Tesis de Posgrado

Aspectos algorítmicos para el cálculo de bases de módulos sobre anillos de polinomios

Almeida, Marcela Silvia

2001

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

UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Aspectos algorítmicos para el cálculo de bases de módulos sobre anillos de polinomios

Marcela Silvia Almeida

Director de Tesis: Dr. Pablo L. Solernó
Lugar de Trabajo: Departamento de Matemática

Trabajo de Tesis para optar por el título de Doctor en Ciencias Matemáticas
Mayo de 2001

Índice General

Aspectos algorítmicos

para el cálculo de bases

de módulos sobre el anillo de polinomios

Resumen

Sea k un cuerpo perfecto infinito, $k[x_1, \ldots, x_n]$ el anillo de polinomios en n variables y $F \in k[x_1, \ldots, x_n]^{M \times M}$ una matriz polinomial de una proyección. Si sus entradas están dadas por un straight line program de tamaño L y sus grados acotados por D, mostramos que existe un algoritmo bien paralelizable que computa una base del núcleo y de la imagen de F en tiempo $(nL)^{O(1)}(MD)^{O(n)}$.
Este resultado nos permite obtener, haciendo uso de la teoría de trazas, un algoritmo simplemente exponencial que computa una base para un anillo intersección completa en posición de Noether.
Además, como una consecuencia de nuestras técnicas podemos mostrar un algoritmo simplemente exponencial que decide si un $k[x_1, \ldots, x_n]$-módulo finito dado por una matriz de presentación es libre y, en ese caso, exhibir una base.

Palabras clave: anillo intersección completa, módulo proyectivo, Teorema de Quillen-Suslin, straight line program, teoría de trazas, matriz unimodular.

Algorithmics aspects

for the computation of bases

of modules over the polynomial ring

Abstract

Let k an infinite perfect field, $k[x_1, \ldots, x_n]$ the polynomial ring in n variables and $F \in k[x_1, \ldots, x_n]^{M \times M}$ a projection polynomial matrix. If the entries of F are polynomials given by a straight line program of size L and their total degrees are bounded by D, we show a well parallelizable algorithm which computes a basis for the kernel and for the image in time $(nL)^{O(1)}(MD)^{O(n)}$.
This result allows to obtain, using trace theory, a simple exponential algorithm to compute a basis of a complete intersection ring in Noether position.
Also, as a consequence of our tecniques we can show a well parallelizable algorithm which decides if a $k[x_1, \ldots, x_n]$-module given by a presentation matrix is free and, in this case, to exhibit a basis.

Keywords: complete intersection ring, projective module, Quillen-Suslin Theorem, straight line program, trace theory, unimodular matrix.

Parte I
Introducción

Este trabajo trata sobre el cómputo de soluciones de sistemas de ecuaciones lineales sobre el anillo de polinomios y en particular sobre el cálculo de bases para ciertos $k[x_1,\ldots,x_n]$-módulos libres.
Son conocidos los obstáculos intrínsecos que presentan los métodos de álgebra lineal como herramienta para el álgebra conmutativa efectiva: por ejemplo, en lo que respecta a los temas que vamos a tratar, en el bien conocido trabajo de Mayr y Meyer [44] (ver también [14]) se demuestra entre otros resultados que el problema de encontrar soluciones para un sistema lineal de ecuaciones sobre $k[x_1,\ldots,x_n]$ requiere tiempo (es decir, cantidad de operaciones sobre k) doblemente exponencial en el número de variables e involucra polinomios de grado de orden similar. Más precisamente se demuestra que existen familias de matrices polinomiales tales que cada sistema de generadores de sus núcleos contiene un vector con una coordenada de grado doblemente exponencial. El resultado se puede enunciar como en [14, Corollaire, pag.10]:

Sea $\varepsilon > 0$. *Sean* n *y* D *enteros tales que* $n \geq 10$, $D \geq 3$, $D \geq 2 + \frac{1}{32\varepsilon}$. *Existe una sucesión polinomial* $P_1,\ldots,P_n$ *de grados acotados por* D *en* $A := k[x_1,\ldots,x_n]$ *(donde* $P_1 := x_1$, $P_2 := x_2$*) tales que cualquier sistema de generadores del* A*-submódulo de* A^n *consistente de todas las sucesiones* U_i *con* $\sum_i U_i P_i = 0$, *contiene al menos un vector cuya primer coordenada tiene grado* $\geq N$, *donde* $\log_2 \log_2 N > (\frac{1}{8} - \varepsilon)n + \log_2 \log_2 D - \frac{9}{4}$.

A pesar de lo desalentador de este resultado, bajo ciertas hipótesis sobre la matriz asociada al sistema de ecuaciones, se pueden hacer estimaciones mejores y más precisas. Por ejemplo, si la matriz de entrada es tal que sus filas pueden extenderse a una base de todo el espacio, se conoce una cota simplemente exponencial para el grado de la base de su núcleo y la complejidad de un algoritmo que la calcula ([9, Corollary 3.2]).
En cierto sentido el presente trabajo de tesis generaliza este tipo de resultados simplemente exponenciales para una familia más amplia de matrices para las que buscamos de manera efectiva bases de su núcleo y de su imagen.
Exhibimos algoritmos simplemente exponenciales para este problema en el caso en que la matriz de entrada F es una proyección y más generalmente para el caso en que F es una matriz unimodular (i.e. cuando los menores no nulos de tamaño máximo generan todo el anillo $k[x_1,\ldots,x_n]$), mostrando así que el caracter doblemente exponencial general del resultado mencionado de Mayr y Meyer no aparece en ese tipo de matrices.
Como consecuencia de estos hechos podemos deducir también nuevos resultados (simplemente exponenciales) relativos al cálculo de bases de ciertos módulos libres sobre el anillo de polinomios: un método que decide si un módulo dado por una matriz de relaciones es libre o no y un algoritmo que calcula bases de anillos intersección completa en posición de Noether (cf. la sección que sigue para los enunciados precisos).
La pregunta natural que surge en este punto es si el carácter simplemente exponencial de los resultados obtenidos es trascendente o no. Sin duda la mejora aunque más no sea en ciertos casos al descender de la clase "doblemente exponencial" a "simplemente

exponencial"es un claro avance desde el punto de vista teórico. Sin duda también el caracter exponencial muestra la imposibilidad aparente de la implementación eficiente de nuestros algoritmos en casos interesantes.
Sin embargo, tampoco podemos soslayar el hecho de que si, por ejemplo, los polinomios de entrada de nuestro algoritmo son polinomios de grado d en $k[x_1,\ldots,x_n]$ dados por sus coeficientes, la sola escritura de los mismos ocupará un espacio del orden d^n (es decir, exponencial).
Para intentar solucionar este problema es que desde hace tiempo se ha trabajado con otras estructuras de datos (polinomios ralos, "straight line programs") hechos que hemos tomado en cuenta en nuestros métodos y estrategias.
Si bien en ciertos casos este cambio de estructura de datos ha dado lugar a algoritmos de eliminación polinomiales en ciertos invariantes geométricos (ver [24], [26], [23], [25], [28] y [30]) el carácter complejo de los algoritmos de este trabajo de tesis no permite aparentemente un reconocimiento sencillo de invariantes similares y es así que la exponencialidad parece no poder ser evitada.
En nuestra defensa deberíamos mencionar que nuestro método está fuertemente fundado en subalgoritmos de eliminación, para los cuales sobran fuertísimas evidencias de su comportamiento intrínseco simplemente exponencial (ver [22], [29] y [12]).

Descripción de los resultados:

Tal como lo mencionamos arriba, en nuestro trabajo combinamos dos estructuras de datos distintas (escritura densa -vector de coeficientes- y programas de evaluación -straight line programs-) y tal hecho se manifiesta en nuestros enunciados.
En la Parte II se obtienen bases para el núcleo y la imagen de la matriz polinomial de una proyección. Más explícitamente tenemos:

Teorema A (ver Teorema 25) *Sea* $F \in k[x_1,\ldots,x_n]^{M\times M}$ *una matriz polinomial correspondiente a una proyección (i.e.* $F^2 = F$*) tal que sus entradas son polinomios de grados acotados por un entero* D *y están dados por un straight line program de tamaño* L*. Entonces existe un algoritmo bien paralelizable que corre en tiempo secuencial* $(nL)^{O(1)}(MD)^{O(n)}$ *que computa dos subconjuntos de* $k[x_1,\ldots,x_n]^M$*:* $\{v_1,\ldots,v_s\}$ *y* $\{v_{s+1},\ldots,v_M\}$ *tales que:*

1. $\{v_1,\ldots,v_M\}$ *es una base de* $k[x_1,\ldots,x_n]^M$.
2. $\{v_1,\ldots,v_s\}$ *es una base de* $\mathrm{Im}(F)$ *y* $\{v_{s+1},\ldots,v_M\}$ *es una base de* $\mathrm{Ker}(F)$.
3. *Las coordenadas de los vectores* v_i *son polinomios de grados acotados por* $(MD)^{O(n)}$ *y están dados por un straight line program de tamaño* $(nL)^{O(1)}(MD)^{O(n)}$.

Las técnicas que aplicamos están sin duda inspiradas en las ideas clásicas de Quillen, Suslin y Vaserstein usadas para resolver la "Conjetura de Serre"(es decir que todo módulo proyectivo finito sobre un anillo de polinomios sobre un cuerpo es libre). Desde el punto de vista algorítmico muchas de estas ideas aparecen en artículos relacionados con el cómputo de bases de módulos libres, combinados con procesos de bases de Groebner (se puede ver [39], [41], [42]) o con el Nullstellensatz efectivo (ver [18], [9]). Nuestro enfoque es el

segundo ya que las cotas teóricas que aparecen con bases de Groebner son muy grandes para nuestros propósitos.
Si nos permitimos cotas un poco menos satisfactorias obtenemos también un resultado similar para el caso en que la matriz es unimodular (no necesariamente una proyección):

Teorema B *Sea* $F \in k[x_1,\ldots,x_n]^{N\times M}$ *una matriz polinomial unimodular cuyas entradas son polinomios de grados acotados por un entero* D *y están dados por un slp de tamaño* L. *Entonces existe un algoritmo bien paralelizable que corre en tiempo secuencial* $(nL)^{O(1)}((M+N)D)^{O(n^4)}$ *computando una base* $\{v_1,\ldots,v_M\}$ *de* $k[x_1,\ldots,x_n]^M$ *y una base* $\{w_1,\ldots,w_N\}$ *de* $k[x_1,\ldots,x_n]^N$ *tal que:*

1. $\{w_1,\ldots,w_s\}$ *es una base de* $\mathrm{Im}(F)$ *y* $\{v_{s+1},\ldots,v_M\}$ *es una base de* $\mathrm{Ker}(F)$.
2. *Las coordenadas de los vectores de ambas bases son polinomios de grados acotados por* $((M+N)D)^{O(n^4)}$ *y están dados por un slp de tamaño* $(nL)^{O(1)}((M+N)D)^{O(n^4)}$.

■

Con algunas de las herramientas algorítmicas que utilizamos para obtener los resultados anteriormente citados, podemos además determinar si un $k[x_1,\ldots,x_n]$-módulo finito dado por generadores y relaciones (es decir, conociendo una matriz de presentación) es libre o no y en caso afirmativo, exhibir una base:

Teorema C *Sea* P *un* $k[x_1,\ldots,x_n]$*-módulo de tipo finito y* $F \in k[x_1,\ldots,x_n]^{N\times M}$ *una matriz de presentación para* P *(ver Definición 3). Supongamos que las entradas de la matriz* F *tienen grados totales acotados por* D *y están dados por un slp de tamaño* L. *Entonces existe un algoritmo bien paralelizable que corre en tiempo secuencial* $(nL)^{O(1)}((M+N)D)^{O(n^4)}$ *que decide si* P *es libre y, en caso afirmativo, computa una base de* P.

En la última parte del trabajo abordamos otro problema relacionado con el cálculo de bases de $k[x_1,\ldots,x_n]$- módulos libres y que aparece de manera natural en la búsqueda de soluciones efectivas de sistemas polinomiales de ecuaciones: sean $f_1,\ldots,f_{n-r} \in k[x_1,\ldots,x_n]$ una sucesión regular sobre el anillo de polinomios sobre un cuerpo perfecto k. Supongamos que las variables están en posición de Noether, es decir que el morfismo canónico $R := k[x_1,\ldots,x_r] \to S := k[x_1,\ldots,x_n]/(f_1,\ldots,f_{n-r})$ es entero e inyectivo. Se sabe que bajo estas hipótesis el anillo S es un $R-$ módulo libre de rango finito (ver [17, Corollary 18.17], [27, Lemma 3.3.1], [49]). Este problema ha sido considerado esencialmente en el caso $0-$dimensional, donde el anillo de base R es un cuerpo k y el anillo S no es otra cosa que un $k-$espacio vectorial. Para este caso existen buenos algoritmos teóricos que computan bases de S pero cuyas técnicas no pueden ser generalizadas al menos de manera obvia para dimensiones mayores.
Haciendo uso de técnicas de dualidad efectiva más o menos conocidas, obtuvimos de manera algorítmica una R-base para S, aplicando los resultados de la Parte II a una matriz construida en base a una cierta "función traza"(que es descripta completamente en la Parte III) . El resultado preciso es el siguiente:

Teorema D (ver Teorema 54) *Sean* $f_1, \ldots, f_{n-r} \in k[x_1, \ldots, x_n]$ *una sucesión regular de polinomios de grados acotados por un entero* d *y dados por un straight line program de tamaño* ℓ, *tal que el morfismo canónico* $R := k[x_1, \ldots, x_r] \to S := k[x_1, \ldots, x_n] / (f_1, \ldots, f_{n-r})$ *es entero e inyectivo ("posición de Noether") y supongamos que el anillo* S *es reducido (i.e.* S *no tiene nilpotentes). Entonces existe un algoritmo bien paralelizable que corre en tiempo secuencial* $O(n)\,\ell d^{O(n^2)}$ *que computa, a partir de los polinomios de input* $f_1, \ldots, f_{n-r}$, *un straight line program de tamaño* $n^{O(1)} d^{O(n^2)}$ *que evalúa una familia de polinomios en* $k[x_1, \ldots, x_n]$ *de grados acotados por* $nd^{O(n^2)}$, *y cuyas clases en* S *son una* $R-$ *base.*
Si S *no es reducido, también es posible computar una* $R-$ *base de* S *mediante un algoritmo (no necesariamente bien paralelizable) que corre en el mismo tiempo secuencial.*

Este resultado también se puede reinterpretar desde el punto de vista topológico. Sea $V \subset \mathbb{A}^n$ la variedad algebraica definida por los polinomios $f_1, \ldots, f_{n-r}$ y sea $\pi : V \to \mathbb{A}^r$ la proyección inducida por la inyección $R \hookrightarrow S$; en términos de fibrados algebraicos, el hecho de que S sea libre sobre R dice que la variedad V es un fibrado trivial sobre $\mathbb{A}^r$. En este sentido el Teorema D da una descripción explícita y algorítmica de esa trivialización.

Tal como mencionamos brevemente, nuestro método para abordar este problema combina herramientas de la teoría clásica de dualidad con los resultados de bases de núcleos e imágenes de matrices de la Parte II. En el intento de ofrecer un trabajo lo más autocontenido posible es que desarrollamos en la Parte III una adaptación de la teoría de trazas para álgebras de Gorenstein (ver [38]) para el caso particular de intersecciones completas y que según nuestros conocimientos no aparece expuesto de manera elemental en la literatura. En este caso (es decir intersección completa) nos fue posible construir una traza para S sobre R de manera explícita (que coincide con la llamada "traza asociada a la sucesión regular"). La Parte III puede ser omitida por aquellos más interesados en comprender el aspecto algorítmico, tomando en cuenta sólo los resultados centrales.
Tal como fue mencionado, a partir de la traza construida en la Parte III, se obtiene una matriz F que resulta ser una proyección y de la que, gracias al Teorema A, podemos encontrar una base para su imagen, que es la base de S buscada. El incremento de las cotas de complejidad en el Teorema D con respecto al Teorema A se debe al tamaño de la matriz F (de orden $d^{O(n)}$).
Con posterioridad a la redacción de la tesis hemos obtenido una manera alternativa para demostrar el Teorema D que sólo hace uso del Teorema B y del bien conocido Teorema de Wiebe para sucesiones regulares (ver Teorema 32) que no está incluida aquí.

Parte II
Algebra lineal efectiva sobre el anillo de polinomios

En esta parte desarrollaremos la construcción de bases para el núcleo y la imagen de matrices polinomiales de proyecciones y, más en general, de matrices polinomiales unimodulares.
En la Sección II.1 nos dedicaremos a la descripción del modelo algorítmico y a la familia de rutinas básicas que utilizaremos a lo largo de este trabajo. Desarrollaremos explícitamente uno de ellos: se trata de un algoritmo que decide la unimodularidad de una matriz polinomial evitando el cálculo de menores superfluos. A partir de esto, obtenemos una manera nueva de decidir si un $k[x_1, \ldots, x_n]$-módulo dado por generadores y relaciones es libre o no (ver Proposición 4).
En la Sección II.2 nos dedicaremos a la construcción de bases para el núcleo y la imagen de la matriz de un proyección (ver Teorema 25).
Por último en la Sección II.3 extenderemos el resultado a matrices unimodulares.

II.1 El modelo computacional

Nuestro modelo computacional sigue aquellos presentados en varios artículos (por ejemplo, [20], [26], [23]), donde se hace un estudio exhaustivo de sus ventajas y limitaciones con respecto a otros modelos alternativos. Por esta razón sólo establecemos acá nociones mínimas acerca de ellos.

Sea k un cuerpo de base perfecto e infinito. Los algoritmos que usaremos se describen mediante *redes aritméticas* (cf. [55]) representadas por grafos acíclicos orientados donde cada nodo representa una constante de k, una variable de input, una operación aritmética $* \in \{+, -, \times, \div\}$ en k, una operación booleana, un test de igualdad o selección. Suponemos que nuestras redes aritméticas son siempre *libres de divisiones:* esto significa que cuando evaluamos la red en un punto genérico (i.e. en sus variables de input) ejecutamos sólo divisiones por constantes no nulas de k (nuestra red aritmética sólo computa polinomios con coeficientes en k).
Computamos operaciones aritméticas o booleanas, tests de igualdad y selecciones con costo unitario y así asociamos a una red aritmética dos medidas de complejidad: *el tiempo secuencial* o *complejidad secuencial*, también llamado *tamaño* (la cantidad de nodos) y *el tiempo paralelo* o *complejidad paralela*, también llamado *profundidad* (el tamaño del camino orientado más largo en el grafo). Una red aritmética sin nodos de selección o decisión (y por consiguiente, sin operaciones booleanas) se llama un *circuito aritmético* o *straight-line program* (escribimos "slp"). De este modo, nuestros slp computarán siempre polinomios en las variables de input con coeficientes en k. Se pueden encontrar definiciones más precisas y propiedades en [8], [55] y [36].

Decimos que un algoritmo es *bien paralelizable* si su tiempo paralelo depende polinomialmente en $\log_2$ (tiempo secuencial) y en la profundidad de los slp de input.

Los polinomios con los que trataremos serán codificados como los circuitos aritméticos que los evalúan. De todas maneras, consideraremos, a veces, polinomios representados por un vector de coeficientes (*forma densa*) y también en una forma mixta: polinomios codificados en forma densa con respecto a variables principales específicas mientras que los coeficientes con respecto a esas variables están codificados por un circuito aritmético.

Un punto clave en nuestros algoritmos, como en muchos algoritmos de eliminación, es el problema de decidir si un polinomio es cero o no. La interpolación trivial requiere la evaluación del polinomio en muchos puntos (si d es el grado del polinomio y n el número de variables, se necesitan $(d+1)^n$ puntos), de modo que los tiempos de complejidad se incrementan significativamente.
A pesar de esto, cuando los polinomios están dados por slp se tiene el siguiente resultado (ver [33] ó [20]):

Teorema (Correct test sequences) *Sea $W(d,n,L)$ un conjunto de polinomios en $k[x_1,\ldots,x_n]$ de grados totales acotados por d, que pueden ser evaluados por un slp de tamaño L. Sea $m := 6(L+n)(L+n+1)$ y Γ un subconjunto arbitrario de k cuyo cardinal es $2L(d+1)^2$. Entonces existe un subconjunto $Q = \{\gamma_1,\ldots,\gamma_m\} \subset \Gamma^n$, que depende sólo de d,n,L y Γ, que verifica la siguiente propiedad: un polinomio $f \in W(d,n,L)$ es el polinomio nulo si y sólo si $f(\gamma_i) = 0$ para todo $i = 1,\ldots,m$.* ■

Los vectores $\gamma_1,\ldots,\gamma_m$ se llaman una *correct test sequence* para el conjunto $W(d,n,L)$. Deasfortunadamente no se conoce un procedimiento eficiente para construir una correct test sequence (los métodos standard para computarla corren en tiempo de complejidad exponencial). Como los grados, el número de variables y la complejidad de la evaluación de todos los polinomios que aparecen en nuestros algoritmos se pueden estimar *a priori,* en nuestro modelo supondremos la hipótesis razonable de que una correct test sequence para todos estos polinomios es dada en un preproceso (ver también [20]). De todas maneras, notemos que se puede hacer una adecuada versión aleatoria ("random") para la elección de una correct test sequence (ver [20, Section 2.1]); este hecho transforma automáticamente nuestros algoritmos en algoritmos probabilísticos con las mismas cotas de complejidad (ver también [43]).

II.1.1 Algoritmos básicos

A.- Pasaje de straight line programs a forma densa. Cómputo de las componentes homogéneas
Sea f un polinomio en $k[x_1,\ldots,x_n]$ dado por un slp de tamaño L. Sea $m \in \mathbb{N}$, $1 \leq m \leq n$, y $d := \deg_{x_{n-m+1},\ldots,x_n}(f)$; entonces existe un algoritmo bien paralelizable que corre en tiempo secuencial $Ld^{O(m)}$ cuyo output son los coeficientes del polinomio f visto como un

polinomio en $k[x_1,\ldots,x_{n-m}][x_{n-m+1},\ldots,x_n]$. Más aun, estos coeficientes están dados por un slp de tamaño $Ld^{O(m)}$ (ver [48, Prop.3.1.1]).
Este procedimiento puede usarse para obtener las componentes homogéneas de un polinomio dado: sea f un polinomio en $k[x_1,\ldots,x_n]$, de grado D, dado por un slp de tamaño L y sea t una nueva variable; el polinomio $g := f(tx_1,\ldots,tx_n) \in k[x_1,\ldots,x_n,t]$ tiene grado acotado por D en t y puede ser evaluado por un slp de tamaño $L+n$. Interpolando con respecto a la variable t, obtenemos las componentes homogéneas de f en tiempo $(L+n)\,D^{O(1)}$ y podemos evaluarlas mediante un slp de tamaño $(L+n)\,D^{O(1)}$.

B.- Determinante, inversa y rango de matrices polinomiales
Sea F una matriz en $k[x_1,\ldots,x_n]^{N\times N}$ cuyas entradas son polinomios dados por un slp de tamaño L. Existen algoritmos bien paralelizables que corren en tiempo $(LN)^{O(1)}$ que computan:

1. un slp que evalúa el determinante y los coeficientes en $k[x_1,\ldots,x_n]$ del polinomio característico de F.
2. un slp que evalúa las entradas de F^{-1} (si F es inversible).
3. el rango de F (como matriz en $k(x_1,\ldots,x_n)^{N\times N}$) y una submatriz de rango maximal.

Los primeros dos ítems se siguen de Berkowitz [5] y el último de Mulmuley [45] (se puede ver también una suscinta descripción en la sección **G**); en ambos casos los algoritmos mencionados se pueden adaptar fácilmente a polinomios multivariados dados por slp.

C.- División polinomial de Euclides
Sean f y g polinomios en $k[x_1,\ldots,x_n]$, de grados $D_1 \le D$ y $D_2 \le D$ respectivamente, dados por un slp de tamaño L, y supongamos que g es mónico en la variable x_n. Entonces existe un algoritmo bien paralelizable que corre en tiempo $(LD)^{O(1)}$ que produce un slp que evalúa el cociente y el resto en la división euclideana de f por g con respecto a x_n. Sus grados totales resultan acotados por D_1D_2. Este procedimiento es una consecuencia directa de la Subrutina **A** y del algoritmo de Berkowitz.

D.- Nullstellensatz efectivo en nuestro modelo
Sean $f_1,\ldots,f_s$ polinomios en $k[x_1,\ldots,x_n]$ de grados acotados por D, dados por un slp de tamaño L. Existe un algoritmo bien paralelizable que corre en tiempo $(nL)^{O(1)}\,D^{O(n)}$ que decide si 1 pertenece al ideal $(f_1,\ldots,f_s)$ y , en ese caso, computa mediante un slp del mismo tamaño ciertos polinomios $p_1,\ldots,p_s \in k[x_1,\ldots,x_n]$ tales que:

1. $1 = p_1f_1 + \cdots + p_sf_s$.
2. $\max_j\{\deg(p_j)\} \le 3n^2D^{n+1}$.

Para una demostración se puede ver [20] ó [26, Th.20] y su bibliografía (ver también los surveys [3] y [53]).

E.- Consistencia de un sistema polinomial de igualdades y desigualdades
Sean $f_1,\ldots,f_s,g_1,\ldots,g_{s'}$ polinomios en $k[x_1,\ldots,x_n]$ de grados acotados por D dados por un slp de tamaño L, y sea $P:=\{f_1=0,\ldots,f_s=0,g_1\neq 0,\ldots,g_{s'}\neq 0\}$. Entonces existe un algoritmo bien paralelizable que corre en tiempo $L^2(ss')^{O(1)}D^{O(n)}$ que decide si P es vacío (ver [48, Remark 3.4.3]).

F.- Cómputo de celdas
Sean $f_1,\ldots,f_s$ polinomios en $k[x_1,\ldots,x_n]$. Cualquier conjunto no vacío de tipo

$$\{f_1\varepsilon_1 0,\ldots,f_s\varepsilon_s 0,\ \varepsilon_i\in\{=,\neq\}\ \forall i\}$$

se llama una *celda*. Siguiendo [48] y el argumento de "divide y reinarás" de [19] es posible enumerar todas las celdas mediante un algoritmo bien paralelizable que corre en tiempo secuencial $L^2s^{O(1)}D^{O(n)}$, donde D es una cota superior para los grados de los polinomios f_i y L es el tamaño del slp que los computa.

G.- Eliminación de menores superfluos

Definición 1 *Sea F una matriz polinomial en $k[x_1,\ldots,x_n]^{N\times M}$ de rango s. Decimos que F es* **unimodular** *si sus menores de tamaño $s\times s$ generan todo el anillo $k[x_1,\ldots,x_n]$. En la literatura se suele llamar unimodulares a las matrices rectangulares en $k[x_1,\ldots,x_n]^{N\times M}$ con $N\leq M$ tales que sus menores de tamaño $N\times N$ generan el anillo de polinomios. Nuestra definición es un poco más general y se corresponde con las matrices cuyas imágenes son sumando directo de $k[x_1,\ldots,x_n]^N$. Notar que entonces la imagen resulta libre por el Teorema de Quillen-Suslin.*

Si F es unimodular tenemos $\binom{M}{s}\binom{N}{s}$ menores de tamaño $s\times s$ que generan $k[x_1,\ldots,x_n]$. En el contexto en que trabajamos buscamos algoritmos con complejidad a lo sumo simplemente exponencial en el número de variables n. Esta cantidad de menores es intratable desde este punto de vista porque resulta exponencial en el tamaño de la matriz. Nuestro propósito, entonces, es poder elegir una cantidad "tratable"(es decir, simplemente exponencial sólo en n) de menores de la matriz que también generen el anillo de polinomios. Con este propósito describimos aquí un algoritmo que calcula un número admisible de menores y que decide, además, si la matriz dada como input es unimodular. Nuestro algoritmo está basado en un procedimiento de K. Mulmuley [45] en el que halla el rango de una matriz sobre un cuerpo.
Empezamos recordando brevemente el algoritmo de Mulmuley para luego mostrar nuestra adaptación para obtener una submatriz de F con rango máximo s.
Sea H una matriz en $k^{N\times M}$. Siempre podemos reducirnos al caso de una matriz cuadrada y simétrica, tomando

$$\begin{pmatrix}0 & H\\ H^t & 0\end{pmatrix}\in k^{(N+M)\times(N+M)}$$

cuyo rango es dos veces el rango de H. Entonces la matriz

$$H'(\lambda) := \begin{pmatrix} 1 & 0 & & 0 \\ 0 & \lambda & & 0 \\ & \ddots & & \\ 0 & 0 & & \lambda^{N+M-1} \end{pmatrix} \begin{pmatrix} 0 & H \\ H^t & 0 \end{pmatrix} \in k[\lambda]^{(N+M)\times(N+M)}$$

donde λ es una indeterminada sobre k, verifica la relación

$$2\mathrm{rk}(H) = \mathrm{rk}(H'(\lambda)) = N + M - \mu$$

donde μ es la máxima potencia de t que divide al polinomio característico $P(t) \in k(\lambda)[t]$ de la matriz $H'(\lambda)$.
Resumiendo, el algoritmo de Mulmuley para calcular el rango de la matriz H consiste en calcular el polinomio característico de la matriz auxiliar $H'(\lambda)$ y determinar la mayor potencia de t que lo divide.
Usaremos lo anterior para, dada una matriz $H \in k^{N\times M}$ de rango s, obtener una submatriz $\bar{H} \in k^{s\times s}$ de rango maximal.
Llamemos $R_1, \ldots, R_N$ a las filas de H y $C_1, \ldots, C_M$ a sus columnas. Usando el algoritmo de Mulmuley, podemos calcular los rangos de las submatrices $H^{(i)} \in k^{i\times M}$ para $i = 1, \ldots, N$ formadas por las primeras i filas de H. Consideremos el conjunto I cuyos elementos son aquellos índices i tales que $\mathrm{rk}(H^{(i)}) > \mathrm{rk}(H^{(i-1)})$. Es claro que el cardinal de I debe ser s. Llamemos $\bar{H}_1 \in k^{s\times M}$ a la matriz $(h_{ij})_{i\in I}$. Haciendo lo mismo con las columnas de H, obtenemos un nuevo conjunto de índices J de modo que las columnas C_j con $j \in J$ son linealmente independientes. Sólo resta ver que la matriz así obtenida $\bar{H} = (h_{ij}) \in k^{s\times s}$ con $i \in I$ y $j \in J$ es inversible. Es claro que la matriz H se puede reducir por operaciones elementales de filas a una matriz del tipo:

$$\begin{pmatrix} \bar{H}_1 \\ 0 \end{pmatrix} = UH$$

donde $U \in k^{N\times N}$ es una matriz inversible. Como las columnas C_j para $j \in J$ son linealmente independientes, esto también es cierto para las correspondientes columnas en UH. Entonces $\bar{H}$ resulta inversible.

Nuestra tarea ahora es eliminar menores superfluos de una matriz F como sigue:

Lema 2 *Sea F una matriz polinomial en $k[x_1, \ldots, x_n]^{N\times M}$ de rango s cuyas entradas son polinomios de grados acotados por D y dados por un slp de tamaño L. Entonces existen $\delta_1, \ldots, \delta_Q \in k[x_1, \ldots, x_n]$ menores no nulos de tamaño $s \times s$ de la matriz F donde $Q \leq ((M+N)^6 D)^n$ tales que $1 \in (\delta_1, \ldots, \delta_Q)$ si y sólo si F es una matriz unimodular.*
En términos algorítmicos estos menores se pueden calcular a través de un algoritmo bien paralelizable en tiempo secuencial $L^{O(1)}((N+M)D)^{O(n)}$ y se pueden dar por medio de un slp de tamaño $(sL)^{O(1)}$. Más aun, este procedimiento da un método que decide si una matriz dada es unimodular en tiempo $L^{O(1)}((N+M)D)^{O(n)}$.

Dem.- Sea $F^{(i)} \in k[x_1, \ldots, x_n]^{i\times M}$ la submatriz de F cuyas filas son las primeras i filas de F para $i = 1, \ldots, N$. Para aplicar el algoritmo de Mulmuley anteriormente citado,

necesitamos tener los coeficientes de la matriz en un cuerpo. Consideramos entonces, para cada $\alpha \in k^n$, el rango de $F^{(i)}(\alpha)$. Por lo anterior, resulta igual a $\frac{M+i-\mu_i}{2}$, donde μ_i es la máxima potencia de t que divide al polinomio característico $P_i(\alpha, \lambda, t)$ de la matriz

$$F^{(i)'}(\alpha, \lambda) := \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ \dots & & \dots \\ 0 & 0 & \lambda^{N+M-1} \end{pmatrix} \begin{pmatrix} 0 & F^{(i)}(\alpha) \\ F^{(i)}(\alpha)^t & 0 \end{pmatrix} \in k[\alpha, \lambda]^{(M+i)\times(M+i)}.$$

Es claro que $P_i(\alpha, \lambda, t)$ es un polinomio en las variables λ y t y también en las coordenadas del punto α. Podemos escribirlo como sigue:

$$P_i(x, \lambda, t) = t^{M+i} + a^i_{M+i-1}(x, \lambda)t^{M+i-1} + \ldots + a^i_{\mu_i}(x, \lambda)t^{\mu_i}$$

donde cada $a^i_j(x, \lambda) \in k[x_1, \ldots, x_n, \lambda]$ es una suma de determinantes de las submatrices cuadradas de tamaño $M+i-j$ de $F^{(i)'}(x, \lambda)$. Entonces, se obtiene la siguiente cota para los grados

$$deg_\lambda a^i_j(x, \lambda) \leq 1 + 2 + \ldots + (M + i - 1) = \frac{(M + i - 1)(M + i)}{2} < \frac{(M + N)^2}{2}.$$

Repitiendo el mismo argumento para las submatrices $C^{(t)}$ cuyas columnas son las primeras t columnas de F obtenemos, de manera análoga, polinomios $b^t_l(x, \lambda)$ con $l = 0, \ldots, N + t - 1$ tales que

$$deg_\lambda b^t_l(x, \lambda) < \frac{(M + N)^2}{2}$$

para $t = 1, \ldots, M$.
Consideremos ahora el conjunto $\Gamma \subset k[x_1, \ldots, x_n]$ cuyos elementos son todos los coeficientes de los polinomios a^i_j y b^t_l en $k[x_1, \ldots, x_n][\lambda]$ para $i = 1, \ldots, N$, $j = 0, \ldots, M + i - 1$, $t = 1, \ldots, M$ y $l = 0, \ldots, N + t - 1$.
Notemos que el cardinal de Γ está acotado por

$$N(N + M)\left(\frac{(N + M)^2}{2} + 1\right) + M(N + M)\left(\frac{(N + M)^2}{2} + 1\right) = (N + M)^{O(1)}.$$

Más aun, observemos que cada condición de signo consistente sobre los polinomios de Γ determina unívocamente el rango de las submatrices $F^{(1)}(\alpha), \ldots, F^{(N)}(\alpha), C^{(1)}(\alpha), \ldots, C^{(M)}(\alpha)$, para cada punto $\alpha \in \bar{k}^n$ que verifica tal condición de signo (donde $\bar{k}$ denota alguna clausura algebraica de k).
Así, si fijamos una condición de signo consistente sobre Γ, la elección de filas y columnas de F como en el procedimiento de Mulmuley antes expuesto es la misma para todos los $\alpha \in \bar{k}^n$ que satisfagan esa condición de signo. En otras palabras, hay una asignación entre el conjunto de las condiciones de signo consistentes sobre Γ y el conjunto de ciertas submatrices de F de rango a lo sumo s tales que para cualquier punto α que verifica una condición fija de signo, su submatriz asociada es inversible cuando se evalúa en α.
Pensemos ahora en la computación de este procedimiento. Como los polinomios a^i_j y b^t_l se pueden evaluar mediante un slp de tamaño $((N + M)L)^{O(1)}$ (mediante el algoritmo

de Berkowitz), interpolando en la variable λ (c.f. [48] ó subrutina **A**), obtenemos los polinomios de Γ también mediante un slp de tamaño $((N+M)L)^{O(1)}$. Luego, computando todas las condiciones de signo consistentes sobre Γ por medio del algoritmo en [19] obtenemos ciertas submatrices distinguidas de F. Tomando en cuenta el cardinal de Γ, los grados de sus elementos y el costo de calcularlos , estas submatrices se pueden obtener en tiempo $L^{O(1)}((N+M)D)^{O(n)}$. Como la cantidad de condiciones de signo consistentes está acotada por $((N+M)^6D)^n$ (ver [32]), la cantidad de submatrices se puede acotar por el mismo número.
Tomamos los polinomios $\delta_1,\ldots,\delta_Q$ como los determinantes de las submatrices asociadas de tamaño $s \times s$.
Falta verificar que estos $\delta_1,\ldots,\delta_Q$ satisfacen lo pedido. Observemos que, si F es unimodular, la matriz en $\bar{k}^{N\times M}$ obtenida por evaluación en un punto arbitrario $\alpha \in \bar{k}^n$ tiene también rango s independientemente del punto α. En otras palabras, $\mathrm{rk}(F) = \mathrm{rk}(F^{(N)}(\alpha)) = \mathrm{rk}(C^{(M)}(\alpha)) = s$ para todo $\alpha \in \bar{k}^n$ (esto es consecuencia del Nullstellensatz y de la definición de unimodular). Por lo tanto, como cada punto $\alpha \in \bar{k}^n$ satisface alguna condición de signo, la submatriz asociada debe tener tamaño $s \times s$ y su determinante debe ser no nulo luego de la evaluación en α; entonces los polinomios $\delta_1,\ldots,\delta_Q$ generan el anillo de polinomios $k[x_1,\ldots,x_n]$. La recíproca es obvia.
Por último, para chequear la unimodularidad de F, es suficiente calcular los polinomios $\delta_1,\ldots,\delta_Q$ y verificar si generan el anillo $k[x_1,\ldots,x_n]$ por medio del Nullstellensatz efectivo. Este procedimiento no incrementa significativamente las complejidades previamente obtenidas. ■

Como una consecuencia fácil de este lema podemos describir un test efectivo para decidir si un $k[x_1,\ldots,x_n]$-módulo finitamente generado dado por generadores y relaciones es libre o no. Este método mejora los resultados previos sobre este problema, al menos desde el punto de vista de la complejidad. (ver también [42])

Definición 3 *Sea P un $k[x_1,\ldots,x_n]$-módulo finitamente generado. Una matriz $F \in k[x_1,\ldots,x_n]^{N\times M}$ se llama una matriz de presentación para P si existe un morfismo suryectivo*

$$\varphi : k[x_1,\ldots,x_n]^M \to P$$

tal que las filas de F son un sistema de generadores para el núcleo de φ.

Tenemos el siguiente resultado (ver también Corolario 29):

Proposición 4 *Sea P un $k[x_1,\ldots,x_n]$-módulo finitamente generado y sea $F \in k[x_1,\ldots,x_n]^{N\times M}$ una matriz de presentación para P. Sea D una cota superior para los grados de las entradas de F y L, para el tamaño del slp que las computa. Entonces existe un algoritmo bien paralelizable que decide si P es libre o no que corre en tiempo secuencial $((N+M)D)^{O(n)}L^{O(1)}$.*

Dem.- Consideremos la siguiente sucesión exacta

$$0 \to \mathrm{Ker}\ (\varphi) \to k[x_1,\ldots,x_n]^M \to P \to 0.$$

Por el Teorema de Quillen-Suslin, sobre el anillo de polinomios es equivalente ser libre a ser proyectivo (es decir, sumando directo de un módulo libre). Entonces P es $k[x_1,\ldots,x_n]$-libre si y sólo si la sucesión anterior se parte. Esto es que Ker (φ) es un sumando directo de $k[x_1,\ldots,x_n]^M$. En este caso, $P\oplus$ Ker $(\varphi) \simeq k[x_1,\ldots,x_n]^M$.
Por lo tanto, es suficiente decidir si Ker $(\varphi) = \mathrm{Im}(F^t)$ es un sumando directo de $k[x_1,\ldots,x_n]^M$ ó, equivalentemente, la unimodularidad de la matriz F. ■

H.- Un cambio lineal de coordenadas
Sea F una matriz polinomial de tamaño $N\times M$ y rango s cuyas entradas son polinomios de grados acotados por una constante D dados por un slp de tamaño L. Siguiendo el algoritmo de Mulmuley mencionado en la Subrutina **B** ítem 3 es posible obtener, en tiempo $(L(N+M))^{O(1)}$, una submatriz no singular de tamaño $s\times s$ de F cuyo determinante $\mu \in k[x_1,\ldots,x_n]$ puede ser evaluado mediante un slp de tamaño $(sL)^{O(1)}$.
En lo que sigue, por razones técnicas, necesitaremos que el polinomio μ sea mónico en todas las variables $x_1,\ldots,x_n$. Más precisamente, si $\delta := \deg(\mu)$ necesitamos que $\mu = \alpha_1 x_1^\delta + \cdots + \alpha_n x_n^\delta + \tilde{\mu}$ donde $\alpha_1,\ldots,\alpha_n \in k$, $\alpha_j \neq 0\ \forall j = 1,\ldots,n$ y $\tilde{\mu} \in k[x_1,\ldots,x_n]$ tiene grado a lo sumo $\delta - 1$. Esto se puede conseguir haciendo un cambio lineal de coordenadas en el anillo de base $k[x_1,\ldots,x_n]$ como sigue: sea μ_K la componente homogénea de μ de máximo grado $K \leq sD$; este polinomio homogéneo μ_K se puede computar a partir de la matriz F por medio de un algoritmo que corre en tiempo secuencial $(Ln(N+M)D)^{O(1)}$, cuyo output es un slp de tamaño $\left((sL)^{O(1)}+n\right)(sD)^{O(1)}$ que evalúa μ_K (ver Subrutina **A**). Es suficiente exhibir un cambio lineal de coordenadas haciendo μ_K mónico en todas las variables.
Para esto, consideremos n^2 nuevas variables $(T_{ij})_{1\leq i,j\leq n}$. Sea $G := \det(T_{ij}) \prod_{j=1}^{n} \mu_K(T_{1j},\ldots,T_{nj})$; es claro que el polinomio G no es el polinomio nulo en las n^2 variables, su grado es $n(K+1) \leq n(sD+1)$ y puede ser evaluado por un slp de tamaño $(LnsD)^{O(1)}$.
Del Teorema de las correct test sequences mencionado en la sección II.1, sabemos que existe un subconjunto $Q \subseteq k^{n^2}$, de cardinal $6\left((LnsD)^{O(1)}+n^2\right)\left((LnsD)^{O(1)}+n^2+1\right) = (LnsD)^{O(1)}$, tal que, para todo polinomio H en n^2 variables de grado a lo sumo $n(sD+1)$ y dado por un slp de tamaño a lo sumo $(LnsD)^{O(1)}$, se tiene:

$$H = 0 \Leftrightarrow H(\gamma) = 0\ \ \forall \gamma \in Q.$$

Por lo tanto, fijando $\gamma = (\gamma_{11},\ldots,\gamma_{1n},\ldots,\gamma_{n1},\ldots,\gamma_{nn}) \in Q$ tales que $G(\gamma) \neq 0$, las nuevas variables $z_1,\ldots,z_n$ están definidas por medio de las siguientes relaciones:

$$x_j := \gamma_{1j}z_1 + \cdots + \gamma_{nj}z_n \quad , j = 1,\ldots,n.$$

Este cambio de variables se puede hacer en tiempo $(Ln(N+M)D)^{O(1)}$.
Más aun, si $f \in k[x_1,\ldots,x_n]$ está dado por un slp de tamaño L, su polinomio correspondiente después del cambio de coordenadas puede ser evaluado por un nuevo slp en las variables $z_1,\ldots,z_n$ de tamaño $L+n^2$.
Observemos que se puede hacer simultáneamente un cambio de coordenadas similar para una familia finita dada de matrices.

II.2 Construcción de bases del núcleo y la imagen de la matriz de una proyección

En esta sección construiremos bases para la imagen y el núcleo de la matriz de una proyección $F \in k[x_1,\ldots,x_n]^{M\times M}$ (i.e. $F^2 = F$). El enfoque que abordamos es similar al de algunos trabajos relacionados con las demostraciones de la ex-conjetura de Serre. Construiremos bases y sistemas de generadores para localizaciones convenientes del núcleo y la imagen de F, que luego pegaremos por medio del Nullstellensatz efectivo y de versiones cuantitativas del Teorema de Vaserstein. En este procedimiento será clave efectuar las localizaciones en polinomios en el anillo $k[x_1,\ldots,x_{n-1}]$ (en una variable menos) que luego serán usadas mediante argumentos recursivos, especializando la última variable en 0.
En lo que sigue denotaremos por $A := k[x_1,\ldots,x_n]$ y por $B := k[x_1,\ldots,x_{n-1}]$. La matriz $F \in k[x_1,\ldots,x_n]^{M\times M}$ será la matriz de una proyección de rango s que llamaremos la matriz de input. Las entradas de F serán polinomios de grado total acotado por D, dados por un slp de tamaño L.
Por simplicidad, suponemos que el primer menor principal μ de tamaño $s\times s$ es mónico en las variables $x_1,\ldots,x_n$. Es decir, asumimos que se ha efectuado un cambio lineal de coordenadas como en el algoritmo **H** para que esto ocurra. El costo en la complejidad y la variación de los tamaños de los slp al efectuar este cambio de coordenadas sólo se tendrán en cuenta en los teoremas principales de esta parte (Teorema 21 -construcción de bases locales- y Teorema 25 -construcción de bases globales-).

II.2.1 Un $k[x_1,\ldots,x_{n-1}]$-módulo libre relacionado con la imagen de F

Denotemos por $C_1,\ldots,C_M$ las columnas de la matriz F y sea $\mathcal{L}$ el $k[x_1,\ldots,x_n]$-módulo libre generado por las primeras s columnas $C_1,\ldots,C_s$. Consideramos la sucesión exacta

$$0 \to \mathcal{L} \to \mathrm{Im}(F) \to Q \to 0 \tag{1}$$

donde $Q := \mathrm{Im}(F)/\mathcal{L}$.
Notar que Q "mide"la diferencia entre $\mathrm{Im}(F)$ y $\mathcal{L}$. Se puede observar también que como F es una proyección, la imagen (y el núcleo) de F son sumandos directos de A^M y, por Quillen-Suslin, son A-libres; así también como B-módulos (aún si en este caso no fueran más finitamente generados).
Gracias a la regla de Cramer, dado que $C_1,\ldots,C_s$ son $k(x_1,\ldots,x_n)$-linealmente independientes y rk $F = s$, se tienen las relaciones

$$\mu C_{s+i} = b_{1i}C_1 + \ldots + b_{si}C_s \tag{2}$$

donde los b_{ji} son polinomios en A unívocamente determinados y μ es el primer menor principal de F. En particular $\mu Q = 0$. Dado que μ se supone mónico en todas las variables, Q admite una estructura de $k[x_1,\ldots,x_{n-1}]$-módulo finito generado por las clases de $x_n^k C_i$ con $k = 0,\ldots,d := \deg(\mu) - 1$, $i = s+1,\ldots,M$.
Más aun, Q es libre como lo muestra la Proposición 6.

Para la demostración necesitamos el siguiente resultado de [37, Ch. IV, Prop.3.4]:
Lema 5 *Sea $(R, \mathfrak{M})$ un anillo local y sea M un R-módulo finitamente presentable. Entonces son equivalentes:*

1. *M es libre*
2. *existe una sucesión exacta de R-módulos $0 \to K \to P \to M \to 0$ con P proyectivo tal que el morfismo inducido $K/\mathfrak{M}K \to P/\mathfrak{M}P$ es inyectivo.* ■

Ahora probamos el resultado sobre Q.

Proposición 6 *Q es un $k[x_1, \ldots, x_{n-1}]$-módulo libre de rango finito.*

Dem.- Mostramos que en cada localización de B la sucesión (1) sigue siendo exacta. Para esto alcanza con que, para todo $\wp$ ideal maximal de B, la sucesión de $B/\wp$-espacios vectoriales

$$0 \to \mathcal{L}/\wp\mathcal{L} \to \mathrm{Im}(F)/\wp\mathrm{Im}(F) \to Q/\wp Q \to 0$$

sea exacta.
Para probar nuestra afirmación es suficiente demostrar que la inyección $\mathcal{L} \to \mathrm{Im}(F)$ de la sucesión (1) se preserva después de tensorizar por $B/\wp$.
Sea $w := \alpha_1 C_1 + \ldots + \alpha_s C_s$ un elemento de $\mathcal{L} \cap \wp\mathrm{Im}(F)$. Entonces w puede escribirse como combinación lineal de las columnas $C_1, \ldots, C_M$ con coeficientes en $\wp A$. Tenemos:

$$\alpha_1 C_1 + \ldots + \alpha_s C_s = w = \beta_1 C_1 + \ldots \beta_M C_M$$

con $\alpha_j \in A$ y $\beta_i \in \wp A$. Multiplicando esta igualdad por μ y usando las relaciones que se deducen de la regla de Cramer (2), obtenemos que

$$\mu\alpha_j = \mu\beta_j + \sum_{i=1}^{M-s} \beta_{s+i} b_{ji}$$

para $j = 1, \ldots, s$, ya que $C_1, \ldots, C_s$ son linealmente independientes.
Considerando esta fórmula como una identidad polinomial en $B[x_n]$ y comparando coeficientes (recordemos que μ es mónico), observamos que los α_j pertenecen a $\wp A$ y que, entonces, $w \in \wp\mathcal{L}$. Es decir, $w = 0$ en $\mathcal{L}/\wp\mathcal{L}$.
Hemos probado la exactitud de la sucesión.
Así, $Q_{\mathcal{P}}$ resulta libre sobre $B_{\mathcal{P}}$ para cada maximal de B. Por lo tanto, Q es localmente libre como B-módulo y es finitamente generado; de aquí se deduce que Q es proyectivo. Por el Teorema de Quillen-Suslin, al ser finitamente generado, resulta que Q es un B-módulo libre de tipo finito. ■

Nuestro objetivo ahora es obtener una matriz de presentación del B-módulo Q (es decir, generadores y relaciones). Para esto construimos la aplicación siguiente:

Definición 7 *Sea* $\varphi : B^m \to Q$, *donde* $m := (d+1)(M-s)$ *definida como sigue: si* $e_{0,s+1}, e_{1,s+1}, \ldots, e_{d,s+1}, \ldots, e_{d-1,M}, e_{d,M}$ *es la base canónica de* B^m, *será* $\varphi(e_{k,i}) := \overline{x_n^k C_i}$. *(Notar que el núcleo de* φ *también es* B *- libre por Quillen-Suslin.)*

En primer lugar, construiremos un sistema de generadores para el núcleo de φ.
Sea $w_1, \ldots, w_M$ el sistema canónico de generadores de $\mathrm{Ker}(F)$. Esto es, los vectores $w_i := e_i - C_i$ con $i = 1, \ldots, M$ donde $\{e_1, \ldots, e_M\}$ es la base canónica de A^M. En particular, sus coordenadas tienen grados acotados por D.
Como μ es mónico en la variable x_n, podemos calcular la división euclidiana de cada coordenada de w_j por μ en $B[x_n]$ (siguiendo la subrutina **C**), obteniendo vectores "cociente" q_j y "resto" r_j en A^M, en tiempo $M(DsL)^{O(1)}$ de modo que

$$w_j = \mu q_j + r_j. \tag{3}$$

El grado en x_n de cada coordenada de r_j está acotado por d, mientras que su grado total está acotado por sD^2. Notar que r_j puede evaluarse por un slp en tiempo $(DsL)^{O(1)}$.
Como hay M vectores w_j, el tiempo total para calcular los q_j y los r_j es $M^2(DsL)^{O(1)}$.
Ahora, para cada $x_n^k r_j \in A^M$ con $j = 1, \ldots, M$ y $k = 0, \ldots, d$ calculamos nuevamente la división euclidiana por μ

$$x_n^k r_j = \mu q_{kj} + r_{kj} \tag{4}$$

donde $r_{kj} \in A^M$, $\deg r_{kj} = 2(sD)^3$ y $\deg_{x_n} r_{kj} \leq d$. Esto se puede computar en tiempo $M^2(DsL)^{O(1)}$ y cada coordenada se puede evaluar por un slp de tamaño $(DsL)^{O(1)}$.
Consideramos ahora, para cada vector r_{kj} el vector formado por sus últimas $M-s$ coordenadas y lo llamamos V_{kj}. Para simplificar la notación, reemplazamos el multiíndice kj por $h = 1, \ldots, M(d+1)$.
Escribiendo los vectores V_h con respecto a la variable x_n tenemos:

$$V_h = V_{h,0} + x_n V_{h,1} + \ldots + x_n^d V_{h,d}$$

donde cada $V_{h,k}$ es un vector en B^{M-s} que escribiremos

$$V_{h,k} = (V_{h,k,s+1}, \ldots, V_{h,k,M}).$$

Todos los polinomios $V_{h,k,l}$ se pueden obtener por medio de la Subrutina **A** en tiempo $M^2(DsL)^{O(1)}$ y cada uno se puede evaluar por medio de un slp de tamaño $(DsL)^{O(1)}$.
Además, se puede ver que:

Proposición 8 *Los vectores* $(V_{h,0,s+1}, V_{h,1,s+1}, \ldots, V_{h,d,s+1}, \ldots, V_{h,d-1,M}, V_{h,d,M}) \in B^{(d+1)(M-s)}$, *con* $h = 1, \ldots, M(d+1)$, *son un sistema de generadores de* $\mathrm{Ker}(\varphi)$.

Dem.- Mostremos, primero, que estos vectores pertenecen a $\mathrm{Ker}(\varphi)$.
Aplicando la definición de φ, tenemos

$$\varphi(V_{h,0,s+1}, V_{h,1,s+1}, \ldots, V_{h,d,s+1}, \ldots, V_{h,d,M}) = \sum_{i,k} V_{h,k,i}\overline{x_n^k C_i} = \sum_{i=s+1}^{M} Q_{h,i}\overline{C_i}.$$

con $Q_{h,i} := \sum_k V_{h,k,i} x_n^k$.

Es suficiente ver que $\sum_{i=s+1}^{M} Q_{h,i}C_i \in \mathcal{L}$.
Con las notaciones anteriores $V_h = (Q_{h,s+1}, \ldots, Q_{h,M})$, y entonces, volviendo atrás en las divisiones euclideanas (3) y (4), existen $P_1, \ldots, P_s \in A$ tales que :

$$(P_1, \ldots, P_s, Q_{h,s+1}, \ldots, Q_{h,M}) = x_n^t w + \mu r$$

donde $t \in \mathbb{N}$, $w \in \mathrm{Ker}(F)$ y $r \in A^M$.

Multiplicando a derecha esta identidad por el vector columna $\begin{pmatrix} C_1 \\ \vdots \\ C_M \end{pmatrix}$ (la traspuesta de F), obtenemos :

$$\sum_{i=1}^{s} P_i C_i + \sum_{i=s+1}^{M} Q_{h,i}C_i = \mu \sum_{i=1}^{M} r_i C_i,$$

ya que $w \in \mathrm{Ker}(F)$.
Como $\mu C_i \in \mathcal{L}$ para todo $i = 1, \ldots, M$, se deduce que $\sum_i Q_{h,i}C_i \in \mathcal{L}$, y, por lo tanto, los vectores están en $\mathrm{Ker}(\varphi)$.

Ahora, mostraremos que son un sistema de generadores de $\mathrm{Ker}(\varphi)$.
Sea $(q_{0,s+1}, q_{1,s+1}, \ldots, q_{d,M})$ un elemento en $\mathrm{Ker}(\varphi) \subset B^{(d+1)(M-s)}$; es decir que

$$q_{0,s+1}C_{s+1} + q_{1,s+1}x_n C_{s+1} + \ldots + q_{d,M}x_n^d C_M \in \mathcal{L}.$$

Escribiendo $Q_i := \sum_k q_{k,i}x_n^k$, para $i = s+1, \ldots, M$, sabemos que existen $P_1, \ldots, P_s \in A$ tales que

$$Q_{s+1}C_{s+1} + \cdots + Q_M C_M = P_1 C_1 + \cdots + P_s C_s.$$

Esto quiere decir que el vector $(-P_1, \ldots, -P_s, Q_{s+1}, \ldots, Q_M) \in A^M$ pertenece a $\mathrm{Ker}(F)$, y entonces, si $\{w_1, \ldots, w_M\}$ es un sistema de generadores de $\mathrm{Ker}(F)$ (por ejemplo el canónico, recordando que F es una proyección), existen $\alpha_1, \ldots \alpha_M \in A$ tales que

$$(-P_1, \ldots, -P_s, Q_{s+1}, \ldots, Q_M) = \sum \alpha_j w_j.$$

Dividiendo los polinomios α_j y los w_j por μ, podemos escribir, para un cierto $w \in A^M$

$$(-P_1, \ldots, -P_s, Q_{s+1}, \ldots, Q_M) = \mu w + \sum \beta_j r_j$$

donde $\deg_{x_n} \beta_j \leq d$ y los r_j son los definidos en (3).
Repitiendo la división (4) obtenemos

$$(-P_1, \ldots, -P_s, Q_{s+1}, \ldots, Q_M) = \mu w' + \sum \beta_{kj} r_{kj}$$

con $\beta_{kj} \in B$.
Comparando las últimas $M - s$ coordenadas, y simplificando la notación, tenemos que

$$(Q_{s+1}, \ldots, Q_M) = \mu v + \sum \beta_h V_h$$

para cierto $v \in A^{M-s}$.
Como $\beta_h \in B$ para todo índice h y como $\deg_{x_n} Q_i$ y $\deg_{x_n} V_h$ son estrictamente menores que $\deg_{x_n} \mu$, obtenemos que v es cero por la unicidad en el algoritmo de Euclides en el anillo $B[x_n]$. Entonces

$$(Q_{s+1}, \ldots, Q_M) \in BV_1 + \cdots + BV_{M(d+1)}.$$

La demostración termina desarrollando esta identidad en potencias de x_n. ■

Resumiendo los últimos resultados, obtenemos que:

Proposición 9 *Existe un sistema de generadores de $Ker(\varphi)$ que se puede construir a partir de la matriz de input F por medio de un algoritmo con tiempo de complejidad $(MDL)^{O(1)}$. Los coeficientes de los vectores pueden evaluarse mediante un slp de tamaño $(DsL)^{O(1)}$.*

Podemos reenunciar lo obtenido en términos de matrices como sigue:

Lema 10 *Existe una matriz $G \in B^{m \times p}$ donde $m := (M-s)(d+1)$, $p := M(d+1)$ y $\deg(G) \leq 2(sD)^3$ tal que $\mathrm{Im}(G) = Ker(\varphi)$. Esta matriz se puede computar a partir de la matriz de input F en tiempo secuencial $(MDL)^{O(1)}$. Las entradas de G se pueden evaluar mediante un slp de tamaño $(DsL)^{O(1)}$.*

Dem.- Basta tomar G como la matriz cuyas columnas son los vectores $(V_{h,0,s+1}, V_{h,1,s+1}, \ldots, V_{h,d.s+1}, \ldots, V_{h,d,M})$, para $h = 1, \ldots, p$. ■

En otras palabras, hemos encontrado una matriz cuya traspuesta es una presentación del B-módulo Q. Usaremos esta presentación más adelante para calcular presentaciones locales del A-módulo $\mathrm{Im}(F)$.

II.2.2 Una presentación para la imagen localizada de F

Usando argumentos elementales basados en la regla de Cramer y en el Lema de Nakayama, es posible exhibir bases de la imagen y del núcleo de F bajo ciertas localizaciones en polinomios convenientes en A. Lamentablemente, no sabemos cómo pegar esas bases locales para obtener una base global. El principal obstáculo para esto parece ser el hecho de que los polinomios en los que se localiza están en $k[x_1, \ldots, x_n]$ y no en $k[x_1, \ldots, x_{n-1}]$. Para evitar este problema, mostraremos presentaciones alternativas para la imagen de F bajo localizaciones de polinomios en B, para poder, allí, aplicar métodos recursivos inspirados en resultados de Vaserstein .
Recordamos las notaciones usadas hasta aquí. Denotamos por s al rango de la matriz de la proyección F y por $\mu \in A$ al primer menor principal de tamaño $s \times s$. Luego del cambio de coordenadas de la subrutina **H**, μ es un polinomio mónico en todas las variables. Sean $d := \deg \mu - 1$ y $m := (d+1)(M-s)$.

Sea $\varphi : B^m \to Q := \mathrm{Im}(F)/\mathcal{L}$ la aplicación B-lineal definida en la base canónica por $\varphi(e_{ki}) := \overline{x_n^k C_i}$, para $k = 0, \ldots, d$ y $i = s+1, \ldots, M$ (donde $\mathcal{L}$ es el A-módulo libre generado por las primeras s columnas de F, denotadas por $C_1, \ldots, C_s$) (ver Definición 7).
Sea $G \in B^{m \times p}$ la matriz construida en la sección anterior, cuyas columnas son un sistema de generadores del núcleo de φ y sea $q \leq m$ el rango del B-módulo libre $\mathrm{Ker}(\varphi)$. Los menores de G tamaño $q \times q$ generan el anillo B ya que $\mathrm{Im}(G) = \mathrm{Ker}(\varphi)$ es un sumando directo de B^m. Sus grados están acotados por $2q(sD)^3 \leq 2(M-s)(sD)^4$. Más aun, podemos calcular un número admisible (i.e. simplemente exponencial) de ellos, usando el procedimiento para eliminar menores superfluos y obtenemos:

Lema 11 *Es posible construir menores $\xi_1, \ldots, \xi_\ell$ de tamaño $q \times q$ de la matriz G tales que:*

- $1 \in (\xi_1, \ldots, \xi_\ell)$,
- $\ell \leq ((m+p)^6 2(sD)^3)^{n-1} = (MD)^{O(n)}$,
- $deg\ (\xi_i) \leq 2q(sD)^3$.

Esto se puede hacer con la matriz F como input en tiempo secuencial $(nL)^{O(1)}(MD)^{O(n)}$ y cada menor ξ_i se puede evaluar por medio de un slp de tamaño $(qsDL)^{O(1)} = (MLD)^{O(1)}$. ■

Desgraciadamente, a pesar de que los polinomios $\xi_1, \ldots, \xi_\ell$ generan el anillo de polinomios B, no sabemos cómo construir una base para el A_ξ-módulo localizado $\mathrm{Im}(F_\xi)$ y necesitaremos refinarlos mediante multiplicaciones convenientes.
Fijemos un menor ξ entre los menores de tamaño $q \times q$ construidos en el lema previo. Sin pérdida de generalidad supondremos que ξ involucra las primeras q columnas de G, las que denotaremos por $K_1, \ldots, K_q$ (recordar que $\varphi(K_1) = \ldots = \varphi(K_q) = 0$).
De las $m-q$ filas que no fueron usadas en la construcción del menor ξ, sean $e_{k_1,i_1}, \ldots, e_{k_{m-q},i_{m-q}}$ los correspondientes $m-q$ vectores de la base canónica de B^m. Por simplicidad, denotaremos los vectores e_{k_j,i_j} por u_j para $j = 1, \ldots, m-q$.
Es claro que de este modo $\{K_1, \ldots, K_q, u_1, \ldots, u_{m-q}\}$ es una base de B_ξ^m ya que el determinante de la matriz Z de tamaño $m \times m$ correspondiente es ξ ó $-\xi$. Observemos que la matriz Z puede construirse directamente a partir de la matriz G. Entonces, tenemos

Proposición 12 *Los vectores $\varphi(e_{kj,ij}) = \overline{x_n^{k_j} C_{i_j}}$ con $j = 1, \ldots, m-q$ forman una base del B_ξ-módulo Q_ξ.* ■

La definición que sigue nos permitirá mostrar una nueva presentación local para la imagen de F que nos servirá luego.

Definición 13 *Sea $\psi : A^{m-q+s} \to \mathrm{Im}(F)$ la aplicación lineal definida por:*

- $\psi(e_j) = x_n^{k_j} C_{i_j}$ *para* $j = 1, \ldots, m-q$
- $\psi(e_j) = C_{j-m+q}$ *para* $j = m-q+1, \ldots, m-q+s$.

Observar que ψ depende de la elección del menor ξ.

Notar que, por la proposición anterior y la definición de Q (ver sucesión exacta (1)), la localización ψ_ξ del morfismo ψ, resulta suryectiva y que, por lo tanto, $\mathrm{Ker}(\psi_\xi)$ es un A_ξ-módulo proyectivo porque $\mathrm{Im}(F_\xi)$ es A_ξ-libre. (De hecho en la Proposición 16 mostraremos que más aun, es libre).

Ahora, vamos a estudiar más en detalle la estructura del morfismo ψ_ξ. Estudiaremos, en primer lugar, el núcleo de este morfismo.
Consideremos los vectores $x_n^{k_1}C_{i_1},\ldots,x_n^{k_{m-q}}C_{i_{m-q}},\ C_1,\ldots,\ C_s$.
De la Proposición 12 y de la definición del B-módulo Q, sabemos que, para cada índice ℓ , $\ell=1,\ldots,m-q$, existen únicos $\widetilde{\beta}_1^{(\ell)},\ldots,\widetilde{\beta}_{m-q}^{(\ell)}\in B_\xi$ y $\widetilde{\alpha}_1^{(\ell)},\ldots,\widetilde{\alpha}_s^{(\ell)}\in A_\xi$ tales que

$$-x_n\,x_n^{k_\ell}C_{i_\ell}=\sum_{j=1}^{m-q}\widetilde{\beta}_j^{(\ell)}\,x_n^{k_j}C_{i_j}+\sum_{i=1}^{s}\widetilde{\alpha}_i^{(\ell)}C_i. \tag{5}$$

En los resultados que siguen nos dedicaremos a describir con más precisión las fracciones $\widetilde{\beta}_j^{(\ell)}$ y $\widetilde{\alpha}_i^{(\ell)}$.

Proposición 14 *Existen polinomios $\beta_j^{(\ell)}\in B$, $j=1,\ldots,m-q$, con grados totales acotados por $2(M-s)(sD)^4$ tales que, para cada índice j se tiene*

$$\widetilde{\beta}_j^{(\ell)}=\frac{\beta_j^{(\ell)}}{\xi}\,.$$

Estos polinomios se pueden construir a partir de la matriz de input F por medio de un algoritmo que corre en tiempo secuencial $(nL)^{O(1)}(MD)^{O(n)}$ y pueden ser evaluados por uns slp de tamaño $(LMD)^{O(1)}$.

Dem.- Supongamos primero que $k_\ell<d$. Tenemos entonces que $-\overline{x_n^{1+k_\ell}C_{i_\ell}}=-\varphi(e)$ para un cierto vector e de la base canónica de B^m (ver Definición 7).
Por otro lado, podemos escribir unívocamente en B_ξ^m:

$$-e=\lambda_1K_1+\cdots+\lambda_qK_q+\lambda_{q+1}u_1+\cdots+\lambda_mu_{m-q}=Z\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_m\end{pmatrix} \tag{6}$$

y, por lo tanto, $\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_m\end{pmatrix}=-Z^{-1}e\in B_\xi^m$.
De este modo, aplicando φ obtenemos

$$-x_n\varphi(u_\ell)=-\overline{x_n^{1+k_\ell}C_{i_\ell}}=-\varphi(e)=\sum_{j=1}^{m-q}\lambda_{q+j}\varphi(u_j)$$

(recordar que $\varphi(K_l)=0$ para todo l y que $\varphi(u_j)=\overline{x_n^{k_j}C_{i_j}}$).

Así en (5) tenemos que $\widetilde{\beta}_j^{(\ell)} := \lambda_{q+j}$, para todo $j = 1, \ldots, m-q$.
En particular, los λ_{q+j} son los últimos $m-q$ coeficientes de la matriz columna $-Z^{-1}e$.
Como Z pertenece a $B^{m\times m}$ y $\det(Z) = \pm\xi$ podemos escribir

$$\widetilde{\beta}_j^{(\ell)} = \frac{\beta_j^{(\ell)}}{\xi} \tag{7}$$

donde los $\beta_j^{(\ell)}$ pueden calcularse como determinantes de matrices apropiadas en $B^{m\times m}$ (mediante la regla de Cramer y la subrutina **B**). Tomando en cuenta el tiempo de complejidad para construir la matriz Z, los polinomios $\beta_j^{(\ell)}$ pueden computarse en tiempo $(nL)^{O(1)}(MD)^{O(n)}$ y se pueden evaluar por un slp de tamaño $(LMD)^{O(1)}$.
Para el caso $k_\ell = d$, en lugar de $-x_n^{1+k_\ell}C_{i_\ell}$, podemos escribir $(x_n^{d+1} - \mu)C_{i_\ell}$ (ya que sus clases son iguales en Q) y la construcción se desarrolla de manera similar.
Las cotas de grado para los polinomios $\beta_j^{(\ell)}$ se siguen de manera directa. ■

Veremos en la proposición siguiente un estudio similar para los polinomios $\alpha_j^{(\ell)}$:

Proposición 15 *Existen polinomios $\alpha_j^{(\ell)} \in A$, $j = 1, \ldots, m-q$, con grados totales acotados por $4(M-s)(sD)^4$, tales que para cada índice j tenemos*

$$\widetilde{\alpha}_j^{(\ell)} = \frac{\alpha_j^{(\ell)}}{\xi}\,.$$

Estos polinomios se pueden construir a partir de la matriz de input F mediante un algoritmo que corre en tiempo secuencial $(nL)^{O(1)}(MD)^{O(n)}$ y pueden ser evaluados por un slp de tamaño $(MLD)^{O(1)}$.

Dem.- En primer lugar, mostremos que $\xi\widetilde{\alpha}_j^{(\ell)}$ pertenece a A.
Reescribiendo la fórmula (5) y usando la proposición anterior, existen $Q_1, \ldots, Q_{M-s} \in B_\xi[x_n]$ tales que vale la igualdad

$$Q_1C_{s+1} + \cdots + Q_{M-s}C_M = \sum_{i=1}^{s} \widetilde{\alpha}_i^{(\ell)}C_i$$

en A_ξ^M y que ξQ_l son polinomios en A de grados acotados por $d + 4(M-s)(sD)^4$ para todo $l = 1, \ldots, M-s$.
Por otro lado, como las primeras s columnas de F son linealmente independientes y el rango de F es s, los vectores columna $\mu C_{s+1}, \ldots, \mu C_M$ se pueden escribir como combinaciones A-lineales de las columnas $C_1, \ldots, C_s$, mediante la regla de Cramer, es decir,

$$C_{s+l} = \sum_{r=1}^{s} \frac{b_{rl}}{\mu}C_r\,, \tag{8}$$

para ciertos $b_{rl} \in A$, con $1 \le r \le s$ y $1 \le l \le M-s$.

Entonces, tenemos,

$$Q_1 C_{s+1} + \cdots + Q_{M-s} C_M = Q_1 \sum_{r=1}^{s} \frac{b_{r1}}{\mu} C_r + \cdots + Q_{M-s} \sum_{r=1}^{s} \frac{b_{r\,M-s}}{\mu} C_r.$$

Como $C_1, \ldots, C_s$ son $k(x_1, \ldots, x_n)$-linealmente independientes deducimos que

$$\widetilde{\alpha}_i^{(\ell)} = \frac{\sum_{l=1}^{M-s} b_{il} Q_l}{\mu},$$

para todo $i = 1, \ldots, s$.
Sea h el mínimo exponente tal que $\xi^h \widetilde{\alpha}_i^{(\ell)} \in A$ (h existe porque $\widetilde{\alpha}_i^{(\ell)} \in A_\xi$). Como $\xi Q_l \in A$ para todo l, y los polinomios μ y ξ son coprimos (porque μ es mónico en todas las variables y ξ pertenece a B), deducimos que $h \leq 1$, y entonces

$$\xi \widetilde{\alpha}_i^{(\ell)} \in A \quad \text{y} \quad \mu \text{ divide a } \xi \sum_{l=1}^{M-s} b_{il} Q_l \text{ en} A. \tag{9}$$

De esta manera, para construir los polinomios $\alpha_i^{(\ell)} := \xi \widetilde{\alpha}_i^{(\ell)}$ procedemos como sigue:

- Reescribiendo $-\xi\, x_n^{k_\ell + 1} C_{i_\ell} - \sum_{j=1}^{m-q} \beta_j^{(\ell)}\, x_n^{k_j} C_{i_j}$ como una combinación $A-$lineal de las últimas columnas $C_{s+1}, \ldots, C_M$ obtenemos los polinomios $\xi Q_1, \ldots, \xi Q_{M-s}$ en A; estos polinomios pueden evaluarse mediante un slp de tamaño $(DLM)^{O(1)}$ y sus grados están acotados por $2\,(M-s)\,(sD)^4 + sD - 1$.

- Reescribiendo $\mu C_{s+1}, \ldots, \mu C_M$ en términos de las primeras columnas $C_1, \ldots, C_s$ como en la relación (8), usando la regla de Cramer y la subrutina **B**, obtenemos los polinomios $b_{il} \in A, 1 \leq i \leq s, 1 \leq l \leq M - s$ de grados acotados por sD; estos polinomios pueden ser evaluados por un slp de tamaño $(sL)^{O(1)}$.

- De los ítems previos calculamos $\sum_{l=1}^{M-s} b_{il} \xi Q_l$ y luego obtenemos $\mu \alpha_j^{(\ell)}$. Siguiendo las estimaciones anteriores estos polinomios pueden evaluarse mediante un slp de tamaño $(DLM)^{O(1)}$ y sus grados están acotados por $2\,(M-s)\,(sD)^4 + 2sD - 2$.

- Finalmente, para obtener $\alpha_j^{(\ell)}$ efectuamos la división euclideana de $\mu \alpha_j^{(\ell)}$ por μ con respecto a x_n como en la subrutina **C** (recordar que μ es mónico en todas las variables).

El tiempo de complejidad de este procedimiento depende esencialmente de la construcción de los polinomios $\beta_j^{(\ell)}$ y por lo tanto es del mismo orden que el establecido en la proposición previa. ■

Más aun, a partir de las construcciones anteriores podemos conseguir una base del núcleo de ψ_ξ (ver Definición (13)) como sigue:

Proposición 16 *Sea* $U \in A_\xi^{(m-q)\times(m-q+s)}$ *la matriz cuya* ℓ*-ésima fila es el vector*

$$(\frac{\beta_1^{(\ell)}}{\xi},\ldots,\frac{\beta_{m-q}^{(\ell)}}{\xi},\frac{\alpha_1^{(\ell)}}{\xi},\ldots,\frac{\alpha_s^{(\ell)}}{\xi}) + x_n e_\ell$$

(e_ℓ *es el* ℓ*-ésimo vector de la base canónica de* A^{m-q+s}*). Entonces* U *es una matriz unimodular en* A_ξ *(i.e. los menores de tamaño* $(m-q)\times(m-q)$ *generan el anillo* A_ξ*) y sus filas son una base de* $\mathrm{Ker}\,(\psi_\xi)$ *(en particular* $\mathrm{Ker}\,(\psi_\xi)$ *resulta libre).*
La matriz $\xi U \in A^{(m-q)\times(m-q+s)}$ *puede ser computada a partir de la matriz de input* F *por un algoritmo que corre en tiempo secuencial* $(nL)^{O(1)}\,(MD)^{O(n)}$*. Más aun, cada entrada de* ξU *se puede evaluar por un slp de tamaño* $(LMD)^{O(1)}$ *y* $\deg \xi U \leq 4(M-s)(sD)^4$*.*

Dem.- Sea $S \subset A_\xi^{m-q+s}$ el submódulo generado por las filas de la matriz U. De la relación (5) y de las Proposiciones 14 y 15 se deduce que $S \subset \mathrm{Ker}(\psi_\xi)$.
Para ver la otra inclusión, observemos que para todo $\ell = 1,\ldots,m-q$ y para todo $p \in A_\xi$ existen $\gamma_1,\ldots,\gamma_{m-q} \in B_\xi$ y $\gamma_{m-q+1},\ldots,\gamma_{m-q+s} \in A_\xi$ (que dependen de ℓ y de p) tales que

$$pe_\ell - \sum_{j=1}^{m-q+s} \gamma_j e_j \in S.$$

(Esto se puede hacer directamente mediante un argumento recursivo, desarrollando p en potencias de la variable x_n.)
Así si $(p_1,\ldots,p_{m-q+s}) \in \mathrm{Ker}(\psi_\xi)$ podemos reescribirlo de la siguiente manera

$$(p_1,\ldots,p_{m-q+s}) = w + \sum_{j=1}^{m-q+s} \gamma_j e_j$$

donde $w \in S$, $\gamma_1,\ldots,\gamma_{m-q} \in B_\xi$ y $\gamma_{m-q+1},\ldots,\gamma_{m-q+s} \in A_\xi$.
Aplicando ψ obtenemos la siguiente identidad en $\mathrm{Im}(F_\xi)$:

$$0 = \sum_{j=1}^{m-q} \gamma_j\, x_n^{k_j} C_{i_j} + \sum_{j=m-q+1}^{m-q+s} \gamma_j C_{j-m+q}. \qquad (10)$$

Analizamos esta igualdad, módulo el A_ξ-módulo libre $\mathcal{L}_\xi$ generado por las columnas $C_1,\ldots,C_s$ (ver (1) en la subsección II.2.1). De allí se deduce la relación en Q_ξ :

$$0 = \sum_{j=1}^{m-q} \gamma_j\, \overline{x_n^{k_j} C_{i_j}},$$

y, como los elementos $\overline{x_n^{k_j} C_{i_j}}$, $j = 1,\ldots,m-q$, son una B_ξ-base de Q_ξ (ver Proposición 12), tenemos $\gamma_j = 0$ para $j = 1,\ldots,m-q$.
De este modo la combinación lineal (10) se puede reducir a

$$0 = \sum_{j=m-q+1}^{m-q+s} \gamma_j C_{j-m+q}.$$

Como los vectores columna $C_1, \ldots, C_s$ son $k(x_1, \ldots, x_n)$-linealmente independientes tenemos también que $\gamma_j = 0$ para $j = m-q+1, \ldots, m-q+s$. Entonces $(p_1, \ldots, p_{m-q+s}) \in S$ y, por lo tanto, $S = \mathrm{Ker}(\psi_\xi)$.
Más aun, las filas de la matriz U son una A_ξ-base de $\mathrm{Ker}(\psi_\xi)$: $\mathrm{Im}(F_\xi)$ es A_ξ-libre de rango s con lo que $\mathrm{Ker}(\psi_\xi)$ es localmente libre de rango $m-q$; como acabamos de ver que las filas de la matriz U generan $\mathrm{Ker}(\psi_\xi)$, por el Lema de Nakayama, son una base de la localización en cada ideal maximal de A_ξ y, por ello, son A_ξ-linealmente independientes. La unimodularidad de la matriz U se sigue de la descomposición $A_\xi^{m-q+s} \simeq \mathrm{Ker}(\psi_\xi) \oplus \mathrm{Im}(F_\xi)$. Las estimaciones de complejidad se siguen de las Proposiciones 14 y 15. ■

Observemos que la matriz U corresponde a una presentación del A_ξ-módulo $\mathrm{Im}(\psi_\xi)$.

II.2.3 Construcción de bases locales para la imagen de F

El resultado principal de esta parte nos permitirá construir polinomios apropiados en B para poder obtener bases para localizaciones de $\mathrm{Im}(F)$ mediante cambios de coordenadas convenientes en $A_\xi^{(m-q+s)}$.
Por simplicidad, siguiendo las notaciones de las Proposiciones 14 y 15, denotaremos por $[\beta] := \left(\beta_j^{(\ell)}\right)_{j,\ell} \in B^{(m-q)\times(m-q)}$ y por $[\alpha] := \left(\alpha_j^{(\ell)}\right)_{j,\ell} \in A^{(m-q)\times s}$.
Siguiendo [37, Ch.IV, Lemma 3.12], podremos hacer una primera simplificación de la matriz U introducida en la Proposición 16: se trata de usar división con resto entre la matriz $\frac{1}{\xi}[\alpha]$ (formada por las últimas s columnas de U) y la matriz $x_n \mathrm{Id}_{m-q} + \frac{1}{\xi}[\beta]$ (consistente de las primeras $m-q$ columnas de U) mirando los polinomios con respecto a la variable x_n en la manera obvia:

Proposición 17 *Existe una matriz $C \in A^{(m-q+s)\times(m-q+s)}$ cuyo determinante es una potencia de ξ (por lo tanto C es inversible como matriz en $A_\xi^{(m-q+s)\times(m-q+s)}$) y matrices $U_1 \in A^{(m-q)\times(m-q)}, U_2 \in B^{(m-q)\times s}$, que satisfacen los siguientes ítems:*

- $UC = (U_1 \mid U_2)$.
- $U_1 = \xi x_n \mathrm{Id}_{m-q} + [\beta]$.
- *C, U_1 y U_2 se pueden obtener a partir de la matriz de input F mediante un algoritmo que corre en tiempo secuencial $(nL)^{O(1)}(MD)^{O(n)}$.*
- *Las entradas de las matrices C, U_1 y U_2 se pueden evaluar mediante un slp de tamaño $(MLD)^{O(1)}$.*
- *Los grados de las entradas de las matrices C y U_2 están acotados por $(MD)^{O(1)}$ y los de U_1 por $2(M-s)(sD)^4$.*

Dem.- Sea $t := 4(M-s)(sD)^4$ la cota superior para los grados totales de las entradas de la matriz $[\alpha]$. Del algoritmo de división de Euclides, sabemos que existen únicas matrices $q_0, \ldots, q_{t-1}, r \in B^{(m-q)\times s}$ de modo que se verifica la siguiente fórmula:

$$\xi^t [\alpha] = (\xi x_n \mathrm{Id}_{m-q} + [\beta]) \left(q_{t-1} x_n^{t-1} + \cdots + q_0\right) + r. \tag{11}$$

Los coeficientes de las columnas de las matrices $q_0, \ldots, q_{t-1}, r$ son las soluciones de s sistemas de ecuaciones lineales de tamaño $(t+1) \times (m-q)$ sobre el anillo B que tienen la misma matriz asociada:

$$\begin{pmatrix} \xi \mathrm{Id}_{(m-q)} & 0 & & & 0 \\ [\beta] & \xi \mathrm{Id}_{(m-q)} & & & \\ 0 & & & & \\ \vdots & & [\beta] & \xi \mathrm{Id}_{(m-q)} & 0 \\ 0 & & 0 & [\beta] & \mathrm{Id}_{(m-q)} \end{pmatrix}.$$

La parte no homogénea de cada sistema está formada por las columnas de las matrices $\xi^t a_t, \ldots, \xi^t a_0$, donde $[\alpha] = x_n^t a_t + \cdots + a_0$ (cada a_i es una matriz en $B^{(m-q)\times s}$); estas entradas pueden computarse interpolando con respecto a x_n los coeficientes de $[\alpha]$ (ver Subrutina **A** o [48, Prop. 3.11]). Esto se puede hacer a partir de la matriz de input F mediante un algoritmo que corre en tiempo secuencial $(nL)^{O(1)}(MD)^{O(n)}$ y que evalúa cada entrada con un slp de tamaño $(MLD)^{O(1)}$.
Como el determinante del sistema es igual a $\xi^{(m-q)t}$, usando la regla de Cramer sin divisiones, obtenemos (sólo computando determinantes) las entradas de las matrices que no conocemos $\xi^{(m-q)t} q_{t-1}, \ldots, \xi^{(m-q)t} r$ con las mismas cotas de complejidad que arriba.
Resumiendo, hemos construido dos matrices polinomiales $Q \in A^{(m-q)\times s}$ y $R \in B^{(m-q)\times s}$ tales que

$$\xi^{(m-q)t+t+1} \frac{[\alpha]}{\xi} = \left(x_n \mathrm{Id}_{m-q} + \frac{[\beta]}{\xi} \right) Q + R$$

(donde $Q := x_n^{t-1} \xi^{(m-q)t+1} q_{t-1} + \cdots + \xi^{(m-q)t+1} q_0$ y $R := \xi^{(m-q)t} r$).
A partir de éstas construimos la matriz

$$C := \begin{pmatrix} \xi \mathrm{Id}_{m-q} & -Q \\ 0 & \xi^{(m-q)t+t+1} \mathrm{Id}_s \end{pmatrix}$$

que verifica lo pedido. ■

La matriz U puede modificarse mediante otro cambio lineal de coordenadas para obtener así una matriz con entradas en localizaciones convenientes de B para poder pasar a una matriz equivalente poniendo $x_n \mapsto 0$. Para esto es útil considerar la matriz UC de la Proposición 17 como una matriz unimodular en $k(x_1, \ldots, x_{n-1})[x_n]$ para poder aplicar el procedimiento de reducción de Suslin siguiendo [40] y [9]. Desafortunadamente, para seguir esta estrategia necesitamos construir nuevos polinomios en B que jueguen el rol de los ξ's. Sobre esto tratan los siguientes dos lemas.

Lema 18 *Sea $V := UC$ donde U y C son las matrices definidas en las proposiciones 16 y 17 respectivamente. Existen matrices inversibles $\Lambda_1, \ldots, \Lambda_T \in k^{(m-q+s)\times(m-q+s)}$, con $T = ((M-s)sD)^{O(1)}$, tales que: si $V^{(i)} := V\Lambda_i, \Delta_1^{(i)} := \det\left[V_1^{(i)}, \ldots, V_{m-q}^{(i)}\right]$ (el menor de tamaño $(m-q) \times (m-q)$ construido a partir de las primeras $m-q$ columnas de $V^{(i)}$), $\Delta_2^{(i)} := \det\left[V_1^{(i)}, \ldots, V_{m-q-1}^{(i)}, V_{m-q+1}^{(i)}\right]$ y $c_i := Res_{x_n}\left(\Delta_1^{(i)}, \Delta_2^{(i)}\right)$ (la resultante de*

$\Delta_1^{(i)}, \Delta_2^{(i)}$ *con respecto a la indeterminada* x_n*), entonces para cada* $z \in \mathbb{A}^{n-1}\backslash\{\xi = 0\}$, *existe un índice* i, $1 \leq i \leq T$, *tal que* $c_i(z) \neq 0$ *(en otras palabras, los polinomios* $c_1, \ldots, c_T$ *generan el anillo* B_ξ*).*
Más aun, estos polinomios, cuyos grados están acotados por $(MD)^{O(1)}$, *se pueden construir a partir de la matriz de input* F *mediante un algoritmo que corre en tiempo secuencial* $(nL)^{O(1)}(MD)^{O(n)}$ *y se pueden evaluar por un slp de tamaño* $(MLD)^{O(1)}$.

Dem.- Mostraremos que para cada $z \in \mathbb{A}^{n-1}\backslash\{\xi = 0\}$ existe una matriz Λ (que depende de z) tal que $Res_{x_n}(\Delta_1, \Delta_2)(z) \neq 0$. Siguiendo esencialmente la demostración de ese resultado, podremos exhibir un procedimiento para encontrar un número finito de matrices Λ y luego un número finito de resultantes que generen B_ξ. La clave para la obtención de esta familia finita es la introducción de correct test sequences como las señaladas en [43, Theorem 26].
Introducimos $(m-q+s)^2$ nuevas indeterminadas sobre k que denotaremos por y_{lj}, $1 \leq l, j \leq (m-q+s)$ y sea Y la matriz cuadrada de tamaño $(m-q+s)\times(m-q+s)$ cuyas entradas son las variables y_{lj}.
Sea z_0 un punto arbitrario (pero fijo) en $\mathbb{A}^{n-1}\backslash\{\xi = 0\}$ y sea $P_{z_0} \in k[y_{lj}]$ el polinomio $Res_{x_n}(\Delta_1, \Delta_2)\det(Y)$, donde $\Delta_1 := \det\left[V_1', \ldots, V_{m-q}'\right]$ es el menor de tamaño $(m-q)\times(m-q)$ construido a partir de las primeras $m-q$ columnas de $V' := V(z_0, x_n)Y$ y $\Delta_2 := \det\left[V_1', \ldots, V_{m-q-1}', V_{m-q+1}'\right]$ es construido análogamente.
Afirmación.- El polinomio P_{z_0} no es el polinomio nulo.
Prueba de la afirmación: Nos conviene reescribir el polinomio P_{z_0} haciendo uso de la conocida fórmula de Binet-Cauchy (ver, por ejemplo, [21, Ch.2]). Tenemos:

$$\Delta_1 := \det[V_1', \ldots, V_{m-q}'] = \sum_I \det(V_I)\det(({}^tY')_I) \tag{12}$$

$$\Delta_2 := \det[V_1', \ldots, V_{m-q-1}', V_{m-q+1}'] = \sum_I \det(V_I)\det(({}^tY'')_I)$$

donde I recorre todas las sucesiones $(i_1, \ldots, i_{m-q})$ tales que $1 \leq i_1 < \cdots < i_{m-q} \leq m-q+s$ y escribimos Y' e Y'' para las matrices de tamaño $(m-q+s)\times(m-q)$, $[Y_1, \ldots, Y_{m-q}]$ y $[Y_1, \ldots, Y_{m-q-1}, Y_{m-q+1}]$ respectivamente.
De la Proposición 17 se deduce inmediatamente que: $m-q = \deg_{x_n}(\det[V_1, \ldots, V_{m-q}]) > \deg_{x_n}(\det(V_I))$ para todas las sucesiones de números naturales $I = (i_1, \ldots, i_{m-q})$ con $1 \leq i_1 < \cdots < i_{m-q} \leq m-q+s$ y $I \neq (1, \ldots, m-q)$. Notar que, además, $z_0 \in \mathbb{A}^{n-1}\backslash\{\xi = 0\}$ y que los coeficientes de $\det(V_1, \ldots, V_{m-q})$ con respecto a x_n no se anulan al evaluar en z_0.
Así, observando la fórmula 12, se deduce que $P_{z_0}(Y) = \mathrm{Res}_{x_n}(\Delta_1(z_0, x_n, Y'), \Delta_2(z_0, x_n, Y''))$.
Supongamos ahora que $P_{z_0}(Y) = 0$. Entonces existe $p \in \bar{k}[x_n, Y]$ con $\deg_{x_n}(p) \geq 1$ tal que p divide a ambos $\Delta_1(z_0, x_n, Y')$ y $\Delta_2(z_0, x_n, Y'')$. En particular tenemos que $p \in \bar{k}[x_n, Y_1, \ldots, Y_{m-q-1}]$. Sea $h \in \bar{k}[x_n, Y']$ tal que

$$ph = \Delta_1 = \sum_I \det(V_I(z_0, x_n))\det(({}^tY')_I). \tag{13}$$

Sea $\mathcal{I} \subset \bar{k}[x_n][Y']$ el ideal generado por todos los determinantes $\det(({}^tY')_I)$; $\mathcal{I}$ es un ideal primo homogéneo (ver [7, Ch.2, Th.2.10]). De (13) vemos que p y h deben ser homogéneos en Y' y que $\deg_{Y'}(p) + \deg_{Y'}(h) = m - q$. El polinomio p no pertenece al ideal $\mathcal{I}$ dado que es independiente de Y_{m-q}.
Como $\Delta_1 \in \mathcal{I}$ por (13) y $\mathcal{I}$ es primo concluimos que $h \in \mathcal{I}$ y que $\deg_{Y'}(h) \geq m - q$. De este modo, $\deg_{Y'}(p) = 0$, i.e. $p \in \bar{k}[x_n]$. Ahora, nuevamente, en virtud de (13), se tiene que p divide a todos los $\det(V_I(z_0, x_n))$.
El hecho de que V es unimodular (Proposiciones 16 y 17) implica que el ideal generado por todos los polinomios $\det(V_I(z_0, x_n))$ es trivial en $k[x_n]$. Por lo tanto, $p \in \bar{k}$, lo que contradice que $\deg_{x_n}(p) \geq 1$. Esto finaliza la prueba de la afirmación.

Por otra parte, notar que P_{z_0} tiene grado acotado por $(m - q + s)^2$ y puede ser evaluado por un slp de tamaño $\lambda := (m - q + s)^{O(1)}$. Es claro que estas estimaciones no dependen del punto z_0, y entonces, si z_0 recorre todos los puntos en $\mathbb{A}^{n-1} \setminus \{\xi = 0\}$, obtenemos una familia infinita $\mathcal{F}$ de polinomios en $k[y_{lj}]$ con las mismas cotas superiores para sus grados y para los tamaños de los slp que los evalúan.
Así (ver Subsección II.1 o [33]), existe una correct test sequence para $\mathcal{F}$, digamos $\gamma_1, \ldots, \gamma_T \in k^{(m-q+s)^2}$, donde $T := 6\left(\lambda + (m - q + s)^2\right)\left(\lambda + (m - q + s)^2 + 1\right)$; en otras palabras para cada $z \in \mathbb{A}^{n-1} \setminus \{\xi = 0\}$ existe al menos un γ_i tal que $P_z(\gamma_i) \neq 0$. Sea Λ_i la matriz cuadrada de tamaño $(m - q + s) \times (m - q + s)$ asociada a γ_i ; claramente las matrices $\Lambda_1, \ldots, \Lambda_T$ verifican el enunciado del lema.
Las cotas de complejidad se siguen de la manera obvia ya que los cómputos sólo involucran productos de matrices, cálculo de determinantes e interpolación con respecto a la variable x_n. ■

Lema 19 *(cf. [9, Lemma 4.5]) Sea $V := UC$ la matriz definida en el Lema 18. Con las notaciones de ese lema, sea i un índice fijo, $1 \leq i \leq T$. Entonces existe una matriz $\Omega_i \in A^{(m-q+s)\times(m-q+s)}$ cuyo determinante es una potencia de c_i (por lo tanto Ω_i es una matriz inversible en $A_{c_i}^{(m-q+s)\times(m-q+s)}$), tal que $V^{(i)}\Omega_i = c_i^2 V^{(i)}(0)$ (donde $V^{(i)}(0)$ denota la matriz $V^{(i)}$ después de la evaluación $x_n \mapsto 0$).*
Esta matriz puede computarse a partir de la matriz de input F mediante un algoritmo que corre en tiempo secuencial $(nL)^{O(1)}(MD)^{O(n)}$. Las entradas de Ω_i se pueden evaluar mediante un slp de tamaño $(MLD)^{O(1)}$ y sus grados son de orden $(MD)^{O(1)}$.

Dem.- Para simplificar la notación escribiremos $W := V^{(i)}, \Delta_1 := \Delta_1^{(i)}, \Delta_2 := \Delta_2^{(i)}$ y $c := c_i$. Dado que c es una resultante, sean $g, h \in A$ tales que

$$c^2 = g\Delta_1 + h\Delta_2 \quad \text{y} \quad \deg_{x_n}(g), \deg_{x_n}(h) < \max\{\deg_{x_n}(\Delta_1), \deg_{x_n}(\Delta_2)\} \leq m - q.$$

Estos polinomios se pueden obtener calculando determinantes de la matiz de Sylvester de Δ_1, Δ_2 donde alguna columna es reemplazada por la columna $\begin{pmatrix} 0 \\ \vdots \\ c \end{pmatrix}$ (calculamos una representación del polinomio c^2 en lugar de la resultante c para evitar divisiones en la regla de Cramer). Esto puede hacerse a partir del output del algoritmo subyacente al lema previo, interpolando los polinomios Δ_1, Δ_2 con respecto a x_n, obteniendo de esta

manera las entradas de la matriz de Sylvester. Finalmente computamos los determinantes mencionados y los tiempos de complejidad no incrementan los obtenidos anteriormente. Consideremos, ahora, las submatrices de W : $B_1 := [W_1, \ldots, W_{m-q}] \in A^{(m-q)\times(m-q)}$ y $B_2 := [W_1, \ldots, W_{m-q-1}, W_{m-q+1}] \in A^{(m-q)\times(m-q)}$.
Para cada j, $m-q+2 \leq j \leq m-q+s$, tenemos

$$c^2 (W_j(0) - W_j) = (g\Delta_1 + h\Delta_2)(W_j(0) - W_j) =$$

$$= gB_1 \mathrm{adj}(B_1)(W_j(0) - W_j) + hB_2 \mathrm{adj}(B_2)(W_j(0) - W_j),$$

donde $\mathrm{adj}(B_l)$ denota la matriz adjunta de B_l, $l = 1, 2$.
Desarrollando esta identidad obtenemos polinomios $g_{kj} \in A, 1 \leq k \leq m-q+1$, tales que

$$c^2 (W_j(0) - W_j) = g_{1j} W_1 + \cdots + g_{m-q+1\,j} W_{m-q+1}.$$

Esto vale para todo índice j, $m-q+2 \leq j \leq m-q+s$. Así la matriz Ω' en $A^{(m-q+s)\times(m-q+s)}$ definida como:

$$\Omega' := \begin{pmatrix} \mathrm{Id}_{m-q+1} & (g_{kj})_{kj} \\ 0 & c^2 \mathrm{Id}_{s-1} \end{pmatrix}$$

verifica:

$$W\Omega' = [W_1, \ldots, W_{m-q+1}, c^2 W_{m-q+2}(0), \ldots, c^2 W_{m-q+s}(0)].$$

Ahora sea $\Theta \in A^{(m-q+1)\times(m-q+1)}$ la matriz definida por

$$\Theta := c\,\mathrm{adj} \begin{pmatrix} W_1 & W_{m-q} & W_{m-q+1} \\ 0 & -h & g \end{pmatrix} \begin{pmatrix} W_1(0) & W_{m-q}(0) & W_{m-q+1}(0) \\ 0 & -h(0) & g(0) \end{pmatrix}.$$

Como c no depende de x_n, se tiene que $\det(\Theta) = c^{3(m-q+1)}$, en particular $\Theta \in SL_{m-q+1}(A_c)$.
Es fácil ver que la matriz Θ verifica

$$[W_1, \ldots, W_{m-q+1}]\,\Theta = c^2 [W_1(0), \ldots, W_{m-q+1}(0)].$$

Ahora se puede chequear que la matriz $\Omega := \Omega' \begin{pmatrix} \Theta & 0 \\ 0 & \mathrm{Id}_{s-1} \end{pmatrix}$ verifica lo pedido. ■

De los lemas anteriores podemos mostrar estimaciones locales para el grado de una base de la imagen de F. Enfatizamos en el hecho de que los polinomios que usamos para localizar sólo involucran las variables $x_1, \ldots, x_{n-1}$:

Lema 20 *Existe un algoritmo que corre en tiempo secuencial* $(nL)^{O(1)}(MD)^{O(n)}$ *a partir de la matriz de input* F, *que computa polinomios* $\pi_1, \ldots, \pi_H \in B$ *tales que*

- $1 \in (\pi_1, \ldots, \pi_H)$,
- $\deg \pi_j = (MD)^{O(1)}$,
- $H = (MD)^{O(n)}$,

- *cada π_j puede ser evaluado por un slp de tamaño $(MLD)^{O(1)}$.*

Más aun, para cada $j = 1, \ldots, H$, el algoritmo computa una base de $\mathrm{Im}(F_{\pi_j})$ formada por vectores polinomiales de grados de orden $(MD)^{O(1)}$ cuyas coordenadas pueden evaluarse mediante un slp de tamaño $(MLD)^{O(1)}$.

Dem.- El algoritmo construye los polinomios π_j como sigue: primero, sea G la matriz definida en el Lema 10 y sean $\xi_1, \ldots, \xi_l \in B$ los menores de tamaño $q \times q$ de G como en el Lema 11; para cada ξ_k, sean $c_1^{(k)}, \ldots, c_T^{(k)} \in B$ los polinomios construidos en el Lema 18 para el caso $\xi := \xi_k$. Las cantidades l y T son de orden $(MD)^{O(n)}$ y $(MD)^{O(1)}$ respectivamente. Dado que los polinomios $\xi_1, \ldots, \xi_l$ generan el anillo B y $c_1^{(k)}, \ldots, c_T^{(k)}$ generan el anilllo B_{ξ_k}, inferimos que los polinomios $\left(\xi_k c_i^{(k)}\right)_{k,i}$ generan todo el anillo B.
Fijemos los índices k, i y sean C, Λ_i y Ω_i las matrices definidas en la Proposición 17, en el Lema 18 y en el Lema 19 respectivamente (para $\xi := \xi_k$ y $c_i := c_i^{(k)}$).
Como $c_i^2 V^{(i)}(0) = V^{(i)}\Omega_i = U\,(C\Lambda_i\Omega_i)$ y las filas de U forman una base de $\mathrm{Ker}\,(\psi_\xi)$ (ver Proposición 16), las filas de $V^{(i)}(0)$ forman una base de $\mathrm{Ker}\,(\psi_{\xi c_i})$ luego del cambio lineal de coordenadas en $A_{\xi c_i}^{(m-q+s)}$ dado por la matriz $c_i^{-2}\,(C\Lambda_i\Omega_i)$.
Dado que $V^{(i)}(0)$ es $B_{\xi c_i}$-unimodular (porque U es $A_{\xi c_i}$-unimodular) sus menores de tamaño $(m-q)\times(m-q)$ generan el anillo $B_{\xi c_i}$. A través del Lema 2, podemos construir efectivamente en tiempo admisible, menores $\mu_1, \ldots, \mu_Q$ donde $Q = (MD)^{O(n-1)}$ y $B_{\xi c_i} = (\mu_1, \ldots, \mu_Q)$ (el hecho de que en este caso el anillo es una localización conveniente de B en lugar de un anillo de polinomios como en el Lema 2 no provoca inconvenientes ya que la enumeración de las celdas no vacías se puede hacer de manera similar fuera de una hipersuperficie; en este caso es suficiente agregar la condición $\{\xi c_i \neq 0\}$). Los grados de estos menores son claramente de orden $(MD)^{O(1)}$.
Observamos que para cada menor μ_u es fácil computar una base de la imagen de la aplicación ψ localizada en el polinomios $\mu_u \xi c_i$: es suficiente tomar la imagen por ψ de aquellas filas de $\mathrm{adj}(C\Lambda_i\Omega_i)$ correspondientes a aquellas columnas de $V^{(i)}(0)$ que no fueron consideradas en la construcción de μ_u.
Tomamos los polinomios π_j como los polinomios $\mu_u \xi_k c_i^{(k)}$ donde $1 \leq k \leq l$, $1 \leq i \leq T$ y $1 \leq u \leq Q$. Observemos que se tiene la cantidad de $(MD)^{O(n)}$ polinomios π_j y que generan el anillo B.
De este modo obtenemos una base para la imagen de F localizada en π_j, cuyos elementos tienen grados acotados por $(MD)^{O(1)}$.
Los enunciados sobre complejidad se siguen de las construcciones previas de la manera natural. ■

II.2.4 Pegado de bases

En esta parte exhibiremos un procedimiento que nos permitirá pegar las bases locales construidas en el Lema 20. Nuestro enfoque hará uso, con algunas adaptaciones, de las técnicas locales-globales de Vaserstein (ver, por ejemplo, [37, Ch.IV, Th.1.18.]). Remarcamos que, en este punto, es crucial que los polinomios en los que vamos a localizar π_j pertenezcan

al anillo B para obtener un procedimiento recursivo (como en las demostraciones clásicas de la conjetura de Serre, ver [40] o [37]).
Por razones técnicas necesitamos bases de $\mathrm{Im}(F)$ y $\mathrm{Ker}(F)$ bajo localizaciones en elementos del anillo B; dado que $\mathrm{Ker}(F) = \mathrm{Im}(\mathrm{Id}_M - F)$, esto puede hacerse aplicando el Lema 20 para las matrices F y $\mathrm{Id}_M - F$ simultáneamente:

Teorema 21 *Existe un algoritmo que corre en tiempo secuencial* $(nL)^{O(1)}(MD)^{O(n)}$ *a partir de la matriz de input* F, *que computa los polinomios* $\pi_1, \ldots, \pi_H \in B$ *tales que*

- $1 \in (\pi_1, \ldots, \pi_H)$,
- $\deg \pi_j = (MD)^{O(1)}$,
- $H = (MD)^{O(n)}$,
- *cada* π_j *puede ser evaluado por un slp de tamaño* $(MLD)^{O(1)}$.

Más aun, para cada $j = 1, \ldots, H$ *el algoritmo computa bases de* $\mathrm{Im}\,(F_{\pi_j})$ *y* $\mathrm{Im}\left((\mathrm{Id} - F)_{\pi_j}\right)$ *(y por lo tanto también una base de* $\mathrm{Ker}(F_{\pi_j})$*) formadas por vectores polinomiales de grados* $(MD)^{O(1)}$ *cuyas coordenadas pueden evaluarse mediante un slp de tamaño* $(MLD)^{O(1)}$.

Dem.- Como hemos observado en la subrutina **H**, podemos hacer el mismo cambio de coordenadas para ambas matrices, F y $\mathrm{Id} - F$, y así obtener menores principales mónicos en todas las variables $x_1, \ldots, x_n$ (este es un punto esencial porque el procedimiento construido en los pasos anteriores es, en algún sentido, un proceso de eliminación de la variable x_n). Así podemos aplicar el Lema 20 a las matrices F y $\mathrm{Id} - F$, obteniendo polinomios π_j y π'_k. Tomamos los polinomios del teorema como todos los productos $\pi_j \pi'_k$. Claramente, esto no incrementa el orden de las consideraciones sobre complejidad. ■

El siguiente resultado muestra una equivalencia explícita local sobre B entre las matrices F y $F(0)$ (recordar que $F(0)$ denota la matriz obtenida reemplazando la variable x_n por 0 en todas las entradas de F).

Lema 22 *Existe un algoritmo que corre en tiempo secuencial* $(nL)^{O(1)}(MD)^{O(n)}$ *y que computa, a partir de la matriz de input* F, *polinomios* $\delta_1, \ldots, \delta_H \in B$ *y matrices* $P_1, \ldots, P_H$, $Q_1, \ldots, Q_H \in A^{M \times M}$, *donde* $H = (MD)^{O(n)}$, *tales que*

- $1 \in (\delta_1, \ldots, \delta_H)$ *y* $\deg \delta_j = (MD)^{O(1)}$.
- $\det(P_j) = \det(Q_j) = \delta_j^M$, $j = 1, \ldots, H$ *(en particular las matrices* P_j *y* Q_j *son inversibles en* A_{δ_j}*) y los grados de sus entradas son de orden* $(MD)^{O(1)}$.
- $\delta_j^2 F = P_j F(0)\, Q_j$.
- *cada* δ_j *y cada entrada de las matrices* P_j *y* Q_j *pueden ser evaluadas por un slp de tamaño* $(MLD)^{O(1)}$.

Dem.- Para cada índice j como en el Teorema 21, sean $\{v_1,\ldots,v_s\}$ y $\{v_{s+1},\ldots,v_M\}$ las bases de $\mathrm{Im}(F_{\pi_j})$ y $\mathrm{Ker}(F_{\pi_j})$ construidas allí. Como F es la matriz de una proyección, $\mathcal{B}_j := \{v_1,\ldots,v_s,v_{s+1},\ldots,v_M\}$ es una base de $A^M_{\pi_j}$. Denotemos por W_j la matriz cuyas columnas son los vectores $v_1,\ldots,v_M$; definimos $\delta_j := \det(W_j)$.
Como la matriz W_j es inversible en A_{π_j}, el polinomio δ_j es un divisor de una potencia de π_j , así δ_j pertenece a B y la familia $\delta_1,\ldots,\delta_H$ genera el anillo B (ya que $\pi_1,\ldots,\pi_H$ tenían esas propiedades).
Definimos, para cada índice j, matrices $P_j := \mathrm{adj}(W_j)W_j(0)$ y $Q_j := \mathrm{adj}(W_j(0))W_j$. Claramente, los polinomios δ_j y las matrices P_j y Q_j se pueden obtener directamente como output del algoritmo subyacente en el Teorema 21 y obtenemos así las estimaciones para la complejidad enunciadas.
Para terminar la demostración del lema, queda sólo demostrar la validez del tercer ítem. Para esto, observemos que se tienen las siguientes relaciones:

$$\delta_j F = \mathrm{adj}(W_j)\begin{pmatrix} \mathrm{Id}_s & 0 \\ 0 & 0 \end{pmatrix} W_j \tag{14}$$

y

$$\delta_j F(0) = \mathrm{adj}(W_j(0))\begin{pmatrix} \mathrm{Id}_s & 0 \\ 0 & 0 \end{pmatrix} W_j(0) \tag{15}$$

De (15) tenemos que

$$\delta_j \begin{pmatrix} \mathrm{Id}_s & 0 \\ 0 & 0 \end{pmatrix} = W_j(0)\,F(0)\,\mathrm{adj}(W_j(0))\,.$$

Entonces, multiplicando la identidad (14) por δ_j y reemplazando $\delta_j \begin{pmatrix} \mathrm{Id}_s & 0 \\ 0 & 0 \end{pmatrix}$ por medio de la última relación, se sigue el resultado. ■

Ahora, haremos uso del argumento de Vaserstein (ver [37, Ch.IV, Th.1.18.]) para "pegar"las matrices P_j's y Q_j's.

Lema 23 *Existe un algoritmo que corre en tiempo secuencial* $(nL)^{O(1)}(MD)^{O(n)}$ *que computa, a partir de la matriz de input* F, *dos matrices inversibles* $P \in A^{M\times M}$ *y* $Q \in A^{M\times M}$ *tales que* $F = PF(0)Q$. *Las entradas de estas matrices tienen grado de orden* $(MD)^{O(n)}$ *y pueden ser evaluadas por un slp de tamaño* $(nL)^{O(1)}(MD)^{O(n)}$.

Dem.- Fijemos un índice j, $j = 1,\ldots,H$, y sea y una nueva variable. Con las notaciones del lema previo, consideremos las matrices con entradas en $A_{\delta_j}[y]$:

$$\Gamma_j := \frac{P_j}{\delta_j}(x_n + \delta_j^M y)\left(\frac{P_j}{\delta_j}\right)^{-1} \quad \text{y} \quad \Lambda_j := \left(\frac{Q_j}{\delta_j}\right)^{-1}\frac{Q_j}{\delta_j}(x_n + \delta_j^M y),$$

donde $\dfrac{P_j}{\delta_j}(x_n + \delta_j^M y)$ denota la matriz $\dfrac{P_j}{\delta_j}$ después de la evaluación $x_n \mapsto x_n + \delta^M y$ y de manera similar para $\dfrac{Q_j}{\delta_j}(x_n + \delta_j^M y)$.

Comenzamos mostrando que estas matrices están en $A[y]^{M\times M}$.
Sea $p_j^{(k,l)} \in A$ la (k,l)-entrada de la matriz P_j; podemos escribir

$$p_j^{(k,l)}(x_n + \delta_j^M y) = p_j^{(k,l)} + \delta_j^M \widetilde{p}_j^{(k,l)}(y), \tag{16}$$

donde $\widetilde{p}_j^{(k,l)}(y)$ es un polinomio en $A[y]$. Denotamos por $\widetilde{P}_j(y) \in A[y]^{M\times M}$ la matriz $\left(\widetilde{p}_j^{(k,l)}(y)\right)_{k,l}$.
Como δ_j^M es el determinante de P_j, tenemos que

$$\left(\frac{P_j}{\delta_j}\right)^{-1} = \mathrm{adj}\left(\frac{P_j}{\delta_j}\right) = \frac{\mathrm{adj}(P_j)}{\delta_j^{M-1}}$$

y, por lo tanto,

$$\Gamma_j = \mathrm{Id}_M + \widetilde{P}_j(y)\mathrm{adj}(P_j) \in A[y]^{M\times M}.$$

El mismo razonamiento aplicado a la matriz $\Gamma_j^{-1} = \dfrac{P_j}{\delta_j}\left(\dfrac{P_j}{\delta_j}\right)^{-1}(x_n + \delta_j^M y)$ muestra que ésta pertenece a $A[y]^{M\times M}$, y, entonces, Γ_j es una matriz inversible en $A[y]^{M\times M}$.
De manera similar se ve que Λ_j se puede descomponer como

$$\Lambda_j = \mathrm{Id}_M + \mathrm{adj}(Q_j)\widetilde{Q}_j(y)$$

donde $\widetilde{Q}_j(y)$ es una matriz adecuada en $A[y]^{M\times M}$, y también que Λ_j es una matriz inversible en $A[y]^{M\times M}$.
Para computar las matrices Γ_j y Λ_j, es suficiente obtener matrices $\widetilde{P}_j$ y $\widetilde{Q}_j$: sea z una nueva indeterminada y consideremos los polinomios $p_j^{(k,l)}(x_n + z) - p_j^{(k,l)} \in A[z]$. Claramente, estos nuevos polinomios pueden computarse con la misma complejidad que la matriz P_j; más aun, interpolando con respecto a la variable z, podemos obtener polinomios $r_1, \ldots, r_d$ en A (donde $d := \deg_{x_n}(p_j^{(k,l)}) = (MD)^{O(1)}$), tales que

$$p_j^{(k,l)}(x_n + z) - p_j^{(k,l)} = \sum_{i=1}^{d} r_i z^i .$$

Así, de la relación (16), el polinomio $\widetilde{p}_j^{(k,l)}(y)$ se puede computar evaluando la relación previa en $z \mapsto \delta_j^M y$ (de hecho $\widetilde{p}_j^{(k,l)}(y) = \sum_{i=1}^{d} r_i \delta_j^{Mi-M} y^i$). Análogamente computamos la matriz $\widetilde{Q}_j$.
Ahora procedemos a la construcción de las matrices P y Q.
Del Lema 22, reemplazando x_n por $x_n + \delta_j^M y$ tenemos :

$$F(x_n + \delta_j^M y) = \frac{P_j}{\delta_j}(x_n + \delta_j^M y)F(0)\frac{Q_j}{\delta_j}(x_n + \delta_j^M y)$$

para $j = 1, \ldots, H$. Y entonces, como $F(0) = \left(\dfrac{P_j}{\delta_j}\right)^{-1} F \left(\dfrac{Q_j}{\delta_j}\right)^{-1}$ (otra vez por Lema 22), obtenemos

$$F(x_n + \delta_j^M y) = \Gamma_j F \Lambda_j \tag{17}$$

para todo j.
Dado que $1 \in (\delta_1^M, \ldots, \delta_H^M)$ (ya que por Lema 22, $1 \in (\delta_1, \ldots, \delta_H)$), aplicando el Nullstellensatz efectivo (ver Subrutina **D** o [26, Th.20]), se tiene en tiempo secuencial $L^{O(1)}(MD)^{O(n)}$ un slp de tamaño $L^{O(1)}(MD)^{O(n)}$, que evalúa los polinomios $\alpha_1, \ldots, \alpha_H \in x_n B$ que verifican:

$$x_n = \alpha_1 \delta_1^M + \cdots + \alpha_H \delta_H^M \qquad \text{y} \qquad \deg \alpha_j = (MD)^{O(n)} \quad \forall j.$$

Considerando la identidad (17) para $j := H$ y reemplazando $x_n \mapsto \sum_{q=1}^{H-1} \alpha_q \delta_q^M$ y $y \mapsto \alpha_H$, se tiene :

$$F = \Gamma_H(\sum_{q=1}^{H-1} \alpha_q \delta_q^M, \alpha_H)\ F(\sum_{q=1}^{H-1} \alpha_q \delta_q^M)\ \Lambda_H(\sum_{q=1}^{H-1} \alpha_q \delta_q^M, \alpha_H).$$

Aplicando una vez más la fórmula (17), con $j := H-1$, y reemplazando $x_n \mapsto \sum_{q=1}^{H-2} \alpha_q \delta^M$ y $y \mapsto \alpha_{H-1}$, se tiene

$$F(\sum_{q=1}^{H-1} \alpha_q \delta_q^M) = \Gamma_{H-1}(\sum_{q=1}^{H-2} \alpha_q \delta_q^M, \alpha_{H-1})\ F(\sum_{q=1}^{H-2} \alpha_q \delta_q^M)\ \Lambda_{H-1}(\sum_{q=1}^{H-2} \alpha_q \delta_q^M, \alpha_{H-1}),$$

y entonces F se puede escribir como:

$$\Gamma_H(\sum_{q=1}^{H-1} \alpha_q \delta_q^M, \alpha_H)\Gamma_{H-1}(\sum_{q=1}^{H-2} \alpha_q \delta_q^M, \alpha_{H-1})\ F(\sum_{q=1}^{H-2} \alpha_q \delta_q^M)\ \Lambda_{H-1}(\sum_{q=1}^{H-2} \alpha_q \delta_q^M, \alpha_{H-1})\Lambda_H(\sum_{q=1}^{H-1} \alpha_q \delta_q^M, \alpha_H).$$

Así, obtenemos para todo índice u, $u = 0, \ldots, j$, donde $j = 1, \ldots, H$, la relación :

$$F = \Big[\prod_{u=0}^{j} \Gamma_{H-u}(\sum_{q=1}^{H-u-1} \alpha_q \delta_q^M, \alpha_{H-u})\Big]\ F(\sum_{q=1}^{H-j} \alpha_q \delta_q^M)\ \Big[\prod_{u=0}^{j} \Lambda_{H-u}(\sum_{q=1}^{H-u-1} \alpha_q \delta_q^M, \alpha_{H-u})\Big].$$

En particular, para $j = H$:

$$F = \Big[\prod_{u=0}^{H} \Gamma_{H-u}(\sum_{q=1}^{H-u-1} \alpha_q \delta_q^M, \alpha_{H-u})\Big]\ F(0)\ \Big[\prod_{u=0}^{H} \Lambda_{H-u}(\sum_{q=1}^{H-u-1} \alpha_q \delta_q^M, \alpha_{H-u})\Big].$$

Podemos entonces tomar

$$P := \prod_{u=0}^{H} \Gamma_{H-u}(\sum_{q=1}^{H-u-1} \alpha_q \delta_q^M, \alpha_{H-u}) \text{ y } Q := \prod_{u=0}^{H} \Lambda_{H-u}(\sum_{q=1}^{H-u-1} \alpha_q \delta_q^M, \alpha_{H-u}).$$

Las cotas de complejidad se siguen directamente del cómputo de las matrices Γ_j y Λ_j y de los polinomios $\alpha_i's$. ■

Observando que $F(0)$ está en las mismas condiciones que F (es decir, es una proyección, los sistemas de generadores del núcleo y la imagen se obtienen poniendo $x_n = 0$, se puede evaluar por un slp del mismo tamaño, etc.), aplicamos el mismo argumento de manera recursiva en el número de variables y se deduce :

Corolario 24 *Existe un algoritmo que corre en tiempo secuencial* $(nL)^{O(1)}(MD)^{O(n)}$ *a partir de la matriz de input* F *que computa dos matrices inversibles* $P \in A^{M\times M}$ *y* $Q \in A^{M\times M}$ *tales que* $F = PF(0,\ldots,0)Q$. *Cada entrada de estas matrices tiene grado de orden* $(MD)^{O(n)}$ *y puede ser evaluada por un slp de tamaño* $(nL)^{O(1)}(MD)^{O(n)}$. ■

Ahora, estamos en condiciones de probar el resultado principal. Subrayamos que las estimaciones para la complejidad (un poco peores que las anteriores) involucran ahora también el cómputo de un cambio lineal de coordenadas conveniente que hace que el menor μ resulte mónico en todas las variables (ver subrutina **H**).

Teorema 25 *Sea* $F \in k[x_1,\ldots,x_n]^{M\times M}$ *una matriz polinomial correspondiente a una proyección lineal (i.e.* $F^2 = F$*) tal que sus entradas son polinomios de grados acotados por un entero* D *y están dadas por un slp de tamaño* L. *Entonces existe un algoritmo bien paralelizable que corre en tiempo secuencial* $(nL)^{O(1)}(MD)^{O(n)}$ *que computa dos subconjuntos de* $k[x_1,\ldots,x_n]^M : \{v_1,\ldots,v_s\}$ *y* $\{v_{s+1},\ldots,v_M\}$ *tales que:*

1. $\{v_1,\ldots,v_M\}$ *es una base de* $k[x_1,\ldots,x_n]^M$.
2. $\{v_1,\ldots,v_s\}$ *es una base de* $\mathrm{Im}(F)$ *y* $\{v_{s+1},\ldots,v_M\}$ *es una base de* $\mathrm{Ker}(F)$.
3. *Las coordenadas de los vectores* v_i *son polinomios de grados acotados por* $(MD)^{O(n)}$ *y están dadas por un slp de tamaño* $(nL)^{O(1)}(MD)^{O(n)}$.

Dem.- Por medio de procedimientos elementales de álgebra lineal sobre el cuerpo k, es fácil construir una base $\{w_1,\ldots,w_M\}$ de k^M cuyos primeros s vectores son una base de la imagen de la matriz $F(0,\ldots,0)$ y los restantes, una base de su núcleo (observemos que la matriz $F(0,\ldots,0) \in k^{M\times M}$ también corresponde a la matriz de una proyección).
Entonces, del Cororlario 24, tomamos $v_1,\ldots,v_s$ como los vectores $Pw_1,\ldots,Pw_s$ y $v_{s+1},\ldots,v_M$ como los vectores $Q^{-1}w_{s+1},\ldots,Q^{-1}w_M$.
Las estimaciones para los grados y los tiempos de complejidad se siguen inmediatamente del Cororlario 24 y del cambio lineal de coordenadas descripto en la Sección II.1.1. ■

II.3 El caso de una matriz unimodular

En esta sección vamos a dar algunas indicaciones para obtener un resultado similar al del último teorema de la sección anterior para el caso más general de una matriz polinomial unimodular (ver Definición 1). No describiremos en detalle los algoritmos para computar bases del núcleo y la imagen de una matriz unimodular porque son casi los mismos que usamos para el caso de la matriz de una proyección; de todas maneras, las cotas de complejidad son peores, aunque siguen siendo simplemente exponenciales.

El Teorema 25 de la sección anterior es suficiente para obtener bases para anillos intersección completa en posición de Noether como haremos en la Parte IV. A pesar de ello nos interesa su generalización a matrices unimodulares. Esto nos permite arribar a un procedimiento efectivo nuevo para saber si los $k[x_1,\ldots,x_n]$-módulos dados por una matriz de una presentación son libres o no y en caso afirmativo construir una base (ver Corolario 29).

En esta sección F denotará una matriz unimodular en $k[x_1,\ldots,x_n]^{N\times M}$ de rango s, cuyas entradas son polinomios de grados acotados por una constante D, dados por un slp de tamaño L. El anillo de polinomios $k[x_1,\ldots,x_n]$ será denotado por A.
La primer diferencia entre el caso unimodular y el caso de una proyección, es la construcción de un sistema de generadores para el núcleo de F; mientras que esto es inmediato para las matrices de una proyección, requiere un tratamiento más cuidadoso para el caso unimodular.

Lema 26 *(cf. [1, Corollary 10] o [54, Corollary 2.4.1]) El núcleo de la matriz F puede ser generado como A-módulo por $(M-s)\left((M+N)^6 D\right)^n$ vectores polinomiales que pueden ser calculados por un algoritmo que corre en tiempo $(nL)^{O(1)}((N+M)D)^{O(n)}$. Las coordenadas de estos vectores son polinomios de grados a lo sumo sD que pueden ser evaluados por un slp de tamaño $(sL)^{O(1)}$.*

Dem.- Consideremos los menores de tamaño $s\times s$, $\delta_1,\ldots,\delta_Q$ como en el Lema 2; entonces se tiene $Q\leq((M+N)^6 D)^n$.
Sin pérdida de generalidad podemos suponer que δ_1 es el primer menor principal; en este caso las primeras s columnas $C_1,\ldots,C_s$ de la matriz F son linealmente independientes sobre $k(x_1,\ldots,x_n)$, y entonces (por la regla de Cramer) tenemos las relaciones:

$$\delta_1 C_{s+i} = b_{1i}^1 C_1 + \ldots + b_{si}^1 C_s \text{ , para } i=1,\ldots,M-s$$

donde los $b_{ji}^1\in A$ tienen grados acotados por sD y pueden ser computados y evaluados (por Cramer y la Subrutina **B**) en tiempo $(sL)^{O(1)}$.
De esta manera, los vectores

$$w_i^1 := \left(b_{1i}^1,\ldots,b_{si}^1,0,\ldots,-\delta_1,\ldots,0\right) ,$$

donde $-\delta_1$ aparece en la coordenada $s+i$, pertenecen al $\mathrm{Ker}(F)$.
Repitiendo esta construcción para $\delta_2,\ldots,\delta_Q$, obtenemos una familia $\mathcal{F}$ de $(M-s)\left((M+N)^6 D\right)^n$ vectores que están en el $\mathrm{Ker}(F)$.
Afirmamos que esta familia genera el $\mathrm{Ker}(F)$.
Para esto es suficiente mostrar que para cualquier ideal maximal $\mathfrak{M}\subset A$ estos vectores generan el núcleo de la aplicación localizada $F_{\mathfrak{M}}: A_{\mathfrak{M}}^M\to A_{\mathfrak{M}}^N$. Es claro que las columnas $C_1,\ldots,C_M$ generan $\mathrm{Im}F_{\mathfrak{M}}$. Por el Lema de Nakayama, dado que $\mathrm{Im}F_{\mathfrak{M}}/\mathfrak{M}\mathrm{Im}F_{\mathfrak{M}}$ es un espacio vectorial de dimensión s, deducimos que existe una base de $\mathrm{Im}F_{\mathfrak{M}}$ que consiste en s columnas apropiadas de la matriz F. Sin pérdida de generalidad, podemos suponer que $C_1,\ldots,C_s$ es una $A_{\mathfrak{M}}$-base de $\mathrm{Im}F_{\mathfrak{M}}$.

Para cada ideal maximal $\mathfrak{M}$, existe algún índice $\underline{j \in \{1,\ldots,Q\}}$, tal que $\delta_j \notin \mathfrak{M}$ (ya que $1 \in (\delta_1,\ldots,\delta_Q)$), y entonces, los $M-s$ vectores $\overline{w_i^j}$ son $A/\mathfrak{M}-$linealmente independientes en $\mathrm{Ker}\,(F_{\mathfrak{M}})\,/\mathfrak{M}\mathrm{Ker}\,(F_{\mathfrak{M}})$ y por lo tanto son una $A/\mathfrak{M}$-base. Esto significa (gracias al Lema de Nakayama), que $\mathcal{F}$ genera $\mathrm{Ker}\,(F_{\mathfrak{M}})$. Como esto ocurre para cada maximal, resulta un resultado global. ■

A partir de este punto, las construcciones para una matriz unimodular son *mutatis mutandis* las mismas que las del caso de una proyección hasta el cómputo de bases para la imagen de F en ciertas localizaciones en el anillo $B := k[x_1,\ldots,x_{n-1}]$ (cf. Secciones II.2.1, II.2.2 y II.2.3). El crecimiento de los tiempos de complejidad se debe esencialmente a la cota simplemente exponencial para la cantidad de elementos en un sistema de generadores de $\mathrm{Ker}(F)$ del Lema 26, que produce un incremento en el tamaño de la matriz G (ver Lema 11). Resumiendo tenemos el siguiente resultado (análogo al Lema 22 demostrado para matrices de proyecciones):

Lema 27 *Existe un algoritmo que corre en tiempo secuencial* $(nL)^{O(1)}\left((M+N)\,D\right)^{O(n^2)}$ *a partir de la matriz de input* F, *que computa polinomios* $\pi_1,\ldots,\pi_H \in B$ *tales que*

- $1 \in (\pi_1,\ldots,\pi_H)$,
- $\deg \pi_j = \left((M+N)\,D\right)^{O(1)}$,
- $H = \left((M+N)\,D\right)^{O(n^2)}$,
- *cada* π_j *puede ser evaluado por un slp de tamaño* $\left((M+N)\,LD\right)^{O(1)}$.

Más aun, para cada $j=1,\ldots,H$, *el algotritmo computa una base de* $\mathrm{Im}\,(F_{\pi_j})$ *formada por vectores polinomiales de grados* $\left((M+N)\,D\right)^{O(1)}$ *cuyas entradas pueden ser evaluadas por un slp de tamaño* $\left((M+N)\,LD\right)^{O(1)}$. ■

Ahora, para ejecutar los procedimientos de pegado de bases como en la Sección II.2.4 necesitamos también bases localizadas para el núcleo de F (ver Teorema 21); en el caso de la proyección era suficiente aplicar el mismo argumento para la matriz $\mathrm{Id}-F$, pero, desafortunadamente, en este caso no sabemos cómo hacer esto de una manera directa. Para sortear este obstáculo, debemos introducir ciertas matrices unimodulares auxiliares relacionadas y repetir los argumentos de las Secciones II.2.1, II.2.2 y II.2.3 para ellas. Para la definición y las propiedades de dichas matrices auxiliares se puede consultar [1, Definition 14].
Por simplicidad evitaremos la descripción de esos argumentos que, también, incrementan las cotas de complejidad.
De este modo se puede obtener un análogo del Teorema 25 para matrices unimodulares:

Teorema 28 *Sea* $F \in k[x_1,\ldots,x_n]^{N\times M}$ *una matriz polinomial unimodular cuyas entradas son polinomios de grados acotados por un entero* D *y están dados por un slp de tamaño* L. *Entonces existe un algoritmo bien paralelizable que corre en tiempo secuencial* $(nL)^{O(1)}\left((M+N)\,D\right)^{O(n^4)}$ *computando una base* $\{v_1,\ldots,v_M\}$ *de* $k[x_1,\ldots,x_n]^M$ *y una base* $\{w_1,\ldots,w_N\}$ *de* $k[x_1,\ldots,x_n]^N$ *tal que:*

1. $\{w_1, \ldots, w_s\}$ *es una base de* $\mathrm{Im}(F)$ *y* $\{v_{s+1}, \ldots, v_M\}$ *es una base de* $\mathrm{Ker}(F)$.

2. *Las coordenadas de los vectores de ambas bases son polinomios de grados acotados por* $((M+N)D)^{O(n^4)}$ *y están dados por un slp de tamaño* $(nL)^{O(1)}((M+N)D)^{O(n^4)}$. ■

Como corolario de este resultado podemos exhibir un algoritmo que decide si un $k[x_1, \ldots, x_n]$-módulo P finito dado mediante su matriz de presentación es libre y, en ese caso, computar una base.

Corolario 29 *Sea* P *un* $k[x_1, \ldots, x_n]$*-módulo de tipo finito y* $F \in k[x_1, \ldots, x_n]^{N \times M}$ *una matriz de presentación para* P *(ver Definición 3). Supongamos que las entradas de la matriz* F *tienen grados totales acotados por* D *y están dados por un slp de tamaño* L. *Entonces existe un algoritmo bien paralelizable que corre en tiempo secuencial* $(nL)^{O(1)}((M+N)D)^{O(n^4)}$ *que decide si* P *es libre y, en caso afirmativo, computa una base de* P.

Dem.- La parte del algoritmo que decide si P es libre ya fue explicada en la Proposición 4. Así si P es libre, la matriz traspuesta F^t es unimodular y entonces se puede aplicar el Teorema 28 y obtener una base $w_1, \ldots, w_M$ de $k[x_1, \ldots, x_n]^M$ tal que $w_1, \ldots, w_s$ es una base de $\mathrm{Im}(F^t)$. Por lo tanto los vectores $w_{s+1}, \ldots, w_M$ dan una base de P. Las cotas de complejidad se siguen directamente. ■

Parte III
Aspectos cuantitativos de la teoría de trazas en anillos intersección completa

Sean k un cuerpo perfecto infinito, $\overline{k}$ su clausura algebraica , $f_1, \ldots, f_{n-r}$ polinomios en $k[x_1, \ldots, x_n]$ de grados acotados por un entero d conformando una sucesión regular y cuyos ceros definen una variedad afín algebraica $V \subset \mathbb{A}^n_{\overline{k}}$. Denotamos por $\deg(V)$ al grado "set theoretical" de la variedad V (ver, por ejemplo, [46, Chapter 5] o [32, Definition 1]); la desigualdad de Bezout establece que $\deg(V) \leq d^{n-r}$ (ver [32, Theorem 1]).
Asumimos que las variables $x_1, \ldots, x_n$ están en posición de Noether con respecto a los polinomios f_i; más precisamente, la aplicación natural $k[x_1, \ldots, x_r] \to k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-r})$ es un morfismo entero e inyectivo.
Escribimos $R := k[x_1, \ldots, x_r]$ y $S := k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-r})$. Para cada polinomio f en $k[x_1, \ldots, x_n]$ denotamos por $\overline{f}$ a su clase en S.
Se sabe que bajo estas hipótesis el anillo S es un R-módulo libre de rango finito (ver, por ejemplo, [17, Corollary 18.17] o [27, Lemma 3.3.1]).

Uno de los objetivos de esta parte es construir una traza para anillos intersección completa y demostrar sus propiedades elementales. Para una visión más general de la teoría de dualidad, pero no constructiva, se puede ver [38]. Para un tratamiento desde el punto de vista de residuos complejos se puede ver por ejemplo [13], [31] o [16].
Con las notaciones y las suposiciones de arriba, consideramos al anillo S como una R-álgebra y denotamos por S^* al espacio dual $\mathrm{Hom}_R(S, R)$. El R-módulo S^* admite una estructura natural de S-módulo de la siguiente manera: para cada par (b, β) en $S \times S^*$ el producto $b.\beta$ es la aplicación R-lineal de S^* definida por $(b.\beta)(s) := \beta(bs)$, para cada s en S.
Nuestras suposiciones sobre R y S nos permitirán mostrar en el Teorema 35 que los S-módulos S y S^* son isomorfos y por lo tanto que S^* puede ser generado por un solo elemento. Un generador σ de S^* se llamará una *traza* de S sobre R.
Bajo nuestras hipótesis tenemos la propiedad adicional de que S es un R-módulo libre finito cuyo rango será denotado por N. Fijemos por un momento una base de este módulo; cada elemento $b \in S$ define, por multiplicación, una matriz cuadrada $M_b \in R^{N \times N}$. Si denotamos por $\mathrm{traza}(M_b)$ a la traza de la matriz de M_b, la aplicación $b \mapsto \mathrm{traza}(M_b)$ define (independientemente de la base de S) un elemento de S^* llamado la *traza usual* y denotado por Tr.
Desafortunadamente la traza usual que es simple de calcular (ver [27]) no es siempre un generador de S^* (en otras palabras, la traza usual no es necesariamente una traza).
Vamos a ver que bajo nuestras hipótesis siempre podemos construir una traza. Nuestro enfoque es bastante similar al de [16] reinterpretando las herramientas de residuos complejos desde el punto de vista de la dualidad algebraica. Como una consecuencia, obtenemos resultados análogos sin restricciones en la característica del cuerpo de base (Teorema 35). Por otro lado, también generalizamos los resultados cuantitativos de [50] (Teorema 46) sin pedir que el ideal $(f_1, \ldots, f_{n-r})$ sea radical.

III.1 Existencia de trazas

Es conocida la traza (de Tate) para anillos de polinomios en una variable. Siguiendo [16], la estrategia será reemplazar la sucesión regular $f_1,\dots,f_{n-r}$ por otra $g_1,\dots,g_{n-r}$, donde cada polinomio g_i está en $R[x_{r+i}]\cap(f_1,\dots,f_{n-r})$. En esta situación usaremos la "traza de Tate"en una variable (ver Proposición 33), y luego, tensorizando, obtendremos una traza σ' de $S':=k[x_1,\dots,x_n]/(g_1,\dots,g_{n-r})$ sobre R.
Finalmente, reescribiendo los polinomios g_i como combinaciones lineales de los f_i mediante el uso de polinomios de grados acotados, estamos en condiciones de construir una traza σ para S a partir de σ' y de allí estimar cotas de grado.

Para hacer una prueba completa, necesitamos un teorema de Wiebe que relaciona los transportadores de dos sucesiones regulares. La lectura de esta demostración puede omitirse para seguir más fácilmente la construcción explícita de las trazas ya que sólo haremos uso del enunciado del Teorema 32 (Teorema de Wiebe para polinomios) pero no de su demostración.

III.1.1 Teorema de Wiebe

Sea $\mathcal{O}$ un anillo local con $f_1,\dots,f_{n-r}$ sucesión regular en $\mathcal{O}$. Sea $g_1,\dots,g_{n-r}$ otra sucesión regular tal que $(g_1,\dots,g_{n-r})\subseteq(f_1,\dots,f_{n-r})$. Supongamos que, para cada $1\leq i\leq n-r$, se tiene la escritura $g_i=\sum_{j=1}^{n-r}a_{ij}f_j$ con $a_{ij}\in\mathcal{O}$.
Llamamos $\mu_{\det(a_{ij})}$ al morfismo $\mathcal{O}$-lineal

$$\mu_{\det(a_{ij})}:\mathcal{O}/(f_1,\dots,f_{n-r})\to\mathcal{O}/(g_1,\dots,g_{n-r})$$

que consiste en multiplicar por $\det(a_{ij})$.
La prueba de la buena definición del morfismo es sencilla. Sean $f,h\in\mathcal{O}$ tales que $f-h\in(f_1,\dots,f_{n-r})$. Podemos escribir $f-h=\sum b_kf_k$. Queremos comprobar que $\det(a_{ij})(f-h)\in(g_1,\dots,g_{n-r})$.
Notemos que aplicando la regla de Cramer al sistema:

$$\begin{pmatrix} a_{11} & a_{1n-r}\\ \vdots & \vdots\\ a_{n-r1} & a_{n-rn-r}\end{pmatrix}\begin{pmatrix} f_1\\ \vdots\\ f_{n-r}\end{pmatrix}=\begin{pmatrix} g_1\\ \vdots\\ g_{n-r}\end{pmatrix}$$

se obtiene que $\det(a_{ij})f_k=\sum c_s^kg_s$ para $k=1,\dots,n-r$. Así, $\det(a_{ij})(f-h)=\sum b_kf_k\det(a_{ij})=\sum b_k(\sum c_s^kg_k)\in(g_1,\dots,g_{n-r})$.

Veamos ahora que $\mu_{\det(a_{ij})}$ no depende de la escritura de los g_i en función de los f_j.

Lema 30 *Sea $\mathcal{O}$ un anillo local y sean $f_1,\dots,f_{n-r}$ y $g_1,\dots,g_{n-r}$ sucesiones regulares en $\mathcal{O}$ tales que $g_i = \sum_{j=1}^{n-r} a_{ij} f_j$ con $i = 1,\dots,n-r$ y $a_{ij} \in \mathcal{O}$.*

Si además hay otra escritura $g_i = \sum_{j=1}^{n-r} d_{ij} f_j$, con $i = 1,\dots,n-r$ y $d_{ij} \in \mathcal{O}$ se tiene que

$$\mu_{\det(a_{ij})} = \mu_{\det(d_{ij})}.$$

Dem.- Sin pérdida de generalidad, podemos suponer que reemplazamos sólo la primera ecuación. Entonces, usamos las escrituras para g_1:

$$\sum_{j=1}^{n-r} (a_{1j} - d_{1j}) f_j = 0.$$

Llamamos $\Delta := \det(a_{ij})$ y $\Delta' := \det(d_{ij})$.
Aplicando la regla de Cramer, obtenemos

$$f_j(\Delta - \Delta') \in (g_2,\dots,g_{n-r}) \tag{18}$$

para $j = 1,\dots,n-r$.
Afirmamos que, para todo $a \in \mathcal{O}$

$$(\Delta - \Delta')a \in (g_2,\dots,g_{n-r}) \subset (g_1,\dots,g_{n-r}).$$

En efecto, supongamos que para algún $a \in \mathcal{O}$, se tiene $(\Delta - \Delta')a \notin (g_2,\dots,g_{n-r})$. Como $g_1 \in (f_1,\dots,f_{n-r})$ vale que $g_1(\Delta - \Delta')a = (g_1(\Delta - \Delta'))a \in (g_2,\dots,g_{n-r})$ en virtud de (18). Esto es absurdo ya que $\mathcal{O}$ es un anillo local y, por lo tanto, culaquier reordenamiento de la sucesión regular $g_1,\dots,g_{n-r}$ resulta también una sucesión regular. Es decir, g_1 es no divisor de cero en $\mathcal{O}/(g_2,\dots,g_{n-r})$. Queda así probada la afirmación.
Entonces $\Delta a = \Delta' a$ en $\mathcal{O}/(g_1,\dots,g_{n-r})$ y, por lo tanto, $\mu_\Delta = \mu_{\Delta'}$. ■

Observación: Debido al lema anterior, el morfismo $\mu_{\det(a_{ij})}$, sólo depende de las sucesiones regulares f y g. Llamaremos, entonces, también μ_g^f a este morfismo. Es claro que valen las siguientes propiedades:

1. si $h_1,\dots,h_{n-r}$ es una sucesión regular con $(h_1,\dots,h_{n-r}) \subset (g_1,\dots,g_{n-r})$, entonces

$$\mu_h^g \circ \mu_g^f = \mu_h^f.$$

2. si $(f_1,\dots,f_{n-r}) = (g_1,\dots,g_{n-r})$, μ_g^f resulta un automorfismo.

Lema 31 *Sea $\mathcal{O}$ un anillo local. Sean $g_1,\ldots,g_{n-r}$ y $f_1,\ldots,f_{n-r}$ dos sucesiones regulares en $\mathcal{O}$ tales que para cada $1\leq i\leq n-r$, $g_i=\sum a_{ij}f_j$ con $a_{ij}\in\mathcal{O}$. Entonces*

$$(det(a_{ij}))=((g_1,\ldots,g_{n-r}):(f_1,\ldots,f_{n-r}))\ y$$

$$(f_1,\ldots,f_{n-r})=((g_1,\ldots,g_{n-r}):det(a_{ij})).$$

Dem.- La demostración sigue [38, Theorem E.20].
Llamamos $\Delta:=\det(a_{ij})$.
Es suficiente ver que $\mu_g^f=\mu_\Delta$, definido como antes, es inyectivo y que su imagen es

$$\{\bar{g}\in\mathcal{O}/(g_1,\ldots,g_{n-r}) \text{ tal que } (f_1,\ldots,f_{n-r})\bar{g}=0\}.$$

Para ello usaremos inducción en la longitud $n-r$ de las sucesiones regulares. Durante la demostración usaremos indistintamente la notación μ_Δ como μ_g^f.
Para $n-r=1$ la prueba es sencilla. En este caso, $g_1=\alpha f_1$, con $\alpha\in\mathcal{O}$. Notemos que como g_1 es no divisor de cero en $\mathcal{O}$, α, también lo es.
Para la inyectividad: si $\alpha\bar{f}=\bar{0}$, entonces $\alpha f\in(g_1)$. Así, $\alpha f=\beta g_1=\beta\alpha f_1$ y, por lo tanto, $f=\beta f_1$. Es decir, $f\in(f_1)$.
Para la imagen: si $\bar{g}$ está en la imagen de μ_Δ, se tiene que $\bar{g}=\alpha\bar{f}$. Entonces $g-\alpha f\in(g_1)$ y, por lo tanto, $f_1(g-\alpha f)=f_1g-g_1f\in(g_1)$. Así, $f_1\bar{g}=0$. Inversamente, si $f_1\bar{g}=0$, se tiene que $f_1g=\beta g_1=\beta\alpha f_1$. En consecuencia, $\bar{g}=\bar{\beta}\alpha=\mu_\Delta(\bar{\beta})$.
Para $n-r>1$. Asumamos que el enunciado es válido para sucesiones regulares de tamaño $n-r-1$.
Afirmación: Se puede considerarque f_1 no es divisor de cero en $\mathcal{O}/(g_2,\ldots,g_{n-r})$.
Dem. de la afirmación Sean $\wp_1,\ldots,\wp_s$ los ideales primos (irredundantes) asociados al ideal $(g_2,\ldots g_{n-r})$. Como g_1 no es divisor de cero en $\mathcal{O}/(g_2,\ldots,g_{n-r})$, no pertenece a ninguno de los $\wp_i$ con $i=1,\ldots,s$. Por lo tanto, $(f_1,\ldots,f_{n-r})$ no está contenido en ninguno de estos ideales primos. Renumerando, eventualmente, podemos suponer que f_1 pertenece a $\wp_1,\ldots,\wp_m$ y no pertenece a $\wp_{m+1},\ldots,wp_s$ con $(m\geq 1)$.
Sea $\mathfrak{M}$ el ideal maximal de $\mathcal{O}$. Se tiene que $(f_1,\ldots,f_{n-r})\mathfrak{M}\wp_{m+1}\ldots\wp_s$ no está contenido en ninguno de los $\wp_1,\ldots,\wp_m$. Elegimos entonces un $x\in(f_1,\ldots,f_{n-r})\mathfrak{M}\wp_{m+1}\ldots\wp_s$ de modo que $x\notin\wp_1,\ldots,x\notin\wp_m$.
Consideremos $f_1':=f_1+x$. Dado que f_1 no pertenece a $\wp_{m+1},\ldots,wp_s$ y que $x\notin\wp_1,\ldots,x\notin\wp_m$, es claro que $f_1'\notin\wp_1,\ldots,f_1'\notin\wp_s$. Por lo tanto f_1' no es divisor de cero de $\mathcal{O}/(g_2,\ldots,g_{n-r})$.
Falta ver que $(f_1,\ldots,f_{n-r})=(f_1',f_2,\ldots,f_{n-r})$. Para ello basta notar que $f_1'=f_1+x=(1+m)f_1+\beta_2f_2+\ldots+\beta_{n-r}f_{n-r}$ con $m\in\mathfrak{M}$ y consecuentemente $1+m$ unidad.
Como $\mu_g^{f'}=\mu_g^f\circ\mu_f^{f'}$ y como $\mu_f^{f'}$ es un automorfismo de $\mathcal{O}/(f_1,\ldots,f_{n-r})$, es suficiente mostrar el resultado para $\mu_g^{f'}$. Podemos suponer, entonces, que f_1 es no divisor de cero en $\mathcal{O}/(g_2,\ldots,g_{n-r})$.
Sea Δ_1 el determinante del sistema asociado a las sucesiones regulares $f_1,g_2,\ldots,g_{n-r}$ y $f_1,\ldots,f_{n-r}$.

$$\begin{aligned} f_1 &= f_1 \\ g_i &= \sum_{k=1}^{n-r} a_{ik}f_k \text{ para } i=2,\ldots,n-r. \end{aligned}$$

Aplicando la regla de Cramer al sistema original, obtenemos

$$g_1\Delta_1 - f_1\Delta \in (g_2, \ldots, g_{n-r}).$$

Por lo tanto el siguiente diagrama conmuta

$$\begin{array}{ccc} \mathcal{O}/(f_1, \ldots, f_{n-r}) & \xrightarrow{\mu_{\Delta_1}} & \mathcal{O}/(f_1, g_2, \ldots, g_{n-r}) \\ \mu_g^f \downarrow & & \mu_{g_1} \downarrow \\ \mathcal{O}/(g_1, \ldots, g_{n-r}) & \xrightarrow{\mu_{f_1}} & \mathcal{O}/(f_1 g_1, g_2, \ldots, g_{n-r}) \end{array}$$

Aplicando la hipótesis inductiva al anillo local $\mathcal{O}/(f_1)$ y a las imágenes de f_i y g_i en $\mathcal{O}/(f_1)$, vemos que μ_{Δ_1} es inyectivo y su imagen es

$$\{\bar{g} \in \mathcal{O}/(f_1, g_2, \ldots, g_{n-r}) \text{ tal que } (f_1, \ldots, f_{n-r})\bar{g} = 0\} =$$

$$= \{g \in \mathcal{O} \text{ tal que } (f_1, \ldots, f_{n-r})g \subset (f_1, g_2, \ldots, g_{n-r})\}/(f_1, g_2, \ldots, g_{n-r}).$$

Dado que f_1 y g_1 son no divisores de cero en $\mathcal{O}/(g_2, \ldots, g_{n-r})$, los morfismos μ_{f_1} y μ_{g_1} son inyectivos. El diagrama anterior muestra, entonces, que μ_g^f es inyectivo.
Más aun,

$$\{\bar{g} \in \mathcal{O}/(g_1, \ldots, g_{n-r}) \text{ tal que } (f_1, \ldots, f_{n-r})\bar{g} = 0\} =$$

$$= \{g' \in \mathcal{O} \text{ tal que } (f_1, \ldots, f_{n-r})g' \subset (g_1, \ldots, g_{n-r})\}/(g_1, \ldots, g_{n-r}).$$

y, como μ_{f_1} es inyectivo, la imagen de este módulo vía μ_{f_1} es

$$\{f_1 g' \text{ tal que } g' \in \mathcal{O},\ (f_1, \ldots, f_{n-r})f_1 g' \subset (f_1, g_2, \ldots, g_{n-r})\}/(f_1 g_1, g_2, \ldots, g_{n-r}).$$

Como μ_{g_1} es inyectivo, obtenemos

$$\mu_{g_1}(im_{\mu_{\Delta_1}}) = \{g_1 g \text{ tal que } g \in \mathcal{O},\ (f_1, \ldots, f_{n-r})g_1 g \subset (f_1 g_1, g_2, \ldots, g_{n-r})\}/(f_1 g_1, g_2, \ldots, g_{n-r}).$$

Dado $g' \in \mathcal{O}$ con $(f_1, \ldots, f_{n-r})f_1 g' \subset (f_1 g_1, g_2, \ldots, g_{n-r})$ tenemos que $f_1^2 g' \in (f_1 g_1, g_2, \ldots, g_{n-r})$ y por lo tanto

$$f_1 g' \equiv g_1 g \ \ mod\,(g_2, \ldots, g_{n-r})$$

con algún $g \in \mathcal{O}$ tal que $(f_1, \ldots, f_{n-r})g_1 g \subset (f_1 g_1, g_2, \ldots, g_{n-r})$.
Inversamente, si es dado un tal $g \in \mathcal{O}$, entonces, en particular, $g_1^2 g \in (f_1 g_1, g_2, \ldots, g_{n-r})$ y por lo tanto

$$g_1 g \equiv f_1 g' \ \ mod\,(g_2, \ldots, g_{n-r}).$$

Esto prueba que la imagen de $\{\bar{g} \in \mathcal{O}/(g_1, \ldots, g_{n-r}) \text{ tal que } (f_1, \ldots, f_{n-r})\bar{g} = 0\}$ vía μ_{f_1} es

$$\mu_{g_1}(im_{\mu_{\Delta_1}}) = im(\mu_{g_1} \circ \mu_{\Delta_1}) = \mu_{f_1}(im_{\mu_\Delta})$$

y, como μ_{f_1} es inyectivo,

$$im_{\mu_\Delta} = \{\bar{g} \in \mathcal{O}/(g_1, \ldots, g_{n-r}) \text{ tal que } (f_1, \ldots, f_{n-r})\bar{g} = 0\}.$$

La inyectividad de μ_Δ prueba la inclusión $(f_1, \ldots, f_{n-r}) \supseteq ((g_1, \ldots, g_{n-r}) : det(a_{ij}))$.
El cálculo de la imagen prueba la igualdad $(det(a_{ij})) = ((g_1, \ldots, g_{n-r}) : (f_1, \ldots, f_{n-r}))$.
Para probar la inclusión que falta sólo hay que aplicar la regla de Cramer al sistema

$$\begin{pmatrix} a_{11} & a_{1n-r} \\ \vdots & \vdots \\ a_{n-r1} & a_{n-rn-r} \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_{n-r} \end{pmatrix} = \begin{pmatrix} g_1 \\ \vdots \\ g_{n-r} \end{pmatrix}$$

donde obtenemos que $\det(a_{ij})f_j \in (g_1, \ldots, g_{n-r})$ para todo $j = 1, \ldots, n-r$. ■

Ahora, aplicando el resultado al anillo de polinomios, se obtiene:

Teorema 32 *(Wiebe) Si* $g_1, \ldots, g_{n-r}$ *y* $f_1, \ldots, f_{n-r}$ *son dos sucesiones regulares en* $k[x_1, \ldots, x_n]$ *tales que, para cada* $1 \leq i \leq n-r$, *se tiene* $g_i = \sum_{j=1}^{n-r} a_{ij} f_j$ *con* $a_{ij} \in k[x_1, \ldots, x_n]$, *entonces*

$$(det(a_{ij})) = ((g_1, \ldots, g_{n-r}) : (f_1, \ldots, f_{n-r})) \text{ y}$$
$$(f_1, \ldots, f_{n-r}) = ((g_1, \ldots, g_{n-r}) : det(a_{ij})).$$

Dem.- La demostración es corolario de la proposición anterior.
Consideramos el anillo de polinomios $A := k[x_1, \ldots, x_n]$. Sea $\mathfrak{M}$ un ideal maximal de A que contenga a la sucesión regular $(f_1, \ldots, f_{n-r})$. Aplicando la proposición anterior al anillo local $\mathcal{O} := A_{\mathfrak{M}}$, se tiene que

$$\mu_{\det(a_{ij})} : \mathcal{O}/(f_1, \ldots, f_{n-r}) \longrightarrow \{\bar{g} \in \mathcal{O}/(g_1, \ldots, g_{n-r}) \text{ tal que } (f_1, \ldots, f_{n-r})\bar{g} = 0\}$$

es un isomorfismo en cada localización en $\mathfrak{M}$ como arriba. Si $\mathfrak{M}$ es un maximal que no contiene a la sucesión regular, el resultado es trivial ya que tanto $\mathcal{O}/(f_1, \ldots, f_{n-r})$ como $\{\bar{g} \in \mathcal{O}/(g_1, \ldots, g_{n-r}) \text{ tal que } (f_1, \ldots, f_{n-r})\bar{g} = 0\}$ resultan 0.
Por lo tanto, es un resultado global. La demostración concluye igual que en el lema previo.
■

III.1.2 Construcción de una traza para anillos intersección completa

Empezamos, ahora, exhibiendo una traza en el caso del anillo de polinomios en una variable de manera constructiva. Esta traza es conocida como la *traza de Tate.*

Proposición 33 *Sean R un anillo íntegro, x una indeterminada sobre R y $g \in R[x]$ un polinomio mónico en x no unidad. Entonces $\sigma_0 : S := R[x]/(g) \to R$ definida por $\sigma_0(s) := b_{d-1}$ si $s = b_{d-1}\bar{x}^{d-1} + \ldots + b_0$ resulta una traza en el sentido siguiente: se cumple que S^* es monógeno con base σ_0 y que para esa traza vale la fórmula (llamada "fórmula de la traza")*

$$s = \sum_{i=0}^{n-1} \sigma_0(\lambda_i s)\bar{x}^i$$

para todo $s \in S$ y para ciertos λ_i en S (independientes de s).

Dem.- Sea $g = x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in R[x]$. Tenemos que mostrar que σ_0 genera el S-módulo S^*, que es libre de torsión y que vale la fórmula enunciada.
Notemos que S es un R-módulo libre con base $\mathcal{B} = \{1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{d-1}\}$. Sea $\{\psi_0, \ldots, \psi_{d-1}\}$ la base dual de $\mathcal{B}$. Es decir, $\psi_i(\bar{x}^j) = \delta_{ij}$.
Veamos que para cada ψ_i, existe $\lambda_i \in S$ tal que $\psi_i = \lambda_i\sigma_0$. Así, dada $\sigma \in S^*$, tendremos que si $\sigma = \sum \alpha_i\psi_i$ con $\alpha_i \in A$, entonces $\sigma = \sum_{i=1}^{d-1} \alpha_i\lambda_i\sigma_0 = (\sum_{i=1}^{d-1} \alpha_i\lambda_i)\sigma_0$.
Para buscar cada $\lambda_i \in S$, necesitamos que

$$\lambda_i\sigma_0(\bar{x}^j) = \sigma_0(\lambda_i\bar{x}^j) = \psi_i(\bar{x}^j) = \delta_{ij} \text{ para } j = 0, \ldots, d-1.$$

Veamos que si definimos $\lambda_i := x^{d-1-i} + a_{n-1}x^{d-i-2} + \ldots + a_{i+1}$ se verifica lo pedido.
Con esta definición es inmediato que se cumple la relación $x^{i+1}\lambda_i = g - a_i x^i - \ldots - a_0$.
Para comprobar que los λ_i son apropiados, basta ver que $\sigma_0(\lambda_i\bar{x}^j) = \delta_{ij}$ para $j = 0, \ldots, d-1$.
Si $i = j$, resulta que $\sigma_0(\lambda_i\bar{x}^i) = \sigma_0((\bar{x}^{d-i-1} + a_{d-1}\bar{x}^{d-i-2} + \ldots + a_{i+1})\bar{x}^i) = \sigma_0(\bar{x}^{d-1} + a_{d-1}\bar{x}^{d-2} + \ldots + a_{i+1}\bar{x}^i) = 1$.
Si $i \neq j$, consideramos dos casos.
Para $j < i$, tenemos $\sigma_0(\bar{x}^j\lambda_i) = \sigma_0(\bar{x}^{d-1+j-i} + \ldots + a_{i+1}\bar{x}^j) = 0$ pues $d-1+j-i < d-1$.
Para $j > i$, se tiene $\bar{x}^j\lambda_i = \bar{x}^{j-(i+1)}\bar{x}^{i+1}\lambda_i = \bar{x}^{j-(i+1)}(\bar{g} - a_i\bar{x}^i - \ldots - a_0)$. Entonces, $\sigma_0(\bar{x}^j\lambda_i) = \sigma_0(\bar{x}^{j-(i+1)}\bar{g} - a_i\bar{x}^{j-1} - \ldots - a_0\bar{x}^{j-i-1}) = \sigma_0(-a_i\bar{x}^{j-1} - \ldots - a_0\bar{x}^{j-i-1}) = 0$ pues $j - 1 < d - 1$.
Por lo tanto los λ_i verifican lo pedido y, dado que $\sigma_0(\lambda_i s) = \sigma_0(\lambda_i \sum_{j=0}^{d-1} b_j\bar{x}_j) = b_i$, se tiene la "fórmula de la traza".
Notar que de esta fórmula se deduce que σ_0 es libre de torsión. ■

Sean $n, r \in \mathbb{N}$ tales que $r < n$ y sean $x_{r+1}, \ldots, x_n$ variables libres sobre un dominio íntegro R. Sean $g_1, \ldots, g_{n-r}$ polinomios tales que $g_i \in R[x_{r+i}]$ son mónicos en la variable x_{r+i} de grado positivo. Consideramos $S' := R[x_{r+1}]/(g_1) \otimes_R \ldots \otimes_R R[x_n]/(g_{n-r})$. Mostraremos ahora un resultado análogo al anterior. Es decir, $(S')^*$ es S'-monógeno con una traza que es el "producto" de la trazas de Tate en cada variable.

Proposición 34 *Sea $S' := R[x_{r+1}]/(g_1) \otimes_R \ldots \otimes_R R[x_n]/(g_{n-r})$ con $g_i \in R[x_{r+i}]$ mónico en la variable x_{r+i} de grado positivo. Sea σ_i' la traza de Tate para $S_i' := R[x_{r+i}]/(g_i)$.*

Entonces $\sigma' \in (S')^*$ *definida por* $\sigma'(s_1 \otimes \ldots \otimes s_{n-r}) := \sigma'_1(s_1)\ldots\sigma'_{n-r}(s_{n-r})$ *resulta una traza para la que vale la fórmula (llamada "fórmula de la traza")*

$$s' = \sum \sigma'(\lambda_{i_1,\ldots,i_{n-r}} s')\bar{x}_{r+1}^{i_1} \otimes \ldots \otimes \bar{x}_n^{i_{n-r}}$$

para todo $s' \in S'$ *y para ciertos* $\lambda_{i_1,\ldots,i_{n-r}}$ *en* S' *(independientes de* $s_1 \otimes \ldots \otimes s_{n-r}$*).*

Dem.- La demostración se sigue de [38, Prop.F.16a y Prop.F.17]. Basta considerar el caso $n = 2,\ r = 0$. Sea $S'_1 = R[x_1]/(g_1)$ que tiene una traza σ'_1 y $S'_2 := R[x_2]/(g_2)$ que es una R-álgebra. En estas condiciones $id_{S'_2} \otimes \sigma'_1 : S'_2 \otimes_R S'_1 \to S'_2 \otimes_R R = S'_2$ es una traza de $S'_2 \otimes_R S'_1$ sobre S'_2.
Ahora, como $S'_2 \otimes_R S'_1$ tiene traza $id_{S'_2} \otimes_R \sigma'_1$ sobre S'_2 y S'_2 tiene traza σ'_2 sobre R, resulta que $\sigma'_2(id_{S'_2} \otimes_R \sigma'_1)$ es traza de $S'_2 \otimes_R S'_1$ sobre R.
Notar que $\sigma'_2(id_{S'_2} \otimes_R \sigma'_1)(s_2 \otimes s_1) = \sigma'_2(s_2 \otimes \sigma'_1(s_1)) = \sigma'_2(s_2\sigma'_1(s_1)) = \sigma'_2(s_2)\sigma'_1(s_1)$.
Para ver que vale la "fórmula de la traza", también operamos inductivamente. Con las notaciones anteriores, consideremos σ' la traza producto de $S'_2 \otimes_R S'_1$ definida por

$$\sigma'(s_1 \otimes_R s_2) := \sigma'_1(s_1)\sigma'_2(s_2).$$

Si $s_1 = \sum_{i=0}^{t} \sigma'_1(\lambda_i^1 s_1)\bar{x}_1^i$ y $s_2 = \sum_{j=0}^{l} \sigma'_2(\lambda_j^2 s_2)\bar{x}_2^j$, en virtud de la Proposición 33 tenemos que

$$\begin{aligned}
s_1 \otimes s_2 &= \sum_{i=0}^{t} \sigma'_1(\lambda_i^1 s_1)\bar{x}_1^i \otimes \sum_{j=0}^{l} \sigma'_2(\lambda_j^2 s_2)\bar{x}_2^j \\
&= \sum_{i=0}^{t}\sum_{j=0}^{l} \sigma'_1(\lambda_i^1 s_1)\sigma'_2(\lambda_j^2 s_2)\bar{x}_2^j\bar{x}_1^i \otimes \bar{x}_2^j \\
&= \sum_{i=0}^{t}\sum_{j=0}^{l} \sigma'(\lambda_i^1 s_1 \otimes \lambda_j^2 s_2)\bar{x}_1^i \otimes \bar{x}_2^j \\
&= \sum_{i=0}^{t}\sum_{j=0}^{l} \sigma'((\lambda_i^1 \otimes \lambda_j^2)(s_1 \otimes s_2))\bar{x}_1^i \otimes \bar{x}_2^j.
\end{aligned}$$

La demostración se sigue inductivamente. ■

Pasamos ahora al caso general.
Sea $f_1, \ldots, f_{n-r}$ una sucesión regular de $k[x_1, \ldots, x_n]$ donde las variables $x_1, \ldots, x_n$ están en posición de Noether con respecto a los polinomios f_i y los grados de los f_i están acotados por d. Introducimos una nueva sucesión regular relacionada con $f_1, \ldots, f_{n-r}$. Consideramos, para ello, la sucesión regular $g_1, \ldots, g_{n-r}$ definida por las ecuaciones de dependencia entera de las variables $x_{r+1}, \ldots, x_n$ sobre $R := k[x_1, \ldots, x_r]$ respectivamente. Es claro entonces que $g_i \in R[x_{r+i}]$. Dado que $(g_1, \ldots, g_{n-r}) \subset (f_1, \ldots, f_{n-r})$, se tiene una escritura del tipo $g_i = \sum_{j=0}^{n-r} a_{ij} f_j$, con los polinomios $a_{ij} \in k[x_1, \ldots, x_n]$, para $i = 1, \ldots, n-r$.

Notar que gracias a la Proposición 34 ya hemos construido una traza σ' sobre R para $S' = k[x_1, \ldots, x_n]/(g_1, \ldots, g_{n-r})$ con la sucesión regular $g_1, \ldots, g_{n-r}$ ya que es claro que $S' \simeq R[x_{r+1}]/(g_1) \otimes_R \ldots \otimes_R R[x_n]/(g_{n-r})$. Ahora, construiremos una traza para S^* a partir de la traza de $(S')^*$, relacionando ambas sucesiones regulares vía el Teorema 32. Recordemos que $S := k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-r})$

Teorema 35 *Para S, S' y R como arriba, sea $\pi : S' \to S$ la proyección canónica. Entonces $\sigma \in S^*$ definida como sigue*

$$\sigma(\pi(f)) := \sigma'(det(a_{ij})f)$$

resulta una traza de S sobre R (Recordar que σ' es una traza de S' sobre R).

Dem.- Hay que demostrar que $S.\sigma = S^*$ y que $S^* \simeq_S S$. Para lo primero, sea $\tau \in S^*$, entonces $\tau o \pi \in (S')^*$ y, por lo tanto, existe $\xi \in S'$ tal que $\tau o \pi = \xi.\sigma'$, ya que σ' es una traza para S'. Es suficiente ver que $\xi = \alpha det(a_{ij})$ para algún $\alpha \in S'$ (pues, entonces, $\tau(\pi(f)) = \sigma'(\alpha det(a_{ij})f) = \sigma(\pi(\alpha)\pi(f)) = (\pi(\alpha).\sigma)(\pi(f))$, es decir, $\tau = \pi(\alpha).\sigma.$). Dado que para cualquier $\lambda \in S'$ vale que $\pi(\lambda f_j) = 0$ para todo índice j, $1 \leq j \leq n - r$, se tiene que $\sigma'(\xi \lambda f_j) = 0$, para todo j y para todo λ; como σ' cumple la fórmula de la traza se deduce que $\xi f_j = 0$ en S' para todo j. En otras palabras, $\xi \in ((g_1, \ldots g_{n-r}) : (f_1, \ldots, f_{n-r})) = (det(a_{ij}))$ (Teorema 32).
Con esto se tiene que $1 \mapsto \sigma$ define un epimorfismo de S en S^* que es claramente un monomorfismo pues si $\pi(\alpha).\sigma = 0$, entonces $\alpha det(a_{ij}) = 0$ en S' y, por el Teorema de Wiebe, $\alpha \in (f_1, \ldots f_{n-r})$ con lo que $\pi(\alpha) = 0$. ■

III.1.3 La fórmula de la traza

Esta fórmula (fórmula de dualidad) nos permitirá reescribir los elementos de S vía un elemento de su dual. Juega un papel similar a la traza usual en espacios vectoriales de dimensión finita como generador del dual. Para probar que una tal fórmula se verifica en el caso de nuestra traza sobre S vamos a dar una nueva descripción que resultará más apropiada para nuestros propósitos.
Sea $f_1, \ldots, f_{n-r} \in k[x_1, \ldots, x_n]$ una sucesión regular tal que

$$R := k[x_1, \ldots, x_r] \hookrightarrow S := k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-r})$$

esté en posición de Noether.
Sean $g_1, \ldots, g_{n-r} \in k[x_1, \ldots, x_n]$, tal que $g_i \in R[x_{r+i}]$ son las ecuaciones de dependencia entera de cada variable $\overline{x_{r+i}} \in S$ sobre R $(1 \leq i \leq n-r)$ y sean $a_{ij} \in k[x_1, \ldots, x_n]$ tales que $g_i = \sum_{j=1}^{n-r} a_{ij} f_j$
Notemos $S' := k[x_1, \ldots, x_n]/(g_1, \ldots, g_{n-r})$.
Sea $\sigma' \in (S')^*$ la traza asociada al producto tensorial de las trazas de Tate de cada $S'_i := R[x_{r+i}]/(g_i)$. Notemos σ la traza de S^* definida como $\sigma(\pi(f)) := \sigma'(\det(\alpha_{ij})f)$, con $\pi : S' \to S$ la proyección canónica (ver las Proposiciones 33, 34 y el Teorema 35 de la sección anterior). Queremos ver ahora que las trazas construidas verifican "fórmulas de la traza" análogas a las de las Proposiciones 33 y 34.

Ya hemos probado en la sección anterior que siempre existe, bajo nuestras hipótesis, una traza para S ó S'.
Consideremos el núcleo del morfismo multiplicación

$$\mu : S \otimes_R S \to S$$

$$\mu(a \otimes b) = ab$$

El núcleo está generado por $\{s \otimes 1 - 1 \otimes s : \ s \in S\}$ (ver [34, Prop. 1.3]). Es claro que $S \otimes S$ tiene dos estructuras como S-módulo (multiplicar en el primer o en el segundo factor). Sobre $\mathrm{Ann}(\ker \mu)$ esas dos estructuras coinciden, ya que

$$\mathrm{Ann}_{S\otimes S}(\ker \mu)(s \otimes 1 - 1 \otimes s) = 0.$$

Definimos, ahora, el morfismo

$$\Phi : S \otimes_R S \to \mathrm{Hom}_R(S^*, S)$$

$$\Phi\left(\sum a_m \otimes b_m\right)(\tau) := \sum a_m \tau(b_m)$$

Se tiene que:
Lema 36 Φ *es un isomorfismo*

Dem.- La demostración se basa en el hecho de que bajo nuestras hipótesis S es un R-módulo libre de tipo finito. Consideremos $\{v_1, \ldots, v_M\}$ una base de S y sea $\{\tau_1, \ldots, \tau_M\}$ la base dual de S^*.
Veamos que Φ es un monomorfismo. Sea $\Phi(\sum a_m \otimes b_m)(\tau_j) = 0$ para todo $j = 1, \ldots, M$. Esto es que si $b_m = \sum b_{mj} v_j$, entonces $\sum a_m \tau_j(b_m) = \sum a_m b_{mj} = 0$ para todo j.
Entonces $\sum a_m \otimes b_m = \sum a_m \otimes \sum b_{mj} v_j = \sum (\sum a_m b_{mj}) \otimes v_j = 0$.
Para ver que es un epimorfismo basta observar que dada $F \in \mathrm{Hom}_R(S^*, S)$ tal que $F(\tau_j) = s_j \in S$, se tiene que $\Phi(\sum_{m=1}^{M} s_m \otimes v_m)(\tau_j) = s_j$. ■
También se puede mostrar que

Proposición 37 Φ *induce un isomorfismo de* S*-módulos*

$$\Phi : \mathrm{Ann}(\ker \mu) \to \mathrm{Hom}_S(S^*, S)$$

En particular, dado que S^* *es monógeno, resulta que* $\mathrm{Ann}(\ker \mu)$ *es principal.*

Dem.- Sea $x = \sum a_j \otimes b_j \in \mathrm{Ann}(\ker \mu)$.
Si $s \in S$, se tiene que $\sum s a_j \otimes b_j = \sum a_j \otimes s b_j$ (pues coinciden las dos estructuras de S-módulo sobre $\mathrm{Ann}(\ker \mu)$.
Sea $l \in S^* = \mathrm{Hom}_R(S, R)$.
Veamos que $\Phi(x) : S^* \to S$ es un morfismo S-lineal. Tenemos, por definición de Φ, que $\Phi(x)(sl) = \sum a_j (sl)(b_j) = \sum a_j l(s b_j) = \sum a_j l(b_j) s = s \sum a_j l(b_j) = s\Phi(x)(l)$.
Más aun, $\Phi(sx) = s\Phi(x)$ y, por lo tanto, Φ restringida al $\mathrm{Ann}(\ker \mu)$ es S-lineal.
Veamos ahora que Φ restringida a $\mathrm{Ann}(\ker \mu)$ es un isomorfismo. Si para $x = \sum a_j \otimes b_j \in S \otimes_R S$, el morfismo $\Phi(x)$ es S-lineal, entonces con $x_1 := \sum s a_j \otimes b_j$ y $x_2 := \sum a_j \otimes s b_j$,

obtenemos para $l \in S^*$, que $\Phi(x_1)(l) = \Phi(x)(sl) = s\Phi(x)(l) = \Phi(x_2)(l)$ y, por lo tanto, $x_1 = x_2$. Es decir, $x \in \mathrm{Ann}(\ker \mu)$. ■

De la proposición anterior y del hecho de que Φ es un isomorfismo tiene sentido la definición siguiente.

Definición 38 *Dada una traza arbitraria $\sigma \in S^*$ y un generador $\sum a_m \otimes b_m$ de $\mathrm{Ann}(\ker \mu)$, diremos que el par $(\sum a_m \otimes b_m, \sigma)$ verifica la fórmula de la traza si*

$$1 = \sum a_m \sigma(b_m).$$

En otras palabras, $\Phi(\sum a_m \otimes b_m)(\sigma) = 1$.

Observar que dado un generador $\mathrm{Ann}(\ker \mu)$ queda unívocamente determinado $\sigma \in S^*$ tal que verifica la fórmula de la traza, y recíprocamente (como consecuencia del isomorfismo de la última proposición).
En el caso de anillos intersección completa es fácil construir un generador del anulador y con ello conseguir una fórmula de la traza explícita como sigue.
Dada una sucesión regular cualquiera $f_1, \ldots, f_{n-r} \in k[x_1, \ldots, x_n]$ con las variables en posición de Noether siempre se puede obtener una traza que verifique la fórmula de la traza.
Dado $f \in k[x_1, \ldots, x_n]$, si $y_{r+1}, \ldots, y_n$ son nuevas variables sobre $R := k[x_1, \ldots, x_r]$, notaremos

$$f^{(y)} := f(x_1, \ldots, x_r, y_{r+1}, \ldots, y_n).$$

Mediante el proceso habitual vía el desarrollo de Taylor (ver por ejemplo [37]): se escriben los polinomios $f_i^{(y)} - f_i$ de la forma:

$$f_i^{(y)} - f_i = \sum_{j=1}^{n-r} d_{ij}(y_{r+j} - x_{r+j}) \tag{19}$$

con $d_{ij} \in k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$, y se considera a $\det(d_{ij})$ como un elemento de $S \otimes_R S$ vía el isomorfismo

$$S \otimes_R S \simeq k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n] / \left(f_1, \ldots, f_{n-r}, f_1^{(y)}, \ldots, f_{n-r}^{(y)}\right).$$

El elemento $\det(d_{ij})$ no depende de la escritura en virtud del Teorema de Wiebe aplicado a las sucesiones regulares $\left\{f_1^{(y)} - f_1, \ldots, f_{n-r}^{(y)} - f_{n-r}\right\}$ y $\{y_{r+1} - x_{r+1}, \ldots, y_n - x_n\}$ en el anillo $k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$.

Proposición 39 $\det(d_{ij})$ *es un generador de* $\mathrm{Ann}(\ker \mu)$.

Dem.-Identificando los generadores del $\ker \mu$ de la forma $1 \otimes s - s \otimes 1$ con los polinomios

$$s^{(y)} - s = \sum_{l=1}^{n-r} a_l (y_{r+l} - x_{r+l})$$

donde $a_l \in k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$.
Se tiene entonces que $\ker \mu$ está generado por la sucesión regular $y_{r+1} - x_{r+1}, \ldots, y_n - x_n$ sobre $k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$.
Por lo tanto $\mathrm{Ann}(\ker \mu) = ((f_1^{(y)} - f_1, \ldots, f_{n-r}^{(y)} - f_{n-r}) : (y_{r+1} - x_{r+1}, \ldots, y_n - x_n)) = (\det(d_{ij}))$, gracias a la escritura (16) y al Teorema de Wiebe. ■

Observar que, como $\det(d_{ij})$ no depende de la escritura (19), entonces la traza asociada vía el isomorfismo Φ sólo depende de la sucesión regular. Tiene sentido , entonces, llamar a esta traza *la traza asociada a la sucesión regular.*

Vamos a ver que la traza σ construida en la Proposición 35 es la traza asociada a la sucesión regular $f_1, \ldots, f_{n-r}$.
Como antes, para comenzar estudiamos el caso de una variable:

Proposición 40 *Sean R un anillo íntegro y $g \in R[x]$ un polinomio mónico en x no unidad. Entonces la traza de Tate $\sigma_0 : S := R[x]/(g) \to R$ definida por $\sigma_0(s) := b_{d-1}$ si $s = b_{d-1}\bar{x}^{d-1} + \ldots + b_0$ resulta la traza asociada a la sucesión regular g.*

Dem.- Sea $g = x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in R[x]$.
Escribimos $g^{(y)} - g = y^d - x^d + a_{d-1}(y^{d-1} - x^{d-1}) + \ldots + a_1(y - x)$. Por lo tanto, $g^{(y)} - g = (\sum_{j=0}^{d-1} y^j x^{d-1-j} + a_{d-1} \sum_{j=0}^{d-2} y^j x^{d-2-j} + \ldots + a_1)(y - x)$.
El $\det(d_{ij})$ de la proposición anterior, en este caso, es

$$\sum_{j=0}^{d-1} y^j \otimes x^{d-1-j} + a_{d-1} \sum_{j=0}^{d-2} y^j \otimes x^{d-2-j} + \ldots + a_1 \in S \otimes_R S.$$

Veamos que la traza que se induce vía Φ es σ_0.
Calculamos $\Phi(\det(d_{ij})(\sigma_0) = \sum_{j=0}^{d-1} \sigma_0(\bar{x}^j)x^{d-1-j} + a_{d-1} \sum_{j=0}^{d-2} \sigma_0(\bar{x}^j)\bar{x}^{d-2-j} + \ldots + a_1\sigma_0(1) = 1$. Como Φ es un isomorfismo, debe ser σ_0 la traza asociada a la sucesión regular. ■

Generalizando lo anterior al producto de trazas de Tate, obtenemos:

Proposición 41 *Sea $S' := R[x_{r+1}]/(g_1) \otimes_R \ldots \otimes_R R[x_n]/(g_{n-r})$ con $g_i \in R[x_{r+i}]$ mónico en la variable x_{r+i}. Sea σ_i' la traza de Tate para $S_i' := R[x_{r+i}]/(g_i)$. Entonces $\sigma' \in (S')^*$ definida por $\sigma'(s_1 \otimes \ldots \otimes s_{n-r}) := \sigma_1'(s_1) \ldots \sigma_{n-r}'(s_{n-r})$ resulta la traza asociada a la sucesión regular $g_1, \ldots, g_{n-r}$.*

Dem.- Para cada g_i, $i = 1, \ldots, n - r$, se tiene la escritura

$$g_i^{(y)} - g_i = a_{ii}(y_{r+i} - x_{r+i})$$

donde $a_{ii} \in R[x_{r+i}, y_{r+i}]$ y $a_{ij} = 0$ para $i \neq j$. Consideramos $\det(a_{ij})$ como un elemento de $S' \otimes_R S'$ y lo llamamos Δ. Resulta $\Delta = a_{11} \dots a_{n-rn-r}$.
Notemos que a_{ii} es el $\det(d_{ij})$ de la proposición anterior en $S_i' \otimes S_i'$. Por lo tanto, $\Phi_i(a_{ii})(\sigma_i') = 1$, donde $\Phi_i : \mathrm{Ann}(\ker \mu) \to \mathrm{Hom}_{S_i}(S_i^*, S_i)$. Calculamos $\Phi(a_{11} \dots a_{n-rn-r})(\sigma') = \Phi_1(a_{11})(\sigma_1') \cdots \Phi_{n-r}(a_{n-rn-r})(\sigma_{n-r}') = 1$. ■

Ahora, pasamos al caso general.

Teorema 42 *Sea $\sigma_f \in S^*$ la traza asociada a la sucesión regular $f_1, \dots, f_{n-r}$. Entonces*

$$\sigma_f = \sigma$$

donde σ es la traza definida en el Teorema 35 de la sección anterior .

Dem.-
En otras palabras, si, como antes, $\overline{\det(d_{ij})} = \sum \overline{a_m} \otimes \overline{b_m}$ definido en (19), hay que probar la igualdad en S:

$$1 = \sum \overline{a_m} \sigma \left(\overline{b_m}\right) \tag{20}$$

donde $\overline{a_m} \in k[x_1, \dots, x_n]/(f_1, \dots, f_{n-r})$ y $\overline{b_m} \in k[x_1, \dots, x_r, y_{r+1}, \dots, y_n]/\left(f_1^{(y)}, \dots, f_{n-r}^{(y)}\right)$.
Es decir que $\Phi(\det(d_{ij}))(\sigma) = 1$.
Usando la definición de σ, la fórmula (20), se puede reescribir

$$1 = \sum \overline{a_m} \sigma' \left(\overline{\det(a_{ij}) b_m}\right) \tag{21}$$

donde $\overline{\det(a_{ij}) b_m}$ es la clase de $\det(a_{ij}) b_m$ en el anillo S'.
De acuerdo a la proposición anterior, la traza σ' es también la traza asociada a la sucesión regular $g_1, \dots, g_{n-r}$ y por lo tanto, se construye así: para cada i, con $1 \leq i \leq n-r$ se escribe

$$g_i = \sum_{k=1}^{n-r} a_{ik} f_k$$

con $a_{ik} \in k[x_1, \dots, x_n]$ y, por lo tanto,

$$g_i^{(y)} - g_i = \sum_{k=1}^{n-r} a_{ik}^{(y)} f_k^{(y)} - \sum_{k=1}^{n-r} a_{ik} f_k.$$

Sumando y restando $\sum_{k=1}^{n-r} a_{ik}^{(y)} f_k$ queda

$$g_i^{(y)} - g_i = \sum_{k=1}^{n-r} a_{ik}^{(y)} \left(f_k^{(y)} - f_k\right) + \sum_{k=1}^{n-r} \left(a_{ik}^{(y)} - a_{ik}\right) f_k.$$

Usando la escritura $f_k^{(y)} - f_k = \sum_{j=1}^{n-r} d_{kj}(y_{r+j} - x_{r+j})$ para cada $k = 1, \ldots, n-r$, se tiene para cada $i = 1, \ldots, n-r$:

$$g_i^{(y)} - g_i = \sum_{k=1}^{n-r} a_{ik}^{(y)} \left(\sum_{j=1}^{n-r} d_{kj}(y_{r+j} - x_{r+j}) \right) + \sum_{k=1}^{n-r} \left(a_{ik}^{(y)} - a_{ik} \right) f_k$$

Reescribiendo la primera sumatoria:

$$g_i^{(y)} - g_i = \sum_{j=1}^{n-r} \left(\sum_{k=1}^{n-r} a_{ik}^{(y)} d_{kj} \right) (y_{r+j} - x_{r+j}) + \sum_{k=1}^{n-r} \left(a_{ik}^{(y)} - a_{ik} \right) f_k.$$

Por otro lado, se puede escribir $a_{ik}^{(y)} - a_{ik}$ de la forma $\sum_{j=1}^{n-r} h_{ikj}(y_{r+j} - x_{r+j})$ con $h_{ikj} \in k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$ y, llamando $\beta_{ij} := \sum_{k=1}^{n-r} a_{ik}^{(y)} d_{kj}$, queda la identidad:

$$\begin{aligned} g_i^{(y)} - g_i &= \sum_{j=1}^{n-r} \beta_{ij}(y_{r+j} - x_{r+j}) + \sum_{k=1}^{n-r} \left(\sum_{j=1}^{n-r} h_{ikj}(y_{r+j} - x_{r+j}) \right) f_k = \\ &= \sum_{j=1}^{n-r} \left(\beta_{ij} + \sum_{k=1}^{n-r} h_{ikj} f_k \right) (y_{r+j} - x_{r+j}). \end{aligned}$$

en el anillo $k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$.
Observemos también que la matriz $(\beta_{ij})_{ij}$ es el producto de las matrices $\left(a_{ij}^{(y)}\right)_{ij}$ y $(d_{ij})_{ij}$.
En otras palabras, el elemento

$$\det \left(\beta_{ij} + \sum_{k=1}^{n-r} h_{ikj} f_k \right), \tag{22}$$

al dividir por el ideal generado por los polinomios g_i y $g_i^{(y)}$, induce un generador Δ' de $\mathrm{Ann}(\ker \mu')$, donde $\mu' : S' \otimes_R S' \to S'$ es la multiplicación.
Escribiendo (22) de la forma $\sum p_t q_t$ con $p_t \in k[x_1, \ldots, x_n]$ y $q_t \in k[x_1, \ldots, y_{r+1}, \ldots, y_n]$, se tiene $\Delta' = \sum \overline{p_t} \otimes \overline{q_t}$ donde la barra denota clase en S'.
Observemos que $\sum p_t q_t - \det(\beta_{ij})$ pertenece al ideal generado por los polinomios f_i en el anillo $k[x_1, \ldots, y_{r+1}, \ldots, y_n]$ y por lo tanto $\sum p_t q_t$ puede escribirse de la forma $\det(\beta_{ij}) + \sum \widetilde{p}_u \widetilde{q}_u$ con $\widetilde{p}_u \in (f_1, \ldots, f_{n-r})\, k[x_1, \ldots, x_n]$ y $\widetilde{q}_u \in k[x_1, \ldots, x_r, y_{r+1}, \ldots, y_n]$.
Teniendo en cuenta que $(\beta_{ij})_{ij} = \left(a_{ij}^{(y)}\right)_{ij} (d_{ij})_{ij}$ se tiene entonces

$$\det \left(\beta_{ij} + \sum_{k=1}^{n-r} h_{ikj} f_k \right) = \sum p_t q_t = \det(a_{ij}^{(y)}) \det(d_{ij}) + \sum \widetilde{p}_u \widetilde{q}_u, \tag{23}$$

con $\widetilde{p}_u \in (f_1, \ldots, f_{n-r})\, k[x_1, \ldots, x_n]$ y $\widetilde{q}_u \in k[x_1, \ldots, x_r, y_{r+1}, \ldots, y_n]$.
Escribiendo $\det(d_{ij}) = \sum a_m b_m$ con $a_m \in k[x_1, \ldots, x_n]$ y $b_m \in k[x_1, \ldots, y_{r+1}, \ldots, y_n]$ (por definición de los a_m y b_m), se tiene que (23) puede escribirse así:

$$\det \left(\beta_{ij} + \sum_{k=1}^{n-r} h_{ikj} f_k \right) = \sum a_m \det(a_{ij}^{(y)}) b_m + \sum \widetilde{p}_u \widetilde{q}_u \tag{24}$$

con los $\widetilde{p}_u$ y $\widetilde{q}_u$ como arriba.
En virtud de la fórmula (24) y dado que σ' coincide la traza asociada a $g_1,\ldots,g_{n-r}$ se sabe que vale la siguiente identidad en S':

$$1 = \sum \overline{a_m}\sigma'\left(\overline{\det(a_{ij})b_m}\right) + \sum \widetilde{\overline{p}_u}\sigma'\left(\widetilde{\overline{q}_u}\right) \tag{25}$$

donde las barras indican tomar las clases en $k[x_1,\ldots,x_n]$ módulo el ideal $(g_1,\ldots,g_{n-r})$. Finalmente, mirando la fórmula (25) y pasando al cociente módulo el ideal $(f_1,\ldots,f_{n-r})$ queda:

$$1 = \sum \overline{a_m}\sigma'\left(\overline{\det(a_{ij})b_m}\right) = \sum \overline{a_m}\sigma\left(\overline{b_m}\right)$$

donde ahora las barras significan tomar las clases módulo $(f_1,\ldots,f_{n-r})$. De esta manera quedan demostradas las relaciones (21) y (20) y así σ es la traza asociada a la sucesión regular $f_1,\ldots,f_{n-r}$. ■

Resumiendo, tenemos:

Teorema 43 *Dados los polinomios $f_1,\ldots,f_{n-r}$ en $k[x_1,\ldots,x_n]$ que forman una sucesión regular, consideramos $R := k[x_1,\ldots,x_r]$ y $S := k[x_1,\ldots,x_n]/(f_1,\ldots,f_{n-r})$ con las variables en posición de Noether. Entonces existe una familia finita de polinomios a_m, c_m en $k[x_1,\ldots,x_n]$ tales que $\Delta := \sum_{m=1}^{M} \bar{a}_m \otimes \bar{c}_m$ es un generador de $\mathrm{Ann}_{S\otimes S}(\ker\mu)$ y una traza σ (que verifica la "fórmula de la traza"):*

$$\text{para todo } s \in S,\ s = \sum a_m \sigma(c_m s).$$

En particular ambas familias $(\bar{a}_m)_m$ y $(\bar{c}_m)_m$ son sistemas de generadores de S sobre R. En el caso en que usamos el desarrollo de Taylor de $f_i^{(y)} - f_i$, los polinomios $\bar{a}_m$ y $\bar{c}_m$ verifican la desigualdad $\deg(a_m) + \deg(c_m) \leq (n-r)(d-1)$ y $M < 3(nd)^{n-r}$. ■

III.2 Una cota superior para el grado de la traza

Sea σ la traza asociada a la sucesión regular $f_1,\ldots,f_{n-r}$ introducida en el Teorema 43 y en el Teorema 35. En esta sección estimaremos una cota superior para el grado de $\sigma(\overline{f})$ que involucra los parámetros $\deg(f), d, n, r$ y $\deg(V)$. Calculamos primero cotas de grado para las ecuaciones de dependencia entera [15, Prop.1.12]):

Proposición 44 *Existen polinomios $g_1,\ldots,g_{n-r}$ tales que cada g_i pertenece a $R[x_{r+i}] \cap (f_1,\ldots,f_{n-r})$, para $i = 1,\ldots,n-r$ y es mónico en la variable x_{r+i}. Es claro que estos polinomios forman una sucesión regular en $k[x_1,\ldots,x_n]$ y que si $S' := k[x_1,\ldots,x_n]/(g_1,\ldots,g_{n-r})$, entonces $R \hookrightarrow S'$ es un morfismo entero e inyectivo. Además se verifica que los grados de los g_i están acotados por $\deg(V)d^n$.*

Dem.- De [50, Prop.1], para cada $i = 1,..,n-r$, existe un polinomio $q_i \in R[x_{r+i}] \cap \sqrt{(f_1,\ldots,f_{n-r})}$, mónico en x_{r+i}, cuyo grado total es acotado por $\deg(V)$. Así, siguiendo [35] o [15, Remark 1.6], $g_i := q_i^{d^n}$ verifica lo pedido. ■

Con las notaciones de la sección anterior, sea $S' := k[x_1,\ldots,x_n]/(g_1,\ldots,g_{n-r})$. Para cada índice i, $i=1,\ldots,n-r$, denotamos por S'_i al anillo $R[x_{r+i}]/(g_i)$. En este caso la traza considerada σ'_i es la traza de Tate (ver Proposición 33 y Proposición 34).
Por lo tanto, para cualquier polinomio $f \in R[x_{r+i}]$, si $\overline{f}$ es su clase en S'_i después de la división por g_i, tenemos que $\sigma'_i(\overline{f})$ es el coeficiente principal de $\overline{f}$ (mirado como un polinomio en x_{r+i}). Así, gracias al algoritmo de Euclides, deducimos la desigualdad (ver Subrutina **C**):

$$\deg \sigma'_i(\overline{f}) \leq \deg(g_i)\deg(f). \tag{26}$$

Ahora, estamos en condiciones de estimar el grado de $\sigma'(\overline{f})$, con $\overline{f} \in S'$:

Proposición 45 *Para cada $\overline{f} \in S'$, se tiene la siguiente desigualdad:*

$$\deg \sigma'(\overline{f}) \leq \deg(f) d^n \deg(V).$$

Proof.- Es claro que $S' \simeq S'_1 \otimes_R S'_2 \otimes_R \ldots \otimes_R S'_{n-r}$ por medio de la correspondencia natural:

$$\sum_\beta a_\beta\, x_{r+1}^{\beta_1}\ldots x_n^{\beta_{n-r}} \mapsto \sum_\beta a_\beta\, x_{r+1}^{\beta_1} \otimes \ldots \otimes x_n^{\beta_{n-r}},\ a_\beta \in R$$

que baja al cociente.
Por la definición de σ' dada en la sección anterior,

$$\sigma'(\overline{f}) = \sum_\beta a_\beta\, \sigma'_1(\overline{x}_{r+1}^{\beta_1})\ldots\sigma'_{n-r}(\overline{x}_n^{\beta_{n-r}}),$$

para cada $f = \sum a_\beta\, x_{r+1}^{\beta_1}\ldots x_n^{\beta_{n-r}} \in k[x_1,\ldots,x_n]$.
Entonces, de la Proposición 44 y la desigualdad (26), se obtiene la siguiente cota de grado:

$$\begin{aligned}
\deg \sigma'(\overline{f}) &\leq \max_\beta \left\{\deg(a_\beta) + \deg(\sigma'_1(\overline{x}_{r+1}^{\beta_1})) + \cdots + \deg(\sigma'_{n-r}(\overline{x}_n^{\beta_{n-r}}))\right\} \\
&\leq \max_\beta \{\deg(a_\beta) + \deg(g_1)\beta_1 + \cdots + \deg(g_{n-r})\beta_{n-r}\} \\
&\leq \max_\beta \{\deg(a_\beta) + d^n\deg(V)\beta_1 + \cdots + d^n\deg(V)\beta_{n-r}\} \\
&\leq \deg(f) d^n \deg(V). \blacksquare
\end{aligned}$$

De esta proposición inferimos una cota superior de grado para la traza σ como sigue:

Teorema 46 *Sean $R := k[x_1,\ldots,x_r]$ y $S := k[x_1,\ldots,x_n]/(f_1,\ldots,f_{n-r})$. Sea $\sigma \in S^*$ la traza asociada a la sucesión regular (Definición 38). Entonces, para cada $\overline{f} \in S$, se tiene la siguiente desigualdad:*

$$\deg \sigma(\overline{f}) \leq \{\deg(f) + (n-r)\left(d^{n-r} + d^n \deg(V)\right)\} d^n \deg(V).$$

Dem.- Dado que el ideal $(g_1,\ldots,g_{n-r})$ está contenido en $(f_1,\ldots,f_{n-r})$, existen polinomios $a_{ij} \in k[x_1,\ldots,x_n]; i,j = 1,\ldots,n-r$ cuyos grados están acotados por $d^{n-r} + d^n\deg(V)$, tales que

$$g_j = \sum_{i=1}^{n-r} a_{ij} f_i$$

(ver [15, Theorem 5.1]).
Por nuestra definición, para cada polinomio $f \in k[x_1, \ldots, x_n]$ se tiene la identidad en $k[x_1, \ldots, x_r]$:

$$\sigma(\overline{f}) = \sigma'\left(\overline{\det(a_{ij})}\,\overline{f}\right)$$

donde las barras denotan clases en los anillos S y S' respectivamente (ver Teorema 35). La Proposición 45 y los argumentos de arriba conducen a la cota de grado enunciada para $\sigma(\overline{f})$ como sigue:

$$\begin{aligned}\deg \sigma(\overline{f}) = \deg \sigma'\left(\overline{\det(a_{ij})}\,\overline{f}\right) &\leq \deg(\det(a_{ij})f)d^n \deg(V) \leq \\ &\leq (\deg(f) + (n-r)\max_{ij}\deg(a_{ij}))d^n \deg(V) \leq \\ &\leq \{\deg(f) + (n-r)(d^{n-r} + d^n \deg(V))\}d^n \deg(V). \blacksquare\end{aligned}$$

Observación Cuando $(f_1, \ldots, f_{n-r})$ es un ideal radical de $k[x_1, \ldots, x_n]$, las cotas que acabamos de obtener pueden mejorarse. De hecho, en este caso, en la Proposición 44 tenemos $\deg(g_i) \leq \deg(V)$ para todo $i = 1, \ldots, n-r$ (ver [50, Prop.1]), y así en el Teorema 46, se obtendría la desigualdad:

$$\deg \sigma(\overline{f}) \leq \{\deg(f) + (n-r)(d^{n-r} + \deg(V))\}\deg(V).$$

De todos modos, en este caso se puede obtener una cota más precisa (ver [50, Theorem 10]):

$$\deg \sigma(\overline{f}) \leq (1 + \max\{\deg(f), (n-r)d\})\deg(V).$$

Parte IV
Construcción de bases en anillos intersección completa en posición de Noether

IV.1 Cotas de grado para una base

Recordamos la notación de la sección anterior: k es un cuerpo perfecto y $x_1, \ldots, x_n$ son indeterminadas sobre k. Sea $f_1, \ldots, f_{n-r}$ una sucesión regular de polinomios en $k[x_1, \ldots, x_n]$ de grados acotados por un entero d. Denotamos al anillo $k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-r})$ por S y por $R := k[x_1, \ldots, x_r]$, y asumimos que el morfismo canónico $R \to S$ es entero e inyectivo.
En esta sección aplicaremos las herramientas de teoría de trazas introducidas anteriormente para acotar los grados de una R-base de un anillo intersección completa S. Lo haremos considerando una matriz de una proyección cuya imagen es isomorfa a S.
Siguiendo las notaciones de la Proposición 43, sea $F \in R^{M \times M}$ la matriz cuyas entradas están definidas por $F_{ij} := \sigma(\overline{a_i c_j})$ (donde σ es la traza asociada a la sucesión regular $f_1, \ldots, f_{n-r}$, ver Proposición 38). El siguiente lema nos permite aplicar el Teorema 25 de la sección 2 a la matriz F:

Lema 47 *La matriz $F \in R^{M \times M}$ es la matriz de una proyección cuyas entradas son polinomios de grados acotados por $D := 3(n-r)d^{4n-2r}$.*

Dem.- Para probar que F es la matriz de una proyección, es suficiente mostrar que $F^2 = F$. De la R-linealidad de σ y de la fórmula de la traza (Proposición 43) tenemos:

$$(F^2)_{ij} = \sum_{k=1}^{M} \sigma(\overline{a}_i \overline{c}_k)\sigma(\overline{a}_k \overline{c}_j) = \sigma((\sum_{k=1}^{M} \sigma(\overline{a}_i \overline{c}_k)\overline{a}_k)\overline{c}_j) = \sigma(\overline{a}_i \overline{c}_j) = F_{ij}.$$

Las cotas de grado obtenidas en el Teorema 46 y en la Proposición 43, además de la desigualdad de Bezout, nos conducen a las cotas de grado enunciadas como sigue:

$$\begin{aligned} \deg(F_{ij}) = \deg \sigma(\overline{a}_i \overline{c}_j) &\leq \{\deg(a_i c_j) + (n-r)(d^{n-r} + d^n \deg(V))\} d^n \deg(V) \leq \\ &\leq \{(n-r)(d-1) + (n-r)(d^{n-r} + d^n \deg(V))\} d^n \deg(V) \\ &\leq 3(n-r)d^{4n-2r}. \blacksquare \end{aligned}$$

El siguiente teorema relaciona explícitamente cada base de la imagen de la proyección F con otra de S. Esta relación nos permite estimar grados de una base de S por medio del Teorema 25:

Teorema 48 *Sea $w_k = (w_{k1}, \ldots, w_{kM}) \in R^M$, $1 \leq k \leq s$, una $R-$base de $\mathrm{Im}(F)$, entonces los elementos $\sum_{j=1}^{M} w_{kj}\overline{c_j}$, with $1 \leq k \leq s$, forman una $R-$base de S.*

En particular, existe una R-base de S cuyos elementos son las clases de polinomios en $k[x_1,\ldots,x_n]$ con grados acotados por $(nd)^{O((n-r)r)}$.

Dem.- Consideremos el siguiente diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}\,(F) & \longrightarrow & R^M & \xrightarrow{F} & \mathrm{Im}\,(F) & \longrightarrow & 0 \\ & & \mathrm{id}\downarrow & & \mathrm{id}\downarrow & & \varphi\downarrow & & \\ 0 & \longrightarrow & \mathrm{Ker}\,(G) & \longrightarrow & R^M & \xrightarrow{G} & S & \longrightarrow & 0 \end{array}$$

donde $G: R^M \to S$ es el morfismo que manda cada elemento e_i de la base canónica de R^M a $\overline{c_i} \in S$ y φ es la aplicación definida por $\varphi(w) := \sum_{j=1}^{M} w_j \overline{c_j}$ para cualquier $w = (w_1,\ldots,w_M) \in \mathrm{Im}\,(F)$. Observemos que G es un epimorfismo porque los elementos $\overline{c_i}$ son un sistema de generadores de S sobre R (Proposición 43).
Por la fórmula de la traza (38)tenemos para cada e_i la siguiente igualdad:

$$\varphi(F(e_i)) = \varphi(\sigma(\overline{a_1 c_i}),\ldots,\sigma(\overline{a_M c_i})) = \sum_{j=1}^{M} \sigma(\overline{a_j c_i})\,\overline{c_j} = \overline{c_i} = G(e_i).$$

Por otro lado, $(w_1,\ldots,w_M) \in \mathrm{Ker}\,(F)$ si y sólo si $\sum_{j=1}^{M} \sigma(\overline{a_i c_j})\, w_j = 0$ para todo $i = 1,\ldots,M$, o equivalentemente $\sigma\left(\overline{a_i}\sum_{j=1}^{M}\overline{c_j} w_j\right) = 0$ para todo $i = 1,\ldots,M$. De la fórmula de la traza (38) esta relación implica que $\sum_{j=1}^{M}\overline{c_j} w_j = 0$, en otras palabras $(w_1,\ldots,w_M) \in \mathrm{Ker}\,(G)$. Resumiendo, vimos que $\mathrm{Ker}\,(F) = \mathrm{Ker}\,(G)$.
De este modo el diagrama anterior resulta conmutativo. Por lo tanto φ es un isomorfismo y si $w_1,\ldots,w_s \in R^M$ es una $R-$base de $\mathrm{Im}\,(F)$, los elementos $\varphi(w_1),\ldots,\varphi(w_s)$ forman una $R-$base de S.
Para finalizar la demostración, resta ver la existencia de una base de S con las cotas de grado enunciadas.
Aplicando el Teorema 25 a la matriz de la proyección F, se obtiene una $R-$base de $\mathrm{Im}\,(F)$ formada por vectores polinomiales w_k con coordenadas w_{ki} den grados acotados por $(MD)^{O(r)}$ (recordar que $R = k[x_1,\ldots,x_r]$ y D es la cota superior para los grados de las entradas de F obtenida en Lema 47). Tomando en cuenta que $M \leq 3(nd)^{n-r}$ (Proposición 43), tenemos:

$$(MD)^{O(r)} < \left(3(nd)^{n-r}\, 3(n-r)d^{4n-2r}\right)^{O(r)} = (nd)^{O((n-r)r)}.$$

Así, mediante el isomorfismo φ, los elementos $\left(\sum_{j=1}^{M} w_k^j \overline{c_j}\right)$ son una base de S y tenemos las siguientes cotas de grado para sus representantes en $k[x_1,\ldots,x_n]$:

$$\deg\left(\sum_{j=1}^{M} w_k^j c_j\right) \leq \max_{kj} \deg\left(w_k^j c_j\right) \leq (nd)^{O((n-r)r)} + (n-r)(d-1) = (nd)^{O((n-r)r)}. \quad \blacksquare$$

IV.2 Cómputo de bases en tiempo simplemente exponencial

A lo largo de esta sección mantendremos las notaciones introducidas previamente: k es un cuerpo perfecto y $x_1, \ldots, x_n$ son indeterminadas sobre k. Sea $f_1, \ldots, f_{n-r}$ una sucesión regular de polinomios en $k[x_1, \ldots, x_n]$ de grados acotados por un entero d y dados por un slp de tamaño ℓ, que definen una variedad V . Denotamos por S al anillo $k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-r})$ y por $R := k[x_1, \ldots, x_r]$, y asumimos que el morfismo canónico $R \to S$ es entero e inyectivo.
Bajo estas hipótesis S es un $R-$módulo libre de rango $\eta \leq d^{n-r} \leq d^n$ (ver por ejemplo [27, Corollary 3.3.2] o [2, Corollary 6]). El objetivo de esta sección es el cálculo de polinomios en $k[x_1, \ldots, x_n]$ cuyas clases sean una $R-$base de S (ver Teorema 54).
Para esto, siguiendo el Teorema 48 y el Teorema 25, es suficiente construir explícitamnete la matriz de la proyección F con entradas en R, introducidas al comienzo de la Parte IV.
El primer paso será dar una versión efectiva de la Proposición 43 con el fin de construir los polinomios $a_m, c_m \in k[x_1, \ldots, x_n]$. Recordemos que estos polinomios no están unívocamente determinados pero que deben verificar la identidad:

$$\det(l_{ij}) = \sum_m a_m(x_1, \ldots, x_r, x_{r+1}, \ldots, x_n) c_m(x_1, \ldots, x_r, y_{r+1}, \ldots, y_n). \tag{27}$$

A pesar de que los coeficientes $l_{ij} \in k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$ tampoco están unívocamnete determinados, satisfacen las relaciones:

$$f_i^{(y)} - f_i = \sum_{j=1}^{n-r} l_{ij} (y_{r+j} - x_{r+j}), \tag{28}$$

para todo $i = 1, \ldots, n-r$ (ver la fórmula (19)).
El desarrollo de Taylor de $f_i^{(y)} - f_i$ como polinomios con coeficientes en $k[x_1, \ldots, x_n]$ y variables $y_{r+1}, \ldots, y_n$ alrededor del punto $(x_{r+1}, \ldots, x_n)$ nos asegura la existencia de los polinomios l_{ij}, pero este método no es conveniente para nuestro punto de vista de la complejidad. Así, para construir los polinomios l_{ij}, podemos interpretar las relaciones (28) como un problema de la pertenencia efectivo de los polinomios $f_i^{(y)} - f_i$ con respecto al ideal generado por $(y_{r+j} - x_{r+j})$ en $k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$. Notemos que los polinomios que encontramos de este modo no son necesariamente los mismos que aquellos obtenidos del desarrollo de Taylor. En este punto podemos hacer uso del siguiente resultado de [26]:

Teorema 49 *([26, Theorem 19]) Sean $g_1, \ldots, g_s$ y g polinomios de $k[x_1, \ldots, x_n]$ tales que $g_1, \ldots, g_s$ forman una sucesión regular y g pertenece al ideal $(g_1, \ldots, g_s)$. Para $1 \leq j \leq s$ denotamos por $\delta_j := \deg(V(g_1, \ldots, g_j))$ al grado de la variedad afín definida por el ideal $(g_1, \ldots, g_j)$ que suponemos radical. Escribimos $\delta := \max_{1 \leq j \leq s-1} \{\delta_j\}$ y $e := \max_{1 \leq j \leq s} \{\deg(g_j)\}$. Suponemos que los polinomios $g_1, \ldots, g_s, g$ son dados por un slp de tamaño L. Entonces existe un algoritmo bien paralelizable que corre en tiempo secuencial $(se\delta L)^{O(1)}$ y computa polinomios $p_1, \ldots, p_s \in k[x_1, \ldots, x_n]$ con las propiedades siguientes:*

1. $g = p_1 g_1 + \cdots + p_s g_s$

2. $\max_{1\leq j\leq s}\{\deg(p_j)\} \leq \left(2s^2e + \max\{e, \deg(g)\}\right)\delta$

Más aun, los polinomios $p_1, \ldots, p_s$ *son dados por un slp de tamaño* $\deg^2(g)\,(se\delta L)^{O(1)}$.
■

Aplicando este teorema tenemos en nuestro caso:

Corolario 50 *Existe un algoritmo bien paralelizable que corre en tiempo secuencial* $((n-r)\,\ell)^{O(1)}$ *a partir de los polinomios de input* $f_1, \ldots, f_{n-r}$, *cuyo output es un slp de tamaño* $d^2\,((n-r)\,\ell)^{O(1)}$ *que evalúa una familia de polinomios* l_{ij}, $i, j = 1, \ldots, n-r$ *que satisfacen las relaciones (28) y* $\max_{ij}\{\deg(l_{ij})\} \leq 2(n-r)^2 + d$.

Dem.- Para cada índice fijo $i = 1, \ldots, n-r$, es fácil ver que los polinomios $g_j := y_{r+j} - x_{r+j}$, $j = 1, \ldots, n-r$, y $g := f_i^{(y)} - f_i$ verifican todas las hipótesis del teorema previo sobre el anillo de polinomios $k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$. Más aun, en este caso tenemos: $s = n-r$, $\delta = e = 1$, $\deg(g) = d$ y $L = 2\ell + 1$.
Así, podemos aplicar $(n-r)$ veces el Teorema 49 y obtener polinomios l_{ij} que verifican lo establecido en el corolario. ■

Con los polinomios l_{ij} obtenidos recién podemos computar los polinomios a_m, c_m como sigue:

Proposición 51 *Existe un algoritmo bien paralelizable que corre en tiempo secuencial* $\ell^{O(1)}\,((n-r)\,d)^{O(n-r)}$ *a partir de los polinomios de input* $f_1, \ldots, f_{n-r}$, *cuyo output es un slp del mismo tamaño que evalúa las dos familias de polinomios:* $a_m \in k[x_1, \ldots, x_r, x_{r+1}, \ldots, x_n]$ *y* $c_m \in k[x_1, \ldots, x_r, y_{r+1}, \ldots, y_n]$, $m = 1, \ldots, M := ((n-r)\,d)^{O(n-r)}$, *verificando lo enunciado en la Proposición 43.*

Dem.- Es suficiente encontrar una descomposición de $\det(l_{ij})$ como en la igualdad (27). El polinomio $\det(l_{ij})$ de grado acotado por $(n-r)\left(2(n-r)^2 + d\right)$ se puede hallar por medio de la subrutina **B** item 1, en tiempo $(d\,(n-r)\,\ell)^{O(1)}$ y está dado por un slp del mismo tamaño. Para obtener los polinomios a_m, c_m basta escribir $\det(l_{ij})$ en forma densa con respecto a las variables $y_{r+1}, \ldots, y_n$ mediante la subrutina **A**, obteniendo de este modo los polinomios $a_m \in k[x_1, \ldots, x_n]$ en tiempo $\ell^{O(1)}\,((n-r)\,d)^{O(n-r)}$ dado por un slp del mismo tamaño. Los polinomios c_m son los monomios correspondientesde grados acotados por $\deg(\det(l_{ij}))$ en las variables $y_{r+1}, \ldots, y_n$ y pueden ser evaluados en la manerra obvia por un slp de tamaño $(n-r)\log(\deg(\det(l_{ij}))) = (n-r)^{O(1)}\log(d)$. Como hay a lo sumo $\deg(\det(l_{ij}))^{(n-r)} = ((n-r)\,d)^{O(n-r)}$ monomios, obtenemos las cotas. ■

El paso siguiente es el cómputo de cada entrada ij, $\sigma(\overline{a_i c_j})$, de la matriz de la proyección F (donde σ es la traza asociada a la sucesión regular $f_1, \ldots, f_{n-r}$ como en la Definición 38). Este problema, la construcción explícita de la traza, ha sido considerado en artículos previos (ver por ejemplo [20, Lemma 3.4.1] y [36]) para obtener un Nullstellensatz efectivo eficiente; los resultados mostrados en esos papers son esencialmente suficientes para nuestro propósitos y por esto sólo repetiremos sus enunciados adaptados a nuestra situación.

Denotamos por $K := k(x_1, \ldots, x_r)$ al cuerpo de cocientes de R y $S' := S \otimes_R K \simeq k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/(f_1, \ldots, f_{n-r})$ (observar que bajo nuestras hipótesis S' es un $K-$espacio vectorial de dimensión $\eta = \mathrm{rank}_R(S)$). Sea $\sigma' := \sigma \otimes_R \mathrm{Id} : S' \to K$ la extensión canónica de la traza σ. El lema siguiente (ver [20, Section 3.4.1]) computa de forma explícita una $K-$ base de S' y la matriz de la aplicación σ' en esta base. Desafortunadamente este lema requiere la hipótesis adicional de que el anillo S sea radical para obtener un algoritmo bien paralelizable, si esta condición no es tenida en cuenta la complejidad secuencial sigue siendo simplemente exponencial pero la paralela se incrementa exponencialmente en n (ver también [20, Section 2.4.1]).

Lema 52 *Supongamos que la sucesión regular $f_1, \ldots, f_{n-r}$ genera un ideal radical. Entonces existe un algoritmo bien paralelizable que corre en tiempo $(n-r)\ell d^{O(n)}$ cuyo input son los polinomios $f_1, \ldots, f_{n-r}$, y cuyo output son los siguientes items:*

1. *un slp de tamaño $d^{O(n)}$ que evalúa un polinomio no nulo τ en R de grado $d^{O(n)}$,*
2. *un slp de tamaño $d^{O(n)}$ que evalúa una familia de polinomios $e_1 := 1, \ldots, e_\eta$ en $k[x_1, \ldots, x_n]$ tales que el conjunto $\mathcal{E}$ formado por sus clases $\overline{e_1}, \ldots, \overline{e_\eta}$ en S' es una $K-$base de S',*
3. *un slp de tamaño $d^{O(n)}$ que evalúa una familia de matrices polinomiales $M_{r+1}, \ldots, M_n$ en $R^{\eta \times \eta}$ tales que: los grados de sus entradas están acotados por $d^{O(n)}$ y $\frac{1}{\tau}M_{r+1}, \ldots, \frac{1}{\tau}M_n$ son las matrices de los $K-$endomorfismos de S', inducidos por la multiplicación por $\overline{x_{r+1}}, \ldots, \overline{x_n}$, en la base $\mathcal{E}$*
4. *un slp de tamaño $d^{O(n)}$ que evalúa una familia de polinomios $\theta_1, \ldots, \theta_\eta$ en R de grados $d^{O(n)}$ tales que la matriz de la traza extendida σ' de S' en la base $\mathcal{E}$ es la matriz $(\theta_1, \ldots, \theta_\eta)$.*

Dem.- Una demostración de este lema se puede encontrar en [20, Section 3.4.1] para el caso de polinomios de input dados en representación densa. Nuestra afirmación (inputs dados por un slp) se sigue inmediatamente de la Subrutina **A** que nos permite computar todos los coeficientes de los polinomios $f_1, \ldots, f_{n-r}$ en tiempo $(n-r)\ell d^{O(n)}$. ■

Mediante el lema anterior podemos construir explícitamente la matriz F:

Corolario 53 *Supongamos que la sucesión regular $f_1, \ldots, f_{n-r}$ genera un ideal radical. Entonces existe un algoritmo bien paralelizable que corre en tiempo $O(n)\,\ell d^{O(n)}$ a partir de los polinomios de input $f_1, \ldots, f_{n-r}$ cuyo output es un slp de tamaño $d^{O(n)}$ que evalúa las entradas de la matriz F.*

Dem.- Dado que las entradas de F son polinomios $\sigma(\overline{a_i c_j})$ es suficiente computarlos. De la Proposición 51, podemos computar los polinomios $a_i c_j$ como una suma de sus monomios (cuyos grados están acotados por $(n-r)(d-1)$). Por lo tanto, para computar $\sigma(\overline{a_i c_j})$ es suficiente computar la imagen vía σ de la clase de cada uno de estos monomios. Sin pérdida de generalidad, podemos computar $\sigma\left(\overline{\prod_{k=1}^{n} x_k^{\alpha_k}}\right)$.

Para cada $f \in k[x_1, \ldots, x_n]$, denotamos por M_f a la matriz en $K^{\eta \times \eta}$ asociada al endomorfismo de S' inducido por la multiplicación por $\overline{f}$ en la base $\mathcal{E}$ del Lema 52 item

2. En el caso particular de que $f := \prod_{k=1}^{n} x_k^{\alpha_k}$ tenemos que $M_f = \prod_{k=1}^{r} x_k^{\alpha_k} \prod_{k=r+1}^{n} M_{x_k}^{\alpha_k} = \prod_{k=1}^{r} x_k^{\alpha_k} \prod_{k=r+1}^{n} \frac{1}{\tau^{\alpha_k}} M_k^{\alpha_k}$, donde M_k son las matrices obtenidas por medio del Lema 52 (item 3). La primer columna de la matriz M_f es un vector de la forma $\left(\frac{\beta_1}{\tau^T}, \ldots, \frac{\beta_\eta}{\tau^T}\right)$ donde $T := \alpha_{r+1} + \cdots + \alpha_n$ y cada $\beta_t \in R$, $1 \leq t \leq \eta$, se puede computar explícitamente.
Como $\overline{e_1} = 1$, deducimos que $\overline{\prod_{k=1}^{n} x_k^{\alpha_k}} = \sum_{t=1}^{\eta} \frac{\beta_t}{\tau^T} \overline{e_t}$ y por lo tanto $\sigma\left(\overline{\prod_{k=1}^{n} x_k^{\alpha_k}}\right) = \sum_{t=1}^{\eta} \frac{\beta_t}{\tau^T} \theta_t \in R$.
El polinomio $\sum_{t=1}^{\eta} \frac{\beta_t}{\tau^T} \theta_t$ tiene grado $d^{O(n)}$ y está dado por un slp (con divisiones!) de tamaño $d^{O(n)}$. Evitando las divisiones mediante el procedimiento de Strassen (ver también [20, Section 2.2]), podemos computar en tiempo $O(r)\, d^{O(n)}$ un slp sin divisiones de tamaño $d^{O(n)}$ que evalúa dicho polinomio.
Finalmente, agregando todos los costos de complejidad, obtenemos el tiempo secuencial establecido. ■

Ahora, con lo hecho hasta aquí, estamos en condiciones de calcular una R-base de S:

Teorema 54 *Supongamos que la sucesión regular $f_1, \ldots, f_{n-r}$ genera un ideal radical. Entonces existe un algoritmo bien paralelizable que corre en tiempo $O(n)\, \ell d^{O(n^2)}$ a partir de los polinomios de input $f_1, \ldots, f_{n-r}$ cuyo output es un slp de tamaño $d^{O(n^2)}$ que evalúa una familia de polinomios en $k[x_1, \ldots, x_n]$ de grados acotados por $nd^{O(n^2)}$, cuyas clases en S forman una base de este módulo sobre R.*

Dem.- Después de aplicar el algoritmo del Teorema 25 a la matriz F, obtenida en el corolario anterior, obtenemos una R-base $\{w_1, \ldots, w_s\}$ de la imagen de F en tiempo $O(n)\, \ell d^{O(n^2)}$, donde cada w_k es un vector polinomial $(w_{k1}, \ldots, w_{kM})$, con $M := d^{O(n)}$. Sus coordenadas tienen grados acotados por $d^{O(n^2)}$ y están dados por un slp de tamaño $n^{O(1)} d^{O(n^2)}$.
Así, los polinomios $\sum_{j=1}^{M} w_{kj} \overline{c_j}$, $k = 1, \ldots, s$, son una R-base de S. ■

Observación: la hipótesis de que el anillo S sea reducido puede obviarse si no estamos interesados en la complejidad paralela (basta remitirse a la observación previa al Lema 52).

Referencias

[1] Almeida M., D'Alfonso L., Solernó P.: On the degrees of bases of free modules over a polynomial ring. Math. Zeitschrift **231**, 679-706 (1999)

[2] Armendáriz I., Solernó P.: On the computation of the radical of polynomial complete intersection ideals. In: G.Cohen, M.Giusti & T.Mora: Appl. Algebra, Algebraic Algorithms and

Error-Correcting Codes, AAECC-11, Paris 1995 (Lect. Notes Comp. Sci. **948**, pp. 106-119) Springer 1995

[3] Berenstein C. and Struppa D.: Recent improvements in the Complexity of the Effective Nullstellensatz. Linear Algebra and its Appl. **157** (1991) 203-215 (1991)

[4] Berenstein C. and Yger A.: Bounds for the degrees in the division problem. Mich. Math. J. **37** 25-43 (1990)

[5] Berkowitz S.: On computing the determinant in small parallel time using a small number of processors. Information Processing Letters **18** 147-150 (1984)

[6] Brownawell D.: Bounds for the degrees in the Nullstellensatz. Ann. of Math. Second Series **126** No.3 577-591 (1987)

[7] Bruns W., Vetter U.: Determinantal Rings (Lect. Notes Math. **1327**, Springer (1988)

[8] Bürguisser P., Clausen M., Amin Shokrollahi M.: Algebraic Complexity Theory (Grundlehren det matematischen Wissenschaften **315**) Springer 1997

[9] Caniglia L., Cortiñas G., Danón S., Heintz J., Krick T., Solernó P.: Algorithmic aspects of Suslin's Proof of Serre's Conjecture. Comput. Complexity **3**, Birkhäuser, 31-55 (1993)

[10] Caniglia L., Galligo A. and Heintz J.: Some new effectivity bounds in computational geometry. In: Proc. 6th Int. Conf. Applied Algebra, Algebraic Algorithms and Error Correcting Codes AAECC–6, Roma 1988, Springer Lect. Notes Comput.Sci. **357** 131-151 (1989)

[11] Caniglia L., Guccione J.A., Guccione J.J.: Local membership problems for polynomial ideals. Effective Methods in Algebraic Geometry MEGA 90, T. Mora and C. Traverso, eds., Progress in Mathematics Vol. **94**, Birkhäuser 31-45 (1991)

[12] Castro D., Giusti M., Heintz J., Matera G., Pardo L.: Universal Elimination Requires Exponential Running Time. Manuscrito (2001)

[13] Coleff N., Herrera M.: Les courants residuels associés à une forme meromorphe. (Lect. Notes Math **633**) Springer 1978

[14] Demazure M.: Le monoïde de Mayr et Meyer. Notes Informelles de Calcul Formel, Ecole Polytechnique, Palaiseau, 1984

[15] Dickenstein A., Fitchas N., Giusti M., Sessa C.: The membership problem for unmixed polynomial ideals is solvable in single exponential time. Discr. Appl. Math. **33** 73-94 (1991)

[16] Dickenstein A., Sessa C.: Duality methods for the membership problem. In: T.Mora & C.Traverso: Effective Methods in Alg. Geom. (MEGA '90) (Progr. Math. **94**, 89-103) Birkhäuser 1990

[17] Eisenbud D.: Commutative Algebra with a view toward Algebraic Geometry (Grad. Texts Math. **150**) Springer 1994

[18] Fitchas N., Galligo A.: Nullstellensatz effectif et Conjecture de Serre (théorème de Quillen-Suslin) pour le Calcul Formel. Math. Nachr. **149** 231-253 (1990)

[19] Fitchas N., Galligo A., Morgenstern J.: Precise secuential and parallel bounds for quantifier elimination over algebraically closed fields. J. Pure Appl. Algebra **67** 1-14 (1990)

[20] Fitchas N., Giusti M., Smietanski F.: Sur la complexité du théorème de zéros. In: J.Guddat et al: Approximation and Optimization in the Caribbean II, Proc. 2nd. Int. Conf. on Non-Linear Optimization and Approximation (Approximation and Optimization volume **8**, 247-329) Peter Lange Verlag 1995

[21] Gantmacher F.: Matrix Theory, Vol.I. Chelsea Publ. Co., New York 1960

[22] Giusti M., Heintz J.: Kronecker's smart, little black-boxes. To appear in Proceedings of Foundations of Computational Mathematics, Oxford 1999 (FoCM'99), A Iserles and R. De Vore, eds., Cambridge University Press, 2001

[23] Giusti M., Heintz J., Morais J., Pardo L.: When Polynomial Equation Systems Can Be "Solved" Fast ? In: G.Cohen, M.Giusti & T.Mora: Appl. Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-11, Paris 1995 (Lect. Notes Comp. Sci. **948**, pp. 205-231) Springer 1995

[24] Giusti M., Heintz J., Hägele K., Morais J.,Montaña J. L., Pardo L. M.: Lower bounds for diophantine approximation. J. Pure Appl. Algebra **117, 118** 277-317 (1997)

[25] Giusti M., Heintz J., Morais J., Pardo L.: Le role des structures de données dans les problems d'elimination. Comptes Rendus de l'Academie de Sciences de Paris **325** 1223-1228 (1997)

[26] Giusti M., Heintz J., Morais J., Morgenstern J., Pardo L.: Straight-line Programs in Geometric Elimination Theory. J. Pure Appl. Algebra **124** 101-146 (1998)

[27] Giusti M., Heintz J., Sabia J.: On the efficiency of effective Nullstellensatz. Comput. Complexity **3**, Birkhäuser, 56-95 (1993)

[28] Heintz J., Krick T., Puddu S., Sabia J., Waissbein A.: Deformation techniques for efficient polynomial equation solving. J. of Complexity **16 (1)** 70-109 (2000)

[29] Heintz J., Morgenstern J.: On the intrinsic complexity of elimination theory. J. of Complexity **9** 471-498 (1993)

[30] Hägele K., Morais J.E., Pardo L.M., Sombra M.: On the Intrinsic Complexity of the Arithmetic Nullstellensatz. J. of Pure and Appl. Algebra **146**, 103-183 (2000)

[31] Hartshorne R.: Residues and Duality. (Lect. Notes Math. **20**) Springer 1966

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

[33] Heintz J., Schnorr C.: Testing polynomials which are easy to compute. In: Logic and Algorithmic, an International Symposium held in Honour of E. Specker, Monographie **30** de l'Enseignement Mathématique, Genève, 237-254 (1982)

[34] Iversen B.: Generic local structure in Commutative Algebra (Lect. Notes Math. **310**) Springer 1973

[35] Kollár J.: Sharp effective Nullstellensatz. J. Amer. Math. Soc. **1** 963-975 (1988)

[36] Krick T., Pardo L.: A computational Method for Diophantine Approximation. In: Effective Methods in Alg. Geom. (MEGA '94) (Progr.Math. **143**, pp.193-253) Birkhäuser 1996

[37] Kunz E.: Introduction to Commutative Algebra and Algebraic Geometry. Birkhäuser 1985

[38] Kunz E.: Kähler Differentials (Adv. Lect. in Math.) Vieweg 1986

[39] Logar A., Sturmfels B.: Algorithms for Quillen-Suslin Theorem. J. Algebra **145** 231-239 (1992)

[40] Lam T.: Serre's Conjecture (Lect. Notes Math. **635**) Springer 1978

[41] Laudenbacher R., Woodburn C.: An algorithm for the Quillen-Suslin theorem for monoid rings. J. Pure Appl. Algebra **117** & **118** 395-429 (1997)

[42] Laudenbacher R., Schlauch K.: An algorithm for the Quillen-Suslin theorem for quotients of polynomial rings by monomial ideals. Preprint (1999)

[43] Matera G.: Probabilistic Algorithms for Geometric Elimination. Appl. Algebra in Eng., Communication and Comput. (AAECC Journal) **9**, 463-520 (1999)

[44] Mayr E., Meyer A.: The complexity of the word problem for commutative semigroups and polynomial ideals. Adv. Math. **46** 305-329 (1982)

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

[46] Mumford D.: Algebraic Geometry I: Complex Projective Varieties. Class. in Math. Springer (1995)

[47] Philippon P.: Dénominateurs dans le théorème des zéros de Hilbert. Acta. Arith. **58** 1-25 (1991)

[48] Puddu S., Sabia J.: An effective algorithm for quantifier elimination over algebraically closed fields using straight line programs. J. Pure Appl. Algebra **129**, 173-200 (1998)

[49] Rossi F., Spangher W.: Some effective methods in the openness of loci for Cohen-Macaulay and Gorenstein properties. In: T.Mora & C.Traverso: Effective Methods in Alg. Geom. (MEGA '90) (Progr. Math. **94**, pp. 441-455) Birkhäuser 1990

[50] Sabia J., Solernó P.: Bounds for traces in Complete Intersections and Degrees in the Nullstellensatz. AAECC Journal **6**, No.6, 353-376 Springer (1995)

[51] Shiffman B.: Degree bounds for the division problem in polynomial ideals. Michigan Math. J. **36** 163-171 (1989)

[52] Sombra M.: Bounds for the Hilbert function of polynomial ideal and for the degrees in the Nullstellensatz. J. of Pure and Appl. Algebra **117** & **118** 565-599 (1997)

[53] Teissier B.: Résultats récents d'algèbre commutative effective. Séminaire Bourbaki 1989-1990, Astérisque vol **189-190** 107-131 (1991)

[54] Vasconcelos W.: Computational Methods in Commutative Algebra and Algebraic Geometry (Algorithms and Computations in Math. 2) Springer 1998

[55] Von zur Gathen J.: Parallel arithmetic computations: a survey. Proc. 13th. Symp. MFCS 1986, Lect. Notes in Comp. Sci. 233, 93-112 (1986)