Biblioteca Digital
F C E N - U B A

BIBLIOTECA CENTRAL LUIS F LELOIR
BIBLIOTECA CENTRAL LELOIR
FACULTAD DE CIENCIAS EXACTAS Y NATURALES UBA

Tesis de Posgrado

La complejidad algorítmica del álgebra lineal en anillos de polinomios-teorema de Serre-Quillen-Suslin en cálculo formal

Danon, Silvia Perla Lucía

1990

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

Este documento forma parte de la colección de tesis doctorales y de maestría de la Biblioteca Central Dr. Luis Federico Leloir, disponible en digital.bl.fcen.uba.ar. Su utilización debe ser acompañada por la cita bibliográfica con reconocimiento de la fuente.

This document is part of the doctoral theses collection of the Central Library Dr. Luis Federico Leloir, available in digital.bl.fcen.uba.ar. It should be used accompanied by the corresponding citation acknowledging the source.

Cita tipo APA:
Danon, Silvia Perla Lucía. (1990). La complejidad algorítmica del álgebra lineal en anillos de polinomios-teorema de Serre-Quillen-Suslin en cálculo formal. Facultad de Ciencias Exactas y Naturales. Universidad de Buenos Aires.
http://digital.bl.fcen.uba.ar/Download/Tesis/Tesis_2311_Danon.pdf

Cita tipo Chicago:
Danon, Silvia Perla Lucía. "La complejidad algorítmica del álgebra lineal en anillos de polinomios-teorema de Serre-Quillen-Suslin en cálculo formal". Tesis de Doctor. Facultad de Ciencias Exactas y Naturales. Universidad de Buenos Aires. 1990.
http://digital.bl.fcen.uba.ar/Download/Tesis/Tesis_2311_Danon.pdf

EXACTAS UBA
Facultad de Ciencias Exactas y Naturales

UBA
Universidad de Buenos Aires

Dirección: Biblioteca Central Dr. Luis F. Leloir, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires. Intendente Güiraldes 2160 - C1428EGA - Tel. (++54 +11) 4789-9293

Contacto: digital@bl.fcen.uba.ar

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

DEPARTAMENTO DE MATEMATICA

LA COMPLEJIDAD ALGORITMICA DEL ALGEBRA LINEAL EN ANILLOS DE POLINOMIOS-TEOREMA DE SERRE-QUILLEN-SUSLIN EN CALCULO FORMAL

autora: SILVIA DANON
director: JOOS HEINTZ
lugar de trabajo: Dpto. de Matemática de la FCEN

TESIS PRESENTADA PARA OPTAR AL TITULO DE DOCTOR DE LA UNIVERSIDAD DE BUENOS AIRES

Buenos Aires, marzo de 1990

2311
ej. 2

Resumen: Sea F una matriz de r filas y s columnas con coeficientes en un anillo de polinomios de n variables sobre un cuerpo infinito k. Notemos con deg(F) el máximo de los grados de los coeficientes de F y sea d:= 1+ deg(F).

Se describe un algoritmo que computa una matriz unimodular M de s filas y s columnas, con $\deg(M)=(rd)^{O(n)}$, y tal que $F.M= [I_r,0]$, donde $[I_r,0]$ nota la matriz de r filas y s columnas obtenida agregando a la matriz identidad I_r, s-r columnas de ceros.

El algoritmo se presenta como una red aritmética con entradas en k y para la complejidad se considera que el costo de cada operación en k y de cada comparación es 1.

La complejidad secuencial de este algoritmo es $s^{O(r^2)}r^{O(n^2)}d^{O(n^2+r^2)}$ (o sea cantidad de operaciones en el cuerpo y comparaciones), mientras que la complejidad paralela es $O(n^4r^4\log^2(srd))$.

Se demuestra que las cotas para el grado de M y para las complejidades mencionadas, son óptimas en orden. Este algoritmo está inspirado en la demostración de Suslin de la Conjetura de Serre.

Introduccion:

En este trabajo se consideran los métodos de Suslin ([16],Chap.III,§1) para resolver la Conjetura de Serre bajo una perspectiva algoritmica y de complejidad algebraica.

Por "Conjetura de Serre", entenderemos el siguiente enunciado: Todo fibrado vectorial algebraico localmente trivial sobre un espacio afín es (globalmente) trivial.(En realidad en su famoso trabajo [FAC], Serre solamente señaló que no se conocía ningún ejemplo de un fibrado vectorial algebraico sobre un espacio afín no trivial).

En [FAC] los fibrados vectoriales algebraicos localmente triviales son interpretados como haces coherentes localmente libres.

Esta interpretación de los fibrados vectoriales nos permite reformular la Conjetura de Serre en la siguiente forma puramente algebraica:

Sea k un cuerpo y $R:=k[X_1,\dots,X_n]$, el anillo de polinomios en las variables $X_1,\dots,X_n$ sobre k. Cualquier R-módulo proyectivo finitamente generado es libre.

Usando un teorema de Serre ([16],Chap.III,Theorem 5.8), esta forma de la Conjetura de Serre puede ser reducida al siguiente enunciado en términos de álgebra lineal sobre el anillo de polinomios R:

Sea $F\in R^{r\times s}$ una matriz unimodular (esto es inversible a derecha en R) Entonces existe una matriz cuadrada unimodular $M\in R^{s\times s}$ tal que $F.M=[I_r,0]$, donde $[I_r,0]$ nota la matriz de rxs obtenida agregando a la matriz identidad I_r, s-r columnas de ceros.

Quillen y Suslin probaron en 1976 independientemente y con diferentes métodos este último enunciado, contestando así la Conjetura de Serre en forma afirmativa.(Ver [16] y [15] para una historia de la Conjetura de Serre, sus motivaciones y aplicaciones)

Veamos brevemente como se efectúa esta última reducción:

Definicion: Sea R un anillo conmutativo. Un R-módulo P se dice **establemente libre de tipo r** ($0 \leq r < \infty$) si $P \oplus R^r$ es libre. Un módulo se dice **establemente libre** si es establemente libre de tipo r para algún r. Restrinjamos nuestra atención a los módulos finitamente generados (f.g.) Un módulo P f.g. es establemente libre si y sólo si $P \cong \ker(R^s \xrightarrow{f} R^r)$ para algún epimorfismo f. Si F es la rxs matriz asociada a f, entonces F es inversible a derecha (o sea existe una matriz N de sxr tal que $M.N = I_r$). Recíprocamente toda matriz F de rxs inversible a derecha define un módulo finitamente generado establemente libre de tipo r, a saber $P = \{ v = (v_1,\dots,v_s) \text{ tq. } F.^t v = 0 \}$ (el espacio solución de F). En este sentido estudiar los módulos f.g. establemente libres es equivalente a estudiar matrices rectangulares inversibles a derecha sobre R.

La siguiente proposición establece un criterio para decidir si un módulo $P \cong \ker(R^s \xrightarrow{f} R^r)$ es libre.

Proposicion: Sea $P \cong \ker(R^s \xrightarrow{f} R^r)$, donde f es un epimorfismo. Entonces P es libre si y sólo si f puede levantarse a un isomorfismo $\bar{f} : R^s \longrightarrow R^r \oplus R^{s-r}$ tal que $\pi.\bar{f} = f$, donde $\pi: R^r \oplus R^{s-r} \longrightarrow R^r$ es la proyección .

Demostracion: Supongamos que $\bar{f}$ existe, entonces $\ker f \cong \ker \pi = R^{s-r}$. Recíprocamente supongamos que $P \cong R^t$ para algún t, y sea g el isomorfismo Pongamos $R^s = Q \oplus P$, luego la restricción de f a Q da un isomorfismo f_o, $f_o: Q \longrightarrow R^r$. Luego $f_o \oplus g: R^s \longrightarrow R^r \oplus R^t$ es el isomorfismo $\bar{f}$ (y se tiene $t = s-r$) ∎

Observemos que si F es la matriz de rxs que corresponde a f, y N la matriz inversible que corresponde a $\bar{f}$, la condición $\pi.\bar{f} = f$ dice que

F es una submatriz de N consistente en sus r primeras filas.

Podemos entonces reformular la proposición en términos de matrices:

Sea F una matriz de rxs inversible a derecha. Entonces el módulo establemente libre P, espacio solución de M, es libre si y sólo si F puede completarse a una matriz cuadrada inversible agregando filas.

Para cualquier anillo R las siguientes condiciones son equivalentes:

(i) todo módulo f.g. establemente libre es libre.

(ii) todo módulo f.g. establemtente libre de tipo 1 (o sea núcleo de una matriz de 1xs) es libre.

(iii) toda fila unimodular puede completarse a una matriz inversible.

Los anillos que satisfacen estas condiciones se llaman **anillos de Hermite.**

Observacion: Una fila unimodular $[a_1,\dots,a_s]$ puede completarse a una matriz inversible N si y sólo si existe una matriz unimodular M de sxs tal que $[a_1,\dots,a_s].M = [1,0,\dots,0]$.

Demostración: Si $[a_1,\dots,a_s]$ puede completarse a una matriz N inversible basta tomar $M = N^{-1}$. Si existe M inversible tal que $[a_1,\dots,a_s].M=[1,0..0]$ entonces $[a_1,\dots,a_s]$ es la primer fila de M^{-1}.■

Sea ahora $R = k[X_1,\dots,X_n]$.El teorema de Serre ([16],Chapter II,Theo.5.8) prueba que todo R-módulo proyectivo f.g. es establemente libre. Luego la Conjetura de Serre puede formularse ahora de la siguiente manera: es $R = k[X_1,\dots,X_n]$ un anillo de Hermite?, o sea , es cierto que toda fila unimodular puede completarse a una matriz inversible?

El problema se ha reducido entonces a lo siguiente: Sea k un cuerpo infinito de característica arbitraria y $f = [f_1,\dots,f_s]$ un vector de s polinomios de grado d en las variables $X_1,\dots,X_n$, unimodular (esto es, que

$f: k[X_1,\dots,X_n]^s \dashrightarrow k[X_1,\dots,X_n]$, $v \dashrightarrow f.{}^t v$, es un epimorfismo,

o equivalentemente, el ideal generado por $f_1,\dots,f_s$ es trivial). Entonces existe una matriz cuadrada M de sxs a coeficientes en $k[X_1,\dots,X_n]$ tal que $[f_1,\dots,f_s].M = [1,0,\dots,0]$.

Idea de la demostracion (Suslin)(ver [16]):

Se eliminan las variables una a una, o sea se prueba que existe una matriz unimodular M_n de sxs que verifica

$[f_1(X_1,\dots,X_n),\dots,f_s(X_1,\dots,X_n)].M_n = [f_1(X_1,\dots,X_{n-1},0),\dots,f_s(X_1,\dots,X_{n-1},0)]$

Una vez conseguido esto, $M:= M_n.M_{n-1}\dots M_1$ verifica:

$[f_1(X_1,\dots,X_n),\dots,f_s(X_1,\dots,X_n)].M = [f_1(0,\dots,0),\dots,f_s(0,\dots,0)]$

Como el último vector pertenece a k^s es trivial encontrar una matriz A tal que $[f_1(0,\dots,0),\dots,f_s(0,\dots,0)].A = [1,0,\dots,0]$.

Entonces el punto es ver cómo probar que existen las matrices M_k. En general, cúando existirá una matriz M unimodular que permita hacer

$$[f_1(X_1,\dots,X_{n-1},b),\dots,f_s(X_1,\dots,X_{n-1},b)].M = \\ = [f_1(X_1,\dots,X_{n-1},b'),\dots,f_s(X_1,\dots,X_{n-1},b')]$$

con $b, b' \in k[X_1,\dots,X_n]$.

Digamos que $b \sim b'$ si existe una tal matriz. Dados $f_1,\dots,f_s$ se define el conjunto

$$\mathcal{C}_{f_1,\dots,f_s} = \{ c \in k[X_1,\dots,X_n] \text{ tq.para todo par } b,b', \text{ vale que } (b \equiv b'_{(\mathrm{mod}\ c.R)} \Rightarrow b \sim b') \}$$

Se prueba que $\mathcal{C}$ es un ideal y que coincide con R, en particular como $X_n \equiv 0_{(\mathrm{mod}\ 1.R)}$, resulta $X_n \sim 0$ y existe entonces M_n.

Usando estas ideas el grupo Noaï Fitchas demostró la siguiente versión cuantitativa y algorítmica de este teorema:

sea k un cuerpo infinito, sean $f_1,\dots,f_s \in R=: k[X_1,\dots,X_n]$,

$d:=1+\max_{1\le i,j\le s}\{\deg(f_i)\}$, y supongamos que $F:=[f_1,\dots,f_s]\in R^{1\times s}$ es un vector fila unimodular. Entonces existe una matriz cuadrada $M = [m_{ij}]\in R^{s\times s}$ tal que

(i) M es unimodular

(ii) $F.M = [1,0,\dots,0] \in R^{1\times s}$

(iii) $\deg(M):=\max_{1\le i,j\le s}\{\deg(m_{ij})\} \le d^{O(n)}$

(iv) M es un producto de $(n^2s^2d^2)$ matrices que son o bien elementales, o bien de la forma $\begin{bmatrix} T & 0 \\ 0 & I_{s-2}\end{bmatrix}$, para alguna matriz $T \in SL_2(R)$.

(v) una matriz que verifique las propiedades (i)a(iv) puede ser computada

en tiempo secuencial: $s^4\, d^{O(n^2)}$

tiempo paralelo: $O(n^4 \log^2 sd)$

Para demostrar el Teorema de Quillen- Suslin constructivamente definimos a partir de $f_1,\dots,f_s$ un conjunto

$C_{f_1,\dots,f_s} = \{\ c\in k[X_1,\dots,X_n]$ tq.para todo par b,b' vale que si $b \equiv b' \mod(c.R)$, entonces existe una matriz M que se puede exhibir tal que

$$[f_1(X_1,\dots,X_{n-1},b),\dots,f_s(X_1,\dots,X_{n-1},b)].M = [f_1(X_1,\dots,X_{n-1},b'),\dots,f_s(X_1,\dots,X_{n-1},b')]\}$$

La idea es caracterizar el conjunto C, dar la forma de construir las matrices correspondientes, y encontrar en él suficientes elementos c_i como para escribir $1 = \sum a_i.c_i$, con $a_i\in k[X_1,\dots,X_n]$.

Este algoritmo constituye una demostración constructiva y más elemental y directa del Teorema de Suslin, y no se incluye en este trabajo ya que el algoritmo que se detallará lo contiene como un caso particular.

La Conjetura de Serre representa además un caso particular del

problema general de resolver sistemas de ecuaciones lineales en el anillo de polinomios R.

Los aspectos cuantitativos y algorítmicos de este problema fueron estudiados por primera vez en 1926,en un artículo de G.Herrmann [14],y reconsiderados luego en [20] y en numerosos artículos sobre bases de Grobner (ver [5] y las referencias dadas allí).

El problema general de resolver sistemas de ecuaciones lineales en anillos de polinomios es espacio exponencial-completo e involucra necesariamente cotas doblemente exponenciales (en el número de variables) para los grados de los polinomios que aparecen como solución.(ver [17],[1])

Consideremos, como un caso particular, el problema (general) de representación para ideales polinomiales:

dados polinomios $f,f_1,\dots,f_s \in R=k[X_1,\dots,X_n]$,tales que f pertenece al ideal generado por $f_1,\dots,f_s$, consideramos el problema de encontrar una representación $f= m_1f_1 +\dots+m_sf_s$ con $m_1,\dots,m_s \in R$

Se sigue,de [Ma-Me] que $m_1,\dots,m_s$ pueden tener grados mayores que una cota inferior que es doblemente exponencial en n.

Sin embargo, si f=1, el problema de encontrar una representación $1=m_1f_1+\dots+m_sf_s$ admite una cota superior simplemente exponencial para los grados de $m_1,\dots,m_s$.Más precisamente vale el siguiente Nullstellensatz efectivo:

sean $f_1,\dots,f_s \in R=k[X_1,\dots,X_n]$, $d:=\max_{1\le i\le s}\{ \deg(f_i)\}$ (donde deg nota el grado total), y supongamos $n > 1$ y $d \geq 3$. Entonces $1\in (f_1,\dots,f_s)$ si y sólo si existen $m_1,\dots,m_s \in R$ tales que $1= m_1f_1+\dots+m_sf_s$ con $\max_{1\le i\le s}\deg(m_if_i)\le d^n$. (Ver [10], [4], o [22] y las referencias dadas allí. Pueden encontrarse demostraciones elementales de este teorema en [10],

[19], o [7]).

La condición $1\in(f_1,\dots,f_s)$ significa que el vector fila $f:=[f_1,\dots,f_s]$ perteneciente a $R^{1\times s}$ es unimodular. El teorema de Quillen-Suslin ([16], Chapter III, Theo. 1.8 y Remark 1.10), dice que bajo estas hipótesis existe una matriz unimodular $M\in R^{s\times s}$ tal que $F.M=[1,0\dots0]$. Esto implica que la primer columna $\begin{bmatrix} m_1 \\ \vdots \\ m \end{bmatrix}$ de M satisface $1=m_1f_1+\dots+m_sf_s$. En particular la demostración de Suslin muestra la existencia de una tal matriz unimodular M, resolviendo así el problema de encontrar una representación de 1 como combinación lineal de $(f_1,\dots,f_s)$. Sin enbargo, las cotas para los grados y para la complejidad que se obtienen revisando esta demostración desde un punto de vista algorítmico son muy gruesas.(ver [8] y [21]). Cabe señalar que el orden de las cotas encontradas en el trabajo del grupo Noaï Fitchas mencionado anteriormente(polinomiales en s y simplemen exponenciales en n), no puede ser mejorado ,como muestra un conocido ejemplo de Mora,Lazard,Masser y Philippon.(ver[3]). Es natural ahora preguntarse si la solución general de la Conjetura de Serre (como fue enunciada antes) admite también cotas simplemente exponenciales para los grados y para la complejidad. Desde el punto de vista **constructivo** esto puede hacerse iterando el algoritmo para una fila, pero esto conduce a cotas que son **doblemente exponenciales** en el número de filas de la matriz En este trabajo se contesta esta pregunta afirmativamente demostrando el siguiente teorema:

sea k un cuerpo infinito , $R:= k[X_1,\dots,X_n]$, y $F\in R^{s\times s}$ una matriz unimodular con coeficientes polinomios.Sea $d:= 1+ \deg(F)$.Entonces existe una matriz cuadrada $M\in R^{s\times s}$ tal que:

(i) M es unimodular

(ii) $F.M = [\ I_r, 0] \in R^{r\times s}$

(iii) $\deg(M) = (rd)^{O(n)}$

(iv) M es un producto de $O(n^2 s^2 (rd^{2n}))$ matrices, que son o bien elementales o bien de la forma $\begin{bmatrix} \Gamma & 0 \\ 0 & I_{s-r-1} \end{bmatrix}$ para alguna matriz $\Gamma \in SL_{r+1}(R)$.

(v) una matriz M que verifique las propiedades (i)a(iv) puede ser computada en tiempo secuencial: $s^{O(r^2)}\ r^{O(n^2)}\ d^{O(n^2+r^2)}$

tiempo paralelo: $O(n^4\ r^4\ \log^2(srd))$

mediante un arithmetical network con entradas en k (ver [13] o [11] para la noción de arithmetical network).

Este resultado es además un caso particular del problema general de resolver sistemas de ecuaciones lineales en el anillo de polinomios R, con la propiedad de que admita cotas simplemente exponenciales para la complejidad y los grados.

Finalmente, observemos que los resultados permiten computar en tiempo simplemente exponencial una base del R-módulo libre dado como el núcleo de una matriz unimodular sobre R.

Este trabajo incluye además dos apéndices, en el primero se da un test eficiente para decidir si un módulo dado por generadores y relaciones sobre el anillo de polinomios es proyectivo (y por lo tanto libre), en el segundo se da un algoritmo para resolver sistemas de ecuaciones lineales con coeficientes polinomiales con la siguiente complejidad:

tiempo secuencial: $m^{O(1)}$

tiempo paralelo: $(\log m)^{O(1)}$

donde m es el tamaño del sistema.

Preliminares

(1.1) Notaciones: Sea k un cuerpo infinito con clausura algebraica $\bar{k}$ y sea $R:= k[X_1,\dots,X_n]$. Sea $Q=[q_{ij}]$ una matriz polinomial con coeficientes q_{ij} en R. Se define $\deg(Q):= \max_{i,j} \{\deg(q_{ij})\}$.(como es usual, deg nota el grado total en $X_1,\dots,X_n$)

Q_j notará la j-ésima columna de Q.Una matriz Q de m columnas será escrita a veces como $|Q_1,\dots,Q_m|$.Más generalmente, si $I=(i_1,\dots,i_r)$ es una sucesión de números naturales con $1 \leq i_1<\dots<i_r\leq m$, Q_I notará la matriz $Q_I:=[Q_{i_1},\dots,Q_{i_r}]$. De aquí en más fijamos una matriz $F=[f_{ij}]\in R^{r\times s}$, donde $r\leq s$, y sea $d:= 1+ \deg (F)$.

(1.2) Observación: También llamaremos F a la aplicación R-lineal

$$R^s \longrightarrow R^r$$
$$g \longrightarrow g\ {}^tF$$

donde ${}^tF$ es la matriz de $s\times r$ obtenida al trasponer F.

Las siguientes condiciones son equivalentes:

(i) $F: R^s\to R^r$ es un epimorfismo

(ii) el ideal de R generado por todos los $r\times r$ subdeterminantes de la matriz F es trivial (o sea contiene al 1)

Demostración:

(i)$\Rightarrow$(ii) La propiedad de ser epimorfismo se preserva bajo especializaciones de los coeficientes de la matriz, luego si todos los menores de tamaño r tuvieran un cero en común $(a_1,\dots,a_n)$, $\operatorname{rango}[f_{ij}(a_1,\dots,a_n)] < r$, y no sería epimorfismo.

(ii)$\Rightarrow$(i) Sea $1 = \sum c_i.D_i$ donde D_i recorre todos los subdeterminantes de $r\times r$. Desarrollando cada uno de estos determinantes por la primer fila y reagrupando los términos obtenemos $1 = \sum f_{1i}.a_i$ para ciertos a_i, y es

inmediato verificar que $F.^t(a_1,\dots,a_s) = (1,0,\dots,0)$. Haciendo lo mismo para cada fila se obtiene que F es un epimorfismo.■

(1.3) Definición: La matriz F se dirá unimodular si satisface las condiciones (i) y (ii) de (1.2).

(1.3.1)Ejemplos: En el caso r=1 la matriz fila $F=[f_1,\dots,f_s]$ es unimodular si y sólo si el ideal $(f_1,\dots,f_s)$ es trivial.

En el caso r=s la matriz cuadrada F es unimodular si y sólo si su determinante pertenece a $k-\{0\}$, o sea sii F es inversible en $R^{s\times s}$.

(1.4)Notaciones: I_r notará la matriz identidad de rxr. Si A y B son matrices cuadradas, entonces $A\oplus B$ notará la matriz $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$.

Una matriz cuadrada se dice **elemental** si es igual a la matriz identidad salvo,eventualmente, un coeficiente no nulo fuera de la diagonal.

$SL_m(R)$ es el subconjunto de $R^{m\times m}$,de matrices de determinante 1.

(1.5) Observación:

Sea $Z=[z_{ij}]\in R^{s\times r}$. Entonces F.Z es una matriz de rxr que satisface:

$$\det(F.Z) = \sum_I \det(F_I) .^t\det((Z)_I)$$

donde I recorre todas las posibles suceciones de números naturales $(i_1,\dots,i_r)$, con $1 \le i_1<\dots<i_r \le s$.

Esta identidad se conoce con el nombre de Fórmula de Binet-Cauchy y puede encontrarse una demostración de la misma en [12],Chapter I,§ 2. Esta fórmula se usará repetidas veces en este trabajo, una primer consecuencia es la siguiente:

sea $A=[a_{ij}]$ la matriz unimodular de s×s:

$$\left[\begin{array}{cccccc|cccc} X_n & 1 & & & & & & & & \\ & X_n & 1 & & & & & & & \\ & & \ddots & \ddots & & & & & & \\ & & & & X_n & & 1 & & & \\ \hline & & & & & & 0 & 1 & & \\ & & & & & & & 0 & 1 & \\ & & & & & & & & 0 & \ddots \\ & & & & & & & & & 1 \\ 1 & & & & & & & & & 0 \end{array}\right]$$

$$\text{o sea} \quad a_{ij} := \begin{cases} X_n & \text{para } i=j \leq r \\ 1 & \text{para } j=i+1 \\ 1 & \text{para } i=s,\ j=1 \end{cases}$$

y $a_{ij}=0$ en los demás lugares . Sea $F'=F.A$ y supongamos que $\deg(\det[F_1,\dots,F_r]) \geq \deg(\det(F_I))$, para todas las sucesiones de números naturales $I=(i_1,\dots,i_r)$, con $1\leq i_1<\dots<i_r \leq s$.

Entonces $\deg(\det[F'_1,\dots,F'_r]) > \deg(\det(F'_I))$, para todo $I=(i_1,\dots i_r)$, I distinto de la sucecesión $(1,\dots,r)$. Además $\deg(F')\leq d= 1+\deg(F)$.

Se elige un producto E de matrices elementales tal que E permuta las columnas de F de manera que para $F'':= F.E$ valga que $\deg(\det[F''_1,\dots,F''_r] \geq \deg(\det(F''_I))$, para todo $I=(i_1,\dots,i_r)$. Además, como k es infinto, puede suponerse luego de un cambio lineal de variables apropiado, que $\det[F''_1,\dots,F''_r]$ es mónico en todas las variables $X_1,\dots,X_n$.

(1.5.2) Vemos entonces que reemplazando a F por F.E.A y realizando un cambio lineal de variables, puede suponerse que $D:= \det[F_1,\dots,F_r]$ es mónico en todas las variables $X_1,\dots,X_n$, y que $\deg(\det[F_1,\dots,F_s])>$ $> \deg(\det(F_I))$, para todo I,distinto de $(1,\dots,r)$.(Observar que este procedimiento puede cambiar d por d+1).

2.Resultados

(2.1) Teorema A: Sea $F\in R^{r\times s}$ unimodular.Entonces existe una matriz cuadrada $M\in R^{s\times s}$ tal que:

(i) M es unimodular

(ii) $F.M = [1_r,0]\in R^{r\times s}$

(iii) $\deg(M)\leq (rd)^{O(n)}$

(iv) M es un producto de $O(n^2s^2(rd)^{2n}$ matrices, que son o bien elementales o bien tienen la forma $T\oplus I_{s-r-1}$ para alguna matriz $T\in SL_{r+1}(R)$.

(2.2)Corolario: Supongamos que $F\in R^{r\times s}$ es unimodular y sea $P\subset R^s$ el núcleo del epimorfismo $F:R^s\to R^r$. Sea $M\in R^{s\times s}$ una matriz cuadrada que satisface las propiedades (i) a (iv) del Teorema A.Entonces las últimas s-r columnas $M_{r+1},\ldots,M_s$ de M forman una base del R-módulo libre P. En particular, P posee una R-base que involucra sólo polinomios de grado $(rd)^{O(n)}$.

(2.3) Teorema B: Sea $F\in R^{r\times s}$ unimodular. Entonces una matriz cuadrada M que satisfaga las propiedades (i) a (iv) del Teorema A puede ser computada mediante un arithmetical network con entradas en k en

tiempo secuencial: $r^{O(n^2)}s^{O(r^2)}d^{(n^2+r^2)}$

tiempo paralelo: $O(n^4r^4\log^2(srd))$

(2.4) Corolario: Sea $F\in R^{r\times s}$ unimodular.Entonces una R-base del núcleo P del epimorfismo $F:R^s\to R^r$ que involucre sólo polinomios de grado a lo sumo $(rd)^{O(n)}$ puede ser computada mediante una red aritmética con las

mismas cotas del Teorema B.

La demostración de los Corolarios (2.2) y (2.3) es inmediata. En particular el Teorema B implica una demostración constructiva de la Conjetura de Serre.

3. Demostracion del Teorema A:

Para demostrar el Teorema A es suficiente con probar la siguiente

(3.1) Proposicion: Sea $F \in R^{r \times s}$ unimodular. Entonces existe una matriz cuadrada $M \in R^{s \times s}$ tal que:

(i) M es unimodular

(ii) $F.M = [f_{ij}(X_1,\dots,X_{n-1},0]$ (o sea F.M es igual a la matriz de rxs obtenida especializando la variable X_n en 0 en la matriz F).

(iii) $\deg(M) = (rd)^{O(n)}$

(iv) M es un producto de $O(n\ s^2(rd)^{2n})$ matrices, que son o bien elementales o bien tienen la forma $T \oplus I_{s-r-1}$ para alguna matriz $T \in SL_{r+1}(R)$.

El Teorema A se obtiene aplicando sucesivamente la Proposición (3.1) a $F=[f_{ij}(X_1,\dots,X_n)]$, $[f_{ij}(X_1,\dots,X_{n-1},0],\dots,[f_{ij}(X_1,\dots,X_i,0,\dots,0)]$, $[f_{ij}(X_1,0,\dots,0)]$.(Observar que especializar variables en 0 no aumenta el grado de los polinomios y que la unimodularidad y lo asumido en (1.5.2) se preservan en el procedimiento.

(3.2) En la Proposición (3.1) la variable X_n juega un rol diferenciado de $X_1,\dots,X_{n-1}$, por lo cual resulta conveniente introducir las siguientes notaciones:

(i) $A:= k[X_1,\dots,X_{n-1}]$

(ii) $t:= X_n$ (luego $A[t] = R$)

(iii) para todo $q,b \in R$, sea $q(b):= q(X_1,\dots,X_{n-1},b)$

(iv) para cualquier matriz $Q=[q_{ij}]$ con coeficientes $q_{ij} \in R$ y para todo $b \in R$ sea $Q(b):= [q_{ij}(b)]$

(v) Notamos por $\mathbb{A}^{n-1}$ al espacio afín de dimensión n-1 sobre $\bar{k}$.

(3.3) A continuación se esbozan los pasos fundamentales de la demostración de la Proposición (3.1):

Paso 1: Se construye una sucesión de polinomios $c_1,\dots,c_N \in A$ de grado acotado por $(rd)^2$, $N \leq (1+rd)^{2n}$, que tienen las siguientes propiedades:

- $1 \in (c_1,\dots,c_N)$, o sea el ideal de A generado por $c_1,\dots,c_n$ es trivial.
- para cada $1 \leq k \leq N$ existe una matriz no singular de sxs con coeficientes en k (en símbolos $\Lambda_k \in GL_s(k)$) tal que

$$c_k = \mathrm{Res}_t\left(\det[\, F_1^{(k)},\dots,F_r^{(k)}],\ \det[\, F_1^{(k)},\dots,F_{r-1}^{(k)},F_{r+1}^{(k)}]\right)$$

donde $F_1^{(k)},\dots,F_s^{(k)}$ son las columnas de $F^{(k)}:= F.\Lambda_k$ y Res_t nota a la resultante con respecto a la variable t.

Paso 2: Como consecuencia del Nullstellensatz efectivo [10] Théorème 1 se obtiene una representación $t = a_1c_1+\dots+a_Nc_N$ con $a_k \in A.t \subset R$ y $\max_{1\leq k\leq N} \deg(a_kc_k) \leq (rd)^{2n} +1$

Paso 3: Para cada $1\leq k \leq N$ se construye una matriz unimodular $M_k \in R^{s\times s}$ (de hecho un producto de (r+1).(s-r-1) matrices elementales y una matriz de la forma $T\oplus I_{s-r-1}$) tal que , para $b_k:= \sum_{1\leq h\leq k} a_hc_h$, $b_{k-1}:= \sum_{1\leq h\leq k-1} a_hc_h$ y $F^{(k)}:= F.\Lambda_k$ vale la siguiente igualdad:

$$F^{(k)}(b_k).M_k = F^{(k)}(b_{k-1})$$

Si llamamos ahora $E_k:= \Lambda_k.M_k.\Lambda_k^{-1}$ obtenemos que $F(b_k).E_k= F(b_{k-1})$.

La matriz E_k es unimodular y es un producto de $(r+1).(r-s-1)+2s^2$ matrices elementales y una matriz de la forma $T\oplus I_{s-r-1}$, con $T\in SL_{r+1}(R)$.
Además se tiene que $\deg E_k \leq \deg M_k \leq rd(1+rd)\max\{\deg(b_k),\deg(b_{k+1})\} =$
$= (rd)^{O(n)}$.

Paso 4: A partir de los pasos 2 y 3 se tienen las siguientes igualdades:

$F=F(t)=F(b_N)$,

$F(b_{N-1})=F(b_N).E_N$,

$F(b_{k-1})=F(b_k).E_k$,

.....

$F(0)=F(b_0)=F(b_1).E_1$.

Así $M:=\prod_{1\leq k\leq N} E_k$ verifica las propiedades (i) a (iv) de la Proposición (3.1).

Los dos lemas siguientes corresponden a [16] Chapter III, lemma 1.4 y Theorem 1.5. La forma particular que tienen se debe a que para la demostración de los teoremas A y B se necesitan argumentos constructivos y que involucren solamente polinomios con grado controlado.

(3.4) Lema: para cada $\xi \in \mathbb{A}^{n-1}$ existe una matriz $\Lambda \in GL_s(k)$ tal que:
sea $F':= F.\Lambda$, $D'_1:= \det[F'_1,\dots,F'_r]$, $D'_2:= \det[F'_1,\dots,F'_{r-1},F'_{r+1}]$ y
$c:= \mathrm{Res}_t(D'_1,D'_2)$ la resultante de D'_1 y D'_2 con respecto a la variable t.
Entonces $c(\xi) \neq 0$.

Demostración:

Sea $\xi=(\xi_1,\dots,\xi_{n-1}) \in \mathbb{A}^{n-1}$ dado. Sea $k[Y]:=k[y_{ij};1\leq i,j\leq s]$ el anillo de polinomios en las s^2 variables nuevas $y_{11},\dots,y_{ss}$ sobre k.
Notaremos con Y a la matriz genérica $[y_{ij}]$ de sxs con columnas $Y_1,\dots,Y_s$

Notaremos con Y' y Y'' a las matrices de $s\times r$ $[Y_1,\dots,Y_r]$ y $[Y_1,\dots,Y_{r-1},Y_{r+1}]$ respectivamente. Sea $F':= F.Y \in (R \otimes_k k[Y])^{r\times s}$

De la fórmula de Binet-Cauchy (Observación (1.5)) vemos que

$$(3.4.1)\quad \begin{cases} D_1':= \det[F_1',\dots,F_r'] = \sum_I \det(F_I)\ \det((^tY')_I) \\ D_2':= \det[F_1',\dots,F_{r-1}',F_{r+1}'] = \sum_I \det(F_I)\ \det((^tY'')_I) \end{cases}$$

donde I recorre todas las sucesiones $(i_1,\dots,i_r)$ tales que $1\le i_1<\dots<i_r\le s$.

Sea $c:= c(X_1,\dots,X_{n-1},Y):= \mathrm{Res}_t(D_1',D_2')$ la resultante de D_1' y D_2' con respecto a la variable t.

Se afirma que $c(\xi,Y) = c(\xi_1,\dots,\xi_{n-1},Y) \neq 0$. Veamos esto: Por (1.5.2) se tiene que $\deg_t(\det[F_1,\dots,F_r]) > \deg_t(\det(F_I))$ para todo $I\neq (1,\dots,r)$ ($\deg_t$ nota el grado en t). Además $\det[F_1,\dots,F_r]$ es mónico en t.

Estos hechos y (3.4.1) implican que tanto en D_1' como en D_2' el monomio de mayor grado en t no tiene a las variables $X_1,\dots,X_{n-1}$ y por lo tanto tomar resultante conmuta con la evaluación en ξ, o sea

$c(\xi,Y) = \mathrm{Res}_t(D_1'(\xi,t,Y'),D_2'(\xi,t,Y''))$.

Supongamos ahora que $c(\xi,Y) = 0$. Entonces existe $p\in \bar{k}[t,Y]$ con $\deg_t(p)\ge 1$ tal que p divide tanto a $D_1'(\xi,t,Y)$ como a $D_2'(\xi,t,Y'')$, (obsérvese que $D_i'(\xi,t)$ no es el polinomio nulo y tiene grado ≥ 1 en t).En particular se tiene que $p\in \bar{k}[t,Y_1,\dots,Y_{r-1}]$. Sea $g\in \bar{k}[t,Y']$ tal que

$$(3.4.2)\qquad p.g = D_1' = \sum_I \det(f_I(\xi,t))\ \det((^tY')_I)$$

Sea $J \subset \bar{k}[t][Y']$ el ideal generado por todos los determinantes $\det((^tY')_I$ J es un ideal primo homogéneo. De (3.4.2) vemos que p y g deben ser homogéneos en Y' y que $\deg_{Y'}(p) + \deg_{Y'}(q) = r$. El polinomio p no pertenece a J ya que es homogéneo en Y' e independiente de Y_r. Como $D_1' \in J$ por (3.4.2) y J es primo se concluye que $q \in J$ y que $\deg_{Y'}(q) \ge r$. Luego $\deg_{Y'}(p) = 0$,esto es $p\in \bar{k}[t]$. Ahora una vez más por (3.4.2) vemos que

esto implica que p divide a cada uno de los $\det(F_I(\xi,t))$, (para ver esto basta evaluar las variables Y_{ij} en unos y ceros apropiadamente.Pero la matriz F es unimodular,o sea que el ideal generado por todos los polinomios $\det(F(\xi,t)$ es trivial, luego $p\in \bar{k}$, lo que contradice que $\deg(p)\geq 1$, probando nuestra afirmación.

Como k es infinito y $c(\xi,Y)\neq 0$ existe una matriz $\Lambda = [\lambda_{ij}] \in k^{s\times s}$ tal que:

- $\det \Lambda \neq 0$
- $\det [\lambda_{ij}]_{1\leq i,j\leq r} \neq 0$
- $c(\xi,\Lambda) \neq 0$

teniendo en cuenta (1.5.2) y (3.4.1) es inmediato verificar que para esta matriz Λ el Lema (3.4) es verdadero.■

(3.5) Lema: Sean $D_1:= \det[F_1,\dots,F_r]$, $D_2:= \det[F_1,\dots,F_{r-1},F_{r+1}]$.
Sea $c:= \mathrm{Res}_t(D_1,D_2)$ la resultante de D_1 y D_2 respecto a t. Entonces para todo b y $b'\in R$ tales que $b \equiv b'$ (mod cR) existe una matriz unimodular M $M\in R^{s\times s}$ que verifica:

(i) $F(b).M = F(b')$

(ii) $\deg M \leq rd(1+2rd)\max\{\deg(b),\deg(b')\}$

(iii) M es un producto de $(r+1)(s-r-1)$ matrices elementales y una matriz de la forma $T\oplus I_{s-r-1}$.

Demostración: Sean g, $h \in R$ tales que

$$c = g.D_1 + h.D_2$$

podemos suponer sin pérdida de generalidad que $\deg(g),\deg(h),\deg(c)\leq(rd)^2$
Sean $b,b' \in R$ dados con $b-b' \in cR$, existe para cada $r+2 \leq j \leq s$ un vector columna $G_j \in R^{r\times 1}$ tal que $F_j(b')-F_j(b) = c.G_{ij}$.
Sea $\beta:=\max\{\deg(b),\deg(b')\}$, notar que $\deg(G_j) \leq d.\beta$. Dado que c no

depende de t tenemos que $c = g(b).D_1(b) + h(b).D_2(b)$, luego

$F_j(b')-F_j(b) = D_1(b).G'_j(b) + D_2(b).G''_j(b)$, donde $G'_j := g(b).G_j$ y

$G''_j := h(b).G_j$. Observar que $\deg(G'_j),\deg(G''_j) \leq (rd)^2\beta + d.\beta$

Sea $B_1 := \operatorname{adj}[F_1(b),\dots,F_r(b)]$ y $B_2 := \operatorname{adj}[F_1(b),\dots,F_{r-1}(b),F_{r+1}(b)]$,

las matrices adjuntas de las matrices de $r\times r$ $[F_1(b),\dots,F_r(b)]$ y

$[F_1(b),\dots,F_{r-1}(b),F_{r+1}(b)]$ respectivamente. Entonces

$D_1(b).G'_j = [F_1(b),\dots,F_r(b)]\,(B_1.G'_j)$ y

$D_2(b).G''_j = [F_1(b),\dots,F_{r-1}(b),F_{r+1}(b)]\,(B_2.G''_j)$.

De estas igualdades se concluye que

$F_j(b') - F_j(b) = g_1.F_1(b) +\dots+ g_{r+1}.F_{r+1}(b)$ para ciertos polinomios

$g_1,\dots,g_{r+1} \in R$, de grado acotado por $r.d.\beta + (r.d)^2\beta$. Esto vale para

todo $r+2 \leq j \leq s$, luego existe una matriz unimodular M' tal que:

- $F(b).M' = [F_1(b),\dots,F_{r+1}(b),F_{r+2}(b'),\dots,F_s(b')]$
- $\deg(M') \leq r.d.\beta + (r.d)^2\beta$
- M' es un producto de $(r+1).(s-r-1)$ matrices elementales.

Ahora cambiemos las primeras $r+1$ columnas:

Sea T la matriz de $(r+1)\times(r+1)$ definida por

$$T := 1/c\ .\ \operatorname{adj}\begin{bmatrix} F_1(b)\dots F_r(b) & F_{r+1}(b) \\ 0\dots\dots -h(b) & g(b) \end{bmatrix}.\begin{bmatrix} F_1(b')\dots F_r(b') & F_{r+1}(b') \\ 0\dots\dots -h(b') & g(b') \end{bmatrix}$$

Como $b \equiv b' \pmod{cR}$ y $c = c(b) = c(b')$ es fácil ver que $T \in R^{(r+1)\times(r+1)}$

y que $\det(T) = 1$. Luego $T \in SL_{r+1}(R)$. Se tiene además que

$[F_1(b),\dots,F_{r+1}(b)].T = [F_1(b'),\dots,F_{r+1}(b')]$ y $\deg(T) \leq 2(rd)^2\beta + rd\beta$

Es fácil ahora verificar que $M := M'.(T\oplus I_{s-r-1})$ verifica (i),(ii) y (iii) ■

(3.6) Fin de la demostracion de la Proposicion (3.1):

Supondremos que $\deg(F) \geq 2$. Así $d\geq 3$.

Paso 1: Para cada $\xi \in \mathbb{A}^{n-1}$ se elige $\Lambda_\xi \in GL_s(k)$ como en el Lema (3.4).

Sean $F^{(\xi)} := F.\Lambda_\xi$, $D_1^{(\xi)} := \det[F_1^{(\xi)},\dots,F_r^{(\xi)}]$,

$D_2^{(\xi)} := \det[F_1^{(\xi)},\dots,F_{r-1}^{(\xi)}, F_{r+1}^{(\xi)}]$, y $c_\xi := \mathrm{Res}_t(D_1^{(\xi)}, D_2^{(\xi)})$. Así,

$c_\xi(\xi) \neq 0$ y $\deg c_\xi \leq (rd)^2$.

Sea $\{c_1,\dots,c_N\} \subseteq \{c_\xi \,;\, \xi \in \mathbb{A}^{n-1}\}$ una base del subespacio k-lineal de $\mathbb{V}$ generado por todos los c_ξ. Es fácil verificar que:

(i) $1 \in (c_1,\dots,c_N)$, es decir el ideal de A generado por $c_1,\dots,c_N$ es trivial. Se tiene además que $\max_{1\leq k\leq N} \deg(c_k) \leq (rd)^2$.

(ii) $N \leq \dim \mathbb{V} \leq (1+rd)^{2n}$

(iii) Para cada $1\leq k\leq N$ existe una matriz $\Lambda_k \in GL_s(k)$ tal que

$c_k = \mathrm{Res}_t\left(\det[\,F_1^{(k)},\dots,F_r^{(k)}],\ \det[\,F_1^{(k)},\dots,F_{r-1}^{(k)},F_{r+1}^{(k)}]\right)$

donde $F^{(k)} = [F_1^{(k)},\dots,F_e^{(k)}] := F.\Lambda_k$.

Paso 2: Del paso 1 (i) y del Nullstellensatz efectivo [10] Théorème 1 concluimos que existe una representación $t = a_1c_1+\dots+a_Nc_N$ con $a_k \in A.t$ y $\max_{1\leq k\leq N} \deg(ac) \leq (rd)^{2n}+1$.

Pasos 3 y 4: Para $1\leq k\leq N$ sean $b_k := \sum_{1\leq h\leq k} a_hc_h$, $b_{k-1} := \sum_{1\leq h\leq k-1} a_hc_h$ y $F^{(k)} := F.\Lambda_k$. Como por construcción $b_k \equiv b_{k-1} \pmod{c_k.R}$ y

$c_k = \mathrm{Res}_t\left(\det[\,F_1^{(k)},\dots,F_r^{(k)}],\ \det[\,F_1^{(k)},\dots,F_{r-1}^{(k)},F_{r+1}^{(k)}]\right)$

se puede aplicar el lema (3.5) a esta situación. Existe entonces una matriz unimodular $M_k \in R^{s\times s}$ que satisface:

- $F^{(k)}(b_k).M_k = F^{(k)}(b_{k-1})$
- $\deg(M_k) \leq rd(1+2rd)\max\{\deg(b_k),\deg(b_{k-1})\} = (rd)^{O(n)}$ (ver paso 2)
- M_k es un producto de $(r+1).(s-r-1)$ matrices elementales y una matriz

de la forma $T \oplus I_{s-r-1}$, con $T \in SL_{r+1}(R)$.

Para $E_k := \Lambda_k . M_k . \Lambda_k^{-1}$ se obtiene que $F(b_k).E_k = F(b_{k-1})$. Finalmente $M := \prod_{1 \le k \le N} E_k$ verifica las propiedades (i) a (iv) de la Proposición (3.1).

4.Demostracion del Teorema B

(i) Usando álgebra lineal sobre k (ver [2], [9], y[18]) y técnicas de interpolación como las descriptas en [11] se deduce inmediatamente el Teorema B en el caso deg f=1 (o sea d=2), y en el caso s = 1. Supondremos entonces, de aquí en más que $d \ge 3$ y que $s \ge 2$. También supondremos $r<s$ (el caso r=s sigue simplemente invirtiendo la matriz F).

(ii) El Teorema A se deduce aplicando iteradamente la Proposición (3.1) cuya demostración es casi algorítmica. Sólo el paso 1 de esta demostración no es algorítmico (ver (3.3) y (3.6)). Este paso se basa en el Lema (3.4). En esta sección se describirá un algoritmo que tiene como datos de salida una familia finita $(\Lambda_k;\ 1 \le k \le N)$ de $N = O((s.r^2 d^2)^r) =$ $= (sd)^{O(r^2)}$ matrices $\Lambda_k \in GL_s(k)$, tales que para cada $\xi \in \mathbb{A}^{n-1}$ existe k, $1 \le k \le N$ con la siguiente propiedad:

$F^{(k)} = [F_1^{(k)},\dots,F_s^{(k)}] := F.\Lambda_k$ y

$$c_k = \mathrm{Res}_t\left(\det[F_1^{(k)},\dots,F_r^{(k)}],\ \det[F_1^{(k)},\dots,F_{r-1}^{(k)},F_{r+1}^{(k)}]\right)$$

entonces $c_k(\xi) \ne 0$. (comparar con Lema (3.4)). Así, $1 \in (c_1,\dots,c_N)$.

Repitiendo ahora los argumentos del final de la demostación de la Proposición (3.1), se obtiene **constructivamente** una matriz $M \in R^{s \times s}$ que verifica las propiedades (i) a (iv) de la Proposición (3.1). Aplicando esta versión algorítmica de la Proposición (3.1) iterativamente (n veces),se eliminan sucesivamente las variables $X_1,\dots,X_n$, y se obtiene el Teorema B

(4.2) Notaciones: Usaremos la notación introducida en (1.1),(1.4) y (3.2)

Establecemos también la siguiente notación adicional:

sean l, m, p número naturales y sea $Q \in R^{l \times m}$.

(i) Supongamos $l \leq m$. Para cada sucesión $I=(i_1,\dots,i_p)$ tal que $1 \leq i_1 < \dots < i_p \leq l$, Q_I notará a la matriz $Q_I := [Q_{i_1},\dots,Q_{i_r}]$

(ii) Supongamos $l > m$. Para cada sucesión $I=(i_1,\dots,i_p)$ tal que $1 \leq i_1 < \dots < i_p \leq l$, Q_I notará a la matriz de $p \times m$ cuyas filas son las filas $i_1,\dots,i_p$ de Q.

(iii) Diremos que Q es unimodular si Q o ${}^tQ$ es unimodular en el sentido de (1.3).

(iv) En lo que sigue I_1 notará la sucesión $I_1 := (1,\dots,r)$ y I_2 la sucesión $I_2 := (1,\dots,r-1,r+1)$.

(4.3) Siguiendo (1.5.2) supondremos de aquí en más que $\det(F_{I_1})$ es mónico en todas las variables y en particular en t, y que

$\deg_t(\det(F_{I_1})) = \deg(\det(F_{I_1})) > \deg(\det(F_I)) \geq \deg_t(\det(F_I))$ para toda sucesión I, $I \neq I_1$.

(4.4) Para cada $1 \leq i \leq r$ elegimos un conjunto finito $A_i \subset k-\{0\}$ de cardinal

$$\#(A_i) \begin{cases} (r+1).d+1 & \text{para } i < r \\ 2r.(s-r).d+1 & \text{para } i = r. \end{cases}$$

Para cada $1 \leq i \leq r-1$ elegimos otro conjunto finito $B_i \subset k-\{0\}$ tal que $\#(B_i) = rsd+1$

Para cada $(\alpha;\beta) := (\alpha_1,\dots,\alpha_r;\beta_1,\dots,\beta_{r-1}) \in \prod_{1 \leq i \leq r} A_i \times \prod_{1 \leq i \leq r-1} B_i$

consideramos la siguiente matriz de $s \times s$:

$$
\Lambda_{(\alpha;\beta)} := \begin{array}{cccccccc}
1 & 0 \ldots\ldots 0 & & & & 0 & 0 \ldots\ldots 0 \\
\alpha_1 & 1 \ldots\ldots 0 & & & & & \ldots\ldots \\
\alpha_1\beta_1 & \alpha_2 \ldots\ldots 0 & & & & \cdot & \ldots\ldots \\
\alpha_1\beta_1^2 & \alpha_2\beta_2 \ldots\ldots 0 & & & & 0 & \ldots\ldots 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots 1 & & & & 0 & 0 \ldots\ldots 0 \\
 & \ldots\ldots \alpha_{r-1} & & & & 1 & 0 \ldots\ldots 0 \\
 & \ldots\ldots \alpha_{r-1}\beta_{r-1} & & & & 0 & 1 \ldots\ldots 0 \\
 & \ldots\ldots & & & & & \alpha_r \ldots\ldots 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\alpha_1\beta_1^{s-2} & \alpha_2\beta_2^{s-3} \ldots & \alpha_{r-1}\beta_{r-1}^{s-r} & & & 0 & \alpha_r^{s-r-1} \ldots 1 \\
\text{numero de col.} & 1 & 2 & & r-1 & r & r+1 \qquad s
\end{array}
\tag{4.4.1}
$$

La matriz $\Lambda_{(\alpha;\beta)} = (\lambda_{ij}) \in k^{s\times s}$ está definida por:

$$
\lambda_{ij} := \begin{cases}
1 & \text{si } i = j \\
\alpha_j\beta_j^{i-j-1} & \text{si } j+1 \le i \ \text{ y } \ j \le r \\
\alpha_r^{i-j} & \text{si } r+1 \le j \le i \\
0 & \text{en los demas lugares}
\end{cases}
$$

Hemos definido así $N := \#(\prod_{1\le i\le r} A_i \times \prod_{1\le i\le r-1} B_i) = O((r^2sd^2)^r)$ matrices $\Lambda_{(\alpha;\beta)}$.

(4.5) Notacion: Para hacer mas simple la exposición elegimos un orden fijo en el conjunto de todos los pares $(\alpha;\beta)$ recién introducidos. Así, si $(\alpha;\beta)$ es el k-ésimo par en este orden escribiremos Λ_k en lugar de $\Lambda_{(\alpha;\beta)}$ donde $1 \le k \le N = O((r^2sd^2)^r)$. Escribiremos también $F^{(k)} := F.\Lambda_k$.

(4.6) Lema: sea i, $1 \le i \le r-1$. Entonces para cada $\xi \in \mathbb{A}^{n-1}$ existe $k, 1 \le k \le N$ tal que $F^{(k)}_{(1,\ldots,i)}(\xi,t) \in (\bar{k}[t])^{r\times i}$ es unimodular, (es decir sus menores de tamaño $i\times i$ no se anulan simultánemente)

Demostracion: Se procederá por inducción en i.

Caso i=1

Para $\alpha \in A_1$ y $\beta \in B_1$ consideramos el vector columna $Q_{\alpha\beta}$ definido por: $Q_{\alpha\beta} = F_1 + \alpha . \sum_{0\le j\le s-2} \beta^j F_{j+2}$, o sea si $(\alpha_1\alpha_2\ldots\alpha_r;\beta_1\beta_2\ldots\beta_{r-1})$ es el k-ésimo par en nuestro orden se tiene que $Q_{\alpha\beta}(\xi,t) = F^{(k)}_{(1)}$. Luego es suficiente con probar la siguiente

Afirmacion: Para cada $\xi \in \mathbb{A}^{n-1}$ existe $\alpha \in A_1$ y $\beta \in B_1$ tales que $Q_{\alpha\beta}$ es unimodular.

Demostración: Supongamos que para algún $\xi \in \mathbb{A}^{n-1}$ dado, ningún vector columna $Q_{\alpha\beta}$ con $\alpha \in A_1$ y $\beta \in B_1$ es unimodular.

Entonces para cada $(\alpha;\beta) \in A_1 \times B_1$ existe $a_{\alpha\beta} \in \bar{k}$ tal que $Q_{\alpha\beta}(\xi,a_{\alpha\beta}) = 0$.

Para $\beta \in B_1$ sea $Q_\beta := [\, F_1, \sum_{0\le j\le s-2} \beta^j F_{j+2} \,]$. Notar que $Q_\beta = [F_1, \alpha^{-1}(Q_{\alpha\beta} - F_1)]$ para cualquier $\alpha \in A_1$. Fijemos por el momento un elemento $\beta \in B_1$. Considera mos la matriz $[Q_\beta, F_2, \ldots, F_{r-1}] \in R^{r\times r}$. Se tiene que $\det[Q_\beta, F_2, \ldots, F_{r-1}] =$

$$= \beta^{r-2}\det[F_1, F_r, F_2, \ldots, F_{r-1}] + \sum_{r-1\le j\le s-2} \beta^j \det[F_1, F_{j+2}, F_2, \ldots, F_{r-1}]$$

Luego (4.3) implica que $\det[Q_\beta, F_2, \ldots, F_{r-1}]$ es mónico en t. Así, $\det[Q_\beta, F_2, \ldots, F_{r-2}][\xi,t] \neq 0$ y la expansión de Laplace a lo largo de las dos primeras columnas de $[Q_\beta, F_2, \ldots, F_{r-1}]$ muestra que existen dos filas digamos la i_1 y la i_2 tales que $\det((Q_\beta)_{(i_1,i_2)})(\xi,t) \neq 0$. Observemos ahora lo siguiente: Nuestra suposición acerca de ξ dice que para cualquier $\alpha \in A_1$ vale que $Q_{\alpha\beta}(\xi,a_{\alpha\beta}) = 0$. Luego, $\text{rango}(Q_\beta(\xi,a_{\alpha\beta})) =$ $\text{rango}\, [F_1(\xi,a_{\alpha\beta}), \alpha^{-1}(Q_{\alpha\beta} - F_1)(\xi,a_{\alpha\beta})] \le 1$. Luego debe ser

$\det((Q_\beta)_{(i_1,i_2)}(\xi,a_{\alpha\beta})) = 0$ para todo $\alpha\in A_1$. Como $\# A_1 \geq 2d+1$ y $\deg(\det((Q_\beta)_{(i_1,i_2)}(\xi,t))) \leq 2d$ concluimos por el principio de los casilleros (pigeon hole principle) que existen dos elementos distintos $\alpha_1, \alpha_2\in A_1$ tales que $a_{\alpha_1\beta} = a_{\alpha_2\beta}$. Definamos $a_\beta := a_{\alpha_1\beta} = a_{\alpha_2\beta}$. Luego tenemos las ecuaciones:

$$0 = Q_{\alpha_1\beta}(\xi,a_\beta) = F_1(\xi,a_\beta) + \alpha_1 \sum_{0\leq j\leq s-2} \beta^j F_{j+2}(\xi,a_\beta)$$

$$0 = Q_{\alpha_2\beta}(\xi,a_\beta) = F_1(\xi,a_\beta) + \alpha_2 \sum_{0\leq j\leq s-2} \beta^j F_{j+2}(\xi,a_\beta)$$

con $\alpha_1 \neq \alpha_2$

esto implica que $F_1(\xi,a_\beta) = 0$ y $\sum_{0\leq j\leq s-2} \beta^j F_{j+2}(\xi,a_\beta) = 0$.

Ahora dejemos que β varíe en B_1: para cada $\beta\in B_1$ elegimos un elemento $a_\beta\in \bar{k}$ tal que $F_1(\xi,a_\beta) = 0$ y $\sum_{0\leq j\leq s-2} \beta^j F_{j+2}(\xi,a_\beta) = 0$.

Sea $\sim$ la relación de equivalencia definida en B_1 por:

$$\beta \sim \beta' :\Longleftrightarrow a_\beta = a_{\beta'} \qquad \text{para } \beta, \beta'\in B_1.$$

Notar que (4.3) implica $F_1(\xi,t) \neq 0$. Por otro lado se tien que $\deg(F_1(\xi,t)) \leq d$. Luego $B_1/\sim$ el conjunto de clases de equivalencia módulo $\sim$ satisface $\#(B_1/\sim) \leq d$. Teniendo en cuenta que $\#B_1 \geq (s-2)d+1$ vemos ,nuevamente por el principio de los casilleros que existe un elemento $\bar{\beta}\in B_1$ tal que $\#\{\beta\in B_1 : \beta \sim \bar{\beta}\} \geq s-1$.

Elegimos ahora elementos $\beta_0,\dots,\beta_{s-2}\in B_1$, distintos dos a dos y tales que $\bar{\beta} \sim \beta_i \sim \beta_j$ para $0 \leq i,j \leq s-2$.

Sea $a := a_{\beta_0} = \dots = a_{\beta_{s-2}}$. Tenemos que

$$F_1(\xi,a) = 0$$

$$\sum_{0\leq j\leq s-2} (\beta_i)^j F_{j+2}(\xi,a) = 0 \qquad \text{para } 0 \leq i \leq s-2.$$

Dado que la matriz de Vandermonde $[(\beta_i)^j]_{0 \leq i,j \leq s-2}$ es inversible concluimos que $F_{j+2}(\xi,a) = 0$ para todo $0 \leq j \leq s-2$. Esto unido a que

$F_1(\xi,a) = 0$ implica $F(\xi,a) = 0$, lo que contradice que F sea unimodular. Esto termina la demostración de la afirmación y establece el caso $i = 1$.

Caso $1 < i < r$:

Sea $\xi \in \mathbb{A}^{n-1}$. Sabemos por hipótesis inductiva que existe k, $1 \le k \le N$ tal que $F^{(k)}_{(1,\ldots,i-1)}(\xi,t)$ es unimodular. Para cada par $(\alpha,\beta) \in A_i \times B_i$ sea $Q_{\alpha\beta}$ la matriz de $r\times i$:

$Q_{\alpha\beta} := [F^{(k)}_{(1,\ldots,i-1)}, F_i + \alpha \sum_{0\le j\le s-i-1} \beta^j F_{j+i+1}$. O, sea si el k-ésimo par en el orden de $\prod_{1\le i\le r} A_i \times \prod_{1\le i\le r-1} B_i$ tiene la forma $(\alpha_1,\ldots,\alpha_i,\ldots,\alpha_r;\beta_1,\ldots,\beta_i,\ldots,\beta_{r-1})$ tenemos que $Q_{\alpha_i\beta_i} = F^{(k)}_{(1,\ldots,i)}$.

Supongamos ahora que el Lema (4.6) es falso para i. Entonces para cada $(\alpha,\beta) \in A_i \times B_i$, existe un elemento $a_{\alpha\beta} \in \bar{k}$ tal que todos los subdeterminantes de $i\times i$ de la matriz $Q_{\alpha\beta}(\xi,a_{\alpha\beta})$ son cero, lo cual implica que $\text{rango}(Q_{\alpha\beta}(\xi,a_{\alpha\beta})) \le i-1$. Fijemos por el momento un elemento $\beta \in B_i$.

Sea $\quad Q_\beta := [F^{(k)}_{(1,\ldots,i-1)}, F_i, \sum_{0\le j\le s-i-1} \beta^j F_{j+i+1}]$

Dado que $\text{rango}\left[[F^{(k)}_{(1,\ldots,i-1)}(\xi,a_{\alpha\beta}),(F_i + \alpha \sum_{0\le j\le s-i-1} \beta^j F_{j+i+1})(\xi,a_{\alpha\beta})]\right] =$

$= \text{rango}\,(Q_{\alpha\beta}(\xi,a_{\alpha\beta})) \le i-1$, se tiene que $\text{rango}(Q_\beta(\xi,a_{\alpha\beta})) \le i$ para todo $\alpha \in A_i$. Luego para cada $\alpha \in A_i$, $a_{\alpha\beta} \in \bar{k}$ es un cero común de todos los subdeterminantes de $(i+1)\times(i+1)$ de la matriz $Q_\beta(\xi,t)$, considerados como elementos de anillo de polinomios $\bar{k}[t]$. Probaremos ahora que por lo menos un subdeterminante de $(i+1)\times(i+1)$ de $Q_\beta(\xi,t)$ es distinto de cero.

Consideremos la matriz $[Q_\beta, F_{i+1},\ldots,F_{r-1}] \in R^{r\times r}$. Dado que Λ_k es triangular inferior(4.4.1), la multilinealidad del determinante y la fórmula de Binet-Cauchy implican que

$\det[Q_\beta, F_{i+1},\ldots,F_{r-1}] = \beta^{s-i-1}\det[F_1,\ldots,F_i,F_r,F_{i+1},\ldots,F_{r-1}] +$

$+ \sum_{I \neq I_1} c_I \det(F_I)$ para ciertos $c_I \in k$.

En virtud de (4.3) esto implica que $\det[Q_\beta, F_{i+1}, \ldots, F_{r-1}]$ es mónico en t y en particular $\det([Q_\beta, F_{i+1}, \ldots, F_{r-1}](\xi,t)) \neq 0$. La expansión de Laplace de este determinante a lo largo de sus primeras (i+1) columnas muestra que existe una sucesión I de i+1 filas de Q_β tal que $\det((Q_\beta)_I(\xi,t)) \neq 0$. Notar que $\deg(\det((Q_\beta)_I(\xi,t))) \leq (i+1)d$ y que $\# A_i \geq (i+1)d+1$. Luego existe por el principio de pigeon hole dos elementos distintos $\alpha_1, \alpha_2 \in$ $\in A_i$ tales que $a_{\alpha_1\beta} = a_{\alpha_2\beta}$. Sea $a_\beta := a_{\alpha_1\beta} = a_{\alpha_2\beta}$.

Como por hipótesis inductiva

$F^{(k)}_{(1,\ldots,i-1)}(\xi,t)$ es unimodular concluimos que $\text{rango}(F^{(k)}_{(1,\ldots,i-1)}(\xi,a_\beta)=i-1$

Por otro lado $F^{(k)}_{(1,\ldots,i-1)}(\xi,a_\beta)$ es una submatriz de $Q_{\alpha_1\beta}(\xi,a_\beta)$ y de

$Q_{\alpha_2\beta}(\xi,a_\beta)$ que tienen a lo sumo rango i-1. Luego

$$i-1 = \text{rango}(F^{(k)}_{(1,\ldots,i-1)}(\xi,a_\beta)) = \text{rango}(Q_{\alpha_1\beta}(\xi,a_\beta)) = \text{rango}(Q_{\alpha_2\beta}(\xi,a_\beta))$$

Esto significa que los vectores columna:

$$F_i(\xi,a_\beta) + \alpha_1 \sum_{0\leq j\leq s-i-1} \beta^j F_{j+i+1}(\xi,a_\beta) \quad \text{y}$$

$$F_i(\xi,a_\beta) + \alpha_2 \sum_{0\leq j\leq s-i-1} \beta^j F_{j+i+1}(\xi,a_\beta)$$

son linealmente dependientes de los vectores columnas de la matriz $F^{(k)}_{(1,\ldots,i-1)}(\xi,a_\beta)$. Dado que $\alpha_1 \neq \alpha_2$ esto implica que

$$\text{rgo}([F^{(k)}_{(1,\ldots,i-1)}, F_i](\xi,a_\beta)) = \text{rgo}\left(\left[F^{(k)}_{(1,\ldots,i-1)}, \sum_{0\leq j\leq s-i-1} \beta^j F_{j+i+1}\right](\xi,a_\beta)\right)=i-1$$

Mediante un argumento similar al usado recién, concluimos que por lo menos un subdeterminante de ixi de la matriz $[F^{(k)}_{(1,\ldots,i-1)}, F_i](\xi,t)$ es distinto de cero. Como $\text{rango}([F^{(k)}_{(1,\ldots,i-1)}, F_i](\xi,a_\beta)) = i-1$, a_β es un cero de este subdeterminante no nulo, el cual tiene a lo sumo grado i.d.

Variando ahora β en B_i, vemos que $\#\{a_\beta;\ \beta\in B_i\} \le i.d$. Dado que $\#B_i \ge i(s-i-1)d+1$ se concluye por el principio de pigeon hole que existen elementos $\beta_0,\dots,\beta_{s-i-1} \in B_i$,distintos dos a dos tales que

$a:= a_{\beta_0} = \dots = a_{\beta_{s-i-1}}$. Luego, los vectores columna:

$F_i(\xi,a)$ y

$\sum_{0\le j\le s-i-1} (\beta_l)^j F_{j+i+1}(\xi,a)$ para $0 \le l \le s-i-1$, pertenecen al k espacio vectorial generado por $F_1^{(k)}(\xi,a),\dots,F_{i-1}^{(k)}(\xi,a)$, columnas de $F^{(k)}_{(1,\dots,i-1)}(\xi,a)$.

Dado que la matriz de Vandermonde $[(\beta_l)^j]_{0\le j,l\le s-i-1}$ es inversible, concluimos que $F_i(\xi,a),F_{i+1}(\xi,a),\dots,F_s(\xi,a)$ pertenecen al k-espacio vectorial generado por $F_1^{(k)}(\xi,a),\dots,F_{i-1}^{(k)}(\xi,a)$. Luego

$\text{rango}([F^{(k)}_{(1,\dots,i-1)},F_i,\dots,F_s](\xi,a)) =$

$\text{rango}[F_1^{(k)}(\xi,a),\dots,F_{i-1}^{(k)}(\xi,a),F_i(\xi,a),\dots,F_s(\xi,a)] = i-1$

Por otro lado, sea $\Lambda\in k^{s\times s}$ la matriz formada por las primeras i-1 columnas de Λ_k y agregando las últimas s-i+1 columnas de la matriz identidad de sxs. De (4.4.1) vemos que Λ es inversible, luego

$[F^{(k)}_{(1,\dots,i-1)},F_i,\dots,F_s] = F.\Lambda$ es unimodular.

Esto implica que $\text{rango}([F^{(k)}_{(1,\dots,i-1)},F_i,\dots,F_s](\xi,a)) = r$, contradición.

Esto termina la demostración del Lema (4.6) ■

(4.7) Proposicion:

Para cada $\xi\in \mathbb{A}^{n-1}$ existe $(\alpha;\beta)\in \prod_{1\le i\le r} A_i \times \prod_{1\le i\le r-1} B_i$ con la siguiente propiedad:

sean $F':= F.\Lambda_{(\alpha;\beta)}$, $D_1':= \det[F_1',\dots,F_r']$, $D_2':= \det[F_1',\dots,F_{r-1}',F_{r+1}']$

y $c := \mathrm{Res}_t(D'_1, D'_2)$. Entonces $c(\xi) \neq 0$.

Demostracion:

La fórmula de Binet-Cauchy (ver observación(1.5)), y (4.3) implican que $\det(F^{(k)}_{I_1})$ es mónico en t para todo $k, 1 \leq k \leq N$. Supongamos que existe $\xi \in \mathbb{A}^{n-1}$ tal que para todo k, $1 \leq k \leq N$

$$\mathrm{Res}_t\left[\det(F^{(k)}_{I_1}(\xi,t)),\ \det(F^{(k)}_{I_2}(\xi,t))\right] = 0$$

De (4.4.1) vemos que $F^{(k)}_{I_1}$ y $F^{(k)}_{I_2}$ tienen la forma:

$F^{(k)}_{I_1} = [F^{(k)}_{(1,\ldots,r-1)}, F_r]$

$F^{(k)}_{I_2} = [F^{(k)}_{(1,\ldots,r-1)}, \sum_{0 \leq j \leq s-r-1} \alpha^j_r F_{j+r+1}]$, si el k-ésimo par en el orden es $(\alpha_1,\ldots,\alpha_r;\beta_1,\ldots,\beta_r)$.

Por el Lema (4.6), existe un ko, $1 \leq ko \leq N$ tal que $F^{(ko)}_{(1,\ldots,r-1)}(\xi,t)$ es unimodular. La suposición (4.7.1) implica ahora que para cada $\alpha \in A^r$ existe un elemento $a_\alpha \in \bar{k}$ tal que $F_r(\xi,a_\alpha)$ y $\sum_{0 \leq j \leq s-r-1} \alpha^j F_{j+r+1}(\xi,a_\alpha)$ pertenecen al k-espacio vectorial generado por $F^{(ko)}_1(\xi,a_\alpha),\ldots,F^{(ko)}_{r-1}(\xi,a_\alpha)$ columnas de $F^{(ko)}_{(1,\ldots,r-1)}(\xi,a_\alpha)$. En particular a_α es una raíz de $\det((F^{(ko)}_{I_1})(\xi,t) = \det\left[[F^{(ko)}_{(1,\ldots,r-1)}, F_r](\xi,t)\right]$ para cada $\alpha \in A_r$.

Como $\det((F^{(ko)}_{I_1})(\xi,t)$ es una especialización de $\det(F^{(ko)}_{I_1})$ que es mónico en t y de grado a lo sumo r.d, concluimos que

$$\#\{ a_\alpha;\ \alpha \in A_r \} \leq rd$$

Dado que $\# A_r \geq r(s-r)d+1$ el principio de pigeon hole implica que existen elementos $\alpha_0,\ldots,\alpha_{s-r-1} \in A_r$, distintos dos a dos tales que $a := a_{\alpha_0} = \ldots = a_{\alpha_{s-r-1}}$.

Luego los vectores columna :

$F_r(\xi,a)$ y

$$\sum_{0\le j\le s-r-1} \alpha_l^j \quad F_{j+r+1}(\xi,a) \qquad\qquad 0\le l\le s-r-1$$

pertenecen al k-espacio vectorial generado por las columnas de $F^{(k0)}_{(1,..,r-1)}(\xi,a)$: $F_1^{(k0)}(\xi,a),\dots,F_{r-1}^{(k0)}(\xi,a)$. Dado que la matriz de Vandermonde $[\alpha_l^j]_{0\le j,l\le s-r-1}$ es inversible, esto implica que rango $\left([F^{(k0)}_{(1,..,r-1)},F_r,\dots,F_s](\xi,a)\right) = r-1$.

Esto contradice la unimodularidad de $[F^{(k0)}_{(1,..,r-1)},F_r,\dots,F_s]$, que se deduce a partir de la unimodularidad de F y (4.4.1). ■

(4.8) Si ahora reemplazamos el Lema (3.4) por la Proposición (4.7) en la demostración de la Proposición(3.1) obtenemos un algoritmo que construye para la matriz unimodular dada $F\in R^{r\times s}$ una matriz $M^{s\times s}$ que satisface las propiedades (i) a (iv) de la Proposición (3.1).

Daremos a continuación un análisis de las cotas para la complejidad y los grados de los pasos principales de este algoritmo. Toda el álgebra lineal involucrada en este algoritmo es paralelisable(ver [2],[9],[18] y [13]).

La verificación de estas cotas es directa.

(4.8.1) Preparación: Multiplicación por una matriz de s×s y cambio lineal de variables: tiempo secuencial: $s^2(rd)^{O(n)}$

tiempo paralelo: $O(n^4 \log^2 srd)$

(4.8.2) Computación de $c_1,\dots,c_N$

tiempo secuencial: $s^{O(r^2)}\ r^{O(n^2)}\ d^{O(n^2+r^2)}$

tiempo paralelo: $O(n^4\log^2 srd)$

(4.8.3) Computación de $a_1,\ldots,a_N$

tiempo secuencial: $s^{O(r^2)}\ r^{O(n^2)}\ d^{O(n^2+r^2)}$

tiempo paralelo: $O(n^4r^4\log^2 srd)$

(4.8.4) Computación de $E_1,\ldots,E_N$

tiempo secuencial: $s^{O(r^2)}\ r^{O(n^2)}\ d^{O(n^2+r^2)}$

tiempo paralelo: $O(n^4\log^2 srd)$

De estas cotas obtenemos finalmente la complejidad del algoritmo correspondiente a la Proposición (3.1)

(4.8.5) Computación de M

tiempo secuencial: $s^{O(r^2)}\ r^{O(n^2)}\ d^{O(n^2+r^2)}$

tiempo paralelo: $O(n^4r^4\log^2 srd)$

Aplicando el algoritmo correspondiente a la Proposición (3.1) n veces se obtienen las cotas para la complejidad del Teorema B.

Referencias:

1.B.Bayer, M.Stillman: On the complexity of computing syzygies. J. Symbolic Computaction 6 (1988) 135-147

2.S.J.Berkowitz: On comuting the determinant in small parallel time using a small number of processors. Information Processing Letters 18 (1984) 147-150

3.W.D.Brownawell: Bounds for the degree in the Nullstellensatz. Ann.Math. Second Series Vol.126 N° 3(1987) 577-591

4.W.D.Brownawell: A prime product version of the Nullstellensatz. Manuscript Pennsylvania State University (1989)

5.B.Buchberger: Gröbner Bases: an algorithmic method in polynomial ideal theory.Chapter 6 in:Multidimensional Systems Theory(ed.N.K.Bose) D.Riedel Publishing Company(1985) 184-232

6.L.Caniglia,A.Galligo,J.Heintz: Some new effectivity bounds in computational geometry.Proc. 6th International Conf.Applied Algebra, Algebraic Algorithms and Error Correcting Codes(AAECC-6)(ed T.Mora), Springer LN Computer Sci.357(1989) 131-151.

7.L.Caniglia,J.Guccione,J.J.Guccione: Local Membership problems for polynomial ideals. Aparecerá en Proc.Metodi Effettivi in Geometria Algebrica (MECiA 90) 1990

8.F.Chaqui: Algorithme de calcul d'une base pour les modules projectifs sur k[x,y] et Z[x]. Thèse 3éme Cycle, Université Paris-Sud, Centre d' Orsay(1983)

9.A.L.Chistov: Fast parallel calculation of the rank of matrices over a field of arbritrary characteristic. Proc.Intern.Conf.FCT 1985, Springer LN Comput.Sci.199(1985) 63-69

10.N Fitchas, A.Galligo: Nullstellensatz effectif et Conjecture de Serre

(Théorème de Quillen-Suslin) pour le Calcul Formel. Aparecerá en Mathematische Nachrichten; versión preliminar en: Séminaire Structures Algebriques Ordoneés,1987-88,Université Paris VII(1989)

11.N.Fitchas, A.Galligo, J.Morgenstern: Algorithmes rapides en sequentiel et parallèle pour l'elimination de quantificateurs en géometrie élémentaire, aparecerá en Séminaire Structures Algebriques Ordoneés, Publ.Université Paris VII; versión preliminar en Séminaire Structures Algébriques Ordoneés 1986-87,UER de Math., Univer.Paris VII(1987)

12.F.R.Gantmaχer:Teoria matrits.Versión en inglés: The theory of matrices Volume I, Chelsea Publishing Company, New York 1977

13.J.von zur Gathen: Parallel arithmetic computations: a survey.Proc.13th Symp.MFCS 1986, Springer LN Comput.Sci.233(1986) 93-112

14.G.Herrmann: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math.Ann.95(1926) 736-788

15.E.Kunz: Einführung in die Kommutative Algebra und algebraische Geometrie. F. Vieweg und Sohn, Braunschweig-Wiesbaden 1980.

16.T.Y.Lam: Serre's Conjecture. Springer LN Math.635(1978)

17.E.Mayr, A.Meyer: The complexity of the word problem for commutative semigroups and polynomial ideals. Advances in Math. 46(1982) 305-329

18.K.Mulmuley: A fast parallel algorithm to compute the rank of a matrix over an arbitrary field.Proc. 18th Ann ACM Symp. Theory of Computing (1986)338-339

19.P.Philippon: Théorème des zéros effectifs d'aprés J.Kollár, Publ.Univ.VI N.88,Probl.Dioph. 1988-89(1988)

20.A.Seidenberg :Constructions in Algebra.Trans.Amer.Math.Soc.197 (1974) 273-313

FAC.J.P.Serre: Faisceaux algébriques cohérents, Ann.Math.61(1955)191-278

21.B.Sturmfels: An algorithmic proof of the Quillen-Suslin Theorem, Manuscript IMA (1988)

22.B.Teissier: Résultats recents d'algèbre commutative effective , Séminaire Bourbaki, 42ème anneé, 1989-90,N° 718 (1989)

Apendice 1

Un test simplemente exponencial para decidir si un submodulo finitamtente generado de $k[X_1,\dots,X_n]^t$ es proyectivo(y por lo tanto libre)

Sea $R:= k[X_1,\dots,X_n]$ y sea M un R módulo de presentación finita:

$$0 \longrightarrow K \longrightarrow R^s \longrightarrow M \longrightarrow 0$$

Sean $\{m_1,\dots,m_s\}$ y $\{a_1,\dots,a_r\}$ sistemas de generadores para M y K respectivamente (K es el módulo de relaciones que satisfacen los generadores $m_1,\dots,m_s$).

Se define para cada i, $i = 0,\dots,s-1$ el ideal de R, $F_i(M)$, generado por todos los subdeterminantes de tamaño s-i, de la matriz A que tiene como filas a los vectores $a_1,\dots,a_k$. Si $i \geq s$ se define $F_i(M) = R$. ($F_i(M)$ se llaman los **ideales de Fitting** o los **invariantes de Fitting** del módulo M. Valen las siguientes propiedades:

a) $F_i(M)$ no depende de la presentación elegida para M (esto es no depende del sistema de generadores de M, $m_1,\dots,m_s$ elegido ni del sistema de generadores $v_1,\dots,v_r$ de K.)

b) $F_0(M) \subseteq F_1(M) \subseteq \dots \subseteq F_s = R$

c) son equivalentes:

i) M es proyectivo (y por lo tanto libre) de rango k.

ii) $F_0(M) = \dots = F_{k-1} = 0$, $F_k(M) = R$.

(ver Kunz, capitulo IV, § 1 Ej.9,§ 3 Ej.2)

Supongamos ahora tener un módulo dado por generadores y relaciones. Para decidir si es o no libre, basta chequear la condición ii). Sin embargo el

número de subdeterminantes que habría que calcular es exponencial en el rango de M. Para decidir si M es libre o no, eficientemente hay que hallar una forma de verificar ii) sin calcular los correspondientes subdeterminantes.

Para esto se usará una idea de K.Mulmuley [18] para calcular el rango de matrices a coeficientes en un cuerpo, en tiempo paralelo polilogarítmico en el tamaño de la matriz.

Sea $(\alpha_1,\ldots,\alpha_n) \in \bar{k}^n$. Especializando cada coeficiente $a_{ij}(X_1,\ldots,X_n)$ de la matriz A, en $(\alpha_1,\ldots,\alpha_n)$ obtenemos una matriz numérica. De esta forma la condición ii) es equivalente a la siguiente:

ii') el rango de la matriz A de relaciones es s-k y este rango se conserva para cualquier especialización en $\bar{k}$

En [18] Mulmuley prueba lo siguiente:

Sea B una matriz de rxs a coeficientes en un cuerpo arbitrario, a la que se le quiere calcular el rango. Consideremos en lugar de B la matriz

$$B' = \begin{bmatrix} 0 & B \\ {}^tB & 0 \end{bmatrix}$$ de (r+s)x(r+s) que tiene rango el doble que el de B.

Sean Y y λ nuevas indeterminadas y sea C la matriz

$$\begin{bmatrix} 1 & & & & \\ & Y & & & \\ & & Y^2 & & \\ & & & \ddots & \\ & & & & Y^{r+s} \end{bmatrix}$$

Consideremos $X(\lambda) = \det(\lambda.I_{r+s} - C.B')$ el polinomio característico de C.B'. Entonces el rango de B'(= 2.rango de B) es r+s-m, donde m es la máxima potencia de λ que divide a $X(\lambda)$.

Sea ahora $A = [a_{ij}]$ la matriz de relaciones del módulo M, con $a_{ij} \in$

$\in k[X_1,\ldots,X_n]$. Supongamos que $A\in k[X_1,\ldots,X_n]^{r\times s}$ y que $\deg a_{ij} \leq d$.

Hagamos $X(\lambda) = \det(\lambda.I_{r+s} - C.A')$

$X(\lambda)$ es un polinomio en λ a coeficientes en $k[X_1,\ldots,X_n,Y]$. Sea m la máxima potencia de λ que divide a $X(\lambda)$. Luego

$$X(\lambda) = a_m(X_1,\ldots,X_n,Y)\,\lambda^m + a_{m+1}(X_1,\ldots,X_n,Y)\,\lambda^{m+1} + \ldots + a_{r+s}(X_1,\ldots,X_n,Y)\,\lambda^{r+s}$$

con $a_m \neq 0$.

Como las operaciones hechas hasta obtener $X(\lambda)$ conmutan con la evaluación de las variables $X_1,\ldots,X_n$, vemos que la condición ii') es equivalente a: $m = s-k$ y no existe ningún punto $(\alpha_1,\ldots,\alpha_n)\in k^n$ tal que

$$a_m(\alpha_1,\ldots,\alpha_n,Y) \equiv 0 \quad \text{como polinomio en } Y.$$

Haciendo

$$a_m(X_1,\ldots,X_n,Y) = b_0(X_1,\ldots,X_n) + b_1(X_1,\ldots,X_n).Y + \ldots + b_l(X_1,\ldots,X_n).Y^l$$

debemos entonces analizar si el ideal generado por $\{b_0,\ldots,b_l\}$ es trivial lo que se hace usando el Nullstellensatz efectivo [10].

Analisis de la complejidad:

Para obtener $X(\lambda)$:

tiempo secuencial : $O((r+s)^3.d^n)$

tiempo paralelo: $O(n^2.\log^2(r+s).d)$

Para el Nullstellensatz efectivo:

Hay que decidir la trivialidad del ideal generado por $b_0,\ldots,b_l$.

Observemos que $l \leq (r+s)^2$ y $\deg(b_i) \leq (d+r+s)(r+s)$, luego las cotas de [Di.,Corollary(1.9.1)] nos dicen que puede decidirse la trivialidad del ideal en

tiempo paralelo: $O(n^4 \log^2(r+s).d)$

tiempo secuencial: $(d(r+s))^{O(n^2)}$

Vemos entonces que este algoritmo decide si M es libre en tiempo **polinomial** con respecto a r y s (y por lo tanto con respecto al rango de M).

[Di.]: A. Dickenstein, N.Fitchas, M.Giusti, C.Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. Aparecerá en Discrete Applied Math., special issue AAECC-7, Toulouse 1989.

Apendice 2

Resolucion de sistemas de ecuaciones lineales con coeficientes polinomiales.

En este apéndice L denota un dominio arbitrario, con cuerpo de fracciones k y con $\bar{k}$ notamos la clausura algebraica de k.

Para una mejor comprensión se tratará primero el caso en que los coeficientes del sistema son constantes en L para luego pasar al caso polinomial.

1.Coeficientes constantes.

Sea $A \in L^{s \times m}$ una matriz, $b \in L^{s \times 1}$ una matriz columna y sea $M := \max\{s,m\}$; se busca resolver el sistema no homogéneo: $\{ A.x = b\}$, donde $x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ es un vector columna de incógnitas.

Proposicion 1:

Es posible resolver el sistema $\{ A.x = b\}$ por medio de una red aritmética R_M en tiempo secuencial: $M^{O(1)}$, tiempo paralelo: $(\log M)^{O(1)}$

Demostracion:

Etapa 1: Encontrar una submatriz de A de rango máximo. Para esto se sigue la idea de [B.G.H.]: sea A_i la submatriz de A formada por las primeras i filas, sea $r_i := \text{rango}(A_i)$ y $r := r_s = rg(A)$

De acuerdo a [Mul] es posible calcular todos los r_i $(1 \leq i \leq s)$ en tiempo secuencial: $M^{O(1)}$, tiempo paralelo: $O(\log^2 M)$.

Si ponemos $r_0 = 0$, entonces el conjunto $\{ 1 \leq i \leq s / r_{i-1} \neq r_i \}$ corresponde a r filas linealmente independientes.

Tomando la submatriz formada por estas r filas y repitiendo el razonamiento anterior se encuentra $\bar{A} \in L^{r\times r}$ tal que $rg\ \bar{A} = r = rg\ A$.

Etapa 2: Por [Mul] es posible saber si hay solución o no. Supongamos que la hay, entonces permutando filas y columnas de A y las correspondientes entradas en los vectores columna x y b se puede llevar la situación original al caso siguiente:

$$\begin{pmatrix} \bar{A} & * \\ C & * \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_m \end{pmatrix} = \begin{pmatrix} b_1 \\ b_s \end{pmatrix} \quad \text{con } \bar{A} \in L^{r\times r},\ \det \bar{A} \neq 0,\ C \in L^{(s-r)\times r}$$

Sea $B \in L^{s\times s}$ la matriz

$$B := \begin{pmatrix} \operatorname{adj} \bar{A} & 0 \\ -C.\operatorname{adj} \bar{A} & \det\bar{A}.Id \end{pmatrix}, \text{ claramente } B \text{ es inversible.}$$

Sea $\begin{pmatrix} b'_1 \\ \vdots \\ b'_s \end{pmatrix} := B.b$. Multiplicando a izquierda por B queda (debido a que no cambia el rango la submatriz inferior dercha es 0)

$$\begin{pmatrix} \det \bar{A}.Id & * \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} b'_1 \\ \vdots \\ b' \end{pmatrix} \quad (\text{ en particular } b'_{r+1} = \ldots = b'_s = 0)$$

(Toda esta construcción se puede realizar en $M^{O(1)}$(secuencial) y $O(\log^2 M)$ (paralelo) utilizando el algoritmo sin divisiones de [Ber] para el cálculo de determinante en NC)

Entonces una solución particular del sistema es: $(x_1,\ldots,x_m)$ tal que $x_i = b'_i/\det \bar{A}$ $(1 \leq i \leq r)$ y $x_i = 0$ $(i > r)$

Las soluciones del sistema homogéneo son claramente

$$\{ (x_1,\ldots,x_m) /\ x_1 = x_2 = \ldots = x_r = 0 \}$$

2. Coeficientes polinomiales

De (1) resulta claro que si el dominio L es un anillo de polinomios en n variables es posible encontrar soluciones pero que eventualmente estarán en el cuerpo de funciones racionales y por lo tanto dichas soluciones no se comportan bien por especialización.

Sean $Y_1,\dots,Y_n$ indeterminadas sobre k.

Definición:([He]) Sea $\mathcal{G} \subseteq \bar{k}[Y_1,\dots,Y_n]$ un conjunto finito, a un conjunto **no vacio** de la forma

$$\{\ y \in \bar{k}^n /\ G_{i_1}(y)=0 \wedge \dots \wedge G_{i_r}(y)=0 \wedge G_{i_{r+1}}(y) \neq 0 \wedge \dots \wedge G_{i_l}(y) \neq 0\ \}$$

(donde $\mathcal{G} = \{\ G_{i_1},\dots,G_{i_l}\}$) se lo llama una $\mathcal{G}$-célula.

se tiene entonces

Proposicion 2: Para cada $\mathcal{G} \subseteq \bar{k}\ [Y_1,\dots,Y_n]$ con $\sum_{G\in \mathcal{G}} \deg G = D$, existe una red que calcula todas las $\mathcal{G}$-células.

Demostracion: [G.H.M.] o [F.G.M.2].

Sea $A \in L[Y_1,\dots,Y_n]^{s\times m}$, $b \in L[Y_1,\dots,Y_n]^{s\times 1}$, $D \in \mathbb{N}$ de modo que $\sum (1+\deg F) \leq D.$, donde se suma sobre todos los $F \in L[Y_1,\dots,Y_n]$ que aparecen en las matrices A y b. Se tiene entonces:

Proposicion 3: Existe una red aritmética $\mathcal{R}_{D,n}$ que construye:

(i) una familia de polinomios $\mathcal{G} \subseteq L[Y_1,\dots,Y_n]$ con $\sum_{G\in\mathcal{G}} \deg G = D^{n^{O(1)}}$, y un subconjunto de $\mathcal{G}$-células, $\mathcal{C}$.

(ii) para cada $\mathcal{G}$-célula $C\in \mathcal{C}$, polinomios $P_1,\dots,P_m,P_{m+1}$ en $L[Y_1,\dots,Y_n]$ con $\sum_{i=1}^{m+1} \deg P_i = D^{n^{O(1)}}$ de modo que, si $\alpha \in \bar{k}^n$ es un elemento de C, entonces $(P_1(\alpha)/P_{m+1}(\alpha),\dots,P_m(\alpha)/P_{m+1}(\alpha)\ )$ es una solución del sistema

$A(\alpha).x = b(\alpha)$. (P_{m+1} es tal que $P_{m+1}(\alpha) \neq 0$).

Esta construción puede hacerse en tiempo secuencial : $D^{n^{O(1)}}$, y tiempo paralelo: $(n.\log D)^{O(1)}$

Demostracion: La demostración es una versión paramètrica de la Proposición 1 combinada con la construcción de K.Mulmuley[Mul] y la Prop. anterior.

Para cada i ($1 \leq i \leq s$) sea A_i la submatriz de A que contiene las primeras i-filas. Aplicando la demostración del resultado de [Mul] se construyen ciertos polinomios en $L[Y_1,\ldots,Y_n]$ (coeficientes de polinomios característicos que determinan el rango de A_i). Tales polinomios se construyen en tiempo admisible y sus grados no sobrepasan $D^{O(1)}$.Repitiendo el razonamiento para cada i (hay a lo sumo s valores de i y $s \leq D$) se construye una familia finita $\mathcal{G}_1 \subseteq L[Y_1,\ldots,Y_n]$ tal que $\sum_{G\in\mathcal{G}_1} G = D^{O(1)}$ y $\mathcal{G}_1$ se calcula en tiempo admisible.

Es inmediato, por la construcción de $\mathcal{G}_1$, que cada $\mathcal{G}_1$-célula W tiene asociada una submatriz A_W de A tal que para cada $\alpha \in W$, $rg\ A_W(\alpha) = rg\ A(\alpha)$ y las filas de $A_W(\alpha)$ son independientes. Fijemos W una $\mathcal{G}_1$-célula.

Repitiendo el razonamiento hecho para las filas de A, ahora para las columnas de A_W se construye en tiempo admisible una familia $\mathcal{G}_W$ tal que $\sum_{G\in \mathcal{G}_W} \deg G = D^{O(1)}$.

Sea $\mathcal{G} := \mathcal{G}_1 \cup \bigcup \mathcal{G}_W$, donde W es $\mathcal{G}_1$-célula, y sea $\mathcal{C}$ el subconjunto de $\mathcal{G}$-células definido como aquellas $\mathcal{G}$-células contenidas en algún conjunto de la forma $W \cap V$ con W $\mathcal{G}_1$-célula y V $\mathcal{G}_W$-célula.

Resulta claro que $\mathcal{C}$ se puede construir en tiempo admisible.

Como consecuencia de la construcción de $\mathcal{C}$ es inmediato comprobar que para cada $C \in \mathcal{C}$ existe una matriz bien determinada, que notaremos A_C tal que:

(i) A_C es una submatriz cuadrada de A

(ii) si $\alpha \in C$ entonces $A_C(\alpha)$ es inversible y rg $A(\alpha)$ = rg $A_C(\alpha)$.

La submatriz $A_C(\alpha)$ corresponde a $\bar{A}(\alpha)$ con la notación de la demostración de la Proposición 1.

Ahora resulta claro como encontrar las soluciones del sistema $A(\alpha).x=b(\alpha)$ pues se aplica la etapa 2 de la demostración de la Proposición 1 paramétricamente y donde $P_1(\alpha) = b'_1(\alpha),\ldots,P_m(\alpha) = b'_m(\alpha)$ y $P_{m+1}(\alpha) = \det A_C(\alpha)$ para todo $\alpha \in C$.

Se toma entonces $P_1 = b'_1,\ldots,P_m = b'_m$ y $P_{m+1} = \det A_C$ con lo que termina la demostración.