Complejidad para problemas de geometría elemental

Krick, Teresa Elena Genoveva

1990

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

Complejidad para problemas de geometría elemental

Teresa E.G. Krick

DIRECTOR DE TESIS
Dr. Joos Heintz

LUGAR DE TRABAJO
Facultad de Ciencias Exactas y Naturales (UBA)
Instituto Argentino de Matemática

Tesis presentada para optar al título de:
DOCTOR EN CIENCIAS MATEMATICAS
– 1990 –

Quiero ante todo expresar mi gratitud a mi director Joos Heintz. Este trabajo es sin duda el fruto de su entusiasmo contagioso y de su dedicación.

Al grupo Noaï Fitchas debo el haberme sentido tan rápidamente cómoda en este nuevo campo de la complejidad: a Pablo Solernó, mi compañero de trabajo, a Silvia Danón y a Leandro Caniglia, por todas las discusiones compartidas.

Bernd Bank fue quien, junto con Joos, me propuso trabajar en el tema de la programación entera y me planteó problemas existentes. Le quedo reconocida por ello.

Quiero agradecer también a todos los que de una manera u otra me ayudaron en esta empresa: a Enzo Gentile por haberme impulsado, a Marie-Francoise Roy, a Annemarie Fellmann, a mi padre y a mis amigos.

A Leticia Scoccia por su inmejorable trabajo, su paciencia y su buen humor.

Finalmente, quiero destacar que me siento en deuda con el CONICET por los cinco años de beca que me permitieron emprender este trabajo.

Teresa Krick

Buenos Aires, 6 de marzo de 1990.

INDICE

RESUMEN

I-a) Sea Ω un cuerpo algebraicamente cerrado y sea K un subcuerpo de Ω. $\mathcal{L}$ nota el lenguaje de primer orden de Ω a constantes en K.

Para cada fórmula prenexa $\Phi \in \mathcal{L}$, sean $F_1, \ldots, F_s \in K[X_1, \ldots, X_n]$ los polinomios que aparecen en Φ.

Se define

$|\Phi| :=$ longitud de Φ

$|D| := 2 + \sum_{1 \leq i \leq s} gr\, F_i$

$r :=$ número de bloques de cuantificadores de Φ

Se exhibe un algoritmo que elimina los cuantificadores de Φ, que funciona en tiempo secuencial $D^{n^{cr}}$ y en tiempo paralelo $n^{cr}(\log_2 D)^c$ (donde c es una constante universal adecuada).

Se muestra además que estas cotas son optimales.

b) Se aplica el algoritmo de (a) para el cálculo eficiente del polinomio de Chow del radical de un ideal polinomial homogéneo débilmente unmixed.

c) Se examina el algoritmo rápido de eliminación de cuantificadores sobre cuerpos real cerrados de J. Heintz, M.-F. Roy y P. Solernó para obtener cotas sobre los grados y el valor absoluto de los coeficientes de los polinomios que aparecen en la fórmula de salida.

II-a) Sean $F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$ polinomios cuasiconvexos de grado acotado por $d \geq 2$, y sea σ una cota para la longitud binaria de los coeficientes de $F_1, \ldots, F_s$. Se muestra que si el sistema $F_1 \leq 0, \ldots, F_s \leq 0$ admite una solución entera, entonces existe tal solución con longitud binaria acotada por $(sd)^{cn^2}\sigma$ (donde c es una constante universal). El caracter simplemente exponencial de la cota es intrínseco al problema.

b) Se utiliza (a) para resolver con cotas similares el problema de hallar el ínfimo del conjunto $\{F_0(x) : x \in \mathbb{Z}^n, F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ si éste se realiza, para un polinomio $F_0 \in \mathbb{Z}[X_1, \ldots, X_n]$ cuasiconvexo también.

INTRODUCCION

Este trabajo abarca cuestiones de complejidad para problemas de geometría elemental y se divide en dos partes:

I. Cotas para la eliminación de cuantificadores sobre cuerpos algebraicamente cerrados.

II. Una cota geométrica para la programación entera con restricciones polinomiales.

A continuación se presentan los resultados obtenidos en cada capítulo, sus antecedentes históricos y aplicaciones.

I. En el primer capítulo, se trata el problema de la complejidad (cotas superiores y cotas inferiores) de la eliminación de cuantificadores para el lenguaje de primer orden de los cuerpos algebraicamente cerrados. Se examinan también los algoritmos exhibidos recientemente por J. Heintz, M.-F. Roy y P. Solernó para el problema análogo en el caso de los cuerpos real cerrados, a fin de obtener estimaciones más precisas que se aplicarán luego en el Capítulo II.

   Se hace ahora una breve descripción del modelo con el que se trabaja a fin de enunciar más claramente los resultados obtenidos. Esta descripción será desarrollada con todo detalle en la sección "El modelo" del Capítulo I.

   Sean K un cuerpo arbitrario y Ω un cuerpo algebraicamente cerrado que lo contiene. Se entiende por *lenguaje de primer orden* $\mathcal{L}_K^\Omega$ del cuerpo Ω, a constantes en K, al conjunto de fórmulas que se obtienen como combinaciones booleanas $(\wedge, \vee, \neg)$ de polinomios (en varias variables y a coeficientes en K) igualados a cero, admitiéndose también los cuantificadores $\exists, \forall$ para modificar únicamente variables.

   Es un hecho clásico de la teoría de modelos que el lenguaje de primer orden de los cuerpos algebraicamente cerrados admite *eliminación de cuantificadores*; es decir para toda fórmula $\Phi \in \mathcal{L}_K^\Omega$, existe una fórmula $\Psi \in \mathcal{L}_K^\Omega$, sin cuantificadores, que describe el mismo subconjunto de Ω^m (donde m es el número de variables de Φ que no están acompañadas por ningún cuantificador).

   Más aún, en [He-Wü] se exhibe un algoritmo de eliminación de cuantificadores para el lenguaje de primer orden de los cuerpos algebraicamente cerrados, es decir se construye a partir de una fórmula Φ la formúla sin cuantificadores Ψ. En realidad, parece ser que

ya hacia 1940, A. Tarski conocía la existencia de algoritmos para ese problema aunque no lo describió explícitamente (ver [Tar]).

De ahí en más, se han ido realizando esfuerzos especiales para exhibir algoritmos de eliminación de cuantificadores cada vez más eficientes.

¿Pero qué se entiende por algoritmo?

La noción de *algoritmo* que más se adecua a este contexto es la de red aritmética definida en [Gat], que se puede representar por un grafo orientado donde en cada nodo se realiza una operación aritmética $(+,-,\cdot)$ o booleana, una comparación de elementos de Ω o una selección. Las entradas son únicamente elementos de K y los polinomios están codificados con representación densa, es decir por el vector de todos sus coeficientes, aún los nulos, permitiéndose para las comparaciones evaluar los polinomios en elementos de Ω.

Para cada red aritmética se tienen dos nociones de complejidad:

(i) la complejidad secuencial: el número de nodos del grafo correspondiente

(ii) la complejidad paralela: la longitud del camino más largo en el grafo correspondiente.

Se consideran los siguientes parámetros para medir una fórmula Φ de $\mathcal{L}_K^\Omega$

$|\Phi| :=$ longitud de $\Phi =$ número de símbolos necesarios para escribir Φ,

y si $F_1, \ldots, F_s \in K[X_1, \ldots, X_n]$ son todos los polinomios que aparecen en Φ:

$n :=$ número de variables

$$D := 2 + \sum_{1 \le i \le s} gr\, F_i$$

En el caso en que todos los cuantificadores aparecen al principio de Φ (fórmula prenexa) se considera también

$r :=$ número de bloques de cuantificadores distintos de Φ.

Las cotas superiores para la complejidad de la eliminación de cuantificadores en Ω presentadas en [He-Wü], [He] y [Wü] son *secuenciales* y doblemente exponenciales de tipo $D^{n^{cn}}|\Phi|$, donde c es una constante universal.

Además en [He] y [Wei] se muestra que la eliminación de cuantificadores para cuerpos algebraicamente cerrados tiene complejidad secuencial intrínsecamente doblemente exponencial en el modelo de representación densa de los polinomios. La única manera de mejorar los resultados consistió hasta hoy en mirar más en detalle los parámetros que

determinan las estimaciones en los algoritmos.

Basados en técnicas fundamentales de [Ch-Gr 1] y [He], en [Ch-Gr 2] y [Gr 1] se considera el problema para fórmulas prenexas y se obtienen las cotas (secuenciales) más precisas hasta la fecha. A saber, $D^{n^{cr}}|\Phi|$ (c constante universal), donde el carácter doblemente exponencial de la cota depende únicamente del número r de bloques de cuantificadores de Φ. Sin embargo la complejidad del algoritmo depende de propiedades aritméticas del cuerpo de constantes K (hecho que se debe a la utilización del subalgoritmos de factorización de polinomios).

Cabe señalar también que ninguno de los algoritmos mencionados arroja buenas cotas en paralelo (es decir cotas del orden del logaritmo en base 2 de las cotas secuenciales).

En el Teorema 2 del Capítulo I, se combinan versiones efectivas del Nullstellensatz (ver [Ko], [Ca 1], [Ph], [Br 2], [Ca-Gu-Gu], que afinaron los resultados de [Br 1], [Ca-Ga-He 1], [Ca-Ga-He 2]) con los métodos de [He] para construir un algoritmo de eliminación de cuantificadores con las mismas cotas secuenciales precisas que [Ch-Gr 2] ó [Gr 1]. Las ventajas son que no solamente se obtienen cotas de orden $n^{cr}D^c + c\log_2(|\Phi|)$ en paralelo (donde c es una constante universal), sino que además se evita que la complejidad dependa del cuerpo de constantes K.

Dado que el planteo de gran parte de los problemas interesantes de la geometría algebraica elemental involucra solamente un número chico de bloques de cuantificadores (por ejemplo resolución de sistemas de ecuaciones polinomiales sobre un cuerpo algebraicamente cerrado, cálculo de la dimensión o del grado de una variedad algebraica), las cotas obtenidas aquí muestran que estos problemas pueden ser resueltos computacionalmente en tiempo secuencial simplemente exponencial y en tiempo paralelo polinomial.

Con respecto a las cotas inferiores para la eliminación de cuantificadores, se muestra que las cotas superiores presentadas aquí son optimales como medida general de complejidad, en el modelo de representación densa de los polinomios, no sólo del punto de vista de la complejidad secuencial ([He], [Wü]) sino también del punto de vista de la complejidad paralela (Teorema 3, Capítulo I). Se exhibe una familia de fórmulas del lenguaje de primer orden de los cuerpos algebraicamente cerrados que verifica que *cualquier* algoritmo de eliminación de cuantificadores aplicado a estas fórmulas requiere tiempo secuencial doblemente exponencial y tiempo paralelo simplemente exponencial para representar o evaluar las fórmulas de salida. Por consiguiente los caracteres doblemente exponencial y simplemente exponencial de las cotas obtenidas son intrínsecos

al problema, siempre que se adopte la representación densa de los polinomios como modelo.

A raíz de este hecho, se está tratando de desarrollar por un lado la teoría de los *polinomios "esparsos"* (con pocos coeficientes no nulos) (ver [Be-Ti] y [Gr-Ka-Si]), y por otro lado la teoría de los *"straight-line programs"* (los polinomios no están dados por sus coeficientes sino por programas que permiten evaluarlos) (ver [He-Sch], [Kal]), pero en general no se han logrado resultados significativos.

En la segunda parte de este primer capítulo, se da un algoritmo eficiente para calcular el polinomio de Chow del radical de un ideal polinomial homogéneo débilmente unmixed, i.e. donde todos los primos minimales tienen misma dimensión (ver, por ejemplo, [Sh] para la definición de polinomio de Chow). Para ello se aplica el algoritmo rápido de eliminación de cuantificadores expuesto en el Teorema 2 a una construcción de [Ne]. Para otro acercamiento al problema, se puede consultar [Ca 2].

Finalmente, se exponen los resultados de eliminación de cuantificadores para *cuerpos real cerrados* obtenidos recientemente en [He-Ro-So 2] (ver también [He-Ro-So 3] ó [Re]): si se nota por R el cuerpo real cerrado y por L un subanillo de R, el lenguaje de primer orden $\mathcal{L}_L^R$ de R a constantes en L se define como en el caso algebraicamente cerrado, pero se admiten también desigualdades polinomiales en las fórmulas. En [He-Ro-So 2] o [He-Ro-So 3], se exhiben para ese caso las mismas cotas superiores precisas que las del Teorema 2, Capítulo I. Los autores se basan fundamentalmente en técnicas desarrolladas en [He-Ro-So 1] y [So], que a su vez utilizan fuertemente las cotas superiores para cuerpos algebraicamente cerrados presentadas aquí combinadas con herramientas de topología diferencial ([Mil], [Th]) aplicadas por primera vez en [Gr 2] y [Gr-Vo].

En la Observación 6, Capítulo I, se examina más en detalle el algoritmo de [He-Ro-So 2] a fin de obtener cotas para los grados y los valores absolutos de los coeficientes de los polinomios que aparecen en la fórmula de salida. Estas serán luego aplicadas a un problema de programación entera con restricciones polinomiales desarrollado en el Capítulo II.

II. En el segundo capítulo, se considera el problema de la programación entera con restricciones polinomiales cuasiconvexas.

Aquí $\mathbb{R}$ denota el cuerpo de números reales y $\mathbb{Z}$ el anillo de enteros.

Se dice que un polinomio $F \in \mathbb{R}[X_1, \ldots, X_n]$ es *cuasiconvexo* sii para todo $\lambda \in \mathbb{R}$ el conjunto $\{x \in \mathbb{R}^n : F(x) \leq \lambda\}$ es un subconjunto convexo de $\mathbb{R}^n$.

El primer resultado (Teorema 1, Capítulo II) que se obtiene es el siguiente:

Sean $F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$ polinomios cuasiconvexos, a coeficientes enteros y de grado acotado por $d \geq 2$, y sea σ una cota superior para la longitud binaria de todos los coeficientes de $F_1, \ldots, F_s$. Se muestra que si el sistema $F_1 \leq 0, \ldots, F_s \leq 0$ admite una solución *entera*, entonces existe una tal solución con longitud binaria acotada por $(sd)^{cn^2}\sigma$, donde c es una constante universal.

Se tiene además que el carácter simplemente exponencial de esta cota es intrínseco al problema, como lo muestra un contraejemplo de [Ta-Kh]. Asimismo, este resultado mejora una cota de orden $d^{(\tilde{n}+d)^c n^{d^c}}\sigma$ (donde $\tilde{n} := \min\{s, d\}$ y c es una constante) anunciada en [Kh] y [Ta-Kh] para polinomios *convexos*.

La prueba del teorema se basa en técnicas de reducción para polinomios cuasiconvexos desarrolladas en [Ba-Ma 1], Capítulos 4 y 5, y simplificados en [Ba-Ma 2]. También se aplica en forma fundamental la cota para grados y valores absolutos (Observación 6, Capítulo I) que resulta del examen del algoritmo de eliminación de cuantificadores para cuerpos real cerrados de [He-Ro-So 2].

El resultado implica un corolario algorítmico (Corolario 1.1, Capítulo II): El problema de decidir si el conjunto $\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ es vacío o no pertenece a la clase de complejidad NEXPTIME ("non deterministically simply exponential time"). Esto significa que no se sabe si se puede decidir si existe una solución del sistema en tiempo (secuencial) simplemente exponencial, pero sí se puede *verificar* que un candidato $x \in \mathbb{Z}^n$ es solución en ese tiempo. (Este concepto está detallado en la demostración del Corolario 1.1, Capítulo II).

El Teorema 2 de este capítulo trata de cotas para el problema de optimisación correspondiente: Si se realiza el ínfimo del conjunto $\{F_0(x) : x \in \mathbb{Z}^n, F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ (donde $F_0 \in \mathbb{Z}[X_1, \ldots, X_n]$ es cuasiconvexo también), entonces se realiza para cierto $x \in \mathbb{Z}^n$ de longitud binaria acotada por $(sd)^{n^c}\sigma$ (con d y σ, como arriba, cotas para el grado máximo y la longitud binaria de $F_0, \ldots, F_s$ y c constante).

Para este teorema se aplican no solamente el resultado del Teorema 1, Capítulo II, sino también los métodos utilizados para su demostración.

Para finalizar, unas palabras acerca de la organización de este trabajo:

En cada capítulo, se exponen en primer lugar en forma precisa todos los resultados mencionados en la introducción, precedidos de los preliminares necesarios para su formulación.

Las demostraciones se encuentran a continuación y están generalmente subdivididas en etapas que comprenden resultados parciales con sus pruebas.

I. COTAS PARA LA ELIMINACION DE CUANTIFICADORES SOBRE CUERPOS ALGEBRAICAMENTE CERRADOS

INTRODUCCION

La primer parte de este capítulo trata el problema de exhibir algoritmos rápidos para la eliminación de cuantificadores en el lenguaje de primer orden de los cuerpos algebraicamente cerrados (Teoremas 1 y 2). Luego se mostrará que esos algoritmos son optimales como medida general de complejidad en función de los parámetros considerados (Teorema 3). A continuación y a modo de aplicación se utiliza el algoritmo presentado para calcular en forma eficiente el polinomio de Chow del radical de un ideal polinomial homogéneo "débilmente unmixed" (es decir, donde todos los primos minimales tienen la misma dimensión) (Aplicación 4). En lo que sigue (Teorema 5) se presentan los resultados análogos a los del Teorema 2 obtenidos recientemente por J. Heintz, M.-F. Roy y P. Solernó ([He-Ro-So 1], [So], [He-Ro-So 2] y [He-Ro-So 3]), y por J. Renegar ([Re]), para la teoría de primer orden de los cuerpos real cerrados. Finalmente se examina más en detalle el algoritmo de [He-Ro-So 2] a fin de obtener cotas para los grados, y el valor absoluto de los coeficientes, de los polinomios que aparecen en la fórmula de salida del algoritmo (Observación 6). Estos resultados se aplicarán luego en el Capítulo II.

Es necesario, por lo tanto, definir ante todo el modelo con el que se trabajará (lenguaje de primer orden y modelo de algoritmo).

EL MODELO

En lo que sigue, K será un cuerpo arbitrario y Ω un cuerpo algebraicamente cerrado que lo contiene, por ejemplo una clausura algebraica de K.

A. Lenguaje de primer orden de un cuerpo algebraicamente cerrado

Se considera el *lenguaje de primer orden (o lenguaje elemental)* $\mathcal{L}_K^{\Omega}$ *sobre* Ω, a *constantes* en K definido de la manera siguiente:

Los símbolos no lógicos de $\mathcal{L}_K^{\Omega}$ son $\{a,\ a \in K\}, +, -, \cdot, =$.

Las variables son indeterminadas $X_1, \ldots, X_n, \ldots$ sobre Ω y los términos son polinomios en varias variables a coeficientes en K. Un término típico tiene la forma $F \in K[X_1, \ldots, X_n]$ y una fórmula atómica es $F = 0$ (ó $F \neq 0$ para su negación).

El lenguaje $\mathcal{L}_K^\Omega$ se construye a partir de estas fórmulas utilizando los conectivos lógicos $\wedge, \vee, \neg$ y los cuantificadores $\exists, \forall$ que sólo se pueden aplicar a elementos de Ω (representados por variables) y no a subconjuntos ni a relaciones de Ω. $\mathcal{L}_K^\Omega$ es así un conjunto de palabras finitas *(fórmulas)* sobre el alfabeto de símbolos de $\mathcal{L}_K^\Omega$ (variables, símbolos no lógicos, conectivos lógicos, cuantificadores, paréntesis).

Cuando no haya confusión posible, notaremos $\mathcal{L}$ en lugar de $\mathcal{L}_K^\Omega$.

Para cada fórmula $\Phi \in \mathcal{L}$, se define la ***longitud*** de Φ:

$|\Phi| :=$ número de símbolos necesarios para escribir Φ.

Las variables que en la fórmula Φ aparecen acompañadas por un cuantificador (existencial o universal) se llaman ***variables ligadas*** (o cuantificadas); en caso contrario son ***variables libres***.

Se dice que una fórmula Φ está dada en *forma preneza* cuando todos los cuantificadores se hallan al principio de la fórmula.

Sean $F_1, \ldots, F_s \in [X_1, \ldots, X_n]$ todos los polinomios que aparecen en la fórmula Φ, dada en forma prenexa. Se consideran también los siguientes parámetros que "miden" la fórmula Φ.

$$D := 2 + \sum_{1 \le i \le s} gr\, F_i \qquad \text{(la suma de los polinomios de } \Phi\text{)}$$

$n :=$ número de variables de Φ

$r :=$ número de bloques de cuantificadores (existenciales y universales) de Φ

Cabe señalar que toda fórmula arbitraria Φ puede ser llevada a una fórmula prenexa renombrando las variables. Este procedimiento no modifica $|\Phi|$. Tampoco modifica el grado de los polinomios que aparecen en Φ y el número de variables de la fórmula prenexa está acotado por la suma del número de variables libres y del número de cuantificadores de Φ.

Ejemplo de $\Phi \in \mathcal{L}_K^\Omega$

$(*) \qquad (\exists X)\ (X \neq 0 \wedge AX = 0)$

(donde $X := {}^t(X_1, \ldots, X_m)$, $A := \begin{pmatrix} A_{11} & \ldots & A_{1m} \\ \vdots & & \vdots \\ A_{m1} & \ldots & A_{mm} \end{pmatrix}$ y por $X \neq 0$ se entiende

$X_1 \neq 0 \vee X_2 \neq 0 \vee \ldots \vee X_m \neq 0$).

Aquí las variables $X_1, \ldots, X_m$ son ligadas mientras que $A_{11}, \ldots, A_{mm}$ son libres. Se tiene $n = m^2 + m$ y $D = 3m$.

La fórmula $(*)$ describe el problema de determinar para qué valores de $A_{11}, \ldots, A_{mm}$ en Ω el sistema homogéneo de ecuaciones lineales dado por la matriz A admite soluciones no triviales en Ω.

En general se dice que dos fórmulas Φ y $\Psi \in \mathcal{L}$ son *equivalentes* sii

(i) Φ y Ψ tienen el mismo número de variables libres

(ii) Si $m := \#\{$ variables libres de Φ (ó Ψ)$\}$, entonces para todo $x \in \Omega^m$, $\Phi(x)$ es verdadera si y sólo si $\Psi(x)$ lo es (donde $\Phi(x)$ (ó $\Psi(x)$) significa evaluar la fórmula Φ (ó Ψ) en $x := (x_1, \ldots, x_m) \in \Omega^m$ en lugar de las variables libres).

Por ejemplo la fórmula $(*)$ es equivalente a la fórmula

$(**)$ $\det A = 0$

Intuitivamente es claro que entre dos fórmulas equivalentes resulta conveniente trabajar con aquella que tiene el menor número de variables (o sea el menor número de variables ligadas), y ¡tanto mejor si no tiene ninguna!

De hecho, muchos problemas geométricos y algebraicos interesantes pueden ser formulados en el lenguaje de primer orden de los cuerpos algebraicamente cerrados, y su solución consiste precisamente en "eliminar los cuantificadores": en el ejemplo, $(**)$ es una versión sin cuantificadores de $(*)$, que resuelve el problema de determinar cuándo un sistema tiene solución no trivial. Este es un caso particular del hecho general (bien conocido por la teoría de modelos de la lógica) que la teoría de primer orden de los cuerpos algebraicamente cerrados de característica arbitraria admite *eliminación de cuantificadores*. Es decir, dada cualquier fórmula $\Phi \in \mathcal{L}_K^\Omega$, siempre existe una fórmula $\Psi \in \mathcal{L}_K^\Omega$ sin cuantificadores y equivalente a Φ.

Cuando la fórmula Φ no contiene variables libres, la fórmula equivalente Ψ sin cuantificadores es una combinación booleana de símbolos no lógicos de $\mathcal{L}_K^\Omega$, que es verdadera o falsa: se dice que se trata de un *problema de decisión*.

En [He-Wü], J. Heintz y R. Wüthrich presentaron por primera vez explícitamente un algoritmo de eliminación de cuantificadores (que resuelve por lo tanto también el problema de la decisión) para la teoría elemental de los cuerpos algebraicamente cerrados de característica arbitraria: a partir de una fórmula de entrada Φ ellos construyen una fórmula Ψ equivalente y sin cuantificadores.

Buenos algoritmos para la eliminación de cuantificadores permiten resolver computacionalmente aquellos problemas geométricos y algebraicos formulables en el lenguaje ele-

mental de los cuerpos algebraicamente cerrados. Es por ello que en la última década se ha realizado un esfuerzo especial para hallar algoritmos cada vez más eficientes.

Pasemos entonces a precisar la noción de algoritmo con la que se trabajará:

B. El modelo algorítmico

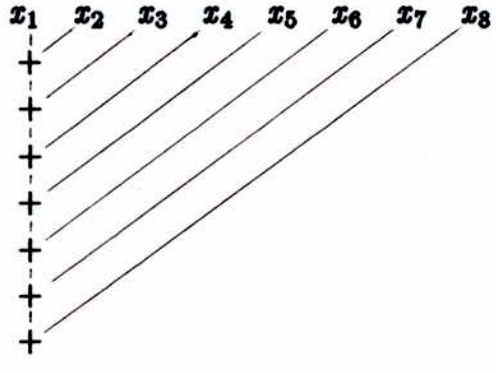
Dado que en nuestro contexto, vamos a tener que realizar operaciones aritméticas $(+,-,.)$ con los polinomios de Φ, la definición de algoritmo que resulta más adecuada es la de *red aritmética* presentada en [Gat].

Los polinomios serán codificados con *representación densa*, es decir por el vector de todos los coeficientes (aún los nulos) en un orden preestablecido de los monomios, fijado el grado. Los coeficientes de nuevos polinomios se computarán por interpolación, evaluando en suficientes elementos de Ω (que es infinito por ser algebraicamente cerrado).

La red aritmética utiliza como entradas las constantes del cuerpo K, y permite las operaciones $+,-,\cdot$, las comparaciones (para decidir por ejemplo si un polinomio es idénticamente nulo, especializando en elementos de Ω), y el uso de selectores para determinar el camino a seguir.

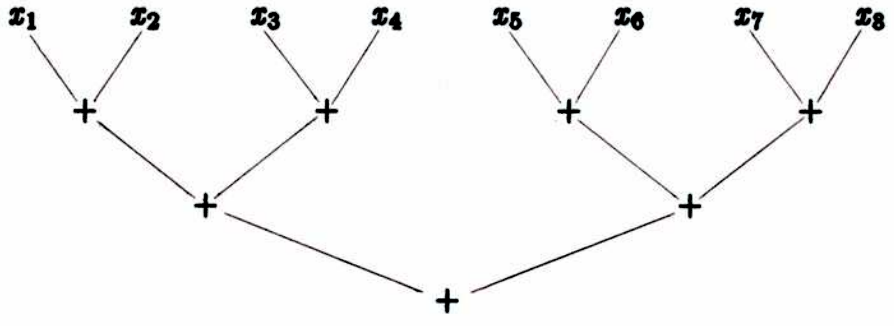
Por ejemplo, sumar 8 números $x_1,\ldots,x_8$ puede ser representado por el grafo siguiente

(1)



También se puede realizar el mismo cálculo por medio del algoritmo :

(2)



Se definen, para un algoritmo dado descrito por un grafo, dos nociones de complejidad:

- la complejidad secuencial (tamaño del grafo): es el número de nodos del grafo (sin contar los nodos de entrada). En los ejemplos (1) y (2), la complejidad secuencial es 7. Si se supone que cada operación se realiza en una unidad de tiempo dada, la complejidad secuencial representa el tiempo necesario para ejecutar el algoritmo con *un* procesador.
- la complejidad paralela (profundidad del grafo): es el número de nodos de una cadena maximal del grafo, es decir el camino (orientado) más largo a seguir para llegar a un resultado. En el ejemplo (1) la profundidad es 7 mientras que en el ejemplo (2) es 3. Dado que la profundidad del grafo refleja el número de operaciones que deben esperar el resultado de operaciones anteriores, esta noción corresponde al tiempo mínimo necesario para realizar el algoritmo, aunque se disponga de un número *arbitrariamente grande* de procesadores funcionando en paralelo.

Algunos autores llaman también "número de procesadores" al tamaño del grafo, pues es la única cota general de la que se dispone hasta hoy para la cantidad de procesadores necesaria para realizar el algoritmo (en realidad, aquí 1 en (1) y 4 en (2)). Esto corresponde a la poco económica suposición que se tira un procesador luego de utilizarlo una sola vez, y se evitará aquí esa expresión. Sería por supuesto interesante obtener cotas para este tipo de parámetro, en función del número de nodos y de la profundidad.

Es intuitivamente claro que la complejidad paralela de un algoritmo no puede ser menor que el logaritmo en base 2 de su complejidad secuencial. Se dice que un algoritmo es *paralelizable* cuando su profundidad tiene orden de magnitud el logaritmo (en base 2) de su tamaño.

Generalmente ocurre que los mejores algoritmos en secuencial no son los mejores desde el punto de vista paralelo, ya que no son paralelizables.

En este capítulo, se exhibe un algoritmo de eliminación de cuantificadores para la teoría

elemental de los cuerpos algebraicamente cerrados que es paralelizable, y que tiene complejidad secuencial de mismo orden que los mejores algoritmos secuenciales conocidos hasta la fecha.

Para concluir esta descripción del modelo, mencionemos que una parte del algoritmo corresponde al manejo puro de las fórmulas de $\mathcal{L}$. Por ejemplo de la fórmula de entrada Φ hay que extraer los polinomios $F_1, \ldots, F_s \in K[X_1, \ldots, X_n]$, que serán transformados en polinomios involucrados en la fórmula de salida Ψ. Hay que construir la fórmula Ψ a partir de estos polinomios. En pocas palabras, se admitirán el mismo tipo de operaciones elementales con los símbolos de $\mathcal{L}$ que con los elementos de K: por ejemplo, concatenación de palabras, intercambio o inserción de símbolos de $\mathcal{L}$. Estas operaciones permiten entre otras cosas transformar la fórmula de entrada Φ en una fórmula prenexa en tiempo lineal $|\Phi|$.

Notación: Sea f una función de $\mathbf{N}$ en $\mathbf{N}$. Se adopta aquí la notación standard $0(f(n))$ para denotar una función lineal en $f(n)$: Es decir, existe una constante c independiente de n tal que $0(f(n)) \leq cf(n)$.
Además, log notará en el trabajo el logaritmo en base 2.

Recordemos que se enunciarán en primer lugar todos los resultados que se quieren probar, y que las demostraciones se encuentran a continuación.

RESULTADOS

En primer lugar, se tratarán dos problemas: el problema de cotas superiores (Teoremas 1 y 2) y el problema de cotas inferiores (Teorema 3) para la complejidad secuencial y paralela de la eliminación de cuantificadores en el lenguaje de primer orden de los cuerpos algebraicamente cerrados de característica arbitraria.

TEOREMA 1. *Para todo $\ell \in \mathbf{N}$, existe una red aritmética $\mathcal{N}_\ell$ sobre los símbolos de $\mathcal{L}_K^\Omega$ de profundidad $\ell^{0(\ell)}$ y tamaño $\ell^{\ell^{0(\ell)}}$ con la propiedad siguiente:*
Para toda fórmula de entrada $\Phi \in \mathcal{L}_K^\Omega$, con $|\Phi| = \ell$, $\mathcal{N}_\ell$ construye una fórmula sin cuantificadores, equivalente a Φ (con respecto a la teoría de primer orden de Ω).
En otras palabras, existe un algoritmo (la familia de redes $\mathcal{N}_\ell$, $\ell \in \mathbf{N}$) que elimina cuantificadores (con respecto a la teoría de primer orden de Ω) en tiempo

– *paralelo:* $|\Phi|^{0(|\Phi|)}$

– *secuencial:* $|\Phi|^{|\Phi|^{0(|\Phi|)}}$

donde $\Phi \in \mathcal{L}_K^{\Omega}$ *es una fórmula arbitraria.*

Las mismas cotas se aplican para el problema de la decisión de la teoría de primer orden de Ω.

En el próximo resultado, se darán cotas más diferenciadas. Asumiremos para ello que Φ es una *fórmula prenexa* y *"convenientemente preparada"*. Esto significa que, además de tener todos sus cuantificadores al principio, los polinomios que aparecen en Φ están explícitamente dados y que la parte libre de cuantificadores de Φ puede ser escrita con respecto a los conectivos lógicos por medio de una red de profundidad $0(\log|\Phi|)$. La preparación de la fórmula, así como su escritura en forma prenexa, exige un trabajo de orden $0(|\Phi|)$ y es generalmente asumida, como en este trabajo, en los artículos sobre este tema.

Si $F_1,\ldots,F_s \in K[X_1,\ldots,X_n]$ son todos los polinomios que aparecen en la fórmula Φ, se considerarán los parámetros n, $D := 2 + \sum_{1\leq i\leq s} gr\, F_i$ y $r :=$ número de bloques de cuantificadores de Φ.

TEOREMA 2

(i) *Existe un algoritmo que elimina los cuantificadores de* Φ *(con respecto al lenguaje de primer orden de* Ω*) y que funciona en tiempo*

– *paralelo* $n^{0(r)}(\log D)^{0(1)} + 0(\log|\Phi|)$

– *secuencial* $D^{n^{0(r)}}|\Phi|$.

(ii) *Las mismas cotas valen para la complejidad de la decisión de la teoría de primer orden de* Ω.

El Teorema 2 implica que los problemas de eliminación de cuantificadores y decisión de la teoría de primer orden de Ω pertenecen a la clase de complejidad NC (i.e. complejidades paralela polilogarítmica y secuencial polinomial) si el número de variables n de las fórmulas de entrada está fijado.

El objetivo del Teorema 3 que se expone a continuación es el de mostrar que el algoritmo descripto en el Teorema 2 es optimal desde el punto de vista de la complejidad general. Más

precisamente, el problema general de la eliminación de cuantificadores sobre cuerpos algebraicamente cerrados tiene una complejidad inherente simplemente exponencial en paralelo y doblemente exponencial en secuencial si se exige la representación densa de los polinomios.

Sea Ω un cuerpo algebraicamente cerrado y $\mathbf{F}$ su cuerpo primo

TEOREMA 3. *Existe una sucesión de fórmulas* $\Phi_\ell \in \mathcal{L}_{\mathbf{F}}^{\Omega}$ $(\ell \in \mathbf{N})$, *con dos variables libres, con las propiedades siguientes:*

(i) $|\Phi_\ell| = 0(\ell^3)$.

(ii) *Para toda fórmula sin cuantificadores* $\Psi \in \mathcal{L}_{\mathbf{F}}^{\Omega}$, *equivalente a* Φ_ℓ, *que involucra los polinomios* $F_1, \ldots, F_s$, *existe* i, $1 \leq i \leq s$ *tal que* $gr\, F_i \geq 2^{2^\ell}$.

La propiedad (ii) implica que $|\Psi| \geq 2^{2^\ell}$, dado que en el lenguaje $\mathcal{L}_{\mathbf{F}}^{\Omega}$ los polinomios están representados en forma densa. En particular cualquier algoritmo secuencial para la eliminación de cuantificadores aplicado a la fórmula de entrada Φ_ℓ necesita tiempo doblemente exponencial en $|\Phi_\ell|$ para escribir la fórmula sin cuantificadores que se obtiene (ver [He] y [We]). Más aún, todo algoritmo paralelo para la eliminación de cuantificadores aplicado a Φ_ℓ necesita tiempo simplemente exponencial en $|\Phi_\ell|$ para evaluar la fórmula sin cuantificadores obtenida, ya que contiene un polinomio de grado doblemente exponencial (ver [Gat]).

A continuación se dará, a modo de aplicación del algoritmo rápido de eliminación de cuantificadores presentado en el Teorema 2, un algoritmo eficiente para el cálculo del polinomio de Chow del radical de un ideal homogéneo débilmente unmixed (ver también [Ca 2]).

Sea Ω un cuerpo algebraicamente cerrado y $\Omega[X_0, \ldots, X_n]$ el anillo de polinomios en las indeterminadas $X_0, \ldots, X_n$ sobre Ω.

Recordemos brevemente la definición de *Forma de Chow* de un ideal homogéneo y primario I de $\Omega[X_0, \ldots, X_n]$.

Se nota con $\mathbf{P}^n$ el espacio proyectivo n-dimensional sobre Ω.

Sea $X := \{x \in \mathbf{P}^n : F(x) = 0 \ (\forall F \in I)\}$ la variedad de $\mathbf{P}^n$ definida por I y sea r su dimensión.

Un hiperplano de $\mathbf{P}^n$ se identificará con un punto de $\mathbf{P}^n$ formado por los coeficientes de

una forma lineal que lo define.

Se considera el subconjunto Γ de $(\mathbf{P}^n)^{r+1} \times X := \underbrace{\mathbf{P}^n \times \ldots \times \mathbf{P}^n}_{r+1} \times X$

definido por:

$\Gamma := \{(y^{(0)}, \ldots, y^{(r)}, x) \in (\mathbf{P}^n)^{r+1} \times X : x \in y^{(i)} \quad (0 \leq i \leq r)\}$

y sea $\varphi(\Gamma) := \{(y^{(0)}, \ldots, y^{(r)}) \in (\mathbf{P}^n)^{r+1} : \exists x \in X \text{ con } x \in y^{(i)} \quad (0 \leq i \leq r)\}$

la proyección de Γ a $(\mathbf{P}^n)^{r+1}$.

Entonces, $\varphi(\Gamma)$ es una hipersuperficie en $(\mathbf{P}^n)^{r+1}$ definible por un polinomio F_X, que se puede elegir sin factores múltiples. Este polinomio F_X se llama la forma de Chow de X (o del radical del ideal I) y determina unívocamente a X (Ver [Sh], Ch I, § 6,5).

Se tiene la caracterización

$$(*) \qquad x \in X \Longleftrightarrow \text{para todo } y^{(0)}, \ldots, y^{(r)} \text{ tal que } x \in y^{(i)} \quad (0 \leq i \leq r),$$
$$F_X(y^{(0)}, \ldots, y^{(r)}) = 0$$

Un interés de la forma de Chow es que su grado es el grado de la variedad irreducible X.

En el caso en que el ideal homogéneo I es débilmente unmixed (es decir todos los primos minimales de I tienen la misma dimensión) se obtiene también una forma F_X que caracterisa a X en el sentido de $(*)$, y se puede por lo tanto hablar en forma análoga de forma de Chow del radical de I (ver por ejemplo [Ne]).

En lo que sigue, se supondrá que Ω es un cuerpo algebraicamente cerrado de característica 0, o bien de característica p, donde se sabe como extraer raíces p-ésimas de polinomios.

Sea $I \subseteq \Omega[X_0, \ldots, X_n]$ un ideal homogéneo débilmente unmixed generado por los polinomios $F_1, \ldots, F_s$. Con $\mathrm{rad}(I)$ se notará el ideal radical de I.

Sea $D := 2 + \sum_{1 \leq i \leq s} gr\, F_i$ y supongamos que el conjunto

$$X := \{x \in \mathbf{P}^n : F_1(x) = \ldots = F_s(x) = 0\} \quad \text{es no vacío,}$$

entonces se tiene la siguiente aplicación del Teorema 2:

APLICACION 4. *Se puede calcular el polinomio de Chow del radical de I por medio de una red aritmética $\mathcal{N}_{D,n}$ de tamaño $D^{n^{O(1)}}$ y de profundidad $(n \log D)^{O(1)}$.*

En lo que sigue, nos interesaremos en los algoritmos de eliminación de cuantificadores para cuerpos real cerrados.

Sea R un cuerpo real cerrado y sea L un subanillo de R.

El lenguaje de primer orden $\mathcal{L}_L^R$ de R a constantes en L se construye en forma análoga al lenguaje de primer orden de los cuerpos algebraicamente cerrados, con la única diferencia que ahora los símbolos no lógicos son $\{a, a \in L\} \cup \{+, -, \cdot, =, <\}$ (se agrega el símbolo $<$ del orden de R).

Se enuncia aquí para $\mathcal{L}_L^R$ el teorema análogo al Teorema 2, que fue obtenido por J.Heintz, M.F. Roy y P. Solernó (1989) y J. Renegar (1989) (ver [He-Ro-So 2], [He-Ro-So 3] ó [Re]):

Sea Φ una fórmula prenexa de $\mathcal{L}_L^R$ y sean $F_1, \ldots, F_s \in [X_1, \ldots, X_n]$ todos los polinomios que aparecen en Φ. Como antes sean

$|\Phi|$ = longitud de Φ

$n :=$ número de variables de Φ

$D := 2 + \sum_{1 \leq i \leq s} gr\, F_i$

$r :=$ número de bloques de cuantificadores de Φ.

TEOREMA 5

(i) *Existe un algoritmo que elimina los cuantificadores de Φ (con respecto al lenguaje de primer orden de R) y que funciona en tiempo*

- *paralelo:* $n^{O(r)}(\log D)^{O(1)} + O(|\Phi|)$
- *secuencial:* $D^{n^{O(r)}}|\Phi|$

(ii) *Las mismas cotas valen para el problema de la decisión en la teoría de primer orden de R.*

Se examinará ahora en detalle la demostración de [He-Ro-So 2] (ó [He-Ro-So 3]) del teorema anterior, considerando también el parámetro $\nu :=$ máximo del valor absoluto de todos los coeficientes de Φ, para obtener cotas sobre los grados y el módulo de los coeficientes de los polinomios que aparecen en la fórmula de salida del algoritmo.

Sea $\theta \in \mathcal{L}_L^R$, se define:

$d(\theta) :=$ máximo de los grados de todos los polinomios que aparecen en θ

$\nu(\theta) :=$ máximo del valor absoluto de los coeficientes de todos los polinomios que aparecen en θ.

OBSERVACION 6

(i) *Existe una fórmula* $\Psi \in \mathcal{L}_L^R$ *sin cuantificadores y equivalente a* Φ *que verifica*

$$d(\Psi) = D^{n^{O(r)}} \qquad y \qquad \nu(\Psi) = \nu^{D^{n^{O(r)}}}$$

(ii) *En el caso* $r = 1$, *se puede elegir* Ψ *de manera que*

$$d(\Psi) = D^{O(n)} \qquad y \qquad \nu(\Psi) = \nu^{D^{O(n)}} .$$

Cabe señalar que las mismas cotas para los grados, y el módulo de los coeficientes, de los polinomios que intervienen en la fórmula de salida valen también para el caso de cuerpos algebraicamente cerrados (ya que el algoritmo de Heintz, Roy y Solernó utiliza en su desarrollo el algoritmo para cuerpos algebraicamente cerrados).

Se pasa ahora a dar las demostraciones de los resultados expuestos.

1.- DEMOSTRACION DEL TEOREMA 2. Dado que el Teorema 1 se deduce del Teorema 2, nos restringiremos aquí a la demostración de este último.

La prueba sigue las lineas generales de los procedimientos de eliminación de cuantificadores de [He], [Ch-Gr 2] y [Gr 1]. Sin embargo, al no ser éstos eficientemente paralelizables, es necesario modificar algunos aspectos esenciales de ellos, obteniendo así también un nuevo algoritmo de eliminación de cuantificadores para cuerpos algebraicamente cerrados (de característica arbitraria) rápido en secuencial.

Sea $\Phi \in \mathcal{L}$ una fórmula arbitraria *prenexa*, que contiene las variables $X_1, \ldots, X_n$, donde $X_1, \ldots, X_m$ son ligadas y $X_{m+1}, \ldots, X_n$ son libres. La fórmula Φ se puede suponer de la forma

$\Phi : \quad (Q_1 X^{(1)}) \ldots (Q_r X^{(r)})\, \theta(X_1, \ldots, X_n)$

donde:

- θ es una fórmula sin cuantificadores
- $X^{(i)} := (X_{m_{i-1}+1}, \ldots, X_{m_i}) \quad 1 \leq i \leq r, \quad m_0 := 0, \quad m_r := m$
- $Q_i \in \{\exists, \forall\}$ y $Q_i \neq Q_{i+1} \quad (1 \leq i \leq r-1)$

- $Q_i X^{(i)} := (Q_i X_{m_{i-1}+1}) \dots (Q_i X_{m_i})$
  (y r es el número de bloques de cuantificadores).

La fórmula θ (sin cuantificadores) es combinación booleana de fórmulas atómicas que involucran los polinomios $F_1, \dots, F_s \in K[X_1, \dots, X_n]$. Sea

$$D := D(\Phi) = 2 + \sum_{1 \le i \le s} gr\, F_i \qquad (gr\, F_i \text{ nota el grado total})$$

El proceso de eliminación que se detalla a continuación es inductivo, eliminándose sucesivamente los bloques de cuantificadores Q_r, Q_{r-1} hasta Q_1. Observemos que el último bloque Q_r (que es el primero a ser eliminado) se puede suponer existencial ya que la fórmula $\forall X_{m_{r-1}+1} \dots \forall X_{m_r}\, \theta(X_1, \dots, X_n)$ es equivalente a la fórmula $\neg(\exists X_{m_{r-1}+1} \dots \exists X_{m_r} \quad (\neg\theta(X_1, \dots, X_n)))$.

1.-A. Escritura de θ en forma disjuntiva "consistente"

El primer paso del algoritmo consiste en reescribir la fórmula θ como una disjunción de *conjunciones consistentes* de polinomios igualados a cero y polinomios distintos de cero (es decir que describen subconjuntos no vacíos de Ω^n). Pediremos además que cada una de esas conjunciones consistente corresponda a una $F_1, \dots, F_s$- célula (según la notación de [Gr 1]) en el sentido siguiente

DEFINICION A.1.

Sea $F_1, \dots, F_s \in K[X_1, \dots, X_n]$, e $I := \{1, \dots, s\}$

Se dice que $Z \subseteq \Omega^n$ es una $F_1, \dots, F_s$-*célula* si

(i) $Z \neq \emptyset$

(ii) Existe $M \subseteq I$ tal que

$$Z = \{x \in \Omega^n : F_i(x) = 0\ (\forall i \in M) \quad \text{y} \quad F_j(x) \neq 0\ (\forall j \in I - M)\}\,. \qquad \blacklozenge$$

Reescribiremos por lo tanto θ en la forma

$$\bigvee_{\substack{M \subseteq I \\ M \text{ define una} \\ F_1,\dots,F_s\text{-célula}}} \bigwedge_{i \in M} F_i(X_1, \dots, X_n) = 0 \wedge \bigwedge_{j \in I - M} F_j(X_1, \dots, X_n) \neq 0$$

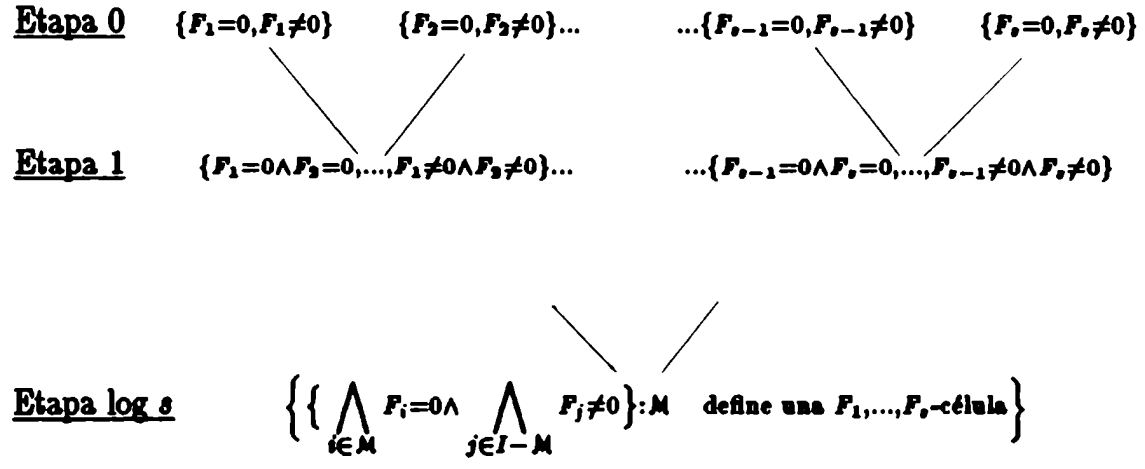
Esto es posible pues las $F_1, \dots, F_s$-células son los átomos del álgebra de Boole de los subconjuntos de Ω^n definidos por fórmulas sin cuantificadores que involucran los polinomios $F_1, \dots, F_s$.

Un hecho fundamental es que se sabe (por [He], Corollary 1) que hay a lo sumo D^n $F_1,\ldots,F_s$-células (donde D es una cota para la suma de los grados).
Para determinar las células construiremos una red de profundidad $0(n \log D)$ con $0(D^{0(n)})$ nodos. Estos tiempos se obtienen gracias a versiones efectivas de Nullstellensatz (por ejemplo [Ko], [Br 2], [Ca-Gu-Gu]), además de la utilización esencial de la estrategia de "dividir y reinar" de [Be-Ko-Re], con la diferencia que se trabaja aquí con polinomios en varias variables (y no en una).

ENUMERACION DE LAS CELULAS A.2. Supongamos por un momento que sabemos decidir "rápidamente" si una conjunción de igualdades y desigualdades polinomiales es consistente (i.e. si define un subconjunto no vacío de Ω^n), y formemos el siguiente árbol binario para enumerar las $F_1,\ldots,F_s$-células.

- Etapa 0: Se determina cuáles de los subconjuntos de Ω^n definidos por $F_i = 0$ ó $F_i \neq 0$ $(1 \leq i \leq s)$ son vacíos.
- Etapa 1: Se construyen $\frac{s}{2}$ conjuntos de conjunciones consistentes que provengan de condiciones consistentes adyacentes de la etapa 0. Son del tipo $\{F_1 = 0 \wedge F_2 = 0,\ F_1 = 0 \wedge F_2 \neq 0,\ F_1 \neq 0 \wedge F_2 = 0,\ F_1 \neq 0 \wedge F_2 \neq 0\},\ldots,\{F_{s-1} = 0 \wedge F_s = 0,\ F_{s-1} = 0 \wedge F_s \neq 0,\ F_{s-1} \neq 0 \wedge F_s = 0,\ F_{s-1} \neq 0 \wedge F_s \neq 0\}$.
  (Si por ejemplo la condición $F_1 = 0$ no es consistente, entonces en el primer conjunto no aparecen $F_1 = 0 \wedge F_2 = 0,\ F_1 = 0 \wedge F_2 \neq 0$).
  $\vdots$
- Etapa j: $(1 \leq j \leq \log s)$, se construyen $\frac{s}{2^j}$ conjuntos de conjunciones consistentes, formados a partir de conjunciones consistentes adyacentes de la etapa inmediata anterior.

Gráficamente se obtiene un árbol del aspecto siguiente



Para todo $1 \leq j \leq \log s$, cada conjunto de la etapa j se compone de conjunciones consistentes que involucran 2^j polinomios, cuya suma de grados está acotada por D. En cada conjunto de la etapa j, hay entonces a lo sumo $\min\{2^{2^j}, D^n\}$ conjunciones ([He], Corollary 1). Dado además que las conjunciones consistentes de la etapa j se determinan a partir de conjunciones consistentes de la etapa $(j-1)$, en cada etapa se realizan a lo sumo $\left(\frac{s}{2^j}\right)D^n \cdot D^n$ tests de consistencia, ejecutables simultáneamente.
Se efectúan por lo tanto en total $2sD^{2n}$ tests de consistencia (en secuencial) y $\log s$ en paralelo.

El algoritmo se completa explicando como se realiza un test de consistencia.

TEST DE CONSISTENCIA A.3.

Sea la conjunción $F_1 = 0 \wedge \ldots \wedge F_t = 0 \wedge F_{t+1} \neq 0 \wedge \ldots \wedge F_s \neq 0$.

¿Cómo decidir "rápidamente" si el subconjunto de Ω^n definido por esta conjunción es vacío o no?

Se utilizará el conocido "Truco de Rabinowitsch".

Planteamos $F := F_{t+1}F_{t+2}\ldots F_s$, y sea T una nueva variable.

Por el Teorema de los Ceros de Hilbert, se sabe que el conjunto

$$\{x \in \Omega^n : F_1(x) = 0, \ldots, F_t(x) = 0, F_{t+1}(x) \neq 0, \ldots, F_s(x) \neq 0\}$$

es vacío si y sólo si el ideal de $K[X_1, \ldots, X_n, T]$ generado por los polinomios $F_1, \ldots, F_t, 1 - TF$ es el trivial (i.e. $1 \in (F_1, \ldots, F_t, 1 - TF)$).

Aplicamos ahora la versión efectiva del Nullstellensatz de [Ko], [Br 2] ó [Ca-Gu-Gu], que

afirma que:

si K es un cuerpo arbitrario, $G_1,\ldots,G_\ell \in K[X_1,\ldots,X_n]$

y $d \geq \max\{gr(G_j),\quad 1 \leq j \leq \ell\}$, entonces

$$1 \in (G_1,\ldots,G_\ell) \Longleftrightarrow \exists P_1,\ldots,P_\ell \in K[X_1,\ldots,X_n] \quad \text{tales que}$$
$$gr\, P_j \leq \max\{3^n, d^n\} \quad (1 \leq j \leq \ell)$$
$$\text{y} \quad 1 = \sum_{1 \leq j \leq \ell} P_j G_j$$

En nuestro caso, se tiene

$1 \in (F_1,\ldots,F_t, 1-TF) \Longleftrightarrow \exists P_1,\ldots,P_t,\ P \in K[X_1,\ldots,X_n,T]$ tales que

$gr(P_i) \leq \tilde{d}^{n+1} (1 \leq i \leq t)$, $gr(P) \leq \tilde{d}^{n+1}$ y $1 = P_1F_1 + \ldots + P_tF_t + P(1-TF)$

(donde $\tilde{d} := \max\{D,3\}$).

Planteando los coeficientes de los polinomios $P_1,\ldots,P_t$, P como incógnitas, y comparando los coeficientes de los polinomios 1 y $\sum_{1 \leq j \leq t} P_jF_j + P(1-TF)$, el problema de la consistencia se reduce a decidir cuando un sistema no homogéneo de ecuaciones lineales sobre K admite una solución en Ω. El orden del sistema está acotado por $\tilde{d}^{cn^2}$, donde $\tilde{d} := \max\{3, D\}$ y c es una constante adecuada.

En otras palabras, hay que comparar el rango de dos matrices de orden $\tilde{d}^{cn^2}$ sobre K, lo que nos lleva al problema de calcular rápidamente (en secuencial y en paralelo) el rango de una matris. Según los resultados de [Mul], esto se puede hacer en tiempo secuencial $\tilde{d}^{O(n^3)}$ y en tiempo paralelo $O(n^4 \log^2 \tilde{d})$.

Por consiguiente, se pueden enunciar las D^n células en tiempo secuencial $2sD^{2n}\tilde{d}^{O(n^3)} = O(D^{O(n^3)})$ y en tiempo paralelo $(\log s)\,O(n^4 \log^2 \tilde{d}) = O(n^4 \log^3 D)$.

Una vez enumeradas las células, $\theta(X_1,\ldots,X_n)$ puede ser llevada a la forma disjuntiva deseada en tiempos secuencial $O(|\theta|)$ y paralelo $O(\log|\theta|)$.

1.-B. La fórmula $(\exists X_1)\ldots(\exists X_\ell)\,(F_1 = 0 \wedge \ldots \wedge F_t = 0 \wedge F_{t+1} \neq 0 \wedge \ldots \wedge F_s \neq 0)$

Dado que los cuantificadores existenciales y las disjunciones conmutan, alcansa ahora con caracterisar los subconjuntos de $\Omega^{n-\ell}$ definibles por una formula del tipo

$$(\exists X_1)\ldots(\exists X_\ell)\,(F_1 = 0 \wedge \ldots \wedge F_t = 0 \wedge F_{t+1} \neq 0 \wedge \ldots \wedge F_s \neq 0)$$

donde $\ell \leq m$ indica la longitud del último bloque de cuantificadores de la fórmula de entrada, que se supuso existencial.

Es decir, hay que describir por medio de una fórmula sin cuantificadores, con polinomios

$G_1,\dots,G_q \in K[X_{\ell+1},\dots,X_n]$, al conjunto

$$B := \{y \in \Omega^{n-\ell} : \exists x \in \Omega^{\ell} \quad \text{tal que} \quad F_1(x,y)=0 \wedge \dots \wedge F_t(x,y)=0 \wedge$$
$$F_{t+1}(x,y) \neq 0 \wedge \dots \wedge F_s(x,y) \neq 0\}$$

(que es la proyección de un conjunto localmente cerrado en la topología de Zariski de Ω^n).
Sea $E := \Omega^{n-\ell} - B$, y como arriba sea $F := F_{t+1} \dots F_s$ y sea T una nueva variable.
Nuevamente por el Teorema de los Ceros de Hilbert se verifica

$$E = \{y \in \Omega^{n-\ell} : 1 \in (F_1(X_1,\dots,X_\ell,y),\dots,F_t(X_1,\dots,X_\ell,y),1-TF(X_1,\dots,X_\ell,y))\}$$

Consideraremos $F_1,\dots,F_t,1-TF$ como polinomios en las variables $X_1,\dots,X_\ell,T$ y a coeficientes en $K[X_{\ell+1},\dots,X_n]$, y usaremos nuevamente el Nullstellensatz efectivo:
Por el momento, reemplacemos $X_{\ell+1},\dots,X_n$ por $y := (y_{\ell+1},\dots,y_n) \in \Omega^{n-\ell}$
Se tiene:

$1 \in (F_1(X_1,\dots,X_\ell,y),\dots,F_t(X_1,\dots,X_\ell,y),\ 1-TF(X_1,\dots,X_\ell,y)) \iff$
existen $P_1,\dots,P_\ell,\ P \in \Omega[X_1,\dots,X_\ell,T]$ tal que
$gr(P_i) \leq \tilde{d}^n \ (1 \leq i \leq \ell),\ gr(P) \leq \tilde{d}^n$ (donde $\tilde{d} := \max\{D,3\}$) y
$1 = P_1F_1(X_1,\dots,X_\ell,y) + \dots + P_tF_t(X_1,\dots,X_\ell,y) + P(1-TF)(X_1,\dots,X_\ell,y)$

Comparemos ahora los coeficientes de estos polinomios en las variables $X_1,\dots,X_\ell,T$, teniendo en cuenta las cotas para los grados y recordando que $F_1,\dots,F_t,1-TF$ son considerados como polinomios en las variables $X_1,\dots,X_\ell,T$ a coeficientes en $K[X_{\ell+1},\dots,X_n]$.
Sean $T_k (1 \leq k \leq N)$ los coeficientes de $P_1,\dots,P_t,P$. Dadas las cotas para los grados, se tiene $N \leq \tilde{d}^{cn^2}$ (c constante), y nos hallamos así ante el problema de analizar la resolubilidad de un sistema no homogéneo de ecuaciones lineales (de orden $\tilde{d}^{cn^2}$), más precisamente, a describir un conjunto del tipo

$$\{y \in \Omega^{n-\ell} : \sum_{1 \leq k \leq N} F_{jk}(y)T_k = F_{j\,N+1}(y),\ 1 \leq j \leq M \quad \text{tiene una}$$
$$\text{solución en} \Omega^N\} \qquad (N, M \leq \tilde{d}^{cn^2})$$

(donde $F_{jk}, F_{j\,N+1} \in K[X_{\ell+1},\dots,X_n]$ son algunos coeficientes de $F_1,\dots,F_t,1-TF$) por una fórmula sin cuantificadores, que involucra polinomios $G_1,\dots,G_q \in K[X_{\ell+1},\dots,X_n]$.
Para ello utilizaremos nuevamente el algoritmo de [Mul], que permite exhibir las condiciones polinomiales necesarias y suficientes sobre $y \in \Omega^{n-\ell}$ para que valga la igualdad en los rangos de las matrices

$$[F_{jk}(y)]_{\substack{1 \leq j \leq M \\ 1 \leq k \leq N}} \qquad \text{y} \qquad [F_{jk}(y)]_{\substack{1 \leq j \leq M \\ 1 \leq k \leq N+1}}$$

Con este fin, consideramos las matrices (genéricas)

$$[F_{jk}(X_{\ell+1},\ldots,X_n)]_{\substack{1\le j\le M\\ 1\le k\le N}} \qquad \text{y} \qquad [F_{jk}(X_{\ell+1},\ldots,X_n)]_{\substack{1\le j\le M\\ 1\le k\le N+1}}$$

El algoritmo de [Mul] calcula el rango de la matriz calculando el orden del cero en el polinomio característico de una matriz que se construye con operaciones de anillo a partir de la matriz de entrada, y de una variable auxiliar Z. Calculamos por medio del algoritmo de [Ber] (que no usa divisiones) los coeficientes (en $X_{\ell+1},\ldots,X_n,Z$) de los dos polinomios característicos obtenidos, y los consideramos como polinomios en Z; evaluando Z en un número suficiente de elementos de Ω (¡qué es infinito!) recuperamos sus coeficientes. Estos serán los polinomios $G_1,\ldots,G_q \in K[X_{\ell+1},\ldots,X_n]$ que se buscan.

El hecho que G_i se anule (resp. no se anule) en un punto dado $(y_{\ell+1},\ldots,y_n) \in \Omega^{n-\ell}$ expresa la multiplicidad del cero en los dos polinomios característicos luego de haber especializado las variables $X_{\ell+1},\ldots,X_n$ en $y_{\ell+1},\ldots,y_n$. Por lo tanto esta construcción permite expresar la igualdad de los rangos de $[F_{jk}(y)]_{\substack{1\le j\le M\\ 1\le k\le N}}$ y $[F_{jk}(y)]_{\substack{1\le j\le M\\ 1\le k\le N+1}}$ mediante una condición booleana de las condiciones $G_i(y)=0$, $G_i(y)\neq 0$ $(1\le i\le q)$.

Esto significa que E puede ser descripto por una fórmula sin cuantificadores que involucra (sólo) los polinomios $G_1,\ldots,G_q$. Dado que $gr\,F_{jk} \le D$, $F_{jk} \in K[X_{\ell+1},\ldots,X_n] \subseteq K[X_1,\ldots,X_n]$ para todo $1\le j\le M$, $1\le k\le N+1$, y que $M,N \le \tilde{d}^{cn^2}$, y teniendo en cuenta las complejidades de los algoritmos de [Mul] y [Ber], se obtiene $\sum_{1\le i\le q} \deg G_i \le \tilde{d}^{cn^2} = D^{O(n^2)}$. Asimismo, se puede computar $G_1,\ldots,G_q$ en tiempo paralelo $O(n^4\log^2 D)$ y secuencial $O(D^{O(n^2)})$.

Las combinaciones booleanas de las fórmulas atómicas $G_1=0, G_1\neq 0,\ldots,G_q=0, G_q\neq 0$ que representan la fórmula sin cuantificadores buscada pueden ser enumeradas por un grafo de profundidad $O(n^2\log D)$ y con $O(D^{O(n^2)})$ nodos.

El hecho que hay a lo sumo D^n células implica que se puede eliminar un bloque de cuantificadores existenciales en tiempos paralelo $O(n^4\log^3 D)$ y secuencial $O(D^{O(n^2)})$, obteniendo así una fórmula que involucra solamente polinomios en número y grado acotado por $O(D^{O(n^2)})$.

La cota general del teorema sigue ahora trivialmente por inducción en el número de bloques de cuantificadores.

♦

2.- DEMOSTRACION DEL TEOREMA 3

2.- A. La fórmula Φ_ℓ

Sea aquí $\mathbf{F}$ el cuerpo primo de Ω.

En [He] se construye inductivamente una sucesión de fórmulas $\Phi_\ell(X,Y) \in \mathcal{L}_{\mathbf{F}}^{\Omega}$ $(\ell \in \mathbf{N}_0)$ en las variables libres X, Y de la manera siguiente

$$\Phi_0(X,Y): \quad X^2 = Y$$

$$\Phi_1(X,Y): \quad (\exists Z^{(1)})(\forall Z_1^{(1)})(\forall Z_2^{(1)})((Z_1^{(1)} = Z^{(1)} \wedge Z_2^{(1)} = Y) \vee (Z_1^{(1)} = X \wedge Z_2^{(1)} = Z)) \longrightarrow \Phi_0(Z_1^{(1)}, Z_2^{(1)})$$

y en general

$$\Phi_\ell(X,Y): \quad (\exists Z^{(\ell)})(\forall Z_1^{(\ell)})(\forall Z_2^{(\ell)})((Z_1^{(\ell)} = Z^{(\ell)} \wedge Z_2^{(\ell)} = Y) \vee (Z_1^{(\ell)} = X \wedge Z_2^{(\ell)} = Z)) \longrightarrow \Phi_{\ell-1}(Z_1^{(\ell)}, Z_2^{(\ell)})$$

Se observa que la fórmula Φ_ℓ tiene 3ℓ cuantificadores (que corresponden a 3ℓ variables cuantificadas (distintas)) y únicamente dos variables libres X e Y. Dado que cada polinomio que aparece en Φ_ℓ tiene grado acotado por 2, el codificarlo con representación densa ocupa $O(\ell^2)$ lugares. Por otro lado se tiene $|\Phi_\ell| = 4c_1\ell^2 + c_2 + |\Phi_{\ell-1}| = \ell(4c_1\ell^2 + c_2)$ (donde c_1 y c_2 son constantes adecuadas), y por lo tanto $|\Phi_\ell| = O(\ell^3)$.

(En el caso de un cuerpo algebraicamente cerrado de característica 2, se considera como fórmula de partida $\Phi_0(X,Y): X^3 = Y$, y las estimaciones no se modifican esencialmente).

La fórmula $\Phi_\ell(X,Y)$ es equivalente a:

$$(\exists Z^{(\ell)})(\forall Z_1^{(\ell)})(\forall Z_2^{(\ell)}) \ (((Z_1^{(\ell)} = Z^{(\ell)} \wedge Z_2^{(\ell)} = Y) \longrightarrow \Phi_{\ell-1}(Z_1^{(\ell)}, Z_2^{(\ell)})) \wedge ((Z_1^{(\ell)} = X \wedge Z_2^{(\ell)} = Z^{(\ell)}) \longrightarrow \Phi_{\ell-1}(Z_1^{(\ell)}, Z_2^{(\ell)})))$$

que se puede simplificar aún más ya que las implicaciones son trivialmente ciertas salvo en el caso en que $Z_1^{(\ell)}$ y $Z_2^{(\ell)}$ tomen los valores indicados en las hipótesis de las implicaciones. Por lo tanto, $\Phi_\ell(X,Y)$ es equivalente a:

$$(\exists Z^{(\ell)})(\Phi_{\ell-1}(Z^{(\ell)}, Y) \wedge \Phi_{\ell-1}(X, Z^{(\ell)}))$$

Así se muestra que $\Phi_1(X,Y)$ es equivalente a $X^{2^2} = Y$ y recursivamente se obtiene que $\Phi_\ell(X,Y)$ es equivalente a la ecuación

$$X^{2^{2^\ell}} = Y$$

Se tiene por lo tanto una sucesión de fórmulas $\Phi_\ell(X,Y)$ $(\ell \in \mathbf{N}_0)$ con las propiedades siguientes:

(i) $|\Phi_\ell| = O(\ell^3)$

(ii) Φ_ℓ define el gráfico de la función de Ω en Ω que aplica x sobre $x^{2^{2^\ell}}$, es decir el conjunto

$$M_\ell := \{X^{2^{2^\ell}} - Y = 0\} := \{(x,y) \in \Omega^2 : x^{2^{2^\ell}} = y\}$$

2.- *B. La fórmula Ψ*

Sea ahora Ψ una fórmula sin cuantificadores equivalente a Φ_ℓ, que contiene los polinomios $F_1,\ldots,F_s \in \mathbf{F}[X,Y]$, y sean $G_1,\ldots,G_t$ los factores primos de $F_1,\ldots,F_s$ en $\Omega[X,Y]$. Se tiene que $\max\{gr\,F_j,\ 1 \le j \le s\} \ge \max\{gr\,G_i,\ 1 \le i \le t\}$. Alcansa por lo tanto con mostrar que existe $i (1 \le i \le t)$ tal que $gr\,G_i \ge 2^{2^\ell}$.

Sea $\mathcal{L}_\Omega^\Omega$ el lenguaje que se obtiene extendiendo las constantes de $\mathcal{L}_\mathbf{F}^\Omega$: las constantes de $\mathcal{L}_\Omega^\Omega$ son $\{a;\ a \in \Omega\}$.

Se reemplasa la fórmula Ψ de $\mathcal{L}_\mathbf{F}^\Omega$ por una fórmula Ψ' de $\mathcal{L}_\Omega^\Omega$, reemplasando cada fórmula atómica $F_j = 0$ por $G_{i_1} = 0 \vee \ldots \vee G_{i_m} = 0$ si $F_j = G_{i_1}^{r_1} \ldots G_{i_m}^{r_m}$ (donde $\{i_1,\ldots,i_m\} \subseteq \{1,\ldots,t\}$ y $r_1,\ldots,r_m \in \mathbf{N}$). Por consiguiente, Ψ' involucra solamente polinomios irreducibles sobre Ω, a saber $G_1,\ldots,G_t$.

Sin pérdida de generalidad, se puede suponer que Ψ' es una disjunción de *conjunciones consistentes* de la forma:

$$(*) \qquad G_{i_1} = 0 \wedge \ldots \wedge G_{i_k} = 0 \wedge G_{i_{k+1}} \neq 0 \wedge \ldots \wedge G_{i_m} \neq 0$$

donde aparecen todos los G_i $(1 \le i \le t)$ (o sea lo que llamamos $G_1,\ldots,G_t$-células en el parágrafo anterior).

Obsérvese que en principio no se puede excluir el caso $k = 0$.

La fórmula Ψ' es una fórmula sin cuantificadores en las variables X,Y, equivalente a Ψ y por lo tanto también a Φ_ℓ en $\mathcal{L}_\Omega^\Omega$. Es decir Ψ' define también el subconjunto M_ℓ de Ω^2, que es cerrado en la topología de Zariski de Ω^2. El conjunto M_ℓ es por lo tanto unión de conjuntos definidos por conjunciones del tipo $(*)$. Al ser M_ℓ cerrado y distinto de Ω^2, tiene que ser $k > 0$ en cada conjunción $(*)$ que define a M_ℓ (pues sino M_ℓ contendría un abierto (denso) de la topología de Zariski de Ω^2). Es decir en cada conjunción $(*)$ de la fórmula Ψ' aparece alguna condición $G_i = 0$.

Además, el Teorema de la Dimensión (ver por ejemplo [La], II, 7, Th.II) permite afirmar que si $k \ge 2$, entonces $(*)$ define un subconjunto *finito* de Ω^2 (dado que los polinomios $G_{i_1},\ldots,G_{i_k}$ de $(*)$ son todos irreductibles y distintos).

Por lo tanto M_ℓ se escribe como unión de conjuntos definidos por conjunciones $(*)$ con $k = 1$ y conjuntos finitos.

Dado que M_ℓ es infinito, existe por lo menos una conjunción $(*)$ con $k = 1$. Consideremos entonces una conjunción de este tipo de Ψ'. Podemos suponer que es

$$(**) \qquad G_1 = 0 \wedge G_2 \neq 0 \wedge \ldots \wedge G_t \neq 0$$

Dado que G_1 es primo y $(**)$ es consistente, la clausura del subconjunto de Ω^2 definido por $(**)$ es $\{G_1 = 0\}$. Por otro lado se sabe que M_ℓ es cerrado, y por lo tanto $\{G_1 = 0\} \subseteq M_\ell$. Se deduce así que M_ℓ se puede escribir como unión finita de conjuntos $\{G_j = 0\}$ y conjuntos finitos.

Por otra parte, $X^{2^{2^\ell}} - Y$ es un polinomio irreducible de $\Omega[X,Y]$ y M_ℓ es el gráfico de $\{X^{2^{2^\ell}} - Y = 0\}$, o sea un conjunto irreductible. Es decir que $X^{2^{2^\ell}} - Y = 0$ es la ecuación minimal de la hipersuperficie irreductible M_ℓ de $\Omega[X,Y]$.

Por consiguiente se tiene que M_ℓ es irreductible e infinito y que los conjuntos $\{G_j = 0\}$ y los conjuntos finitos que aparecen en la decomposición de M_ℓ son cerrados. Es decir que, existe $j \in \{1,\ldots,t\}$ tal que $\{X^{2^{2^\ell}} - Y = 0\} = M_\ell = \{G_j = 0\}$. Dado que $X^{2^{2^\ell}} - Y = 0$ es la ecuación minimal de M_ℓ, $X^{2^{2^\ell}} - Y = G_j$ y $gr(G_j) = 2^{2^\ell}$.

3.- *DEMOSTRACION DE LA APLICACION 4*

A. Se puede calcular la dimensión proyectiva de X en tiempo secuencial $D^{n^{O(1)}}$ y tiempo paralelo $(n \log D)^{O(1)}$, aplicando por ejemplo [Ca 1] o [Di-Fi-Gi-Se].

Sea $r := \dim X$, y para todo i, $0 \leq i \leq r$, sea

$L^{(i)} := Y_0^i X_0 + \ldots + Y_n^i X_n$, donde $(Y_j^i)_{\substack{0 \leq i \leq r \\ 0 \leq j \leq n}}$ son nuevas indeterminadas sobre $\Omega[X_0,\ldots,X_n]$.

Sea $\Gamma \subseteq (\mathbf{P}^n)^{r+1} \times \mathbf{P}^n$ el conjunto de ceros del ideal generado por $F_1,\ldots,F_s,L^{(0)},\ldots,L^{(r)}$ en $\Omega[X_0,\ldots,X_n,Y_j^i]_{\substack{0 \leq i \leq r \\ 0 \leq j \leq n}}$.

B. Sea $\varphi : (\mathbf{P}^n)^{r+1} \times \mathbf{P}^n \to (\mathbf{P}^n)^{r+1}$ la proyección canónica.

El Lema 4 de [Ne] muestra que $\varphi(\Gamma)$ es un conjunto cerrado. Además como $\mathrm{rad}(I)$ es un ideal unmixed (i.e. todos sus primos tienen misma dimensión) ya que I es débilmente unmixed, se tiene que $\varphi(\Gamma) = \{y \in (\mathbf{P}^n)^{r+1} : F(y) = 0\}$ para algún poli-

nomio $F \in \Omega[Y_j^i]_{\substack{0\le i\le r\\ 0\le j\le n}}$. Entonces el polinomio $\mathrm{rad}(F)$ es el polinomio de Chow del ideal $\mathrm{rad}(I)$ (donde con $\mathrm{rad}(F)$ se nota el polinomio libre de cuadrados formado por los factores irreductibles de F). (Ver [Ne], Prop. 2 y Corollary Prop. 3).
Por simplicidad, supondremos directamente que F es libre de cuadrados.

C. Sea $W := \{w \in \Omega^{(n+1)(r+1)} : F(w) = 0\}$.
W se puede describir por medio de la fórmula Φ:

$$(\exists X_0)\dots(\exists X_n)(F_1(X_0,\dots,X_n) = 0 \wedge \dots \wedge F_s(X_0,\dots,X_n) = 0$$
$$\wedge L^{(0)}(X_0,\dots,X_n,Y_0^0,\dots,Y_n^0) = 0 \wedge \dots \wedge L^{(r)}(X_0,\dots,X_n,Y_0^r,\dots,Y_n^r) = 0)$$

con un solo bloque de cuantificadores, con $(n+1)(r+2)$ variables y tal que $D(\Phi) = D + 2(r+1)$.
Aplicando el algoritmo rápido de eliminación de cuantificadores presentado en el Teorema 2, se obtiene una fórmula Ψ sin cuantificadores, equivalente a Φ, en tiempos

- paralelo $\quad \big((n+1)(r+2)\log(D+2(r+1))\big)^{0(1)} = (n \log D)^{0(1)}$
- secuencial $\quad (D+2(r+1))^{((n+1)(r+2))^{0(1)}} = D^{n^{0(1)}}$

La fórmula Ψ (sin cuantificadores) obtenida es una disjunción de conjunciones donde aparecen ciertos polinomios $G_1,\dots,G_M \in \Omega[Y_j^i]_{\substack{0\le i\le r\\ 0\le j\le n}}$. Además, se puede aplicar un test rápido de consistencia para decir cuáles de las conjunciones
$G_{k_1} = 0 \wedge \dots \wedge G_{k_m} = 0 \wedge G_{k_{m+1}} \neq 0$ definen subconjuntos vacíos de $\Omega^{(n+1)(r+1)}$.
Por lo tanto se puede suponer que se obtuvo una descripción de W como sigue:
$W := \bigcup_k W_k$ donde

(i) W_k tiene la forma $\{G_{k_1} = 0 \wedge \dots \wedge G_{k_m} = 0 \wedge G_{k_{m+1}} \neq 0\}$, con
$G_{k_\ell} \in K[Y_j^i]_{\substack{0\le i\le r\\ 0\le j\le n}}$ y $\sum_{k,\ell} gr\, G_{k_\ell} = D^{n^{0(1)}}$

(ii) $W_k \neq \emptyset$ para todo k.

D. La versión efectiva del Nullstellensatz de por ejemplo [Ca-G-H 2] o del lema de Noether de [Di-Fi-Gi-Se] permite para todo k calcular la dimensión $\dim_\Omega W_k$ (en tiempos $D^{n^{0(1)}}$ y $(n \log D)^{0(1)}$ respectivamente).
Se define $N := (n+1)(r+1)$ y sea $\mathrm{I} = \{k : \dim W_k = N-1\}$.
Se tiene $\mathrm{I} \neq \emptyset$ pues $\dim_\Omega W = N-1$ y $W = \cup W_k$.

E. Sea $k_0 \in \mathrm{I}$, y pongamos $W_{k_0} := \{G_1 = 0 \wedge \ldots \wedge G_m = 0 \wedge G_{m+1} \neq 0\}$.

Si G_{m+1} no aparece, se pone $G_{m+1} = 1$.

Se tiene $m > 0$ pues sino $\dim_\Omega W_{k_0} = N$.

Sea $F := F_1 \ldots F_t$ la descomposición en factores irreductibles (y coprimos) del polinomio de Chow F de $\mathrm{rad}(I)$.

Dado que $\dim_\Omega W_{k_0} = N - 1$, existe $1 \leq \ell \leq t$ tal que si $Z(F_\ell) := \{F_\ell = 0\}$, $\dim_\Omega(Z(F_\ell) \cap W_{k_0}) = N - 1$, y así, para todo i, $1 \leq i \leq m$, se tiene $Z(F_\ell) \subseteq Z(G_i)$. Por lo tanto $F_\ell | G_i$ $(1 \leq i \leq m)$ y $F_\ell \not| G_{m+1}$.

F. Para todo $k \in \mathrm{I}$, sea $M_k := (G_{k_1} : \ldots : G_{k_m})$ y pongamos

$$T_k := \frac{\mathrm{rad}(M_k)}{(G_{k_{m+1}} : \mathrm{rad}(M_k))} \in K[Y_j^i]_{\substack{0 \leq i \leq r \\ 0 \leq j \leq n}}$$

La construcción de M_k y de T_k puede hacerse en tiempo $D^{m^{O(1)}}$ (secuencial) y $(n \log D)^{O(1)}$ (paralelo) por medio de los algoritmos rápidos de cálculo de máximo común divisor (ver [Bro], que aplica al cálculo de máximo común divisores teoría de subresultantes y sucesiones de restos polinomiales desarrollada por [Co]). Es aquí donde si Ω tiene característica p, se aplica la suposición que se puede extraer raíces p-ésimas de polinomios.

Sea $T := \prod_{k \in \mathrm{I}} T_k$

Afirmación: $rad(T) = F$

Demostración: Alcanza con mostrar que los únicos factores irreducibles que dividen a T son exactamente $F_1, \ldots, F_t$.

Sea $1 \leq j \leq t$. Se tiene:

$Z(F_j) = \bigcup_k (W_k \cap Z(F_j))$

Existe, por lo tanto, k_0 tal que $\dim_\Omega(W_{k_0} \cap Z(F_j)) = N - 1$ (ya que $\dim Z(F_j) = N - 1$), por lo tanto $k_0 \in \mathrm{I}$, y por la etapa **E** se obtiene que $F_j | T_{k_0}$.

Por consiguiente $F | T$.

Para finalizar, se supone que T tiene un factor irreducible H que no divide a F, y sea $k_0 \in \mathrm{I}$ tal que $H | T_{k_0}$.

Entonces $H | M_{k_0}$ y $H \not| G_{k_{0_{m+1}}}$.

Así, se obtiene $Z(H) \cap \{G_{k_{0_{m+1}}} \neq 0\} \subseteq W_{k_0} \subseteq W$,

y $\dim_{\Omega}(Z(H) \cap \{G_{k_{0_{m+1}}} \neq 0\}) = N-1$. Se tendría entonces $Z(H) \subseteq W := Z(F)$, y por lo tanto $H|F$. Contradicción.

G. Finalmente se calcula $\mathrm{rad}\,(T)$ en tiempo secuencial $D^{n^{O(1)}}$ y paralelo $(n \log D)^{O(1)}$ y queda probado el resultado.

♦

4.- DEMOSTRACION DE LA OBSERVACION 6

(i) La afirmación sobre el grado forma parte del enunciado del Teorema 3 de [He-Ro-So 2] (o bien del Teorema 5 de [He-Ro-So 3]). La cota para $\nu(\Psi)$ se obtiene por simple inspección del algoritmo mencionado.

(ii) La aparición en $d(\Psi)$ de $D := \sum_{1 \leq i \leq s} gr\, F_i$ se debe a la etapa de reducción (a) (siguiendo la notación de [He-Ro-So 2]) y a la eliminación de una variable (última parte de la demostración de [He-Ro-So 2], Théorème 3). El exponente $O(n)$ proviene de la aplicación del Nullstellensatz efectivo (que interviene en el algoritmo para cuerpos algebraicamente cerrados que se utiliza) (parte (c) de [He-Ro-So 2]) y del cálculo de una base standard en dimensión 0 (parte (d)).

La cota para $\nu(\Psi)$ se obtiene haciendo el mismo razonamiento que para el grado.

II. UNA COTA GEOMETRICA PARA LA PROGRAMACION ENTERA CON RESTRICCIONES POLINOMIALES

INTRODUCCION Y NOTACIONES

En todo lo que sigue, $\mathbb{R}$ notará el cuerpo de los números reales y $\mathbb{Z}$ el anillo de los números enteros.

Sean $X_1, \ldots, X_n$ indeterminadas sobre $\mathbb{R}$.

Se dice que un polinomio $F \in \mathbb{R}[X_1, \ldots, X_n]$ es *cuasiconvexo* si para todo $\lambda \in \mathbb{R}$ el conjunto de nivel $\{x \in \mathbb{R}^n : F(x) \leq \lambda\}$ es un subconjunto convexo de $\mathbb{R}$.

También se adoptará la siguiente convención:

Si V es un conjunto finito de vectores de $\mathbb{Z}^n$, notaremos por $\sigma(V)$ la longitud binaria máxima de todas las coordenadas de todos los vectores de V. Análogamente, si $\mathcal{F} \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ es un conjunto finito de polinomios, $\sigma(\mathcal{F})$ será la longitud binaria máxima de todos los coeficientes (¡enteros!) que aparecen en todos los polinomios de $\mathcal{F}$.

A lo largo de este capítulo, $F_0, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$ serán polinomios cuasiconvexos en n variables y a coeficientes enteros, de grado total acotado por un número $d \geq 2$, y tal que $\sigma(\{F_0, \ldots, F_s\}) \leq \sigma$.

El propósito de este capítulo es el de probar los siguientes teoremas:

TEOREMA 1. *Si el conjunto $\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ es no vacío, entonces contiene un punto (entero) en una bola cerrada $B(0, R)$, centrada en el origen, y de radio R de longitud binaria acotada por $(sd)^{0(n^2)} \cdot \sigma$.*
El valor de la constante que interviene en el término $0(n^2)$ se puede calcular y es intrínseco al algoritmo (no depende de los parámetros s, d, n, σ considerados).

Este teorema geométrico conduce al corolario algorítmico siguiente:

COROLARIO 1.1. *Se puede decidir por medio de una máquina de Turing no determinística si el conjunto $\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ es no vacío en tiempo $(sd)^{n^{0(1)}} \cdot \sigma$.*

En otras palabras, el problema de la programación entera, que involucra únicamente polinomios cuasiconvexos, en tanto que problema de decisión pertenece a la clase de com-

plejidad NEXPTIME ("non deterministically simply exponential time"). Esto significa que se puede *verificar* si un candidato a solución del sistema es solución en tiempo (secuencial) simplemente exponencial.

TEOREMA 2. *Supongamos que el conjunto* $\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ *es no vacío y consideremos ahora también el polinomio (cuasiconvexo)* F_0. *Si el ínfimo de los valores de* $F_0(x)$, *con* x *tomado en el conjunto* $\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ *se realiza, entonces coincide con el ínfimo de los valores de* $F_0(x)$, *con* x *tomado en el conjunto* $\{x \in \mathbb{Z}^n \cap B(0, \tilde{R}) : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$, *donde el radio* $\tilde{R}$ *tiene longitud binaria acotada por* $(sd)^{n^{O(1)}} . \sigma$.

Expresado de otra manera: Si $\{F_1 \leq 0, \ldots, F_s \leq 0\} \cap \mathbb{Z}^n \neq \emptyset$, entonces
$\inf \{F_0(x),\ x \in \mathbb{Z}^n \cap \{F_1 \leq 0, \ldots, F_s \leq 0\}\} = \mu > -\infty$
$\Longrightarrow \mu = \inf\{F_0(x),\ x \in \mathbb{Z}^n \cap \{F_1 \leq 0, \ldots, F_s \leq 0\} \cap B(0, \tilde{R})\}$
donde $\tilde{R}$ es tal que $\sigma(\tilde{R}) = (sd)^{n^{O(1)}} . \sigma$.

El resultado del Teorema 1 mejora una cota superior del tipo $\sigma(R) = (d^{(\tilde{n}+d)} n^d)^{O(1)} \sigma$ (con $\tilde{n} := \min\{s, n\}$) anunciada por Khachiyan y Tarasov ([Ta-Kh] y [Kh]), para el caso de polinomios convexos (que constituyen un caso particular de los polinomios considerados aquí).

Por otro lado el carácter exponencial de la cota obtenida es intrínseco al problema, como lo muestra el ejemplo siguiente estudiado en [Ta-Kh]:
Al considerar los n polinomios cuadráticos y convexos, $F_1 = -X_1 + 2^\sigma$, $F_2 = X_1^2 - X_2, \ldots$, $F_n = X_{n-1}^2 - X_n$ (de grado acotado por 2 y tales que $\sigma(\{F_1, \ldots, F_n\}) = \sigma$), los autores muestran que todas las soluciones, aún reales, del sistema $F_1(x) \leq 0, \ldots, F_n(x) \leq 0$ se hallan fuera de la bola $B(0, R)$, con $\sigma(R) = 2^{n-1} . \sigma$. Es decir, la cota obtenida en el Teorema 1 es optimal, como medida general de complejidad, en término de los parámetros considerados.

1.- DEMOSTRACION DEL TEOREMA 1

La prueba se basa en técnicas de reducción para la programación cuasiconvexa desarrolladas por B. Bank y R. Mandel ([Ba-Ma 1], cap. 4 y 5, y [Ba-Ma 2]). Se aplican también fundamentalmente los resultados precisos de geometría semialgebraica algorítmica sobre $\mathbb{R}$ que

resultan del examen del algoritmo "rápido" de eliminación de cuantificadores para cuerpos real cerrados ([So], [He-Ro-So 2], [He-Ro-So 3] o bien [Re]), presentados en el Capítulo I *(Observación 6)*.

1.-A. Propiedades de polinomios cuasiconvexos

El fin de esta sección es mostrar tres propiedades fundamentales de los polinomios cuasiconvexos, indispensables para la obtención de las cotas buscadas. Son las siguientes:

PROPOSICION A.1. Sea $F \in \mathbb{R}[X_1,\ldots,X_n]$ cuasiconvexo.
Sean $x,u \in \mathbb{R}^n$, $u \neq 0$. Si el polinomio $F(x+Tu)$ en la variable T es estrictamente decreciente (respectivamente constante), entonces el polinomio $F(y+Tu)$ es estrictamente decreciente (respectivamente constante) para todo $y \in \mathbb{R}^n$.
Esta es una suerte de propiedad de "uniformidad" de los polinomios cuasiconvexos, ya que el carácter de decrecimiento (estricto) o de constancia se mantiene sobre todas las direcciones paralelas.

PROPOSICION A.2. (Propiedad de "linealidad" de los polinomios cuasiconvexos).
Sea $F = \sum_{0\leq i\leq d} P_i \in \mathbb{R}[X_1,\ldots,X_n]$ un polinomio cuasiconvexo, escrito como suma de formas homogéneas P_i de grado i.
Entonces para todo $0 \leq i \leq d$, se tiene que el conjunto:
$L_i := L_i(F) := \{x \in \mathbb{R}^n : P_d(x) = 0,\ldots,P_i(x) = 0\}$ es un subespacio lineal de $\mathbb{R}^n$
y que el conjunto:
$K_i := K_i(F) := \{x \in \mathbb{R}^n : P_d(x) = 0,\ldots,P_{i+1}(x) = 0,\ P_i(x) \leq 0\}$ o bien es un semisubespacio lineal de $\mathbb{R}^n$ (que contiene a L_i), o bien coincide con L_i.
Si además F tiene coeficientes enteros, se muestra que L_i admite una base entera $\mathcal{B}_i$ con $\sigma(\mathcal{B}_i) = \tilde{d}^{0(n^2)}\sigma(F)$, donde $\tilde{d} := \max\{2,d\}$. Análogamente, K_i admite un sistema de generadores $\mathcal{G}_i := \{v_1,\ldots,v_\ell\}$ (es decir $K_i = \{\sum_{1\leq i\leq \ell} \lambda_i v_i,\ \lambda_i \geq 0\}$), tal que $\sigma(\mathcal{G}_i) = \tilde{d}^{0(n^2)}\sigma(F)$ (donde $\tilde{d} := \max\{2,d\}$).

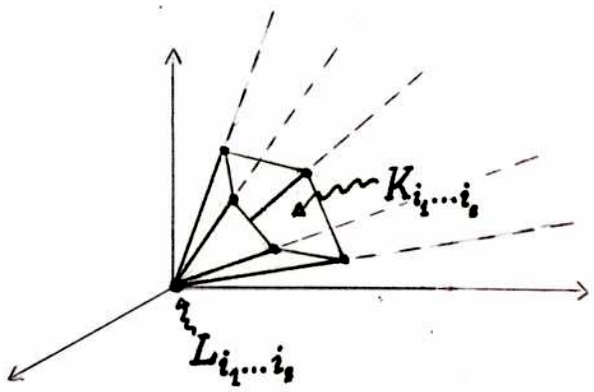
A.3. PROPOSICION. Sean $F_1,\ldots,F_s \in \mathbb{Z}[X_1,\ldots,X_n]$ cuasiconvexos de grado $d_1,\ldots,d_s$ respectivamente. Sea $\tilde{d} := \max\{d_1,\ldots,d_s,2\}$. Entonces para todo $0 \leq i_j \leq d_j$ $(1 \leq j \leq s)$, siguiendo la notación de la Proposición A.2, el conjunto:

$L_{i_1 \ldots i_s} := L_{i_1}(F_1) \cap \ldots \cap L_{i_s}(F_s)$ es un subespacio lineal de $\mathbf{R}^n$, que admite una base entera $\mathcal{B}$ con $\sigma(\mathcal{B}) = \tilde{d}^{0(n^2)}\sigma$

y el conjunto:

$K_{i_1 \ldots i_s} := K_{i_1}(F_1) \cap \ldots \cap K_{i_s}(F_s)$

es un cono poliedral de $\mathbf{R}^n$ (es decir una intersección finita de semiespacios lineales de $\mathbf{R}^n$) que admite un sistema de generadores $\mathcal{G}$ con $\sigma(\mathcal{G}) = \tilde{d}^{0(n^2)}\sigma$.



Las demostraciones de las tres proposiciones abarcan desde la Observación A.4 hasta el Lema A.9.

OBSERVACION A.4.

(i) La definición de polinomio cuasiconvexo dada más arriba admite la formulación equivalente:

Para todo $x, y \in \mathbf{R}^n$, para todo $\alpha \in (0,1)$, se verifica:

$$F(\alpha x + (1-\alpha)y) \leq \max\{F(x), F(y)\}$$

Esta definición alternativa permite deducir inmediatamente que los polinomios convexos constituyen un caso particular de estos. Más aún, existen polinomios cuasiconvexos que no son convexos, como por ejemplo el polinomio X^3, y por lo tanto la clase de polinomios cuasiconvexos es estrictamente más amplia que la de polinomios convexos.

(ii) Sea ahora $F \in \mathbf{R}[X]$ un polinomio cuasiconvexo, en una sola variable. Entonces

- Si F es de grado par no nulo, F no puede tener coeficiente director negativo, pues en ese caso, dado que $\lim_{x \to +\infty} F(x) = \lim_{x \to -\infty} F(x) = -\infty$, existirían $x_1 < x_2 < x_3$ en $\mathbf{R}$ tales que $F(x_2) > \max\{F(x_1), F(x_3)\}$, lo que contradiría la cuasiconvexidad de F.
- Si F es de grado impar $\neq -1$, F es una función de $\mathbf{R}$ en $\mathbf{R}$ estrictamente creciente o estrictamente decreciente, según el signo de su coeficiente director, ya que un polinomio cuasiconvexo (no nulo) de grado impar no admite máximos ni mínimos locales (pues $\lim_{x \to +\infty} F(x) \neq \lim_{x \to -\infty} F(x)$).

– En ambos casos, un polinomio cuasiconvexo no constante en una variable no admite máximos locales.

LEMA A.5 Sea $F = \sum_{i=0}^{d} P_i \in \mathbb{R}[X_1, \ldots, X_n]$ un polinomio cuasiconvexo de grado d, escrito como en la Proposición A.2 como suma de formas homogéneas de grado i. Entonces

(i) La forma P_d resulta cuasiconvexa también.

(ii) Dadas $x, u \in \mathbb{R}^n . (u \neq 0)$, el polinomio F_x en la variable T, dado por $F_x(T) := F(x + Tu)$ es cuasiconvexo.
Además si el polinomio $F_y(T) := F(y + Tu)$ $(y \in \mathbb{R}^n)$ es el polinomio F considerado sobre la recta paralela en y a la recta $\{x + tu,\ t \in \mathbb{R}\}$, se tiene que F_x y F_y o bien son ambos constantes, o bien tienen mismo grado $r \neq -1, 0$, y en ese caso, tienen el mismo coeficiente director.

Demostración:

(i) Sean $x, y \in \mathbb{R}^n$, y $\alpha \in (0,1)$ fijado. Se quiere probar que $P_d(\alpha x + (1-\alpha)y) \leq \max\{P_d(x), P_d(y)\}$

Pero $P_d(x) = \lim_{t \to +\infty} t^{-d} F(tx)$

y $F\big(t(\alpha x + (1-\alpha)y)\big) = F\big(\alpha(tx) + (1-\alpha)(ty)\big) \leq \max\{F(tx), F(ty)\}$.

O sea, para $t > 0$, $t^{-d} F\big(t(\alpha x + (1-\alpha)y)\big) \leq \max\{t^{-d}F(tx), t^{-d}F(ty)\}$, y el resultado se obtiene tomando límite.

(ii) Sean $t_1, t_2 \in \mathbb{R}$, $\alpha \in (0,1)$ arbitrarios

$$\begin{aligned} &F_x(\alpha t_1 + (1-\alpha)t_2) = F(x + (\alpha t_1 + (1-\alpha)t_2)u) = \\ &= F(\alpha(x + t_1 u) + (1-\alpha)(x + t_2 u)) \leq \\ &\max\{F(x + t_1 u), F(x + t_2 u)\} = \max\{F_x(t_1), F_x(t_2)\} \end{aligned}$$

Por lo tanto F_x es cuasiconvexa. Pongamos:

$$\begin{aligned} F_x(T) &= a_r T^r + \ldots + a_0 \qquad (a_r \neq 0) \\ F_y(T) &= b_s T^s + \ldots + b_0 \qquad (b_s \neq 0) \end{aligned}$$

y $\alpha \in (0,1)$ fijado. Elijamos ahora $v_\alpha, w_\alpha \in \mathbb{R}^n$ tales que

$$y = \alpha x + (1-\alpha)v_\alpha \qquad \text{y} \qquad x = \alpha y + (1-\alpha)w_\alpha$$

pertenezcan de esa manera respectivamente a los segmentos (x, v_α) e (y, w_α).

Por la cuasiconvexidad de F, se obtiene que para todo $t \in \mathbb{R}^n$ vale

$$\begin{cases} F(y + \alpha tu) \leq \max\{F(x + tu), F(v_\alpha)\} \\ F(x + \alpha tu) \leq \max\{F(y + tu), F(w_\alpha)\} \end{cases}$$

o sea, para todo $t \in \mathbb{R}^n$ vale:

$$(*) \qquad \begin{cases} b_s(\alpha t)^s + \ldots + b_0 \leq \max\{a_r t^r + \ldots + a_0,\ F(v_\alpha)\} \\ a_r(\alpha t)^r + \ldots + a_0 \leq \max\{b_s t^s + \ldots + b_0,\ F(w_\alpha)\} \end{cases}$$

Tomando en cuenta que si s (resp. r) es par > 0, b_s (resp. a_r) no puede ser negativo (Observación A.4(ii)), y que por lo tanto en cualquier caso en que r y s son mayores que 0, los miembros de la isquierda en $(*)$ se pueden hacer arbitrariamente grandes (eligiendo $t \to \pm\infty$), se deduce que $r = s$ (ya que $F(v_\alpha)$ y $F(w_\alpha)$ quedan fijados por el valor de α). Más aún, en ese caso $(r \geq 1)$, el examen de las dos desigualdades muestra que a_r y b_r tienen mismo signo.

Supongamos que se tiene a_r y b_r positivos, y $a_r \neq b_r$, por ejemplo $0 < b_r < a_r$. Eligiendo entonces adecuadamente $\alpha \in (0, 1)$ tal que se mantenga la desigualdad $0 < b_r < a_r \alpha^r$ se contradice la segunda afirmación de $(*)$ para $t \to +\infty$.

En el caso en que a_r y b_r son ambos negativos (por lo tanto r es impar) y $0 > b_r > a_r$, se toma α de modo que $0 > br > a_r \alpha^r$ y $t \to -\infty$, llegando a la misma conclusión.

Con lo que resulta $a_r = b_r$.

Para concluir la demostración, falta considerar el caso en que F_x o F_y es constante. Pero en ese caso $(*)$ muestra que obligatoriamente los dos resultan simultáneamente constantes.

♦

Demostración de la Proposición A.1:

El caso $F(x + Tu)$ constante se deduce inmediatamente del Lema A.5(ii) anterior.

Si ahora $F_x(T) = F(x + Tu) = a_r T^r + \ldots + a_0 \quad (a_r \neq 0)$ es estrictamente decreciente, se deduce por la Observación A.4(ii) que $r \geq 1$ es impar y que $a_r < 0$.

Sean $t_1, t_2 \in \mathbb{R}$ tales que $t_1 < t_2$. Se quiere probar que $F_y(t_1) = F(y + t_1 u) > F(y + t_2 u) = F_y(t_2)$ (es decir F_y es estrictamente decreciente también).

Dado que el coeficiente director de F_y es igual al de F_x (por el lema anterior) y por lo tanto negativo, se puede elegir $t_3 > t_2$ de manera que $F_y(t_3) < \min\{F_y(t_1), F_y(t_2)\}$. Por

lo tanto se tiene que t_2 pertenece al segmento (t_1, t_3) y entonces, por la cuasiconvexidad de F_y, resulta

$$F_y(t_2) \leq \max\{F_y(t_1), F_y(t_3)\} = F_y(t_1)$$

Por último, si fuera $F_y(t_2) = F_y(t_1)$, o bien el polinomio F_y sería constante en el segmento (t_1, t_2) (Absurdo pues $r \geq 1$), o bien existiría t_4 con $t_4 < t_2 < t_3$ tal que

$$F_y(t_2) > \max\{F_y(t_4), F_y(t_3)\} \qquad \text{(Observación A.4(ii))}$$

Absurdo por ser F_y cuasiconvexo. Por lo tanto tiene que ser $F_y(t_2) < F_y(t_1)$.

La Proposición A.1 permite mostrar el resultado siguiente, preliminar teórico para la Proposición A.2

LEMA A.6. Sea $P_d \in \mathbb{R}[X_1, \ldots, X_n]$ una forma homogénea cuasiconvexa de grado $d \geq 1$. Sean

$$L := \{x \in \mathbb{R}^n : P_d(x) = 0\}$$
$$K := \{x \in \mathbb{R}^n : P_d(x) \leq 0\}$$

Entonces se cumple

(i) L es un subespacio lineal de $\mathbb{R}^n$.

(ii) Si d es par, $L = K$.

(iii) Si d es impar, entonces L es un hiperplano de $\mathbb{R}^n$ y K es un semiespacio (limitado por L).

Demostración:

(i) Sea V el subespacio lineal de $\mathbb{R}^n$, de dimensión máxima contenido en L (existe pues $0 \in L$), y supongamos que existe $u \in L$ tal que $u \notin V$.
Dado que $u \in L$, se tiene que $P_d(tu) = t^d P_d(u) = 0$, $\forall t \in \mathbb{R}$, y por lo tanto $P_d(x + Tu)$ es un polinomio constante para cualqnier elección de $x \in \mathbb{R}^n$ (Proposición A.1). Consideremos entonces el subespacio lineal $\langle V, u \rangle := \{v + tu, t \in \mathbb{R}, v \in V\}$ (que verifica $V \subsetneq \langle V, u \rangle$).
Se tiene que $P_d(v + tu) = P_d(v)$ $(\forall t \in \mathbb{R})$ por ser constante, y $P_d(v) = 0$ $(\forall v \in V)$ implica $P_d(v + tu) = 0$ $(\forall v \in V)$. Por lo tanto sería $\langle V, u \rangle \subseteq L$, lo que contradiría la elección de V.

(ii) Sea d par y supongamos que existe $x \in \mathbb{R}^n$ tal que $P_d(x) < 0$. Entonces se tendría

$P_d(-x) = (-1)^d P_d(x) = P_d(x) < 0$ y resultaría $0 = P_d(0) \leq \max\{P_d(x), P_d(-x)\} < 0$. Contradicción.

(iii) Sea d impar.

Se tiene que $L \neq \mathbb{R}^n$ pues $P_d \neq 0$.

Supongamos que $\dim_{\mathbb{R}} L < n-1$. Por lo tanto se pueden elegir x e y linealmente independientes en el complemento ortogonal $L^\perp$ de L.

Al ser d impar, se puede suponer $P_d(x) < 0$ y $P_d(y) > 0$ (tomando eventualmente $-x$ en lugar de x, etc...).

Por lo tanto, por la continuidad de P_d, existe $\alpha \in (0,1)$ tal que $P_d(\alpha x + (1-\alpha)y) = 0$. Pero por otro lado $\alpha x + (1-\alpha)y \neq 0$ al ser x e y linealmente independientes. Eso contradice la condición $L \cap L^\perp = \{0\}$ y luego L es un hiperplano de $\mathbb{R}^n$.

Sea ahora $L^\perp = \{ty,\ t \in \mathbb{R}\}$, con y elegido de manera que $P_d(y) < 0$. Se afirma que $K := \{x \in \mathbb{R}^n : P_d(x) \leq 0\} = \{x \in \mathbb{R}^n : {}^t y \,.\, x \geq 0\}$ (o sea el semiespacio positivo limitado por el hiperplano ${}^t y \,.\, x = 0$):

Sea $x \in \mathbb{R}^n$; x admite una decomposición en forma única $x = x' + ty$, con $x' \in L$ y $t \in \mathbb{R}$.

Al ser d impar y $P_d(y) < 0$, se deduce que $P_d(ty) = t^d P_d(y)$ es estrictamente decreciente (Observación A.4(ii)) y por lo tanto, por la Proposición A.1, el polinomio $P_d(x' + Ty)$ también lo es; por lo tanto

$$P_d(x) = P_d(x' + ty) \leq P_d(x') = 0 \quad \Longleftrightarrow \quad t \geq 0$$

o sea $\qquad x \in K \Longleftrightarrow t \geq 0$

Luego $\qquad x \in K \Longleftrightarrow {}^t y \,.\, x = {}^t y(x' + ty) = t\,\|y\|^2 \geq 0.$

♦

Se probará en lo que sigue una versión constructiva de este lema, que exhibe una base $\mathcal{B}$ de L construída a partir de los coeficientes de la forma homogénea P_d. Para ello necesitaremos previamente el resultado siguiente:

LEMA A.7. Sea $F = \sum_{0 \leq i \leq d} P_i$ la escritura del polinomio cuasiconvexo F como suma de formas homogéneas con $P_d \neq 0$. Entonces existe una variable X_j $(1 \leq j \leq n)$ para la cual

el polinomio F es mónico en X_j (i.e. existe $a \in \mathbb{R} - \{0\}$ tal que el monomio aX_j^d aparece en P_d, o equivalentemente $gr_{X_j} P_d = d$).

Demostración: Sea $P_d(X_1, \ldots, X_n) = \sum_{i_1+\ldots+i_n=d} a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$ la forma (no nula) de mayor grado de F, y sea X_j cualquier variable que ocurre en P_d (es decir tal que $gr_{X_j} P_d > 0$). Se probará que $gr_{X_j} P_d = d$.

Sin pérdida de generalidad tomemos $j = 1$, y supongamos que $gr_{X_1} P_d < d$, o sea si $u := (1, 0, \ldots, 0)$, se tiene $P_d(u) = 0$. Por lo tanto, para todo $t \in \mathbb{R}$, $P_d(tu) = t^d P(u) = 0$. Dado que P_d es cuasiconvexo (Lema A.5(i)) aplicando la Proposición A.1 resulta que $P_d(x + Tu)$ es un polinomio constante, para todo $x \in \mathbb{R}^n$.

Por otro lado escribamos $P_d(X_1, \ldots, X_n) = a_r(X_2, \ldots, X_n) X_1^r + \ldots + a_0(X_2, \ldots, X_n)$ con $a_r(X_2, \ldots, X_n) \neq 0$ y elijamos $(x_2, \ldots, x_n) \in \mathbb{R}^{n-1}$ tal que $a_r(x_2, \ldots, x_n) \neq 0$.

Tomando ahora $x := (0, x_2, \ldots, x_n)$, resulta que

$$P_d(x + Tu) = P_d(T, x_2, \ldots, x_n) = a_r(x_2, \ldots, x_n) T^r + \ldots + a_0(x_2, \ldots, x_n)$$

tiene grado en T mayor que cero, y por lo tanto no puede ser un polinomio constante. Debía ser entonces $P_d(1, 0, \ldots, 0) \neq 0$.

Nota: De la demostración sigue que cualquier variable X_j que ocurre en P_d es tal que $gr_{X_j} P_d = d$.

♦

LEMA A.8. Sea $P_d \in \mathbb{Z}[X_1, \ldots, X_n]$ una forma cuasiconvexa homogénea de grado d, y a coeficientes enteros, con $\sigma := \sigma(P_d)$. Entonces el subespacio lineal $L := \{x \in \mathbb{R}^n : P_d(x) = 0\}$ admite una base *entera* $\mathcal{B}$ tal que $\sigma(\mathcal{B}) = \tilde{d}^{\mathcal{O}(n)} . \sigma$ donde $\tilde{d} := \max\{2, d\}$.

Análogamente, en el caso en que d es impar, el semiespacio K admite un sistema de generadores *enteros* $\mathcal{G}$ con $\sigma(\mathcal{G}) = \tilde{d}^{\mathcal{O}(n)} . \sigma$.

Demostración: Se procede por inducción en n.

Se puede claramente suponer $n \geq 2$.

Si $L \neq \{0\}$, sea $u \in L - \{0\}$.

Se tiene $P_d(tu) = t^d P_d(u) = 0$, $\forall t \in \mathbb{R}$, y por lo tanto para todo $x \in \mathbb{R}^n$, el polinomio $P_d(x + Tu)$ es constante como polinomio en T (Proposición A.1). Luego se cumple que

para todo $x \in \mathbb{R}^n$, $P_d(x+u) = P_d(x)$, o sea

$$(*) \qquad P_d(X+u) = P_d(X)$$

Supongamos además sin pérdida de generalidad y gracias al lema anterior, que X_1 es tal que $gr_{X_1} P_d = d$.
Se tiene entonces:

$$P_d(X_1,\ldots,X_n) = a_d(X_2,\ldots,X_n)X_1^d + a_{d-1}(X_2,\ldots,X_n)X_1^{d-1} + \ldots + a_0(X_2,\ldots,X_n)$$

donde $a_d(X_2,\ldots,X_n) \neq 0$, y para $0 \leq i \leq d$, $a_i(X_2,\ldots,X_n) \in \mathbb{Z}[X_2,\ldots,X_n]$ es una forma homogénea de grado $d-i$ (por lo tanto $a_d(X_2,\ldots,X_n) = a_d \in \mathbb{Z} - \{0\}$ y $a_{d-1}(X_2,\ldots,X_n) = \sum_{2\leq k\leq n} a_{1k}X_k$ es una forma lineal (entera)).
Evaluemos ahora P_d en $X+u := (X_1+u_1,\ldots,X_n+u_n)$

$$P_d(X+u) = a_d(X_1+u_1)^d + \Big(\sum_{2\leq k\leq n} a_{1k}(X_k+u_k)\Big)(X_1+u_1)^{d-1} +$$
$$+ a_{d-2}(X_2+u_2,\ldots,X_n+u_n)(X_1+u_1)^{d-2} + \ldots + a_0(X_2+u_2,\ldots,X_n+u_n)$$

Reordenando se obtiene

$$P_d(X+u) = P_d(X) + X_1^{d-1}(da_du_1 + \sum_{2\leq k\leq n} a_{1k}u_k) + \ldots + P_d(u)$$

Por lo tanto, dado que los términos en los puntos suspensivos son de grado menor que $(d-1)$ en X_1, aplicando $(*)$ se deduce que debe ser:

$$(**) \qquad da_du_1 + \sum_{2\leq k\leq n} a_{1k}u_k = 0 \qquad (\forall\, u \in L)$$

Luego L está incluído en el hiperplano $L^{(1)}$ definido por la condición $(**)$ (que es efectivamente un hiperplano dado que $a_d \neq 0$).
Este hiperplano $L^{(1)}$ admite la base entera

$$\{(-a_{12}, da_d, 0,\ldots,0),\ (-a_{13}, 0, da_d, 0,\ldots,0),\ldots,(-a_{1n}, 0,\ldots,0, da_d)\}$$

que se puede extender a una base entera $\mathcal{B}^{(1)}$ de $\mathbb{R}^n$ agregando el vector $(1,0,\ldots,0)$.
Observemos que $\sigma(\mathcal{B}^{(1)}) \leq \sigma + \log d$.

Si $(x_1,\dots,x_n)$ son las coordenadas de x en la base canónica e $(y_1,\dots,y_n)$ son sus coordenadas en la base $\mathcal{B}^{(1)}$, se tiene el cambio

$$(***)\qquad \begin{bmatrix} x_1 \\ \vdots \\ \\ \\ \\ \\ \vdots \\ x_n \end{bmatrix} = \left[\begin{array}{cc|c|cc} -a_{12} & -a_{13} & & -a_{1n} & 1 \\ da_d & 0 & & 0 & 0 \\ 0 & da_d & & & \\ \hline & & & & \\ \hline & & & 0 & 0 \\ 0 & & & da_d & 0 \end{array}\right] \begin{bmatrix} y_1 \\ \vdots \\ \\ \\ \\ \\ \vdots \\ y_n \end{bmatrix}$$

Mediante este cambio de coordenadas, se puede representar la forma cuasiconvexa original $P_d(x_1,\dots,x_n)$ por una forma cuasiconvexa en $y_1,\dots,y_n$ (representada en la base $\mathcal{B}^{(1)}$). Luego se restringe a $L^{(1)}$ poniendo $y_n = 0$, conservando los mismos ceros (módulo el cambio de base) ya que $L \subseteq L^{(1)}$.

La forma cuasiconvexa de grado d (o nula) $Q_d^{(1)}(Y_1,\dots,Y_{n-1})$ que se obtiene mediante este procedimiento es del tipo

$$Q_d^{(1)}(Y_1,\dots,Y_{n-1}) = a_d(-a_{12}Y_1 - \dots - a_{1n}Y_{n-1})^d + a_{d-1}(da_dY_1,\dots,da_dY_{n-1})\cdot(-a_{12}Y_1 - \\ - \dots - a_{1n}Y_{n-1})^{d-1} + \dots + a_0(da_dY_1,\dots,da_dY_{n-1})$$

y por lo tanto verifica la estimación "grosera"

$$\sigma(Q_d^{(1)}) \le (d+1)\sigma + d\log n + d\log d + \log(d+1)$$

En el caso en que L no coincida con $L^{(1)}$, esta forma $Q_d^{(1)}$ no es la forma nula y se repite el procedimiento con $Q_d^{(1)}(Y_1,\dots,Y_{n-1})$. Esto se hace a lo sumo $\dim_{\mathbf{R}} \mathbf{R}^n = n$ veces.

Supongamos que $L = L^{(r+1)}$ (donde r es tal que $0 \le r \le n-1$), es decir la forma $Q_d^{(r+1)}$ restringida a $L^{(r)}$ es la forma nula. Un cálculo desagradable arroja la estimación

$$\sigma(Q_d^{(r)}) \le (d+1)^r\sigma + (2^r-1)(d^r\log(nd) + d^{r-1}\log(d+1))$$

y la base $\mathcal{B}^{(r+1)}$ (o sea la base en que calculamos L) escrita en términos de la base $\mathcal{B}^{(r)}$ verifica

$$\sigma(\mathcal{B}^{(r+1)}) \le (d+1)^r\sigma + (2^r-1)(d^r\log(nd) + d^{r-1}\log(d+1)) + \log d$$

Finalmente se recupera la escritura de $\mathcal{B}^{(r+1)}$ en la base canónica (llamémosla $\mathcal{B}$), multiplicando r matrices del tipo $(***)$, obteniendo así en forma poco precisa

$$\sigma(\mathcal{B}) \leq (r-1)\log n + r((d+1)^r\sigma + (2^r-1)(d^r \log nd + d^{r-1}\log(d+1)) + \log d$$

Teniendo en cuenta que $r < n$, se obtiene

$$\sigma(\mathcal{B}) = (2d)^{O(n)} \cdot \sigma$$

o tomando $\tilde{d} := \max\{2, d\}$,

$$\sigma(\mathcal{B}) = \tilde{d}^{O(n)} \cdot \sigma$$

Observemos que el proceso anterior da un algoritmo para calcular una base entera de L en tiempo $\tilde{d}^{O(n)} \cdot \sigma$, ya que involucra solamente cálculos de algebra lineal (cambios de base y multiplicación de matrices).

En el caso en que d sea un número impar, el hiperplano L admite como vector normal el vector $(da_d, a_{12}, \ldots, a_{1n})$, con lo que se obtiene un sistema de generadores $\mathcal{G}$ de K, tal que $\sigma(\mathcal{G})$ verifica las mismas estimaciones que la base $\mathcal{B}$ de L.

♦

Ya ahora queda claro el proceso a seguir para la demostración de la Proposición A.2.

Demostración de la Proposición A.2:

Sea $F = \sum_{0 \leq i \leq d} P_i$ con $P_i(tX) = t^i P_i(X)$ y $P_d \neq 0$.

Por el lema anterior, se sabe que el conjunto $L_d := \{x \in \mathbb{R}^n : P_d(x) = 0\}$ es un subespacio lineal de $\mathbb{R}^n$. Restrinjamos entonces F a este subespacio L_d: se obtiene que $\deg(F|_{L_d}) \leq d-1$ y dado que por el Lema A.5(i) la forma homogénea de grado máximo de $F|_{L_d}$ es cuasiconvexa, se puede repetir el procedimiento. Así se concluye que para todo $0 \leq i \leq d$, el conjunto L_i es un subespacio lineal de $\mathbb{R}^n$, y de la misma manera K_i es o bien un semisubespacio lineal de $\mathbb{R}^n$, o bien coincide con L_i.

Hagamos ahora el análisis de las cotas para el caso en que F tenga coeficientes enteros:

Sea el subespacio lineal L_d de dimensión digamos r_d, y con base $\mathcal{B}^{(d)}$ que verifica (por el Lema A.8) $\sigma(\mathcal{B}^{(d)}) \leq \tilde{d}^{cn} \cdot \sigma$ donde $\tilde{d} := \max\{2, d\}$ y c es una constante universal.

Haciendo el cambio de coordenadas $\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = A \begin{pmatrix} Y_1 \\ \vdots \\ Y_{r_d} \end{pmatrix}$, donde $A \in \mathbb{Z}^{n \times r_d}$ tiene por columnas las coordenadas de los vectores de la base $\mathcal{B}^{(d)}$ de L_d, se obtiene $P_{d-1}(Y_1, \ldots, Y_{r_d})$ (que corresponde a P_{d-1} restringida a L_d), con:

$\sigma(P_{d-1}(Y_1,\ldots,Y_{r_d})) \leq (d+1)\tilde{d}^{cn}\sigma + d\log nd + \log(d+1) \leq c'\tilde{d}^{cn+1}\sigma$ (c' constante adecuada).

Sea $L'_{d-1} := \{(y_1,\ldots,y_{r_d}) \in \mathbb{R}^{r_d} : P_{d-1}(y_1,\ldots,y_{r_d}) = 0\}$. L'_{d-1} es un subespacio lineal de $\mathbb{R}^{r_d}$ que admite una base $\mathcal{B}^{(d-1)}$ con $\sigma(\mathcal{B}^{(d-1)}) \leq \tilde{d}^{cn}(c'\tilde{d}^{cn+1}\sigma) = c'\tilde{d}^{2cn+1}\sigma$ (según la demostración del Lema A.8).

Reiterando este procedimiento i veces, se obtiene una base $\mathcal{B}^{(i)}$ de $L'_i := \{(y_1,\ldots,y_{r_{i+1}}) \in \mathbb{R}^{r_{i+1}} : P_i(y_1,\ldots,y_{r_{i+1}}) = 0\}$, escrita en términos de la base $\mathcal{B}^{(i+1)}$ con $\sigma(\mathcal{B}^{(i)}) \leq c'^n\tilde{d}^{cn^2}\sigma$.

Finalmente, al recuperar la escritura de esta base $\mathcal{B}^{(i)}$ en términos de la base canónica (multiplicando matrices del tipo de A), se obtiene la estimación final $\sigma(\mathcal{B}) = \tilde{d}^{O(n^2)}\sigma$.

La afirmación con respecto a K_i es evidente, aplicando por ejemplo el lema auxiliar siguiente (que nos será útil a lo largo de esta sección): si $K_i \neq L_i$, se halla un vector ortogonal a L_i dentro de L_{i+1} que cumple la condición $P_i(x) \leq 0$. El sistema de generadores de K_i tiene entonces a lo sumo $2n$ vectores.

♦

LEMA A.9 (Lema auxiliar).

(i) Sean $\varphi_1,\ldots,\varphi_r \in \mathbb{Z}[X_1,\ldots,X_n]$ r ecuaciones lineales a coeficientes enteros, y sea $\sigma := \sigma(\{\varphi_1,\ldots,\varphi_r\})$. Se construye una base entera $\{v_1,\ldots,v_s\} \subseteq \mathbb{Z}^n$ del subespacio de $\mathbb{R}^n$ solución del sistema con

$$\sigma(\{v_1,\ldots,v_s\}) = n(\log n + \sigma)$$

(ii) Recíprocamente, sea $\{v_1,\ldots,v_s\} \subseteq \mathbb{Z}^n$ una familia finita de vectores enteros, y sea $\sigma := \sigma(\{v_1,\ldots,v_n\})$. Se construye un sistema de ecuaciones lineales $\varphi_1,\ldots,\varphi_r$, a coeficientes enteros, anulador del subespacio de $\mathbb{R}^n$ generado por $\{v_1,\ldots,v_s\}$ de manera que

$$\sigma(\{\varphi_1,\ldots,\varphi_r\}) = n(\log n + \sigma)$$

Demostración:

(i) Se puede suponer sin pérdida de generalidad que $\varphi_1,\ldots,\varphi_r$ son formas lineales linealmente independientes (y por lo tanto $r \leq n$).

Sea $\begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rn} \end{bmatrix}$ la matriz del sistema.

Se extrae de esta matriz una submatriz de rango r, digamos

$$A := \begin{bmatrix} a_{11} & \dots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rr} \end{bmatrix}$$

y se considera la matriz ampliada:

$$\left[\begin{array}{ccc|c} a_{11} & \dots & a_{1r} & -a_{1r+1}X_{r+1} - \dots - a_{1n}X_n \\ \vdots & & \vdots & \\ a_{r1} & \dots & a_{rr} & -a_{rr+1}X_{r+1} - \dots - a_{rn}X_n \end{array}\right]$$

Sea $A_i := \begin{bmatrix} a_{11} \dots -a_{1r+1}X_{r+1} - \dots - a_{1n}X_n \dots a_{1r} \\ \vdots \qquad\qquad\qquad\qquad \vdots \qquad\qquad \vdots \\ a_{r1} \dots -a_{rr+1}X_{r+1} - \dots - a_{rn}X_n \dots a_{rn} \end{bmatrix}$ la matriz que se obtiene reemplazando la columna i de A por la columna de la derecha de la matriz ampliada.

Aplicando la regla de Cramer, se tiene que para todo $1 \leq i \leq r$,

$$X_i = \frac{\det A_i}{\det A} = \frac{A_i^{(r+1)}X_{r+1} + \dots + A_i^{(n)}X_n}{\det A}$$

Tomando ahora alternadamente $X_{r+1} = \det A,\ X_{r+2} = 0, \dots, X_n = 0$

$$\vdots$$

$$X_{r+1} = 0, \dots, X_{n-1} = 0,\ X_n = \det A$$

se obtiene la siguiente base de soluciones del sistema:

$$\{(A_1^{(r+1)}, \dots, A_r^{(r+1)}, \det A, 0, \dots, 0), \dots, (A_1^{(n)}, \dots, A_r^{(n)}, 0, \dots, 0, \det A)\}$$

y es fácil ver que $\sigma(\det A) \leq r(\log r + \sigma)$

y $\sigma(A_i^{(j)}) \leq r(\log r + \sigma) \qquad (r+1 \leq j \leq n)$.

Luego resulta $\sigma(\{v_1, \dots, v_s\}) \leq n(\log n + \sigma)$.

(ii) En este caso se puede suponer de entrada $s \leq n$, extrayendo de la familia dada un sistema linealmente independiente sobre $\mathbb{R}$ maximal. Se construye el anulador de este sistema calculando por (i) una base entera del subespacio ortogonal a $\{v_1, \dots, v_s\}$ en $\mathbb{R}^n$.

Las cotas que se obtienen son por lo tanto las mismas.

♦

Podemos pasar ahora a la demostración de la Proposición A.3.

Demostración de la Proposición A.3.

La primera afirmación acerca de la longitud binaria de una base entera de $L_{i_1\ldots i_s}$ se desprende inmediatamente de la Proposición A.2 y del lema auxiliar anterior.

Es claro también que $K_{i_1\ldots i_s} = K_{i_1}(F_1) \cap \ldots \cap K_{i_s}(F_s)$ es un cono poliedral, ya que es una intersección finita de semisubespacios lineales de $\mathbb{R}^n$.

La estimación se sigue de la construcción hecha en la demostración del teorema de Farkas-Minkowski-Weyl ([Sc], Corollary 7.1a) que muestra que un cono convexo es poliedral (i.e. es una intersección finita de semiespacios lineales) si y sólo si admite un sistema finito de generadores (es decir una familia finita de vectores $\{v_1, \ldots, v_\ell\}$ tal que
$K = \Big\{ \sum_{1 \le i \le \ell} \lambda_i v_i,\ \lambda_i \ge 0 \Big\}$).

Para todo $1 \le j \le s$, se consiguen las matrices $A^{(j)}$ tales que $K_{i_j}(F_j) = \{x \in \mathbb{R}^n : A^{(j)}.x \le 0\}$ (aplicando la Proposición A.2 y el lema auxiliar A.9). Se obtiene $A^{(j)} \in \mathbb{Z}^{t \times n}$ (para algún $t \le 2n$) y $\sigma(A^{(j)}) = \tilde{d}^{0(n^2)}.\sigma$.

Busquemos ahora un sistema de generadores para $K_{i_1\ldots i_s} := K_{i_1}(F_1) \cap \ldots \cap K_{i_s}(F_s)$:

Sea $A := \begin{bmatrix} A^{(1)} \\ \hline \vdots \\ \hline A^{(s)} \end{bmatrix}$ la matriz tal que $K_{i_1\ldots i_s} = \{x \in \mathbb{R}^n : Ax \le 0\}$ y consideremos los vectores $\{a_1, \ldots, a_N\}$ formados por las filas de la matriz A (se tiene $N \le 2ns$).

– Primer caso: Supongamos que $\langle a_1, \ldots, a_N \rangle = \mathbb{R}^n$ (es decir el subespacio generado por $\{a_1, \ldots, a_N\}$ es todo $\mathbb{R}^n$). Se consideran entonces todos los semiespacios $S := \{x \in \mathbb{R}^n : \varphi_S(x) \le 0\}$ (φ_S forma lineal) que verifican

(i) $\{a_1, \ldots, a_N\} \subseteq S$

(ii) El hiperplano $H_S := \{x \in \mathbb{R}^n : \varphi_S(x) = 0\}$ está generado por $(n-1)$ vectores linealmente independientes $\{c_1, \ldots, c_{n-1}\}$, extraídos en la familia $\{a_1, \ldots, a_N\}$.

Dado que hay a lo sumo $\binom{N}{n-1} \le (2ns)^{n-1}$ elecciones posibles de $\{c_1, \ldots, c_{n-1}\}$ en estas

condiciones, se tienen a lo sumo $2(2ns)^{n-1}$ formas lineales φ_S posibles (que se construyen mediante A.9). Así resulta $\sigma(\varphi_S) = \tilde{d}^{0(n^2)} \cdot \sigma$.

Aplicando aquí el *Teorema Fundamental de Desigualdades Lineales* de programación lineal ([Sc], Teorema 7.1), se afirma que el cono $C\{a_1,\ldots,a_N\}$ generado por $\{a_1,\ldots,a_N\}$ es exactamente el cono poliedral determinado por la intersección de estos semiespacios S:

Recordemos para ello el enunciado del *Teorema Fundamental de Desigualdades Lineales:*

Sean $v_1,\ldots,v_m$, $w \in \mathbb{R}^n$. Entonces, o bien

(i) w es una combinación lineal no negativa de vectores linealmente independientes de la familia $\{v_1,\ldots,v_m\}$

o bien

(ii) existe un hiperplano $\{x : cx = 0\}$, que contiene $(t-1)$ vectores linealmente independientes de $\{v_1,\ldots,v_m\}$ tal que $cw > 0$ y $cv_1 \leq 0,\ldots,cv_m \leq 0$ (donde $t = \text{rango}\{v_1,\ldots,v_m,w\}$).

Probemos entonces la afirmación:

Si $b \in C\{a_1,\ldots,a_N\}$, entonces para todo semiespacio lineal S tal que $\{a_1,\ldots,a_N\} \in S$ se tiene claramente $b \in S$.

Recíprocamente, si $b \notin C\{a_1,\ldots,a_N\}$, b no cumple (i) del teorema de desigualdades lineales, y por lo tanto existe un hiperplano $H := \{x : cx = 0\}$ generado por $(n-1)$ vectores linealmente independientes de $\{a_1,\ldots,a_N\}$ tal que $ca_i \leq 0$ $(1 \leq i \leq N)$ y $cb > 0$, por lo tanto b no pertenece al semiespacio S determinado por H y $\{a_1,\ldots,a_N\}$.

Se afirma ahora que $K_{i_1\ldots i_s} := K_{i_1}(F_1) \cap \ldots \cap K_{i_s}(F_s)$ es el cono generado por los vectores $\{b_1,\ldots,b_M\}$, formados por los coeficientes de las formas lineales φ_S elegidas en el proceso, o sea $M \leq 2(2ns)^{n-1}$ y $\sigma(\{b_1,\ldots,b_M\}) = \tilde{d}^{0(n^2)} \cdot \sigma$.

Prueba de la afirmación:

Dado que ${}^t b_j \cdot a_i \leq 0$ $(1 \leq i \leq N,\ 1 \leq j \leq M)$, se tiene que $\{b_1,\ldots,b_M\} \subseteq K_{i_1\ldots i_s}$, y por lo tanto el cono $C\{b_1,\ldots,b_M\}$ generado por $\{b_1,\ldots,b_M\}$ también.

Recíprocamente, supóngase que existe $y \in K_{i_1\ldots i_s}$ tal que $y \notin C\{b_1,\ldots,b_M\}$. Dado que $C\{b_1,\ldots,b_M\}$ es un cono poliedral existe un vector w tal que ${}^t w b_1 \leq 0,\ldots,{}^t w b_M \leq 0$ y ${}^t w y > 0$; por lo tanto, por la definición de $C\{a_1,\ldots,a_N\}$, se tiene que $w \in C\{a_1,\ldots,a_N\}$, luego ${}^t w x \leq 0$, $\forall x \in K_{i_1\ldots i_s}$. Esto contradice el hecho que $y \in K_{i_1\ldots i_s}$ y ${}^t w y > 0$.

– Segundo caso: En el caso en que $\langle a_1,\ldots,a_N\rangle \subsetneq \mathbb{R}^n$, se extiende ortogonalmente $\{a_1,\ldots,a_N\}$ a un sistema de generadores de $\mathbb{R}^n$, aplicando el Lema A.9, y se procede

como en el primer caso considerando únicamente las familias $\{c_1,\ldots,c_{n-1}\}$ que contienen todos los vectores agregados (de manera que el suplemento ortogonal de $\langle a_1,\ldots,a_N\rangle$ está contenido en los hiperplanos H).

Finalmente se agregan las ecuaciones que determinan el subespacio $\langle a_1,\ldots,a_N\rangle$ de $\mathbb{R}^n$.

♦

1.-B. Eliminación de restricciones superfluas y reducción a un conjunto acotado

Sean como antes $F_1,\ldots,F_s \in \mathbb{Z}[X_1,\ldots,X_n]$ polinomios cuasiconvexos (a coeficientes enteros), sea $d \geq \max_{1\leq i\leq s}\{2,\deg F_i\}$ y $\sigma := \sigma(\{F_1,\ldots,F_s\})$.

Sea M el conjunto convexo definido por

$$M := \{x \in \mathbb{R}^n : F_1(x) \leq 0,\ldots,F_s(x) \leq 0\}$$

El propósito de esta sección es estudiar cuáles de las restricciones $F_1,\ldots,F_s$ "sobran", es decir, determinar un convexo M' definido por eventualmente menos restricciones que M de modo que tenga una aspecto más uniforme que M y que cumpla la propiedad:

$$M \cap \mathbb{Z}^n \neq \emptyset \Longleftrightarrow M' \cap \mathbb{Z}^n \neq \emptyset\,.$$

PROPOSICION B.1. Existe $\{i_1,\ldots,i_\ell\} \subseteq \{1,\ldots,s\}$ tal que si
$M' := \{x \in \mathbb{R}^n : F_{i_1}(x) \leq 0,\ldots,F_{i_\ell}(x) \leq 0\}$, entonces se cumple

(i) $M \cap \mathbb{Z}^n \neq \emptyset \Longleftrightarrow M' \cap \mathbb{Z}^n \neq \emptyset$

(ii) A partir de cada punto entero $x' \in M'$, se construye un punto entero $x \in M$ tal que $\sigma(x) \leq d^n\sigma(x') + d^{0(n^2)}\sigma$

(iii) $M' = V + (M' \cap V^\perp)$
donde V es un *subespacio lineal* de $\mathbb{R}^n$, que admite una base entera $\mathcal{B}$ con $\sigma(\mathcal{B}) = d^{0(n^2)}\sigma$, y $M' \cap V^\perp$ es un *subconjunto compacto* de $\mathbb{R}^n$.

La demostración abarca los lemas B.2 hasta B.11.

Notación: Para todo $1 \leq j \leq s$, sea $M_j := \{x \in \mathbb{R}^n : \bigwedge_{\substack{1\leq i\leq s\\ i\neq j}} F_i(x) \leq 0\}$

y si $\{i_1,\ldots,i_\ell\} \subseteq \{1,\ldots,s\}$, $M_{i_1\ldots i_\ell} := \{x \in \mathbb{R}^n : \bigwedge_{\substack{1\leq i\leq s\\ i\neq i_1,\ldots,i_\ell}} F_i(x) \leq 0\}$.

LEMA B.2. Sea $1 \leq j \leq s$ fijado y supongamos que existe una dirección $u \in \mathbb{R}^n - \{0\}$ tal que $F_j(Tu)$ sea estrictamente decreciente como polinomio en T y que para todo $1 \leq i \leq s$, $i \neq j$, $F_i(Tu)$ sea decreciente o constante (en ese caso se dice que u es una *dirección de recesión* de $F_1, \ldots, F_s$, *no constante* para F_j). Entonces vale:

$$M \neq \emptyset \Longleftrightarrow M_j \neq \emptyset$$

y diremos que F_j es una *restricción superflua.*

Demostración:

($\Longrightarrow$) es trivial

($\Longleftarrow$) Supongamos que existe $x' \in M_j : F_i(x') \leq 0 \ \ (\forall i \neq j)$

Dado que $F_j(Tu)$ es estrictamente decreciente, $F_j(x' + Tu)$ es también estrictamente decreciente (Proposición A.1) y por lo tanto $\lim_{t \to +\infty} F_j(x' + tu) = -\infty$, o sea existe $t > 0$ tal que $F_j(x' + tu) \leq 0$.

Definamos $x := x' + tu$. Entonces $F_j(x) \leq 0$; y si $i \neq j$,

$F_i(x) = F_i(x' + tu) \leq F_i(x' + 0u) = F_i(x') \leq 0$

(por hipótesis y nuevamente Proposición A.1).

Por consiguiente $x \in M$.

♦

El problema consiste entonces en hallar direcciones de recesión u, no constantes para alguna restricción. ¿Dónde buscarlas?

DEFINICION B.3.

(i) Sea $F \in \mathbb{R}[X_1, \ldots, X_n]$ cuasiconvexo. Se define

$$K(F) := \{u \in \mathbb{R}^n : \sup\{F(tu), t \geq 0\} < \infty\}$$

el conjunto de las direcciones de semirrectas $[0, +\infty)$ en las cuales F no crece (o sea es decreciente o constante), y

$$L(F) := \{u \in \mathbb{R}^n : \sup\{F(tu), t \in \mathbb{R}\} < \infty\}$$

el conjunto de las direcciones de rectas en las cuales F es constante.

(ii) Sea $F(X) = \sum_{0 \le i \le d} P_i(x)$ con $P_i(tX) = t^i P_i(X)$ $(\forall t \in \mathbb{R})$,

y sea $I := I(F) := \{i \in \{1, \ldots, d\} :$ existe $u \in \mathbb{R}^n$ que verifica
$P_d(u) = \ldots = P_{i+1}(u) = 0$ y $P_i(u) < 0\}$

Se define el *índice* $i_0 := i_0(F)$ en la forma

$$i_0 := i_0(F) := \begin{cases} \max\{i : i \in I\} & \text{si } I \neq \emptyset \\ 1 & \text{si } I = \emptyset \end{cases}$$

y $K^*(F) := \{u \in \mathbb{R}^n : P_i(u) = 0,\ i_0 + 1 \le i \le d\}$.

OBSERVACION B.4.

(i) $K^*(F)$ es un subespacio lineal de $\mathbb{R}^n$ (Proposición A.2).

(ii) i_0 siempre es impar (Lema A.6(ii)).

LEMA B.5.

Sea $F \in \mathbb{R}[X_1, \ldots, X_n]$ un polinomio cuasiconvexo de grado $d \ge 1$. Entonces vale

(i) $K(F) = K^*(F) \cap \{u \in \mathbb{R}^n : P_{i_0}(u) \le 0\}$
$= \{u \in \mathbb{R}^n : P_d(u) = 0, \ldots, P_{i_0+1}(u) = 0,\ P_{i_0}(u) \le 0\}$

(ii) $L(F) = K^*(F) \cap \{u \in \mathbb{R}^n : P_{i_0}(u) = 0\}$
$= \{u \in \mathbb{R}^n : P_d(u) = 0, \ldots, P_{i_0}(u) = 0\}$

Demostración:

(i)$\subseteq$: Sea $u \in K(F)$, i.e. $F(tu)$ es constante o estrictamente decreciente para $t \ge 0$.
Pongamos
$F(Tu) := P_r(u)T^r + \ldots + P_0$ (donde $r = gr\,(F(Tu))$
Si $r \ge 1$, se tiene $P_d(u) = \ldots = P_{r+1}(u) = 0$, $P_r(u) < 0$ y por lo tanto $i_0 \ge r$. En el caso en que $i_0 > r$, vale $P_{i_0}(u) = 0$ y en el caso en que $i_0 = r$, vale $P_{i_0}(u) < 0$.
Si $r = 0$, por definición se tiene $i_0 \ge r$ (pues $i_0 \in \{1, \ldots, d\}$) y por lo tanto vale $P_{i_0}(u) = 0$.

Por consiguiente en todos los casos se tiene $u \in K^*(F) \cap \{u \in \mathbb{R}^n : P_{i_0}(u) \le 0\}$.

$\supseteq$: Sea $u \in K^*(F) \cap \{u \in \mathbb{R}^n : P_{i_0}(u) \le 0\}$.
Si es $P_{i_0}(u) < 0$, entonces $F(Tu)$ es estrictamente decreciente (Observación A.4) y por lo tanto $u \in K(F)$.
Falta considerar el caso en que $P_{i_0}(u) = 0$, o sea falta averiguar si vale que $F(Tu)$ es

decreciente o constante en ese caso. Claramente se puede suponer $i_0 > 1$, pues en el caso $i_0 = 1$, $F(Tu)$ resulta constante y $u \in K(F)$.

Supongamos entonces que $F(Tu)$ no es decreciente ni constante para $t \geq 0$, entonces por A.4, $\lim_{t \to +\infty} F(tu) = +\infty$, o sea existe $t_0 > 0$ tal que $F(t_0 u) > F(0)$. Además sea $u_0 \in \mathbb{R}^n$ tal que $P_d(u_0) = 0, \ldots, P_{i_0+1}(u_0) = 0$, $P_{i_0}(u_0) < 0$ (existe por la definición de i_0).

Para todo $\alpha \in [0,1]$, sea $u_\alpha := (1-\alpha)u_0 + \alpha(t_0 u)$.

Al ser $K^*(F)$ un subespacio lineal de $\mathbb{R}^n$ y $K^*(F) \cap \{u \in \mathbb{R}^n : P_{i_0}(u) < 0\}$ un semiespacio de $K^*(F)$ (Observación B.4 y Lema A.6(ii)), se deduce que $\forall \alpha \in [0,1)$, $u_\alpha \in K^*(F) \cap \{u \in \mathbb{R}^n : P_{i_0}(u) < 0\}$ pues $u_0 \in K^*(F)$, $t_0 u \in K^*(F)$, $P_{i_0}(u_0) < 0$ y $P_{i_0}(t_0 u) = 0$.

Esto significa que fijado $\alpha \in [0,1)$, el polinomio cuasiconvexo $F(Tu_\alpha)$ es estrictamente decreciente. Luego $F(u_\alpha) = F(1 . u_\alpha) < F(0 . u_\alpha) = F(0)$, y por continuidad, tomando $\alpha \to 1$ resulta que $F(t_0 u) \leq F(0)$, lo que contradice la elección de t_0. Por lo tanto $F(Tu)$ es decreciente o constante y $u \in K(F)$.

(ii) $u \in L(F) \iff \sup_{t \in \mathbb{R}} F(tu) < \infty$

$\iff \sup_{t \geq 0} F(tu) < \infty$ y $\sup_{t \leq 0} F(tu) < \infty$

$\iff u \in K(F)$ y $-u \in K(F)$

$\iff P_d(u) = 0, \ldots, P_{i_0+1}(u) = 0$, $P_{i_0}(u) \leq 0$ y $-P_{i_0}(u) \leq 0$ (i_0 impar)

$\iff u \in K^*(F) \cap \{u \in \mathbb{R}^n : P_{i_0}(u) = 0\}$.

♦

COMENTARIO B.6. El lema anterior muestra que $L(F)$ es un subespacio lineal de $\mathbb{R}^n$. Es claro que $L(F)$ es el subespacio lineal de $\mathbb{R}^n$ más grande contenido en $K(F)$, y que $K^*(F)$ es el subespacio lineal de $\mathbb{R}^n$ más pequeño que contiene a $K(F)$.

OBSERVACION B.7. Retomando el Lema B.2, una dirección $u \in \mathbb{R}^n - \{0\}$ es de recesión de $F_1, \ldots, F_s$, no constante para F_j si y sólo si $u \in K(F_1) \cap \ldots \cap K(F_s)$ y $u \notin L(F_j)$ (o sea si u pertenece al cono poliedral $K(F_1) \cap \ldots \cap K(F_s)$ pero no al espacio lineal $L(F_j)$ ($\subseteq K(F_j)$).

Este hecho permite mostrar lo siguiente:

LEMA B.8. Dado j $(1 \leq j \leq s)$ en las condiciones del Lema B.2 (i.e. existe $u \in \mathbb{R}^n - \{0\}$ dirección de recesión de $F_1, \ldots, F_s$, no constante para F_j), entonces vale:

$$M \cap \mathbb{Z}^n \neq \emptyset \Longleftrightarrow M_j \cap \mathbb{Z}^n \neq \emptyset$$

Más aún, dado $x' \in M_j \cap \mathbb{Z}^n$, se recupera $x \in M \cap \mathbb{Z}^n$ con $\sigma(x) = d(\sigma(x') + d^{O(n^2)}\sigma)$.

Demostración: Existe $u \in \bigcap_{1 \leq i \leq s} K(F_i) - L(F_j)$ si y sólo si $\bigcap_{1 \leq i \leq s} K(F_i) \not\subseteq L(F_j)$, es decir si el cono poliedral $\bigcap_{1 \leq i \leq s} K(F_i)$ no está contenido en el espacio lineal $L(F_j)$. Esto ocurre si y sólo si alguno de los generadores del cono poliedral $\bigcap_{1 \leq i \leq s} K(F_i)$ no pertenece a $L(F_j)$. La Proposición A.3 permite entonces asegurar que (en ese caso) se puede elegir la dirección u *entera* tal que $\sigma(u) = d^{O(n^2)}\sigma$. Repitiendo ahora el procedimiento de la demostración del Lema B.2, se tiene que $F_j(x' + Tu)$ es estrictamente decreciente, y por lo tanto se puede elegir $t \in \mathbf{N}$ de tal modo que $F_j(x' + tu) \leq 0$.

Estimaremos la longitud binaria de un tal t:

Sea $F_j(x' + Tu) = a_r T^r + \ldots + a_0 \quad (a_r \neq 0)$. Se tiene que $r \geq 1$ y $a_r < 0$. Elijamos $t = |a_{r-1}| + \ldots + |a_0|$, entonces se verifica que $F_j(x' + tu) \leq 0$, ya que:

- Si para todo $0 \leq i \leq r-1$, $|a_i| = 0$, es $F_j(t) \leq F_j(0) = 0$
- Si existe i, $0 \leq i \leq r-1$, tal que $|a_i| \neq 0$, entonces se tiene $t \geq 1$ y $F_j(x' + tu) = a_r t^r \left(1 + \frac{a_{r-1}}{a_r} t^{-1} + \ldots + \frac{a_0}{a_r} t^{-r}\right)$.
  Dado que $\left|\frac{a_{r-1}}{a_r} t^{-1} + \ldots + \frac{a_0}{a_r} t^{-r}\right| \leq (|a_{r-1}| + \ldots + |a_0|)\,|t|^{-1} \leq 1$ se obtiene que $F_j(x' + tu)$ tiene el signo de a_r, y por lo tanto $F_j(x' + tu) \leq 0$. Claramente para todo $i \neq j$, $F_i(x' + tu) \leq 0$, por la elección de u.

Observemos que si $x' \in M_j \cap \mathbb{Z}^n$ y $u \in Z^n$, el polinomio $F_j(x' + Tu)$ tiene coeficientes *enteros* $\{a_r, \ldots, a_0\}$ que verifican

$$\sigma(\{a_r, \ldots, a_0\}) = O(d \max\{\sigma(x'), \sigma(u)\})$$

y por lo tanto, definiendo $x := x' + tu$, resulta que $x \in M \cap \mathbb{Z}^n$ y

$$\sigma(x) = \sigma(x' + tu) = d(\sigma(x') + d^{O(n^2)}\sigma).$$

♦

Este lema da una idea intuitiva de una construcción posible para la exhibición de un conjunto $\{i_1, \ldots, i_t\}$ de índices en las condiciones del Lema B.1 (o sea de índices que corresponden a restricciones superfluas).

CONSTRUCCION B.9.(Eliminación de restricciones superfluas).

- Sea i_1 $(1 \leq i_1 \leq s)$ tal que existe $u^{(i_1)} \in \mathbb{R}^n - \{0\}$ que verifica

$$u^{(i_1)} \in \bigcap_{1 \leq i \leq s} K(F_i) \qquad \text{y} \qquad u^{(i_1)} \notin L(F_{i_1})$$

  Entonces $M \cap \mathbb{Z}^n \neq \emptyset \Longleftrightarrow M_{i_1} \cap \mathbb{Z}^n \neq \emptyset$.

- Sea i_2 $(1 \leq i_2 \leq s,\ i_2 \neq i_1)$ tal que existe $u^{(i_2)} \in \mathbb{R}^n - \{0\}$ que verifica

$$u^{(i_2)} \in \bigcap_{\substack{1 \leq i \leq s \\ i \neq i_1}} K(F_i) \qquad \text{y} \qquad u^{(i_2)} \notin L(F_{i_2})$$

  Entonces $M_{i_1} \cap \mathbb{Z}^n \neq \emptyset \Longleftrightarrow M_{i_1,i_2} \cap \mathbb{Z}^n \neq \emptyset$.

y recursivamente

- Sea i_k $(1 \leq i_k \leq s,\ i_k \neq i_1, \ldots, i_{k-1})$ tal que existe $u^{(i_k)} \in \mathbb{R}^n - \{0\}$ que verifica

$$u^{(i_k)} \in \bigcap_{\substack{1 \leq i \leq s \\ i \neq i_1, \ldots, i_{k-1}}} K(F_i) \qquad \text{y} \qquad u^{(i_k)} \notin L(F_{i_k})$$

  Entonces $M_{i_1,\ldots,i_{k-1}} \cap \mathbb{Z}^n \neq \emptyset \Longleftrightarrow M_{i_1,\ldots,i_k} \cap \mathbb{Z}^n \neq \emptyset$.
  En definitiva $M \cap \mathbb{Z}^n \neq \emptyset \Longleftrightarrow M_{i_1,\ldots,i_k} \cap \mathbb{Z}^n \neq \emptyset$.

Se plantean, por lo tanto, los dos problemas siguientes:

(i) ¿Qué pasa cuando no existe más índice j cumpliendo con las condiciones? Es decir cuando $\{i_1, \ldots, i_t\}$ es una subsucesión maximal (ordenada) de $\{1, \ldots, s\}$ definida como arriba.

(ii) Si $M' := M_{i_1 \ldots i_t}$, ¿cómo se recupera a partir de $x' \in M' \cap \mathbb{Z}^n$ un punto entero $x \in M \cap \mathbb{Z}^n$, de longitud binaria "corta"?

Se tratará en primer lugar el problema (ii), que resuelve la parte (ii) de la Proposición B.1.

LEMA B.10. Sea $\{i_1,\dots,i_t\}$ una subsucesión maximal de $\{1,\dots,s\}$ construida como en B.9 (eventualmente $t=0$ ó s).
Sea $M' := M_{i_1\dots i_t} = \{x\in\mathbb{R}^n : \bigwedge_{\substack{1\le i\le s\\ i\neq i_1,\dots,i_t}} F_i(x)\le 0\}$ y sea $x'\in M'\cap\mathbb{Z}^n$.
Entonces existe $x\in M\cap\mathbb{Z}^n$ que verifica $\sigma(x)=d^n\sigma(x')+d^{O(n^2)}\sigma$.
(En el caso $t=s$, se puede tomar $x'=0$).

Demostración: Si se aplicara directamente el resultado del Lema B.8, se obtendría la siguiente cota

$$\sigma(x)\le d^s(\sigma(x')+sd^{O(n^2)}\sigma)$$

ya que la única cota a priori sobre el número de restricciones F_i $(1\le i\le s)$ que se suprimen es el número s de restricciones. Esta *no es la cota deseada* ya que s aparece en el exponente.
El razonamiento siguiente permite acotar la cantidad de iteraciones por la dimensión n del espacio ambiente. Para ello dado un cono poliedral $K\subseteq\mathbb{R}^n$, recordemos que

$$\dim_{\mathbb{R}} K := \min\{\dim_{\mathbb{R}} L : L \text{ subespacio lineal de } \mathbb{R}^n \text{ y } K\subseteq L\}$$

Supongamos que $\{i_1,\dots,i_t\}=\{s,\dots,r+1\}$. Es decir que se extrajeron *en ese orden* las restricciones F_i correspondientes a los subíndices $s, s-1,\dots,r+1$.
Por simplicidad, definamos

$$\begin{aligned} K_r &:= \bigcap_{1\le i\le r} K(F_i)\\ K_{r+1} &:= \bigcap_{1\le i\le r+1} K(F_i)\\ &\vdots\\ K_s &:= \bigcap_{1\le i\le s} K(F_i)\end{aligned}$$

Se tiene la relación $K_s\subseteq K_{s-1}\subseteq\dots\subseteq K_{r+1}\subseteq K_r$.
Examinemos los saltos de dimensión que ocurren en esa sucesión (hay a lo sumo n ya que $K_r\subseteq\mathbb{R}^n$). Por ejemplo se tiene:

$$\begin{aligned}\dim_{\mathbb{R}} K_{r+1}=\dots=\dim_{\mathbb{R}} K_{r+\ell} > \dim_{\mathbb{R}} K_{r+\ell+1}=\dots=\\ =\dim_{\mathbb{R}} K_{r+\ell+\ell'} > \dim_{\mathbb{R}} K_{r+\ell+\ell'+1}=\dots\end{aligned}$$

Consideremos $K_{r+1},\dots,K_{r+\ell}$ (ℓ conos incluídos uno en otro tales que no se produce salto de dimensión). Para todo $1 \le i \le \ell$, se tiene:

$$\dim_{\mathbf{R}}(K_{r+1} \cap L(F_{r+i})) < \dim_{\mathbf{R}}(K_{r+1})$$

pues si fuera $\dim_{\mathbf{R}}(K_{r+1} \cap L(F_{r+i})) = \dim_{\mathbf{R}}(K_{r+1})$ sería $K_{r+1} \subseteq L(F_{r+i})$ (ya que si L es un subespacio lineal de $\mathbf{R}^n$, mínimo tal que $K_{r+1} \subseteq L$, entonces $K_{r+1} \cap L(F_{r+i}) \subseteq L$, y por tener la misma dimensión tiene que ser $L \cap L(F_{r+i}) = L$, es decir, $L \subseteq L(F_{r+i})$, o sea $K_{r+1} \subseteq L(F_{r+i})$). En ese caso no existiría $u \in K_{r+1}$ tal que $u \notin L(F_{r+i})$, y por lo tanto no existiría tampoco $u \in K_{r+i}$ tal que $u \notin L(F_{r+i})$ (pues $K_{r+i} \subseteq K_{r+1}$), y no se podría haber suprimido el índice $r+i$ del conjunto $\{1,\dots,r,\dots,r+i\}$. Por lo tanto se tiene

$$(*) \qquad \dim_{\mathbf{R}}(K_{r+1} \cap L(F_{r+i})) < \dim_{\mathbf{R}}(K_{r+1}) = \dots = \dim_{\mathbf{R}}(K_{r+\ell}) \quad (1 \le i \le \ell)$$

Se construye entonces $u \in K_{r+\ell}$ tal que $u \notin \bigcup_{1 \le i \le \ell} (K_{r+1} \cap L(F_{r+i}))$ (o sea, dado que $K_{r+\ell} \subseteq K_{r+1}$, se construye $u \in K_{r+\ell}$ tal que $u \notin L(F_{r+i})$ $(1 \le i \le \ell)$), de la manera siguiente:

Se considera un sistema de generadores $\mathcal{G}$ del cono $K_{r+\ell} = \bigcap_{1 \le i \le r+\ell} K(F_i)$, con $\sigma(\mathcal{G}) = d^{\mathcal{O}(n^2)}\sigma$ (dado por la Proposición A.3) y sea $\{v_1,\dots,v_e\} \subseteq \mathcal{G}$ un sistema linealmente independiente maximal de $\mathcal{G}$ (se tiene $e \le n$). Pongamos $u := v_1 + \dots + v_e \in K_{r+\ell}$ (por ser un cono). Por $(*)$, para todo $1 \le i \le \ell$, existe $k(i)$ tal que $v_{k(i)} \notin K_{r+\ell} \cap L(F_{r+i})$, por lo tanto dado $1 \le i \le \ell$, $F_{r+i}(Tv_{k(i)})$ es estrictamente decreciente. Luego

$$(**) \qquad F_{r+i}(v_{k(i)}) < F_{r+i}(0)$$

Por otro lado si $v^{(k(i))} := \sum_{\substack{i \le j \le e \\ j \ne k(i)}} v_j$, se tiene $v^{(k(i))} \in K_{r+\ell}$ y por consiguiente $F_{r+i}(Tv^{(k(i))})$ es constante o decreciente, con lo cual $F_{r+i}(v_{k(i)} + Tv^{(k(i))})$ es constante o decreciente.

Se obtiene luego, por $(**)$

$$F_{r+i}(u) = F_{r+i}(v_1 + \dots + v_e) \le F_{r+i}(v_{k(i)}) < F_{r+i}(0)$$

o sea $F_{r+i}(u)$ no es constante, i.e. $u \notin L(F_{r+i})$. Claramente $\sigma(u) = d^{\mathcal{O}(n^2)}\sigma$.

Este razonamiento permite elegir una dirección de recesión u (entera) para muchas restricciones a la vez, y gracias al procedimiento del Lema B.8, a partir de $x' \in M_{r+1\dots s}$ se recupera $x \in M_{r+\ell+1\dots s}$ con $\sigma(x) = d(\sigma(x') + d^{\mathcal{O}(n^2)}\sigma)$.

Dado que esta construcción se repite a lo sumo n veces, a partir de $x' \in M' \cap \mathbb{Z}^n = M_{r+1\ldots s} \cap \mathbb{Z}^n$, se recupera $x \in M \cap \mathbb{Z}^n$ con $\sigma(x) = d^n(\sigma(x') + d^{0(n^2)}\sigma)$.

♦

Para concluir la demostración de la Proposición B.1, hay que responder al problema (i) planteado arriba.

LEMA B.11. Sea $\{i_1,\ldots,i_t\} \subseteq \{1,\ldots,s\}$ tal que para todo $j \neq i_1,\ldots,i_t$, *no existe* $u^{(j)} \in \mathbb{R}^n - \{0\}$ que verifique

$$u^{(j)} \in \bigcap_{\substack{1\le i\le s\\ i\neq i_1,\ldots,i_t}} K(F_i) \qquad \text{y} \qquad u^{(j)} \notin L(F_j)$$

Entonces si $M' := M_{i_1\ldots i_t} = \{x \in \mathbb{R}^n : \bigwedge_{\substack{1\le i\le s\\ i\neq i_1,\ldots,i_t}} F_i(x) \le 0\}$, se tiene que $M' = V + (M' \cap V^{\perp})$, donde V es un subespacio *lineal* de $\mathbb{R}^n$ y $M' \cap V^{\perp}$ es un subconjunto convexo *compacto* de $\mathbb{R}^n$. Además existe una base entera $\mathcal{B}$ de V tal que $\sigma(\mathcal{B}) = d^{0(n^2)}\sigma$.

Demostración: Sin pérdida de generalidad se puede suponer $t = 0$, o sea $\{i_1,\ldots,i_t\} = \emptyset$ y en ese caso $M = M'$. La condición $\forall j$, $\nexists u^{(j)} \in \mathbb{R}^n - \{0\}$ con $u^{(j)} \in \bigcap_{1\le i\le s} K(F_i) - L(F_j)$, significa que $\bigcap_{1\le i\le s} K(F_i) = \bigcap_{1\le i\le s} L(F_i)$
(ya que por definición $\bigcap_{1\le i\le s} L(F_i) \subseteq \bigcap_{1\le i\le s} K(F_i)$),
es decir el conjunto de direcciones de recesión

$$\bigcap_{1\le i\le s} K(F_i) = \{u \in \mathbb{R}^n : F_i(Tu) \quad \text{es decreciente o constante} \quad (1 \le i \le s)\}$$

coincide con el conjunto de direcciones constantes

$$\bigcap_{1\le i\le s} L(F_i) := \{u \in \mathbb{R}^n : F_i(Tu) \quad \text{es constante} \quad (1 \le i \le s)\}$$

Pongamos $V := \bigcap_{1\le i\le s} L(F_i) = \bigcap_{1\le i\le s} K(F_i)$.

Por B.5 y A.3, se sabe que V es un subespacio lineal de $\mathbb{R}^n$, que admite una base $\mathcal{B}$ con $\sigma(\mathcal{B}) = d^{0(n^2)}\sigma$.

Sea ahora $x \in M$. Existe una representación de x en la forma $x = y + u$, con $y \in V^\perp$, $u \in V$. Entonces $y = x - u \in M$ ya que la linealidad de V implica que $-u \in V$ y por A.1 y la definición de V, $F_i(x+(-u)) \le F_i(x) \le 0$ $(1 \le i \le s)$. Por lo tanto $x \in (M \cap V^\perp) + V$. La inclusión recíproca se muestra análogamente.

Falta mostrar que $M \cap V^\perp$ es compacto:

Si el conjunto convexo cerrado $M \cap V^\perp$ no lo fuera, contendría una semirrecta $\{x + tu, t \ge 0\}$, con $x \in M \cap V^\perp$, y $u \in \mathbb{R}^n - \{0\}$ (ver por ejemplo [Ro]). Esto implicaría que u es una dirección de recesión de $F_1, \ldots, F_s$ y por lo tanto $u \in V$. Por otro lado se muestra que $u \in V^\perp$. Contradicción.

♦

1.- C. Una cota semialgebraica

En virtud de la Proposición B.1, para concluir la demostración del Teorema 1, alcanza con probar que $M' \cap \mathbb{Z}^n$ es no vacío si y sólo si contiene un punto entero de longitud binaria acotada por $(sd)^{0(n^2)}\sigma$.

Dado que M' se descompone como un conjunto compacto y un subespacio lineal de $\mathbb{R}^n$, nos reduciremos a la consideración de un conjunto acotado, de radio dependiente del compacto y aplicaremos luego los resultados de geometría semialgebraica expuestos en el Capítulo I para acotar el radio de ese compacto.

Sin pérdida de generalidad, podemos suponer en esta sección que $M := \{x \in \mathbb{R}^n : F_1(x) \le 0, \ldots, F_s(x) \le 0\}$ ya no contiene ninguna restricción superflua (en el sentido dado en la Sección B) lo que implica que $M = (M \cap V^\perp) + V$, con $M \cap V^\perp$ compacto y V lineal, (con base $\mathcal{B}$ entera que verifica $\sigma(\mathcal{B}) = d^{0(n^2)}\sigma$).

OBSERVACION C.1. Si $M \cap \mathbb{Z}^n$ es no vacío, entonces M contiene un punto entero en $M \cap V^\perp + B$, donde $B = \{\sum_{1\le i\le m} \beta_i v_i,\ 0 \le \beta_i < 1\}$ si $\{v_1, \ldots, v_m\}$ es una base entera de V.

Demostración: Sea $x \in M \cap \mathbb{Z}^n$.
Se tiene la descomposición $x = y + u$, $y \in M \cap V^\perp$, $u \in V$. Sea $\{v_1, \ldots, v_m\}$ una base entera de V, y sea $u = \tau_1 v_1 + \ldots + \tau_m v_m$ $(\tau_1, \ldots, \tau_m \in \mathbb{R})$ la representacin de u en la base $\mathcal{B}$. Para todo $1 \leq j \leq m$, escribamos

$$\tau_j = \tilde{\tau}_j + \lfloor \tau_j \rfloor, \quad \text{donde} \quad \lfloor \tau_j \rfloor \in \mathbb{Z} \quad \text{y} \quad 0 \leq \tilde{\tau}_j < 1$$

y sea $\tilde{x} := y + \tilde{\tau}_1 v_1 + \ldots + \tilde{\tau}_m v_m$. Se tiene entonces que $\tilde{x} = x - (\lfloor \tau_1 \rfloor v_1 + \ldots + \lfloor \tau_m \rfloor v_m) \in \mathbb{Z}^n$. Además $\tilde{x} \in M + V \subseteq M$. Por lo tanto $\tilde{x} \in M \cap \mathbb{Z}^n$ y $\tilde{x} \in M \cap V^\perp + \mathcal{B}$.

Esto significa que si $M \cap \mathbb{Z}^n$ es no vacío, entonces contiene un punto "cerca" del conjunto acotado $M \cap V^\perp$. Dado que se puede elegir la base entera $\mathcal{B}$ de V con $\sigma(\mathcal{B}) = d^{O(n^2)}\sigma$ (Proposición B.1), para terminar la demostración del teorema, alcanza con mostrar la existencia de un radio $R \in \mathbf{N}$, con $\sigma(R) = (sd)^{O(n^2)}\sigma$ tal que $M \cap V^\perp \subseteq B(0, R)$.

LEMA C.2. En las mismas condiciones se tiene la estimación siguiente:
$M \cap V^\perp \subseteq B(0, R)$, donde $R \in \mathbf{N}$ es tal que $\sigma(R) = (sd)^{O(n)}\sigma$.

Demostración: El conjunto semialgebraico $M \cap V^\perp$ se puede definir por una formula sin cuantificadores del lenguaje de primer orden de $\mathbb{R}$ a constantes en $\mathbb{Z}$, en la cual intervienen sólo los polinomios $F_1, \ldots, F_s$ y las ecuaciones del subespacio lineal $V^\perp$. A partir de ella se puede describir el conjunto semialgebraico $S := \{\rho \in \mathbb{R} : M \cap V^\perp \subseteq B(0, \rho)\}$ por la fórmula Φ (con un solo bloque de cuantificadores) siguiente:

$$\Phi: \qquad (\forall X) \quad (X \in M \cap V^\perp \Longrightarrow \|X\|^2 \leq \rho^2)$$

donde $X = (X_1, \ldots, X_n)$ son las variables ligadas y ρ es la variable libre.
Si aplicamos a Φ la Observación 6 del Capítulo I (en el caso particular en que se tiene una sola variable libre y un bloque de cuantificadores), se obtiene una fórmula Ψ sin cuantificadores, en la variable ρ, que describe al conjunto S. Ψ será un disyunción de conjunciones de condiciones de signo sobre polinomios $G_1, \ldots, G_\ell \in \mathbb{Z}[\rho]$. Dado que la fórmula de entrada Φ involucra sólo parámetros de longitud binaria acotada por $d^{O(n^2)}\sigma$, el algoritmo garantiza que los polinomios $G_1, \ldots, G_\ell$ de Ψ son tales que

$$(*) \qquad \max\{gr\, G_k,\ 1 \leq k \leq \ell\} = (sd)^{O(n)} \quad y \quad \sigma(\{G_1, \ldots, G_\ell\}) = (sd)^{O(n^2)}\sigma$$

Ahora, si $\alpha := \max\{\beta \in \mathbb{R}^n ; \exists k \ \ (1 \leq k \leq \ell) \text{ con } G_k(\beta) = 0\}$ es la máxima de las raíces reales de alguno de los polinomios $G_1, \ldots, G_\ell$, se tiene que la fórmula Ψ es siempre verdadera o siempre falsa en el intervalo $(\alpha, +\infty)$ (ya que a la derecha de α ya no se producen cambios de signo en Ψ). Por cuanto el conjunto semialgebraico cerrado S tiene la forma $[\gamma, +\infty]$ (con $\gamma \geq 0$), Ψ resulta siempre verdadera en el intervalo $(\alpha, +\infty)$ y por lo tanto la mayor raíz real (en módulo) de los polinomios $G_1, \ldots, G_\ell$ es un radio R que cumple la condición exigida.

Por $(*)$, una estimación directa del tamaño de las raíces reales de los polinomios $G_1, \ldots, G_\ell$ arroja una cota superior $R \in \mathbf{N}$ con $\sigma(R) = (sd)^{0(n^2)}\sigma$ (para ello se usa por ejemplo la desigualdad de Cauchy dada en [Mi]).

♦

Demostración del Teorema 1 (Redondeo).

Sean $F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$ cuasiconvexos con $\sigma := \sigma(\{F_1, \ldots, F_s\})$ y $d := \max\{2, gr\, F_i,\ 1 \leq i \leq s\}$. Sea $M := \{x \in \mathbb{R}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$.

Por la Proposición B.1, se tiene que existe

$$M' := \{x \in \mathbb{R}^n : F_{i_1}(x) \leq 0, \ldots, F_{i_t}(x) \leq 0\} \supseteq M$$

que verifica $M \cap \mathbb{Z}^n \neq \emptyset \iff M' \cap \mathbb{Z}^n \neq \emptyset$

y si $x' \in M' \cap \mathbb{Z}^n$, entonces existe $x \in M \cap \mathbb{Z}^n$ con $\sigma(x) = d^n \sigma(x') + d^{0(n^2)}\sigma$.

Por otro lado $M' \cap \mathbb{Z}^n \neq \emptyset$ si y sólo si contiene un punto entero x' que verifica $\sigma(x') = (sd)^{0(n^2)}\sigma$ (Lema C.2 y Observación C.1).

Por lo tanto, $\sigma(x) = (sd)^{0(n^2)}\sigma$ y se concluye que $M \cap \mathbb{Z}^n$ es no vacío si y sólo si contiene un punto entero de longitud binaria acotada por $(sd)^{0(n^2)}\sigma$.

♦

1.1.- DEMOSTRACION DEL COROLARIO 1.1

Vamos a precisar un poco el sentido de "clase de complejidad NEXPTIME" ("non deterministically simply exponential time").

Un problema de decisión $\mathcal{P}$ pertenece a la clase NEXPTIME si existe un problema de decisión $\mathcal{P}'$, resoluble en tiempo exponencial con una máquina de Turing determinística, y un polinomio ϕ tal que para todo input z se tiene

$$(*) \qquad z \in \mathcal{P} \iff \exists z' : (z, z') \in \mathcal{P}' \quad \text{y} \quad \sigma(z') \leq 2^{\phi(\sigma(z))} .$$

Como interpretación, z' juega aquí el rol de "prueba de longitud exponencial" del hecho de que z esté en $\mathcal{P}$. La "prueba" puede ser verificada en tiempo exponencial (ya que $\mathcal{P}'$ es resoluble en tiempo exponencial). El hecho crucial es que no se requiere que z' en $(*)$ se halle en tiempo exponencial: z' puede ser pensado como un certificado para z, entregado al jefe para convencerlo de que z está en $\mathcal{P}$. Para testear si $z \in \mathcal{P}$, podemos adivinar (con un oráculo) un candidato z' tal que $(z, z') \in \mathcal{P}'$. De ahí proviene el nombre de "no determinístico".

En nuestro contexto, dada una familia $F_1, \ldots, F_s$ de polinomios cuasiconvexos a coeficientes enteros, queremos decidir si existe $x \in \mathbb{Z}^n$ tal que $F_1(x) \leq 0, \ldots, F_s(x) \leq 0$. Se probó que esto ocurre si y sólo si existe $y \in B(0,R) \cap \mathbb{Z}^n$ tal que $F_1(y) \leq 0, \ldots, F_s(y) \leq 0$. Dado que $\sigma(R) = (sd)^{0(n^2)}$, verificar si un certificado y cumple las condiciones tiene complejidad $(sd)^{0(n^2)}\sigma$ (pues consiste en evaluar s polinomios de grado d y longitud binaria σ en un punto entero de longitud binaria $(sd)^{0(n^2)}\sigma$), y por lo tanto requiere tiempo exponencial en n (ver [Gat]).

(Desde el punto de vista determinístico, el problema tiene a priori complejidad doblemente exponencial ya que hay $2^{(sd)^{0(n^2)}\sigma}$ puntos enteros en $B(0,R)$, que podrían cumplir las condiciones).

♦

2.- *DEMOSTRACION DEL TEOREMA 2*

Para probar este teorema de minimisación, se aplicará no sólo el resultado del Teorema 1 sino también los métodos desarrollados para su demostración (Construcción 1.-B.9 y Lema 1.-B.11). Se siguen aquí las notaciones de la demostración del Teorema 1.

Sea $M := \{x \in \mathbb{R}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$

A. Supondremos en primer lugar que $M \cap \mathbb{Z}^n \neq \emptyset$ y que $\inf\{F_0(x),\ x \in M\} > -\infty$ (o sea una condición aparentemente más fuerte que la hipótesis del teorema).

Entonces se tiene

(i) Existe $x_0 \in M \cap \mathbb{Z}^n \cap B(0,R)$, donde $\sigma(R) = (sd)^{0(n^2)}\sigma$ (por el Teorema 1)
Sea $\lambda := F_0(x_0)$. Se verifica $\sigma(\lambda) = (sd)^{0(n^2)}\sigma$.

(ii) Existe $\nu \in \mathbb{R}$ tal que para todo $x \in M$, $\quad F_0(x) \geq \nu$

(i) implica que si $\mu := \inf\{F_0(x), x \in M \cap \mathbb{Z}^n\}$ (claramente $\mu > -\infty$), entonces $\mu \leq \lambda$, y por lo tanto, si $N := \{x \in \mathbb{R}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0,\ F_0(x) \leq \lambda\}$, se tiene $N \cap \mathbb{Z}^n \neq \emptyset$ y $\mu = \inf\{F_0(x), x \in N \cap \mathbb{Z}^n\}$.

Repitamos entonces para la sucesión $F_1, \ldots, F_s, F_0 - \lambda$ la Construcción B.9 de la Demostración del Teorema 1 , para eliminar las restricciones superfluas (esto se puede hacer ya que $F_0 - \lambda$ es cuasiconvexo también). Se tiene entonces:

LEMA 1. Si N' es el conjunto que se obtiene eliminando de N una sucesión maximal de restricciones superfluas, se verifica:

$$\inf\{F_0(x),\ x \in N \cap \mathbb{Z}^n\} = \inf\{F_0(x),\ x \in N' \cap \mathbb{Z}^n\}$$

Demostración: La observación crucial para la desigualdad no trivial consiste en verificar que al construir N', nunca se suprime la restricción $F_0 - \lambda$. En efecto, por (ii), se tiene que para todo $x \in M$, $F_0(x) \geq \nu$ y las restricciones F_j que se suprimieron son tales que existe $u \in \mathbb{R}^n - \{0\}$ con $F_j(Tu)$ estrictamente decreciente (y Tu constante o decreciente para las restricciones no suprimidas aún).

Supóngase que se eliminaron (en ese orden) $F_1, \ldots, F_r, F_0 - \lambda$ (eventualmente $r = 0$).

Se afirma que $\inf\{F_0(x'),\ x' \in M_{1\ldots r}\} \geq \nu$:

Sea sino $x' \in M_{1\ldots r}$ con $F_0(x') < \nu$ y sean

$$u_1 \in \bigcap_{i \neq 1} K(F_i) \cap K(F_0 - \lambda) - L(F_1)$$

$$\vdots$$

$$u_r \in \bigcap_{i \neq 1, \ldots, r} K(F_i) \cap K(F_0 - \lambda) - L(F_r)$$

Se verifica entonces que para valores adecuados de $t_1, \ldots, t_r$, $x := x' + t_r u_r + \ldots + t_1 u_1 \in M$ y que $F_0(x) \leq F_0(x') < \nu$. Contradicción.

Por lo tanto es como si se suprimiera la restricción $F_0 - \lambda$ en primer término, pero en ese caso, para todo $x \in M$, sería $x + tu \in M$ $(\forall t \geq 0)$ y $F_0(x + Tu)$ estrictamente decreciente. Absurdo.

La prueba de la igualdad es ahora similar a la de más arriba, observando simplemente que se pueden elegir $u_1, \ldots, u_r$ en $\mathbb{Z}^n$ y $t_1, \ldots, t_n$ en $\mathbf{N}$.

♦

Para finalizar la demostración de este primer caso, alcanza con probar el resultado siguiente:

LEMA 2. Sea N' como en el lema anterior, y por lo tanto $N' = (N' \cap W^{\perp}) + W$, donde $N' \cap W^{\perp}$ es compacto y W es lineal (Lema 1.-B.11) y sea $\{v_1, \ldots, v_m\}$ una base entera de W,
entonces se tiene,

$$\inf\{F_0(x),\, x \in N' \cap \mathbb{Z}^n\} = \inf\{F_0(x),\, x \in (N' \cap W^{\perp} + B) \cap N' \cap \mathbb{Z}^n\}$$

donde $B := \{ \sum_{1 \le i \le m} \beta_i v_i,\ 0 \le \beta_i < 1\}$

Demostración:
Sea $\mu := \inf\{F_0(x),\, x \in N' \cap \mathbb{Z}^n\}$ y sea $x_0 \in N' \cap \mathbb{Z}^n$ tal que $F_0(x_0) = \mu$.
Sea $x_0 = y + \alpha_1 v_1 + \ldots + \alpha_m v_m$ con $y \in N' \cap W^{\perp}$ y $\alpha_1 v_1 + \ldots + \alpha_m v_m \in W$.
Para $1 \le i \le m$, pongamos $\alpha_i = \lfloor \alpha_i \rfloor + \tilde{\alpha}_i$ con $\lfloor \alpha_i \rfloor \in \mathbb{Z}$ y $\tilde{\alpha}_i \in [0,1)$, entonces se tiene que $y + \tilde{\alpha}_1 v_1 + \ldots + \tilde{\alpha}_m v_m \in (N' \cap W^{\perp} + B) \cap N' \cap \mathbb{Z}^n$ (Observación 1.-C.1).
Además, para todo $v \in W$, $F_0(Tv)$ es constante (ya que existe $I \subseteq \{1, \ldots, s\}$ tal que $W = \bigcap_{i \in I} K(F_i) \cap K(F_0 - \lambda) = \bigcap_{i \in I} L(F_i) \cap L(F_0 - \lambda)$ (dado que F_0 no se eliminó).
Por lo tanto $F_0(y + \tilde{\alpha}_1 v_1 + \ldots + \tilde{\alpha}_m v_m) = F_0(x_0) = \mu$
y luego $\inf\{F_0(x),\, x \in (N' + W^{\perp} + B) \cap N' \cap \mathbb{Z}^n\} \le \mu$.
Como la otra desigualdad es trivial, queda completada la prueba.

♦

Aplicando la Proposición 1.-B.1 a la familia $\{F_0 - \lambda, F_1, \ldots, F_s\}$, se muestra que existe una base entera $\{v_1, \ldots, v_m\}$ de W con $\sigma(\{v_1, \ldots, v_m\}) = d^{0(n^2)}\sigma(\{F_0 - \lambda, F_1, \ldots, F_s\}) = (sd)^{0(n^2)}\sigma$. Dado que $(N' \cap W^{\perp}) \subseteq B(0,R)$, con $\sigma(R) = (sd)^{0(n^2)}\sigma$ (Lema 1.-C.2), el lema anterior permite concluir que

$$\mu = \inf\{F_0(x),\, x \in N' \cap \mathbb{Z}^n\} = \inf\{F_0(x),\, x \in N' \cap B(0,R) \cap \mathbb{Z}^n\}\,.$$

En la demostración del Lema 1, se mostró que a partir de cada punto $x' \in N'$, se recupera un punto $x := x' + t_1 u_1 + \ldots + t_r u_r \in N$ con $F_0(x) = F_0(x')$ (ya que las direcciones $u_1, \ldots, u_r$ son tales que $F_0(Tu_i)$ es constante). Además, aplicando aquí las estimaciones del Lema 1.-B.10, se obtiene que $x \in M \cap B(0, \tilde{R}) \cap \mathbb{Z}^n$, con $\sigma(\tilde{R}) = (sd)^{0(n^2)}\sigma$.

Por consiguiente

$$\mu \geq \inf\{F_0(x),\ x \in M \cap B(0, \tilde{R}) \cap \mathbb{Z}^n\}$$

y por lo tanto

$$\mu = \inf\{F_0(x),\ x \in M \cap B(0, \tilde{R}) \cap \mathbb{Z}^n\}$$
$$\text{donde} \quad \sigma(\tilde{R}) = (sd)^{0(n^2)}\sigma$$

B. Para completar la demostración del Teorema 2, se probará el resultado siguiente:

LEMA 3. Si $M \cap \mathbb{Z}^n$ es no vacío, entonces

$$\inf\{F_0(x),\ x \in M\} > -\infty \Leftrightarrow \inf\{F_0(x),\ x \in M \cap \mathbb{Z}^n\} > -\infty$$

Demostración: La demostración es muy parecida a la del Lema 1, y utiliza las mismas propiedades de los polinomios cuasiconvexos.

Sea $x_0 \in M \cap \mathbb{Z}^n \neq \emptyset$. Consideremos la familia de polinomios cuasiconvexos $\mathcal{F} := \{F_1, \ldots, F_s, F_0 - F_0(x_0)\}$.

Se define $N := \{x \in \mathbb{R}^n : F(x) \leq 0, \forall F \in \mathcal{F}\}$ (observemos que $N \cap \mathbb{Z}^n \neq \emptyset$).

Supongamos que $\inf\{F_0(x),\ x \in M\} = -\infty$, entonces se tiene que
$\inf\{F_0(x),\ x \in N\} = -\infty$.

Apliquemos a la familia $\mathcal{F}$ la construcción 1.-B.9 de eliminación de restricciones superfluas, obteniendo así la familia $\mathcal{F}' \subseteq \mathcal{F}$.

- Supóngase en primer lugar que $F_0 - F_0(x_0) \in \mathcal{F}'$.
  Sea $N' = \{x \in \mathbb{R}^n : F(x) \leq 0, \forall F \in \mathcal{F}'\}$.
  Claramente, $\inf\{F_0(x),\ x \in N'\} = -\infty$.
  Por otro lado, se tiene la descomposición $N' = (N' \cap W^{\perp}) + W$ donde $N' \cap W^{\perp}$ es compacto y W coincide con el conjunto de direcciones constantes de la familia $\mathcal{F}'$ (en particular dado $v \in W$, $F_0(Tv)$ es constante, y por lo tanto $F_0(y + Tv)$ también, $\forall y \in \mathbb{R}^n$).
  Para todo $x \in N'$, se escribe $x = x' + v$, con $x' \in N' \cap W^{\perp}$ y $v \in W$.

Vale la igualdad: $F_0(x') = F_0(x'+tv)$ $(\forall t \in \mathbb{R})$, y por consiguiente, $F_0(x') = F_0(x)$.

Se prueba así que $\inf\{F_0(x) : x \in N'\} = \inf\{F_0(x) : x \in N' \cap W^{\perp}\}$.
Pero dado que $N' \cap W^{\perp}$ es compacto, no puede ser

$$\inf\{F_0(x) : x \in N' \cap W^{\perp}\} = -\infty. \qquad \text{Contradicción}$$

– Luego, para obtener $\mathcal{F}'$ se suprimió la restricción $F_0 - F_0(x_0)$.
Se puede suponer sin pérdida de generalidad que se eliminaron $F_1, F_2, \ldots, F_r, F_0 - F_0(x_0)$ en ese orden (pudiendo ser $r = 0$).
Se afirma que para todo $\ell \in \mathbf{N}$, existe $x_\ell \in M \cap \mathbb{Z}^n$ tal que $F_0(x_\ell) < -\ell$, y por lo tanto $\inf\{F_0(x) : x \in M \cap \mathbb{Z}^n\} = -\infty$, con lo que queda probado el lema:

Prueba de la afirmación: Sea $\ell \in \mathbf{N}$, y sean $u_1, \ldots, u_r$ las direcciones (que se pueden tomar *enteras*) que se eligieron para suprimir $F_1, \ldots, F_r, F_0 - F_0(x_0)$.
Dado que $F_0(Tu_0)$ es estrictamente decreciente, existe $t_0 \in \mathbf{N}$ de manera que $F_0(x_0 + t_0 u_0) < -\ell$.
Además, para todo $k > r$, se verifica $F_k(x_0 + t_0 u_0) \leq F_k(x_0) \leq 0$ pues $u_0 \in \bigcap_{r<k\leq s} K(F_k)$.
Para todo $1 \leq j \leq r$, las condiciones "$F_j(Tu_j)$ estrictamente decreciente" y "$u_j \in \bigcap_{j<i\leq s} K(F_i) \cap K(F_0 - F_0(x_0))$" implican que se pueden elegir recursivamente $t_r, t_{r-1}, \ldots, t_1 \in \mathbf{N}$ tales que si se define

$$x_j := x_0 + t_0 u_0 + t_r u_r + \ldots + t_j u_j$$

vale:

– $F_j(x_j) \leq 0$
– para $r < k \leq s$, $F_k(x_j) \leq F_k(x_0 + t_0 u_0) \leq 0$;
– para $j < k \leq r$, $F_k(x_j) \leq F_k(x_k) \leq 0$;
– $F_0(x_j) \leq F_0(x_0 + t_0 u_0) < -\ell$.

Por consiguiente, definiendo $x_\ell := x_1 = x_0 + t_0 u_0 + t_r u_r + \ldots + t_1 u_1$, se verifica que $x_\ell \in M \cap \mathbb{Z}^n$ y $F_0(x_\ell) < -\ell$.

REFERENCIAS

[Ba-Ma 1] B. Bank, R. Mandel: *Parametric integer optimisation*. Akademie-Verlag, Berlin (1988).

[Ba-Ma 2] B. Bank, R. Mandel: *(Mixed-) Integer solutions of quasiconvex polynomial inequalities*. Mathematical Research Advances in Mathematical Optimisation, Akademie-Verlag, Berlin, Vol. 45 (1988) 20-34.

[Be-Ko-Re] M. Ben-Or, M. Kozen, J. Reif: *The complexity of elementary algebra and geometry*. J. of Comp. and System Sci. 32 (1986) 251- 264.

[Be-Ti] M.Ben-Or, P. Tiwari: *A deterministic algorithm for sparse multivariate polynomial interpolation* (Extended abstract). 20th Ann. ACM Symp. Theory of Computing (1988) 301-309.

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

[Bro] W.S. Brown: *On Euclid's algorithm and the computation of polynomial greatest common divisors*. J. ACM, Vol. 18 (1971) 478-504.

[Br 1] D. Brownawell: *Bounds for the degrees in the Nullstellensatz*. Ann. Math. Second Series, Vol. 126 N°3 (1987) 577-591.

[Br 2] D. Brownawell: *A prime power version of Nullstellensatz*. Preprint (1989).

[Ca 1] L. Caniglia: *Complejidad de algoritmos en geometría algebraica computacional*. Tesis, Universidad de Buenos Aires (1989).

[Ca 2] L. Caniglia: *How to compute the Chow form of an unmixed ideal in subexponential time*. Preprint (1989).

[Ca-Ga-He 1] L. Caniglia, A. Galligo, J. Heintz: *Some new effectivity bounds in computational geometry*. Proc. 6th Int'l Conf. Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Rome 1988, Springer LN Comput. Sci. 357 (1989) 131-151.

[Ca-Ga-He 2] L. Caniglia, A. Galligo, J. Heintz: *Borne simple exponentielle pour les degrés dans le théorème des séros sur un corps de caractéristique quelconque*. C.R. Acad. Sci. Paris, t. 307, Série I (1988) 255-258.

[Ca-Gu-Gu] L. Caniglia, J. Guccione, J.J. Guccione: *Local membership problems for polynomial ideals*. Preprint (1989).

[Ch-Gr 1] A.L. Chistov, D.Yu. Grigor'ev: *Subexponential time solving systems of algebraic equations I, II*. LOMI preprints E-9-83, E-10-83, Leningrad 1983.

[Ch-Gr 2] A.L. Chistov, D.Yu. Grigor'ev: *Complexity of quantifier elimination in the theory of algebraically closed fields*. Proc. 11th Symp. MFCS 1984, Springer LN Comp. Sci. 176 (1984) 17-31.

[Co] G.E. Collins: *Subresultants and reduced polynomial remainder sequences.* J. ACM, Vol. 14 (1967) 128-142.

[Di-Fi-Gi-Se] A. Dickenstein, N. Fitchas, M. Giusti, C. Sessa: *The membership problem of unmixed polynomial ideals is solvable in single exponential time.* A aparecer en Discrete and Applied Mathematics, Special Issue, AAECC-7, Toulouse (1989).

[Gat] J. von zur Gathen: *Parallel arithmetic computation: a survey.* Proc. 13th Conf. MFCS (1986).

[Gr 1] D.Yu. Grigor'ev: *The complexity of the decision for the first-order theory of algebraically closed fields.* Math. USRR Izvestija, Vol. 29 N°2 (1987) 459-475.

[Gr 2] D.Yu. Grigor'ev: *Complexity of deciding Tarski algebra.* J. Symbolic Comput. 5 (1988) 65-108.

[Gr-Ka-Si] D.Yu. Grigor'ev, M. Karpinski, M. Singer: *Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields.* Univ. Bonn Research Report N°8523 (1988).

[Gr-Vo] D.Yu. Grigor'ev, N. Vorobjov: *Solving systems of polynomial inequalities in subexponential time.* J. Symbolic Comput. 5 (1988) 37-64.

[He] J. Heintz: *Definability and fast quantifier elimination over algebraically closed fields.* Theoret. Comput. Sci. 24 (1983) 239-277; Traducción rusa en Kyberniticeskij Sbornik, Novaja Serija, Vyp. 22, Mir Moscow (1985) 113-158.

[He-Ro-So 1] J. Heintz, M.-F. Roy, P. Solernó: *On the complexity of semialgebraic sets* (Extended abstract). Proc. IFIP Congress'89, IX World Computer Congress, North-Holland (1989).

[He-Ro-So 2] J. Heintz, M.-F. Roy, P. Solernó: *Complexité du principe de Tarski-Seidenberg.* C.R. Acad. Sci. Paris, T. 309, Série I (1989) 825-830.

[He-Ro-So 3] J. Heintz, M.-F. Roy, P. Solernó: *Sur la complexité du principe de Tarski-Seidenberg.* A aparecer en Bull. Soc. Math. France (1990).

[He-Sch] J. Heintz, C.P. Schnorr: *Testing polynomials which are easy to compute.* Monographie de l'Enseignement Mathématique, Vol. 30, Impr. Kundig, Genève.

[He-Wü] J. Heintz, R. Wüthrich: *An efficient quantifier elimination algorithm for algebraically closed fields.* SIGSAM Bull. 9 (1975) 11.

[Kal] E. Kaltofen: *Greatest common divisors of polynomials given by Straight-Line Programs.* Math. Sci. Research Inst. Preprint, vol. 01918-86, Berkeley, CA (1986).

[Kh] L.G. Khachiyan: *Convexity and complexity in polynomial programming.* Proc. Int. Congress Math., Varsovia (1983).

[Ko] J. Kollár: *Sharp effective Nullstellensatz.* Preprint (1989).

[La] S. Lang: *Introduction to algebraic geometry.* Interscience tracts in pure and applied mathematics, 1958.

[Mi] M. Mignotte: *Some useful bounds.* Computer Algebra (Symbolic and Algebraic Computation). Springer-Verlag (1982) 259-264.

[Mil] J. Milnor: *On the Betti numbers of real algebraic varieties.* Proc. Amer. Math. Soc. 15/2 (1964) 275-280.

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

[Ne] Yu.V. Nesterenko: *Estimates for the orders of zeros of functions of a certain class and applications in the theory of transcendental numbers.* Math. USSR Izvestija Vol 11 (1977) N°2. Izvestia Akad. Nauk. SSR Set-Mat. Tom 41 (1977) N°2.

[Ph] P. Philippon: *Théorème des zéros effectif d'après J. Kollár.* Séminaire I.H.P. (1988).

[Re] J. Renegar: *On the computational complexity and geometry of the first order theory of the reals. Part III. Quantifier elimination.* Technical Report 856, Cornell University (1989).

[Ro] R. Tyrrell Rockafellar: *Convex Analysis.* Princeton Mathematical Series N°28. (1970).

[Sc] A. Schrijver: *Theory of linear and integer programming.* Wiley Interscience Series in Discrete Mathematics (1989).

[Sh] I.R. Shafarevich: *Algebraic Geometry.* Springer, Berlin (1984).

[So] P. Solernó: *Complejidad de conjuntos semialgebraicos.* Tesis, Universidad de Buenos Aires (1989).

[Ta-Kh] S.P. Tarasov, L.G. Khachiyan: *Bounds of solutions and algorithmic complexity of systems of convex diophantine inequalities.* Soviet. Math. Adel., Vol. 22, N°3 (1980).

[Tar] A. Tarski: *A decision method for elementary algebra and geometry.* 2nd ed. Univ. of California Press, Berkeley (1951).

[Th] R. Thom: *Sur l'homologie de variétés algebriques réelles.* Differential and Combinatorial Topology (Princeton) (1965) 255-265.

[Wei] V. Weispfenning: *The complexity of linear problems in fields.* J. Symbolic Comput. 5 (1988) 3-28.

[Wü] R. Wüthrich: *Ein Quantorenelimination verfahren für die Theorie der algebraisch abgeschlossenen Körper.* Ph.D. Thesis, University of Zurich (1977).