, B_n, X_1, \ldots, X_n]$:

$$\widehat{H}(\varepsilon^{1/d}, B_1, \ldots, B_n, X_1, \ldots, X_n) := H(\varepsilon, (B_1 + X_1)\varepsilon^{1/d}, \ldots, (B_n + X_n)\varepsilon^{1/d}),$$

$$\widehat{F_i}(\varepsilon^{1/d}, B_1, \ldots, B_n, X_1, \ldots, X_n) := F_i(\varepsilon, (B_1 + X_1)\varepsilon^{1/d}, \ldots, (B_n + X_n)\varepsilon^{1/d})$$

para $1 \leq i \leq n$.

Observación 44 *Los polinomios $\widehat{F_1}, \ldots, \widehat{F_n}, \widehat{H}$ pueden ser computados por un straight-line program en $\mathbb{Q}[\varepsilon^{1/d}]$ que usa espacio $O(\mathcal{S} + n + \log d)$ y tiempo $O(\mathcal{T} + n + \log d)$.*

Demostración.– El polinomio ε se obtiene a partir del polinomio $\varepsilon^{1/d}$ en espacio y tiempo $O(\log d)$. Los polinomios $(B_1 + X_1)\varepsilon^{1/d}, \ldots, (B_n + X_n)\varepsilon^{1/d}$ se obtienen en espacio y tiempo adicional $O(n)$. Componiendo estos polinomios en los polinomios $F_1, \ldots, F_n, H$ se obtienen los polinomios pedidos con la complejidad afirmada.

Los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$ definidos en (6) se obtienen como cociente de los polinomios $\widehat{F_1}, \ldots, \widehat{F_n}$ por el polinomio ε. Para evitar divisiones por polinomios en

nuestro algoritmo, trabajaremos con los polinomios $\widehat{F_1}, \ldots, \widehat{F_n}$ en lugar de los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$.

El Teorema 45 es el resultado principal de esta tesis, y se ha desarrollado adaptando el Teorema 11 de ([HMW99]) y las ideas de ([HKP$^+$98]) al contexto del sistema de Pham–Brieskorn (1).

Idea general del algoritmo: queremos un straight–line program que compute el polinomio m_H, para lo cual primero vamos a obtener un straight–line program que compute el polinomio característico q_H correspondiente a la homotecia "multiplicar por H" en el álgebra B (recordar Proposición 31), luego computaremos el máximo común divisor entre q_H y su derivada en la variable T y por último obtendremos el polinomio m_H que es igual a $q_H/MCD(q_H; \frac{\partial q_H}{\partial T})$.
Recordamos la definición de las matrices $\mathcal{N}_j^{(\kappa)}$ para $1 \leq j \leq n$ dada en (17),

$$\mathcal{N}_j^{(\kappa)} := (M_{B_j} + g_j^{(\kappa)}(M_{B_1}, \ldots, M_{B_n}, 0, \ldots, 0).h^{(\kappa)}(M_{B_1}, \ldots, M_{B_n}, 0, \ldots, 0)^{-1})\varepsilon^{1/d}.$$

En lugar de computar el polinomio q_H calculamos el polinomio característico $\chi_{\mathcal{M}}$ de la matriz $\mathcal{M}_H := H(\mathcal{N}_1^{(\kappa)}, \ldots, \mathcal{N}_n^{(\kappa)})$, luego computamos su representación separable $\widetilde{m}_H = \chi_{\mathcal{M}}/MCD(\chi_{\mathcal{M}}; \frac{\partial \chi_{\mathcal{M}}}{\partial T})$ ya que el polinomio minimal m_H se obtiene a partir de $\widetilde{m}_H$ según se desprende de la cota de grado total del polinomio minimal m_H dada en la Proposición 28: $\deg(m_H) \leq d^n \deg(H)$ y de la relación de congruencia entre m_H y $\widetilde{m}_H$ dada en el Lema 43. Ahora se imponen dos observaciones:

- Las matrices $\mathcal{N}_j^{(\kappa)}$ tienen tamaño $d^n \times d^n$ y son funciones de M, la matriz compañera de $q(T)$. Si el polinomio $q(T)$ se factoriza en s factores no constantes de $\mathbb{Q}[T]$, $q(T) = \prod_{i=1}^{s} q_i(T)$, la matriz M es semejante a la matriz por bloques formados por las matrices compañeras de q_i según se observó en la Subsección 5.1. Para $1 \leq i \leq s, 1 \leq j \leq n$ se definen las matrices $M_{(B_j,i)} := v_j(M_i)$ donde M_i es la matriz compañera de q_i, y a partir de éstas se definen (18) para $1 \leq i \leq s, 1 \leq j \leq n$ las matrices $\mathcal{N}_{(j,i)}^{(\kappa)}$:

$$\mathcal{N}_{(j,i)}^{(\kappa)} := (M_{(B_j,i)} + \frac{g_j^{(\kappa)}}{h^{(\kappa)}}(M_{(B_1,i)}, \ldots, M_{(B_n,i)}, 0, \ldots, 0))\varepsilon^{1/d}.$$

  Cada matriz $\mathcal{N}_j^{(\kappa)}$ es semejante a la matriz por bloques formados por las s matrices $\mathcal{N}_{(j,i)}^{(\kappa)}$, y entonces la matriz $\mathcal{M}_H = H(\mathcal{N}_1^{(\kappa)}, \ldots, \mathcal{N}_n^{(\kappa)})$ es semejante a la matriz por bloques formados por las matrices $\mathcal{M}_{H,i} := H(\mathcal{N}_{(1,i)}^{(\kappa)}, \ldots, \mathcal{N}_{(n,i)}^{(\kappa)})$. El polinomio característico $\chi_{\mathcal{M}}$ es producto de los polinomios característicos de $\mathcal{M}_{H,i}$. La idea es entonces trabajar con las s matrices $\mathcal{M}_{H,i}$ en lugar de $\mathcal{M}$ puesto que se produce una economía de espacio y tiempo. Esta idea viene de [HKP$^+$98].

- En la definición de las matrices $\mathcal{N}_{(j,i)}^{(\kappa)}$ se utilizan las inversas de las matrices $h^{(\kappa)}(M_{(B_1,i)},\ldots,M_{(B_n,i)},0,\ldots,0)$. Para controlar la compejidad en espacio y tiempo de esta operación (y por ende del algoritmo) utilizaremos las rutinas de álgebra lineal y seguiremos la estrategia de [HMW99].

La estrategia a seguir en el agoritmo es la siguiente: primero se calculan los polinomios característicos de $\mathcal{M}_{H,i}$ para $1 \leq i \leq s$, luego los polinomios minimales $\widetilde{m}_{H,i}$ de $\mathcal{M}_{H,i}$ a partir de éstos , y después se calcula el mínimo común múltiplo de $\widetilde{m}_{H,1},\ldots,\widetilde{m}_{H,s}$. Por último, "truncando" hasta el grado $d^n \deg(H)$ la serie de potencias en $\varepsilon^{1/d}$ de este último polinomio se obtiene el polinomio minimal m_H.

Teorema 45 *Bajo las hipótesis y notaciones anteriores, los coeficientes del polinomio minimal $m_H \in \mathbb{Q}[\varepsilon][T]$ que satisface la condición $m_H(\varepsilon,H) \in (F_1,\ldots,F_n)$ pueden ser computados a partir de una solución geométrica de la variedad V' por un straight-line program en $\mathbb{Q}[\varepsilon^{1/d}]$ que usa espacio $O((\mathcal{S}+n+\log d)\deg(H)(n+\deg(H))(D_1^2+\ldots+D_s^2))$ y tiempo $O((\mathcal{T}+n+\log d)\deg(H)+n^4)s^2D_s^3\log^2 d^n \log\log d^n)$.*

Demostración.– A partir del straight–line program dado como input, calculamos los polinomios $\widehat{F_1},\ldots,\widehat{F_n},\widehat{H}$ en espacio del orden de $\widetilde{\mathcal{S}} := \mathcal{S}+n+\log d$ y tiempo del orden de $\widetilde{\mathcal{T}} := \mathcal{T}+n+\log d$ según la Observación 44. Aplicamos la $\kappa = \lceil \log(\deg(H)d^{n+1})\rceil$–ésima iteración del Operador de Newton a los polinomios $\widehat{F_1},\ldots,\widehat{F_n}$ de acuerdo al straight–line program definido en el Lema 37 y en la Observación 38, obteniendo entonces los numeradores $g_1^{(\varepsilon^{1/d},\kappa)},\ldots,g_n^{(\varepsilon^{1/d},\kappa)} \in \mathbb{Q}[\varepsilon^{1/d},B_1,\ldots,B_n,X_1,\ldots,X_n]$ y el denominador $h^{(\varepsilon^{1/d},\kappa)} \in \mathbb{Q}[\varepsilon^{1/d},B_1,\ldots,B_n,X_1,\ldots,X_n]$ tales que

$$N_{\widehat{F}}^{(\kappa)} = \left(\frac{g_1^{(\varepsilon^{1/d},\kappa)}}{h^{(\varepsilon^{1/d},\kappa)}},\ldots,\frac{g_n^{(\varepsilon^{1/d},\kappa)}}{h^{(\varepsilon^{1/d},\kappa)}}\right) \qquad .$$

El operador de Newton–Hensel es aplicable a los polinomios $\widehat{F_1},\ldots,\widehat{F_n}$ según se demostró en la Observación 38. En esta Observación se prueba que los polinomios $g_1^{(\varepsilon^{1/d},\kappa)},\ldots,g_n^{(\varepsilon^{1/d},\kappa)},h^{(\varepsilon^{1/d},\kappa)}$ son $\widetilde{w}-$ múltiplos de $g_1^{(\kappa)},\ldots,g_n^{(\kappa)},h^{(\kappa)}$ donde $\widetilde{w}$ es una potencia de $\varepsilon^{1/d}$ y $g_1^{(\kappa)},\ldots,g_n^{(\kappa)},h^{(\kappa)} \in \mathbb{Q}[\varepsilon^{1/d},B_1,\ldots,B_n,X_1,\ldots,X_n]$ son los numeradores y el denominador que se obtienen en la κ–ésima iteración del Operador de Newton aplicado a los polinomios $\widetilde{F_1},\ldots,\widetilde{F_n}$. En particular se tiene la igualdad $N_{\widehat{F}}^{(\kappa)} = N_{\widetilde{F}}^{(\kappa)}$ en $\mathbb{Q}(B_1,\ldots,B_n,\varepsilon^{1/d},X_1,\ldots,X_n)$.

El cálculo de los polinomios $g_1^{(\varepsilon^{1/d},\kappa)},\ldots,g_n^{(\varepsilon^{1/d},\kappa)},h^{(\varepsilon^{1/d},\kappa)}$ se realiza en espacio $O(\widetilde{\mathcal{S}}n)$ y tiempo $O((\widetilde{\mathcal{T}}n+n^4)\log(\deg(H)d^{n+1}))$ según se establece en la Observación 38.

Recordamos que la forma lineal $U \in \mathbb{Q}[B_1,\ldots,B_n]$ y los polinomios $v_1(T),\ldots,v_n(T) \in \mathbb{Q}[T]$ correspondientes a la solución geométrica de V' verifican que $v_j(U) = B_j$

en A' para todo $1 \leq j \leq n$. Especializando las variables $X_1, \ldots, X_n$ en $0, \ldots, 0$ y las variables $B_1, \ldots, B_n$ en los polinomios $v_1(T), \ldots, v_n(T)$ se tienen los siguientes polinomios de $\mathbb{Q}[\varepsilon^{1/d}][T]$:

- $g_j(T) := g_j^{(\varepsilon^{1/d},\kappa)}(\varepsilon^{1/d}, v_1(T), \ldots, v_n(T), 0, \ldots, 0)$ para $1 \leq j \leq n$,
- $h(T) := h^{(\varepsilon^{1/d},\kappa)}(\varepsilon^{1/d}, v_1(T), \ldots, v_n(T), 0, \ldots, 0)$.

Para $1 \leq i \leq s$, consideramos en $\mathbb{Q}(\varepsilon^{1/d})[T]$ la función racional

$$f(T) := \widehat{H}(\varepsilon^{1/d}, v_1(T), \ldots, v_n(T), \frac{g_1(T)}{h(T)}, \ldots, \frac{g_n(T)}{h(T)})$$

módulo el polinomio $q_i(T)$. Recordamos que $q(T) = \prod_{i=1}^{s} q_i(T)$ es el polinomio minimal de la forma lineal U en el álgebra A'. Para evitar divisiones por polinomios en el cálculo de $f(T)$, computamos la descomposición homogénea de $\widehat{H}$,

$$\widehat{H}(\varepsilon^{1/d}, B_1, \ldots, B_n, X_1, \ldots, X_n) = \sum_{k=0}^{\deg(H)} \widehat{H}_k(\varepsilon^{1/d}, B_1, \ldots, B_n, X_1, \ldots, X_n)$$

considerando a $\widehat{H}$ un polinomio en las variables $X_1, \ldots, X_n$ con coeficientes en el anillo $\mathbb{Q}[\varepsilon^{1/d}, B_1, \ldots, B_n]$. Esta descomposición se calcula mediante el procedimiento descrito en la demostración del Lema 5 usando espacio $O(\widetilde{\mathcal{S}} \deg(H))$ y tiempo $O(\widetilde{\mathcal{T}} \deg(H) \log \deg(H) \log\log \deg(H))$. Considerando en $\mathbb{Q}(\varepsilon^{1/d})[T]$ las siguientes identidades:

$$\begin{aligned}
f(T) &:= \widehat{H}(\varepsilon^{1/d}, v_1(T), \ldots, v_n(T), \frac{g_1(T)}{h(T)}, \ldots, \frac{g_n(T)}{h(T)}) \\
&= \sum_{k=0}^{\deg(H)} \widehat{H}_k(\varepsilon^{1/d}, v_1(T), \ldots, v_n(T), \frac{g_1(T)}{h(T)}, \ldots, \frac{g_n(T)}{h(T)}) \\
&= \sum_{k=0}^{\deg(H)} \frac{\widehat{H}_k(\varepsilon^{1/d}, v_1(T), \ldots, v_n(T), g_1(T), \ldots, g_n(T))}{(h(T))^k} \\
&= \frac{\sum_{k=0}^{\deg(H)} \widehat{H}_k(\varepsilon^{1/d}, v_1(T), \ldots, v_n(T), g_1(T), \ldots, g_n(T))(h(T))^{\deg(H)-k}}{(h(T))^{\deg(H)}},
\end{aligned}$$

concluímos que el numerador y el denominador de la función racional $f(T)$ se calculan en espacio $O(\widetilde{\mathcal{S}}(n + \deg(H)))$ y tiempo $O((\widetilde{\mathcal{T}} n \deg(H) + n^4) \log(\deg(H) d^n))$ realizando divisiones por elementos no nulos de $\mathbb{Q}$.

Es necesaria la siguiente afirmación técnica.

Afirmación: Los polinomios $h(T)$ y $q(T) = \prod_{i=1}^{s} q_i(T)$ son coprimos en $\mathbb{Q}(\varepsilon^{1/d})[T]$.

Recordamos que en la Subsección 5.1 se probó que el polinomio $q(T) \in \mathbb{Q}[T]$ se factoriza $\prod_{j=1}^{d^n}(T - U(\xi^{(j)}))$ donde $\xi^{(j)} \in \mathbb{A}^n$ son n–uplas de raíces d–ésimas de $\alpha_1, \ldots, \alpha_n$, es decir que $\{\xi^{(j)} : 1 \leq j \leq d^n\}$ es la variedad V'. Por lo tanto basta ver que el polinomio $h(T)$ no se anula en $U(\xi^{(j)})$ para ningún $1 \leq j \leq d^n$. Recordamos que $v_i(U) \equiv B_i$ en A' para todo $1 \leq i \leq n$ implica las igualdades $v_i(U(\xi^{(j)})) = \xi_i^{(j)}$ para todo $1 \leq i \leq n, 1 \leq j \leq d^n$. Fijamos $1 \leq j \leq d^n$ y evaluamos $h(T)$ en $U(\xi^{(j)})$:

$$h(U(\xi^{(j)})) = h^{(\varepsilon^{1/d},\kappa)}(\varepsilon^{1/d}, v_1(U(\xi^{(j)})), \ldots, v_n(U(\xi^{(j)})), 0, \ldots, 0) = \\ = h^{(\varepsilon^{1/d},\kappa)}(\varepsilon^{1/d}, \xi_1^{(j)}, \ldots, \xi_n^{(j)}, 0, \ldots, 0). \tag{21}$$

Recordamos que el polinomio $h^{(\varepsilon^{1/d},\kappa)}$ es el denominador que se obtiene en la κ–ésima iteración del Operador de Newton aplicado a los polinomios $\widehat{F_1}, \ldots, \widehat{F_n}$, y es $\widetilde{w}$–múltiplo del polinomio $h^{(\kappa)}$ donde $\widetilde{w}$ es una potencia de $\varepsilon^{1/d}$ y $h^{(\kappa)} \in \mathbb{Q}[\varepsilon^{1/d}, B_1, \ldots, B_n, X_1, \ldots, X_n]$ es el denominador que se obtiene en la κ–ésima iteración del Operador de Newton aplicado a los polinomios $\widetilde{F_1}, \ldots, \widetilde{F_n}$. Ahora bien, el polinomio $h^{(\kappa)}$, evaluando las indeterminadas $X_1, \ldots, X_n$ en $0, \ldots, 0$, es inversible en $\mathcal{R} = \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)[|\varepsilon^{1/d}|]$ (ver Lema 37), por lo tanto existe $h_0 \in A' = \mathbb{Q}[B_1, \ldots, B_n]/(B_1^d - \alpha_1, \ldots, B_n^d - \alpha_n)$ inversible tal que

$$h^{(\kappa)}(\varepsilon^{1/d}, B_1, \ldots, B_n, 0, \ldots, 0) \equiv h_0 \text{ módulo } \varepsilon^{1/d} \text{ en } \mathcal{R}. \tag{22}$$

Dado que h_0 es inversible en A', se sigue que $h_0(\xi^{(j)}) \neq 0$ y por lo tanto $h^{(\kappa)}(\varepsilon^{1/d}, \xi^{(j)}, 0, \ldots, 0) \neq 0$. Retomando la ecuación (21) se sigue que

$$h(U(\xi^{(j)})) = \widetilde{w} h^{(\kappa)}(\varepsilon^{1/d}, \xi^{(j)}, 0, \ldots, 0) \neq 0$$

para $1 \leq j \leq d^n$ que es lo que se quería probar.

Dado entonces que $h(T)$ y $q(T) = \prod_{i=1}^{s} q_i(T)$ son coprimos en $\mathbb{Q}(\varepsilon^{1/d})[T]$ se puede aplicar, para cada $1 \leq i \leq s$, el procedimiento descrito en el comienzo de la demostración del Lema 1 para calcular polinomios $\widetilde{f}_i(T) \in \mathbb{Q}[\varepsilon^{1/d}][T]$ de grado en T a lo sumo $D_i - 1$ y elementos $\alpha_i \in \mathbb{Q}[\varepsilon^{1/d}]$ satisfaciendo en $\mathbb{Q}[\varepsilon^{1/d}][T]$ la condición

$$(h(T))^{\deg(H)} \widetilde{f}_i(T) \equiv \alpha_i \mathcal{G}(T) \text{ módulo } q_i(T)$$

donde

$$\mathcal{G}(T) := \sum_{1 \leq k \leq \deg(H)} \widehat{H}_k(\varepsilon^{1/d}, v_1(T), \ldots, v_n(T), g_1(T), \ldots, g_n(T)).(h(T))^{\deg(H)-k}.$$

Entonces tenemos en $\mathbb{Q}(\varepsilon^{1/d})[T]$ la relación de congruencia $\widetilde{f}_i(T) \equiv \alpha_i f(T)$ módulo $q_i(T)$ para $1 \leq i \leq s$.
Evaluando la indeterminada T en M_i, la matriz compañera de $q_i(T)$, se tiene para cada $1 \leq i \leq s$:

$$\begin{aligned} \widetilde{f}_i(M_i) &= \alpha_i f(M_i) \\ &= \alpha_i H(\varepsilon, \mathcal{N}_{(1,i)}, \ldots, \mathcal{N}_{(n,i)}) = \alpha_i \mathcal{M}_{H,i} \end{aligned}$$

donde las matrices $\mathcal{N}_{(j,i)}$ se definían en (18) y la matriz $\mathcal{M}_{H,i}$ es por definición la matriz $H(\varepsilon, \mathcal{N}_{(1,i)}, \ldots, \mathcal{N}_{(n,i)})$. Para cada $1 \leq i \leq s$, los polinomios $\widetilde{f}_i(T)$ y α_i pueden ser calculados por un straight-line program en espacio $O(\widetilde{\mathcal{S}}(D_i)(n+\deg(H)))$ y tiempo $O((\widetilde{\mathcal{T}} \deg(H) + n^4)(D_i^2) \log^2 d^n \log\log d^n)$.

Usando un procedimiento similar al de la demostración del Lema 2 podemos calcular, para cada $1 \leq i \leq s$, $\alpha_i^{D_i}$- múltiplos de los coeficientes del polinomio característico $\chi_i(T) := \chi_{\mathcal{M}_{H,i}}(T)$ de $\mathcal{M}_{H,i}$ en espacio $O(\widetilde{\mathcal{S}}(D_i)(n + \deg(H)))$ y tiempo $O((\widetilde{\mathcal{T}} \deg(H) + n^4)(D_i^2) \log^2 d^n \log\log d^n)$. Supongamos entonces que tenemos computados para todo $1 \leq i \leq s$ los coeficientes del polinomio $\alpha_i^{D_i} \chi_{\mathcal{M}_{H,i}}(T)$.

Dado que la matriz $\mathcal{M}_H$ es semejante a la matriz por bloques formados por las s matrices $\mathcal{M}_{H,i}$, el polinomio característico $\chi(T)$ de $\mathcal{M}_H$ es el producto de los polinomios característicos $\chi_{\mathcal{M}_{H,1}}(T), \ldots, \chi_{\mathcal{M}_{H,s}}(T)$. Puesto que estamos interesados en computar el polinomio minimal $\widetilde{m}_H$ de $\mathcal{M}_H$ y dado que la matriz $\mathcal{M}_H$ es diagonalizable, es suficiente entonces eliminar del polinomio característico $\chi(T) = \prod_{i=1}^{s} \chi_{\mathcal{M}_{H,i}}(T)$ los factores múltiples para obtener el polinomio minimal $\widetilde{m}_H$ de $\mathcal{M}_H$. Para ello primero queremos calcular para todo $1 \leq i \leq s$ el numerador mónico de la representación irreducible de la función racional $\frac{\alpha_i^{D_i}\chi_i(T)}{\alpha_i^{D_i}\chi_i'(T)} = \frac{\chi_i(T)}{\chi_i'(T)}$. Este numerador mónico es el polinomio minimal $\widetilde{m}_{H,i} = \sum_{k=0}^{\deg(\widetilde{m}_{H,i})} a_{(k,i)}$ de $\mathcal{M}_{H,i}$. El polinomio minimal $\widetilde{m}_H$ de $\mathcal{M}_H$ es el mínimo común múltiplo de los polinomios $\widetilde{m}_{H,1}, \ldots, \widetilde{m}_{H,s}$.

Para cada $1 \leq i \leq s$ queremos aplicar el Lema 7 a la función racional $\frac{\alpha_i^{D_i}\chi_i(T)}{\alpha_i^{D_i}\chi_i'(T)}$ y computar elementos $\gamma_i \in \mathbb{Q}[\varepsilon^{1/d}]$ y γ_i-múltiplos de los coeficientes $a_{(0,i)}, \ldots, a_{(\deg(\widetilde{m}_{H,i}),i)}$ del polinomio minimal $\widetilde{m}_{H,i}$ tal que $\gamma_i a_{(0,i)}, \ldots, \gamma_i a_{(\deg(\widetilde{m}_{H,i}),i)}$ sean elementos de $\mathbb{Q}[\varepsilon^{1/d}]$. Para poder aplicar el Lema 7 es necesario conocer el grado en T del numerador de la representación irreducible de $\frac{\alpha_i^{D_i}\chi_i(T)}{\alpha_i^{D_i}\chi_i'(T)}$, es decir el grado en T de $\widetilde{m}_{H,i}$. Este grado se averigua evaluando $\varepsilon^{1/d}$ en un elemento $y \in \mathbb{Q}$ genérico y calculando el máximo común divisor de los polinomios $\alpha_i^{D_i}(y)\chi_i(y,T), \alpha_i^{D_i}(y)\chi_i'(y,T) \in \mathbb{Q}[T]$. Siendo y un punto genérico, el grado de este máximo común divisor coincide con el grado en T del máximo común divisor de $\alpha_i^{D_i}\chi_i(T), \alpha_i^{D_i}\chi_i'(T)$ en $\mathbb{Q}(\varepsilon^{1/d})[T]$. La

complejidad del cálculo del máximo común divisor de dos polinomios en $\mathbb{Q}[T]$ (de grado acotado por D_i) es del orden de $O(D_i \log D_i \log\log D_i)$ en espacio y $O(D_i^2 \log D_i \log\log D_i)$ en tiempo (ver [BP94]). Conociendo el grado del máximo común divisor, y conociendo el grado (en T) de $\alpha_i^{D_i}\chi_i(T)$ se conoce el grado (en T) de $\widetilde{m}_{H,i}$. Aplicar el Lema 7 a la función racional $\frac{\alpha_i^{D_i}\chi_i(T)}{\alpha_i^{D_i}\chi_i'(T)}$ se hace con espacio $O(\widetilde{\mathcal{S}}(n+\deg(H))(D_i))$ y tiempo $O((\widetilde{\mathcal{T}}\deg(H)+n^4)(D_i^2)\log^2 d^n \log\log d^n)$, para cada $1 \leq i \leq s$.

El straight–line program β_1 definido hasta el momento computa los polinomios $\gamma_1, \ldots, \gamma_s \in \mathbb{Q}[\varepsilon^{1/d}]$ y los polinomios $\gamma_1\widetilde{m}_{H,1}, \ldots, \gamma_s\widetilde{m}_{H,s} \in \mathbb{Q}[\varepsilon^{1/d}, T]$ y tiene complejidad $O(\widetilde{\mathcal{S}}(n+\deg(H))(\sum_{i=1}^s D_i))$ en espacio y
$O((\widetilde{\mathcal{T}}\deg(H)+n^4)(\sum_{i=1}^s D_i^2)\log^2 d^n \log\log d^n)$ en tiempo. Debemos calcular el mínimo común múltiplo de $\widetilde{m}_{H,1}, \ldots, \widetilde{m}_{H,s}$ y es lo que haremos a continuación. Para ello, vamos a eliminar los factores repetidos de estos polinomios utilizando el siguiente procedimiento: dados dos polinomios separables u_1 y $u_2 \in \mathbb{Q}[\varepsilon^{1/d}, T]$, y supongamos por simplicidad que $\deg_T u_1 > \deg_T u_2$, calculamos un polinomio $\gamma \in \mathbb{Q}[\varepsilon^{1/d}]$ y el γ–múltiplo del numerador irreducible n_1 de la fracción $\frac{u_1}{u_2}$ utilizando el straight–line program dado por el Lema 7. Los polinomios n_1 y u_2 son separables y coprimos entre sí y su producto es el mínimo común múltiplo de los polinomios u_1 y u_2 en $\mathbb{Q}(\varepsilon^{1/d})[T]$.

Este procedimiento utiliza dos straight–line programs , uno calcula el grado en la variable T del polinomio n_1 y otro es el dado por el Lema 7.

El straight–line program aplica este procedimiento, tomando de a dos a los polinomios $\widetilde{m}_{H,1}, \ldots, \widetilde{m}_{H,s}$, es decir que se repite $s(s-1)$ veces el procedimiento; esto explica el factor s^2 en la complejidad en tiempo del straight–line program .
Vamos a definir el straight–line program esbozado; para ello, supongamos que para algún $1 \leq i_0 < s$ fijo vale la siguiente condición:

- Los polinomios $\widetilde{m}_{H,1}, \ldots, \widetilde{m}_{H,i_0}$ son coprimos en $\mathbb{Q}[\varepsilon^{1/d}][T]$.

Definamos el conjunto $S_{i_0} := \{\widetilde{m}_{H,1}, \ldots, \widetilde{m}_{H,i_0}\}$. Bajo la suposición anterior, este conjunto está formado por polinomios mónicos en T y coprimos en $\mathbb{Q}[\varepsilon^{1/d}][T]$ y decimos que está en las *condiciones iniciales*.
Más generalmente, decimos que un conjunto $S = \{u_1, \ldots, u_k\} \subset \mathbb{Q}[\varepsilon^{1/d}][T]$ está en las *condiciones iniciales* si valen las siguientes condiciones:

- Los polinomios $u_1, \ldots, u_k$ son mónicos en T y coprimos en $\mathbb{Q}[\varepsilon^{1/d}][T]$.

- El polinomio $\prod_{i=1}^{k} u_i$ es el mínimo común múltiplo de los polinomios $\widetilde{m}_{H,1}, \ldots, \widetilde{m}_{H,k}$

Notar que el conjunto S_1, formado por un único elemento, $\widetilde{m}_{H,1}$, está en las *condiciones iniciales*.

Volviendo al conjunto S_{i_0} definido anteriormente y bajo la suposición que el mismo está en las *condiciones iniciales*, nuestro primer paso es obtener un straight–line program que compute polinomios $u_1, \ldots, u_{i_0+1}$ coprimos en $\mathbb{Q}[\varepsilon^{1/d}][T]$ tales que el producto de ellos sea el mínimo común múltiplo de los polinomios $\widetilde{m}_{H,1}, \ldots, \widetilde{m}_{H,i_0+1}$.

Paso I: Computar el mínimo común múltiplo de dos polinomios de $\mathbb{Q}[\varepsilon^{1/d}][T]$.

Para calcular el mínimo común múltiplo entre $\widetilde{m}_{H,1}$ y $\widetilde{m}_{H,i_0+1}$ vamos a calcular un múltiplo del numerador de la representación irreducible de la fracción $\frac{\gamma_{i_0+1}\widetilde{m}_{H,i_0+1}}{\gamma_1\widetilde{m}_{H,1}}$ (ó bien de la fracción $\frac{\gamma_1\widetilde{m}_{H,1}}{\gamma_{i_0+1}\widetilde{m}_{H,i_0+1}}$ si $\deg_T(\widetilde{m}_{H,1}) \geq \deg_T(\widetilde{m}_{H,i_0+1})$), utilizando el straight–line program dado por el Lema 7. Como sabemos, es necesario conocer el grado en T de los polinomios $\widetilde{m}_{H,1}, \widetilde{m}_{H,i_0+1}$ y de su máximo común divisor. Para ello, evaluamos $\varepsilon^{1/d}$ en un $y \in \mathbb{Q}$ genérico y calculamos el máximo común divisor entre $\gamma_1(y)\widetilde{m}_{H,1}(y)$ y $\gamma_{i_0+1}(y)\widetilde{m}_{H,i_0+1}(y)$. El cálculo de la representación densa de los polinomios $\gamma_1(y)\widetilde{m}_{H,1}(y)$ y $\gamma_{i_0+1}(y)\widetilde{m}_{H,i_0+1}(y)$ y el cálculo de su máximo común divisor se realiza con complejidades inferiores a las del Lema 7

Si $\deg_T(\widetilde{m}_{H,i_0+1}) \geq \deg_T(\widetilde{m}_{H,1})$ entonces aplicamos el straight–line program dado por el Lema 7 al cociente de polinomios $\frac{\gamma_{i_0+1}\widetilde{m}_{H,i_0+1}}{\gamma_1\widetilde{m}_{H,1}}$ (si en cambio $\deg_T(\widetilde{m}_{H,1}) < \deg_T(\widetilde{m}_{H,i_0+1})$ aplicamos el straight–line program dado por el Lema 7 al cociente de polinomios $\frac{\gamma_1\widetilde{m}_{H,1}}{\gamma_{i_0+1}\widetilde{m}_{H,i_0+1}}$ y se continúa de manera análoga) obteniendo un polinomio $\gamma^{(1)} \in \mathbb{Q}[\varepsilon^{1/d}]$ y un $\gamma^{(1)}$- múltiplo del numerador mónico de la representación irreducible de esta fracción en $\mathbb{Q}[\varepsilon^{1/d}][T]$, es decir que obtenemos polinomios $\gamma^{(1)} \in \mathbb{Q}[\varepsilon^{1/d}]$, $u^{(1)} \in \mathbb{Q}[\varepsilon^{1/d}][T]$ que verifican:

- El polinomio $\frac{u^{(1)}}{\gamma^{(1)}}$ pertenece a $\mathbb{Q}[\varepsilon^{1/d}][T]$ y es mónico.
- $\frac{u^{(1)}}{\gamma^{(1)}}$ y $\widetilde{m}_{H,1}$ son coprimos en $\mathbb{Q}[\varepsilon^{1/d}][T]$.
- El polinomio $\frac{u^{(1)}}{\gamma^{(1)}}$ es igual al polinomio $\widetilde{m}_{H,i_0+1}/MCD(\widetilde{m}_{H,i_0+1}; \widetilde{m}_{H,1})$.

Recordando que suponemos $D_1 \leq \ldots \leq D_s$, entonces utilizar el straight–line program dado por el Lema 7 representa un costo adicional de $O(\widetilde{\mathcal{S}}(n+\deg(H))+D_{i_0+1})$ en espacio y $O((\widetilde{\mathcal{T}}\deg(H)+n^4)(D_{i_0+1}^2)\log^2 d^n \log\log d^n)$ en tiempo.

Luego de estos cómputos, tenemos un straight–line program que computa polinomios $\gamma_1, \ldots, \gamma_{i_0}, \gamma^{(1)}, \gamma_{i_0+2}, \ldots, \gamma_s \in \mathbb{Q}[\varepsilon^{1/d}]$, y polinomios
$\gamma_1\widetilde{m}_{H,1}, \ldots, \gamma_{i_0}\widetilde{m}_{H,i_0}, u^{(1)}, \gamma_{i_0+2}\widetilde{m}_{H,i_0+2}, \ldots, \gamma_s\widetilde{m}_{H,s} \in \mathbb{Q}[\varepsilon^{1/d}, T]$ tales que

- Los polinomios $\widetilde{m}_{H,1}, \ldots, \widetilde{m}_{H,i_0}$ son coprimos en $\mathbb{Q}[\varepsilon^{1/d}][T]$.
- Los polinomios $\widetilde{m}_{H,1}$ y $\frac{u^{(1)}}{\gamma^{(1)}}$ son coprimos en $\mathbb{Q}[\varepsilon^{1/d}][T]$ y $\frac{u^{(1)}}{\gamma^{(1)}}\widetilde{m}_{H,1}$ es el mínimo común múltiplo de los polinomios $\widetilde{m}_{H,1}$ y $\widetilde{m}_{H,i_0+1}$.

Fin Paso I

Entonces repetimos el Paso I, esta vez con los polinomios $\gamma_2, \gamma^{(1)} \in \mathbb{Q}[\varepsilon^{1/d}]$ y $\widetilde{m}_{H,2}, u^{(1)} \in \mathbb{Q}[\varepsilon^{1/d}, T]$. Para evitar complicar la notación supongamos nuevamente que $\deg_T(\widetilde{m}_{H,2}) \geq \deg_T(u^{(1)})$. Se obtiene entonces un nuevo $\gamma^{(2)} \in \mathbb{Q}[\varepsilon^{1/d}]$ y un nuevo $u^{(2)} \in \mathbb{Q}[\varepsilon^{1/d}, T]$ que verifica que es coprimo con los polinomios $\widetilde{m}_{H,1}, \widetilde{m}_{H,2}$ y el producto $\frac{u^{(2)}}{\gamma^{(2)}}.\widetilde{m}_{H,1}.\widetilde{m}_{H,2}$ es el mínimo común múltiplo de $\widetilde{m}_{H,1}, \widetilde{m}_{H,2}, \widetilde{m}_{H,i_0+1}$ (igual que antes, si $\deg_T(\widetilde{m}_{H,2}) < \deg_T(u^{(1)})$, al aplicar el Paso I el polinomio modificado resulta ser $\widetilde{m}_{H,2}$). Resumiendo, partiendo del conjunto S_{i_0} en las condiciones iniciales, se repite i_0 veces el Paso I y se obtiene un straight–line program que computa polinomios $\widetilde{\gamma}_1, \ldots, \widetilde{\gamma}_{i_0+1}, \gamma_{i_0+2}, \ldots, \gamma_s \in \mathbb{Q}[\varepsilon^{1/d}]$, y polinomios
$u_1, \ldots, u_{i_0+1}, \gamma_{i_0+2}\widetilde{m}_{H,i_0+2}, \ldots, \gamma_s\widetilde{m}_{H,s} \in \mathbb{Q}[\varepsilon^{1/d}, T]$ tales que

- Las funciones racionales $\frac{u_1}{\widetilde{\gamma}_1}, \ldots, \frac{u_{i_0+1}}{\widetilde{\gamma}_{i_0+1}}$ son polinomios en $\mathbb{Q}[\varepsilon^{1/d}][T]$, mónicos en la variable T.
- $\frac{u_1}{\widetilde{\gamma}_1}, \ldots, \frac{u_{i_0+1}}{\widetilde{\gamma}_{i_0+1}}$ son coprimos en $\mathbb{Q}[\varepsilon^{1/d}][T]$.
- El polinomio $\prod_{i=1}^{i_0+1} \frac{u_i}{\widetilde{\gamma}_i}$ es el mínimo común múltiplo de los polinomios $\widetilde{m}_{H,1}, \ldots, \widetilde{m}_{H,i_0+1}$ en $\mathbb{Q}[\varepsilon^{1/d}][T]$.

Definimos el conjunto $S_{i_0+1} := S_{i_0} \cup \{\frac{u_{i_0+1}}{\widetilde{\gamma}_{i_0+1}}\}$. Este conjunto verifica las *condiciones iniciales* y repetimos entonces el Paso I, ahora con el conjunto S_{i_0+1}.

Debemos establecer la complejidad del ciclo i_0–ésimo que a partir del conjunto S_{i_0} en las *condiciones iniciales* obtiene un conjunto S_{i_0+1} en las *condiciones iniciales*. Para ello vemos que computamos i_0 veces el Paso I cuya complejidad asintótica es la del Lema 7. Dado que aplicamos este Lema a polinomios de grado en T acotado por D_{i_0+1} y recordando que el input del ciclo era un straight–line program β_1 de espacio $O(\widetilde{\mathcal{S}}(n+\deg(H))(\sum_{i=1}^s D_i))$ y tiempo $O((\widetilde{\mathcal{T}}\deg(H)+n^4)(\sum_{i=1}^s D_i^2)\log^2 d^n \log\log d^n)$, concluímos que la complejidad del straight–line program definido por el ciclo i_0–ésimo es $O(\widetilde{\mathcal{S}}(n+\deg(H))(\sum_{i=1}^s D_i))$ en espacio y

$O((\widetilde{\mathcal{T}}\deg(H)+n^4)(\sum_{i=1}^{i_0+1} D_{i_0+1}^2+\sum_{i=1}^{s} D_i^2)\log^2 d^n \log\log d^n) =$
$O((\widetilde{\mathcal{T}}\deg(H)+n^4)((i_0+1)D_{i_0+1}^2+\sum_{i=1}^{s} D_i^2)\log^2 d^n \log\log d^n)$ en tiempo.

Ahora bien, originalmente sabemos que el conjunto $S_1=\{\widetilde{m}_{H,1}\}$ se encuentra en lo que definimos como las *condiciones iniciales*. Iterando $s-1$ veces el ciclo anterior a partir de β_1 y S_1 obtenemos finalmente un straight–line program β_2 que computa polinomios $\widetilde{\gamma}_1,\ldots,\widetilde{\gamma}_s\in\mathbb{Q}[\varepsilon^{1/d}]$, $u_1,\ldots,u_s\in\mathbb{Q}[\varepsilon^{1/d}][T]$ tales que:

- Las funciones racionales $\frac{u_1}{\widetilde{\gamma}_1},\ldots,\frac{u_s}{\widetilde{\gamma}_s}$ pertenecen a $\mathbb{Q}[\varepsilon^{1/d}][T]$ y son polinomios mónicos en T.
- El producto $\prod_{i=1}^{s}\frac{u_i}{\widetilde{\gamma}_i}$ es el mínimo común múltiplo de los polinomios $\widetilde{m}_{H,1},\ldots,\widetilde{m}_{H,s}$, es decir es igual al polinomio minimal $\widetilde{m}_H$ de $\mathcal{M}_H$.

La complejidad del straight–line program β_2 es la siguiente: ya estimamos la compejidad del ciclo i_0– ésimo, para obtener a β_2 iteramos $s-1$ veces el ciclo anterior, por lo tanto la complejidad es $O(\widetilde{\mathcal{S}}(n+\deg(H))(\sum_{i=1}^{s} D_i))$ en espacio y $O((\widetilde{\mathcal{T}}\deg(H)+n^4)((s-1)D_s^2+(s-2)D_{s-1}^2+\ldots+D_2^2)\log^2 d^n\log\log d^n)\leq$
$\leq O((\widetilde{\mathcal{T}}\deg(H)+n^4)(s^2D_s^2)\log^2 d^n\log\log d^n)$ en tiempo.

Tomando en cuenta la relación de congruencia

$$m_H\equiv\widetilde{m}_H=\prod_{i=1}^{s}\frac{u_i}{\widetilde{\gamma}_i}\text{ módulo }(\varepsilon)^{\deg(H)d^n}$$

en $\mathbb{Q}[\varepsilon^{1/d}][T]$ (ver 43) y del hecho que $\deg(m_H)\leq\deg(H)d^n$ (ver 28) deducimos que se obtiene el polinomio m_H a partir del cálculo, para cada $1\leq k\leq D_s$, para cada $1\leq i\leq s$, de la expansión en series de potencias (en $\varepsilon^{1/d}$) hasta grado $\deg(H)d^n$ del k–ésimo coeficiente $a_{(k,i)}$ del polinomio $\frac{u_i}{\widetilde{\gamma}_i}$. Dado que para cada $1\leq i\leq s$ los polinomios $\gamma_i a_{(0,i)},\ldots,\gamma_i a_{(D_i,i)},\gamma_i\in\mathbb{Q}[\varepsilon^{1/d}]$ fueron calculados por un straight-line program sin divisiones, podemos computar los polinomios $a_{(0,i)},\ldots,a_{(D_i,i)}$ utilizando el Lema 5. Esto se realiza en espacio $O(\widetilde{\mathcal{S}}\deg(H)(n+\deg(H))(D_1^2+\ldots+D_s^2))$ y tiempo $O((\widetilde{\mathcal{T}}n\deg(H)+n^4)\deg(H)(D_1^3+\ldots+D_s^3)\log^3 d^n\log^2\log d^n)$. Por último se calcula el producto $\prod_{i=1}^{s}\frac{u_i}{\gamma_i}$, que no cambia la complejidad asintótica final. La compejidad final entonces es $O(\widetilde{\mathcal{S}}\deg(H)(n+\deg(H))(D_1^2+\ldots+D_s^2))$ en espacio y $O((\widetilde{\mathcal{T}}\deg(H)+n^4)\max(\sum_{i=1}^{s} D_i^3;\sum_{i=1}^{s}(s-1-i)D_i^2)\log^2 d^n\log\log d^n)\leq$
$O((\widetilde{\mathcal{T}}\deg(H)+n^4)\max(sD_s^3;s^2D_s^2)\log^2 d^n\log\log d^n)$ en tiempo.

□

Si el polinomio $q\in\mathbb{Q}[T]$ correspondiente a la solución geométrica de V' es irreducible en $\mathbb{Q}[T]$, el algoritmo anterior tiene las complejidades del algoritmo de [HMW99, Theorem 11]. Eso es lo que dice la siguiente Observación:

Observación 46 *Si el polinomio $q \in \mathbb{Q}[T]$ correspondiente a la solución geométrica de V' es irreducible en $\mathbb{Q}[T]$ (es decir $s = 1$), existe un straight–line program que computa los coeficientes del polinomio minimal $m_H \in \mathbb{Q}[\varepsilon][T]$ que satisface la condición $m_H(\varepsilon, H) \in (F_1, \ldots, F_n)$ utilizando espacio $O((\mathcal{S} + n + \log d)\deg(H)(n + \deg(H))(d^{2n}))$ y tiempo $O(((\mathcal{T} + n + \log d)\deg(H) + n^4)d^{3n}\log^2 d^n \log\log d^n)$.*

Demostración.– Bajo estas hipótesis, el straight–line program β_1 definido en el Teorema anterior computa un polinomio $\gamma \in \mathbb{Q}[\varepsilon^{1/d}]$ y un polinomio $\gamma\widetilde{m}_H \in \mathbb{Q}[\varepsilon^{1/d}, T]$ y tiene complejidad $O((\mathcal{S} + n + \log d)(n + \deg(H))(d^n))$ en espacio y $O(((\mathcal{T} + n + \log d)\deg(H) + n^4)(d^{2n})\log^2 d^n \log\log d^n)$ en tiempo.
Tomando en cuenta la relación de congruencia

$$m_H \equiv \widetilde{m}_H \text{ módulo } (\varepsilon)^{\deg(H)d^n}$$

en $\mathbb{Q}[\varepsilon^{1/d}][T]$ (ver 43) y del hecho que $\deg(m_H) \leq \deg(H)d^n$ (ver 28) deducimos que se obtiene el polinomio m_H a partir del cálculo, para cada $1 \leq k \leq \deg(m_H)$, de la expansión en series de potencias hasta grado $\deg(H)d^n$ del k–ésimo coeficiente $a_{(k)}$ del polinomio $\frac{\gamma\widetilde{m}_H}{\gamma}$. Para ello utilizando el Lema 5. Esto se realiza en espacio $O((\mathcal{S}+n+\log d)\deg(H)(n+\deg(H))((d^n)^2))$ y tiempo $O(((\mathcal{T}+n+\log d)n\deg(H)+n^4)\deg(H)((d^n)^3)\log^3 d^n \log^2\log d^n)$.

□

References

[Abd97] J. Abdeljaoued. *Algorithmes rapides pour le Calcul du Polynôme Caractéristique*. PhD thesis, Université de Franche Compte, Besançon, France, 1997.

[ABRW96] M. E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. In *Algorithms in Algebraic Geometry and Applications. Proceedings of MEGA'94*, volume 142 of *Progress in Mathematics*, pages 1–15. Birkhäuser, 1996.

[AHU76] A.V. Aho, J.E. Hopcroft, and J.D. Ullman. *The design and analysis of computer algorithms*. Addison–Wesley, Reading, Massachusetts, 1976.

[AM69] M.F. Atiyah and I.G. Macdonald. *Introducción al Algebra Conmutativa*. Editorial Reverté, S.A., 1969.

[Amo96] F. Amoroso. On a conjeture by c. bernstein and a. yger. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Aplications*, volume 143 of *Progress in Mathematics*, pages 17–28. Elsevier Science Publishers, 1996.

[AS88] W. Auzinger and H.J. Stetter. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. *International Series of Numerical Mathematics*, 80:11–30, 1988.

[BCA97] P. Bürgisser, M. Clausen, and M. Amin Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1997.

[BCW82] H. Bass, E. Conelle, and T. Wright. The jacobian conjeture: Reduction of degree and formal expansion of the inverse. *Bull. AMS*, 7(1), 1982.

[BDG88] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural complexity I*, volume 11 of *EATCS*. Springer, 1988.

[BGHM97] B. Bank, M. Giusti, J. Heintz, and G. Mbakop. Polar varieties and efficient real equation solving: The hypersurface case. *J. of Complexity*, 13(1):5–27, 1997.

[BM72] A. Borodin and J. Munro. *The Computational Complexity of Algebraic and Numeric Problems*. Elsevier, 1972.

[Bor93] A. Borodin. Time space tradeoffs (getting closer to the barrier ?). In *Algorithms and Computation. Proceedings 4. ISSAC*, volume 762 of *LNCS*, pages 209–220. Springer, 1993.

[BP94] D. Bini and V. Pan. *Polynomial and matrix computations*. Progress in theoretical computer science. Birkhäuser Boston–Basel–Berlin, 1994.

[Bro87] D. W. Brownawell. Bounds for the degree in the nullstellensatz. *Annals of Math.*, 126:577–591, 1987.

[BS88] D. Bayer and M. Stillman. On the complexity of computing syzygies. *Journal of Symbolic Computation*, 6:135–147, 1988.

[BS98] E. Bach and J. Shallit. *Algorithmic Number Theory*, volume I of *Foundations of Computing*. MIT Press, Cambridge, Massachusetts, London, England, 1998.

[Buc85] B. Buchberger. Gröbner bases: An algoritmic method in polynomial ideal theory. In N. K. Bose et al, editor, *Multidimensional System Theory*, pages 374–383. Reidel, Dordrecht, 1985.

[BY91a] C. Berenstein and A. Yger. Effective Bézout identities in $Q[X_1, \ldots, X_n]$. *Acta. Math.*, 166:69–120, 1991.

[BY91b] C. Berenstein and A. Yger. Une formule de jacobi et ses conséquences. *Ann. Sci. E.N.S.*, 24(4):363–377, 1991.

[Caf99] A.A. Cafure. Eliminación geométrica sobre cuerpos finitos, 1999.

[Can88] J. Canny. Some algebraic and geometric problems in PSPACE. In *Proceedings 20. ACM STOC*, pages 460–467, 1988.

[CG83] A. L. Chistov and D. Y. Grigoriev. Subexponential time solving systems of algebraic equations. LOMI preprint E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.

[CGG91] L. Caniglia, J. A. Guccione, and J. J. Guccione. Local membership problems for polynomial ideals. In T. Mora and C. Traverso, editors, *Effective Methods in Algebraic Geometry*, volume 94 of *Progress in Mathematics*, pages 31–45. Birkhäuser, 1991.

[CGH88] L. Caniglia, A. Galligo, and J. Heintz. Borne simple exponentielle pour les degrés dans le théorème des zéros sur un corps de charactéristique quelconque. *C. R. Acad. Sci. Paris*, 307:255–258, 1988.

[CGH89] L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. In T. Mora et al, editor, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes. Proceedings of AAECC-6*, volume 357 of *LNCS*, pages 131–152. Springer, 1989.

[CGH+99] D. Castro, M. Giusti, J. Heintz, G. Matera, and L.M. Pardo. Data structures and smooth interpolation procedures in elimination theory. Manuscrito de 49 hojas, 1999.

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: an introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts in Mathematics. Springer Verlag, Berlin, 1992.

[Col67] G.E. Collins. Subresultants and reduced polynomial sequences. *Journal of the Association for Computing Machinery*, 14:128–142, 1967.

[Dav96] J. H. Davenport. Prooving and certifying polynomial irreducibility. *Submitted to Math. Comp.*, 1996.

[Dav98] J. H. Davenport. Galois group and the simplification of polynomials. *Journal*, pages 1–17, 1998.

[DFGS91] A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Applied Mathematics*, 33:73–94, 1991.

[DH88] J. H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *Journal of Symbolic Computation*, 5:29–35, 1988.

[Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. GTM 150. Springer, 1995.

[FF63] D.K. Faddeev and V.N. Faddeeva. *Computational methods of linear algebra*. W.H. Freeman, San Francisco, 1963.

[FG90] Noai Fitchas and A. Galligo. Nullstellensatz effectif et conjecture de serre (théorème de quillen-suslin) pour le calcul formel. *Math. Nachr.*, 149:231–253, 1990.

[FGM90a] N. Fitchas, A. Galligo, and J. Morgenstern. Algorithmes rapides en sequentiel et en parallele pour l'élimination des quantificateurs en Géométrie élementaire. *Seminaire sur les structures algebraiques ordonnees*, pages 103–145, 1990.

[FGM90b] N. Fitchas, A. Galligo, and J. Morgenstern. Precise sequential and parallel complexity bounds for quantifier elemination over algebraically closed fields. *Journal of Pure and Applied Algebra*, 67:1–14, 1990.

[FGS95] N. Fitchas, M. Giusti, and F. Smietanski. Sur la complexité du théorème des zéros. In J. Guddat et al, editor, *Approximation and Optimization in the Caribbean II, Proceedings 2nd Int. Conf. on Non-Linear Optimization and Approximation*, volume 8 of *Approximation and Optimization*, pages 247–329. Peter Lange Verlag, Frankfurt am Main, 1995.

[Ful84] W. Fulton. *Intersection Theory*, volume 2 of *Ergebnisse der Mathematik*. Springer, 1984.

[GH93] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In

D. Eisenbud and L. Robbiano, editors, *Computational Algebraic Geometry and Commutative Algebra*, volume XXXIV of *Symposia Matematica*, pages 216–256. Cambridge University Press, 1993.

[GHH+97] M. Giusti, K. Hägele, J. Heintz, J. E. Morais, J. L. Montaña, and L. M. Pardo. Lower bounds for diophantine approximation. In *Proceedings of MEGA'96*, volume 117,118, pages 277–317. Journal of Pure and Applied Algebra, 1997.

[GHM+98] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo. Straight–line programs in geometric elimination theory. *J. of Pure and App. Algebra*, pages 1–46, 1998.

[GHMP95] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. When polynomial equation systems can be solved fast ? In G. Cohen, H. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

[GHS93] M. Giusti, J. Heintz, and J. Sabia. On the efficiency of effective nullstellensätze. *Computational Complexity*, 3:56–95, 1993.

[GJ79] M. Garey and D. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. Freeman, San Francisco, 1979.

[GLS99] M. Giusti, G. Leceref, and B. Salvy. A new algorithm to solve polynomial equations implemented en magma system. Manuscrito École Polytechnique, 1999.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comput. Sci.*, 24(3):239–277, 1983.

[HKP+98] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein. Deformation techniques for efficient polynomial equation solving. In T. Lickteig, M. Shub, F. Cucker, M.–F. Roy editors, *Journal of Complexity* (special issue "Complexity and Continuous Algorithms"), 2000.

[HMPS97] K. Hägele, J. E. Morais, L. M. Pardo, and M. Sombra. On the intrinsic complexity of the arithmetic nullstellensatz. In *Proceedings of TERA'97, Córdoba, Argentina*, September 1997.

[HMPS98] K. Hägele, J. E. Morais, L. M. Pardo, and M. Sombra. On the intrinsic complexity of the arithmetic nullstellensatz. Preprint 4/99 Depto. Matemáticas, Universidad de Cantabria, Santander, Spain, april 1998.

[HMPW98] J. Heintz, G. Matera, L. M. Pardo, and R. Wachenchauzer. About the intrinsic complexity of elimination. WAIT'97, Buenos Aires, Argentina, 1998.

[HMW99] J. Heintz, G. Matera, and A. Waissbein. On the time–space complexity of geometric elimination procedures. Manuscript 61 pages, submitted to AAECC Journal, 1999.

[HS80] J. Heintz and M. Sieveking. Lower bounds for polynomials with algebraic coefficients. *Theo. Comp. Sci.*, 11:321–330, 1980.

[HS80] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute. In *Proccedings of ACM 12th Symposium on Theory of Computing* , 262-272, 1980.

[HS82] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute. In *Logic and Algorithmic*, volume 30 of *Monographie de l'Enseignement Mathématique*, pages 237–254, 1982.

[HW75] J. Heintz and R. Wüthrich. An efficient quantifier elimination algorithm for algebraically closed fields of any characteristic. *SIGSAM Bulletin*, 9(4):11, 1975.

[IM83] O. H. Ibarra and S. Moran. Equivalence of straight-line programs. *Journal of the ACM*, 30:217–228, 1983.

[IMR81] O. H. Ibarra, S. Moran, and L. E. Rosier. Probabilistic algorithms and straight-line programs for some rank decision problems. *Information Processing Letters*, 12(5):227–232, 1981.

[Ive73] B. Iversen. *Generic local structure of the morphisms in Commutative Algebra*, volume 310 of *LNM*. Springer, 1973.

[Ja'83] J. Ja'Ja'. Time–space tradeoffs for some algebraic problems. *Journal of the Association for Computing Machinery*, 30(3):657–667, 1983.

[Kal86] E. Kaltofen. Uniform closure properties of P-computable functions. In *Proceedings of the 18th Ann. ACM Symposium on Theory of Computing (Berkeley, CA)*, pages 330–337, New York, 1986. ACM, ACM Press.

[Kal94] E. Kaltofen. Asymptotically fast solution of toeplitz–like singular linear systems. In J. von zur Gathen and M. Giesbrecht, editors, *Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation, ISSAC'94 (Oxford, July 20–22 1994)*, ACM Press, pages 297–304, New York, 1994. ACM.

[Kol88] J. Kollár. Sharp effective nullstellensatz. *J. of the AMS*, 1:963–975, 1988.

[KP96] T. Krick and L. M. Pardo. A computational method for diophantine approximation. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications. Proceedings of MEGA'94*, volume 143 of *Progress in Mathematics*, pages 193–254. Birkhäuser Verlag, 1996.

[Kro82] L. Kronecker. Grundzüge einer arithmetischen theorie de algebraischen grössen. *J. reine angew. Math.*, 92:1–122, 1882.

[Kru28] W. Krull. Primidealketten in allgemmeinen ringbereichen. *S.–B. Heidelberg Akad. Wiss.*, 7, 1928.

[KSS97] T. Krick, J. Sabia, and P. Solernó. On intrinsic bounds in the nullstellensatz. *Applicable Algebra in Engineering Communications and Computing (AAECC Journal)*, 8:125–134, 1997.

[Kun85] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, 1985.

[Laz81] D. Lazard. Résolution des systèmes d'équations algébriques. *Theo. Comp. Sci.*, 15:77–110, 1981.

[LV93] D. Lazard and A. Valibouze. Computing subfields: reverse and primitive element problem. In *Proceedings MEGA '92*, volume 109 of *Progress in Mathematics*, pages 163–176. Bifhäuser, Boston, 1993.

[Mat86] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, 1986.

[Mat97] G. Matera. *Sobre la complejidad en espacio y tiempo de la eliminación geométrica.* PhD thesis, Universidad de Buenos Aires, Argentina, 1997.

[Mis93] B. Mishra. *Algorithmic Algebra.* Springer Verlag, New York, 1993.

[ML78] R. A. De Millo and R. J. Lipton. A probabilistic remark on algebraic program testing. *Inf. Proc. Letters*, 7(4):193–195, 1978.

[MM82] E. Mayr and A. Meyer. The complexity of the word problem for commutative semigroups. *Adv. in Math.*, 46:305–329, 1982.

[MMP96] J. L. Montaña, J. E. Morais, and L. M. Pardo. Lower bounds for arithmetic networks II: Sum of betti numbers. *Applicable Algebra in Engineering Communications and Computing*, 7:41–51, 1996.

[Mor97] J. E. Morais. *Resolución eficaz de sistemas de ecuaciones polinomiales*. PhD thesis, Universidad de Cantabria, Santander, Spain, 1997.

[MP93] J. L. Montaña and Luis M. Pardo. Lower bounds for arithmetic networks. In *AAECC-4*, AAECC, pages 1–24. Springer, 1993.

[Mum88] David Mumford. *The Red Book of Varieties and Schemes*, volume 1358 of *LNM*. Springer, Berlin, 1 edition, 1988.

[Mus78] D. R. Musser. On the efficiency of a polynomial irreducibility test. *J. ACM*, 25:271–282, 1978.

[Ost54] A. M. Ostrowski. On two problems in abstract algebra connected with horner's rule. In *Studies in Math. and Mech. presented to Richard von Mises*, pages 40–48. Academic Press, 1954.

[Par95] Luis M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, H. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes. Proceedings of AAECC-11*, volume 948 of *LNCS*. Springer, 1995.

[Phi91] P. Philippon. Sur des hauteurs alternatives, I. *Math. Ann.*, 289:255–283, 1991.

[Phi94] P. Philippon. Sur des hauteurs alternatives, II. *Ann. Inst. Fourier, Grenoble*, 44(2):1043–1065, 1994.

[Phi95] P. Philippon. Sur des hauteurs alternatives, III. *J. Math. Pures Appl.*, 74:345–365, 1995.

[Rou96] F. Rouillier. *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux*. PhD thesis, Université de Rennes I, France, 1996.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, October 1980.

[Sen90] J.R. Sendra. *Algoritmos simbólicos de Hankel en álgebra computacional*. PhD thesis, Universidad de Alcalá de Henares, Madrid, Spain, 1990.

[Sha84] I.R. Shafarevich. *Basic algebraic geometry*. Graduate Texts in Mathematics. Springer-Verlag, 1984.

[Sie72] M. Sieveking. Algorithm for division of power series. *Computing*, 10:153–156, 1972.

[SL92] R. Sendra and J. Llovet. An extended polynomial gcd algorithm using hankel matrices. *Journal of Symbolic Computation*, 13:25–39, 1992.

[Som96] M. Sombra. Bounds for the hilbert function of polynomial ideal and for the degrees in the nullstellensatz. In *Proceedings of MEGA'96*. North-Holland, 1996.

[SS94] M. Shub and S. Smale. Complexity of Bézout's theorem V: Polynomial time. *Theor. Comp. Sci.*, 133:141–164, 1994.

[SS96] J. Sabia and P. Solernó. Bounds for traces in complete intersections and degrees in the nullstellensatz. *Applicable Algebra in Engineering Communications and Computing (AAECC Journal)*, 6:353–376, 1996.

[Str73] V. Strassen. Vermeidung von divisionen. *Crelle J. Reine Angew. Math,*, 264:182–202, 1973.

[Str90] V. Strassen. Algebraic complexity theory. In *Handbook of Theoretical Computer Science*, chapter 11, pages 634–671. Elsevier, 1990.

[vdW54] B.L. van der Waerden. *Science Awakening*. P. Noordhoff Ltd. – Groningen, Holland, 1954.

[Vog84] W. Vogel. *Results on Bezout's Theorem*. Tata Institute of Fundamental Research. Springer, 1984.

[vzG86] J. von zur Gathen. Parallel arithmetic computations: a survey. In B. Rovan J. Gruska and J. Wiedermann, editors, *Proceedings of the 12th Symposium on Mathematical Foundations of Computer Science*, volume 233 of *LNCS*, pages 93–112, Bratislava, Czechoslovakia, August 1986. Springer.

[vzG93] J. von zur Gathen. Parallel linear algebra. In John H. Reif, editor, *Synthesis of Parallel Algorithms*. Morgan Kaufmann, 1993.

[Wai99] A. Waissbein. Eliminación en la argentina. Master's thesis, FCEyN, Universidad de Buenos Aires, Argentina, 1999.

[Wal78] R.J. Walker. *Algebraic curves*. Springer-Verlag, Berlin Heidelberg New York, 1978.

[WB93] V. Weispfenning and T. Becker. *Groebner bases: a computational approach to commutative algebra*, volume 141 of *Graduate Texts in Mathematics: readings in mathematics*. Springer, 1993.

[Wei88] V. Weispfennig. The complexity of linear problems in fields. *Journal of Symbolic Computation*, 5(5):3–27, 1988.

[Yap91] C.K. Yap. A new lower bound construction for commutative thues systems with applications. *Journal of Symbolic Computation*, 12:1–27, 1991.

[Zar95] O. Zariski. *Algebraic surfaces*. Classics in Mathematics. Springer Verlag, 1995.

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings EUROSAM' 79*, volume 72 of *LNCS*, pages 216–226, 1979.

[Zip90] R. Zippel. Interpolating polynomials from their values. *J. Symbol. Comput.*, 9:147–175, 1990.

[Zip93] R. Zippel. *Effective Polynomial Computation*. ECS 241. Kluwer Academic Publishers, 1993.