Ideología de Conjuntos Cuestores: Kakeya sets, Nullstellensatz Combinatorio y Generalizaciones a Sucesiones Secantes

(Ideology of Correct Test Sequences: Kakeya sets, Combinatorial Nullstellensatz and Generalizations to Secant Sequences)

Antonio Fernández González

Trabajo de Fin de Grado

para acceder al

Grado en Matemáticas

Facultad de Ciencias

Universidad de Cantabria

Director: Luis Miguel Pardo Vasallo

Julio - 2019

*A **mi familia**, por aguantarme (que no es fácil),*
*a **Gema Miñón**, por enseñarme lo que son las matemáticas,*
*a **Cecilia y Cristina**, por el bautismo matemático y el cariño,*
*a **mis profesores**, por guiarme en este camino,*
*a **mis compañeros**, por los buenos momentos pasados,*
*a **María**, por el apoyo desde la distancia,*
*a **Luis Miguel Pardo**, por la confianza depositada en mí*
y a quien se aventure a leer esto.

"It is possible that the life of a mathematician is one which no perfectly reasonable man would elect to live."
— *G. H. Hardy,* Some famous problems of the theory of numbers and in particular Waring's Problem

Abstract. Some of the first examples of probabilistic algorithms were those of Solovay-Strassen and Miller-Rabin for testing primality. Soon afterwards, probabilistic algorithms appeared for testing nulity of polynomials given by evaluation. Two were the ideologies for facing this problem: Schwartz-Zippel tests and Correct Tests Sequences (J. Heintz, C.-P. Schnorr). The aim of this project is to generalize and better comprehend this notion of Correct Test Sequence.

In order to do that, we first need a Bézout's Inequality for constructible sets (Chapter 1). Then, we generalize the definition of Correct Test Sequence and show that Kakeya sets over finite fileds and the Combinatorial Nullstellensatz are particular cases of this definition (Chapter 2). Finally, we generalize the main result of J. Heintz and C.-P. Schnorr, studying a way to test whether a list of polynomials forms a secant sequence (Chapter 3).

Key words: Algebraic geometry, Bézout's Inequality, Correct Test Sequences, Kakeya sets, Combinatorial Nullstellensatz, secant sequences.

Resumen. Algunos de los primeros ejemplos de algoritmos probabilistas fueron los de Solovay-Strassen y Miller-Rabin para el problema de primalidad. Poco después, aparecieron algoritmos probabilistas para testar la nulidad de polinomios dados en evaluación. Dos fueron las ideologías para hacer frente a este problema: los tests de Schwartz-Zippel y los Conjuntos Cuestores (J. Heintz y C.-P. Schnorr). El objetivo de este trabajo es generalizar y comprender mejor la noción de Conjunto Cuestor.

Para ello, necesitamos primero una Desigualdad de Bézout para conjuntos constructibles (Capítulo 1). Después, generalizamos la definición de Conjunto Cuestor y vemos que los conjuntos de Kakeya sobre cuerpos finitos y el Nullstellensatz Combinatorio son casos particulares de esta definición (Capítulo 2). Finalmente, generalizamos el resultado principal de J. Heintz y C.-P. Schnorr, estudiando una forma de testar si una lista de polinomios es sucesión secante (Capítulo 3).

Palabras clave: Geometría algebraica, Desigualdad de Bézout, Conjuntos Cuestores, Conjuntos de Kakeya, Nullstellensatz Combinatorio, sucesiones secantes.

Índice

CAPÍTULO 0

Introducción y resumen de los prinicpales resultados de la memoria

Índice

0.1. El contexto: algoritmos probabilstas

Una de las grandes tradiciones en el diseño de algoritmos eficientes es el diseño de *algoritmos probabilistas*. La incorporación de dichos algoritmos comienza con el diseño de *algoritmos de tipo MonteCarlo* (denotados mediante las clases de complejidad **RP** y co−**RP**) introducidos para enfrentar la decisión del problema PRIMES: decidir si un número natural $n \in \mathbb{N}$ es o no primo. La dificultad obvia es que todos los algoritmos conocidos hasta los años 70 eran de complejidad exponencial en tiempo (o, en términos menos técnicos, el tiempo de ejecución es una función polinomial en el propio número natural $n \in \mathbb{N}$ dado como input). Un algoritmo de este tipo (como la Criba de Eratóstenes) es muy ineficiente y nulamente útil para cualquier aplicación de interés. Los algoritmos eficientes para decidir si un entero $n \in \mathbb{N}$ es o no primo son aquellos cuyo tiempo de ejecución es polinomial en la talla de su representación decimal o binaria (lo que se puede traducir vulgarmente en un tiempo de ejecución acotado por una función polinomial en $\log_2 n$).
Para paliar la dificultad de PRIMES surgieron, casi simultáneamente, los algoritmos tipo MonteCarlo de Solovay-Strassen (cf. [**SoSt, 77**]) o de Miller-Rabin (cf. [**Mi, 75**], [**Ra, 80**]). Aunque fueron llamados "Tests de Primalidad', en realidad son "Tests de Composición", puesto que la respuesta es segura solamente si responden COMPUESTO. Y es que esta es la cualidad fundamental de los tests de tipo **RP** para decidir si un input x pertenece a una clase L:

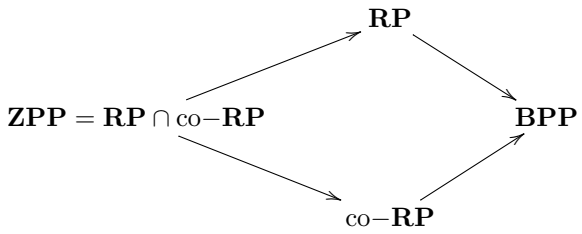
i) Solidez: Si $x \in L$, el algoritmo realiza elecciones aleatorias de datos y de tal modo que, sea cual sea la elección de y, el algoritmo responde afirmativamente.
ii) Completitud: Si $x \notin L$, el algoritmo realiza elecciones aleatorias de datos y de tal modo que la probabilidad (en el espacio de elecciones de los y) de que el algoritmo responda negativamente es muy alta.

De hecho, se suele asumir una formulación simple del tipo: Si $x \notin L$, la probabilidad de error estaría acotada por

$$\text{Prob}_y[\text{el algoritmo responde Sí actuando sobre } x \text{ e } y] \leq 1/3.$$

Los algoritmos de Solovay-Strassen y Miller-Rabin son algoritmos probabilistas que resuelven el problema decisional $n \in$ COMPUESTO? en tiempo polinomial en $\log_2 n$.
A partir de la clase **RP** surgen dos clases: los algoritmos de la clase **BPP** y los algoritmos de tipo *Las Vegas* (o clase **ZPP**). De hecho, se tiene el diagrama siguiente de clases de algoritmos probabilistas (donde las flechas son inclusiones):

(0.1.1)



La clase **BPP** es la clase de algoritmos probabilistas que pueden dar respuestas erróneas a ambos lados de la pregunta decisional (tanto para $x \in L$ como para $x \notin L$), pero la probabilidad de error aparece controlada; i.e.,

$$\text{Prob}_y[\text{el algoritmo responde erróneamente actuando sobre } x \text{ e } y] \leq 1/3.$$

La clase de algoritmos **ZPP** (que coincide con la intersección $\mathbf{RP} \cap \text{co}-\mathbf{RP}$) es la clase de algoritmos cuyo tiempo de ejecución es, en promedio, polinomial en la talla de la representación del input, cuyas respuestas son siempre correctas (no comete errores). Podría requerir de un tiempo exponencial, pero la probabilidad de que eso sucediera sería baja (Markov-Chebyshev). Es decir, no comete errores y

$$\text{E}_y[\text{tiempo de ejecución en } x \text{ e } y] \leq |x|^{O(1)},$$

donde $|x|$ es la talla de la representación del input. Obviamente, cuanto más grande es la clase en (0.1.1), peor es la calidad del algoritmo. La "fórmula del éxito" para el estudio de algoritmos eficientes comenzaría buscando un algoritmo en **BPP**; seguiría buscando un algoritmo en **RP** o co-**RP**; después se intentaría bajar a **ZPP** y, en caso de llegar a este nivel, hay esperanza de poder llegar a los algoritmos de tipo determinista que requieren solamente tiempo polinomial en el caso peor: la clase **P** de los *algoritmos tratables*.

Desafortunadamente, esa "fórmula del éxito" es dudosa. De hecho, uno de los problemas centrales de la Complejidad Computacional (tan duro como la afamada Conjetura de Cook) consiste en decidir si alguna de las relaciones del diagrama 0.1.1 es un contenido estricto o una igualdad. Nadie conoce la respuesta.

Así que podemos hablar de "casos de éxito". Así, tras los tests de composición de Solovay-Strassen y Miller-Rabin, Adleman y Huang lograron los primeros test de primalidad en **ZPP** (cf. [**AdHu, 92**]) y, finalmente, la "gloria" alcanzó a M. Agrawal, N. Kayal y N. Saxena (cf. [**AKS, 04**]) cuando obtuvieron su test determinista polinomial para el problema PRIMES.

0.2. Tests probabilistas de nulidad de polinomios multivariados

El siguiente problema para el que se desarrollaron algoritmos probabilistas son los TESTS DE NULIDAD DE POLINOMIOS MULTIVARIADOS: el input del problema es un polinomio multivariado $f \in K[X_1, \ldots, X_n]$ del que se conoce un algoritmo eficiente de evaluación en un punto (como, por ejemplo, los esquemas de evaluación descritos en el Anexo B) o un simple oráculo que los evalúa (conocidos como *black-boxes*), pero no se conocen sus coeficientes. La pregunta a decidir es si f es o no el polinomio nulo.

Nótese que la dificultad pasa por no poder "interpolar" el polinomio, es decir, no se pueden hallar todos sus coeficientes. La razón es que si $f \in K[X_1, \ldots, X_n]$ es un polinomio de grado a lo sumo d, el número de posibles coeficientes no nulos es

$$\binom{d+n}{n} \approx d^n,$$

con lo que, a priori, habría que hallar una cantidad exponencial de coeficientes para decidir si es o no nulo y, por tanto, un algoritmo que requiera interpolación sería altamente ineficiente.

La alternativa a una interpolación brutal pasa por algoritmos probabilistas basados en evaluación. Las primeras ideas obvias pasan por evaluar en pocos puntos para testar nulidad. Esa fue, por ejemplo, la idea subyacente al test de No Nulidad de Schwartz-Zippel (cf. [**Sch, 80**], [**Zp, 79**]): disponiendo de un control d de los grados y de un conjunto amplio de posibles elecciones de valores (por ejemplo, la clase $\mathcal{C} = ([0, 2d+1] \cap \mathbb{Z})^n$), la probabilidad de que un polinomio no nulo $f \in X[X_1, \ldots, X_n] \setminus \{0\}$ se anule en m puntos $x_1, \ldots, x_m$ elegidos aleatoriamente en $\mathcal{C}^m$ está acotada por

$$\text{Prob}_{(x_1,\ldots,x_m)\in\mathcal{C}^m}[f(x_i) = 0, 1 \leq i \leq m, f \neq 0] \leq \frac{1}{2^m}.$$

Esto ofrece un algoritmo en **RP** para detectar polinomios no nulos. El modelo de algoritmo propuesto por Schwartz-Zippel adolece de muchos inconvenientes. El mayor es que la clase $\mathcal{C}$ donde se eligen los puntos es excesivamente grande. Esto hace imposible usar esta estrategia para profundizar en la complejidad del

problema. De hecho, no se conocen algoritmos en **ZPP** para resolver el problema de decidir nulidad de polinomios multivariados dados mediante programas, redes neuronales o black-boxes.
Más aún, son muy escasas las esperanzas de una completa "derandomización" del problema de los "Tests de Identidad Polinomial" (o PIT, una versión equivalente de los "Tests de Nulidad Polinomial") como señalan, por ejemplo, Kabanets e Impagliazzo en [**KaIm, 04**] y sus referencias.

0.3. Correct test sequences (o conjuntos cuestores)

La principal dificultad de ataque del Problema de Nulidad Polinomial con técnicas a la Schwartz-Zippel es la *carencia de certificados seguros de nulidad de tamaño tratable*. Dicho de otra manera, supongamos que exigimos la certidumbre (nula probabilidad de error) en la respuesta "El polinomio dado es nulo". Un test de Schwartz-Zippel **exigiría evaluar nuestro input en todos los puntos del conjunto** $\mathcal{C}$ de Schwartz-Zippel. La "certidumbre de nulidad" en el test propuesto anteriormente exige la evaluación en $(2d+1)^n$ puntos, lo que, a la postre, es incluso menos eficiente que interpolar los $\begin{pmatrix} d+n \\ n \end{pmatrix}$ coeficientes.
Para paliar esta dificultad surgen las *Correct Test Sequences* en [**HeSc, 83**] de 1983. J. Heintz y C. P. Schnorr se inspiran lejanamente en la prueba de L. Adleman de $\mathbf{BPP} \subseteq \mathbf{P/poly}$ para generar su concepto.

Definición 1 (Correct Test Sequences, [**HeSc, 83**]). *Dada una variedad* Ω *de polinomios en* $\mathbb{K}[X_1, \ldots, X_n]$, *de dimensión de Krull finita,* $\mathbb{K}$ *algebraicamente cerrado, una lista de puntos afines* $\mathcal{Q} = (x_1, \ldots, x_m) \in (\mathbb{K}^n)^m$ *se dice conjunto cuestor (o correct test sequence) para* Ω *con respecto al problema de Nulidad (con respecto a* $\{0\}$*) si verifica*

$$\forall f \in \Omega, f(x_1) = \ldots = f(x_m) = 0 \Longrightarrow f \equiv 0.$$

El resultado principal de Heintz-Schnorr se resume en el siguiente enunciado:

Teorema 0.3.1. *Con las notaciones precedentes, supongamos que* $\mathrm{char}(\mathbb{K}) = 0$, *y que para todo* $f \in \Omega$, *su grado total está acotado por* d. *Consideramos el conjunto* $\{1, \ldots, u\} \subseteq \mathbb{Z}$ *de números enteros y el retículo* $\Lambda = \{1, \ldots, u\}^n \subseteq \mathbb{K}^n$, *siendo* $u \geq 2d^2$.
Sea $s \geq 6 \dim(\Omega)$, *donde* $\dim(\Omega)$ *es la dimensión de Krull de* Ω. *Entonces:*

i) **Existencia***: Existen correct test sequences* $\mathcal{Q} = (x_1, \ldots, x_s) \in \Lambda^s$, *para* Ω *con respecto a* $\{0\}$.
ii) **Alta probabilidad***: Además, la probabilidad de que una lista* $\mathcal{Q} \in \Lambda^s$ *de puntos del retículo sea correct test sequence para* Ω *con respecto a* $\{0\}$ *es mayor o igual que*

$$1 - \frac{1}{u^{s/6}},$$

donde la probabilidad considerada en Λ^s *es la uniforme.*

El resultado presenta rasgos propios que lo diferencian del test de Schwartz-Zippel. Obviamente, puede usarse como test probabilista de NO Nulidad en la clase **RP** tan aceptable como el de Schwartz-Zippel. De hecho, se ha usado de manera masiva en diversos algoritmos para la resolución simbólica eficiente de sistemas de ecuaciones polinomiales multivariadas: los conjuntos cuestores son claves en los algoritmos del grupo TERA-Kronecker (ver [**GHMMP, 98**], [**GHMP, 97**], [**CGHMP, 03**], [**HMPS, 00**] y sus referencias).
Sin embargo, la idea de "certificación de nulidad" o su amplia aplicabilidad no son suficientes para explicar con claridad lo que son las CTS's o su potenciabilidad para mejor la eficacia de los algoritmos que tratan este problema. Contextualmente, y más allá del contenido de este TFG, tres son las preguntas que se plantean en el estudio a largo plazo de los conjuntos cuestores:

Problema 1. *¿Permitirían los conjuntos cuestores hallar algoritmos en la clase* **ZPP** *para testar si un polinomio es nulo o no?*

Problema 2. *Dado que la inspiración inicial de los conjuntos cuestores fue la prueba de L. Adleman de* $\mathbf{BPP}_{\mathbb{F}_2} \subseteq \mathbf{P}_{\mathbb{F}_2}\mathbf{/poly}$ *para el cuerpo* $K = \mathbb{F}_2 = \{0, 1\}$, *¿es posible usar conjuntos cuestores para probar* $\mathbf{BPP}_{\mathbb{K}} \subseteq \mathbf{P}_{\mathbb{K}}\mathbf{/poly}$ *para cuerpos algebraicamente cerrados* $\mathbb{K}$*?*

Problema 3. *Las inclusiones* $\mathbf{BPP}_{\mathbb{R}} \subseteq \mathbf{P}_{\mathbb{R}}\mathbf{/poly}$ *tienen una fuerte relación con la dimensión de Vapnik-Chervonenkis de Teoría del Aprendizaje Estadístico, ¿qué relación tienen los conjuntos cuestores con la dimensión VC?*

La respuesta a las tres preguntas se escapa de las posibilidades de un Trabajo de Fin de Grado de Matemáticas. Sin embargo, mucha es la tarea aún pendiente antes de iniciar el asalto a estos tres Problemas. Para empezar, conviene reconsiderar toda la teoría introducida por J. Heintz y C. P. Schnorr desde los mismos principios. Y es ahí donde comienza este TFG:

Ideología de Conjuntos Cuestores: Kakeya sets, Nullstellensatz Combinatorio y Generalizaciones a Sucesiones Secantes.

0.4. Resumen de Resultados

La memoria se ha dividido en tres capítulos, a los que hemos añadido dos anexos (Anexos A y B) conteniendo material técnico conocido de uso común a lo largo de los tres capítulos de la memoria. Debe señalarse que esencialmente *todo el material de los tres capítulos de la memoria es original*, como se expondrá en este resumen. Los tres Capítulos son los siguientes:

- Capítulo 1: Desigualdad de Bézout geométrica para constructibles: una prueba completa.
- Capítulo 2: Conjuntos Cuestores y aplicaciones: conjuntos de Kakeya sobre cuerpos finitos (Dvir) y Nullstellensatz Combinatorio (Alon-Tao).
- Capítulo 3: Sobre la densidad de los conjuntos cuestores en variedades cero-dimensionales: aplicación a la detección de sucesiones secantes.

0.4.1. Capítulo 1. La desigualdad de Bézout es un resultado esencial en Teoría de la Intersección Geométrica. Contrariamente a la convicción del folklore, y a su nombre, la Desigualdad de Bézout es un resultado relativamente reciente en la historia de las matemáticas. A principios de los años ochenta, tres autores llegaron de manera independiente a establecer por vez primera nociones de grado de variedades algebraicas y a demostrar desigualdades de Bézout para cada una de ellas.

- J. Heintz en [**He, 83**], introduce la noción de grado geométrico de una variedad algebraica afín y demuestra una desigualdad de Bézout afín.
- W. Vogel en [**Vo, 84**], utiliza la noción de grado introducida por el coeficiente director del polinomio de Hilbert de una variedad algebraica proyectiva y establece su versión proyectiva de la desigualdad de Bézout.
- W. Fulton en [**Fu, 83**], usa la teoría de divisores para introducir una noción de grado que tiene en cuenta la presencia de multiplicidades y establece su igualdad de Bézout.

En esta memoria seguiremos esencialmente la noción de grado geométrico introducida por J. Heintz que, de hecho, es equivalente a la de Vogel a través de la clausura proyectiva. Sin embargo, sólo J. Heintz intenta hacer un desarrollo apropiado de una desigualdad de Bézout para constructibles. Sin embargo, J. Heintz hizo una elección inapropiada de la noción de grado de un constructible afín: en la Remark 2.(2) de [**He, 83**], se define el grado de un constructible afín $C \in \mathbb{A}^n(\mathbb{K})$ como el grado de su clausura en la topología de Zariski (es lo que hemos llamado Z-deg(C) en la Sección 1.4). Como se observa en la Proposición 1.4.1, el Z-deg no satisface la desigualdad de Bézout. Aunque el ejemplo que aportamos es de cosecha propia, J. Heintz también observó esta dificultad en su Corrigendum (cf. [**He, 85**]).
En este Capítulo 1 pretendemos corregir esa elección inapropiada para demostrar una desigualdad de Bézout geométrica para constructibles. Para ello, introducimos una nueva noción de grado de un conjunto constructible afín (la noción de $\deg(C)$ introducida en la Definición 6). Probamos que es una noción bien definida (probando la existencia de descomposición minimal de constructibles como unión finita de localmente cerrados irreducibles en Proposición 1.2.5), probamos que es una cota superior del Z-deg y que coincide con la noción original de [**He, 83**] en el caso de variedades algebraicas afines (Proposición 1.4.4). Además, se prueba que nuestra noción es subaditiva (Proposición 1.4.5) y se porta bien en la intersección con variedades afines lineales (reparando la Remark 2.(2) de [**He, 83**] en la Proposición 1.4.8). Probamos, finalmente, que el Z-deg de la imagen de un constructible por una aplicación lineal no crece más allá del grado original (Proposición 1.5.1):

$$\deg\left(\overline{\varphi(C)}^Z\right) \leq \deg(C).$$

Estas herramientas nos bastan para demostrar el resultado esencial del Capítulo 1: el Teorema 1.5.5:

Teorema 0.4.1 (**Desigualdad de Bézout para constructibles**). *Sean $C, D \subseteq \mathbb{A}^n(\mathbb{K})$ dos conjuntos constructibles afines donde $\mathbb{K}$ es un cuerpo algebraicamente cerrado. Entonces,*

$$\deg(C \cap D) \leq \deg(C) \cdot \deg(D).$$

Nótese que no hemos probado la estabilidad de la noción de grado por transformaciones lineales. La última Sección del Capítulo se dedica a probar un par de variaciones técnicas útiles de la desigualdad de Bézout: en la Proposición 1.6.1 probamos que la desigualdad introducida en [**HeSc, 83**] sigue siendo cierta para constructibles y en la Proposición 1.6.2 probaremos que si $C \subseteq \mathbb{A}^n(\mathbb{K})$ es constructible y $\varphi : C \longrightarrow \mathbb{A}^m(\mathbb{K})$ es una aplicación polinomial dada por polinomios de grado a lo sumo $d \geq 1$, se tiene

$$\deg\left(\overline{\varphi(C)}^Z\right) \leq \deg(C) \cdot d^m.$$

Este último resultado se aplica, por ejemplo, para dar acotaciones finas del número de puntos $\mathbb{F}$-racionales de una variedad algebraica $\mathbb{F}$-definible, cuando $\mathbb{F}$ es un cuerpo finito (Corolario 1.6.3).

0.4.2. Capítulo 2. En este Capítulo generalizamos la noción clásica de conjunto cuestor ("correct test sequence") introducida originalmente por J. Heintz y C. P. Schnorr en [**HeSc, 83**]. En lugar de considerar conjuntos cuestores como tests de nulidad, en la Definición 7 hacemos la siguiente generalización: Consideramos $\Omega \subseteq K[X_1, \ldots, X_n]$ un constructible de dimensión finita y equidimensional cuyos elementos son polinomios multivariados. Supongamos $\Sigma \subseteq \Omega$ un subconjunto de codimensión positiva; un conjunto cuestor para Ω con respecto a Σ es una lista de puntos $\mathcal{Q} := (x_1, \ldots, x_n) \in (\mathbb{A}^n(\mathbb{K}))^m$ tal que

$$\forall f \in \Omega, \text{ si } f(x_i) = 0, 1 \leq i \leq m, \text{ entonces } f \in \Sigma.$$

Es decir, tenemos un certificado de pertenencia a una subvariedad discriminante Σ basado en la evaluación en $\mathcal{Q}$ de los elementos de Ω. El caso original de [**HeSc, 83**] es el caso en el que el discriminante Σ está formado por el polinomio nulo (i.e., $\Sigma = \{0\}$) y se corresponde con los "Tests de Nulidad de Polinomios Multivariados". Tras establecer la noción y probar una cota inferior elemental para su longitud (Proposición 2.2.4), pasamos a las aplicaciones anunciadas en el título.
La Sección 2.3 se dedica a redemostrar y generalizar un resultado de Z. Dvir sobre los conjuntos de Kakeya sobre cuerpos finitos. Los conjuntos de Kakeya (o conjuntos de Besikovitch) tienen su origen en los trabajos de S. Kakeya en 1917, como subconjuntos del espacio euclídeo real que contienen segmentos de longitud unidad definidos por cualquier dirección posible. En su survey sobre los conjuntos de Kakeya [**Wo, 99**], T. Wolff trasladó la noción al contexto de cuerpos finitos, generando la pregunta sobre la cardinalidad de los mismos. En el trabajo [**Dv, 09**], Z. Dvir mostró una cota inferior para la cardinalidad de los conjuntos de Kakeya sobre cuerpos finitos dando lugar al llamado "Polynomial Method". Para más referencias sobre los conjuntos de Kakeya sobre cuerpos finitos, véase el trabajo de T. Tao [**Tao, 14**].
El objetivo de nuestro estudio consiste en probar que el resultado de Dvir no es sino una afortunada casualidad: los conjuntos de Kakeya sobre cuerpos finitos no son sino conjuntos cuestores para ciertos constructibles de polinomios de grado acotado.
Dedicamos unos primeros párrafos a presentar algunas propiedades del polinomio de Hilbert. En la Subsección 2.3.2 introducimos nuestra noción de conjunto de Kakeya sobre un cuerpo finito (Definición 8) que generaliza la definición habitual.
Nuestra noción de conjunto de Kakeya comienza fijando una variedad algebraica de puntos en el infinito $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$, donde $\overline{\mathbb{F}}$ es la clausura algebraica del cuerpo finito $\mathbb{F}$. Consideramos seguidamente los puntos $\mathbb{F}$-racionales de V que denotaremos por $V_{\mathbb{F}}$. Un subconjunto $E \subseteq \mathbb{A}^n(\mathbb{F})$ se denomina conjunto de Kakeya con direcciones en $V_{\mathbb{F}}$ si para caa dirección $v \in V_{\mathbb{F}}$ existe una recta $r_v \subseteq E$ con dirección v. La noción clásica de Wolff, Dvir o Tao consiste simplemente en suponer $V = \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ y $V_{\mathbb{F}} = \mathbb{P}_{n-1}(\mathbb{F})$.
Nuestra primera observación es que un conjunto de Kakeya con direcciones en $V_{\mathbb{F}}$ es un conjunto cuestor para $P_d^{\overline{\mathbb{F}}}(X_1, \ldots, X_n)$ con respecto a un constructible propio dependiente solamente de V y d y que denotamos por $\Sigma_d(V_{\mathbb{F}})$ (ver Teorema 2.3.5), con $1 \leq d \leq \sharp(\mathbb{F}) - 1$.
A partir de este resultado, desvelamos la presencia de la función de Hilbert del conjunto de puntos $\mathbb{F}$-racionales $V_{\mathbb{F}}$ de una variedad algebraica proyectiva $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ (Teorema 2.3.6). Posteriormente, estudiaremos el caso de variedades proyectivas irreducibles $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ cuyos puntos $\mathbb{F}$-racionales son altamente densos (ver Definición 10). En ese caso, se prueba que las funciones de Hilbert de V y $V_{\mathbb{F}}$ (χ_V y $\chi_{V_{\mathbb{F}}}$, respectivamente) coinciden por debajo del término de densidad $q^{1-\varepsilon}$ de los puntos $\mathbb{F}$-racionales en la Proposición 2.3.7. A partir de aquí, probamos en el Teorema 2.3.8 una generalización del Teorema de Dvir.
En su trabajo [**Tao, 14**], T. Tao incorpora un resultado clásico de N. Alon, conocido como el Nullstellensatz Combinatorio, a los ejemplos de técnicas conocidas del "Polynomial Method" (cf. [**Al, 99**] para la versión original). El Nullstellensatz Combinatorio de Alon consiste en la detección de conjuntos finitos de puntos $E \subseteq \mathbb{A}^n(\mathbb{F})$ en los que no se anulan ciertos polinomios $P \in \mathbb{F}[X_1, \ldots, X_n]$. En la Sección 2.4, redemostramos el Teorema de Alon en la versión de Tao usando intensamente la dualidad y la traza sobre $\mathbb{F}$-álgebras cero-dimensionales. La primera observación es el Teorema 2.4.3, en el que se prueba lo siguiente:
Sean $P \in \mathbb{F}[X_1, \ldots, X_n]$ un polinomio no nulo y $E \subseteq \mathbb{A}^n(\mathbb{F})$ un conjunto finito de ideal $I(E) \subseteq \mathbb{F}[X_1, \ldots, X_n]$. Si existe un subespacio $W \in I(E)$, con dual (para la traza) W^* (dependiente de una base de W) y $P + I(E)$ admite una descomposición de la forma

$$P + I(E) = P_1 + P_2 + I(E)$$

de tal modo que

i) $P_1 \neq 0$ y $P_1 \in W$, y
ii) $P_2 \perp W^*$,

entonces $P \notin I(E)$ o, equivalentemente, P no se anula idénticamente en E.
En otras palabras, E es un conjunto cuestor para los conjuntos de polinomios $\Omega(W)$ (que satisfacen las propiedades *i)* y *ii)* anteriores) con respecto a $\{0\}$.
A partir de este resultado general, tratamos de encontrar ejemplos, dando una construcción en el Lema 2.4.4. Seguidamente, probamos que la estrategia de T. Tao en [**Tao, 14**] es un caso particular de nuestras condiciones en el Lema 2.4.5. Finalmente, el Nullstellensatz Combinatorio de Alon en [**Al, 99**] surge como caso particular de nuestros análisis en el Corolario 2.4.7.

0.4.3. Capítulo 3. Como ya hemos indicado anteriormente, el principal resultado de [**HeSc, 83**] consiste no solamente en probar la existencia de conjuntos cuestores de longitud sucinta para los tests de nulidad, sino que, además, muestran resultados sobre la densidad de esos conjuntos cuestores en variedades cero-dimensionales de tipo reticular (i.e., $(\{0,1,\ldots,u\}^n)^s$) a través de cotas finas para la probabilidad.
En este Capítulo se introduce una generalización estricta del principal resultado de [**HeSc, 83**]:

- En primer lugar, trabajaremos sobre *variedades de incidencia* $V(\Omega)$ de morfismos regulares que trataremos como "evaluaciones",
$$ev : \Omega \times \mathbb{A}^n(\mathbb{K}) \longrightarrow \mathbb{A}^m(\mathbb{K}) \text{ siendo } V(\Omega) = ev^{-1}(\{0\}).$$
Esto permitirá, por ejemplo, trabajar con listas de ecuaciones polinomiales $f = (f_1,\ldots,f_m) \in K[X_1,\ldots,X_n]^m$ en lugar de trabajar con polinomios individuales como se hace en [**HeSc, 83**].
- En segundo lugar, no nos restringimos solamente a "tests de nulidad" sino que podemos tratar *aspectos de dimensión* en las fibras $\pi_1^{-1}(f)$, con $f \in \Omega$, donde $\pi_1 : V(\Omega) \longrightarrow \Omega$ es la proyección en la primera coordenada. Los "aspectos de dimensión" consisten en considerar un cierto *discriminante* $\Sigma(\Omega) \subseteq \Omega$, formado por aquellos sistemas $f \in \Omega$ tales que la fibra $\pi_1^{-1}(f)$ tiene dimensión estrictamente mayor que la genérica. Esto conduce a la noción de *conjuntos cuestores para Ω con respecto a $\Sigma(\Omega)$*.
- En tercer lugar, nuestros estudios de probabilidad de la elección de conjuntos cuestores no se restringe a variedades de tipo "reticular" como las usadas en [**HeSc, 83**]. De hecho, mostraremos *la existencia de conjuntos cuestores muy probables en variedades cero-dimensionales cualesquiera* con tal de que tengan suficientemente muchos puntos.

Estas variaciones de la noción original permiten el siguiente resultado que extiende el principal resultado de [**HeSc, 83**]:

Teorema Principal 0.4.2. *Sea $ev : \mathbb{A}^N(\mathbb{K})\times\mathbb{A}^n(\mathbb{K}) \longrightarrow \mathbb{A}^m(\mathbb{K})$ una aplicación polinomial K-definible sobre algún subcuerpo K de $\mathbb{K}$, siendo $\mathbb{K}$ algebraicamente cerrado. Sean $W = ev^{-1}(\{0\})$ la variedad de incidencia, $\Omega \subseteq \mathbb{A}^N(\mathbb{K})$ un constructible de clausura Zariski irreducible y sean $\Sigma \subseteq \Omega$ y $r \in \mathbb{N}$ de tal modo que r es la dimensión genérica de la fibra de π_1 sobre puntos de Ω y Σ es una variedad discriminante para la dimensión en Ω (i.e., $\dim(\pi_1^{-1}(\{f\})) > r$ para cada $f \in \Sigma$, mientras que $\dim(\pi_1^{-1}(\{f\})) = r$ para cada $f \in \Omega \setminus \Sigma$), con $\overline{\Sigma}^Z \subsetneq \overline{\Omega}^Z$.*
Sean $s, d \in \mathbb{N}$ dos números enteros que satisfacen las siguientes desigualdades:
$$s \geq 6\dim(\Omega),$$
$$d \geq 2\left(\deg(\Omega)^{1/\dim(\Omega)} \cdot \deg(W)^6\right)^{1/5},$$
Entonces, para cualquier variedad cero-dimensional $V \subseteq \mathbb{A}^n(\mathbb{K})$ dada por ecuaciones de grado a lo sumo d tal que su grado satisface
$$\deg(V) \geq d^{r+1},$$
se verifica la siguiente propiedad:
$$\mathrm{Prob}_{\mathcal{Q}\in V^s}[(f(\underline{x}_i) = 0, 1 \leq i \leq s) \wedge (f \in \Sigma)] \leq \frac{1}{2^{5\dim(\Omega)}},$$
donde la probabilidad en V^s es la dada por la distribución uniforme en este conjunto finito.

Este resultado permite obtener extensiones a varios casos (Corolarios 3.1.4, 3.1.5, 3.1.7 o 3.1.8).
En la Sección 3.2 nos ocupamos de una aplicación estrictamente más general que la expuesta en [**HeSc, 83**]. Se consideran las listas de ecuaciones polinomiales
$$f \in \mathcal{P}_{(d)} := \prod_{i=1}^{m} P_{d_i}(X_1,\ldots,X_n),$$
donde $(d) = (d_1,\ldots,d_m)$. Se considera una representación de las listas $f = (f_1,\ldots,f_m)$ mediante esquemas de evaluación Γ de talla L y profundidad ℓ. Y se considera $\Omega_{(d)}(\Gamma)$ como el constructible formado

por las listas de m ecuaciones $f = (f_1, \ldots, f_m) \in \mathcal{P}_{(d)}$ evaluadas por Γ. Supondremos que las listas $f = (f_1, \ldots, f_m) \in \Omega_{(d)}(\Gamma)$ son genéricamente sucesiones secantes (i.e., $\dim(V_{\mathbb{A}}(f_1, \ldots, f_m) = n - m$ genéricamente en $\Omega_{(d)}(\Gamma)$).
Introducimos así un algoritmo probabilista (el Algoritmo 3.2.5) que, por mera evaluación de los polinomios $f_1, \ldots, f_m$ en $O(L^2)$ puntos, permite decidir si forman o no una sucesión secante. Esto se prueba en el Teorema 3.2.6 donde se concluye que la probabilidad de error del algoritmo verifica

$$\text{Prob[Algoritmo 3.2.5 responde erróneamente]} \leq \frac{1}{2^{\dim(\Omega_{(d)}(\Gamma))}}.$$

El algoritmo así obtenido es un algoritmo de la clase $\mathbf{BPP}_K$, donde K es el cuerpo de coeficientes y el modelo es el modelo de máquinas BSS (o modelos de máquinas Blum-Shub-Smale introducidas en [**BSS, 84**] o en el texto [**BCSS, 98**]). En el caso $m = 1$, el problema de la detección de sucesiones secantes se convierte en el "Test de Nulidad" original de [**HeSc, 83**]. En ese caso, nuestro algoritmo se convierte en un algoritmo de la clase $\mathbf{RP}_K$ (Corolario 3.2.8).
En la Sección 3.3, retomamos el problema de la detección de sucesiones secantes pero desde una perspectiva mucho más amplia. Es claro que el algoritmo de la clase $\mathbf{BPP}_K$ puede resultar insatisfactorio para muchas de sus aplicaciones prácticas, en especial la búsqueda de puntos fuera de conjuntos definibles. Por eso afrontamos el nivel siguiente:

PROBLEMA 4. *¿Existen algoritmos de la clase $\mathbf{RP}_K$ para detectar sucesiones secantes? ¿Y de la clase $\mathbf{ZPP}_K$ admitiendo codificaciones mediante esquemas de evaluación?*

No hemos conseguido responder a estas preguntas en este TFG, ni siquiera mediante las generalizaciones de las técnicas de [**HeSc, 83**] descritas en la Sección 3.2 del Capítulo 3.
Por tanto, hemos intentado un enfoque distinto, muy cercano a la filosofía de las técnicas de aprendizaje estadístico, aunque evitaremos entrar en esa analogía. La primera reflexión es meramente conceptual. Observemos la equivalencia entre los dos conceptos siguientes:

i) Dada una lista de polinomios $f = (f_1, \ldots, f_m)$ y dado un punto $x \in \mathbb{A}^n(\mathbb{K})$, decidir si $x \in V_{\mathbb{A}}(f)$ (o, equivalentemente, decidir si $f_1(x) = \ldots = f_m(x) = 0$).
ii) Dada una lista de polinomios $f = (f_1, \ldots, f_m)$ y dada una variedad afín lineal $L_x \subseteq \mathbb{A}^n(\mathbb{K})$ formada por un sólo punto, $L_x = \{x\}$, decidir si $V_{\mathbb{A}}(f) \cap L_x \neq \emptyset$.

Esta equivalencia conceptual sugiere que transformar la cuestión de saber si un polinomio se anula en un punto es un caso particular del Nullstellensatz (que denotaremos por **HN**, Hilbert's Nullstellensatz). Nos planteamos, por tanto, reemplazar la mera evaluación en un punto por un oráculo capaz de responder a la pregunta siguiente:

> **HN** como oráculo: Dada una sucesión de polinomios $f = (f_1, \ldots, f_m)$ y dada una variedad afín lineal $L \subseteq \mathbb{A}^n(\mathbb{K})$, el oráculo decide si $V_{\mathbb{A}}(f_1, \ldots, f_m) \cap L = \emptyset$ o no.

En estas condiciones, queremos trasladar los Tests de Nulidad de Polinomios por evaluación a la utilización de **HN** como oráculo para el tratamiento de la cuestión dimensional con sucesiones secantes. Para simplificar nuestro análisis, reduciremos la clase de objetos a tratar a variedades algebraicas proyectivas intersección completa $V_{\mathbb{P}}(f_1, \ldots, f_m) \subseteq \mathbb{P}_n(\mathbb{K})$ y variedades lineales $L \subseteq \mathbb{P}_n(\mathbb{K})$ de dimensión apropiada.
Para poder tratar adecuadamente este caso, consideraremos una representación de la variedad de Grassmann $\mathbb{G}_{n,r}$ mediante la clase de matrices $M \in \mathcal{G}_{n,r}$ de rango $n - r$ que definen $V_{\mathbb{P}}(L) \in \mathbb{G}_{n,r}$ como el conjunto de las soluciones proyectivas $x \in \mathbb{P}_n(\mathbb{K})$ del sistema homogéneo $MX = 0$ asociado.
Para trabajar en esta situación, consideramos listas de m polinomios homogéneos $f = (f_1, \ldots, f_m) \in \mathcal{H}^{\mathbb{K}}_{(d)}(X_0, \ldots, X_n)$ donde $(d) = (d_1, \ldots, d_m)$ es una lista de grados y

$$\mathcal{H}^{\mathbb{K}}_{(d)} := \mathcal{H}^{\mathbb{K}}_{(d)}(X_0, \ldots, X_n) = \prod_{i=1}^{m} H^{\mathbb{K}}_{d_i}(X_0, \ldots, X_n).$$

Consideramos así un constructible $\Omega \subseteq \mathcal{H}^{\mathbb{K}}_{(d)}$ formado por listas de polinomios $f = (f_1, \ldots, f_m) \in \mathcal{H}^{\mathbb{K}}_{(d)}$ y un discriminante para la dimensión $\Sigma \subseteq \Omega$ de codimensión mayor o igual que 1 y tales que

i) $\dim(V_{\mathbb{P}}(f)) = n - m, \forall f \in \Omega \setminus \Sigma$,
ii) $\dim(V_{\mathbb{P}}(f)) > n - m, \forall f \in \Sigma$.

Con estas hipótesis, introducimos el conjunto de matrices $\mathcal{G}_{n,m-1} \subseteq \mathcal{H}^{\mathbb{K}}_{(1)}$, donde $(1) = (1, \ldots, 1) \in \mathbb{N}^{n-m+1}$, formado por matrices M con $n - m + 1$ filas y $n + 1$ columnas de rango $n - m + 1$. Nótese que $\mathcal{G}_{n,m-1}$ es el conjunto de las matrices L tales que $\dim(V_{\mathbb{P}}(L)) = m - 1$. Con estas notaciones, estudiamos la variedad de incidencia $V^{(s)}_{\mathcal{G}}(\Omega)$ que generaliza a la descrita en la Sección 3.2. En las Proposiciones 3.3.1 y 3.3.2

analizamos las propiedades necesarias sobre la dimensión de algunas de las componentes irreducibles de $V_{\mathcal{G}}^{(s)}(\Omega)$ y acotamos su grado geométrico.
Una vez resueltas estas propiedades técnicas introducimos la noción de conjunto cuestor módulo **HN** en la Definición 13. Concluimos este TFG con el siguiente Teorema abstracto que generaliza el Teorema 3.1.3 y el Teorema 3.2.6:

Teorema Principal 0.4.3. *Sean Ω y Σ conjuntos constructibles satisfaciendo las hipótesis precedentes. Supongamos $\Omega \subseteq \mathcal{H}_{(d)}^{(m)}$, con $(d) = (d_1, \ldots, d_m)$ y sea*

$$D := \max\{d_1, \ldots, d_m\}.$$

Sean $s, d \in \mathbb{N}$ verificando

$$s \geq 6\dim(\Omega),$$

$$d \geq 2\left(\deg(\Omega)^{1/3\dim(\Omega)}\left(\prod_{i=1}^{m}(d_i+1)2^{n-m+1}\right)^2\right).$$

Sea $N = (n-m+1)(n-1)$. Entonces, para cualquier variedad algebraica cero-dimensional $V \subseteq \mathbb{A}^N(\mathbb{K}) = \mathcal{M}_{(n-m+1)\times(n+1)}(\mathbb{K})$ dada por polinomios de grado a lo sumo d de tal modo que

$$\deg(V) \geq d^{N-1/2},$$

se verifica:

$$\mathrm{Prob}_{(L_1,\ldots,L_s)\in V}[(V_{\mathbb{P}}(f) \cap V_{\mathbb{P}}(L_i) = \emptyset, 1 \leq i \leq s) \wedge (f \notin \Sigma)] \leq \frac{1}{2^{3\dim(\Omega)}},$$

donde la distribución en V^s es la distribución uniforme.

En términos técnicos de Complejidad Computacional, el anterior resultado significa que el problema de la detección de sucesiones secantes homogéneas (SSH) está en la clase de algoritmos en $\mathbf{RP}_K$ con oráculos en **HN**, esto es

$$\mathrm{SSH} \in \mathbf{RP}_K^{\mathbf{HN}}.$$

Pero dado que **HN** es $\mathbf{NP}_K$-completo (en el modelo de máquina BSS), el resultado es insuficiente para disponer de un algoritmo en $\mathbf{RP}_K$. Quedará como investigación posterior a este TFG la explotación de este resultado para el diseño de algoritmos eficientes.

0.5. Sobre el estilo y la ortografía usados en este TFG

En algún caso precedente se ha discutido el estilo y la ortografía de las memorias presentadas como Trabajo de Fin de Grado en Matemáticas. En evitación de intervenciones innecesarias, queremos clarificar algunos aspectos relativos al estilo elegido en este texto.
Se ha elegido el formato de libro (book) de la *American Mathematical Society (AMS)*. Aunque el idioma utilizado es el español, hemos tratado de seguir lo más fielmente posible las recomendaciones del Libro de Estilo de esta asociación[1], juntamente con las reglas de estilo recomendadas por D. E. Knuth y co-autores para la *Mathematical Asociation of America (MAA)*[2].
Específicamente, hemos tratado de seguir atentamente las siguientes dos reglas:

- *"Numbered theorems, lemmas, etc. are proper nouns and, thus, are capitalized: Theorem 2.3, Lemma 3.1, Figure 4.5"* (p. 79 del *AMS Style Guide*).
- *"Rule 19. Capitalize names like Theorem 1, Lemma 2, Algorithm 3, Method 4"* (en D. E. Knuth *et al.*).

[1] M. Letourneau, J. Wright Sharp, *AMS Style Guide, Journals, October 2017*, AMS, Providence, 2017
[2] D. E. Knuth, T. Larrabee, P. M. Roberts, *Mathematical Writing*, MAA, 1989

CAPÍTULO 1

Desigualdad de Bézout geométrica para constructibles: una prueba completa

Índice

1.1. Introducción

A pesar de lo común del término y del uso del nombre de Bézout, la desigualdad de Bézout es un resultado matemático relativamente reciente: las primeras demostraciones vienen de la primera mitad de los años 80 del pasado siglo. Tres demostraciones simultáneas, diferentes y obtenidas independientemente son publicadas entre los años 1981 y 1983. Aquí seguiremos inicialmente la desigualdad de Bézout introducida por J. Heintz en [**He, 83**]: trata del grado geométrico de variedades algebraicas afines. Alternativamente, W. Vogel introduce su desigualdad de Bézout en [**Vo, 84**] para variedades algebraicas proyectivas, definiendo el grado a partir del coeficiente director del polinomio de Hilbert de la variedad y probando el significado geométrico de su definición de grado a partir de la regularidad de la función de Hilbert. La tercera de las demostraciones es debida a W. Fulton en [**Fu, 83**]: este autor usa la teoría de divisores para enfrentar una noción de grado que tiene en cuenta multiplicidades y probar una igualdad de Bézout.
Empezaremos este primer Capítulo recogiendo una serie de definiciones, notaciones y resultados básicos de la Geometría Algebraica.

1.2. Notaciones y términos básicos

En lo que sigue K será un cuerpo y denotaremos por $\mathbb{K}$ su clausura algebraica. Salvo cuando los distingamos expresamente, supondremos $K = \mathbb{K}$, esto es, que K es algebraicamente cerrado.
Dados enteros $d, n \in \mathbb{N}$, denotaremos por $H_d^K(X_0, \ldots, X_n)$ y $P_d^K(X_1, \ldots, X_n)$ a los espacios vectoriales sobre K formados, respectivamente, por los polinomios homogéneos de grado d en las variables $\{X_0, \ldots, X_n\}$ y por los polinomios en las variables $\{X_1, \ldots, X_n\}$ de grado acotado por d. Omitiremos los superíndices K cuando no haya lugar a confusión. Denotaremos por $K[Y_1, \ldots, Y_n]$ al anillo de polinomios en el conjunto de las variables $\{Y_1, \ldots, Y_n\}$ con coeficientes en el cuerpo K. Recordemos la descomposición en componentes homogéneas dada por

$$K[Y_1, \ldots, Y_n] = \bigoplus_{d \in \mathbb{N}} H_d^K(Y_1, \ldots, Y_n). \tag{1.2.1}$$

Obsérvese que $H_d^K(X_0, \ldots, X_n)$ es un K-espacio vectorial de dimensión finita sobre K. Su dimensión es una cantidad conocida que denotaremos mediante

$$N_d := \dim_K(H_d^K(X_0, \ldots, X_n) = \begin{pmatrix} d+n \\ n \end{pmatrix}. \tag{1.2.2}$$

Dado un polinomio $f \in K[X_0, \ldots, X_n]$, la descomposición (1.2.1) nos permite escribir f como una suma finita única

$$f = f_d + \ldots, + f_m,$$

con $m \leq d$, donde $f_i \in H_i(X_0, \ldots, X_n), 0 \leq m \leq i \leq d$. Esta escritura se denomina descomposición de f en componentes homogéneas y a cada f_i se le denomina *componente homogénea de grado* i.

En lo que respecta a $P_d^K(X_1,\ldots,X_n)$, podemos observar que también tiene la dimensión N_d como K-espacio vectorial. Una forma natural de observarlo pasa por el proceso de homogeneización de polinomios afines hasta un cierto grado fijado a priori. Así, sea $f \in K[X_1,\ldots,X_n]$ un polinomio y consideremos su descomposición en componentes homogéneas

$$f = f_0 + f_1 + \ldots + f_r$$

con $r = \deg(f)$ (i.e., $f_r \neq 0$) y $f_i \in H_i(X_1,\ldots,X_n)$. Llamamos polinomio homogeneizado de f (con respecto a una nueva variable X_0) al polinomio homogéneo

$${}^h f := X_0^r f_0 + X_0^{r-1} f_1 + \ldots + f_r \in H_r(X_0,\ldots,X_n).$$

Llamaremos homogeneizado hasta grado d de f al polinomio

$${}^H f := X_0^{d-\deg(f)h} f \in H_d(X_0,\ldots,X_n).$$

Tenemos así un isomorfismo natural entre espacios vectoriales

$$\begin{array}{ccc} P_d^K(X_1,\ldots,X_n) & \longrightarrow & H_d^K(X_1,\ldots,X_n) \\ f & \longmapsto & X_0^{d-\deg(f)h} f \in H_d(X_0,\ldots,X_n). \end{array}$$

Denotaremos por $\mathbb{A}^n(K)$ (o simplemente K^n) al *espacio afín de dimensión n sobre el cuerpo K* y por $\mathbb{P}_n(K)$ al *espacio proyectivo* con coordenadas homogéneas en el mismo cuerpo. Siguiendo la tradición francesa, las coordenadas homogéneas de un punto proyectivo $x \in \mathbb{P}_n(K)$ se denotarán, al modo clásico, mediante $x = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}_n(K)$.

Una *variedad algebraica* (o conjunto algebraico) *afín* será un subconjunto $V \subseteq \mathbb{A}^n(\mathbb{K})$ dado como el conjunto de ceros comunes a una familia finita de polinomios. Esto es, $V \subseteq \mathbb{A}^n(\mathbb{K})$ es una variedad algebraica si y solamente si existen polinomios $f_1,\ldots,f_s \in K[X_1,\ldots,X_n]$ tales que

$$V = V_{\mathbb{A}}(f_1,\ldots,f_s) = \{x \in \mathbb{A}^n(\mathbb{K}) : f_1(x) = \ldots = f_s(x) = 0\}.$$

Si K no es un cuerpo algebraicamente cerrado, diremos que V es *K-definible*. El Teorema de la Base de Hilbert ($K[X_1,\ldots,X_n]$ es un anillo noetheriano) nos permite garantizar que una variedad algebraica es, de hecho, el conjunto de ceros comunes a un ideal de $K[X_1,\ldots,X_n]$. Es decir, dado $\mathfrak{a} \subseteq K[X_1,\ldots,X_n]$, el siguiente conjunto es una variedad algebraica afín:

$$V_{\mathbb{A}}(\mathfrak{a}) := \{x \in \mathbb{A}^n(\mathbb{K}) : f(x) = 0, \forall f \in \mathfrak{a}\}.$$

De hecho, si $\{f_1,\ldots,f_s\}$ es un conjunto finito de generadores de $\mathfrak{a}$, se tiene que

$$V_{\mathbb{A}}(\mathfrak{a}) = V_{\mathbb{A}}(f_1,\ldots,f_s).$$

Aunque los polinomios homogéneos no definen propiamente funciones sobre el espacio proyectivo, sí es posible analizar el conjunto de los ceros proyectivos de un polinomio homogéneo. Así, dado $f \in H_d(X_0,\ldots,X_n)$ y dado un punto $x = (x_0,\ldots,x_n) \in K^{n+1} \setminus \{0\}$ tendremos que $\forall \lambda \in K \setminus \{0\}$ se satisface que

$$f(\lambda x) = \lambda^d f(x),$$

por cuanto tiene sentido considerar para cada polinomio homogéneo $f \in H_d(X_0,\ldots,X_n)$ el siguiente conjunto de puntos proyectivos:

$$V_{\mathbb{P}}(f) := \{x = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}_n(\mathbb{K}) : f(x_0,\ldots,x_n) = 0\}.$$

Definiremos *variedad algebraica proyectiva* a todo subconjunto $V \subseteq \mathbb{P}_n(\mathbb{K})$ tal que existe una familia finita de polinomios homogéneos $\{f_1,\ldots,f_s\} \subseteq K[X_0,\ldots,X_n]$, no todos del mismo grado, tales que

$$V = V_{\mathbb{P}}(f_1,\ldots,f_s) = \{x \in \mathbb{P}_n(\mathbb{K}) : f_1(x) = \ldots, f_n(x) = 0\}.$$

Haciendo otra vez la distinción entre K y $\mathbb{K}$, llamaremos a V *variedad proyectiva K-definible*.

Un *ideal* $\mathfrak{a} \subseteq K[X_0,\ldots,X_n]$ se dice *homogéneo* si satisface

$$\mathfrak{a} = \bigoplus_{d\in\mathbb{N}} (\mathfrak{a} \cap H_d(X_0,\ldots,X_n)).$$

Se puede probar fácilmente que un ideal $\mathfrak{a} \subseteq K[X_0,\ldots,X_n]$ es homogéneo si y solamente si, para cada polinomio $f \in \mathfrak{a}$, todas las componentes homogéneas de f están en $\mathfrak{a}$. En particular, un ideal $\mathfrak{a}$ de $K[X_0,\ldots,X_n]$ es homogéneo si y sólamente si está generado por una familia finita de polinomios homogéneos, i.e., $\mathfrak{a} \subseteq K[X_0,\ldots,X_n]$ es homogéneo si y solamente si existen $f_1,\ldots,f_s \in K[X_0,\ldots,X_n]$, no todos del mismo grado, tales que

$$\mathfrak{a} = (f_1,\ldots,f_s).$$

Esto permite definir la variedad algebraica proyectiva definida por un ideal homogéneo $\mathfrak{a} \subseteq K[X_0, \ldots, X_n]$ mediante el abuso de notación

$$V_{\mathbb{P}}(\mathfrak{a}) := \{x \in \mathbb{P}_n(\mathbb{K}) : f(x) = 0, \forall f \in \mathfrak{a}\}.$$

Es sencillo verificar que las variedades algebraicas afines y proyectivas definen una única topología respectivamente en $\mathbb{A}^n(\mathbb{K})$ y $\mathbb{P}_n(\mathbb{K})$: estas topologías se denominan *topologías de Zariski*. Los cerrados en la topología de Zariski de $\mathbb{A}^n(\mathbb{K})$ son las variedades algebraicas afines y los cerrados en la topología de Zariski de $\mathbb{P}_n(\mathbb{K})$ son las variedades algebraicas proyectivas. Por ser ambas topologías, dado $S \subseteq \mathbb{A}^n(\mathbb{K})$ (resp. $T \subseteq \mathbb{P}_n(\mathbb{K})$), podemos hablar de la *clausura Zariski* de S (resp. de T) como el menor cerrado de la topología de Zariski de $\mathbb{A}^n(\mathbb{K})$ (resp. de $\mathbb{P}_n(\mathbb{K})$) que contiene a S (resp. a T). Denotaremos mediante $\overline{S}^Z$ (resp. $\overline{T}^Z$) a esa clausura Zariski.

Un tipo de conjuntos especialmente interesantes en la topología de Zariski son los objetos definibles mediante fórmulas de primer orden libres de cuantificadores de la teoría de cuerpos: *los conjuntos constructibles*. Un subconjunto $C \subseteq X$ (siendo $X = \mathbb{A}^n(\mathbb{K})$ o $X = \mathbb{P}_n(\mathbb{K})$) se dice *localmente cerrado* si es la intersección de un abierto y un cerrado en la correspondiente topología de Zariski.

En el caso afín, un subconjunto $C \subseteq \mathbb{A}^n(\mathbb{K})$ se dice constructible si es una unión finita de subconjuntos localmente cerrados. En el caso proyectivo, los subconjuntos localmente cerrados $C \subseteq \mathbb{P}_n(\mathbb{K})$ se denominan *variedades quasi-proyectivas*. Nótese que con la inclusión natural

$$(x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbb{K}) \hookrightarrow (1 : x_1 : \ldots : x_n) \in \mathbb{P}_n(\mathbb{K}),$$

las variedades algebraicas afines $V \subseteq \mathbb{A}^n(\mathbb{K})$ son variedades quasi-proyectivas en $\mathbb{P}_n(\mathbb{K})$:

$$V = \overline{V}^Z \cap \{x \in \mathbb{P}_n(\mathbb{K}) : x_0 \neq 0\},$$

siendo $\overline{V}^Z$ la clausura Zariski de V en $\mathbb{P}_n(\mathbb{K})$. En ocasiones, para distinguir las topologías de Zariski afín y proyectiva, para $V \subseteq \mathbb{A}^n(\mathbb{K})$, denotaremos por $\overline{V}^{\mathbb{P}}$ a su clausura Zariski en $\mathbb{P}_n(\mathbb{K})$.

El interés de los conjuntos constructibles en nuestra discusión nace de los teoremas clásicos de Teoría de la Eliminación (de cuantificadores).

Una *función polinomial* sobre un cerrado Zariski afín $V \subseteq \mathbb{A}^n(\mathbb{K})$ será una aplicación $\varphi : V \longrightarrow \mathbb{K}$ tal que existe un polinomio $f \in K[X_1, \ldots, X_n]$ tal que

$$\varphi(x) = f(x), \forall x \in V.$$

El conjunto de las aplicaciones polinomiales sobre $V \subseteq \mathbb{A}^n(\mathbb{K})$ forma una K-álgebra (anillo conmutativo con unidad que contiene a K) con las operaciones naturales de suma y producto de aplicaciones. Denotaremos por $K[V]$ a este anillo. En ocasiones, llamaremos *función regular* a todo elemento de $K[V]$.

Una aplicación polinomial entre dos variedades afines $V \subseteq \mathbb{A}^n(\mathbb{K}), W \subseteq \mathbb{A}^m(\mathbb{K})$ es cualquier aplicación $\varphi : V \longrightarrow W$ tal que existen polinomios $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ tales que

$$\varphi(x) = (f_1(x), \ldots, f_m(x)), \forall x \in V.$$

Se dice K-definible cuando distinguimos K y $\mathbb{K}$. En ocasiones diremos que φ es un *morfismo regular*.

Los constructibles surgen de manera natural por el siguiente resultado clásico:

Teorema 1.2.1. *Sean K un cuerpo, $\mathbb{K}$ su clausura algebraica y $\varphi : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ una aplicación polinomial. Sea $C \subseteq \mathbb{K}^n$ un constructible, entonces $\varphi(C)$ también es constructible. Más aún, si C es K-definible y φ es K-definible, entonces $\varphi(C)$ es K-definible.*

En particular, las imágenes de variedades algebraicas afines por aplicaciones polinomiales son constructibles. Es sencillo demostrar que la noción es necesaria en el caso afín: dadas la curva $V = \{(x, y) \in \mathbb{K}^2 : xy - 1 = 0\}$ y la proyección natural $\pi : \mathbb{K}^2 \longrightarrow \mathbb{K}, \pi(x, y) = x, \forall (x, y) \in \mathbb{K}^2$, se observa que $\pi(V) \subseteq \mathbb{K}$ no es variedad algebraica sino un constructible $\pi(V) = \{x \in \mathbb{K} : x \neq 0\}$ (de hecho, es un abierto Zariski).

En el caso proyectivo, no son necesarios los constructibles porque las variedades proyectivas son completas, aunque evitaremos entrar en ese aspecto clásico de la Teoría de la Eliminación.

Otro resultado esencial en la Geometría Algebraica, de gran influencia conceptual, es el Nullstellensatz de Hilbert. A través de él, los objetos geométricos (cerrados Zariski) se identifican con cierto tipo de ideales (ideales radicales) hasta generar una equivalencia natural entre los espacios topológicos sobre las variedades algebraicas afines y las K-álgebras reducidas (sin elementos nilpotentes) finitamente generadas. Resumiremos aquí parte de esa identificación.

Sea $S \subseteq \mathbb{A}^n(\mathbb{K})$ un subconjunto, denotemos por $I_{\mathbb{A}}(S) \subseteq K[X_1, \ldots, X_n]$ el ideal dado mediante

$$I_{\mathbb{A}}(S) := \{f \in K[X_1, \ldots, X_n] : f(x) = 0, \forall x \in S\}.$$

Es fácil observar que $I_{\mathbb{A}}(S)$ ayuda a determinar la clausura Zariski de S puesto que se tiene

$$\overline{S}^Z = V_{\mathbb{A}}(I_{\mathbb{A}}(S)).$$

Recordemos que para un ideal $\mathfrak{a}$ en un anillo R, se denomina *radical* al ideal formado por todos los elementos nilpotentes módulo $\mathfrak{a}$:

$$\sqrt{\mathfrak{a}} := \{f \in R : \exists m \in \mathbb{N}, f^m \in \mathfrak{a}\}.$$

Un *ideal se dice radical* si coincide con su radical (i.e., $\mathfrak{a} = \sqrt{\mathfrak{a}}$) y un anillo R se dice *reducido* si el ideal (0) es radical. Clásicamente se observa, asumiendo el Axioma de Zorn, que el radical de un ideal es la intersección de todos los ideales primos que contienen al ideal, i.e.,

$$\sqrt{a} = \bigcap\{\mathfrak{p} \in Spec(R) : \mathfrak{p} \supseteq \mathfrak{a}\}.$$

El Nullstellensatz de Hilbert[1] (que es simultáneamente debido a L. Kronecker[2], aunque este nombre se pierde, y a Netto[3], a veces reconocido) es el siguiente enunciado descrito en la versión de Rabinowitz[4]:

Teorema 1.2.2 (Nullstellensatz). *Si K es un cuerpo algebraicamente cerrado, para cada ideal $\mathfrak{a}$ de $K[X_1, \ldots, X_n]$ se tiene que*

$$I_{\mathbb{A}}(V_{\mathbb{A}}(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

El resultado es análogamente cierto en el caso proyectivo. Así, dado $S \subseteq \mathbb{P}_n(\mathbb{K})$, definimos

$$I_{\mathbb{P}}(S) := (\{f \in K[X_0, \ldots, X_n] : f \text{ homogéneo}, f(x) = 0, \forall x \in S\}). \tag{1.2.3}$$

Nótese que los paréntesis $(\cdots)$ indican "ideal generado por". Al ser un ideal generado por polinomios homogéneos, se trata de un ideal homogéneo de $K[X_0, \ldots, X_n]$. Se tiene, además, que el radical de un ideal homogéneo es homogéneo y que

$$\sqrt{a} = \bigcap\{\mathfrak{p} \in Spec(R) : \mathfrak{p} \text{ homogéneo }, \mathfrak{p} \supseteq \mathfrak{a}\}.$$

Asimismo, es fácil demostrar que la clausura Zariski de $S \subseteq \mathbb{P}_n(\mathbb{K})$ viene dada por

$$\overline{S}^Z = V_{\mathbb{P}}(I_{\mathbb{P}}(S)).$$

El Nullstellensatz proyectivo resulta ser

Teorema 1.2.3 (Nullstellensatz Proyectivo). *Si K es un cuerpo algebraicamente cerrado, para cada ideal homogéneo $\mathfrak{a}$ de $K[X_0, \ldots, X_n]$ se tiene que*

$$I_{\mathbb{P}}(V_{\mathbb{P}}(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

Ambos resultados, expresados de forma combinada, dicen que podemos identificar las variedades algebraicas afines (resp. variedades algebraicas proyectivas) con los ideales radicales de $K[X_1, \ldots, X_n]$ (resp. ideales homogéneos radicales de $K[X_0, \ldots, X_n]$) y que esa identificación se hace a través de las biyecciones $V_{\mathbb{A}}$ e $I_{\mathbb{A}} = V_{\mathbb{A}}^{-1}$ (resp. $V_{\mathbb{P}}$ e $I_{\mathbb{P}} = V_{\mathbb{P}}^{-1}$).
Un tipo de variedades especialmente importantes en Geometría Algebraica son las *irreducibles*. Si $(X, \mathscr{T})$ es un espacio topológico, un cerrado $F \subseteq X$ se dice *reducible* si existen dos cerrados $F_1, F_2 \subseteq X$ tales que

$$F = F_1 \cup F_2, \quad \text{siendo } F_i \neq F,\ i = 1, 2.$$

Un cerrado se dice irreducible si no es reducible. Es fácil observar la siguiente

Proposición 1.2.4. *Con las notaciones precedentes:*

i) Un cerrado Zariski $V \subseteq \mathbb{A}^n(\mathbb{K})$ es irreducible si y solamente si el ideal $I_{\mathbb{A}}(V) \subseteq K[X_1, \ldots, X_n]$ es un ideal primo (i.e., $I_{\mathbb{A}}(V) \in Spec(K[X_1, \ldots, X_n])$). Más aún, si K es algebraicamente cerrado, $I_{\mathbb{A}}$ define una biyección entre los cerrados irreducibles afines y los ideales primos de $K[X_1, \ldots, X_n]$.

ii) Un cerrado Zariski $V \subseteq \mathbb{P}_n(\mathbb{K})$ es irreducible si y solamente si el ideal $I_{\mathbb{P}}(V) \subseteq K[X_0, \ldots, X_n]$ es un ideal homogéneo y primo. Más aún, si K es algebraicamente cerrado, $I_{\mathbb{P}}$ define una biyección entre los irreducibles proyectivos y los ideales primos homogéneos de $K[X_0, \ldots, X_n]$.

---

[1] D. Hilbert, *Über die vollen Invariantensysteme.* Mathematische Annalen **42** (1893), 313-373.

[2] L. Kronecker, *Grundzüge einer arithmetischen Theorie de algebraischen Grössen.* J. reine angew. Math. **92** (1882), 1-122.

[3] E. Netto, *Zur Theorie der Elimination*, Acta Mathematica **7**(1) (1885), 101-104

[4] G. Y. Rainich, (pseudónimo J. L. Rabinowitz), *Zum Hilbertschen Nullstellensatz.* Math. Ann. **102** (1929), 520.

La *condición noetheriana* en un espacio topológico $(X, \mathscr{T})$ es la condición de cadena descendente para cerrados. Un *espacio topológico* $(X, \mathscr{T})$ *se dice noetheriano* si para cualquier cadena numerable descendente de cerrados

$$C_1 \supseteq C_2 \supseteq \ldots \supseteq C_n \supseteq \ldots$$

existe un término $C_m, m \in \mathbb{N}$ a partir del cual la cadena se estabiliza ($C_n = C_m, \forall n \geq m$). El Teorema de la Base de Hilbert nos permite concluir fácilmente que las topologías de Zariski en $\mathbb{A}^n(\mathbb{K})$ y $\mathbb{P}_n(\mathbb{K})$ son noetherianas. Más aún, si se asume el Axioma de Elección Dependiente, se tiene:

PROPOSICIÓN 1.2.5 (Existencia de Descomposición en Irreducibles). *Si $(X, \mathscr{T})$ es un espacio topológico noetheriano, todo cerrado $C \subseteq X$ admite una descomposición minimal como unión finita de irreducibles:*

$$C = C_1 \cup \ldots \cup C_r.$$

Además, esa descomposición minimal es única y los cerrados irreducibles $C_1, \ldots, C_r$ se denominan componentes irreducibles de C.

El famoso Teorema de Lasker-Noether (cf. [**AtMc, 96**]) sobre descomposición primaria de ideales en anillos noetherianos nos permite identificar descomposiciones irreducibles con ideales primos minimales. Escribimos la versión en el caso algebraicamente cerrado.

PROPOSICIÓN 1.2.6. *Si K es un cuerpo algebraicamente cerrado y $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ es un ideal propio, existe una biyección entre las componentes irreducibles de $V_{\mathbb{A}}(\mathfrak{a})$ y los ideales primos de $K[X_1, \ldots, X_n]$ minimales entre los que contienen al ideal $\mathfrak{a}$.*

Un resultado análogo se sigue en el caso proyectivo, simplemente añadiendo el adjetivo "homogéneo" apropiadamente.
En el caso de variedades irreducibles es especialmente útil manejar las *funciones racionales*. Así, dada $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible, una función racional sobre V es una aplicación parcialmente definida en V

$$\varphi : D(\varphi) \subseteq V \longrightarrow \mathbb{K}$$

tal que existen dos polinomios $f, g \in K[X_1, \ldots, X_n]$ verificándose

$$\forall x \in D(\varphi), g(x) \neq 0,\ \varphi(x) = \frac{f(x)}{g(x)}.$$

Denotamos por $K(V)$ al conjunto de las funciones racionales sobre V, que es un cuerpo con las operaciones naturales de suma y producto.
En el caso proyectivo, la noción de función racional se define de manera análoga salvo que supondremos "dos polinomios homogéneos del mismo grado $f, g \in K[X_0, \ldots, X_n]$" para que tenga sentido definir el cociente $f(x)/g(x)$ en términos de coordenadas homogéneas. También en el caso proyectivo $K(V)$ es un cuerpo con las operaciones naturales de suma y producto parcialmente definidas en V.
Nótese que si $V \subseteq \mathbb{A}^n(\mathbb{K})$ es una variedad algebraica afín, el anillo de funciones polinomiales sobre V viene dado como el cociente

$$K[V] = K[X_1, \ldots, X_n] \Big/ I_{\mathbb{A}}(V).$$

En el caso particular de que $V \subseteq \mathbb{A}^n(\mathbb{K})$ sea irreducible, el anillo $K[V]$ es un dominio de integridad (equivalente a que $I_{\mathbb{A}}(V)$ es primo) y el cuerpo de funciones racionales sobre V será el cuerpo de fracciones de $K[V]$, i.e.,

$$K(V) = q.f.(K[V]).$$

Resumamos brevemente algunas de las ideas que subyacen a la equivalencia natural entre variedades algebraicas y K-álgebras reducidas finitamente generadas cuando K es algebraicamente cerrado. Así, dado un morfismo regular $\varphi : V \longrightarrow W$ entre dos variedades algebraicas afines, tendremos un morfismo de K-álgebras

$$\begin{array}{rccl} \varphi^* & : K[W] & \longrightarrow & K[V] \\ & h & \longmapsto & h \circ \varphi \quad : V \longrightarrow K. \end{array}$$

Son especialmente interesantes en este manuscrito los términos siguientes:

i) El morfismo φ se dice *dominante* si $\varphi(V)$ es denso en W (esto es, si $\overline{\varphi(V)}^Z = W$. Es sencillo verificar que φ es dominante si y solamente si φ^* es un monomorfismo de K-álgebras.

ii) Para cada subvariedad algebraica $T \subseteq W$, llamaremos *fibra de φ sobre T* a la subvariedad algebraica $\varphi^{-1}(T) \subseteq \mathbb{A}^n(\mathbb{K})$. Igualmente usaremos la expresión "fibra" si T es constructible. Nótese que un morfismo es dominante si y solamente si el conjunto de puntos de fibra no vacía es denso en W, i.e.,

$$\overline{\{x \in W : \varphi^{-1}(\{x\}) \neq \emptyset\}}^{Z} = W.$$

iii) Decimos que V y W son *birregularmente isomorfos* si existen morfismos regulares $\varphi : V \longrightarrow W, \psi : W \longrightarrow V$ tales que ambos son biyecciones y $\varphi = \psi^{-1}$. Dos variedades algebraicas afines V y W son birregularmente isomorfas si y solamente si sus K-álgebras $K[V]$ y $K[W]$ son isomorfas (como K-álgebras).

Aunque en el caso de una variedad algebraica proyectiva $V \subseteq \mathbb{P}_n(\mathbb{K})$ el anillo graduado

$$K[V] := K[X_1, \ldots, X_n] \Big/ I_{\mathbb{P}}(V)$$

es una herramienta poderosamente rica en información (sobre todo a través del polinomio de Hilbert, del que hablaremos en el Capítulo 2 en un caso particular) se tiende más a usar los isomorfismos birracionales para identificar variedades proyectivas. Sean $V \subseteq \mathbb{P}_n(\mathbb{K}), W \subseteq \mathbb{P}_m(\mathbb{K})$ dos variedades quasi-proyectivas. Diremos que son *birracionalmente isomorfas* si $K(V)$ y $K(W)$ son dos cuerpos isomorfos como extensiones del cuerpo K.
Se define para las variedades algebraicas una noción de *dimensión* que será esencial en este manuscrito. En el Apéndice A aparece la definición de esta noción, así como una serie de definiciones y resultados que utilizaremos durante las siguientes páginas.

1.3. Grado de una variedad algebraica

Como hemos indicado, seguiremos principalmente las ideas de J. Heintz. El siguiente resultado es esencial para la definición de grado de una variedad algebraica y aparece en [**He, 83**]. Omitiremos su prueba.

PROPOSICIÓN 1.3.1 ([**He, 83**], Prop. 1). *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado, $W \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica afín e irreducible de dimensión m. Sea $\varphi = (f_1, \ldots, f_m) : W \to \mathbb{A}^m(\mathbb{K})$ una aplicación polinomial dominante. Entonces, la extensión de cuerpos $\mathbb{K}(\mathbb{A}^m(\mathbb{K})) \subset \mathbb{K}(W)$ es finita. Supongamos que la extensión de cuerpos es separable. Entonces,*

i) Para cada $y \in W$ tal que la fibra $\varphi^{-1}(\{y\})$ es una variedad cero-dimensional, se verifica que

$$\sharp\left(\varphi^{-1}(\{y\})\right) \leq [\mathbb{K}(W) : \mathbb{K}(\mathbb{A}^m(\mathbb{K}))]$$

ii) Además, existe un abierto Zariski $U \subseteq \mathbb{A}^n(\mathbb{K})$ tal que $\forall y \in U$ se tiene

$$\sharp\left(\varphi^{-1}(\{y\})\right) = [\mathbb{K}(W) : \mathbb{K}(\mathbb{A}^m(\mathbb{K}))]$$

En [**He, 83**] se exhibe una demostración esencialmente auto-contenida, se indica otra posible demostración usando el Zariski Main Theorem y una última prueba es indicada usando anillos de valoración. También se observa que el resultado es igualmente cierto si $\mathbb{A}^m(\mathbb{K})$ es reemplazado por una variedad lisa e irreducible. Para transformar el resultado anterior en un análisis de la intersección con variedades afines lineales, el ingrediente principal es el siguiente morfismo. Dada $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible de dimensión m, consideremos el siguiente morfismo regular:

$$\begin{array}{rccc} \varphi : & V \times \mathcal{M}_{m\times n}(\mathbb{K}) & \longrightarrow & \mathbb{A}^m(\mathbb{K}) \times \mathcal{M}_{m\times n}(\mathbb{K}) \\ & (\underline{x}, M) & \longmapsto & (M \cdot \underline{x}, M) \end{array}$$

El siguiente resultado se prueba en [**He, 83**]:

PROPOSICIÓN 1.3.2. *El morfismo φ es un morfismo dominante entre variedades algebraicas de la misma dimensión. Además, se tiene que la siguiente extensión de cuerpos es finita y separable:*

$$\mathbb{K}(\mathbb{A}^m(\mathbb{K}) \times \mathcal{M}_{m\times n}(\mathbb{K})) \subseteq \mathbb{K}(V \times \mathcal{M}_{m\times n}(\mathbb{K}))$$

Seguidamente haremos intervenir de forma explícita lo que de forma implícita aparece en [**He, 83**]: la presencia del Lema de Normalización de Noether y de los Teoremas de Krull-Cohen-Seidenberg.

PROPOSICIÓN 1.3.3. *Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible de dimensión m. Entonces, existe un abierto Zariski $U \subseteq \mathcal{M}_{m\times n}(\mathbb{K})$ de matrices tales que se verifican las siguientes propiedades:*

i) [NOETHER] *Para cada matriz $M \in U$, las formas lineales*

$$\begin{pmatrix} L_1(X_1,\ldots,X_n) \\ \vdots \\ L_m(X_1,\ldots,X_n) \end{pmatrix} = M \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

satisfacen lo siguiente:
Sean $\ell_i := L_i + I(V), 1 \leq i \leq m$, las clases definidas en $\mathbb{K}[V]$ por las formas lineales $L_1,\ldots,L_m$. Entonces, $\{\ell_1,\ldots,\ell_m\}$ son algebraicamente independientes sobre $\mathbb{K}$ y la siguiente es una extensión entera de álgebras de tipo finito sobre $\mathbb{K}$,

$$\mathbb{K}[\ell_1,...,\ell_m] \subseteq \mathbb{K}[V].$$

En particular, $\mathbb{K}[V]$ es un $\mathbb{K}[\ell_1,\ldots,\ell_m]-$módulo finitamente generado.

ii) [KRULL-COHEN-SEIDENBERG] *El morfismo siguiente es suprayectivo:*

$$\begin{array}{rccc} \Lambda: & V & \longrightarrow & \mathbb{A}^m(\mathbb{K}) \\ & \underline{x} & \longmapsto & (L_1(\underline{x}),\ldots,L_m(\underline{x})) \end{array}$$

Además, las fibras serán finitas y de cardinal acotado. Es decir, para cada $\underline{y} \in \mathbb{A}^m(\mathbb{K})$, la fibra $\Lambda^{-1}(\{\underline{y}\})$ es una variedad algebraica cero-dimensional y se verifica:

$$\sharp\left(\Lambda^{-1}(\{\underline{y}\})\right) \leq [\mathbb{K}(V\times\mathcal{M}_{m\times n}(\mathbb{K})) : \mathbb{K}(\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K}))]$$

Más aún, existe un abierto Zariski $O \subseteq \mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K})$ tal que para cada $(\underline{y}, M) \in O$ se verifican i) y ii) y, además, se tiene

$$\sharp\left(\Lambda^{-1}(\{\underline{y}\})\right) = [\mathbb{K}(V\times\mathcal{M}_{m\times n}(\mathbb{K})) : \mathbb{K}(\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K}))]$$

El conjunto de proposiciones precedentes permite definir la noción de grado de una variedad algebraica afín al estilo de [**He, 83**].

DEFINICIÓN 2. *Dada $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible de dimensión m, llamaremos* grado (geométrico) de la variedad V *al siguiente número entero positivo asociado a V:*

$$\begin{aligned} \deg(V) :=& [\mathbb{K}(V\times\mathcal{M}_{m\times n}(\mathbb{K})) : \mathbb{K}(\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K}))] \\ =& \max\{\sharp(V\cap L) : L \text{ es variedad afín lineal de codimensión } m \text{ tal que } \sharp(V\cap L) < +\infty\} \end{aligned}$$

Nótese que identificando $\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K})$ con el conjunto $\mathscr{L}_{m,n}$ de variedades afines lineales de codimensión m, existe un abierto Zariski $O \subseteq \mathscr{L}_{m,n}$ tal que para cada $L \in O$ se verifica

$$\sharp(V\cap L) = \deg(V).$$

Para variedades algebraicas en general definimos el grado mediante:

DEFINICIÓN 3. *Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica y sea $V = W_1 \cup \ldots \cup W_s$ su descomposición en componentes irreducibles. Definimos el* grado de V *como*

$$\deg(V) := \sum_{i=1}^{s} \deg(W_i).$$

También podemos definir grado para los conjuntos constructibles localmente cerrados irreducibles del modo siguiente:

DEFINICIÓN 4. *Sea $C \subseteq \mathbb{A}^n(\mathbb{K})$ un abierto Zariski no vacío en una variedad algebraica irreducible. Definimos el* grado geométrico de C *como*

$$\deg(C) := \max\{\sharp(C\cap L) : L \text{ es variedad afín lineal de codimensión } m \text{ tal que } \sharp\left(\overline{C}^Z \cap L\right) < +\infty\}$$

Nótese que hemos introducido $\overline{C}^Z$ en la definición del grado de C. El siguiente Corolario explica la buena definición de grado de localmente cerrados irreducibles.

COROLARIO 1.3.4. *Sean $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible de dimensión m, $U \subseteq \mathbb{A}^n(\mathbb{K})$ un abierto Zariski y $C = U \cap V \neq \emptyset$ un constructible no vacío localmente cerrado irreducible. Entonces, existe un abierto Zariski $O \subseteq \mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K})$ tal que para cada $L \in O$ se tiene*

$$\sharp(C\cap L) = \deg(V).$$

En particular, si C es un abierto Zariski en un cerrado irreducible, $\deg(C) = \deg(\overline{C}^Z)$.

Demostración. Retomemos el siguiente morfismo entre variedades irreducibles, que es dominante entre variedades de la misma dimensión

$$\begin{array}{rccc} \varphi: & V\times\mathcal{M}_{m\times n}(\mathbb{K}) & \to & \mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K}) \\ & (\underline{x},M) & \longmapsto & (M\cdot\underline{x},M) \end{array}$$

Si $W\subseteq V$ es una variedad algebraica propia, entonces $\dim(W\times\mathcal{M}_{m\times n}(\mathbb{K}))<\dim(\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K}))=m(n+1)$. Por tanto, $\dim(\varphi(W\times\mathcal{M}_{m\times n}(\mathbb{K})))<m(n+1)$.
Sea $O\subseteq\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K})$ el abierto Zariski tal que $\forall L\in O$,

$$\sharp(V\cap L)=\deg(V).$$

Entonces, definamos $O_1\subseteq\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K})$ el abierto Zariski dado mediante $O_1:=O\smallsetminus W_1$, donde W_1 es la clausura Zariski siguiente:

$$W_1:=\overline{\varphi(W\times\mathcal{M}_{m\times n}(\mathbb{K}))}^Z.$$

Como O es abierto Zariski en un irreducible $(\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K}))$ y W_1 es un cerrado de codimensión mayor o igual que 1, entonces O_1 es un abierto Zariski no vacío. Además, dada $L\in O_1$, tendremos que $\varphi^{-1}(L)\cap(W\times\mathcal{M}_{m\times n}(\mathbb{K}))=\emptyset$. En particular, para cada $L\in O_1$, $W\cap L=\emptyset$.
Es decir, hemos probado que dada $W\subsetneq V$ una subvariedad algebraica propia de V irreducible, existe $O_1\subseteq\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K})$ abierto Zariski no vacío tal que se satisface

$$\forall L\in O_1\subseteq O,\ \sharp(V\cap L)=\deg(V)\ \wedge\ V\cap L=L\cap(V\smallsetminus W).$$

Considerando un abierto Zariski no vacío $C\subseteq V$, tomando $W=V\smallsetminus C$, tendremos un cerrado propio de codimensión mayor que 1 y existe un abierto Zariski tal que $\forall L\in O_1,\sharp(V\cap L)<+\infty$ y

$$\sharp(C\cap L)=\deg(V). \tag{1.3.1}$$

Por la definición de $\deg(C)$, si $L\in\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K})$ es tal que $\sharp(V\cap L)<+\infty$, es obvio que $\sharp(C\cap L)\leq\sharp(V\cap L)$, con lo que es obvio también que $\deg(C)\leq\deg\left(\overline{C}^Z\right)$ en este caso. Pero, además, la identidad (1.3.1) nos indica que $\forall L\in O_1\neq\emptyset,\sharp(C\cap L)=\deg(V)$, por lo que concluimos que

$$\deg(C)=\deg\left(\overline{C}^Z\right).$$

□

Corolario 1.3.5. *Sea $V\subseteq\mathbb{A}^n(\mathbb{K})$ una variedad algebraica equidimensional de dimensión m (i.e., todas sus componentes irreducibles tienen dimensión m). Entonces existe un abierto Zariski $O\subseteq\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K})$ tal que para cada $L\in O$ se tiene*

$$\sharp(V\cap L)=\deg(V).$$

Con ello, podemos extender la definición de grado geométrico dada para irreducibles hasta las variedades algebraicas equidimensionales mediante

$$\deg(V)=\max\{\sharp(V\cap L):L\text{ es variedad afín lineal de codimensión }\dim(V),\ \sharp(V\cap L)<+\infty\} \tag{1.3.2}$$

Demostración. Sea $V=V_1\cup\ldots\cup V_s$ la descomposición de V en componentes irreducibles, todas de dimensión m. Consideremos $\mathcal{A}=\{L\in\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K}):\sharp(V\cap L)<+\infty\}$. Entonces, $\forall L\in\mathcal{A}$, $\sharp(V_i\cap L)<+\infty$ y, obviamente,

$$\sharp(V\cap L)\leq\sum_{i=1}^s\sharp(V_i\cap L)\leq\sum_{i=1}^s\deg(V_i)=\deg(V).$$

Por tanto, de la igualdad (1.3.2) tenemos probado que

$$\deg(V)\geq\max\{\sharp(V\cap L):L\text{ es variedad afín lineal de codimensión }\dim(V)\wedge\sharp(V\cap L)<+\infty\}.$$

De otro lado, consideramos los siguientes conjuntos constructibles en V,

$$U_i=V\smallsetminus\left(\bigcup_{j\neq i}V_i\right).$$

Como $V=V_1\cup\ldots\cup V_s$ es la descomposición de V en irreducibles, $U_i\neq\emptyset$ para cada $i,1\leq i\leq s$. Más aún, U_i es un abierto Zariski en V y el constructible

$$C_i:=U_i\cap V_i$$

es un abierto Zariski no vacío en el irreducible de dimensión m V_i. Aplicando el Corolario 1.3.4, existirá $O_i\subseteq\mathbb{A}^m(\mathbb{K})\times\mathcal{M}_{m\times n}(\mathbb{K})$ un abierto Zariski no vacío tal que

i) $\forall L \in O_i, \sharp(V_i \cap L) < +\infty$,
ii) $\forall L \in O_i, \sharp(C_i \cap L) = \deg(V_i)$.

Definamos $O = O_1 \cap \ldots \cap O_s \subseteq \mathbb{A}^m(\mathbb{K}) \times \mathcal{M}_{m\times n}(\mathbb{K})$. Como $\mathbb{A}^m(\mathbb{K}) \times \mathcal{M}_{m\times n}(\mathbb{K})$ es irreducible, O es un abierto Zariski no vacío. Tendremos además que para cada $L \in O$, se tiene

i) $V \cap L \subseteq \bigcup_{i=1}^s (V_i \cap L)$, luego $\sharp(V \cap L) < +\infty$,
ii)

$$\deg(V) = \sum_{i=1}^s \deg(V_i) = \sum_{i=1}^s \sharp(V_i \cap L) = \sum_{i=1}^s \sharp(C_i \cap L) = \sharp\left(\left(\bigcup_{i=1}^s C_i\right) \cap L\right)$$

porque $C_i \cap C_j = \emptyset, \forall i \neq j$.

Finalmente, observemos que $\bigcup_i C_i \subseteq V$, luego

$$\deg(V) = \sharp\left(\left(\bigcup_{i=1}^s C_i\right) \cap L\right) \leq \sharp(V \cap L) \leq \deg(V).$$

En particular, hemos demostrado la otra desigualdad de la identidad (1.3.2) y, por tanto, la afirmación principal. □

1.4. Grado de un constructible (Reparando el "Corrigendum")

En el Corrigendum a su artículo del 83 ([**He, 85**]), J. Heintz señala la existencia de una dificultad en su prueba de la desigualdad de Bézout para conjuntos constructibles. Heintz observa que su desigualdad de Bézout se mantiene como cierta si los constructibles involucrados son localmente cerrados. En esta Sección vamos a modificar la noción de grado de un constructible para concluir que la desigualdad de Bézout para constructibles es siempre cierta (sean o no localmente cerrados). El único elemento clave es que el grado de un conjunto constructible no puede ser definido como el grado de su clausura Zariski.
El origen de esta dificultad se encuentra en una observación (la Remark 2.(2) de [**He, 83**]). Dado $C \subseteq \mathbb{A}^n(\mathbb{K})$ un constructible, definamos el Z-grado de C como el grado de su clausura Zariski, i.e.,

$$\text{Z-deg}(C) := \deg\left(\overline{C}^Z\right).$$

Se tiene el siguiente resultado que contradice la Remark 2.(2) de [**He, 83**]:

Proposición 1.4.1. *El Z-grado de un constructible no satisface la desigualdad de Bézout. De hecho, la Remark 2.(2) de* [**He, 83**] *no es correcta y existen conjuntos algebraicos constructibles C y variedades afines lineales $E \subseteq \mathbb{A}^n(\mathbb{K})$ tales que*

$$\text{Z-deg}(C \cap E) \not\leq \text{Z-deg}(C) \cdot \text{Z-deg}(E) = \text{Z-deg}(C).$$

Demostración. Basta dar un contraejemplo como el siguiente:
Consideremos en $\mathbb{C}^3$ el plano $\pi := \{(x_1, x_2, x_3) \in \mathbb{C}^3 : x_3 = 0\}$ y $A_1 \subseteq \mathbb{C}^3$ el constructible dado mediante

$$A_1 = \pi \setminus \{(x_1, x_2, x_3) \in \mathbb{C}^3 : x_1 x_2 = 0\}.$$

Definamos

$$A_2 := \{(1, 0, 0), (-1, 0, 0)\},$$
$$A_3 := \{(0, 1, 0), (0, -1, 0)\}$$

y definamos el constructible

$$C := A_1 \cup A_2 \cup A_3.$$

Observamos que $\overline{C}^Z = \pi$ porque π es irreducible, A_1 es abierto en π y $A_2, A_3 \subseteq \pi$. Por tanto, $\text{Z-deg}(C) = \deg\left(\overline{C}^Z\right) = 1$.
Ahora consideramos E la recta

$$E := \{(x_1, x_2, x_3) \in \mathbb{C}^3 : x_1 = 0, x_3 = 0\}.$$

Observamos que $C \cap E = \{(0, 1, 0), (0, -1, 0)\}$ es una variedad algebraica formada por dos puntos, luego

$$\text{Z-deg}(C \cap E) = \deg(C \cap E) = 2.$$

Por tanto, tenemos que

$$\text{Z-deg}(C \cap E) = 2 \not\leq 1 = \text{Z-deg}(C).$$

□

Para corregir este problema, analizaremos las posibles descomposiciones de un conjunto constructible en constructibles localmente cerrados irreducibles. Recordemos que un conjunto constructible $C \subseteq \mathbb{A}^n(\mathbb{K})$ se dice localmente cerrado irreducible si es un abierto Zariski en una variedad algebraica irreducible.

DEFINICIÓN 5. *Dado un conjunto constructible $C \subseteq \mathbb{A}^n(\mathbb{K})$ no vacío, llamaremos* descomposición minimal de C en localmente cerrados irreducibles *a toda descomposición*

$$C = A_1 \cup \ldots \cup A_s \tag{1.4.1}$$

donde:

i) Cada $A_i \neq \emptyset$ es localmente cerrado irreducible, i.e., existen $U_i \subseteq \mathbb{A}^n(\mathbb{K})$ abiertos Zariski, $V_i \subseteq \mathbb{A}^n(\mathbb{K})$ variedades algebraicas irreducibles con $A_i = U_i \cap V_i, 1 \leq i \leq s$.

ii) Los V_i anteriores verifican que $V_i \neq V_j, \forall i \neq j$.

A los irreducibles $V_1, \ldots, V_s$ los denominaremos irreducibles asociados a la descomposición (1.4.1) de C.

PROPOSICIÓN 1.4.2. *Todo conjunto constructible $C \subseteq \mathbb{A}^n(\mathbb{K})$ admite una descomposición minimal en localmente cerrados irreducibles.*

DEMOSTRACIÓN. Recuérdese que un constructible es una unión finita de abiertos Zariski en variedades algebraicas, i.e.,

$$C = \bigcup_{i=1}^{t} (V_i \cap O_i),$$

donde $V_i \subseteq \mathbb{A}^n(\mathbb{K})$ es una variedad algebraica y $O_i \subseteq \mathbb{A}^n(\mathbb{K})$ es un abierto Zariski. Ahora descomponemos en irreducibles cada variedad algebraica V_i y concluimos que C admite una descomposición como unión finita de localmente cerrados irreducibles

$$C = \bigcup_{i=1}^{s} A_i$$

donde A_i es localmente cerrado irreducible; es decir, existen abiertos Zariski $U_i \subseteq \mathbb{A}^n(\mathbb{K})$ y cerrados irreducibles $W_i \subseteq \mathbb{A}^n(\mathbb{K})$ tales que $A_i = U_i \cap W_i$. Ahora consideremos la familia de las variedades algebraicas irreducibles así detectadas y supongamos

$$\{W_1, \ldots, W_s\} = \{Z_1, \ldots, Z_r\}$$

con $r \leq s$ de tal modo que $\sharp\{Z_1, \ldots, Z_r\} = r$. En particular, $Z_i \neq Z_j, \forall i \neq j$. Agrupando los abiertos podemos definir, para cada $j, 1 \leq j \leq r$,

$$R_j = \bigcup_{W_i = Z_j} U_i \subseteq \mathbb{A}^n(\mathbb{K}),$$

abiertos Zariski en $\mathbb{A}^n(\mathbb{K})$. Entonces,

$$C = \bigcup_{j=1}^{r} (R_j \cap Z_j) \tag{1.4.2}$$

y la descomposición (1.4.2) es minimal en el sentido de la Definición 5 precedente. Las variedades algebraicas irreducibles $Z_1, \ldots, Z_r$ son las componentes asociadas a la descomposición (1.4.2). □

PROPOSICIÓN 1.4.3. *Sea $C \subseteq \mathbb{A}^n(\mathbb{K})$ un conjunto algebraico constructible, sea*

$$C = A_1 \cup \ldots \cup A_s \tag{1.4.3}$$

una descomposición minimal de C en localmente cerrados irreducibles. Sean $\{V_1, \ldots, V_s\}$ las variedades algebraicas irreducibles asociadas a la descomposición (1.4.3). Sean $\{W_1, \ldots, W_r\}$ las componentes irreducibles de la clausura Zariski $\overline{C}^Z$. Entonces,

$$\{W_1, \ldots, W_r\} \subseteq \{V_1, \ldots, V_s\},$$

pero la igualdad no siempre se da. A los irreducibles asociados a (1.4.3) que no son componentes irreducibles de $\overline{C}^Z$ se les denomina componentes asociadas inmersas, y satisfacen que

$$\forall V \in \{V_1, \ldots, V_s\} \setminus \{W_1, \ldots, W_r\}, \text{ existe } j, 1 \leq j \leq r, \text{ tal que } V \subseteq W_j.$$

DEMOSTRACIÓN. Observando la descomposición (1.4.3) tenemos que

$$\overline{C}^Z = \overline{A_1}^Z \cup \ldots \cup \overline{A_s}^Z = V_1 \cup \ldots \cup V_s = W_1 \cup \ldots \cup W_r \tag{1.4.4}$$

Entonces, como $V_i \neq V_j, \forall i \neq j$, y $\overline{C}^Z = W_1 \cup \ldots \cup W_r$ es la descomposición en componentes irreducibles, claramente se tiene:

i) $\{W_1, \ldots, W_r\} \subseteq \{V_1, \ldots, V_s\}$
ii) El contenido es estricto en ocasiones como se muestra en el ejemplo descrito en la Proposición 1.4.1
$$C = A_1 \cup A_2 \cup A_3 \text{ con } \overline{C}^Z = \overline{A_1}^Z = \pi$$
iii) Para las componentes inmersas basta con usar la igualdad (1.4.4) para concluir que si $V = V_i \in \{V_1, \ldots, V_s\} \setminus \{W_1, \ldots, W_r\}$, entonces
$$V_i = \bigcup_{j=1}^{r} (V_i \cap W_j)$$
y, como V_i es irreducible, concluimos que $\exists j, 1 \leq j \leq r$, tal que $V_i \subseteq W_j$.

□

Con estas ideas podemos definir la noción de grado de un constructible como sigue:

DEFINICIÓN 6. *Sea $C \subseteq \mathbb{A}^n(\mathbb{K})$ un conjunto constructible. Definimos el* grado de C *como el mínimo* $\deg(C) := \min \mathrm{Deg}(C)$, *donde* $\mathrm{Deg}(C)$ *es el conjunto siguiente:*
$$\mathrm{Deg}(C) := \left\{ \sum_{i=1}^{s} \deg(V_i) : \begin{array}{c} \{V_1, \ldots, V_s\} \textit{ son los irreducibles asociados a alguna} \\ \textit{descomposición minimal de } C \textit{ en localmente cerrados irreducibles.} \end{array} \right\}.$$

PROPOSICIÓN 1.4.4. *Con las notaciones precedentes, para cada conjunto constructible afín $C \subseteq \mathbb{A}^n(\mathbb{K})$ se tiene que* $\deg\left(\overline{C}^Z\right) \leq \deg(C)$ *y la igualdad no siempre se verifica. Más aún, si $C \subseteq \mathbb{A}^n(\mathbb{K})$ es una variedad algebraica, el grado definido según la Definición 6 coincide con el grado geométrico definido en* [**He, 83**] *y en las Definiciones 2 y 3 precedentes.*

DEMOSTRACIÓN. En el ejemplo descrito en la Proposición 1.4.1 se exhibe un conjunto constructible C tal que
$$1 = \text{Z-deg}(C) = \deg\left(\overline{C}^Z\right) < \deg(C) = 5.$$
De otro lado, es claro que si C es constructible, $\deg\left(\overline{C}^Z\right) \leq \deg(C)$ por lo siguiente:
Supongamos dada una descomposición minimal de C como unión finita de localmente cerrados irreducibles,
$$C = A_1 \cup \ldots \cup A_s \tag{1.4.5}$$
donde $A_i = U_i \cap W_i \neq \emptyset$ con $U_i \subseteq \mathbb{A}^n(\mathbb{K})$ abierto Zariski, $W_i \subseteq \mathbb{A}^n(\mathbb{K})$ cerrado Zariski irreducible con $W_i \neq W_j, \forall i \neq j$. Como A_i es un abierto Zariski no vacío en W_i, entonces es Zariski denso en W_i. Por tanto, $\overline{A_i}^Z = W_i$, y
$$\overline{C}^Z = W_1 \cup \ldots \cup W_s \tag{1.4.6}$$
con $W_i \neq W_j, \forall i \neq j$.
De otro lado, $\overline{C}^Z$ posee, como variedad algebraica que es, una descomposición minimal en componentes irreducibles
$$\overline{C}^Z = V_1 \cup \ldots \cup V_r. \tag{1.4.7}$$
Por ser minimal, esta descomposición verifica $V_i \subsetneq V_j, \forall i \neq j$. Comparando (1.4.6) y (1.4.7), siento los W_i y los V_j irreducibles, tendremos
$$V_i = \bigcup_{j=1}^{s} (V_i \cap W_j) \Rightarrow \exists j : V_i \subseteq W_j,$$
$$W_j = \bigcup_{i=1}^{r} (W_j \cap V_i) \Rightarrow \exists k : W_j \subseteq V_k.$$
Podemos definir una aplicación
$$\begin{array}{rccc} \varphi : & \{1, \ldots, r\} & \longrightarrow & \{1, \ldots, s\} \\ & i & \longmapsto & \min\{j \in \{1, \ldots, s\} : V_i \subseteq W_j\}. \end{array}$$
Tendremos que $V_i \subseteq W_{\varphi(i)}$ pero $W_{\varphi(i)} \subseteq V_k$ para algún $k \in \{1, \ldots, r\}$, con lo que, debido a que no hay inclusiones estrictas entre las componentes irreducibles de $\overline{C}^Z$, concluiremos
$$V_i = W_{\varphi(i)}, \forall i \in \{1, \ldots, r\}.$$

Además, como $W_j \neq W_{j'} \forall j \neq j'$ en (1.4.6), tendremos que φ es inyectiva y $s \geq r$, con lo que

$$\deg\left(\overline{C}^Z\right) = \sum_{i=1}^{r} \deg(V_i) \leq \sum_{ji=1}^{s} \deg(W_j).$$

Por tanto, $\deg\left(\overline{C}^Z\right)$ es necesariamente menor o igual que el mínimo de las sumas de los grados de los irreducibles que aparecen en descomposiciones del tipo (1.4.5). Concluiremos que para cada constructible se tiene

$$\deg\left(\overline{C}^Z\right) \leq \deg(C).$$

Si, además, $C = V$ es una variedad algebraica, toda descomposición en componentes irreducibles

$$V = V_1 \cup \ldots \cup V_r$$

es una descomposición minimal en localmente cerrados irreducibles. Por tanto, su grado D como constructible (el mínimo de las sumas de los grados de los irreducibles en descomposiciones minimales) satisface

$$D \leq \sum_{i=1}^{r} \deg(V_i) = \deg(V) = \deg\left(\overline{V}^Z\right) \leq D.$$

□

En otras palabras, nuestra noción de grado de un constructible (Definición 6) generaliza la noción de grado de una variedad algebraica como en [**He, 83**].
Estamos así en condiciones de "reparar" la Remark 2.(2) de [**He, 83**].

PROPOSICIÓN 1.4.5. *La noción de grado de un constructible que acabamos de definir es subaditiva. Es decir, dados $C_1, C_2 \subseteq \mathbb{A}^n(\mathbb{K})$ dos conjuntos constructibles, entonces*

$$\deg(C_1 \cup C_2) \leq \deg(C_1) + \deg(C_2).$$

DEMOSTRACIÓN. La idea es que dadas dos descomposiciones minimales de C_1 y C_2 respectivamente,

$$C_1 = A_1 \cup \ldots \cup A_s,\ C_2 = B_1 \cup \ldots \cup B_r, \tag{1.4.8}$$

entonces tenemos una descomposición de $C_1 \cup C_2$ como unión finita de localmente cerrados irreducibles.

$$C_1 \cup C_2 = A_1 \cup \ldots \cup A_s \cup B_1 \cup \ldots \cup B_r.$$

Por la Proposición 1.4.2, toda descomposición en localmente cerrados irreducibles puede refinarse a una descomposición minimal en localmente cerrados irreducibles. Por tanto, tendremos

$$C_1 \cup C_2 = O_1 \cup \ldots \cup O_t$$

con

$$\left\{\overline{O_1}^Z, \ldots, \overline{O_t}^Z\right\} \subseteq \left\{\overline{A_1}^Z, \ldots, \overline{A_s}^Z, \overline{B_1}^Z, \ldots, \overline{B_r}^Z\right\}.$$

Por tanto,

$$\deg(C_1 \cup C_2) \leq \sum_{k=1}^{t} \deg\left(\overline{O_k}^Z\right) \leq \sum_{i=1}^{s} \deg\left(\overline{A_i}^Z\right) + \sum_{j=1}^{r} \deg\left(\overline{B_j}^Z\right).$$

Eligiendo las descomposiciones minimales en localmente irreducibles en (1.4.8) tales que

$$\sum_{i=1}^{s} \deg\left(\overline{A_i}^Z\right) = \deg(C_1) \ \wedge \ \sum_{j=1}^{r} \deg\left(\overline{B_j}^Z\right) = \deg(C_2),$$

tenemos probada la subaditividad. □

LEMA 1.4.6. *Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica de dimensión m y $L \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad afín lineal tal que $V \cap L \neq \emptyset$ y $\sharp(V \cap L) < +\infty$. Entonces, la codimensión de L verifica*

$$\operatorname{codim}(L) \geq m.$$

DEMOSTRACIÓN. Basta con usar el resultado clásico sobre la dimensión de la intersección de las variedades algebraicas afines. Si $X, Y \subseteq \mathbb{A}^n(\mathbb{K})$ son dos variedades afines con $X \cap Y \neq \emptyset$, entonces

$$\dim(X \cap Y) \geq \dim(X) + \dim(Y) - n.$$

Por tanto, si $V \cap L \neq \emptyset$ y $\sharp(V \cap L) < +\infty$, $\dim(V \cap L) = 0$, luego tenemos

$$0 \geq \dim(V) + \dim(L) - n.$$

Así,

$$\dim(L) \leq n - m$$

y, como las variedades afines lineales satisfacen $\dim(L) + \operatorname{codim}(L) = n$, concluimos finalmente que $\operatorname{codim}(L) \geq m$. □

LEMA 1.4.7. *Sea $C \subseteq \mathbb{A}^n(\mathbb{K})$ un constructible de dimensión m y sea $L \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad afín lineal tal que $C \cap L \neq \emptyset$ y $\sharp(C \cap L) < +\infty$. Entonces, existe una variedad afín lineal $L' \subseteq \mathbb{A}^n(\mathbb{K})$ tal que*

i) $L' \supseteq L$,
ii) $\operatorname{codim}(L') = m$,
iii) $\sharp(C \cap L') < +\infty$ *y, en particular,* $\sharp(C \cap L) \leq \sharp(C \cap L')$.

DEMOSTRACIÓN. Por el Lema 1.4.6 precedente, la codimensión de L es mayor o igual que m. Si $\operatorname{codim}(L) = m$ ya habríamos terminado. Por tanto, supongamos $\operatorname{codim}(L) = t > m$. Entonces, existen

- una matriz $A \in \mathcal{M}_{t\times n}(\mathbb{K}), \operatorname{rank}(A) = t$,
- un vector $b = (b_1, \ldots, b_t) \in \mathbb{A}^t(\mathbb{K})$

tales que los polinomios de grado 1 siguientes

$$\begin{pmatrix} \ell_1(X_1, \ldots, X_n) \\ \vdots \\ \ell_t(X_1, \ldots, X_n) \end{pmatrix} = A \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_t \end{pmatrix}$$

satisfacen que

$$L = \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : \ell_1(\underline{x}) = 0, \ldots, \ell_t(\underline{x}) = 0\}.$$

Nuestro objetivo es construir una matriz $P \in \mathcal{M}_{m\times t}(\mathbb{K})$ de rango m tal que los polinomios de grado 1

$$\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} = P \cdot \begin{pmatrix} \ell_1(X_1, \ldots, X_n) \\ \vdots \\ \ell_t(X_1, \ldots, X_n) \end{pmatrix}$$

verifican que la variedad $L' = \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : r_1(\underline{x}) = 0, \ldots, r_m(\underline{x}) = 0\}$ satisface las propiedades deseadas. Nótese que si $\operatorname{rank}(P) = m$, entonces las propiedades *i)* y *ii)* se satisfarán de manera inmediata.
Procedamos inductivamente a la construcción de la matriz P buscada. Probaremos por inducción lo siguiente:
Con las anteriores notaciones, para cada $i, 1 \leq i \leq m$, existe una matriz $P_i \in \mathcal{M}_{i\times t}(\mathbb{K})$ de rango $\operatorname{rank}(P_i) = i$ tal que definiendo

$$\begin{pmatrix} r_1 \\ \vdots \\ r_i \end{pmatrix} = P_i \cdot \begin{pmatrix} \ell_1(X_1, \ldots, X_n) \\ \vdots \\ \ell_t(X_1, \ldots, X_n) \end{pmatrix}$$

se tiene que

$$C \cap \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : r_1(\underline{x}) = 0, \ldots, r_i(\underline{x}) = 0\}$$

es una variedad algebraica no vacía que contiene a $C \cap L$ y tiene dimensión a lo sumo $m - i$.
Caso $i = 1$: Consideremos una descomposición minimal de C en componentes localmente cerradas irreducibles:

$$C = W_1 \cup \ldots \cup W_s.$$

Sea $\rho \leq s$ tal que $\dim(W_j) \geq 1$ si y sólamente si $1 \leq j \leq \rho$.
Para cada $j, 1 \leq j \leq \rho$, $W_j \smallsetminus (C \cap L) \neq \emptyset$ y sea $\underline{x}_j \in W_j \smallsetminus (C \cap L)$.
Consideremos variables $T_1, \ldots, T_t$ y el polinomio

$$q_1(T_1, \ldots, T_t) = \prod_{j=1}^{\rho} (T_1\ell_1(\underline{x}_j) + \ldots + T_t\ell_t(\underline{x}_j)) \in \mathbb{K}[T_1, \ldots, T_t].$$

Es un polinomio no nulo porque para cada $j, 1 \leq j \leq \rho$, existe $k, 1 \leq k \leq t$, tal que $\ell_k(\underline{x}_j) \neq 0$ y, por tanto, el coeficiente de T_k es no nulo en el factor

$$(T_1\ell_1(x_j) + \ldots + T_t\ell_t(x_j)).$$

Elijamos un punto $(\lambda_{1,1}, \ldots, \lambda_{1,t}) \in \mathbb{K}^t$ tal que

$$\left(\left(\prod_{j=1}^{t} \lambda_{1,j}\right) - 1\right) \cdot q_1(\lambda_{1,1}, \ldots, \lambda_{1,t}) \neq 0.$$

Definamos

$$P_1 = \begin{pmatrix} \lambda_{1,1} & \cdots & \lambda_{1,t} \end{pmatrix},$$

que es una matriz de rango $\operatorname{rank}(P_1) = 1$ con polinomio asociado

$$r_1 = P_1 \cdot \begin{pmatrix} \ell_1(X_1, \ldots, X_n) \\ \vdots \\ \ell_t(X_1, \ldots, X_n) \end{pmatrix} = \lambda_{1,1}\ell_1(X_1, \ldots, X_n) + \ldots + \lambda_{1,t}\ell_t(X_1, \ldots, X_n)$$

según hemos definido antes. Para cada $j, 1 \leq j \leq \rho$, como r_1 no se anula en W_j, tampoco se anula idénticamente en $\overline{W}^Z$ y, por el Teorema del Ideal Principal de Krull,

$$\dim(W_j \cap \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : r_1(\underline{x}) = 0\}) = \dim(W_j) - 1.$$

Así, $\dim(C \cap \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : r_1(\underline{x}) = 0\}) = \dim(C) - 1$.
Caso $2 \leq i \leq m$: Suponemos cierto el resultado para $i-1$. Analicemos el caso i. Para ello, escribamos el constructible

$$C_{i-1} = C \cap \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : r_1(\underline{x}) = 0, \ldots, r_{i-1}(\underline{x}) = 0\}.$$

Como $\dim(C) = m$, el Teorema del Ideal Principal de Krull nos dice que la dimensión de C_{i-1} es, al menos, $m - i + 1$. Pero, como por hipótesis inductiva tenemos que $\dim(C_{i-1}) \leq m - i + 1$, entonces es $\dim(C_{i-1}) = m - i + 1$. Como $i \leq m$, entonces $i - 1 \leq m - 1$ y $\dim(C_{i-1}) \geq 1$.
Consideremos, de nuevo, variables $\{T_1, \ldots, T_t\}$ y una descomposición minimal de C_{i-1} en componentes localmente cerradas irreducibles

$$C_{i-1} = W_1 \cup \ldots \cup W_s$$

donde cada W_i es un abierto Zariski en una variedad algebraica irreducible. Sea, de nuevo, $\rho \leq s$ tal que $\dim(W_j) \geq 1$ si y sólo si $1 \leq j \leq \rho$.
Como $W_j \setminus (C \cap L) \neq \emptyset$, para cada $j, 1 \leq j \leq \rho$ sea $\underline{x}_j \in W_j \setminus (C \cap L)$ y definamos el polinomio

$$q_i(T_1, \ldots, T_t) = \prod_{j=1}^{\rho} (T_1\ell_1(\underline{x}_j) + \ldots + T_t\ell_t(\underline{x}_j)) \in \mathbb{K}[T_1, \ldots, T_t].$$

De nuevo, el polinomio q_i es un polinomio no nulo. Adicionalmente, consideremos la matriz extendida

$$\mathcal{P}_i = \left(\begin{array}{ccc} & P_{i-1} & \\ \hline T_1 & \cdots & T_t \end{array} \right).$$

Como $\operatorname{rank}(P_{i-1}) = i - 1$, entonces hay un menor $i \times i$ de $\mathcal{P}_i$ que no es idénticamente cero como polinomio en $\mathbb{K}[T_1, \ldots, T_t]$. Obsérvese que esto es así porque $i \leq m$ y $t \geq m$.
Sea $M(T_1, \ldots, T_t) \in \mathbb{K}[T_1, \ldots, T_t]$ ese menor $i \times i$ no idénticamente nulo. Sea ahora $(\lambda_{i,1}, \ldots, \lambda_{i,t}) \in \mathbb{K}^t$ un punto tal que

$$q_i(\lambda_{i,1}, \ldots, \lambda_{i,t}) \cdot M(\lambda_{i,1}, \ldots, \lambda_{i,t}) \neq 0.$$

Entonces, tenemos que la matriz $P_i \in \mathcal{M}_{i \times t}(\mathbb{K})$ dada mediante

$$P_i = \left(\begin{array}{ccc} & P_{i-1} & \\ \hline \lambda_{i,1} & \cdots & \lambda_{i,t} \end{array} \right)$$

es una matriz de rango i. Consideremos, además, el nuevo polinomio de grado 1 asociado a P_i,

$$r_i := \lambda_{1,1}\ell_1(X_1, \ldots, X_n) + \ldots + \lambda_{1,t}\ell_t(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n].$$

Entonces, $\dim(C_{i-1} \cap \{x \in \mathbb{A}^n(\mathbb{K}) : r_i(x) = 0\}) \leq \dim(C_{i-1}) - 1 = m - i$. Así tenemos probado el resultado.
Por construcción, definiendo $L_i := \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : r_1(\underline{x}) = 0, \ldots, r_i(\underline{x}) = 0\}$, tenemos una variedad lineal afín de codimensión i, $L \subseteq L_i$ y $C \cap L \subseteq C \cap L_i$.
Tomando $i = m$ y la variedad $L' = L_m$, tendremos:

i) Por construcción de los $r_1, \ldots, r_m$, si $\underline{x} \in \mathbb{A}^n(\mathbb{K})$ es tal que $\ell_j(\underline{x}) = 0$ para cada $j, 1 \leq j \leq t$, entonces $r_1(\underline{x}) = 0, \ldots, r_m(\underline{x}) = 0$ y se tiene que

$$L' = L_m \supseteq L.$$

ii) La construcción de la matriz P_m de rango m se ha hecho para que la matriz de coeficientes de las formas afines $r_1, \ldots, r_m$ tenga rango m. Por tanto, $L' = L_m$ es una variedad afín lineal de codimensión m.

iii) Por construcción, $\dim(C \cap L_m) \leq m - m = 0$. Pero, además, $C \cap L \subseteq C \cap L_m$, luego $C \cap L_m \neq \emptyset$. Un constructible de dimensión 0 es un conjunto finito de puntos y, por tanto,

$$\sharp(C \cap L) \leq \sharp(C \cap L') = \sharp(C \cap L_m) < +\infty.$$

□

PROPOSICIÓN 1.4.8 (Reparando Rk 2.(2) de [**He, 83**]). *Sea $C \subseteq \mathbb{A}^n(\mathbb{K})$ un conjunto constructible y $E \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad afín lineal. Entonces,*

$$\deg(C \cap E) \leq \deg(C).$$

DEMOSTRACIÓN. En primer lugar, observemos que basta con probar el resultado para el caso en que C es un localmente cerrado irreducible.
Si C no fuera localmente cerrado irreducible, tomemos una descomposición minimal de C como unión finita de localmente cerrados irreducibles

$$C = V_1 \cup \ldots \cup V_s$$

tal que $\deg(C) = \sum_{i=1}^{s} \deg(V_i)$. Entonces,

$$C \cap E = (V_1 \cap E) \cup \ldots \cup (V_s \cup E).$$

Como el grado es subaditivo, tenemos que

$$\deg(C \cap E) \leq \sum_{i=1}^{s} \deg(V_i \cap E).$$

Pero si tenemos probado el resultado para localmente cerrados irreducibles, concluiremos que $\deg(V_i \cap E) \leq \deg(V_i)$ para cada $i, 1 \leq i \leq s$, y, entonces,

$$\deg(C \cap E) \leq \sum_{i=1}^{s} \deg(V_i \cap E) \leq \sum_{i=1}^{s} \deg(V_i) = \deg(C).$$

Probemos por tanto el resultado para C un localmente cerrado irreducible. Procederemos por inducción en $\operatorname{codim}(E)$:
Caso $\operatorname{codim}(E) = 1$: Podemos suponer $\ell \in \mathbb{K}[X_1, \ldots, X_n]$ un polinomio afín de grado 1 tal que

$$E = \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : \ell(\underline{x}) = 0\}.$$

Ahora, puede ocurrir que $C \cap E = C$, en cuyo caso es obvio que se satisface

$$\deg(C \cap E) \leq \deg(C).$$

Supongamos entonces que $C \cap E \subsetneq C$. Y supongamos que $C = U \cap V$ con $U \in \mathbb{A}^n(\mathbb{K})$ abierto Zariski y $V \in \mathbb{A}^n(\mathbb{K})$ variedad algebraica irreducible.
Consideramos ahora el anillo de funciones polinomiales $\mathbb{K}[V]$ sobre V y la clase definida por $\ell, \overline{\ell} := \ell + I(V)$. Como $C \cap E \subsetneq C$, entonces $V \cap E \subsetneq V$ y, por tanto, $\overline{\ell}$ no es divisor de cero en $\mathbb{K}[V]$. Así, aplicando el Teorema del Ideal Principal de Krull, todos los ideales primos de $\mathbb{K}[V]$ minimales sobre $(\overline{\ell})$ son de altura 1. Esto significa que las componentes irreducibles de $V \cap E$ son todas de dimensión igual a $\dim(V) - 1$. Es decir,

$$V \cap E = V_1 \cup \ldots \cup V_s$$

tales que V_i es irreducible y $\dim(V_i) = \dim(V) - 1$. Ahora,

$$C \cap E = U \cap V \cap E = (U \cap V_1) \cup \ldots \cup (U \cap V_s),$$

con lo que $C \cap E$ admite una descomposición minimal (ver Proposición 1.4.2) en localmente cerrados irreducibles

$$C \cap E = W_1 \cup \ldots \cup W_s$$

con $\dim(W_i) = \dim(C) - 1$ y, por la subaditividad del grado, $\deg(C \cap E) \leq \sum_{i=1}^{s} \deg(W_i)$.
Como $C \cap E$ es equidimensional, existe un abierto Zariski $O \subseteq \mathcal{M}_{(m-1)\times n}(\mathbb{K}) \times \mathbb{A}^{m-1}(\mathbb{K})$ tal que, para cada $L \in O$, $\sharp(C \cap E \cap L) = \deg(C \cap E) < +\infty$ (Corolario 1.3.5). Podemos suponer L tal que $\operatorname{codim}(E \cap L) = m$ (por ser O abierto Zariski) y tendremos:

$$\deg(C \cap E) = \sharp(C \cap (E \cap L)) \leq \deg(C).$$

Caso $\operatorname{codim}(E) \geq 2$: Sea $\operatorname{codim}(E) = r \geq 2$. Existen

- una matriz $M \in \mathcal{M}_{r\times n}(\mathbb{K}), \operatorname{rank}(M) = r$,
- un vector $b = (b_1, \ldots, b_r) \in \mathbb{K}^r$

tales que los polinomios de grado 1

$$\begin{pmatrix} \ell_1(X_1,\dots,X_n) \\ \vdots \\ \ell_r(X_1,\dots,X_n) \end{pmatrix} = M \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}$$

satisfacen

$$E = \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : \ell_1(\underline{x}) = 0, \dots, \ell_r(\underline{x}) = 0\}.$$

Ahora consideremos la variedad afín lineal de codimensión 1

$$E_1 := \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : \ell_1(\underline{x}) = 0\}$$

y consideremos $C_1 := C \cap E_1$. Y definamos $E_2 = \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : \ell_2(\underline{x}) = 0, \dots, \ell_r(\underline{x}) = 0\}$ una variedad afín lineal de codimensión $r-1$.
Consideremos una descomposición minimal en localmente cerrados irreducibles de C_1

$$C_1 = W_1 \cup \ldots \cup W_s$$

de tal modo que $\deg(C_1) = \sum_{i=1}^{s} \deg(W_i)$.
Por hipótesis inductiva, tendremos que $\deg(W_i \cap E_2) \leq \deg(W_i)$ y, por tanto, aplicando subaditividad,

$$\deg(C \cap E) = \deg(C_1 \cap E_2) \leq \sum_{i=1}^{s} \deg(W_i \cap E_2) \leq \sum_{i=1}^{s} \deg(W_i) = \deg(C_1).$$

Aplicando el caso $\operatorname{codim}(E) = 1$, tendremos que $\deg(C_1) = \deg(C \cap E_1) \leq \deg(C)$. Con todo habremos probado

$$\deg(C \cap E) \leq \deg(C_1) \leq \deg(C).$$

□

1.5. La Desigualdad de Bézout para constructibles

La siguiente es una propiedad esencial en la demostración de la Desigualdad de Bézout para constructibles:

PROPOSICIÓN 1.5.1. *Sea $\varphi : \mathbb{A}^n(\mathbb{K}) \to \mathbb{A}^m(\mathbb{K})$ una aplicación afín lineal, sea $C \subseteq \mathbb{A}^n(\mathbb{K})$ un constructible. Entonces, el constructible $\varphi(C)$ satisface*

$$\deg\left(\overline{\varphi(C)}^Z\right) \leq \deg(C).$$

DEMOSTRACIÓN. El Teorema de Chevalley (o la versión afín del Teorema Fundamental de la Teoría de la Eliminación) nos garantiza que $\varphi(C)$ es un constructible. Supongamos que C es localmente cerrado irreducible. Entonces, $\overline{\varphi(C)}^Z \subseteq \mathbb{A}^m(\mathbb{K})$ es una variedad algebraica irreducible y $\varphi(C)$ contiene un abierto Zariski de $\overline{\varphi(C)}^Z$. Sea, ahora, $E \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad afín lineal tal que

$$\deg\left(\overline{\varphi(C)}^Z\right) = \sharp(\varphi(C) \cap E).$$

Consideramos $F = \varphi^{-1}(E) \subseteq \mathbb{A}^n(\mathbb{K})$. Como φ es lineal, F es una variedad afín lineal. Además, observamos que

$$\varphi(C \cap F) = \varphi(C) \cap E.$$

Consideramos una descomposición minimal de $C \cap F$ en localmente cerrados irreducibles

$$C \cap F = V_1 \cup \ldots \cup V_s, \text{ con } \deg(C \cap F) = \sum_{i=1}^{s} \deg(V_i).$$

Cada V_i satisface que $\overline{\varphi(V_i)}^Z \subseteq (\varphi(C) \cap E)$ es un irreducible. Como $\varphi(C) \cap E$ es cero-dimensional, sus componentes irreducibles son puntos, y $\overline{\varphi(V_i)}^Z$ ha de ser un punto. Por tanto, para cada $i, 1 \leq i \leq s$, tenemos que existe un punto $y_i \in \varphi(C) \cap E$ tal que $\varphi(V_i) = \{y_i\}$. Pero, además,

$$\varphi(C \cap F) = \varphi(V_1) \cup \ldots \cup \varphi(V_s) = \varphi(C) \cap E.$$

Por tanto, el número de puntos en $\varphi(C) \cap E$ está acotado por el número de componentes irreducibles de $C \cap F$ y, en particular, por el grado de $C \cap F$. Es decir,

$$\deg\left(\overline{\varphi(C)}^Z\right) = \sharp(\varphi(C) \cap E) \leq s \leq \sum_{i=1}^{s} \deg(V_i) = \deg(C \cap F) \leq \deg(C).$$

En el caso de que C sea un constructible, bastará con descomponerlo en una unión de localmente cerrados irreducibles y, usando la subaditividad del grado, tendremos el resultado general. □

PROPOSICIÓN 1.5.2. *Sean $C_1 \subseteq \mathbb{A}^n(\mathbb{K})$ y $C_2 \subseteq \mathbb{A}^m(\mathbb{K})$ dos constructibles. Entonces, $C_1 \times C_2$ es un constructible en $\mathbb{A}^{n+m}(\mathbb{K})$ y se verifica:*

$$\deg(C_1 \times C_2) \leq \deg(C_1) \cdot \deg(C_2).$$

DEMOSTRACIÓN. En [**He, 83**] se prueba la igualdad para variedades algebraicas. La desigualdad en el caso de constructibles se debe a la subaditividad del grado. □

Estamos así en condiciones de probar el siguiente

TEOREMA 1.5.3 ([**He, 83**], Desigualdad de Bézout). *Sean $V, W \subseteq \mathbb{A}^n(\mathbb{K})$ dos variedades algebraicas afines. Entonces,*

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

DEMOSTRACIÓN. Por la Proposición 1.5.2 precedente,

$$\deg(V \times W) = \deg(V) \cdot \deg(W).$$

Consideremos la variedad afín lineal dada como la diagonal

$$\Delta := \{(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{A}^{2n}(\mathbb{K}) : x_i - y_i = 0, 1 \leq i \leq n\}.$$

Consideramos también la aplicación lineal proyección

$$\begin{array}{rccc} \pi : & \mathbb{A}^{2n}(\mathbb{K}) & \to & \mathbb{A}^n(\mathbb{K}) \\ & (x_1, \ldots, x_n, y_1, \ldots, y_n) & \longmapsto & (x_1, \ldots, x_n) \end{array}$$

y la variedad algebraica

$$C = (V \times W) \cap \Delta \subseteq \mathbb{A}^{2n}(\mathbb{K}).$$

Observamos que

$$\pi(C) = V \cap W,$$

que es también una variedad algebraica afín. Entonces, $\overline{\pi(C)}^Z = V \cap W$.
Por la Proposición 1.5.1 anterior, tendremos

$$\deg(V \cap W) = \deg\left(\overline{\pi(C)}^Z\right) \leq \deg(C) = \deg((V \times W) \cap \Delta)$$

y, como Δ es lineal,

$$\deg((V \times W) \cap \Delta) \leq \deg(V \times W) = \deg(V) \cdot \deg(W).$$

□

El resultado siguiente nos permitirá demostrar la Desigualdad de Bézout para conjuntos constructibles.

PROPOSICIÓN 1.5.4. *Sean $C \subseteq \mathbb{A}^n(\mathbb{K})$ y $C' \subseteq \mathbb{A}^m(\mathbb{K})$ dos constructibles localmente cerrados irreducibles. Sea $\varphi : \mathbb{A}^n(\mathbb{K}) \to \mathbb{A}^m(\mathbb{K})$ una aplicación lineal y supongamos $\varphi(C) = C'$. Entonces,*

$$\deg(\varphi(C)) = \deg(C') \leq \deg(C).$$

DEMOSTRACIÓN. Supongamos $V \subseteq \mathbb{A}^n(\mathbb{K}), W \subseteq \mathbb{A}^m(\mathbb{K})$ dos variedades algebraicas irreducibles y $U \subseteq \mathbb{A}^n(\mathbb{K}), O \subseteq \mathbb{A}^m(\mathbb{K})$ dos abiertos Zariski tales que

$$C = U \cap V \ , \ C' = O \cap W.$$

Por el Corolario 1.3.4, supongamos $L \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad afín lineal tal que

$$\deg(W) = \deg(C') = \sharp(C' \cap L).$$

Consideramos $F \subseteq \mathbb{A}^n(\mathbb{K})$ la variedad afín lineal dada mediante $F = \varphi^{-1}(L)$. Tenemos que $\varphi(C \cap F) = C' \cap L$.
Además, supongamos una descomposición minimal en localmente cerrados irreducibles

$$C \cap F = V_1 \cup \ldots \cup V_s.$$

Tendremos que $\varphi(V_i) \subseteq C' \cap L$ es no vacío y su clausura Zariski es irreducible. Entonces, $\varphi(V_i)$ se reduce a un punto de $C' \cap L$ porque $C' \cap L$ es finito. En particular,

$$s \geq \sharp(C' \cap L),$$

luego tenemos

$$\deg(C) \geq \deg(C \cap F) \geq s \geq \sharp(C' \cap L) = \deg(C').$$

□

Ahora estamos en condiciones de probar

TEOREMA 1.5.5 (Desigualdad de Bézout para conjuntos constructibles). *Sean $C_1, C_2 \subseteq \mathbb{A}^n(\mathbb{K})$ dos conjuntos constructibles. Entonces,*

$$\deg(C_1 \cap C_2) \leq \deg(C_1) \cdot \deg(C_2).$$

DEMOSTRACIÓN. Reproducimos el esquema de prueba original. Consideremos $C_1 \times C_2 \subseteq \mathbb{A}^{2n}(\mathbb{K})$ y consideremos la variedad afín lineal dada como la diagonal $\Delta \subseteq \mathbb{A}^{2n}(\mathbb{K})$:

$$\Delta := \{(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{A}^{2n}(\mathbb{K}) : x_i - y_i = 0, 1 \leq i \leq n\}.$$

Finalmente, consideremos el constructible

$$C := (C_1 \times C_2) \cap \Delta.$$

Por la Proposición 1.4.8, tenemos que

$$\deg(C) \leq \deg(C_1 \times C_2) \leq \deg(C_1) \cdot \deg(C_2),$$

donde la última igualdad viene de la Proposición 1.5.2.
Consideremos ahora una descomposición minimal de C en localmente cerrados irreducibles:

$$C = W_1 \cup \ldots \cup W_s$$

donde $W_i = U_i \cap V_i$ con $U_i \subseteq \mathbb{A}^{2n}(\mathbb{K})$ abierto en Δ, $V_i \subseteq \Delta$ cerrado irreducible y $\deg(C) = \sum_{i=1}^{s} \deg(W_i)$. Consideremos ahora para cada $i, 1 \leq i \leq s$:

- $O_i \subseteq \mathbb{A}^n(\mathbb{K})$ dado mediante

$$O_i := \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : (\underline{x}, \underline{x}) \in U_i\},$$

- $Q_i \subseteq \mathbb{A}^n(\mathbb{K})$ dado mediante

$$Q_i := \{\underline{x} \in \mathbb{A}^n(\mathbb{K}) : (\underline{x}, \underline{x}) \in V_i\}.$$

Observamos fácilmente que O_i es abierto Zariski en $\mathbb{A}^n(\mathbb{K})$, Q_i es cerrado irreducible en $\mathbb{A}^n(\mathbb{K})$ y, si $\pi : \mathbb{A}^{2n} \to \mathbb{A}^n(\mathbb{K})$ es la proyección canónica, entonces

$$\pi(W_i) = O_i \cap Q_i.$$

Ahora, aplicando la Proposición 1.5.4, tendremos que

$$\deg(\pi(W_i)) = \deg(Q_i) = \deg(O_i \cap Q_i) \leq \deg(W_i).$$

Finalmente, es fácil verificar que

$$C_1 \cap C_2 = (O_1 \cap Q_1) \cup \ldots \cup (O_s \cap Q_s),$$

y, aplicando la subaditividad del grado, tendremos que

$$\deg(C_1 \cap C_2) \leq \sum_{i=1}^{s} \deg(O_i \cap Q_i) \leq \sum_{i=1}^{s} \deg(W_i) = \deg(C) \leq \deg(C_1) \cdot \deg(C_2).$$

□

Con esto arreglamos lo que faltaba en [**He, 83**].

1.6. Variaciones sobre la Desigualdad de Bézout

A continuación, probaremos algunas variaciones de la Desigualdad de Bézout que nos serán útiles más adelante. La primera de ellas aparece en [**HeSc, 83**] para variedades algebraicas: aquí la extenderemos a conjuntos constructibles.

PROPOSICIÓN 1.6.1 ([**HeSc, 83**], Prop. 2.3). *Sean $C_i \subseteq \mathbb{A}^n(\mathbb{K}), i = 1, \ldots, r$, conjuntos constructibles. Se tiene*

$$\deg\left(\bigcap_{i=1}^{r} C_i\right) \leq \deg(C_1) \left(\max_{2 \leq i \leq r} \{\deg(C_i)\}\right)^{\dim(C_1)}.$$

Demostración. Probaremos el resultado por inducción en el número de conjuntos r.
El caso $r = 2$ es evidente, ya que se da la Desigualdad de Bézout.
Sea $r > 2$ y supongamos cierto el resultado para $r - 1$.
Sea $C_1 = W_1 \cup \ldots \cup W_s$ una descomposición minimal en componentes localmente cerradas irreducibles de C_1 con

$$\deg(C_1) = \sum_{i=1}^{s} \deg(W_i).$$

Así, basta probar

$$\deg\left(W_j \cap \left(\bigcap_{i=2}^{r} C_i\right)\right) \leq \deg(W_j)\left(\max_{2\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(W_j)}$$

para $j \in \{1, \ldots, s\}$, ya que tendríamos

$$\deg\left(C_1 \cap \left(\bigcap_{i=2}^{r} C_i\right)\right) = \deg\left(\bigcup_{j=1}^{s}\left(W_j \cap \left(\bigcap_{i=2}^{r} C_i\right)\right)\right) \leq \sum_{j=1}^{s} \deg(W_j)\left(\max_{2\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(W_j)},$$

donde la desigualdad es la subaditividad del grado. Además, como $\dim(W_j) \leq \dim(C_1)$ para todo $j, 1 \leq j \leq r$,

$$\deg\left(C_1 \cap \left(\bigcap_{i=2}^{r} C_i\right)\right) \leq \left[\sum_{j=1}^{s} \deg(W_j)\right]\left(\max_{2\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(C_1)} = \deg(C_1)\left(\max_{2\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(C_1)},$$

que es la desigualdad enunciada. Así, sea $j \in \{1, \ldots, s\}$.

Si $W_j \subseteq C_2$, tenemos que $W_j \cap C_2 = W_j$, luego

$$W_j \cap \left(\bigcap_{i=2}^{r} C_i\right) = W_j \cap \left(\bigcap_{i=3}^{r} C_i\right)$$

y estamos en el caso de $r - 1$ conjuntos. Por tanto, con la hipótesis de inducción,

$$\deg\left(W_j \cap \left(\bigcap_{i=2}^{r} C_i\right)\right) \leq \deg(W_j)\left(\max_{3\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(W_j)} \leq \deg(W_j)\left(\max_{2\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(W_j)}.$$

Si $W_j \not\subseteq C_2$, reagrupando los conjuntos podemos escribir

$$W_j \cap \left(\bigcap_{i=2}^{r} C_i\right) = (W_j \cap C_2) \cap \left(\bigcap_{i=3}^{r} C_i\right)$$

y aplicar la hipótesis de inducción para obtener

$$\deg\left(W_j \cap \left(\bigcap_{i=2}^{r} C_i\right)\right) \leq \deg(W_j \cap C_2)\left(\max_{3\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(W_j\cap C_2)}.$$

Ahora, tenemos $\dim(W_j \cap C_2) = \dim\left(\overline{W_j \cap C_2}^{Z}\right) \leq \dim\left(\overline{W_j}^{Z} \cap C_2\right) < \dim\left(\overline{W_j}^{Z}\right) = \dim(W_j)$, luego

$$\deg(W_j \cap C_2)\left(\max_{3\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(W_j\cap C_2)} \leq \deg(W_j \cap C_2)\left(\max_{3\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(W_j)-1}.$$

Ahora, aplicando la Desigualdad de Bézout, tenemos que

$$\begin{aligned}\deg(W_j \cap C_2)\left(\max_{3\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(W_j)-1} &\leq \deg(W_j)\deg(C_2)\left(\max_{3\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(W_j)-1} \\ &\leq \deg(W_j)\left(\max_{2\leq i\leq r}\{\deg(C_i)\}\right)^{\dim(W_j)}.\end{aligned}$$

En los dos casos se da la desigualdad que queríamos probar y se sigue el resultado. □

El siguiente resultado extiende el de la Proposición 1.5.1 para cualquier aplicación polinomial φ mediante la Desigualdad de Bézout.

PROPOSICIÓN 1.6.2. *Sea $C \subseteq \mathbb{A}^n(\mathbb{K})$ un conjunto constructible, y sea $\varphi : C \longrightarrow \mathbb{A}^m(\mathbb{K})$ una aplicación polinomial, $\varphi = (f_1, \ldots, f_m)$ con f_i funciones polinomiales. Entonces, se tiene*

$$\deg\left(\overline{\varphi(C)}^Z\right) \leq \deg(C)\left(\max\{\deg(f_1), \ldots, \deg(f_m), 1\}\right)^m.$$

DEMOSTRACIÓN. Consideramos el grafo de φ,

$$\mathrm{Gr}(\varphi) := \{(x,y) \in C{\times}\mathbb{A}^m(\mathbb{K}) : y_i - f_i(x) = 0, i = 1, \ldots, m\} = (C{\times}\mathbb{A}^m(\mathbb{K})) \cap \left(\bigcap_{i=1}^m \{y_i - f(x_i) = 0\}\right).$$

Sea $\Phi : C \longrightarrow \mathrm{Gr}(\varphi)$ la aplicación que lleva a cada $x \in C$ al par $(x, \varphi(x))$. Como φ es polinomial, esta también lo es. Además, $\Phi(C) = \mathrm{Gr}(\varphi)$, luego $\mathrm{Gr}(\varphi)$ es un conjunto constructible.
Consideramos también la proyección $\pi : \mathbb{A}^n(\mathbb{K}){\times}\mathbb{A}^m(\mathbb{K}) \longrightarrow \mathbb{A}^m(\mathbb{K})$. Así, $\varphi(C) = \pi(\mathrm{Gr}(\varphi))$ y

$$\deg\left(\overline{\varphi(C)}^Z\right) = \deg\left(\overline{\pi(\mathrm{Gr}(\varphi))}^Z\right).$$

Como π es una aplicación afín lineal, por la Proposición 1.5.1, tenemos que

$$\deg\left(\overline{\pi(\mathrm{Gr}(\varphi))}^Z\right) \leq \deg(\mathrm{Gr}(\varphi)).$$

Ahora, usando la Desigualdad de Bézout,

$$\deg(\mathrm{Gr}(\varphi)) = \deg\left((C{\times}\mathbb{A}^m(\mathbb{K})) \cap \left(\bigcap_{i=1}^m \{y_i - f(x_i) = 0\}\right)\right) \leq \deg(C{\times}\mathbb{A}^m(\mathbb{K})) \prod_{i=1}^m \deg(\{y_i - f_i(x) = 0\}),$$

y como $\deg(C{\times}\mathbb{A}^m(\mathbb{K})) \leq \deg(C)\deg(\mathbb{A}^m(\mathbb{K})) = \deg(C)$ y para cada $i \in \{1, \ldots, m\}$ el grado de la hipersuperficie $\{y_i - f_i(x) = 0\}$ es $\deg(Y_i - f_i(X)) = \max\{\deg(f_i), 1\}$, tenemos

$$\deg(C{\times}\mathbb{A}^m(\mathbb{K})) \prod_{i=1}^m \deg(\{y_i - f_i(x) = 0\}) \leq \deg(C)\left(\max\{\deg(f_1), \ldots, \deg(f_m), 1\}\right)^m.$$

Concluimos entonces la desigualdad enunciada. □

Uno de los casos clásicos en los que se distingue el cuerpo K (de coeficientes de los polinomios que definen un constructible) y $\mathbb{K}$ (la clausura algebraica de K) es el caso en el que K es un cuerpo primo. Así, dada una variedad $V \subseteq \mathbb{A}^n(\mathbb{K})$ K-definible, se definen sus puntos K-racionales como los puntos de V con coordenadas en K. Es decir, los puntos

$$V_K := V \cap \mathbb{A}^n(K) = V \cap K^n.$$

La resolución del problema X de Hilbert por Matiyásevich hace que el estudio de los ceros $\mathbb{Q}$-racionales pase a la Conjetura de Birch y Swinnerton-Dyer. Aquí nos ocuparemos del caso de los ceros $\mathbb{F}$-racionales cuando $\mathbb{F}$ es un cuerpo finito. La Proposición 1.6.1 implica el siguiente Corolario:

COROLARIO 1.6.3. *Sea $\mathbb{F}$ un cuerpo finito, $\overline{\mathbb{F}}$ su clausura algebraica y $C \subseteq \mathbb{A}^n(\overline{\mathbb{F}})$ un constructible $\mathbb{F}$-definible. Entonces, el número de puntos $\mathbb{F}$-racionales en C satisface*

$$\sharp(C_{\mathbb{F}}) = \sharp(C \cap \mathbb{A}^n(\mathbb{F})) \leq \deg(C) \cdot \sharp(\mathbb{F})^{\dim(C)} = \deg(C) \cdot q^{\dim(C)}.$$

DEMOSTRACIÓN. Obviamente, $\mathbb{F}$ es el cuerpo de escisión de la ecuación $X^q - X = 0$. Por tanto,

$$C_{\mathbb{F}} = C \cap \mathbb{A}^n(\mathbb{F}) = C \cap \{(x_1, \ldots, x_n) \in \overline{\mathbb{F}}^n : x_i^q - x_i = 0, 1 \leq i \leq n\}.$$

Por tando, aplicando la Proposición 1.6.1, tenemos

$$\sharp(C_{\mathbb{F}}) = \deg(C_{\mathbb{F}}) \leq \deg(C) \cdot \left(\max\{\deg(C_i) : 1 \leq i \leq n\}\right)^{\dim(C)},$$

donde

$$C_k := \{(x_1, \ldots, x_n) \in \overline{\mathbb{F}}^n : x_k^q - x_k = 0\} = \overline{\mathbb{F}}^{k-1}{\times}\mathbb{F}{\times}\overline{\mathbb{F}}^{n-k},$$

lo cual implica claramente la cota del enunciado. □

Los Teoremas de Weil y Stepanov indican que la cota del Corolario precedente es esencialmente óptima en el caso de que C sea una variedad algebraica. Pero eso se escapa del interés de este TFG y omitiremos toda discusión.

CAPÍTULO 2

Conjuntos cuestores y aplicaciones: conjuntos de Kakeya sobre cuerpos finitos (Dvir) y Nullstellensatz Combinatorio (Allon-Tao)

Índice

2.1. Introducción

Los años finales de los setenta y principios de los ochenta del pasado siglo fueron prolíficos en la generación de algoritmos probabilistas para el tratamiento de diversos problemas, siendo uno de ellos el problema de nulidad de polinomios dados "en evaluación". Dos fueron las ideologías para enfrentar este problema: la filosofía Schwartz-Zippel (cf. [Sch, 80], [Zp, 79]) y la filosofía de los conjuntos cuestores o "correct test sequences" (cf. [HeSc, 83]). La primera depende de la reescritura (o de la presentación minimal) de los polinomios a testar, mientras que la segunda sólo depende de la clase (variedad unirracional) donde habitan los polinomios a testar. La primera define una clase grande (exponencial en tamaño siempre) en la que la probabilidad de que haya un cero de un polinomio no nulo es baja. La segunda establece una clase pequeña (de tamaño lineal en la dimensión de la clase que contiene a los polinomios a testar) en la que ningún polinomio no nulo se anula idénticamente.
En este Capítulo generalizaremos la noción de conjunto cuestor, observando que igualmente se pueden considerar para distinguir dos clases de conjuntos constructibles donde viven los polinomios a tratar. Esta es la noción primaria con la que comenzaremos el Capítulo en la Sección 2.2.

2.2. Conjuntos cuestores o "correct test sequences"

Comenzamos generalizando la noción de conjunto cuestor de [HeSc, 83] del modo siguiente. Consideramos K un cuerpo y $\mathbb{K}$ su clausura algebraica.

Definición 7. *Sea $d \in \mathbb{N}$ un número entero positivo. Sean $\Omega \subseteq K[X_1, \ldots, X_n]$ un constructible equidimensional (i.e., los irreducibles asociados a una descomposición minimal son todos de la misma dimensión) de polinomios de grado acotado por d y $\Sigma \subseteq \Omega$ un constructible de codimensión al menos 1 en Ω (i.e., $\dim(\Omega) - \dim(\Sigma) \geq 1$). Un conjunto de puntos $\mathcal{Q} \subseteq K^n$ se denomina* conjunto cuestor (o "correct test sequence") para Ω sobre Σ *si verifica:*

$$\forall f \in \Omega, f|_{\mathcal{Q}} \equiv 0 \Rightarrow f \in \Sigma.$$

Observación 2.2.1. Consideramos Ω una familia de polinomios parametrizada por un espacio afín. Es decir, una aplicación polinomial

$$\varepsilon : \mathbb{K}^m \longrightarrow \Omega \subseteq P_d(X_1, \ldots, X_n).$$

Ejemplos típicos pueden ser los polinomios dados por esquemas de evaluación de talla y profundidad controladas (cf. [HeSi, 80], [HeSc, 83], [KrPa, 96], por ejemplo, ver Anexo B). Otro ejemplo típico son los polinomios sparse: dado un politopo $A \subseteq \mathbb{R}^n$, cuyos puntos enteros $A \cap \mathbb{N}^n$ determinan polinomios de grado a lo sumo d, definimos $P(A) \subseteq P_d(X_1, \ldots, X_n)$ como el conjunto de los polinomios con soporte A (i.e., sus términos corresponden a monomios con exponente en $A \cap \mathbb{N}^n$). Tenemos $\Omega = P(A)$ y una aplicación lineal obvia

$$\varepsilon : \mathbb{K}^{\sharp(A \cap \mathbb{N}^n)} \longrightarrow \Omega = P(A) \subseteq P_d(X_1, \ldots, X_n).$$

Un caso particular serían los polinomios determinados por un subconjunto finito $B \subseteq \mathbb{N}^n$ que son los polinomios con pocos términos no nulos (fewnomials).

OBSERVACIÓN 2.2.2. Se pretende usualmente que los conjuntos cuestores sean conjuntos finitos de puntos.

OBSERVACIÓN 2.2.3. Los tests de nulidad de polinomios se corresponden al caso en que $\Sigma = \{0\}$ es el polinomio nulo en $P_d(X_1, \ldots, X_n)$.

El siguiente resultado es una consecuencia inmediata del Teorema del Ideal Principal de Krull (cf. Teorema A.0.5).

PROPOSICIÓN 2.2.4. *Sea $\Omega \subseteq P_d(X_1, \ldots, X_n)$ un conjunto constructible localmente cerrado irreducible, $\Sigma \subseteq \Omega$ una subvariedad y $\mathcal{Q} \subseteq K^n$ un conjunto cuestor finito para Ω sobre Σ. Entonces,*

$$\dim(\Omega) - \dim(\Sigma) \leq \sharp(\mathcal{Q}),$$

donde $\dim(\cdot)$ *representa la dimensión de Krull del constructible en cuestión, como en el Capítulo precedente. En particular, si $\Sigma = \{0\}$ (i.e., si se trata de un test de nulidad) se tiene*

$$\dim(\Omega) \leq \sharp(\mathcal{Q}).$$

DEMOSTRACIÓN. Supongamos $\mathcal{Q} = \{x_1, \ldots, x_s\} \subseteq K^n$. Entonces, cada punto $x_i \in \mathcal{Q}$ define una ecuación lineal sobre $P_d(X_1, \ldots, X_n)$:

$$\begin{array}{rccc} \ell_i : & P_d(X_1, \ldots, X_n) & \longrightarrow & \mathbb{K} \\ & f & \longmapsto & f(x_i). \end{array}$$

En particular tendremos que, para cada $t \leq s$,

$$\{f \in \Omega : f(x_i) = 0, 1 \leq i \leq t\} = \Omega \cap V_{P_d}(\ell_1) \cap \ldots \cap V_{P_d}(\ell_t),$$

y, por el Teorema del Ideal Principal de Krull,

$$\dim(\{f \in \Omega : f(x_i) = 0, 1 \leq i \leq t\}) \geq \dim(\Omega) - t.$$

Ahora, como $\{f \in \Omega : f(x_i) = 0, 1 \leq i \leq s\} \subseteq \Sigma$, tenemos que

$$\dim(\Omega) - s \leq \dim(\{f \in \Omega : f(x_i) = 0, 1 \leq i \leq s\}) \leq \dim(\Sigma),$$

de donde sale el resultado enunciado. □

2.3. Conjuntos de Kakeya sobre cuerpos finitos

Comencemos retomando la proyección canónica $\pi : \overline{\mathbb{F}}^n \setminus \{0\} \longrightarrow \mathbb{P}_{n-1}(\overline{\mathbb{F}})$. Para cada variedad algebraica proyectiva $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$, denotemos por $V_{\mathbb{F}} = V \cap \mathbb{P}_{n-1}(\mathbb{F})$ el conjunto de sus puntos $\mathbb{F}$-racionales y por $\widetilde{V}$ el cono proyectante sobre V, i.e., $\widetilde{V} = \pi^{-1}(V) \cup \{0\}$. Denotamos por $\widetilde{V}_{\mathbb{F}} = \widetilde{V} \cap \mathbb{F}^n$ a los puntos $\mathbb{F}$-racionales del cono afín $\widetilde{V} \subseteq \mathbb{A}^n(\overline{\mathbb{F}})$.
En lo que sigue, vamos a hacer un breve recordatorio de la función de Hilbert asociada a una variedad algebraica proyectiva. El lector puede seguir muchas de las propiedades en referencias clásicas de Geometría Algebraica y Álgebra Conmutativa (como [**AtMc, 96**], [**Ku, 85**], [**Ma, 80**], [**Na, 75**], [**ZS, 75**] o [**Vo, 84**]).
Retomando la noción de ideal homogéneo discutido en la Sección 1.2, para un ideal homogéneo $\mathfrak{a}$ en $K[X_1, \ldots, X_n]$, escribiremos $\mathfrak{a}_d$ para denotar su parte homogénea de grado d, $\mathfrak{a}_d := \mathfrak{a} \cap H_d^K(X_1, \ldots, X_n)$.
Dada una variedad algebraica proyectiva $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ y su ideal proyectivo asociado $I_{\mathbb{P}}(V) \subseteq \overline{\mathbb{F}}[X_1, \ldots, X_n]$, de acuerdo con la definición introducida en la Identidad (1.2.3), denotaremos por $I_d(V)$ a $I_{\mathbb{P}}(V) \cap H_d(X_1, \ldots, X_n)$.
Si $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ es una variedad algebraica proyectiva, $V_{\mathbb{F}} \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ también lo es. De hecho, $V_{\mathbb{F}}$ es una variedad proyectiva cero-dimensional (i.e., un conjunto finito de puntos) y tiene sentido considerar tanto $I_{\mathbb{P}}(V_{\mathbb{F}})$ como $I_d(V_{\mathbb{F}})$ con las notaciones precedentes.
Un resultado clásico debido a Hilbert es el siguiente:

TEOREMA 2.3.1. *Sea $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ una variedad algebraica proyectiva y definamos*

$$\begin{array}{rccl} \chi_V : & \mathbb{N} & \longrightarrow & \mathbb{R}_+ \\ & r & \longmapsto & \chi_V(r) := \dim_{\overline{\mathbb{F}}} \left(H_r(X_1, \ldots, X_n) \Big/ I_r(V) \right), \end{array}$$

donde $\dim_{\overline{\mathbb{F}}}(\cdot)$ *significa dimensión como $\overline{\mathbb{F}}$-espacio vectorial. Entonces,*

i) Existe un $r_0 \in \mathbb{N}$ y un único polinomio univariado $p \in \mathbb{Q}(T)$ tal que

$$\forall r \geq r_0,\ \chi_V(r) = p(r).$$

Denotaremos igualmente a p y a χ_V, salvo confusión. Al menor r_0 que cumple la identidad anterior se le denomina la regularidad de la función de Hilbert de V.

ii) Si $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ tiene dimensión de Krull d en $\mathbb{P}_{n-1}(\overline{\mathbb{F}})$ para la topología de Zariski en $\mathbb{P}_{n-1}(\overline{\mathbb{F}})$, entonces el grado de p coincide con esa dimensión:

$$\dim(V) = \deg(\chi_V) = \deg(p) = d.$$

iii) [**Vo, 84**] *Con las notaciones precedentes, si V es equidimensional, existe un único número entero $D \in \mathbb{N}$ tal que el polinomio de Hilbert $\chi_V(T) \in \mathbb{Q}[T]$ satisface:*

$$\chi_V(T) = \frac{D}{d!}T^d + h,$$

donde $h \in \mathbb{Q}[T]$ es un polinomio de grado $\leq d-1$. A ese D se le denomina grado de V y lo denotaremos mediante $\deg(V)$.

iv) Si $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ es cero-dimensional, $\deg(V) = \sharp(V)$ *(es decir, el grado coincide con el cardinal si V es un conjunto finito).*

v) Si $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ es irreducible,

$$\deg(V) = \max\{\sharp(V \cap L) : L \text{ es una variedad lineal proyectiva tal que } V \cap L \text{ es finito}\}.$$

vi) [**Vo, 84**] *El grado satisface la desigualdad de Bézout, i.e.,*

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

En el caso de los puntos $\mathbb{F}$-racionales de una variedad algebraica proyectiva $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$, $V_{\mathbb{F}}$ es una variedad proyectiva cero-dimensional y se satisfacen las propiedades siguientes:

PROPOSICIÓN 2.3.2. *Con las notaciones precedentes, se tiene:*

i) Se verifica la desigualdad

$$\deg(V_{\mathbb{F}}) = \sharp(V_{\mathbb{F}}) \leq \deg(V) \cdot \sharp(\mathbb{F})^{\dim(V)}.$$

ii) El polinomio de Hilbert asociado a $V_{\mathbb{F}}$ verifica

$$\chi_{V_{\mathbb{F}}}(r) = \sharp(V_{\mathbb{F}}),$$

para cada r mayor o igual que la regularidad de la función de Hilbert de $V_{\mathbb{F}}$.

iii) Si $V_{\mathbb{F}} = \emptyset$, entonces la función de Hilbert toma los siguientes valores:

$$\chi_{V_{\mathbb{F}}}(r) := \begin{cases} 1, & \text{si } r = 0, \\ 0, & \text{si } r \geq 1, \end{cases}$$

y la regularidad de la función de Hilbert es 1 en ese caso.

2.3.1. Puntos "en el infinito". La manera clásica en que Gaspard Monge y otros "polytechniciens" del siglo XIX interpretaban el espacio proyectivo era como una manera de formalizar los "puntos en el infinito" y las asíntotas si las hubiere. Progresivamente, el proyectivo se interpreta como una compactificación natural del espacio afín que se porta de modo muy natural con ecuaciones polinomiales a través de la homogeneización (definida en la Sección 1.2).
El "hiperplano del infinito" con respecto a la variable X_0 es la variedad proyectiva lineal

$$H_\infty^K := \{(x_0 : x_1 : \ldots : x_n) \in \mathbb{P}_n(K) : x_0 = 0\},$$

donde $(x_0 : ... : x_n)$ son las coordenadas homogéneas. Obviamente, podemos identificar H_∞^K con $\mathbb{P}_{n-1}(K)$. Supongamos ahora una variedad algebraica afín $W \subseteq \mathbb{A}^n(\overline{\mathbb{F}})$. Mediante la inmersión natural $(x_1, \ldots, x_n) \in \mathbb{A}^n(\overline{\mathbb{F}}) \to (1 : x_1 : \ldots : x_n) \in \mathbb{P}_n(\overline{\mathbb{F}})$ podemos suponer que $W \subseteq \mathbb{P}_n(\overline{\mathbb{F}})$. Consideremos la clausura Zariski de W en $\mathbb{P}_n(\overline{\mathbb{F}})$ que denotaremos por $\overline{W}^{\mathbb{P}}$. El paso a la clausura Zariski proyectiva supone añadir algunos puntos "en el infinito" a W, esto es,

$$\overline{W}^{\mathbb{P}} = W \cup W_\infty,$$

donde $W_\infty = \overline{W}^{\mathbb{P}} \cap H_\infty$ son los "puntos en el infinito" de W. Podemos caracterizar estos puntos en el infinito de W mediante:

PROPOSICIÓN 2.3.3. *Con las notaciones precedentes, se tiene que*

$$W_\infty = V_{\mathbb{P}}(\{{}^h f(0, X_1, \ldots, X_n) : f \in I_{\mathbb{A}}(W)\}).$$

Equivalentemente, si para cada $f \in \overline{\mathbb{F}}[X_1, \ldots, X_n]$ definimos su componente homogénea de mayor grado como $H_{\deg}(f)$, tendremos que

$$H_{\deg}(f) = {}^h f(0, X_1, \ldots, X_n).$$

Además,

$$W_\infty = V_{\mathbb{P}}(\{H_{\deg}(f) : f \in I_{\mathbb{A}}(W)\}).$$

Supongamos ahora $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}}) = H_\infty(\mathbb{P}_n(\overline{\mathbb{F}}))$ una variedad algebraica proyectiva. Con esta identificación, podemos ver V como $V = W_\infty$ para alguna variedad afín $W \subseteq \mathbb{A}^n(\overline{\mathbb{F}})$.

2.3.2. Generalización de un resultado de [Dv, 09] y [Tao, 14] sobre conjuntos de Kakeya.

DEFINICIÓN 8 (Kakeya sets en el caso de cuerpos finitos). *Sea $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ una variedad algebraica proyectiva (i.e., puntos en el infinito de $\mathbb{P}_n(\overline{\mathbb{F}})$) y $V_{\mathbb{F}}$ el conjunto de sus puntos $\mathbb{F}$-racionales. Un subconjunto $E \subseteq \mathbb{A}^n(\mathbb{F})$ se denomina un conjunto de Kakeya con direcciones en $V_{\mathbb{F}}$ si, para cada $v \in V_{\mathbb{F}}$, existe $x_v \in E$ tal que la recta*

$$r_v := \{x_v + t\tilde{v} : t \in \mathbb{F}\} \subseteq E,$$

donde $\tilde{v} \in \mathbb{F}^n \setminus \{0\}$ es un representante del punto $v \in V_{\mathbb{F}}$.

Nótese que el punto en el infinito de la recta

$$\overline{r_v} := \{x_v + t\tilde{v} : t \in \overline{\mathbb{F}}\} \subseteq \mathbb{A}^n(\overline{\mathbb{F}})$$

es, precisamente, el punto $v \in V_{\mathbb{F}}$.

PROPOSICIÓN 2.3.4. *Un subconjunto finito $E \subseteq \mathbb{A}^n(\mathbb{F})$ es un conjunto de Kakeya con direcciones en $V_{\mathbb{F}}$ para $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ si y sólo si el conjunto de los puntos en el infinito de las rectas $\mathbb{F}$-definibles contenidas en E contiene a los puntos de $V_{\mathbb{F}}$. Es decir, dado $E \subseteq \mathbb{A}^n(\mathbb{F})$, definamos el siguiente conjunto: Dada una recta $r \subseteq \mathbb{A}^n(\mathbb{F})$ definamos $\overline{r} \subseteq \mathbb{A}^n(\overline{\mathbb{F}})$ como la recta $\mathbb{F}$-definible en $\mathbb{A}^n(\overline{\mathbb{F}})$ determinada por r del modo siguiente: si*

$$r = \left\{ (x_1, \ldots, x_n) \in \mathbb{F}^n : A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} \right\},$$

con $A \in \mathcal{M}_{(n-1)\times n}(\mathbb{F})$ y $(b_1, \ldots, b_{n-1}) \in \mathbb{F}^{n-1}$, entonces

$$\overline{r} = \left\{ (x_1, \ldots, x_n) \in \overline{\mathbb{F}}^n : A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} \right\},$$

Definamos

$$E_\infty^{\mathbb{F}} = \bigcup_{r \subseteq \mathbb{A}^n(\mathbb{F}),\ r \text{ recta},\ r \subseteq E} \overline{r} \cap H_\infty.$$

Entonces, E es Kakeya con direcciones en V si y solamente si

$$V_{\mathbb{F}} \subseteq E_\infty^{\mathbb{F}},$$

es decir, si los puntos de $V_{\mathbb{F}}$ están entre los puntos en el infinito de las rectas $\mathbb{F}$-definibles contenidas en E.

DEMOSTRACIÓN. Es una mera reescritura de la Definición. □

Con las notaciones precedentes, supongamos $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ una variedad algebraica proyectiva. Definimos el conjunto de los polinomios en $\overline{\mathbb{F}}[X_1, \ldots, X_n]$ tales que la hipersuperficie que definen contiene a V entre sus puntos en el infinito. Es decir,

$$\begin{aligned} \Sigma(V) &= \{f \in \overline{\mathbb{F}}[X_1, \ldots, X_n] : {}^h f(0, x) = 0, \forall x \in V\} \\ &= \{f \in \overline{\mathbb{F}}[X_1, \ldots, X_n] : i = \deg(f) \in \mathbb{N}, f_i \in I_{\mathbb{P}}(V),\ f_i \text{ comp. homogénea de grado } i \text{ de } f\}. \end{aligned}$$

Del mismo modo, podemos considerar $\Sigma(V_{\mathbb{F}})$ para los puntos $\mathbb{F}$-racionales. Para cada $d \in \mathbb{N}$, consideramos

$$\Sigma_d(V) = \Sigma(V) \cap P_d(X_1, \ldots, X_n).$$

TEOREMA 2.3.5. *Sea $1 \leq d \leq q-1$ con $q = \sharp(\mathbb{F})$. Sea $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ una variedad algebraica proyectiva en el hiperplano del infinito. Sea $E \subseteq \mathbb{A}^n(\mathbb{F})$ un conjunto de Kakeya con direcciones en $V_{\mathbb{F}}$. Entonces, E es una "correct test sequence" para $P_d^{\overline{\mathbb{F}}}(X_1, \ldots, X_n)$ con respecto a $\Sigma_d(V_{\mathbb{F}})$.*

DEMOSTRACIÓN. Sea $f \in P_d^{\overline{\mathbb{F}}}(X_1, \ldots, X_n)$ y supongamos que $f|_E \equiv 0$. Consideremos la descomposición de f en componentes homogéneas

$$f = f_0 + \ldots + f_r,$$

con $r \leq d$. Consideremos su homogeneizado ${}^h f = \sum_{i=0}^{r} X_0^{r-i} f_i$ y el polinomio ${}^h f(0, X_1, \ldots, X_n) = f_r(X_1, \ldots, X_n) \in H_r^{\overline{\mathbb{F}}}(X_1, \ldots, X_n)$. Consideremos $v \in V_{\mathbb{F}}$ un punto cualquiera, $\tilde{v} \in \mathbb{F}^n \setminus \{0\}$ un representante del punto proyectivo v y sea $r_v \subseteq E$ la recta asociada por ser conjunto de Kakeya, esto es,

$$r_v = \{x_v + t\tilde{v} : t \in \mathbb{F}\} \subseteq E,$$

donde $x_v \in E$ es el punto asociado a v. Entonces, $f|_{r_v} \equiv 0$ (por ser $f|_E \equiv 0$). Veamos que ${}^h f(0, X_1, \ldots, X_n) \in I(V_{\mathbb{F}})$. Por tanto, $f \in \Sigma_d(V_{\mathbb{F}})$. Una forma sencilla de hacerlo es pasar por el polinomio univariado

$$F(T) := f(x_v + T\tilde{v}) \in \overline{\mathbb{F}}[T].$$

$F(T)$ es un polinomio de grado $r \leq q-1$ que tiene la forma

$$F(T) = f_r(\tilde{v})T^r + h(T),$$

donde $\deg(h) \leq r-1$. Como $F(t) = 0, \forall t \in \mathbb{F}$ y $r \leq q-1$, entonces, necesariamente, $f_r(\tilde{v}) = 0$, lo que es equivalente a decir que

$$f_r = {}^h f(0, X_1, \ldots, X_n) \in I_{\mathbb{P}}(V_{\mathbb{F}}).$$

□

En el caso usual, los autores ([**Wo, 99**], [**Dv, 09**], [**Tao, 14**] y sus referencias) consideran $V = \mathbb{P}_{n-1}(\overline{\mathbb{F}})$. El siguiente resultado generaliza las ideas de [**Dv, 09**]:

TEOREMA 2.3.6. *Sea $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ una variedad algebraica proyectiva $\mathbb{F}$-definible. Sea $V_{\mathbb{F}} \subseteq \mathbb{P}_{n-1}(\mathbb{F})$ el conjunto de sus puntos $\mathbb{F}$-racionales. Supongamos $q = \sharp(\mathbb{F})$ y sea $d \in \mathbb{N}$ con $1 \leq d \leq q-1$. Entonces, para cada conjunto de Kakeya $E \subseteq \mathbb{A}^n(\mathbb{F})$ para direcciones en V, se verifica*

$$\sharp(E) \geq \binom{d+n}{n} - \max_{i=0}^{d} \left\{ \binom{d+i}{i} + \chi_{V_{\mathbb{F}}}(i) \right\},$$

donde $\chi_{V_{\mathbb{F}}}$ es la función de Hilbert de $V_{\mathbb{F}}$ como variedad proyectiva cero-dimensional.

DEMOSTRACIÓN. Con las notaciones precedentes, consideremos el espacio afín $P_d(X_1, \ldots, X_n) := P_d^{\overline{\mathbb{F}}}(X_1, \ldots, X_n) = \overline{\mathbb{F}}^{N_d}$, donde $N_d = \binom{d+n}{n}$. Consideremos el conjunto constructible $\Sigma_d(V_{\mathbb{F}}) \subseteq P_d(X_1, \ldots, X_n)$ dado mediante

$$\Sigma_d(V_{\mathbb{F}}) = \{f \in P_d(X_1, \ldots, X_n) : {}^h f(0, X_1, \ldots, X_n) \in I_{\mathbb{P}}(V_{\mathbb{F}})\}.$$

Nótese que $\Sigma_d(V_{\mathbb{F}})$ está formado por todos los polinomios de grado menor o igual que d tales que su componente homogénea de mayor grado se anula en $V_{\mathbb{F}}$. Podemos descomponer este conjunto en función del grado del modo siguiente. Para cada $i, 0 \leq i \leq d$, sea

$$\Sigma_d^{(i)}(V_{\mathbb{F}}) := \{f \in P_d(X_1, \ldots, X_n) : \deg(f) = i, {}^h f(0, X_1, \ldots, X_n) \in I_i(V_{\mathbb{F}})\}.$$

Tenemos la descomposición de $\Sigma_d(V_{\mathbb{F}})$ mediante

$$\Sigma_d(V_{\mathbb{F}}) = \bigcup_{i=0}^{d} \Sigma_d^{(i)}(V_{\mathbb{F}}),$$

y la dimensión de Krull de $\Sigma_d(V_{\mathbb{F}})$ satisface

$$\dim(\Sigma_d(V_{\mathbb{F}})) = \max_{i=0}^{d} \{\dim(\Sigma_d^{(i)}(V_{\mathbb{F}}))\}.$$

Así, aplicando la Proposición 2.2.4, concluiremos que

$$\sharp(E) \geq N_d - \dim(\Sigma_d(V_{\mathbb{F}})) = \binom{d+n}{n} - \max_{i=0}^{d} \{\dim(\Sigma_d^{(i)}(V_{\mathbb{F}}))\}.$$

Lo único que quedaría por analizar es la dimensión de Krull de los conjuntos $\Sigma_d^{(i)}(V_{\mathbb{F}})$. En este enunciado, analizamos esa dimensión a través de la función de Hilbert de $V_{\mathbb{F}}$ discutida anteriormente.

Recordemos que, para cada i,

$$\chi_{V_{\mathbb{F}}}(i) := \dim_{\overline{\mathbb{F}}}\left(H_i^{\overline{\mathbb{F}}}(X_1,\ldots,X_n) \Big/ I_i(V_{\mathbb{F}}) \right).$$

Ahora, un polinomio $f \in \overline{\mathbb{F}}[X_1,\ldots,X_n]$ con $\deg(f) = i$ está en $\Sigma_d^{(i)}(V_{\mathbb{F}})$ si y solamente si su descomposición en componentes homogéneas es de la forma

$$f = f_i + f_{i-1} + \ldots + f_0$$

con $f_i \neq 0$, $f_j \in H_j^{\overline{\mathbb{F}}}(X_1,\ldots,X_n)$ y $f_i \in I_i(V_{\mathbb{F}})$. Por tanto,

$$\Sigma_d^{(i)}(V_{\mathbb{F}}) = \left(\bigoplus_{j=0}^{i-1} H_j^{\overline{\mathbb{F}}}(X_1,\ldots,X_n) \right) \oplus I_i(V_{\mathbb{F}}).$$

Como $I_i(V_{\mathbb{F}})$ es un $\overline{\mathbb{F}}$-espacio vectorial, su dimensión de Krull coincide con su dimensión como $\overline{\mathbb{F}}$-espacio vectorial. Así, tenemos

$$\begin{aligned} \dim(\Sigma_d^{(i)}(V_{\mathbb{F}})) &= \dim(P_{i-1}^{\overline{\mathbb{F}}}(X_1,\ldots,X_n)) + \dim(I_i(V_{\mathbb{F}})) \\ &= \binom{i-1+n}{n} + \dim_{\overline{\mathbb{F}}}(H_i^{\overline{\mathbb{F}}}(X_1,\ldots,X_n)) - \chi_{V_{\mathbb{F}}}(i) \\ &= \binom{i-1+n}{n} + \binom{i+n-1}{n-1} - \chi_{V_{\mathbb{F}}}(i), \end{aligned}$$

con lo que concluimos

$$\dim(\Sigma_d^{(i)}(V_{\mathbb{F}})) = \binom{i+n}{n} - \chi_{V_{\mathbb{F}}}(i),$$

quedando probado el resultado. □

Veamos una variante de este resultado.

Definición 9. *Sea $V \subseteq \mathbb{A}^n(\overline{\mathbb{F}})$ una variedad algebraica equidimensional. Sea $\varepsilon \in \mathbb{R}$ con $0 \leq \varepsilon < 1$. Diremos que los puntos $\mathbb{F}$-racionales de V son altamente densos en V con parámetro de densidad ε si*

$$\deg(V) \cdot q^{\dim(V)-\varepsilon} \leq \sharp(V_{\mathbb{F}}),$$

siendo $q = \sharp(\mathbb{F})$.

Ejemplos de variedades algebraicas con puntos $\mathbb{F}$-racionales altamente densos son las variedades lineales $\mathbb{F}$-definibles (con parámetro $\varepsilon = 0$).
Dada una variedad proyectiva $V \subseteq \mathbb{P}_n(\overline{\mathbb{F}})$, definiremos el cono proyectante sobre V a la variedad algebraica afín $\widetilde{V} \subseteq \mathbb{A}^{n+1}(\overline{\mathbb{F}})$ dada mediante

$$\widetilde{V} = \pi^{-1}(V) \cup \{0\},$$

donde $\pi : \overline{\mathbb{F}}^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}_n(\overline{\mathbb{F}})$ es la proyección canónica. Nótese que $\dim(\widetilde{V}) = \dim(V) + 1$ y que $\sharp(\widetilde{V}_{\mathbb{F}}) = \sharp(\mathbb{F}) \cdot \sharp(V_{\mathbb{F}})$.

Definición 10. *Dada una variedad algebraica proyectiva equidimensional $V \subseteq \mathbb{P}_n(\overline{\mathbb{F}})$, diremos que sus puntos $\mathbb{F}$-racionales son altamente densos con parámetro ε, $0 \leq \varepsilon < 1$, si los puntos $\mathbb{F}$-racionales de su cono proyectante son altamente densos con parámetro ε.*

A modo de ejemplo obvio, si $V = \mathbb{P}_{n-1}(\overline{\mathbb{F}})$, sus puntos $\mathbb{F}$-racionales son altamente densos con parámetro $\varepsilon = 0$.

Proposición 2.3.7. *Sean $V \subseteq \mathbb{P}_n(\overline{\mathbb{F}})$ una variedad algebraica irreducible, $V_{\mathbb{F}} \subseteq \mathbb{P}_n(\mathbb{F})$ el conjunto de sus puntos $\mathbb{F}$-racionales. Supongamos que los puntos $\mathbb{F}$-racionales de V son altamente densos con parámetro ε. Entonces, para cada i, $0 \leq i < q^{1-\varepsilon}$, se verifica*

$$\chi_V(i) = \chi_{V_{\mathbb{F}}}(i),$$

donde χ_V y $\chi_{V_{\mathbb{F}}}$ son, respectivamente, las funciones de Hilbert de V y $V_{\mathbb{F}}$, vista $V_{\mathbb{F}}$ como variedad proyectiva equidimensional.
En el caso particular $V = \mathbb{P}_n(\overline{\mathbb{F}})$, se tendrá

$$\chi_{V_{\mathbb{F}}}(i) = \chi_V(i) = \binom{i+n}{n}$$

para cada i, $0 \leq i \leq q-1$.

DEMOSTRACIÓN. Usaremos el Corolario 1.6.3. Supongamos $f \in H_i^{\overline{\mathbb{F}}}(X_0,\ldots,X_n)$ un polinomio homogéneo de grado i, $i \geq 1$, no nulo. Supongamos que $f \in I_{\mathbb{P}}(V_{\mathbb{F}})$. Sea $\widetilde{V}$ el cono proyectante sobre V con dimensión $\dim(V)+1$. Por ser los puntos F-racionales de V altamente densos con parámetro ε tendremos

$$\sharp(\widetilde{V}_F) \geq \deg(\widetilde{V}) \cdot q^{\dim(V)+1-\varepsilon}. \tag{2.3.1}$$

De otro lado, $\widetilde{V}_{\mathbb{F}} \subseteq \widetilde{V} \cap V_{\mathbb{A}}(f)$. Supongamos que $f \notin I_{\mathbb{P}}(V)$. Entonces, por el Teorema del Ideal Principal de Krull, como f no es divisor de cero módulo $I_{\mathbb{A}}(\widetilde{V})$ tendremos que

$$\dim(\widetilde{V} \cap V_{\mathbb{A}}(f)) = \dim(\widetilde{V}) - 1 = \dim(V).$$

Por la Desigualdad de Bézout (Teorema 1.5.3 o [**He, 83**]) tendremos que

$$\deg(\widetilde{V} \cap V_{\mathbb{A}}(f)) \leq \deg(\widetilde{V}) \cdot \deg(V_{\mathbb{A}}(f)) = \deg(\widetilde{V}) \cdot i.$$

Aplicando el Corolario 1.6.3, tendremos que

$$\sharp(\widetilde{V}_{\mathbb{F}}) \leq \sharp((\widetilde{V} \cap V_{\mathbb{A}}(f))_{\mathbb{F}}) \leq \deg(\widetilde{V}) \cdot i \cdot q^{\dim(V)}. \tag{2.3.2}$$

Combinando las desigualdades (2.3.1) y (2.3.2) anteriores,

$$q^{1-\varepsilon} \leq i.$$

Por tanto, si $0 \leq i < q^{1-\varepsilon}$, tendremos

$$I_{\mathbb{P}}(V) \cap H_i^{\overline{\mathbb{F}}}(X_0,\ldots,X_n) \subseteq I_{\mathbb{P}}(V_{\mathbb{F}}) \cap H_i^{\overline{\mathbb{F}}}(X_0,\ldots,X_n) \subseteq I_{\mathbb{P}}(V) \cap H_i^{\overline{\mathbb{F}}}(X_0,\ldots,X_n),$$

lo que, dada la definición de la función de Hilbert (cf. Teorema 2.3.1), significa

$$\chi_V(i) = \chi_{V_{\mathbb{F}}}(i)$$

para cada i con $0 \leq i < q^{1-\varepsilon}$. En el caso particular $V = \mathbb{P}_n(\overline{\mathbb{F}})$ y $V_{\mathbb{F}} = \mathbb{P}_n(\mathbb{F})$, concluimos que para cada i, $0 \leq i < q-1$,

$$\chi_{V_{\mathbb{F}}}(i) = \chi_V(i) = \left(\begin{array}{c} i+n \\ n \end{array} \right).$$

□

TEOREMA 2.3.8 (Generalización del Teorema de Dvir en [**Dv, 09**] o [**Tao, 14**]). *Sea $\mathbb{F}$ un cuerpo finito de cardinal q y sea $\overline{\mathbb{F}}$ su clausura algebraica. Sea $V \subseteq \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ una variedad proyectiva irreducibe. Supongamos que los puntos $\mathbb{F}$-racionales de V son altamente densos con parámetro $\varepsilon \in [0,1)$. Sea $E \subseteq \mathbb{A}^n(\mathbb{F})$ un conjunto de Kakeya con direcciones en $V_{\mathbb{F}}$. Entonces, para cada $d \in \mathbb{N}$, $1 \leq d \leq q^{1-\varepsilon}-1$, se tiene*

$$\sharp(E) \geq \left(\begin{array}{c} d+n \\ n \end{array} \right) - \max_{i=0}^{d} \left\{ \left(\begin{array}{c} i+n \\ n \end{array} \right) - \chi_V(i) \right\}. \tag{2.3.3}$$

En particular, se tiene el Teorema de Dvir: Para $V = \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ y $V_{\mathbb{F}} = \mathbb{P}_{n-1}(\mathbb{F})$, todo conjunto de Kakeya E con direcciones en $\mathbb{P}_{n-1}(\mathbb{F})$ verifica

$$\sharp(E) \geq \left(\begin{array}{c} d+n \\ n \end{array} \right).$$

DEMOSTRACIÓN. Es consecuencia de combinar la Proposición 2.3.7 anterior con el Teorema 2.3.6. Dado que los puntos $\mathbb{F}$-racionales de V son altamente densos con parámetro ε, se tiene que para cada i, $0 \leq i \leq q^{1-\varepsilon}-1$,

$$\chi_V(i) = \chi_{V_{\mathbb{F}}}(i).$$

Así, el Teorema 2.3.6 implica la desigualdad (2.3.3) anterior. En el caso particular $V = \mathbb{P}_{n-1}(\overline{\mathbb{F}})$ y $V_{\mathbb{F}} = \mathbb{P}_{n-1}(\mathbb{F})$, tendremos que $\varepsilon = 0$ y que

$$\chi_{V_{\mathbb{F}}}(i) = \chi_V(i) = \left(\begin{array}{c} i+n \\ n \end{array} \right) \quad \text{para } 0 \leq i \leq q-1.$$

Por tanto, la desigualdad (2.3.3) se transforma en

$$\sharp(E) \geq \left(\begin{array}{c} d+n \\ n \end{array} \right).$$

□

COROLARIO 2.3.9. *Con las notaciones e hipótesis del Teorema 2.3.6 anterior, sea r_0 la regularidad de la función de Hilbert $\chi_{V_\mathbb{F}}$. Supongamos $r_0 \leq q-1$. Entonces, todo conjunto de Kakeya $E \subseteq \mathbb{A}^n(\mathbb{F})$ con direcciones en $V_\mathbb{F}$ verifica*

$$\begin{aligned} \sharp(E) &\geq \min\left\{\sharp(V_\mathbb{F}), \min_{i=0}^{r_0-1}\left\{\binom{d+n}{n} - \binom{i+n}{n} + \chi_{V_\mathbb{F}}(i)\right\}\right\} \\ &\geq \min\left\{\sharp(V_\mathbb{F}), \binom{q-1+n}{n} - \binom{r_0-1+n}{n}\right\}. \end{aligned}$$

DEMOSTRACIÓN. Como $V_\mathbb{F}$ es visto como variedad cero-dimensional proyectiva, para cada $i \in \mathbb{N}$, $r_0 \leq i \leq q-1$, la función de Hilbert satisface

$$\chi_{V_\mathbb{F}}(i) = \deg(V_\mathbb{F}) = \sharp(V_\mathbb{F}).$$

Así,

$$\max_{i=r_0}^{d}\left\{\binom{i+n}{n} - \chi_{V_\mathbb{F}}(i)\right\} = \binom{d+n}{n} - \sharp(V_\mathbb{F}).$$

Por tanto, usando el Teorema 2.3.6, concluimos que, para $d = q-1$,

$$\begin{aligned} \sharp(E) &\geq \binom{d+n}{n} - \max_{i=0}^{d}\left\{\binom{i+n}{n} - \chi_{V_\mathbb{F}}(i)\right\} \\ &= \binom{d+n}{n} - \max\left\{\binom{d+n}{n} - \sharp(V_\mathbb{F}), \max_{i=0}^{r_0-1}\left\{\binom{i+n}{n} - \chi_{V_\mathbb{F}}(i)\right\}\right\} \\ &= \min\left\{\sharp(V_\mathbb{F}), \binom{d+n}{n} - \max_{i=0}^{r_0-1}\left\{\binom{i+n}{n} - \chi_{V_\mathbb{F}}(i)\right\}\right\} \\ &= \min\left\{\sharp(V_\mathbb{F}), \min_{i=0}^{r_0-1}\left\{\binom{d+n}{n} + \chi_{V_\mathbb{F}}(i) - \binom{i+n}{n}\right\}\right\} \\ &\geq \min\left\{\sharp(V_\mathbb{F}), \binom{q-1+n}{n} - \binom{r_0-1+n}{n}\right\}. \end{aligned}$$

□

OBSERVACIÓN 2.3.10. Como observación final de la Sección, indiquemos que hemos trabajado solamente con el grado geométrico de variedades afines y proyectivas sin tener en cuenta multiplicidades. Como se observa en [**Tao, 14**] y el trabajo de T. Tao con otros co-autores, es posible refinar las cotas inferiores de los conjuntos de Kakeya poniendo en juego multiplicidades. Pero esto conduce a análisis más fuertes de la estabilidad del grado bajo proyecciones si se tienen en cuenta multiplicidades que no caben en la extensión de este Trabajo de Fin de Grado. Se propondrá como posible investigación futura.

2.4. Sobre el Nullstellensatz Combinatorio de Alon y Tao

En su trabajo de 1999 [**Al, 99**], N. Alon introduce el concepto de Nullstellensatz Combinatorio para definir una clase de conjunto cuestor de gran tamaño, muy similar a la clase de los resultados de J. T. Schwartz y R. Zippel. En 2014, T. Tao retoma ese Nullstellensatz Combinatorio en [**Tao, 14**] dando una prueba alternativa del mismo resultado. En esta Sección, vamos a dar una demostración más general del Nullstellensatz Combinatorio, que permitirá enunciados más amplios y explicará mejor el significado de ese Teorema. Todo el material de esta sección es original y se sigue de un uso racional del clásico Teorema Chino de los Restos.

Como en la Sección precedente, $\mathbb{F}$ será un cuerpo finito. Dado un subconjunto $E \subseteq \mathbb{A}^n(\mathbb{F})$, tendremos que E es un conjunto finito, cuyo cardinal coincide con su grado geométrico $\sharp(E) = \deg(E)$. En esta Sección, escribiremos $I(E) := I_\mathbb{F}(E)$ los polinomios en $\mathbb{F}[X_1, \ldots, X_n]$ que se anulan en E.

LEMA 2.4.1. *Con las notaciones precedentes, supongamos $D = \deg(E)$ y*

$$E = \{z_1, \ldots, z_D\} \subseteq \mathbb{A}^n(\mathbb{F}).$$

Entonces, el ideal $I(E) \subseteq \mathbb{F}[X_1, \ldots, X_n]$ es un ideal cero-dimensional radical que satisface

$$I(E) = \bigcap_{i=1}^{D} \mathfrak{m}_{z_i},$$

donde $\mathfrak{m}_{z_i} = I(\{z_i\}) \subseteq \mathbb{F}[X_1, \ldots, X_n]$ *es el ideal maximal asociado al punto afín* $z_i \in \mathbb{A}^n(\mathbb{F})$.

Por tanto, la $\mathbb{F}$-álgebra cociente $\mathbb{F}[E] = \mathbb{F}[X_1, \ldots, X_n] \Big/ I(E)$ es $\mathbb{F}$-espacio vectorial de dimensión finita sobre $\mathbb{F}$. Además, por el Teorema Chino de los Restos, tenemos el siguiente isomorfismo de $\mathbb{F}$-álgebras:

$$\begin{array}{ccc} \mathbb{F}[E] & \longrightarrow & \prod_{i=1}^{D} \mathbb{F}[X_1, \ldots, X_n] \Big/ \mathfrak{m}_{z_i} \\ f + I(E) & \longmapsto & (f + \mathfrak{m}_{z_1}, \ldots, f + \mathfrak{m}_{z_D}). \end{array}$$

Nótese, además, que para cada $f \in \mathbb{F}[X_1, \ldots, X_n]$ y cada $z \in \mathbb{A}^n(\mathbb{F})$, tenemos el siguiente obvio isomorfismo de cuerpos:

$$\begin{array}{ccc} \mathbb{F}[X_1, \ldots, X_n] \Big/ \mathfrak{m}_z & \longrightarrow & \mathbb{F} \\ f + \mathfrak{m}_z & \longmapsto & f(z). \end{array}$$

Por tanto, podemos entender el isomorfismo del Teorema Chino de los Restos del modo siguiente:

$$\begin{array}{ccc} \mathbb{F}[E] & \longrightarrow & \mathbb{F}^D \\ f + I(E) & \longmapsto & (f(z_1), \ldots, f(z_D)) \end{array},$$

que no sólo es isomorfismo de espacios vectoriales, sino también isomorfismo de anillos cuando en $\mathbb{F}^D$ se considera la estructura de anillo producto (i.e., suma y producto "coordenada a coordenada"). Para cada $h \in \mathbb{F}[X_1, \ldots, X_n]$ definimos la homotecia de razón h sobre $\mathbb{F}[E]$ como el endomorfismo de espacios vectoriales

$$\begin{array}{rccc} \eta_h : & \mathbb{F}[E] & \longrightarrow & \mathbb{F}[E] \\ & f + I(E) & \longmapsto & hf + I(E). \end{array}$$

Denotaremos, finalmente, por Tr a la traza de un endomorfismo e introduciremos la forma bilineal simétrica siguiente:

$$\begin{array}{rccc} \langle \cdot, \cdot \rangle_E : & \mathbb{F}[E] \times \mathbb{F}[E] & \longrightarrow & \mathbb{F} \\ & (f + I(E), g + I(E)) & \longmapsto & \mathrm{Tr}(\eta_f \circ \eta_g) \quad = \mathrm{Tr}(\eta_g \circ \eta_f). \end{array}$$

Dada una base $\beta = \{v_i : i \in I\}$ de $\mathbb{F}[E]$ como $\mathbb{F}$-espacio vectorial, llamaremos base dual de β a toda base $\beta^* = \{w_i : i \in I\}$ de $\mathbb{F}[E]$ tal que

$$\langle v_i, w_j \rangle_E = \delta_{ij}, \forall i, j, 1 \leq, i, j, \leq n,$$

donde δ_{ij} es la delta de Kronecker. El siguiente Lema resume las propiedades esenciales de esta forma bilineal simétrica.

LEMA 2.4.2. *Con las notaciones precedentes, se tiene:*

i) Para cada $h \in \mathbb{F}[X_1, \ldots, X_n]$, *el endomorfismo* η_h *es diagonalizable y su forma canónica de Jordan es la matriz diagonal*

$$\mathrm{Diag}(h(z_1), \ldots, h(z_D)).$$

En particular, la traza satisface

$$\mathrm{Tr}(\eta_h) = \sum_{i=1}^{D} h(z_i) = \sum_{z \in E} h(z).$$

ii) Toda base $\beta = \{v_1, \ldots, v_D\}$, $v_i = f_i + I(E)$, *de* $\mathbb{F}[E]$ *como* $\mathbb{F}$*-espacio vectorial posee una base dual* $\beta^* = \{w_1, \ldots, w_D\}$, $w_j = g_j + I(E)$, *que, además, satisface*

$$\langle v_i, w_j \rangle_E = \sum_{z \in E} f_i(z) g_j(z) = \delta_{ij}.$$

DEMOSTRACIÓN. La propiedad *i)* es inmediata y es consecuencia del Teorema Chino de los Restos. Se explica de modo inmediato mediante el diagrama conmutativo siguiente:

$$\begin{array}{ccc} \mathbb{F}[E] & \xrightarrow{\quad\eta_h\quad} & \mathbb{F}[E] \\ \Big\downarrow{\scriptstyle\varphi} & \circlearrowleft & \Big\downarrow{\scriptstyle\varphi} \\ \prod_{i=1}^{D}\mathbb{F}[X_1,\ldots,X_n]\Big/\mathfrak{m}_{z_i} & \xrightarrow{\quad\widetilde{\eta}_h\quad} & \prod_{i=1}^{D}\mathbb{F}[X_1,\ldots,X_n]\Big/\mathfrak{m}_{z_i} \end{array}$$

donde los morfismos φ son los del Teorema Chino de los Restos y $\widetilde{\eta}_h$ es el endomorfismo

$$\begin{array}{rccc} \widetilde{\eta}_h: & \prod_{i=1}^{D}\mathbb{F}[X_1,\ldots,X_n]\Big/\mathfrak{m}_{z_i} & \longrightarrow & \prod_{i=1}^{D}\mathbb{F}[X_1,\ldots,X_n]\Big/\mathfrak{m}_{z_i} \\ & (f+\mathfrak{m}_{z_1},\ldots,f+\mathfrak{m}_{z_D}) & \longmapsto & (hf+\mathfrak{m}_{z_1},\ldots,hf+\mathfrak{m}_{z_D}). \end{array}$$

Es fácil ver que la matriz de $\widetilde{\eta}_h$ en las bases canónicas de $\mathbb{F}^D$ es la matriz diagonal $\mathrm{Diag}(h(z_1),\ldots,h(z_D))$ y que las matrices de $\eta_h = \widetilde{\eta}_h$ son semejantes por tenerse

$$\widetilde{\eta}_h = \varphi\circ\eta_h\circ\varphi^{-1}.$$

En consecuencia, las trazas coinciden y, por tanto,

$$\mathrm{Tr}(\widetilde{\eta}_h) = \mathrm{Tr}(\eta_h) = \sum_{i=1}^{D} h(z_i) = \sum_{z\in E} h(z).$$

ii) Esta segunda afirmación es también sencilla de probar mediante la construcción siguiente:
Sea $\beta = \{v_1,\ldots,v_D\}$ una base de $\mathbb{F}[E]$. Nótese que cada $v_i = f_i + I(E)$ es la clase definida por un polinomio. Tenemos el isomorfismo $\widetilde{\varphi}$ extendido del Teorema Chino de los Restos que es isomorfismo de $\mathbb{F}$-álgebras y, por tanto, isomorfismo de $\mathbb{F}$-espacios vectoriales:

$$\begin{array}{rccc} \widetilde{\varphi}: & \mathbb{F}[E] & \longrightarrow & \mathbb{F}^D \\ & f+I(E) & \longmapsto & (f(z_1),\ldots,f(z_D)). \end{array}$$

En particular, tendremos que β es una base de $\mathbb{F}[E]$ como $\mathbb{F}$-espacio vectorial si y solamente si los siguientes vectores son linealmente independientes:

$$\{(f_i(z_1),\ldots,f_i(z_D)) : 1\le i\le D\}.$$

Esto nos permite construir la matriz de (pseudo-)Vandermonde asociada a la base β y al conjunto E siguiente:

$$vdM(\beta,E) = \begin{pmatrix} f_1(z_1) & \cdots & f_1(z_D) \\ \vdots & \ddots & \vdots \\ f_D(z_1) & \cdots & f_D(z_D) \end{pmatrix} \in \mathcal{M}_D(\mathbb{F}).$$

Si β es una base de $\mathbb{F}[E]$, la matriz $vdM(\beta,E)$ tiene rango D y es, por tanto, inversible. Ahora consideremos $\{e_i : 1\le i\le D\}$ la base "canónica" de $\mathbb{F}^D$ y los sistemas de ecuaciones lineales

$$S_i \equiv vdM(\beta,E)\cdot\begin{pmatrix} X_1 \\ \vdots \\ X_D \end{pmatrix} = e_i, 1\le i\le D.$$

Por lo dicho anteriormente, todos estos sistemas de ecuaciones lineales son compatibles determinados y cada uno de ellos posee solución única no nula: sean $\{\underline{x}_i : 1\le i\le D\}\subseteq\mathbb{F}^D$ de tal modo que $\underline{x}_i$ es solución del sistema de ecuaciones lineales S_i para cada $i, 1\le i\le D$.
Retomando $\widetilde{\varphi}$, para cada $i, 1\le i\le D$, existirá $g_i\in\mathbb{F}[X_1,\ldots,X_n]$ tal que

$$\underline{x}_i = \widetilde{\varphi}(g_i+I(E)) = (g_i(z_1),\ldots,g_i(z_D)).$$

En particular, los $g_i + I(E)$ son no nulos en $\mathbb{F}[E]$.
Además, como $vdM(\beta,E)\cdot\underline{x}_i = e_i$ para cada $i, 1\le i\le D$, la familia $\{\underline{x}_1,\ldots,\underline{x}_D\}$ es una base de $\mathbb{F}^D$ (porque $vdM(\beta,E)$ es una matriz regular). En particular, la siguiente familia

$$\{w_i := \widetilde{\varphi}^{-1}(\underline{x}_i), 1\le i\le D\}$$

es una base de $\mathbb{F}[E]$ con $w_i = g_i + I(E), g_i \in \mathbb{F}[X_1, \ldots, X_n]$. Finalmente, tenemos que

$$e_i = vdM(\beta, E) \cdot \underline{x}_i = \begin{pmatrix} f_1(z_1) & \cdots & f_1(z_D) \\ \vdots & \ddots & \vdots \\ f_D(z_1) & \cdots & f_D(z_D) \end{pmatrix} \cdot \begin{pmatrix} g_i(z_1) \\ \vdots \\ g_i(z_D) \end{pmatrix} = \begin{pmatrix} \langle f_1, g_i \rangle_E \\ \vdots \\ \langle f_D, g_i \rangle_E \end{pmatrix},$$

lo que permite concluir, $\forall i, j, 1 \leq i, j \leq D$,

$$\langle v_i, w_j \rangle_E = \mathrm{Tr}(\eta_{f_i} \circ \eta_{g_j}) = \sum_{z \in E} f_i(z) g_j(z) = \delta_{i,j}.$$

□

Supongamos ahora $W \subseteq I(E)$ un subespacio y sea β una base de W. Llamaremos dual de W con respecto a β a cualquier $\mathbb{F}$-subespacio vectorial $W(\beta)^*$ generado por una base dual de β. Es decir, por el Lema precedente, si $\beta = \{v_1, \ldots, v_N\}$ es una base de W, existe una familia de vectores linealmente independientes $\beta^* = \{w_1, \ldots, w_N\}$ tales que $\langle v_i, w_j \rangle_E = \delta_{i,j}, \forall i, j, 1 \leq i, j \leq N$.
Para ver esto, simplemente tenemos que extender β hasta una base $\widetilde{\beta}$ de $\mathbb{F}[E]$, hallar una base dual $(\widetilde{\beta})^*$ como se indica en el Lema y, tomando β^* como los N primeros elementos de $(\widetilde{\beta})^*$, habremos definido $W(\beta)^* = \mathbb{F}\langle \beta^* \rangle$, el subespacio generado por β^*.

Teorema 2.4.3. *Con las notaciones precedentes, sea $P \in \mathbb{F}[X_1, \ldots, X_n]$ un polinomio no nulo. Sea $E \subseteq \mathbb{A}^n(\mathbb{F})$ un conjunto finito, $I(E)$ su ideal y $\mathbb{F}[E]$ el anillo de funciones polinomiales definidas sobre E. Supongamos que existe un subespacio vectorial $W \subseteq I(E)$, una base β de W de tal modo que $P + I(E)$ admite una descomposición de la forma*

$$P + I(E) = P_1 + P_2 + I(E)$$

con

i) $P_1 \in W$ y $P_1 \neq 0$,
ii) $P_2 \perp W(\beta)^*$ (i.e., $\langle P_2, g \rangle_E = 0, \forall g \in W(\beta)^*$).

Entonces, P no se anula idénticamente en E.

Demostración. Aplicando la construcción precedente a este Teorema, supongamos

$$\beta = \{v_1, \ldots, v_N\}, \beta^* = \{w_1, \ldots, w_N\},$$

con $N = \dim(W)$. Entonces, tenemos que, para cada $i, 1 \leq i \leq N$,

$$\langle P + I(E), w_i \rangle_E = \langle P_1, w_i \rangle_E \text{ (porque } \langle P_2, w_i \rangle_E = 0, \forall i).$$

Como $P_1 \neq 0$, tendremos que existe $i \in \{1, \ldots, N\}$ tal que

$$P_1 = \sum_{j=1}^{N} \lambda_j v_j \text{ con } \lambda_i \neq 0.$$

Entonces, $\langle P + I(E), w_i \rangle_E = \lambda_i \neq 0$. Nótese que, por la definición de la forma bilineal $\langle \cdot, \cdot \rangle_E$, se tendrá

$$\lambda_i = \langle P + I(E), w_i \rangle_E = \sum_{z \in E} P(z) g_i(z),$$

donde $w_k = g_k + I(E), 1 \leq k \leq N$, con $g_k \in \mathbb{F}[X_1, \ldots, X_n]$. Como $\lambda_i \neq 0$, no puede suceder que $P(z) = 0, \forall z \in E$, con lo que $P \notin I(E)$. □

Lema 2.4.4. *Sean $h_1, \ldots, h_n \in \mathbb{F}[T]$ polinomios univariados de grados respectivos $D_1, \ldots, D_n$. Supongamos que $h_1, \ldots, h_n$ factorizan completamente sobre $\mathbb{F}$ con raíces distintas. Es decir, supongamos que para cada $i, 1 \leq i \leq n$, se tiene que*

$$\sharp\{z \in \mathbb{F} : h_i(z) = 0\} = D_i = \deg(h_i).$$

Consideremos el ideal $\mathfrak{a} = (h_1(X_1), \ldots, h_n(X_n)) \subseteq \mathbb{F}[X_1, \ldots, X_n]$ y sean $E_i \subseteq \mathbb{F}$ los conjuntos de ceros en $\mathbb{F}$ de cada h_i, definiendo $E = E_1 \times \ldots \times E_n \subseteq \mathbb{A}^n(\mathbb{F})$. Se tiene:

i) $\mathfrak{a} = I(E)$ es un ideal radical.
ii) La familia $\{h_1(X_1), \ldots, h_n(X_n)\}$ es una base de Gröbner del ideal $\mathfrak{a} = I(E)$ con respecto al orden grado+lexicográfico con $X_1 < X_2 < \ldots < X_n$.
iii) La siguiente es una base monomial de $\mathbb{F}[E] = \mathbb{F}[X_1, \ldots, X_n]/\mathfrak{a}$:

$$\beta = \{X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} : 0 \leq \mu_i \leq D_i - 1, 1 \leq i \leq n\}.$$

iv) Para cada $i, 1 \leq i \leq n$, denotemos por

$$\beta_i^* := \{g_{\mu_i}^{(i)}(T) + (h_i) : 0 \leq \mu \leq D_i - 1\} \subseteq \mathbb{F}[E_i] := \mathbb{F}[T]/(h_i)$$

a la base dual de $\beta_i = \{T^{\mu_i} + (h_i) : 0 \leq \mu \leq D_i - 1\} \subseteq \mathbb{F}[E_i]$. Entonces, la siguiente es una base dual de β con respecto al producto $\langle \cdot, \cdot, \rangle_E$:

$$\beta^* = \left\{ \left(\prod_{i=1}^{n} g_{\mu_i}^{(i)}(X_i) \right) + \mathfrak{a} : (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n, 0 \leq \mu_i \leq D_i - 1, 1 \leq i \leq n \right\}.$$

Demostración. Las primeras propiedades *i), ii), iii)* son conocidas y no merece la pena escribirlas. Nos ocuparemos de la propiedad *iv)* que es la propiedad original. Nótese que se tiene para cada $i, 1 \leq i \leq n$,

$$\sum_{z_i \in E_i} g_{\mu_i}^{(i)}(z_i) \cdot z_i^{\theta_j} = \delta_{\mu_i, \theta_j}.$$

Consideremos ahora $\underline{\theta} = (\theta_1, \ldots, \theta_n), \underline{\mu} = (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$ con $0 \leq \theta_i, \mu_i \leq D_i - 1$ y definamos

$$C_{\underline{\theta}, \underline{\mu}}^{(n)} := \sum_{(z_1, \ldots, z_n) \in E} \prod_{i=1}^{n} \left(g_{\theta_i}^{(i)}(z_i) \cdot z_i^{\mu_i} \right) = \left\langle \left(\prod_{i=1}^{n} g_{\theta_i}^{(i)}(X_i) \right) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E.$$

Si $n = 1$, tendremos que

$$C_{\theta, \mu}^{(1)} = \delta_{\theta, \mu}.$$

Para $n \geq 2$, supongamos que $\underline{\theta} \neq \underline{\mu}$ y, sin pérdida de generalidad y por simplicidad de la escritura, supongamos que es $\theta_1 \neq \mu_1$. Entonces, se tiene:

$$C_{\underline{\theta}, \underline{\mu}}^{(n)} = \left(\sum_{z_1 \in E_1} g_{\theta_1}^{(1)}(z_1) \cdot z_1^{\mu_1} \right) \cdot C_{\underline{\theta}', \underline{\mu}'}^{(n-1)} = 0 \cdot C_{\underline{\theta}', \underline{\mu}'}^{(n-1)} = 0, \tag{2.4.1}$$

donde

$$C_{\underline{\theta}', \underline{\mu}'}^{(n-1)} = \sum_{(z_2, \ldots, z_n) \in E_2 \times \cdots \times E_n} \prod_{i=2}^{n} \left(g_{\theta_i}^{(i)}(z_i) \cdot z_i^{\mu_i} \right), \tag{2.4.2}$$

donde $\underline{\theta}' = (\theta_2, \ldots, \theta_n)$ y $\underline{\mu}' = (\mu_2, \ldots, \mu_n)$. Entonces, tendremos

$$C_{\underline{\theta}, \underline{\mu}}^{(n)} = 0 = \left\langle \prod_{i=1}^{n} g_{\theta_i}^{(i)}(X_i) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E.$$

Supongamos, en cambio, que $\underline{\theta} = \underline{\mu}$. Entonces, tendremos también una identidad como (2.4.1),

$$C_{\underline{\theta}, \underline{\mu}}^{(n)} = \left(\sum_{z_1 \in E_1} g_{\theta_1}^{(1)}(z_1) \cdot z_1^{\mu_1} \right) \cdot C_{\underline{\theta}', \underline{\mu}'}^{(n-1)},$$

donde $C_{\underline{\theta}', \underline{\mu}'}^{(n-1)}$ se define como en (2.4.2). En conclusión,

$$C_{\underline{\theta}, \underline{\mu}}^{(n)} = 1 \cdot C_{\underline{\theta}', \underline{\mu}'}^{(n-1)}.$$

Aplicando el obvio argumento inductivo, dado que $\underline{\theta}' = \underline{\mu}'$, concluiremos que

$$C_{\underline{\theta}, \underline{\mu}}^{(n)} = 1.$$

Hemos probado que

$$\left\langle \prod_{i=1}^{n} g_{\theta_i}^{(i)}(X_i) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E = \delta_{\underline{\theta}, \underline{\mu}} = \begin{cases} 1, & \text{si } \underline{\mu} = \underline{\theta} \\ 0, & \text{en caso contrario.} \end{cases}$$

Por tanto, β^* es base dual de β con respecto a $\langle \cdot, \cdot \rangle_E$. □

El siguiente Lema es la reinterpretación en términos de traza y dualidad de la estrategia seguida en [**Tao, 14**] para redemostrar el Nullstellensatz Combinatorio de [**Al, 99**].

LEMA 2.4.5 ([Tao, 14]). *Con las notaciones del Lema precedente, sea* $\underline{\theta} = (\theta_1, \ldots, \theta_n) \in \mathbb{N}^n$ *con* $0 \leq \theta_i \leq D_i - 1$. *Sea* $\underline{\mu} = (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$ *tal que* $|\underline{\mu}| = \mu_1 + \cdots + \mu_n \leq (\sum_{i=1}^n D_i) - n$. *Supongamos que existe* i *con* $\mu_i \geq D_i$ *y que el conjunto*

$$\{j \in \{1, \ldots, n\} : \mu_j \neq \theta_j, 0 \leq \mu_j \leq D_j - 1\} \neq \emptyset. \tag{2.4.3}$$

Entonces,

$$C^{(n)}_{\underline{\theta},\underline{\mu}} = \left\langle \left(\prod_{i=1}^n g^{(i)}_{\theta_i}(X_i) \right) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E = 0.$$

DEMOSTRACIÓN. Tenemos que $\mu_i \geq D_i$, y con la hipótesis (2.4.3), existe j con $0 \leq \mu_j \leq D_j - 1, \mu_j \neq \theta_j$.
Supongamos, sin pérdida de generalidad, que $j = 1$. Tendremos entonces

$$C^{(n)}_{\underline{\theta},\underline{\mu}} = \left(\sum_{z_1 \in E_1} g^{(1)}_{\theta_1}(z_1) \cdot z_1^{\mu_1} \right) \cdot C^{(n-1)}_{\underline{\theta}',\underline{\mu}'},$$

donde $C^{(n-1)}_{\underline{\theta}',\underline{\mu}'}$ es dado como en la ecuación (2.4.2) de la Demostración precedente. Entonces, como $0 \leq \theta_1 \leq D_1 - 1$ y $0 \leq \mu_1 \leq D_1 - 1$ se tiene

$$\sum_{z_1 \in E_1} g^{(1)}_{\theta_1}(z_1) \cdot z_1^{\mu_1} = 0$$

y, por tanto,

$$C^{(n)}_{\underline{\theta},\underline{\mu}} = 0 \cdot C^{(n-1)}_{\underline{\theta}',\underline{\mu}'} = 0.$$

□

COROLARIO 2.4.6. *Con las notaciones de los Lemas precedentes, sean* $\underline{\theta}, \underline{\mu} \in \mathbb{N}^n$ *tales que*

i) $|\underline{\mu}| = \mu_1 + \cdots + \mu_n \leq (D_1 - 1) + \cdots + (D_n - 1)$,
ii) $\underline{\theta} = (\theta_1, \ldots, \theta_n)$ *con* $0 \leq \theta_i \leq D_i - 1$,
iii) $|\underline{\mu}| \leq |\underline{\theta}|$.

Entonces, si $\underline{\theta} \neq \underline{\mu}$,

$$C^{(n)}_{\underline{\theta},\underline{\mu}} = \left\langle \left(\prod_{i=1}^n g^{(i)}_{\theta_i}(X_i) \right) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E = 0.$$

DEMOSTRACIÓN. Si $\underline{\mu} = (\mu_1, \ldots, \mu_n)$ es tal que $|\underline{\mu}| \leq (D_1 - 1) + \cdots + (D_n - 1)$ y $|\underline{\mu}| \leq |\underline{\theta}|$, supongamos que existe i con $\mu_i \geq D_i$; entonces, ha de existir $j \in \{1, \ldots, n\}$ tal que $\mu_j < \theta_j$. Aplicando el Lema precedente, concluiremos que

$$C^{(n)}_{\underline{\theta},\underline{\mu}} = 0.$$

En otro caso, es decir, si $0 \leq \mu_i \leq D_i - 1$ para cada $i, 1 \leq i \leq n$, tendremos que $X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \in \beta$ y es distinto de $X_1^{\theta_1} \cdots X_n^{\theta_n} + \mathfrak{a} \in \beta$. Por tanto, al ser β^* la base dual de β con respecto a $\langle \cdot, \cdot \rangle_E$ concluiremos que

$$C^{(n)}_{\underline{\theta},\underline{\mu}} = \left\langle \left(\prod_{i=1}^n g^{(i)}_{\theta_i}(X_i) \right) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E = \delta_{\underline{\theta},\underline{\mu}} = 0.$$

□

COROLARIO 2.4.7 (Nullstellensatz Combinatorio de [Al, 99]). *Sean* $D_1, \ldots, D_n \in \mathbb{N}$. *Sea* $D \leq D_1 + \ldots + D_n - n$, *y sea* $\Delta := \{\underline{\mu} = (\mu_1, \ldots, \mu_n) : |\underline{\mu}| = D, \mu_i \leq D_i - 1\}$. *Sea* Ω_D *la siguiente clase de polinomios:*

$$\Omega_D := \{f \in P_D^{\mathbb{F}}(X_1, \ldots, X_n) : \exists \underline{\theta} \in \Delta, f_{\underline{\theta}} \neq 0\} \cup \{0\},$$

siendo $f_{\underline{\theta}}$ *el coeficiente del término de grado* $\underline{\theta}$ *en* f.
Entonces, dados $E_1, \ldots, E_n \subseteq \mathbb{F}$ *conjuntos con* $\sharp(E_i) = D_i$, $E = E_1 \times \ldots \times E_n$ *es un conjunto cuestor para* Ω_D *con respecto a* $\{0\}$.

DEMOSTRACIÓN. Sea $f \in \Omega_D$, escribamos

$$f = \sum_{|\underline{\mu}| \leq \deg(f)} f_{\underline{\mu}} X_1^{\mu_1} \cdots X_n^{\mu_n},$$

tendremos, en virtud de los Lemas anteriores, los casos siguientes:

i) Si $|\underline{\mu}| < \deg(f) = \theta_1 + \ldots + \theta_n$,

$$\left\langle \left(\prod_{i=1}^{n} g_{\theta_i}^{(i)}(X_i) \right) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E = 0.$$

ii) Si $|\underline{\mu}| = \deg(f) = \theta_1 + \ldots + \theta_n$ con $\underline{\mu} \neq \underline{\theta}$,

$$\left\langle \left(\prod_{i=1}^{n} g_{\theta_i}^{(i)}(X_i) \right) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E = 0.$$

iii) Por último, si $\underline{\mu} = \underline{\theta}$,

$$\left\langle \left(\prod_{i=1}^{n} g_{\theta_i}^{(i)}(X_i) \right) + \mathfrak{a}, X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \right\rangle_E = 1.$$

Por tanto,

$$\left\langle \left(\prod_{i=1}^{n} g_{\theta_i}^{(i)}(X_i) \right) + \mathfrak{a}, f + \mathfrak{a} \right\rangle_E = f_{\underline{\theta}}.$$

En particular,

$$f_{\underline{\theta}} = \sum_{(z_1,\ldots,z_n)\in E} \prod_{i=1}^{n} g_{\theta_i}^{(i)}(z_i) \cdot f(z_1, \ldots, z_n)$$

Si $f_{\underline{\theta}} \neq 0$, entonces $f(z_1, \ldots, z_n) \neq 0$ para algún $(z_1, \ldots, z_n) \in E$ y $f|_E \not\equiv 0$. □

Observación 2.4.8. Sería conveniente disponer de versiones más amplias del Nullstellensatz Combinatorio, basadas en un mayor conocimiento de cómo son las bases duales en este contexto. Por el momento no tenemos resultados más amplios.

CAPÍTULO 3

Sobre la densidad de los conjuntos cuestores en variedades cero-dimensionales: aplicación a la detección de sucesiones secantes

Índice

3.1. Sobre la densidad de los conjuntos cuestores

En esta Sección vamos a mostrar una generalización estricta del resultado principial de [**HeSc, 83**]. No solamente se trata de generalizar el resultado a un espectro más aimplio de problemas, sino también mostrar que la densidad es alta en cualquier variedad (suficientemente amplia) de dimensión cero y que, en el fondo, se trata de una manera de controlar variaciones de la dimensión simplemente mediante evaluación en puntos bien elegidos. Comencemos fijando un poco las notaciones del contexto.
Sea $\mathbb{A}^N(\mathbb{K})$ un "lineal" (puntos afines sobre un cuerpo $\mathbb{K}$ algebraicamente cerrado). Supongamos que tenemos una aplicación polinomial de "evaluación" definible sobre un subcuerpo $K \subseteq \mathbb{K}$:

$$ev : \mathbb{A}^N(\mathbb{K}) \times \mathbb{A}^n(\mathbb{K}) \longrightarrow \mathbb{A}^m(\mathbb{K}).$$

Nótese que podemos interpretar $ev = (ev_1, \ldots, ev_m)$ como una sucesión de aplicaciones polinomiales $ev_i \in K[Y_1, \ldots, Y_N, X_1, \ldots, X_n]$, donde las variables $\{Y_1, \ldots, Y_N\}$ representan las coordenadas en $\mathbb{A}^N(\mathbb{K})$ y las variables $\{X_1, \ldots, X_n\}$ representan las coordenadas de los puntos en $\mathbb{A}^n(\mathbb{K})$.
Escribamos D_i para denotar el grado total de la aplicación polinomial ev_i y d_i para el grado de ev_i en las variables $\{X_1, \ldots, X_n\}$.
Consideremos ahora un constructible $\Omega \subseteq \mathbb{A}^N(\mathbb{K})$ formado por funciones que, a su vez, satisfacen unas ecuaciones polinomiales. Más adelante veremos algunos ejemplos; por ahora supongamos que $\overline{\Omega}^Z$ es irreducible.
Denotemos por $W = ev^{-1}(\{0\})$ a la fibra de la función de evaluación sobre el $0 \in \mathbb{A}^m(\mathbb{K})$ y sea $V(\Omega) = (\Omega \times \mathbb{A}^n(\mathbb{K})) \cap W$. Llamaremos a $V(\Omega)$ la *variedad de incidencia* de la evaluación sobre Ω. Consideremos también las proyecciones canónicas

$$\pi_1 : V(\Omega) \longrightarrow \Omega,$$
$$\pi_2 : V(\Omega) \longrightarrow \mathbb{A}^n(\mathbb{K}).$$

Supongamos, además, que la dimensión de la fibra genérica de π_1 sobre puntos de Ω está fijada. Es decir, supongamos que existe $\Sigma \subseteq \overline{\Omega}^Z$ una subvariedad propia tal que existe $r \in \mathbb{N}$ entero positivo verificándose:

i) $\forall f \in \Omega \setminus \Sigma, \dim(\pi_1^{-1}(\{f\})) = r$,
ii) $\forall f \in \Sigma, \dim(\pi_1^{-1}(\{f\})) > r$.

Diremos que Σ *es un discriminante de* Ω *con respecto a la dimensión.*
Nótese que el grado de las fibras de π_1 sobre elementos de Ω está acotado por una cantidad conocida como el número de Bézout:

$$\deg(\pi_1^{-1}(\{f\})) \leq \prod_{i=1}^{m} d_i = \mathscr{D}.$$

Nótese, además, que nuestras hipótesis representan la situación más usual. Por ejemplo, en el caso denso $\Omega = \mathbb{A}^N(\mathbb{K}) = \mathcal{P}_{(d)}(X_1, \ldots, X_n)$, para una lista de grados $(d) = (d_1, \ldots, d_m)$, se satisfacen las hipótesis descritas con $r = n - m, m \leq n$.

Proposición 3.1.1. *Con las notaciones precedentes:*

i) $\deg(V(\Omega)) \leq \deg(\Omega) \cdot \deg(W) \leq \deg(\Omega) \cdot \prod_{i=1}^{m} D_i$.

ii) Para cada componente irreducible C de $V(\Omega)$ tal que $\pi_1(C) \smallsetminus \Sigma \neq \emptyset$ se tiene que

$$\dim(C) \leq \dim(\Omega) + r.$$

Si, además, $\pi_1(C)$ es denso Zariski en Ω, la anterior es una igualdad.

DEMOSTRACIÓN. *i)* La primera afirmación es consecuencia inmediata de la Desigualdad de Bézout para conjuntos constructibles. Es decir, como $W = ev^{-1}(\{0\})$, entonces

$$W = \{(y,x) \in \mathbb{A}^N(\mathbb{K}) \times \mathbb{A}^n(\mathbb{K}) : ev_1(y,x) = \ldots = ev_m(y,x) = 0\}.$$

Por tanto, concluiremos

$$V(\Omega) = (\Omega \times \mathbb{A}^n(\mathbb{K})) \cap W \Rightarrow$$

$$\deg(V(\Omega)) \leq \deg(\Omega \times \mathbb{A}^n(\mathbb{K})) \cdot \deg(W) \leq \deg(\Omega) \cdot \deg(W) \leq \deg(\Omega) \cdot \prod_{i=1}^{m} D_i.$$

ii) Para la segunda usaremos el Teorema de la Dimensión en la Fibra. Así, para cada $f \in \overline{\pi_1(C)}^Z$ (que es irreducible), tendremos el siguiente morfismo dominante entre irreducibles,

$$\pi_1|_C : C \longrightarrow \overline{\pi_1(C)}^Z,$$

y $\dim(\pi_1^{-1}(\{f\})) \geq \dim(C) - \dim\left(\overline{\pi_1(C)}^Z\right)$. Además, genéricamente en $\overline{\pi_1(C)}^Z$ se da la igualdad

$$\dim(\pi_1^{-1}(\{f\})) = \dim(C) - \dim\left(\overline{\pi_1(C)}^Z\right). \tag{3.1.1}$$

Como $\pi_1(C) \smallsetminus \Sigma \neq \emptyset$, tenemos un abierto no vacío en $\overline{\pi_1(C)}^Z \smallsetminus \Sigma \neq \emptyset$, y como (3.1.1) es genéricamente cierta en $\overline{\pi_1(C)}^Z$, existe algún $f \in \pi_1(C) \smallsetminus \Sigma$ en el que se cumple la igualdad, con lo que concluiremos

$$r = \dim(\pi_1^{-1}(\{f\})) = \dim(C) - \dim\left(\overline{\pi_1(C)}^Z\right)$$

y

$$\dim(C) = r + \dim\left(\overline{\pi_1(C)}^Z\right) \leq r + \dim(\Omega).$$

En particular, si $\overline{\pi_1(C)}^Z = \overline{\Omega}^Z$, se tendrá la igualdad. □

Con las notaciones precedentes, entendamos nuestra variedad de incidencia del modo siguiente: dado $s \in \mathbb{N}$ un entero positivo, definamos

$$V_s(\Omega) := \{(f, \underline{x}_1, \ldots, \underline{x}_s) \in \Omega \times (\mathbb{A}^n(\mathbb{K}))^s : (f, \underline{x}_i) \in V(\Omega), 1 \leq i \leq s\}$$

y consideremos las proyecciones naturales extendidas

$$\pi_1 : V_s(\Omega) \longrightarrow \Omega,$$
$$\pi_2 : V_s(\Omega) \longrightarrow (\mathbb{A}^n(\mathbb{K}))^s.$$

PROPOSICIÓN 3.1.2. *Con las notaciones precedentes,*

i) $\deg(V_s(\Omega)) \leq \deg(\Omega) \cdot \deg(W)^s \leq \deg(\Omega) \cdot \left(\prod_{i=1}^m D_i\right)^s$.

ii) Para cada componente irreducible C de $V_s(\Omega)$ tal que $\pi_1(C) \cap (\Omega \smallsetminus \Sigma) \neq \emptyset$ se tiene que

$$\dim(C) \leq \dim(\Omega) + rs.$$

Si, además, $\pi_1(C)$ es denso Zariski en Ω, la anterior es una igualdad.

DEMOSTRACIÓN. Las pruebas son análogas a las de la Proposición precedente. □

Estamos ya en condiciones de mostrar la generalización siguiente del resultado principal de [**HeSc, 83**]:

TEOREMA 3.1.3. *Sea $ev : \mathbb{A}^N(\mathbb{K}) \times \mathbb{A}^n(\mathbb{K}) \longrightarrow \mathbb{A}^m(\mathbb{K})$ una aplicación polinomial K-definible sobre algún subcuerpo K de $\mathbb{K}$, siendo $\mathbb{K}$ algebraicamente cerrado. Sean $W = ev^{-1}(\{0\})$ la variedad de incidencia, $\Omega \subseteq \mathbb{A}^N(\mathbb{K})$ un constructible de clausura Zariski irreducible y sean $\Sigma \subseteq \Omega$ y $r \in \mathbb{N}$ de tal modo que r es la dimensión genérica de la fibra de π_1 sobre puntos de Ω y Σ es una subvariedad discriminante de Ω con respecto a la dimensión.*
Sean $s, d \in \mathbb{N}$ dos números enteros que satisfacen las siguientes desigualdades:

$$s \geq 6 \dim(\Omega),$$

$$d \geq 2\left(\deg(\Omega)^{1/\dim(\Omega)} \cdot \deg(W)^6\right)^{1/5},$$

Entonces, para cualquier variedad cero-dimensional $V \subseteq \mathbb{A}^n(\mathbb{K})$ dada por ecuaciones de grado a lo sumo d tal que su grado satisface

$$\deg(V) \geq d^{r+1}, \tag{3.1.2}$$

se verifica la siguiente propiedad:
La probabilidad de que una elección aleatoria de puntos $\mathcal{Q} = (x_1, \ldots, x_s) \in V^s$ sea un conjunto cuestor para Ω sobre Σ está acotada inferiormente por

$$1 - \frac{1}{2^{5\dim(\Omega)}}.$$

Demostración. Escribamos $\mathcal{D}$ para el grado de la variedad global de incidencia W, i.e., $\mathcal{D} = \deg(W)$. Comencemos considerando la clase de componentes irreducibles de $V_s(\Omega)$ dada mediante

$$\mathcal{C} := \{C : \overline{\pi_1(C)}^Z \smallsetminus \Sigma \neq \emptyset\}.$$

Por los resultados precedentes tendremos que, si $B = \bigcup_{C\in\mathcal{C}} C$, se verifica

i) $\deg(B) \leq \deg(V_s(\Omega)) \leq \deg(\Omega) \cdot \mathcal{D}^s$.
ii) $\dim(B) \leq \dim(\Omega) + rs$.

Consideremos la intersección

$$B' := B \cap (\mathbb{A}^N(\mathbb{K}) \times V^s).$$

Por la Proposición 1.6.1 se tiene que

$$\deg(B') \leq \deg(B) \cdot d^{\dim(B)}.$$

La razón es que, si $V = V(f_1, \ldots, f_t)$, entonces

$$B' = B \cap \left(\bigcap_{i=1}^{s} \bigcap_{j=1}^{t} \left(\mathbb{A}^N(\mathbb{K}) \times (\mathbb{A}^n(\mathbb{K}))^{i-1} \times V(f_j) \times (\mathbb{A}^n(\mathbb{K}))^{s-i}\right) \right),$$

luego

$$\deg(B') \leq \deg(B) \cdot \left(\max\{\deg(f_j)\}\right)^{\dim(B)}.$$

Así, con las cotas sobre la dimensión y el grado de B, tenemos que

$$\deg(B') \leq \deg(\Omega) \cdot \mathcal{D}^s \cdot d^{\dim(\Omega)+rs}.$$

Considerando ahora la proyección $\pi_2 : V_s(\Omega) \longrightarrow (\mathbb{A}^n(\mathbb{K}))^s$ observamos que

$$\pi_2(B) \cap V^s = \pi_2(B')$$

y, como $\pi_2(B')$ es cero-dimensional, $\overline{\pi_2(B')}^Z = \pi_2(B')$, por lo que

$$\deg(\pi_2(B')) = \deg\left(\overline{\pi_2(B')}^Z\right) \leq \deg(B') \leq \deg(\Omega) \cdot \mathcal{D}^s \cdot d^{\dim(\Omega)+rs}.$$

Ahora observemos la propiedad siguiente:
Supongamos que $(\underline{x}_1, \ldots, \underline{x}_s) \in V^s$ no es conjunto cuestor para Ω sobre Σ. Entonces, $\exists f \in \Omega \smallsetminus \Sigma$ tal que $ev(f, \underline{x}_i) = 0, 1 \leq i \leq s$. Pero, entonces, $(f, \underline{x}_1, \ldots, \underline{x}_s)$ estará en alguna componente irreducible C de $V_s(\Omega)$ tal que $\overline{\pi_1(C)}^Z \smallsetminus \Sigma \neq \emptyset$ (porque $f \in \overline{\pi_1(C)}^Z \smallsetminus \Sigma$), luego

$$(f, \underline{x}_1, \ldots, \underline{x}_s) \in B \cap (\mathcal{P}_{(d)} \times V^s).$$

Con lo cual,

$$(\underline{x}_1, \ldots, \underline{x}_s) \in \pi_2(B')$$

y las listas de puntos que no son conjuntos cuestores están contenidas en $\pi_2(B')$. Así, la probabilidad de que una lista $(\underline{x}_1, \ldots, \underline{x}_s) \in V^s$ sea un conjunto cuestor para Ω sobre Σ está acotada inferiormente por

$$1 - \frac{\sharp(\pi_2(B'))}{\sharp(V)^s} \tag{3.1.3}$$

Acotemos el término negativo: tenemos

$$\frac{\sharp(\pi_2(B'))}{\sharp(V)^s} = \frac{\deg(\pi_2(B'))}{(\deg(V))^s} \leq \frac{\deg(\Omega) \cdot \mathcal{D}^s \cdot d^{\dim(\Omega)+rs}}{d^{(r+1)s}} = \frac{\deg(\Omega) \cdot \mathcal{D}^s \cdot d^{\dim(\Omega)}}{d^s}.$$

Ahora, como $s = 6\dim(\Omega)$, queda

$$\frac{\sharp(\pi_2(B'))}{\sharp(V)^s} = \frac{\deg(\Omega) \cdot \mathcal{D}^{6\dim(\Omega)}}{d^{5\dim(\Omega)}} = \left(\frac{\deg(\Omega)^{1/\dim(\Omega)} \cdot \mathcal{D}^6}{d^5}\right)^{\dim(\Omega)}.$$

Por construcción, tenemos $d^5 \geq 2^5 \deg(\Omega)^{1/\dim(\Omega)}\mathcal{D}^6$, luego

$$\frac{\sharp(\pi_2(B'))}{\sharp(V)^s} \leq \left(\frac{1}{2}\right)^{5\dim(\Omega)}$$

y el Teorema se sigue de (3.1.3). □

COROLARIO 3.1.4. *Con las notaciones del Teorema precedente, si $D_i = \deg(ev_i)$ para $1 \leq i \leq m$, sean $s, d \in \mathbb{N}$ tales que:*

$$s \geq 6\dim(\Omega),$$
$$d \geq 2\left(\deg(\Omega)^{1/\dim(\Omega)} \cdot \left(\prod_{i=1}^{m} D_i\right)^6\right)^{1/5}.$$

Entonces, para cualquier variedad cero-dimensional $V \subseteq \mathbb{A}^n(\mathbb{K})$ dada por ecuaciones de grado a lo sumo d tal que su grado satisface

$$\deg(V) \geq d^{r+1},$$

se verifica la siguiente propiedad:
La probabilidad de que una elección aleatoria de puntos $\mathcal{Q} = (x_1, \ldots, x_s) \in V^s$ sea un conjunto cuestor para Ω sobre Σ está acotada inferiormente por

$$1 - \frac{1}{2^{5\dim(\Omega)}}.$$

COROLARIO 3.1.5 (El caso denso). *Con las notaciones del Teorema precedente, consideremos $(d) = (d_1, \ldots, d_m)$ una lista de grados. Sea $\mathcal{P}_{(d)} = \mathcal{P}_{(d)}(X_1, \ldots, X_n)$ el espacio vectorial de las listas de polinomios $f = (f_1, \ldots, f_m)$ con coeficientes en $\mathbb{K}$ en las variables $\{X_1, \ldots, X_n\}$, de grados respectivos $\deg(f_i) \leq d_i, 1 \leq i \leq m$. Supongamos $\Omega = \mathcal{P}_{(d)} = \mathbb{A}^N(\mathbb{K})$ y sea $\Sigma \subseteq \Omega$ el discriminante de los sistemas $f = (f_1, \ldots, f_m)$ tales que $V_{\mathbb{A}}(f_1, \ldots, f_m)$ tiene dimensión mayor que $n - m$.*
Sea $N_{(d)}$ la dimensión de $\mathcal{P}_{(d)}$, i.e.,

$$N_{(d)} = \sum_{i=1}^{m} \binom{d_i + n}{n}.$$

Sean dados $s, d \in \mathbb{N}$ tales que

$$s \geq 6N_{(d)},$$
$$d \geq 2\left(\prod_{i=1}^{m}(d_i + 1)\right)^{6/5}.$$

Entonces, para cualquier variedad cero-dimensional $V \subseteq \mathbb{A}^n(\mathbb{K})$ dada por ecuaciones de grado a lo sumo d tal que su grado satisface

$$\deg(V) \geq d^{r+1},$$

se verifica la siguiente propiedad:
La probabilidad de que una elección aleatoria de puntos $\mathcal{Q} = (x_1, \ldots, x_s) \in V^s$ sea un conjunto cuestor para Ω sobre Σ está acotada inferiormente por

$$1 - \frac{1}{2^{5\dim(\Omega)}}.$$

DEMOSTRACIÓN. La única precisión a hacer es considerar

$$\begin{array}{rccc} ev: & \mathcal{P}_{(d)} \times \mathbb{A}^n(\mathbb{K}) & \longrightarrow & \mathbb{A}^m(\mathbb{K}) \\ & (f, \underline{x}) & \longmapsto & f(\underline{x}) \end{array}$$

y observar que el grado de las aplicaciones ev_i es $d_i + 1$ (i.e., $D_i = d_i + 1$). El resto se sigue de los resultados anteriores. □

Como se observa en [**HeSi, 80**], [**HeSc, 83**] o [**KrPa, 96**], un ejemplo natural de clases Ω de instancias a las que aplicar los conjuntos cuestores son los sistemas de ecuaciones dados en evaluación (i.e., mediante un programa, un esquema de evaluación o una red neuronal, que las evalúa). El lector puede acudir al Anexo B en el que se describen algunas propiedades de la clase $\Omega(\Gamma)$ asociada a un esquema de evaluación de talla L y profundidad ℓ. Como se observa en la proposición B.0.3, la clase $\Omega(\Gamma)$ es un constructible cuya clausura Zariski es una *variedad unirracional*.

DEFINICIÓN 11. *Una variedad algebraica $\Omega \subseteq \mathbb{A}^n(\mathbb{K})$ se denomina variedad unirracional si existen*

- *un espacio afín $\mathbb{A}^m(\mathbb{K})$, y*

- *una aplicación polinomial* $\varphi := (\varphi_1, \ldots, \varphi_n) : \mathbb{A}^m(\mathbb{K}) \longrightarrow \mathbb{A}^n(\mathbb{K})$

tales que $\Omega = \overline{\varphi(\mathbb{A}^m(\mathbb{K}))}^Z$.

Es decir, se trata de las clausuras Zariski de imágenes de variedades afines lineales por aplicaciones polinomiales. El siguiente resultado es obvio para variedades polinomiales en función de lo descrito en el Capítulo 1.

LEMA 3.1.6. *Sea* $\Omega \subseteq \mathbb{A}^n(\mathbb{K})$ *una variedad algebraica unirracional tal que* $\exists \varphi := (\varphi_1, \ldots, \varphi_n) : \mathbb{A}^m(\mathbb{K}) \longrightarrow \mathbb{A}^n(\mathbb{K})$ *con* $\Omega = \overline{\varphi(\mathbb{A}^m(\mathbb{K}))}^Z$. *Supongamos* $\deg(\varphi_i) \leq \Delta$ *para cada* i. *Entonces,*

i) Ω *es una variedad algebraica irreducible,*
ii) $\dim(\Omega) \leq m$,
iii) $\deg(\Omega) \leq \Delta^m$,
iv) si las fibras genéricas $\varphi^{-1}(y)$ *son finitas para* $y \in \Omega$, *entonces*

$$\deg(\Omega)^{1/\dim(\Omega)} \leq \Delta.$$

DEMOSTRACIÓN. Las propiedades *i)* y *ii)* son geometría algebraica elemental. Para la propiedad *iii)*, aplicando la Proposición 1.6.2, tenemos que

$$\deg(\Omega) = \deg\left(\overline{\varphi(\mathbb{A}^m(\mathbb{K}))}^Z\right) \leq \deg(\mathbb{A}^m(\mathbb{K}))(\max\{\deg(\varphi_1), \ldots, \deg(\varphi_n), 1\})^n \leq \Delta^n.$$

Para la propiedad *iv)*, nótese que el Teorema de la Dimensión en la Fibra indica que, genéricamente en Ω,

$$0 = \dim(\varphi^{-1}(\{y\})) = \dim(\mathbb{A}^m(\mathbb{K})) - \dim(\Omega),$$

con lo que $\dim(\Omega) = \dim(\mathbb{A}^m(\mathbb{K})) = m$ y la propiedad se sigue de modo obvio. □

En el caso de variedades unirracionales, el Teorema 3.1.3 se transforma en el siguiente:

COROLARIO 3.1.7. *Con las notaciones precedentes, sea* $\Omega \subseteq \mathbb{A}^N(\mathbb{K})$ *un constructible unirracional, es decir, sea dada una aplicación polinomial*

$$\varphi := (\varphi_1, \ldots, \varphi_N) : \mathbb{A}^u(\mathbb{K}) \longrightarrow \mathbb{A}^N(\mathbb{K})$$

de tal modo que $\Omega = \overline{\varphi(\mathbb{A}^u(\mathbb{K}))}^Z$, *y sea* $\Delta = \max\{\deg(\varphi_i) : 1 \leq i \leq N\}$. *Sea* $ev : \mathbb{A}^N(\mathbb{K}) \times \mathbb{A}^n(\mathbb{K}) \longrightarrow \mathbb{A}^m(\mathbb{K})$ *una aplicación polinomial con variedad de incidencia sobre* Ω *dad mediante*

$$V(\Omega) := \{(f, x) \in \Omega \times \mathbb{A}^n(\mathbb{K}) : ev(f, x) = 0\}.$$

Supongamos que $ev = (ev_1, \ldots, ev_m)$ *son polinomios con*

$$D_i := \deg(ev_i), 1 \leq i \leq m,$$

$$d_i := \deg_X(ev_i), 1 \leq i \leq m.$$

Supongamos, finalmente, que las fibras $\varphi^{-1}(\{y\}) \subseteq \mathbb{A}^u(\mathbb{K})$ *son genéricamente finitas (o, equivalentemente,* $\dim(\Omega) = u$*).*
Sean $s, d \in \mathbb{N}$ *enteros positivos verificando*

$$s \geq 6 \dim(\Omega) = 6u,$$

$$d \geq 2\left(\Delta\left(\prod_{i=1}^{m} D_i\right)^6\right)^{1/5}.$$

Entonces, para cualquier variedad cero-dimensional $V \subseteq \mathbb{A}^n(\mathbb{K})$ *dada por ecuaciones de grado a lo sumo* d *tal que*

$$\deg(V) \geq d^{n+1}$$

se verifica la siguiente propiedad:
La probabilidad de que una elección aleatoria de puntos $\mathcal{Q} = (x_1, \ldots, x_s) \in V^s$ *sea un conjunto cuestor para* Ω *sobre* Σ *está acotada inferiormente por*

$$1 - \frac{1}{2^{5\dim(\Omega)}}.$$

Dado un esquema de evaluación de polinomios Γ sobre un cuerpo $\mathbb{K}$ en las variables $\{X_1, \ldots, X_n\}$, podemos mirar los nodos de mayor profundidad como nodos de output (ver Anexo B para más detalles). Así, un SLP Γ de talla L, profundidad ℓ y m nodos de output (profundidad máxima) define una aplicación polinomial

$$\begin{array}{rccl} \Gamma: & \mathbb{A}^N(\mathbb{K}) & \longrightarrow & \mathcal{P}_{(2^\ell)}(X_1, \ldots, X_n) \\ & (\underline{\alpha}, \underline{\beta}) & \longmapsto & (Q_{\ell,1}(\underline{\alpha}, \underline{\beta}, X_1, \ldots, X_n), \ldots, Q_{\ell,m}(\underline{\alpha}, \underline{\beta}, X_1, \ldots, X_n)), \end{array}$$

donde $N = 2L(L-(n+1))$ es el número total de parámetros, $Q_{\ell,j}(\underline{\alpha}, \underline{\beta}, X_1, \ldots, X_n)$ es el j-ésimo polinomio evaluado en profundidad ℓ, de grado (en las variables $\{X_1, \ldots, X_n\}$) a lo sumo 2^ℓ y $(2^\ell) = (2^\ell, \ldots, 2^\ell) \in \mathbb{N}^m$. Denotemos por $\Omega(\Gamma)$ el constructible dado como la imagen de Γ y, por la Proposición B.0.3, tendremos que $\overline{\Omega(\Gamma)}^Z$ es irreducible y verifica

$$\dim(\Omega(\Gamma)) \leq N, \ \deg\left(\overline{\Omega(\Gamma)}^Z\right) \leq (2^{\ell+1} - 2)^N.$$

Corolario 3.1.8. *Con las notaciones anteriores, sea Γ un SLP de talla L, profundidad ℓ y parámetros en un cuerpo $K \subseteq \mathbb{K}$ y variables $\{X_1, \ldots, X_n\}$ y m nodos de output. Sea $\Omega(\Gamma)$ el constructible de las listas de polinomios evaluables por Γ. Supongamos que Γ preserva la dimensión del espacio de parámetros (i.e., $\dim(\Omega(\Gamma)) = N$) y supongamos que la dimensión de la variedad algebraica afín $V_{\mathbb{A}}(f)$, con $f \in \Omega(\Gamma)$ es genéricamente igual a $m - n$. Sea $\Sigma \subseteq \Omega(\Gamma)$ el discriminante para la dimensión.*
Sean $s, d \in \mathbb{N}$ enteros positivos verificando

$$s \geq 6 \dim(\Omega(\Gamma)) = 12L(L - (n+1)),$$

$$d \geq 2\left((2^{\ell-1} - 2) \cdot (2^\ell + 1)^6 m\right)^{1/5}.$$

Entonces, para cualquier variedad cero-dimensional $V \subseteq \mathbb{A}^n(\mathbb{K})$ dada por ecuaciones de grado a lo sumo d tal que

$$\deg(V) \geq d^{n-m+1}$$

se verifica la siguiente propiedad:
La probabilidad de que una elección aleatoria de puntos $\mathcal{Q} = (x_1, \ldots, x_s) \in V^s$ sea un conjunto cuestor para $\Omega(\Gamma)$ sobre Σ está acotada inferiormente por

$$1 - \frac{1}{2^{5N}}.$$

3.2. Conjuntos cuestores en acción: "Suite Sécante" $\in \mathbf{BPP}_K$ por mera evaluación

Originalmente, los estudios sobre conjuntos cuestores en [**HeSc, 83**] trataban de analizar tests de nulidad de polinomios. Ahora vamos a ver cómo esta misma ideología permite desarrollar algoritmos para detectar sucesiones secantes de polinomios con ceros afines.

Definición 12 (**Suites sécantes**). *Consideremos $P_d(X_1, \ldots, X_n) := \{f \in \mathbb{K}[X_1, \ldots, X_n] : \deg(f) \leq d\}$ y consideremos $m \in \mathbb{N}, 1 \leq m \leq n$ y una lista de grados $(d) = (d_1, \ldots, d_m)$. Denotemos por $\mathcal{P}_{(d)}$ la clase de listas de polinomios asociada a la lista (d):*

$$\mathcal{P}_{(d)} = \prod_{i=1}^{m} P_{d_i}(X_1, \ldots, X_n).$$

Una lista $f = (f_1, \ldots, f_m) \in \mathcal{P}_{(d)}$ se dice suite secante (sucesión secante) si la variedad afín de sus ceros comunes $V_{\mathbb{A}}(f) = V_{\mathbb{A}}(f_1, \ldots, f_m)$ es una variedad algebraica de dimensión $n - m$.

Observación 3.2.1.
i) Un ejemplo típico de suite sécante se sigue del caso de las sucesiones regulares de polinomios (discutidas en el Anexo A).
ii) De otro lado, el Teorema "de la Pureza" de Macaulay nos dice que si $f_1, \ldots, f_m$ es una suite sécante, entonces todas las componentes irreducibles de la variedad $V_{\mathbb{A}}(f_1, \ldots, f_m)$ son de dimensión $n - m$ ("unmixed" o "puras").
iii) Existe un abierto Zariski $\Omega_0 \subseteq \mathcal{P}_{(d)}$ tal que para cada $f \in \Omega_0, f = (f_1, \ldots, f_m)$ es una suite sécante.
iv) Existe una variedad algebraica propia $\mathcal{N} \subseteq \mathcal{P}_{(d)}$ de tal modo que $V_{\mathbb{A}}(f) = \emptyset$ si y sólo si $f \in \mathcal{P}_{(d)} \setminus \mathcal{N}$.

Supongamos dado un esquema de evaluación Γ de talla L, profundidad ℓ con m nodos de output en profundidad ℓ y tal que evalúa polinomios en las variables $\{X_1, \ldots, X_n\}$. Sea $N = 2L(L - (n+1))$ el

número total de parámetros. Consideremos la aplicación polinomial que define a partir de sus nodos de output:

$$\Gamma : \mathbb{A}^N(\mathbb{K}) \longrightarrow \mathcal{P}^{\mathbb{K}}_{2^\ell}(X_1, \ldots, X_n),$$

donde $\mathbb{K}$ es un cuerpo algebraicamente cerrado de característica cero, $(2^\ell) = (2^\ell, \ldots, 2^\ell) \in \mathbb{N}^m$. Denotemos por $\Omega(\Gamma)$ la imagen de Γ, que es un constructible con clausura Zariski irreducible y tal que

$$\dim(\Omega(\Gamma)) \leq N,\ \deg(\Omega(\Gamma)) \leq (2^{\ell-1} - 2)^N.$$

Consideremos ahora una lista de grados $(d) = (d_1, \ldots, d_m)$ y el $\mathbb{K}$-espacio vectorial $\mathcal{P}^{\mathbb{K}}_{(d)}$ de las listas de polinomios $f = (f_1, \ldots, f_m)$ tales que $f_i \in \mathbb{K}[X_1, \ldots, X_n], \deg(f_i) \leq d_i$ para cada $i, 1 \leq i \leq m$.
Denotemos por $\Omega_{(d)}(\Gamma) = \Omega(\Gamma) \cap \mathcal{P}^{\mathbb{K}}_{(d)}$ la clase de las listas de polinomios en $\mathcal{P}^{\mathbb{K}}_{(d)}$ que son evaluables por Γ. Dependiendo de la relación de d_i con 2^ℓ, podríamos entender esta intersección bien como intersección con una variedad lineal (si $2^\ell \geq d_i$) o bien como un mero contenido (si $d_i \geq 2^\ell$). En cualquier caso, es claro que tenemos

Proposición 3.2.2. *Con las notaciones precedentes,*

i) $\dim(\Omega_{(d)}(\Gamma)) \leq N = 2L(L - (n+1))$,
ii) $\deg(\Omega_{(d)}(\Gamma)) \leq (2^{\ell-1} - 2)^N$.

Para un entero positivo $s \in \mathbb{N}$, podemos definir la variedad de incidencia

$$W^{(s)}_{(d)}(\Gamma) := \{(f, \underline{x}_1, \ldots, \underline{x}_s) \in \Omega_{(d)}(\Gamma) \times (\mathbb{A}^n(\mathbb{K}))^s : f(\underline{x}_i) = 0, 1 \leq i \leq s\}.$$

Se tiene:

Proposición 3.2.3. *Con las notaciones precedentes, se tiene*

$$\deg\left(W^{(s)}_{(d)}(\Gamma)\right) \leq \deg(\Omega_{(d)}(\Gamma)) \cdot \left(\prod_{i=1}^{m}(d_i + 1)\right)^s.$$

Demostración. Es una mera aplicación de la Desigualdad de Bézout. □

Consideremos, como en casos anteriores, las dos proyecciones canónicas

$$\pi_1 : W^{(s)}_{(d)}(\Gamma) \longrightarrow \Omega_{(d)}(\Gamma),$$

$$\pi_2 : W^{(s)}_{(d)}(\Gamma) \longrightarrow (\mathbb{A}^n(\mathbb{K}))^s.$$

Añadamos la siguiente hipótesis de dimensionalidad: supongamos que existe $\Sigma \subseteq \Omega_{(d)}(\Gamma)$ una subvariedad propia tal que

i) para cada $f \in \Omega_{(d)}(\Gamma) \setminus \Sigma$, f es una "suite sécante" (i.e., $V_{\mathbb{A}}(f) \neq \emptyset$ es de dimensión $n - m$),
ii) para cada $f \in \Sigma$, $V_{\mathbb{A}}(f)$ es o bien vacío o de dimensión mayor o igual que $n - m + 1$.

Proposición 3.2.4. *Con las notaciones precedentes, sea $\mathcal{C}$ el conjunto de las componentes irreducibles C de $W^{(s)}_{(d)}(\Gamma)$ tales que $\pi_1(C) \setminus \Sigma \neq \emptyset$. Definamos*

$$B := \bigcup_{C \in \mathcal{C}} C \subseteq W^{(s)}_{(d)}(\Gamma).$$

Se verifica:

i) $\dim(B) \leq N + s(n - m)$.
ii) El grado de B está acotado por el grado de $W^{(s)}_{(d)}(\Omega)$. Lo mismo sucede para $\sharp(\mathcal{C})$.

Demostración. La afirmación *ii)* es obvia porque B está formado por componentes irreducibles de $W^{(s)}_{(d)}(\Gamma)$.
Para la propiedad *i)* usemos, una vez más, el Teorema de la Dimensión en la Fibra. Si $f \in \pi_1(C) \setminus \Sigma$, tendremos

$$s(n - m) = \dim(\pi_1^{-1}(\{f\})) \geq \dim(C) - \dim(\Omega_{(d)}(\Gamma))$$

y la desigualdad se sigue de manera obvia. □

ALGORITMO 3.2.5 (**Detección de "suites sécantes" por mera evaluación**).

INPUT: *-Un esquema de evaluación* Γ *de talla* L *y profundidad* ℓ*, con* m *nodos de output en las variables* $\{X_1, \ldots, X_n\}$

-Una lista de grados $(d) = (d_1, \ldots, d_m)$

-Parámetros $\underline{\alpha}, \underline{\beta} \in \mathbb{K}^N$ *para* Γ *que permiten evaluar una lista* $f = (f_1, \ldots, f_m) \in \mathcal{P}_{(d)}$

initialize $s := 6N = 12(L(L-(n+1)))$

$u \in \mathbb{N}$ *un entero positivo tal que*

$$u > 2\left((2^{\ell+1}-1)^{1/6}\prod_{i=1}^{m}(d_i+1)\right)^{\frac{1}{m-1/6}}$$

$V := \{1, \ldots, u\}^n$

guess at random $\mathcal{Q} := (\underline{x}_1, \ldots, \underline{x}_s) \in V^s$

eval $f(\underline{x}_1), \ldots, f(\underline{x}_s)$

if $\exists i, 1 \leq i \leq s$ *con* $f(\underline{x}_i) \neq 0$,

OUTPUT **probablemente es una "suite sécante"**

else OUTPUT **probablemente no es una "suite sécante"**

end

TEOREMA 3.2.6. *Con las notaciones precedentes, el anterior algoritmo probabilista decide en tiempo cúbico (número de operaciones aritméticas)*

$$O(L^3)$$

si el input dado es una sucesión secante. El algoritmo pertenece a la clase $\mathbf{BPP}_K$*, y la probabilidad de error está acotada superiormente por*

$$\frac{1}{2^s} = \frac{1}{2^{6N}} = \frac{1}{2^{12(L(L-(n+1)))}}.$$

DEMOSTRACIÓN. Obsérvese que la probabilidad de error del algoritmo está acotada por la probabilidad de que la lista $\mathcal{Q} := (\underline{x}_1, \ldots, \underline{x}_s) \in (\{1, \ldots, u\}^n)^s$ no sea un conjunto cuestor. Retomemos la prueba ya discutida en varias ocasiones, adaptada a este caso. Se tiene que la probabilidad de que $\mathcal{Q}$ no sea un conjunto cuestor está acotada por

$$\frac{\sharp(B')}{u^{ns}} = \frac{\sharp(B')}{\sharp(V)^s},$$

donde $B' = \pi_2(B) \cap V^s$ con B como aparece definido en la Proposición 3.2.4 anterior. Como B' es cero-dimensional,

$$\sharp(B') = \deg(B') \leq \deg\left(\overline{\pi_2(B)}^Z \cap V^s\right) \leq \deg(B) \cdot u^{\dim(B)}.$$

Por tanto,

$$\frac{\sharp(B')}{u^{ns}} \leq \frac{(2^{\ell+1}-2)^N \cdot (\prod_{i=1}^m (d_i+1))^s \cdot u^{N+(n-m)s}}{u^{ns}},$$

luego

$$\frac{\sharp(B')}{u^{ns}} \leq \frac{(2^{\ell+1}-2)^{s/6} \cdot (\prod_{i=1}^m (d_i+1))^s}{u^{(m-1/6)s}}.$$

Es decir,

$$\frac{\sharp(B')}{u^{ns}} \leq \frac{\left((2^{\ell+1}-2)^{1/6} \cdot \prod_{i=1}^m (d_i+1)\right)^s}{u^{(m-1/6)s}} \leq \left(\frac{(2^{\ell+1}-2)^{1/6} \cdot \prod_{i=1}^m (d_i+1)}{u^{(m-1/6)s}}\right)^s.$$

Como hemos supuesto $u \geq 2\left((2^{\ell+1}-2)^{1/6} \cdot \prod_{i=1}^{m}(d_i+1)\right)^{1/(m-1/6)}$, tenemos el control de la probabilidad de error con

$$\frac{\sharp(B')}{u^{ns}} \leq \frac{1}{2^s} = \frac{1}{2^{6N}}.$$

□

OBSERVACIÓN 3.2.7. Hemos optado por escribir el algoritmo en el caso de característica cero por simplificar la presentación de la variedad V donde elegimos el conjunto cuestor $\mathcal{Q}$ de manera aleatoria. En caso de característica positiva deberíamos adaptar la elección de V buscando, por ejemplo, polinomios ciclotómicos. Nótese que, en todo caso, la elección aleatoria en característica cero se hace usando números enteros cuya talla es polinomial en el tamaño de la entrada. Suponiendo $m \geq 1$ y eligiendo

$$u = 2\left(\left(2^{\ell+1}-2\right)^{1/6}\prod_{i=1}^{m}(d_i+1)\right)^{6/5}$$

nos quedaría que la talla bit de las coordenadas de cualquier punto está acotada por la desigualdad

$$5/6\log_2(u) \leq (\ell+1) + m\max\{\log_2(d_i+1)\},$$

lo cual se corresponde con la polinomialidad del algoritmo.

Si $m = 1$ la condición de ser sucesión secante equivale a ser no nulo y no constante. Así, tenemos el siguiente Corolario, que ya está presente en [**HeSc, 83**]:

COROLARIO 3.2.8. *En el caso $m = 1$, el anterior algoritmo prueba que el conjunto de los polinomios evaluables por un esquema de evaluación de talla dada que son no nulos es un problema en $\mathbf{RP}_K$. Si f es un polinomio no nulo, el algoritmo devuelve "Probablemente no nulo" con probabilidad mayor que*

$$1 - \frac{1}{2^{6N}} > 2/3.$$

DEMOSTRACIÓN. Dejamos al lector la adaptación del Algoritmo 3.2.5 al problema de los tests de nulidad de polinomios dados por esquemas de evaluación. De hecho, basta con reemplazar m por 1 y "suite sécante" por "no nulo" en el texto de ese algoritmo. En cuanto al análisis del error, es claro que si Γ evalúa $f = 0$ con parámetros $\underline{\alpha}, \underline{\beta}$, entonces el algoritmo devuelve "Probablemente nulo" sea quien sea el $\mathcal{Q} \in V^s$ elegido. En cambio, si Γ evalúa $f \neq 0$ con parámetros $\underline{\alpha}, \underline{\beta}$, el error sólo se produce si el $\mathcal{Q}$ elegido no es un conjunto cuestor, por lo que la probabilidad de error estará acotada por $1/2^s$. □

3.3. El caso de ecuaciones homogéneas y la intersección

En la Sección precedente hemos introducido un algoritmo de la clase $\mathbf{BPP}_K$ para la detección de sucesiones secantes por mera evaluación en un conjunto cuestor de talla apropiada. En esta Sección vamos a explorar la posibilidad de detectar la condición de ser "suite sécante" mediante algoritmos del tipo MONTECARLO. Perderemos la condición de trabajar solamente en evaluación. Ahora tendremos que enfrentarnos a realizar llamadas al Nullstellensatz de Hilbert (**HN**). La idea pasa por considerar ecuaciones de entrada homogéneas y tomar al azar puntos en la variedad de Grassmann de "dimensión inapropiada". El algoritmo pasará a una clase probabilista más reducida ($\mathbf{RP}_K$) pero requiere oráculos que decidan el Nullstellensatz de Hilbert.

Sea $m \in \mathbb{N}$ un entero positivo, $m \geq 1$, y sea $(d) = (d_1, \ldots, d_m)$ una lista de grados. Denotaremos por $(1) = (1, \ldots, 1)$ a cualquier lista de grados 1 (i.e., formas lineales), donde el número de 1's que aparecen en esta lista se sobreentenderá usualmente por el contexto. Para una lista de grados (d) llamaremos $\mathcal{H}^{(K,m)}_{(d)}(X_0, \ldots, X_n)$ (o, simplemente, $\mathcal{H}^{(m)}_{(d)}$) al K-espacio vectorial

$$\mathcal{H}^{(m)}_{(d)} := \mathcal{H}^{(K,m)}_{(d)}(X_0, \ldots, X_n) := \prod_{i=1}^{m} H^K_{d_i}(X_0, \ldots, X_n),$$

donde el cuerpo K y el número de variables se sobreentienden. Como en secciones precedentes, llamaremos $V_{\mathbb{P}}(f) \subseteq \mathbb{P}_n(\mathbb{K})$ a la variedad proyectiva K-definible, con coordenadas homogéneas en $\mathbb{K}$, formada por los ceros comunes a las ecuaciones $f_1 = 0, \ldots, f_m = 0$.

Para el caso $(d) = (1)$, consideraremos la clase $\mathcal{H}^{(m)}_{(d)}$ de matrices siguiente:

$$\mathcal{H}^{(m)}_{(1)} := \mathcal{H}^{(\mathbb{K},m)}_{(1)}(X_0, \ldots, X_n) = \prod_{i=1}^{m} H^{\mathbb{K}}_1(X_0, \ldots, X_n) = \mathcal{M}_{m\times m}(\mathbb{K}).$$

Para cada matriz (o lista) $L \in \mathcal{H}^{(m)}_{(1)}$, denotaremos por $V_{\mathbb{P}}(L)$ a la variedad proyectiva lineal en $\mathbb{P}_n(\mathbb{K})$ definida mediante

$$V_{\mathbb{P}}(L) := \left\{ \underline{x} = (x_0 : \ldots : x_n) \in \mathbb{P}_n(\mathbb{K}) : L \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \right\}.$$

Genéricamente en $\mathcal{H}_{(1)}^{(m)}$, la dimensión de $V_{\mathbb{P}}(L)$ es $n-m$. En otras palabras, existe un abierto Zariski en $\mathcal{H}_{(1)}^{(m)}$ dado mediante

$$\mathcal{G}_{n,n-m} := \{L \in \mathcal{H}_{(1)}^{(m)} : \dim(V_{\mathbb{P}}(L)) = n-m\}.$$

En particular, si $\mathbb{G}_{n,n-m}$ es la variedad de Grassmann, la siguiente es una aplicación suprayectiva:

$$\begin{array}{ccc} \mathcal{G}_{n,n-m} & \longrightarrow & \mathbb{G}_{n,n-m} \\ L & \longmapsto & V_{\mathbb{P}}(L). \end{array}$$

De hecho, el abierto Zariski $\mathcal{G}_{n,n-m} \subseteq \mathcal{H}_{(1)}^{(m)}$ se caracteriza como el conjunto de las matrices tales que poseen una coordenada de Plücker (i.e., un menor $m\times m$) no nula.
Sea ahora $\Omega \subseteq \mathcal{H}_{(d)}^{(m)}$ un conjunto algebraico irreducible (de sistemas de ecuaciones polinomiales) con coeficientes en un cuerpo $\mathbb{K}$ algebraicamente cerrado, y sea $s \geq 1$ un número entero. Definamos el conjunto algebraico en $\mathcal{H}_{(d)}^{(m)} \times (\mathcal{G}_{n,m-1})^s$ dado mediante la siguiente identidad

$$V_{\mathcal{G}}^{(s)}(\Omega) := \{(f, L_1, \ldots, L_s) \in \Omega \times (\mathcal{G}_{n,m-1})^s : V_{\mathbb{P}}(f) \cap V_{\mathbb{P}}(L_i) \neq \emptyset, 1 \leq i \leq s\}.$$

Supongamos que existe $\Sigma \subseteq \Omega$ una subvariedad propia (de co-dimensión ≥ 1) tal que se satisfacen las siguientes dos propiedades:

i) $\forall f \in \Omega \setminus \Sigma, \dim(V_{\mathbb{P}}(f)) = n-m$,
ii) $\forall f \in \Sigma, \dim(V_{\mathbb{P}}(f)) \geq n-m+1$.

Tenemos la siguiente primera propiedad, análoga a la que encontrábamos en el caso afín.

PROPOSICIÓN 3.3.1. *Sea $\pi_1 : \mathcal{H}_{(d)}^{(m)} \times (\mathcal{G}_{n,m-1})^s \longrightarrow \mathcal{H}_{(d)}^{(m)}$ la proyección canónica que "olvida" las componentes en las ecuaciones que definen puntos en la variedad de Grassmann. Sea C una componente irreducible de $V_{\mathcal{G}}^{(s)}(\Omega)$ tal que $\pi_1(C) \setminus \Sigma \neq \emptyset$. Entonces,*

$$\dim(C) \leq \dim(\Omega) + s\left(\dim(\mathcal{G}_{n,m-1}) - 1\right).$$

DEMOSTRACIÓN. Sigue la misma pauta de usar el Teorema de la Dimensión en la Fibra. Así, como $\pi_1(C) \setminus \Sigma \neq \emptyset$, existe $f \in \pi_1(C)$ tal que $f \notin \Sigma$. Entonces considerando $\pi = \pi_1|_C$ como la restricción a C de la proyección π_1, tendremos

$$\dim(\pi^{-1}(\{f\})) \geq \dim(C) - \dim\left(\overline{\pi(C)}^Z\right).$$

Como $\overline{\pi(C)}^Z \subseteq \Omega$, concluimos fácilmente que

$$\dim(C) \leq \dim(\pi^{-1}(\{f\})) + \dim(\Omega). \tag{3.3.1}$$

De otro lado, como $f \notin \Sigma$, tenemos que la dimensión de $V_{\mathbb{P}}(f)$ satisface

$$\dim(V_{\mathbb{P}}(f)) = n-m.$$

Entonces, existe un abierto Zariski $U(f) \subseteq \mathcal{G}_{n,m-1}$ tal que

$$\forall L \in U(f), V_{\mathbb{P}}(f) \cap V_{\mathbb{P}}(L) = \emptyset.$$

El abierto Zariski $U(f)$ se puede caracterizar ecuacionalmente usando la resultante multivariada como

$$U(f) := \{L \in \mathcal{G}_{n,m-1} : \mathrm{Res}(f, L) \neq 0\}.$$

Ahora, como $\mathcal{G}_{n,m-1}$ es un abierto Zariski en un irreducible, el cerrado Zariski $Z(f) := \mathcal{G}_{n,m-1} \setminus U(f)$ verifica $\pi^{-1}(\{f\}) \subseteq \{f\} \times Z(f)^s$. Además $\dim(Z(f)) \leq \dim\left(\mathcal{G}_{n,m-1}\right) - 1$, por lo que tendremos

$$\dim(\pi^{-1}(\{f\})) \leq s\left(\dim\left(\mathcal{G}_{n,m-1}\right) - 1\right).$$

Combinando esta desigualdad con la desigualdad (3.3.1) precedente habremos concluido la demostración de la Proposición. □

En lo que concierne al grado, observamos la siguiente propiedad:

PROPOSICIÓN 3.3.2. *Con las notaciones precedentes, se tiene que*

$$\deg\left(\overline{V_{\mathcal{G}}^{(s)}(\Omega)}^Z\right) \leq \deg(\Omega)\left(\prod_{i=1}^{m}(d_i+1)2^{n-m+1}\right)^s.$$

Demostración. Para empezar, consideremos la siguiente variedad quasi-proyectiva:

$$\widetilde{V}_{\mathcal{G}}^{(s)}(\Omega) := \left\{(f, \underline{x}_1, \ldots, \underline{x}_s, L_1, \ldots, L_s) \in \Omega \times \mathbb{P}_n(\mathbb{K})^s \times \mathcal{G}_{n,m-1}^s : \underline{x}_i \in V_{\mathbb{P}}(f) \cap V_{\mathbb{P}}(L_i), 1 \leq i \leq s\right\}.$$

Ahora observemos que $\widetilde{V}_{\mathcal{G}}^{(s)}(\Omega)$ viene dada por las ecuaciones

i) $f = (f_1, \ldots, f_m) \in \Omega$,
ii) $f_k(\underline{x}_i) = 0, 1 \leq k \leq m, 1 \leq i \leq s$ (ecuaciones de grados respectivos $d_1 + 1, \ldots, d_m + 1$),
iii) $L_i \underline{x}_i = 0, 1 \leq i \leq s$ (ecuaciones de grado 2). Nótese que $L_i \underline{x}_i$ son $n - m + 1$ ecuaciones.

Por tanto,

$$\deg\left(\widetilde{V}_{\mathcal{G}}^{(s)}(\Omega)\right) \leq \deg(\Omega) \left(\prod_{i=1}^{m}(d_i + 1)\right)^s 2^{s(n-m+1)}.$$

Ahora, consideremos $p : \mathcal{H}_{(d)}^{(m)} \times \mathbb{P}_n(\mathbb{K})^s \times \mathcal{G}_{n,m-1}^s \longrightarrow \mathcal{H}_{(d)}^{(m)} \times \mathcal{G}_{n,m-1}^s$ la proyección que "olvida" las coordenadas en $\mathbb{P}_n(\mathbb{K})^s$. Entonces observamos que $V_{\mathcal{G}}^{(s)}(\Omega) = p\left(\widetilde{V}_{\mathcal{G}}^{(s)}(\Omega)\right)$, por lo que

$$\deg\left(\overline{V_{\mathcal{G}}^{(s)}(\Omega)}^Z\right) \leq \deg\left(\widetilde{V}_{\mathcal{G}}^{(s)}(\Omega)\right) \leq \deg(\Omega) \left(\prod_{i=1}^{m}(d_i + 1)2^{n-m+1}\right)^s,$$

como habíamos enunciado. □

Definición 13. *Dados Ω y Σ como en páginas precedentes, llamaremos* conjunto cuestor módulo **HN** (CTS mod **HN**) *a toda sucesión de puntos*

$$\mathcal{Q} = (L_1, \ldots, L_s) \in (\mathcal{M}_{(n-m+1)\times(n+1)}(\mathbb{K}))^s$$

de tal modo que $\forall f \in \Omega$, se verifica

$$f \in \Sigma \Longleftrightarrow \forall i, V_{\mathbb{P}}(L_i) \cap V_{\mathbb{P}}(f) \neq \emptyset.$$

Teorema 3.3.3. *Sean Ω y Σ conjuntos constructibles satisfaciendo las hipótesis precedentes. Supongamos $\Omega \subseteq \mathcal{H}_{(d)}^{(m)}$, con $(d) = (d_1, \ldots, d_m)$ y sea*

$$D := \max\{d_1, \ldots, d_m\}.$$

Sean $s, d \in \mathbb{N}$ verificando

$$s \geq 6 \dim(\Omega),$$

$$d \geq 2\left(\deg(\Omega)^{1/3\dim(\Omega)} \left(\prod_{i=1}^{m}(d_i + 1)2^{n-m+1}\right)^2\right).$$

Sea $N = (n-m+1)(n-1)$. Entonces, para cualquier variedad algebraica cero-dimensional $V \subseteq \mathbb{A}^N(\mathbb{K}) = \mathcal{M}_{(n-m+1)\times(n+1)}(\mathbb{K})$ dada por polinomios de grado a lo sumo d de tal modo que

$$\deg(V) \geq d^{N-1/2},$$

se verifica:
La probabilidad de que una elección aleatoria de puntos $\mathcal{Q} = (L_1, \ldots, L_s) \in V^s$ sea un conjunto cuestor módulo **HN** *para Ω con respecto a Σ es mayor o igual que*

$$1 - \frac{1}{2^{3\dim(\Omega)}}.$$

Demostración. La demostración es análoga a la del Teorema 3.1.3. Utilizaremos las dos Proposiciones precedentes. Consideramos las dos proyecciones naturales:

$$\pi_1 : V_{\mathcal{G}}^{(s)}(\Omega) \longrightarrow \Omega,$$

$$\pi_2 : V_{\mathcal{G}}^{(s)}(\Omega) \longrightarrow (\mathcal{G}_{n,m-1})^s,$$

y consideremos la clase $\mathcal{C}$ de componentes irreducibles C de $V_{\mathcal{G}}^{(s)}(\Omega)$ tales que $\overline{\pi_1(C)}^Z \setminus \Sigma \neq \emptyset$. Definamos $B := \bigcup_{C \in \mathcal{C}} C \subseteq V_{\mathcal{G}}^{(s)}(\Omega)$. Tendremos, por una parte,

$$\deg(B) \leq \deg\left(\overline{V_{\mathcal{G}}^{(s)}(\Omega)}^Z\right) \leq \deg(\Omega) \left(\prod_{i=1}^{m}(d_i + 1)2^{n-m+1}\right)^s,$$

mientras que la dimensión de cualquier componente irreducible $C \in \mathcal{C}$ está acotada y podemos concluir

$$\dim(B) \leq \max\{\dim(C) : C \in \mathcal{C}\} \leq \dim(\Omega) + s(\dim(\mathcal{G}_{n,m-1}) - 1),$$

es decir,

$$\dim(B) \leq \dim(\Omega) + s(N-1).$$

Definamos la intersección $B' := B \cap (\mathcal{H}_{(d)}^{(m)} \times V^s)$ donde V es una variedad cero-dimensional que satisface las hipótesis del enunciado. Entonces, por la Proposición 1.6.1 se tiene $\deg(B') \leq \deg(B) \cdot d^{\dim(B)}$.
En particular,

$$\deg(B') \leq \deg(\Omega) \left(\prod_{i=1}^{m} (d_i + 1) 2^{n-m+1} \right)^s \cdot d^{\dim(\Omega)+s(N-1)}.$$

Ahora, como en el Teorema 3.1.3, si una lista $(L_1, \ldots, L_s) \in V^s$ no es una CTS mod **HN** para Ω con respecto a Σ, entonces existirá $f \in \Omega \setminus \Sigma$ tal que

$$V_{\mathbb{P}}(f) \cap V_{\mathbb{P}}(L_i) \neq \emptyset, \forall i, 1 \leq i \leq s.$$

Entonces, $(f, L_1, \ldots, L_s)$ estará en alguna componente irreducible $C \in \mathcal{C}$ de $V_{\mathcal{G}}^{(s)}(\Omega)$ porque $f \in \overline{\pi_1(C)}^Z \setminus \Sigma \neq \emptyset$. Así, $(f, L_1, \ldots, L_s) \in B'$ y, por tanto, $(L_1, \ldots, L_s) \in \pi_2(B') \subseteq V^s$.
Como V es una variedad cero-dimensional y, por tanto, es un conjunto finito, el constructible $\pi_2(B')$ es una variedad algebraica cero-dimensional y tendremos, por la Proposición 1.6.2 que se verifica

$$\sharp(\pi_2(B')) = \deg(\pi_2(B')) = \deg\left(\overline{\pi_2(B')}^Z\right) \leq \deg(B').$$

En conclusión, la probabilidad de que una lista $\mathcal{Q} = (L_1, \ldots, L_s) \in V^s$ no sea una sucesión correcta de test módulo **HN** para Ω con respecto a Σ está acotada por

$$\frac{\deg(\pi_2(B'))}{\deg(V)^s}.$$

Usando las cotas obtenidas anteriormente tendremos que la probabilidad de que una lista $\mathcal{Q} = (L_1, \ldots, L_s)$ no sea una CTS mod **HN** para Ω con respecto a Σ está acotada por

$$\begin{aligned}
\frac{\deg(\pi_2(B'))}{\deg(V)^s} &\leq \frac{\deg(\Omega) \left(\prod_{i=1}^{m} (d_i+1) 2^{n-m+1}\right)^s \cdot d^{\dim(\Omega)+s(N-1)}}{d^{s(N-1/2)}} \\
&\leq \frac{\deg(\Omega) \left(\prod_{i=1}^{m} (d_i+1) 2^{n-m+1}\right)^s \cdot d^{\dim(\Omega)}}{d^{s/2}} \\
&\leq \frac{\left(\deg(\Omega)^{1/\dim(\Omega)} \left(\prod_{i=1}^{m} (d_i+1) 2^{n-m+1}\right)^6\right)^{\dim(\Omega)}}{d^{3\dim(\Omega)}}.
\end{aligned}$$

Ahora, como

$$d \geq 2 \left(\deg(\Omega)^{1/3\dim(\Omega)} \prod_{i=1}^{m} (d_i+1) 2^{n-m+1} \right)^2,$$

tenemos que

$$\frac{\deg(\pi_2(B'))}{\deg(V)^s} \leq \frac{1}{2^{3\dim(\Omega)}},$$

lo que demuestra el resultado enunciado. □

APÉNDICE A

Algunas propiedades sobre la dimensión de Krull

En su trabajo clásico sobre la teoría de ideales, W. Krull[1] introduce una sencilla noción de dimensión fácilmente transportable a espacios topológicos noetherianos (como $\mathbb{A}^n(\mathbb{K})$ y $\mathbb{P}_n(\mathbb{K})$ con las respectivas topologías de Zariski). Aquí resumiremos unas pocas de las propiedades que usaremos a lo largo de la memoria. Las referencias básicas son clásicos como [**AtMc, 96**], [**Ku, 85**], [**RaSiSr, 75**] o [**Shf, 74**].

DEFINICIÓN 14 (Dimensión de Krull). *Dado un espacio topológico noetheriano $(X, \mathscr{T})$ y un cerrado $F \subseteq X$, llamaremos* dimensión de Krull de F *y denotaremos por* $\dim_K(F)$ *al máximo de las longitudes de cadenas de cerrados irreducibles contenidos en F, i.e., el máximo de los $r \in \mathbb{N}$ tales que existen*

$$V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_r \subseteq F,$$

con $V_i \subseteq X$ cerrado irreducible. Diremos que $\dim_K(\emptyset) = -1$. *Para cualquier subconjunto $S \subseteq X$, definiremos su dimensión de Krull como la dimensión de su clausura.*

Se observa fácilmente que si los conjuntos unipuntuales $\{x\}$ son cerrados en X, entonces los puntos y los conjuntos finitos de puntos tienen dimensión de Krull cero. En espacios topológicos noetherianos, se tienen las siguientes sencillas propiedades.

PROPOSICIÓN A.0.1. *Sea $(X, \mathscr{T})$ un espacio topológico noetheriano. Se tiene:*

i) Si $F \subseteq X$ es cerrado, su dimensión de Krull es el máximo de las dimensiones de Krull de sus componentes irreducibles.

ii) La dimensión de Krull satisface que $\forall S, T \subseteq X$,

$$\dim_K(S \cup T) \leq \max\{\dim_K(S), \dim_K(T)\}.$$

iii) Si $F \subseteq G \subseteq X$ son dos cerrados y G es irreducible, se tiene que

$$\dim_K(F) = \dim_K(G) \iff F = G.$$

Las ideas de dimensión de Krull están cualificadas para ser trasladadas a anillos e ideales, especialmente gracias al Nullstellensatz.

DEFINICIÓN 15. *Sea R un anillo, $\mathfrak{p} \in Spec(R)$ un ideal primo:*

i) Definimos la altura de $\mathfrak{p}$ *como el máximo de las longitudes de cadenas de ideales primos contenidos en $\mathfrak{p}$, i.e., el máximo de los $r \in \mathbb{N}$ tales que existe una cadena*

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_r \subseteq \mathfrak{p}$$

con $\mathfrak{q}_i \in Spec(R)$. La denotamos por $\mathrm{ht}(\mathfrak{p})$.

ii) Definimos la co-altura de $\mathfrak{p}$ *como el máximo de las longitudes de cadenas de ideales primos contenidos en $\mathfrak{p}$, i.e., el máximo de los $r \in \mathbb{N}$ tales que existe una cadena*

$$\mathfrak{p} \subsetneq \mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_r \subseteq R$$

con $\mathfrak{q}_i \in Spec(R)$. La denotamos por $\text{co-ht}(\mathfrak{p})$.

iii) Se llama dimensión de Krull de un anillo R *y denotaremos por* $\dim_K(R)$ *al máximo de las longitudes de cadenas de primos de R. Se satisface*

$$\dim_K(R) = \max\{\mathrm{ht}(\mathfrak{p}) : \mathfrak{p} \in Spec(R)\} = \max\{\text{co-ht}(\mathfrak{q}) : \mathfrak{q} \in Spec(R)\}.$$

Ni siquiera en el caso de anillos noetherianos se tiene la garantía de que la dimensión de Krull de un anillo sea finita (para ver un ejemplo, consultar el clásico [**Na, 75**]). Ahora bien, en el caso de anillos locales noetherienos (i.e., anillos noetherianos R con un único ideal maximal) la dimensión de Krull es finita.

TEOREMA A.0.2 (de la Dimensión Local). *Sea $(R, \mathfrak{m})$ un anillo local noetheriano. Se verifica que las siguientes cantidades son iguales:*

[1] W. Krull, *"Idealtheorie"*. Springer, 1935.

i) La altura del ideal maximal $\mathfrak{m}$, $\mathrm{ht}(\mathfrak{m})$.
ii) La dimensión de Krull de R, $\dim_K(R)$.
iii) La dimensión de Hilbert de R *(el grado del polinomio de Samuel).*
iv) La dimensión de Chevalley de R *definida mediante*

$$\min\{s \in \mathbb{N} : \exists \mathfrak{q} \subsetneq R \text{ ideal}, \sqrt{\mathfrak{q}} = \mathfrak{m} \text{ y } \mathfrak{q} \text{ está generado por } s \text{ elementos}\}.$$

En particular, $\dim_K(R) < +\infty$.

No probaremos este duro resultado (cuya prueba se extiende más allá de lo que cabe en las páginas de una memoria como esta). Tampoco vamos a especificar la noción de dimensión de Hilbert para no extendernos en exceso. Las referencias a pruebas del enunciado son las usuales de Álgebra Local ([**AtMc, 96**], [**Ma, 80**], [**Na, 75**], [**RaSiSr, 75**],...)
Nótese que si $\mathfrak{p} \in Spec(R)$ es un ideal primo, entonces

$$\mathrm{ht}\,\mathfrak{p} = \dim_K(R_{\mathfrak{p}}),$$

donde $R_{\mathfrak{p}}$ es la localización de R por el sistema multiplicativamente cerrado $R \setminus \mathfrak{p}$ por cuanto la altura de todo ideal primo en un anillo noetheriano es finita.
Dado un ideal $\mathfrak{a}$ en un anillo noetheriano, llamaremos co-altura de $\mathfrak{a}$ a la dimensión de Krull del anillo cociente, i.e.,

$$\text{co-ht}(\mathfrak{a}) = \dim_K(R/\mathfrak{a}) = \max\{\text{co-ht}(\mathfrak{p}) : \mathfrak{p} \in Spec(R), \mathfrak{p} \supseteq \mathfrak{a}\}.$$

El Teorema de Lasker-Noether en anillos noetherianos nos garantiza que todo ideal admite descomposición primaria. Un ideal $\mathfrak{q}$ de un anillo R se dice primario si satisface la siguiente propiedad:

$$\forall x, y \in R, xy \in \mathfrak{q} \Longrightarrow (x \in \mathfrak{q}) \vee (\exists n \in \mathbb{N}, y^n \in \mathfrak{q}).$$

Los ideales primarios tienen radical primo, aunque no todo ideal cuyo radical es primo es un ideal primario. Si $\mathfrak{q}$ es primario y $\mathfrak{p} = \sqrt{\mathfrak{q}}$, diremos que $\mathfrak{q}$ es $\mathfrak{p}$-primario.

Teorema A.0.3 (de Lasker-Noether). *Sea* R *un anillo noetheriano. Entonces, para todo ideal propio* $\mathfrak{a} \subseteq R$ *existe una descomposición primaria minimal de* $\mathfrak{a}$*, es decir, una presentación minimal*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s,$$

donde cada $\mathfrak{q}_i$ *es* $\mathfrak{p}_i$*-primario,* $\mathfrak{p}_i \neq \mathfrak{p}_j, \forall i \neq j$*. Más aún, la lista de ideales primos* $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ *es única para el ideal* $\mathfrak{a}$ *y se denominan sus primos asociados. Se denota*

$$Ass(R/\mathfrak{a}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}.$$

Se tiene que los primos minimales conteniendo a $\mathfrak{a}$ están entre los asociados (aunque puede haber primos asociados que no son primos minimales: los primos inmersos) con lo que tendremos

$$\text{co-ht}(\mathfrak{a}) = \max\{\text{co-ht}(\mathfrak{p}_i) : 1 \leq i \leq s\} = \dim_K(R/\mathfrak{a}).$$

Nótese que $\sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s$ y $\text{co-ht}(\mathfrak{a}) = \text{co-ht}(\sqrt{\mathfrak{a}})$.
Tanto en el caso de subconjuntos de un espacio topológico como en el caso de ideales de un anillo, pueden aparecer elementos de distinta dimensión. Por eso se introducen las nociones siguientes:

- Un cerrado $F \subseteq X$, con $(X, \mathcal{T})$ un espacio topológico noetheriano, se denomina equidimensional si todas sus componentes irreducibles tienen la misma dimensión. De igual manera, un constructible C se denomina equidimensional si lo es $\overline{C}^Z$.
- Un ideal $\mathfrak{a}$ de un anillo noetheriano R se denomina equidimensional si todos sus primos asociados tienen la misma altura.

La relación entre la dimensión de variedades algebraicas y la teoría de ideales es de fuerte identidad como consecuencia del Nullstellensatz:

Proposición A.0.4. *Sean* $\mathbb{K}$ *un cuerpo algebraicamente cerrado,* $V \subseteq \mathbb{A}^n(\mathbb{K})$ *una variedad algebraica afín,* $W \subseteq \mathbb{P}_n(\mathbb{K})$ *una variedad algebraica proyectiva y* $\mathfrak{a}$ *un ideal de* $\mathbb{K}[X_1, \ldots, X_n]$*. Se tiene:*

i)
$$\dim_K(V) = \dim_K(\mathbb{K}[V]) = \text{co-ht}(I_{\mathbb{A}}(V)).$$

ii) Sean $\varphi_i : \mathbb{A}^n(\mathbb{K}) \to \mathbb{P}_n(\mathbb{K}), \varphi_i(x_1, \ldots, x_n) = (x_1 : \ldots : x_{i-1} : 1 : x_i : \ldots : x_n)$ *las* $n+1$ *inmersiones del espacio afín en el proyectivo correspondiente. Entonces,*

$$\dim_K(W) = \max\{\dim_K(W \cap \varphi_i(\mathbb{A}^n(\mathbb{K}))) : 1 \leq i \leq n+1\}.$$

iii)
$$\text{co-ht}(\mathfrak{a}) = \dim_K(V_{\mathbb{A}}(\mathfrak{a})) = \dim_K(V_{\mathbb{A}}(\sqrt{\mathfrak{a}})).$$

Uno de los primeros resultados obtenidos a partir del Teorema de la Dimensión Local es el clásico Teorema del Ideal Principal de Krull:

TEOREMA A.0.5 (Krull Hauptidealsatz). *Sean R un anillo noetheriano, $f \in R$ y $\mathfrak{a} = (f)$ el ideal que genera. Se tiene:*

i) La altura de todo ideal primo minimal sobre $\mathfrak{a}$ es, a lo sumo, 1.
ii) Si f no es divisor de cero en R, todo primo minimal sobre $\mathfrak{a}$ tiene altura 1.

Aunque no todo anillo noetheriano es de dimensión finita, los anillos de polinomios y las K-álgebras finitamente generadas son de dimensión finita. Aunque el resultado general sigue siendo cierto para cuerpos K arbitrarios, daremos una sencilla prueba de la siguiente Proposición en el caso algebraicamente cerrado:

PROPOSICIÓN A.0.6. *Si $\mathbb{K}$ es algebraicamente cerrado,*

$$\dim_K \mathbb{K}[X_1, \ldots, X_n] = n.$$

DEMOSTRACIÓN. Es sencillo ver que $\dim_K \mathbb{K}[X_1, \ldots, X_n] \geq n$ gracias a la siguiente cadena de ideales primos:

$$(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n) = \mathbb{K}[X_1, \ldots, X_n].$$

De otro lado, todo maximal en $\mathbb{K}[X_1, \ldots, X_n]$, por el Nullstellensatz, es de la forma

$$\mathfrak{m}_\alpha = (X_1 - \alpha_1, \ldots, X_n - \alpha_n) \text{ con } \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{A}^n(\mathbb{K}).$$

Por tanto, todos los ideales maximales de $\mathbb{K}[X_1, \ldots, X_n]$ tienen altura acotada por n y $\dim_K(\mathbb{K}[X_1, \ldots, X_n]) = \max\{\text{ht}(\mathfrak{m}) : \mathfrak{m} \text{ es maximal}\} \leq n$, lo que concluye la prueba. □

De hecho, la dimensión de las K-álgebras finitamente generadas está ligada a la dimensión de los anillos de polinomios a través de un gran resultado conocido como Lema de Normalización de Noether. Para ello, necesitamos recordar livianamente las extensiones enteras de anillos.

DEFINICIÓN 16. *Una extensión $R \subseteq R'$ de anillos se dice* extensión entera *si para todo $\alpha \in R'$ existe un polinomio mónico $p(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_0 \in R[T]$ tal que $p(\alpha) = 0$ en R'.*

No analizaremos todas las buenas propiedades de las extensiones enteras de anillos. Nos limitaremos a recordar el Teorema del Ascenso (o Going Up) de Krull, Cohen y Seidenberg, que lo obtuvieron independientemente.

PROPOSICIÓN A.0.7. *Sea $R \subseteq R'$ una extensión de anillos.*

i) Si $\mathfrak{p} \in Spec(R')$ es un ideal primo, su contracción $\mathfrak{q} = \mathfrak{p}^c = \mathfrak{p} \cap R$ es un ideal primo en R. En general, la contracción de ideales maximales no es un ideal maximal.
ii) Si $R \subseteq R'$ es una extensión entera de anillos, la contracción $\mathfrak{m}^c = \mathfrak{m} \cap R$ de todo ideal maximal de R' es un ideal maximal en R.
iii) Si $R \subseteq R'$ es una extensión entera de anillos, la aplicación siguiente es suprayectiva:

$$\begin{array}{ccc} Spec(R') & \longrightarrow & Spec(R) \\ \mathfrak{p} & \longmapsto & \mathfrak{p}^c \end{array}.$$

Además, no hay inclusión estricta entre primos de R' que se contraen en el mismo primo de R.
iv) (Teorema del Ascenso) *Sean $R \subseteq R'$ una extensión entera de anillos, $\mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ una cadena de ideales primos en R, $\mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_m$ una cadena de ideales primos de R' tales que*

$$\mathfrak{q}_i^c = \mathfrak{p}_i, 1 \leq i \leq m,$$

con $m \leq n$. Entonces, existe una extensión de la cadena de primos de R'

$$\mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_m \subsetneq \ldots \subsetneq \mathfrak{q}_n$$

de tal modo que $\mathfrak{q}_j^c = \mathfrak{p}_j, 1 \leq j \leq n$.
v) Si $R \subseteq R'$ es una extensión entera de anillos, las dimensiones de Krull de R y R' coinciden,

$$\dim_K(R) = \dim_K(R').$$

El Lema de Normalización de Noether nos ayuda a recuperar la noción de dimensión en los términos siguientes:

TEOREMA A.0.8 (Lema de Normalización de Noether). *Sea K un cuerpo infinito, $\mathfrak{a}$ un ideal de $K[X_1,\dots,X_n]$ y r la dimensión de Krull de $K[X_1,\dots,X_n]/\mathfrak{a}$. Entonces, existe un abierto Zariski $U \subseteq \mathcal{M}_{r\times m}(K)$ (dependiente solo de $\mathfrak{a}$) formado por matrices con r filas y n columnas tales que para cada matriz $M \in U$ se tiene que definiendo*

$$\begin{pmatrix} L_1 \\ \vdots \\ L_r \end{pmatrix} = M \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \tag{A.0.1}$$

se satisfacen las siguientes propiedades:

i) Las clases $\ell_i = L_i + \mathfrak{a}, 1 \le i \le r$, son algebraicamente independientes sobre K. Equivalentemente, si $K[\ell_1,\dots,\ell_r]$ es la subálgebra de $K[X_1,\dots,X_n]/\mathfrak{a}$ generada por $\{\ell_1,\dots,\ell_r\}$, entonces $K[\ell_1,\dots,\ell_r]$ es un anillo de polinomios en r variables sobre K y, en particular,

$$\dim_K(K[\ell_1,\dots,\ell_r]) = r.$$

ii) La extensión siguiente de anillos es una extensión entera:

$$K[\ell_1,\dots,\ell_r] \hookrightarrow K[X_1,\dots,X_n]/\mathfrak{a}.$$

Podemos interpretar geométricamente el resultado en los términos siguientes: supongamos que $\mathbb{K}$ es algebraicamente cerrado, $\mathfrak{a} \in \mathbb{K}[X_1,\dots,X_n]$ un ideal y $V = V_{\mathbb{A}}(\mathfrak{a})$ la variedad algebraica afín que define. Supongamos $r = \dim_K(V)$, $U \subseteq \mathcal{M}_{r\times n}(\mathbb{K})$ el abierto Zariski al que hace referencia el Lema de Normalización de Noether.
Sea $M \in U$ una matriz y $L_1,\dots,L_r$ las aplicaciones lineales definidas en la Ecuación (A.0.1). Supongamos la aplicación lineal

$$\Lambda : \mathbb{K}^n \longrightarrow \mathbb{K}^r, \Lambda(x) := (L_1(x),\dots,L_r(x)), \forall x \in \mathbb{K}^n.$$

Entonces, $\Lambda|_V$ es suprayectiva (i.e., $\Lambda(V) = K^r$). Para cada $y \in \mathbb{K}^r$, la fibra $(\Lambda|_V)^{-1}(\{y\}) \subseteq V$ es cero-dimensional, esto es, está formada por un número finito de puntos de V.
Otra de las consecuencias del Lema de Normalización de Noether es la siguiente caracterización de la dimensión de Krull:

PROPOSICIÓN A.0.9. *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado, y sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible. Entonces, la dimensión de Krull satisface*

$$\dim_K(V) = \dim_K(\mathbb{K}[V]) = \text{gr. tr}_{\mathbb{K}}(\mathbb{K}(V)),$$

donde $\text{gr. tr}_{\mathbb{K}}(\cdot)$ es el grado de trascendencia sobre $\mathbb{K}$.

Veamos una de las consecuencias de esta caracterización:

COROLARIO A.0.10. *Sea $\varphi : V \longrightarrow W$ una aplicación polinomial, $\varphi(V) \subseteq (W)$ el constructible dado como la imagen de V. Entonces,*

$$\dim_K(\varphi(V)) = \dim_K(\overline{\varphi(V)}^Z) \le \dim_K(V).$$

DEMOSTRACIÓN. Bastará con que veamos el caso en el que V es irreducible. Nótese que si V es irreducible, $Z := \overline{\varphi(V)}^Z$ también lo será. La razón es que si $\varphi : V \longrightarrow Z$ es un morfismo dominante, el siguiente es un monomorfismo de $\mathbb{K}$-álgebras:

$$\begin{array}{rccc} \varphi^* : & \mathbb{K}[Z] & \longrightarrow & \mathbb{K}[V] \\ & f & \longmapsto & f \circ \varphi \end{array}.$$

Por tanto, como $\mathbb{K}[V]$ es dominio de integridad, también lo será $\mathbb{K}[Z]$ y, por tanto, Z es irreducible también. Más aún, si V es irreducible, tenemos, a través de φ^*, una identificación del cuerpo $\mathbb{K}(Z)$ con un subcuerpo de $\mathbb{K}(V)$. Por tanto, el grado de trascendencia de $\mathbb{K}(Z)$ es menor o igual que el grado de trascendencia de $\mathbb{K}(V)$ sobre $\mathbb{K}$ (existe el "Teorema del Reemplazamiento" en el caso de bases de trascendencia). Es decir,

$$\dim_K(\varphi(V)) = \dim_K(Z) = \text{gr. tr}_{\mathbb{K}}(\mathbb{K}(Z)) \le \text{gr. tr}_{\mathbb{K}}(\mathbb{K}(V)) = \dim_K(V).$$

□

Otra de las consecuencias del Lema de Normalización de Noether es la condición de catenaridad universal de los cuerpos. Lo dividiremos en dos puntos.

COROLARIO A.0.11. *Si K es un cuerpo y $\mathfrak{p} \subseteq K[X_1, \ldots, X_n]$ es un ideal primo del anillo de polinomios, se tiene*

$$\mathrm{ht}(\mathfrak{p}) + \text{co-ht}(\mathfrak{p}) = n.$$

La propiedad se satisface igualmente para ideales equidimensionales.
Más aún, si $\mathbb{K}$ es un cuerpo algebraicamente cerrado y $V \subseteq \mathbb{A}^n(\mathbb{K})$ es una variedad algebraica irreducible o equidimensional,

$$\dim_K(V) + \mathrm{ht}(I_{\mathbb{A}}(V)) = n.$$

A la cantidad $n - \dim_K(V) = \mathrm{ht}(I_{\mathbb{A}}(V))$ se la denomina codimensión de V en $\mathbb{A}^n(\mathbb{K})$.

COROLARIO A.0.12. *Todo cuerpo K es universalmente catenario. Es decir, dados $\mathfrak{p} \subseteq \mathfrak{q}$ dos ideales primos de $K[X_1, \ldots, X_n]$, entonces*

$$\mathrm{ht}(\mathfrak{q}/\mathfrak{p}) = \mathrm{ht}(\mathfrak{q}) - \mathrm{ht}(\mathfrak{p})$$

y existen cadenas de primos de longitud $r = \mathrm{ht}(\mathfrak{q}) - \mathrm{ht}(\mathfrak{p})$ entre $\mathfrak{p}$ y $\mathfrak{q}$, i.e.,

$$\mathfrak{p} = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_r = \mathfrak{q}.$$

Algunas de las consecuencias inmediatas de las reflexiones anteriores son las siguientes caracterizaciones, donde $\mathbb{K}$ es algebraicamente cerrado:

i) Una variedad algebraica $V \subseteq \mathbb{A}^n(\mathbb{K})$ es de dimensión cero si y solamente si es un conjunto finito de puntos. Lo mismo sucederá para variedades algebraicas proyectivas.

   Una de las implicaciones es obvia. Para la otra, si $V \subseteq \mathbb{A}^n(\mathbb{K})$ es de dimensión cero, entonces su ideal $I_{\mathbb{A}}(V)$ es necesariamente un ideal de altura n en $\mathbb{K}$. Por tanto $I_{\mathbb{A}}(V)$ es una intersección de ideales maximales y, por el Teorema de Lasker-Noether, una intersección finita de maximales. Como, por el Nullstellensatz, los maximales de $\mathbb{K}[X_1, \ldots, X_n]$ están identificados por puntos, entonces V es una unión finita de puntos.

ii) Una variedad equidimensional $V \subseteq \mathbb{A}^n(\mathbb{K})$ es de codimensión 1 si y solamente si es una hipersuperficie, i.e., $\exists f \in \mathbb{K}[X_1, \ldots, X_n] \setminus \{0\}$ tal que $V = V_{\mathbb{A}}(f)$.

   Como $\mathbb{K}[X_1, \ldots, X_n]$ es un dominio de factorización única, dado $f \in \mathbb{K}[X_1, \ldots, X_n] \setminus \{0\}$, f es un producto finito de polinomios irreducibles. Entonces,

$$\sqrt{(f)} = (f_1) \cap \ldots \cap (f_n),$$

   donde los ideales $(f_i) = \mathfrak{p}_i$ son ideales primos, de altura 1 por el Hauptidealsatz. Por tanto,

$$\dim_K(V_{\mathbb{A}}(f)) = n - 1,$$

   y $V_{\mathbb{A}}(f)$ es equidimensional.

   De otro lado, si $\dim_K(V) = n - 1$, entonces $I_{\mathbb{A}}(V)$ es un ideal no trivial y contiene algún elemento no nulo $f \in I_{\mathbb{A}}(V)$. Ahora, como V es equidimensional, todas sus componentes irreducibles tienen dimensión $n - 1$. Pero si C es componente irreducible de V, entonces

$$C \subseteq V_{\mathbb{A}}(f) = V_{\mathbb{A}}(f_1) \cup \ldots \cup V_{\mathbb{A}}(f_r),$$

   donde $f_1, \ldots, f_r$ son los factores irreducibles de f. Por ser C irreducible, debe existir i con $C \subseteq V_{\mathbb{A}}(f_i)$, ambos irreducibles con $\dim_K(C) = \dim_K(V_{\mathbb{A}}(f_i))$. Luego $C = V_{\mathbb{A}}(f_i)$. Tomando todas las componentes irreducibles de V, seleccionamos un subconjunto $J \subseteq \{1, \ldots, r\}$ de tal modo que

$$h = \prod_{j \in J} f_j$$

   satisface que $V_{\mathbb{A}}(h) = V$ y V es una hipersuperficie.

iii) Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica equidimensional, $f \in \mathbb{K}[X_1, \ldots, X_n]$ un polinomio. Entonces, si $V \cap V_{\mathbb{A}}(f) \neq \emptyset$,

$$\dim_K(V \cap V_{\mathbb{A}}(f)) \geq \dim_K(V) - 1,$$

   y si f no es divisor de cero en $\mathbb{K}[V]$ (i.e., si f no se anula idénticamente en ninguna componente irreducible de V) se tiene

$$\dim_K(V \cap V_{\mathbb{A}}(f)) = \dim_K(V) - 1.$$

iv) La generalización del resultado se extiende a través de la noción de sucesión regular. Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ equidimensional, $f_1, \ldots, f_r \in \mathbb{K}[X_1, \ldots, X_n]$ tales que $V \cap V_{\mathbb{A}}(f_1, \ldots, f_r) \neq \emptyset$. Entonces,

$$\dim_K(V \cap V_{\mathbb{A}}(f_1, \ldots, f_r)) \geq \dim_K(V) - r.$$

   Diremos que $f_1, \ldots, f_r$ es una sucesión regular con respecto a V si

- f_i no es divisor de cero en $\mathbb{K}[V]$,
- f_i no es divisor de cero módulo $I_{\mathbb{A}}(V) + (f_1, \ldots, f_{i-1})$, y
- $V \cap V_{\mathbb{A}}(f_1, \ldots, f_r) \neq \emptyset$.

Entonces, si $f_1, \ldots, f_r$ es una sucesión regular con respecto a V, se tiene

$$\dim_K(V \cap V_{\mathbb{A}}(f_1, \ldots, f_r)) = \dim_K(V) - r.$$

Obviamente, la longitud r de las sucesiones regulares con respecto a V está limitada por la codimensión de V.

Un resultado clásico más general es el

TEOREMA A.0.13 (Dimensión de la Intersección). *Sean $V, W \subseteq \mathbb{A}^n(\mathbb{K})$ dos variedades algebraicas afines. Supongamos $V \cap W \neq \emptyset$. Entonces,*

$$\dim_K(V \cap W) \geq \dim_K(V) + \dim_K(W) - n.$$

Una prueba puede verse en [**Shf, 74**], por ejemplo. También en [**Shf, 74**] podemos encontrar el siguiente resultado que responde a una versión dimensional de los Teoremas de Morse-Sard. Para versiones más delicadas, ver los Teoremas de Bertini, también en [**Shf, 74**].

TEOREMA A.0.14 (de la Dimensión en la Fibra). *Sean $\mathbb{K}$ un cuerpo algebraicamente cerrado, $V \subseteq \mathbb{A}^n(\mathbb{K})$ y $W \subseteq \mathbb{A}^m(\mathbb{K})$ dos variedades algebraicas afines con V irreducible. Sea $\varphi : V \longrightarrow W$ un morfismo dominante. Entonces, se tiene:*

i) Para cada $y \in W$, si la fibra $\varphi^{-1}(\{y\})$ es no vacía, entonces

$$\dim_K(\varphi^{-1}(\{y\})) \geq \dim_K(V) - \dim_K(W).$$

ii) Existe un abierto Zariski U en W tal que para cada $y \in U$

$$\dim_K(\varphi^{-1}(\{y\})) = \dim_K(V) - \dim_K(W).$$

APÉNDICE B

Codificación de polinomios por programas

La idea clásica de codificar polinomios mediante programas que los evalúan se remonta a los años 70 y 80 del pasado siglo, aunque hubo que esperar a los desarrollos del programa TERA-Kroenecker para entender un enorme influencia en los problemas de diseño de algoritmos eficientes en Geometría Algebraica. No vamos a entrar en los desarrollos propios de esta tendencia y nos vamos a limitar a exponer unas pocas nociones que se usan a lo largo del manuscrito. Las nociones han sido tomadas de [**KrPa, 96**].

DEFINICIÓN 17. *Un esquema de evaluación con inputs $X_1, \dots X_n$ es un par $\Gamma := (\mathcal{G}, Q)$, donde $\mathcal{G}$ es un grafo dirigido sin ciclos, con $n+1$ puertas de entrada, abanico de entrada no acotado, y Q es una función que asigna a cada puerta (i,j) una de las siguientes instrucciones:*

$$i = 0: \qquad Q_{0,1} := 1, Q_{0,2} := X_1, \dots, Q_{0,n+1} := X_n,$$

$$1 \le i \le \ell: \quad Q_{i,j} := \left(\sum_{r \le i-1, 1 \le s \le L_r} A_{i,j}^{r,s} Q_{r,s} \right) \cdot \left(\sum_{r' \le i-1, 1 \le s' \le L_{r'}} B_{i,j}^{r',s'} Q_{r',s'} \right),$$

donde $A_{i,j}^{r,s}, B_{i,j}^{r',s'}$ son indeterminadas sobre K llamadas parámetros introducidos en Γ. El tamaño del esquema de evaluación Γ es $L(\Gamma) = L_0 + \ldots + L_\ell$ (donde $L_0 := n+1$) y su profundidad es $\ell(\Gamma) = \ell$ (estas nociones coinciden con las nociones de tamaño y profundidad del grafo subyacente).

Notemos que, con esta notación, los subíndices de los parámetros $A_{i,j}^{r,s}$ y $B_{i,j}^{r',s'}$ representan el nodo al que están asignados y los superíndices se corresponden con los resultados previos que involucran en la multiplicación. Denotemos a estos por $\underline{A} = \left(A_{i,j}^{r,s}\right)$ y $\underline{B} = \left(B_{i,j}^{r',s'}\right)$.
Semánticamente, el esquema de evaluación Γ define un algoritmo de evaluación de los polinomios (resultados intermedios):

$$Q_{i,j} = \sum_{|\mu| \le 2^i} Q_{i,j}^{\mu}(\underline{A}, \underline{B}) X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

Aquí, cada coeficiente $Q_{i,j}^{\mu}(\underline{A}, \underline{B})$ pertenece al anillo de polinomios $K[\underline{A}, \underline{B}]$. El resultado $Q_{i,j}$ tienen grados acotados por 2^i respecto de las variables $X_1, \dots, X_n$.
Sea K un cuerpo. Una especialización del SLP Γ en el cuerpo K es una sustitución de las listas de parámetros $\underline{A}, \underline{B}$ por listas $\underline{\alpha} = \left(\alpha_{i,j}^{r,s}\right), \underline{\beta} = \left(\beta_{i,j}^{r',s'}\right)$ cuyas coordenadas están en K. Así, una especialización de Γ en $\underline{\alpha}, \underline{\beta}$ es una lista de polinomios

$$Q_{i,j}(\underline{\alpha}, \underline{\beta}, X_1, \dots, X_n) = \sum_{|\mu| \le 2^i} Q_{i,j}^{\mu}(\underline{\alpha}, \underline{\beta}) X_1^{\mu_1} \cdots X_n^{\mu_n} \in K[X_1, \dots, X_n].$$

Si las coordenadas de $\underline{\alpha}, \underline{\beta}$ se eligen en un subconjunto $\mathcal{F} \subseteq K$ (i.e., $\alpha_{i,j}^{r,s}, \beta_{i,j}^{r',s'} \in \mathcal{F}$), diremos que es una especialización con parámetros en $\mathcal{F}$.
En este sentido, diremos que un polinomio $P \in K[X_1, \dots, X_n]$ es evaluable, o computable, por (una especialización de) un esquema de evaluación Γ si existe una especialización $\underline{A} \to \underline{\alpha}, \underline{B} \to \underline{\beta}$ de los parámetros de Γ tal que, para algún nodo (i,j), se tiene la siguiente igualdad:

$$P(X_1, \dots, X_n) = Q_{i,j}(\underline{\alpha}, \underline{\beta}, X_1, \dots, X_n).$$

Un ejemplo clásico de la interpretación por esquemas de evaluación de los procesos que representan polinomios multivariados es la que se hace [**KrPa, 96**] del algoritmo de Berkowitz para el cálculo del determinante.

PROPOSICIÓN B.0.1. *Sea R un anillo. Existe un esquema de evaluación de tamaño $O(N^5)$, profundidad $O(\log_2 n)$ y parámetros en $\{-1, 0, 1\}$ que calcula, a partir de las entradas de una matriz $A \in \mathcal{M}_n(R)$, los coeficientes de su polinomio característico y, en particular, su determinante* $\det(A)$.

Algunos resultados útiles en nuestro estudio son los siguientes:

LEMA B.0.2. *Dado un esquema de evaluación* Γ*, el grado de los polinomios* $Q^{\mu}_{i,j} \in K[\underline{A}, \underline{B}]$ *es* $2^{i+1} - 2$ *(independientemente de los valores de* μ *y* j*).*

Esto permite modelizar los polinomios "dados por esquemas de evaluación" del modo siguiente. Sea Γ un esquema de evaluación de talla L y profundidad ℓ. Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Supongamos que Γ posee un único nodo de output y consideremos la aplicación polinomial

$$\begin{array}{rccl} \Gamma: & \mathbb{A}^N(\mathbb{K}) & \longrightarrow & P^{\mathbb{K}}_{2^\ell}(X_1, \ldots, X_n) \\ & (\underline{\alpha}, \underline{\beta}) & \longmapsto & Q_{(\ell,1)}(\underline{\alpha}, \underline{\beta}, X_1, \ldots, X_n), \end{array}$$

donde $N = 2L(L - (n+1))$ es el número de variables paramétricas $\underline{A}, \underline{B}$ que aparecen en Γ, 2^ℓ es la cota superior del grado en las variables $X_1, \ldots, X_n$ y $P^{\mathbb{K}}_{2^\ell}(X_1, \ldots, X_n)$ es el $\mathbb{K}$-espacio vectorial de los polinomios de grado a lo sumo 2^ℓ con coeficientes en $\mathbb{K}$ y variables $\{X_1, \ldots, X_n\}$. El siguiente resultado puede verse en [**KrPa, 96**].

PROPOSICIÓN B.0.3. *Con las notaciones precedentes, denotemos por* $\Omega(\Gamma)$ *a la imagen de la aplicación* Γ *anterior. Se tiene:*

i) $\Omega(\Gamma)$ *es un constructible cuya clausura Zariski es un irreducible,*
ii) $\dim(\Omega(\Gamma)) \leq 2L(L - (n+1))$*,*
iii) $\deg(\Omega(\Gamma)) \leq (2^{\ell+1} - 2)^{2L(L-(n+1))}$.

OBSERVACIÓN B.0.4. Como bien indica su nombre, un esquema de evaluación describe una forma de evaluar un polinomio $Q_{\ell,1}(\underline{\alpha}, \underline{\beta}, X_1, \ldots, X_n)$ sobre datos $(x_1, \ldots, x_n) \in \mathbb{K}^n$. Las operaciones que se indican son las operaciones a realizar y dada su estructura interna como grafo, se puede modelizar la evaluación bien secuencialmente o, incluso, en paralelo.
En lo que concierne a este TFG, sólo nos preocupa la evaluación en secuencial, nodo tras nodo se realizan las operaciones aritméticas indicadas, usando solamente la información precomputada en profundidad menor. La complejidad de este proceso se puede definir conforme a dos modelos de computación:

i) *En el modelo de máquinas de Turing*, la complejidad depende de varios ingredientes: el coste de las operaciones aritméticas sobre elementos de un cuerpo K computable (determinado por una función $M : \mathbb{N} \longrightarrow \mathbb{R}_+$ que depende de la talla de los elementos involucrados), el crecimiento de las tallas de los resultados intermedios (que obviamente depende de los parámetros $\underline{\alpha}, \underline{\beta}$, las tallas de las coordenadas del input $(x_1, \ldots, x_n) \in K^n$ y del ritmo de crecimiento de las tallas tras operar) que denotaremos como $T(\Gamma, \underline{\alpha}, \underline{\beta}, \underline{x})$ y, finalmente, del número de operaciones realizadas. Por tanto, en el modelo de Turing, la complejidad de evaluar Γ con parámetros $\underline{\alpha}, \underline{\beta}$ en un punto $\underline{x} \in K^n$ vendrá acotada por

$$O(L^2 M(T(\Gamma, \underline{\alpha}, \underline{\beta}, \underline{x}))).$$

ii) *En el modelo BSS* (Blum-Shub-Smale), la única medida de complejidad considerada es el número de operaciones aritméticas realizadas al simular la evaluación de Γ con parámetros $\underline{\alpha}, \underline{\beta}$ sobre un input $\underline{x} \in K^n$. *Este es el modelo que seguiremos* en este TFG, y la complejidad de evaluar Γ de talla L en secuencial está acotada por

$$O(L^2).$$

Bibliografía

[AdHu, 92] L. M. Adleman, M.-D. A. Huang, *"Primality Testing and Abelian Varieties Over Finite Fields"*, Springer-Verlag Berlin Heidelberg, 1992.

[AKS, 04] M. Agrawal, N. Kayal, N. Saxena, PRIMES *is in* **P**. Annals of Mathematics **160** (2) (2004), 781-793.

[Al, 99] N. Alon, *Combinatorial Nullstellensatz*. Combin. Probab. Comput. **8** (1999), 7-29.

[AtMc, 96] M. F. Atiyah, I. G. Macdonald, *"Introduction to Commutative Algebra"*, Addison-Weskey Publishing Co., 1969. [Edición en español por Ed. Reverté, 1980]

[BCSS, 98] L. Blum, F. Cucker, M. Shub, S. Smale, *"Complexity and Real Computation"*, Springer-Verlag New York, 1998.

[BSS, 84] L. Blum, M. Shub, S. Smale, *On a Theory of Computation and Complexity over the Real Numbers: NP-completeness, Recursive Functions and Universal Machines*. B. of the A.M.S. **21** (1) (1984), 1-46.

[CGHMP, 03] D. Castro, M. Giusti, J. Heintz, G. Matera, L. M. Pardo, *The Hardness of Polynomial Equation Solving*. Foundations of Computational Mathematics **3** (2003), 347-420.

[Dv, 09] Z. Dvir, *On the size of Kakeya sets on infinite fields*. J. of the A.M.S. **22** (2009), 1093-1097.

[Fu, 83] W. Fulton, *"Intersection theory"*. New York-Heidelberg-Berlin Tokyo Springer, 1983.

[GHMMP, 98] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, L. M. Pardo, *Straight-line programs in geometric elimination theory* . Journal of Pure and Applied Algebra **124** (1998), 101-146.

[GHMP, 97] M. Giusti, J. Heintz, J. E. Morais, L. M. Pardo, *Le rôle des structures des données dans les problèmes d'élimination*. Comptes Rendues Acad. Sci. Paris, Sér. I **325** (1997), 1223-1228.

[HMPS, 00] K. Hägele, J. E. Morais, L. M. Pardo, M. Sombra, *The intrinsic complexity of the Arithmetic Nullstellensatz*. Journal of Pure and Applied Algebra **146** (2000), 103-183.

[HvdH, 19] D. Harvey, J. van der Hoeren, *Integer Multiplication in Time $O(n \log n)$*. HAL (2019).

[He, 83] J. Heintz, *Fast Quantifier Elimination for Algebraically Closed Fields*. Theoret. Comput. Sci. **24** (1983), 239-277.

[He, 85] J. Heintz, *Corrigendum: Definability and Fast Quantifier Elimination in Algebraically Closed Fields*. Theoret. Comput. Sci. **39** (1985), 343.

[HeSc, 83] J. Heintz, C. P. Schnorr, *Testing polynomials which are easy to compute*. Logic and algorithmic: An international symposium held in honor of Ernst Specker, Monographie No. **30** de l'Enseignement Mathématique, 1982, 237-254.

[HeSi, 80] J. Heintz, M. Sieveking, *Lower Bounds for Polynomials with Algebraic Coefficients*. Theoret. Comput. Sci. **11** (1980), 321-330.

[KaIm, 04] V. Kabanetz, R. Impagliazzo, *Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds*. Computational Complexity **13** (2004), 1-46.

[KrPa, 96] T. Krick, L. M. Pardo, *A computational method for diophantine approximation*. En "Algorithms in Algebraic Geometry", Progress in Math **143**, Birkhauser Verlag, 1996, 193-253.

[Ku, 85] E. Kunz, *"Introduction to Commutative Algebra and Algebraic Geometry"*, Birkhäuser, 1985.

[Ma, 80] H. Matsumura, *"Commutative Algebra (2nd. Edition)"*, Benjamin/Cummings, 1980.

[Mi, 75] G. Miller, *Riemann's Hypothesis and tests for primality*. Journal of Computer and System Sciences **13** (3) (1975), 300-317.

[Na, 75] M. Nagata, *"Local Rings"*, Robert E. Krieger, 1975.

[Pa, 12] L. M. Pardo, *La Conjetura de Cook (¿P=NP?) II: Probabilidad, Interactividad y Comprobación Probabilista de Demostraciones*. La Gaceta de la RSME **15** (2012), 303-333.

[Ra, 80] M. Rabin, *Probabilistic algorithm for testing primality*. Journal of Number Theory **12** (1) (1980), 128-138.

[RaSiSr, 75] S. Raghavan, B. Singh, R. Sridharan, *"Homologial Methods in Commutative Algebra"*, Tata Institute for Fund. Res., Oxford University Press, 1975.

[Sch, 80] J. P. Schwarz, *Fast Probabilistic Algorithms for Verification of Polynomial Identities*. J. of the A.C.M. **27** (1980), 701-717.

[Shf, 74] I. R. Shafarevich, *"Basic Algebraic Geometry"*, Springer-Verlag, 1974.

[SoSt, 77] R. Solovay, V. Strassen, *A Fast Monte-Carlo Test for Primality*. SIAM J. Comput. **6** (1977), 84-85.

[Tao, 14] T. Tao, *Algebraic Combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*. EMS Surveys Math. Sci. **1** (2014), 1-46.

[Vo, 84] W. Vogel, *"Lectures on Bézout's Theorem"*. Tata Inst. for Fundamenta Research, Springer-Verlag, 1984.

[Wo, 99] T. Wolff, *Recent work connected with Kakeya problem*. En "Prospects in mathematics", Amer. Math. Soc., 1999, 129-162.

[ZS, 75] O. Zariski, P. Samuel, *"Commutative Algebra (2 vols.)"*, GTM Springer, 1975.

[Zp, 79] R. Zippel, *Probabilistic Algorithms for Sparse Polynomials*. En "Symbolic and Algebraic Computation (EUROSAM'79)", Lecture Notes in Computer Science **72**, Springer, 1979, 216-266.