Conjuntos Cuestores I

Grado de conjuntos constructibles, desigualdad de Bézout y densidad

Daniel Sebastián San Martín
Trabajo realizado junto a Luis Miguel Pardo Vasallo

Universidad de Cantabria

6 de mayo de 2021

Índice

Nuestro objetivo

¿Qué podemos "aprender" de una variedad algebraica sin hacer "casi nada" con ella?

Trabajaremos en el caso afín y con variedades definidas por polinomios que viven en un conjunto constructible $\Omega \subseteq K[X_1, \ldots, X_n]$.

Una pregunta básica

Sea $f \in \Omega$, *¿podemos "aprender" si* $f \equiv 0$ *únicamente mediante evaluación?*

Ejemplo 1:

$$¿\ (X_1 + X_2)(X_1 - X_2) - (X_1^2 - X_2^2) \equiv 0\ ?$$

Ejemplo 2:

- Ω: conjunto de polinomios evaluables por una red neuronal.
- $f, g \in \Omega$ (no conocemos su expansión monomial ni sus coeficientes, sólo los podemos evaluar).

$$¿\ f \equiv 0\ ? \quad ¿\ f \equiv g\ ?$$

Test de DeMillo–Lipton–Schwartz–Zippel

Test de DeMillo–Lipton–Schwartz–Zippel ([DML, 78], [Sch, 80] y [Zp, 79])

Sea $f \in \mathcal{P}_d(X_1, \ldots, X_n)$ no nulo y sea C un subconjunto finito de K. Entonces:

$$\operatorname*{Prob}_{(x_1,\ldots,x_n)\in C^n} [f(x_1, \ldots, x_n) = 0] \leq \frac{d}{\#(C)}$$

Dificultad: si exigimos certidumbre en la respuesta:

"el polinomio dado es nulo",

el test anterior exige evaluar nuestro polinomio en todos los puntos de C^n:

¡Un conjunto de tamaño exponencial!

Para paliar esta dificultad surgen los **conjuntos cuestores** de J. Heintz y C. P. Schnorr [HeSc, 82].

Definición (en el sentido de [HeSc, 82])

Decimos que un conjunto $\{x_1, \ldots, x_L\} \subseteq \mathbb{A}^n(K)$ es un conjunto cuestor para Ω si:

$$\forall f \in \Omega,\ f(x_1) = \cdots = f(x_L) = 0 \Rightarrow f \equiv 0$$

Ejemplo básico: si $\Omega := \{f \in K[X] \,:\, deg(f) \leq d\}$, entonces cualquier conjunto de $d+1$ puntos distintos es un conjunto cuestor para Ω.

Pregunta: ¿existen los conjuntos cuestores?, ¿dónde los puedo encontrar?

Teorema fundamental de Heintz & Schnorr ([HeSc, 82])

Teorema ([HeSc, 82])

Supongamos que $char(K) = 0$. Sea Ω un conjunto constructible parametrizable de polinomios de grado acotado por d, $\Lambda \subseteq \mathbb{A}^n(K)$ un retículo y $L \geq 6\dim(\Omega)$.

Entonces:

- **Existencia:** existen conjuntos cuestores $\mathbf{Q} := (x_1, \ldots, x_L) \in \Lambda^L$ para Ω.
- **Densidad:**

$$\underset{(x_1,\ldots,x_L)\in\Lambda^L}{\text{Prob}} [(x_1, \ldots, x_L) \text{ es un conjunto cuestor para } \Omega] \geq 1 - \frac{1}{u^{L/6}}.$$

- Herramienta principal: **teoría del grado para conjuntos localmente cerrados** de [He, 83].

- **Algunas limitaciones:** $char(K) = 0$, conjuntos constructibles parametrizables, Λ es un retículo, ...

En el trabajo realizado junto a Luis Miguel Pardo Vasallo tratamos de dar respuesta a la siguiente pregunta:

- **Pregunta:** *¿Qué son los conjuntos cuestores y qué puedo hacer con ellos?*

- **Un problema en el camino:** Para trabajar con conjuntos cuestores necesitamos definir y saber cómo utilizar la noción de grado para conjuntos constructibles.

Un intento fallido: en la Remark (2) de [He, 83] se define el Z-grado ($\deg_z$) de un conjunto constructible como el grado de su clausura Zariski.

Sin embargo, como ya se observó en [He, 85], esta noción presenta algunos problemas...

¿Qué es un grado?

De acuerdo con el paradigma establecido en [He, 83], una **noción de grado para conjuntos constructibles** debe ser una cantidad (actuando como un volumen) que verifica las siguientes propiedades:

(1) Es siempre finita y coincide con la noción usual para conjuntos localmente cerrados.

(2) Es sub–aditiva:

(3) Tiene un buen comportamiento respecto a la intersección con variedades lineales y respecto al producto cartesiano.

(4) Es controlable por proyecciones e imágenes de aplicaciones lineales.

(5) Satisface una Desigualdad de Bézout: el grado de la intersección está acotado por el producto de los grados.

(6) Satisface alguna variación de la Proposición 2.3. de [HeSc, 82] **(¡resultado clave para los resultados de existencia y densidad de conjuntos cuestores!).**

Grado de Heintz: Conjuntos localmente cerrados

Para la noción usual de grado (localmente cerrados) usaremos $\deg(V)$.

Proposición: Propiedades básicas del grado para conjuntos localmente cerrados

- Para todo conjunto localmente cerrado $V \subseteq \mathbb{A}^n(K)$, su grado coincide con el grado de su clausura Zariski: $\deg(V) = \deg(\overline{V}^z)$.
- El grado de un conjunto finito $C \subseteq \mathbb{A}^n(K)$ coincide con su cardinal: $\deg(C) = \#(C)$.
- El grado de una variedad lineal afín es 1.
- Para cualquier polinomio $f \in K[X_1, \ldots, X_n]$ no constante, el grado de la hipersuperficie $V(f)$ es a lo sumo $\deg(f)$ y, $\deg(V(f)) = \deg(f)$ si y sólo si f es libre de cuadrados.

Los problemas del Z-grado

Consideramos el conjunto constructible:

$$C =: \{(x,y) \in \mathbb{A}^2(\mathbb{C}) : xy \neq 0\} \cup \{(\pm 1, 0), (0, \pm 1)\},$$

que no es localmente cerrado, y la variedad algebraica:

$$D := \{(x,y) \in \mathbb{A}^2(\mathbb{C}) \ : \ xy = 0\}.$$

Tenemos que:

- $\overline{C}^z = \mathbb{A}^2(\mathbb{C})$ y, por lo tanto, $\deg_z(C) = 1$.
- $\deg(D) = 2$ por ser $f(x,y) = xy$ libre de cuadrados.
- $C \cap D = \{(\pm 1, 0), (0, \pm 1)\}$ y, por lo tanto, $\deg(C \cap D) = 4$.

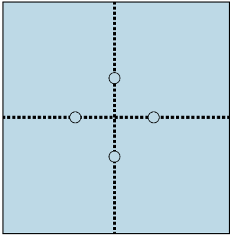

Figura: Conjunto constructible C.

De lo anterior, se deduce que:

$$4 = \deg(C \cap D) \not\leq \deg_z(C) \cdot \deg(D) = 1 \cdot 2 = 2$$

Por lo tanto, el Z-grado no cumple la desigualdad de Bézout. Esto **nos lleva a buscar nuevas nociones de grado para conjuntos constructibles** que verifiquen una desigualdad de este tipo.

Nueva noción: *LCI*-grado

Definición: *LCI*-grado de un conjunto constructible

Sea $C \subseteq \mathbb{A}^n(K)$ un conjunto constructible. Sea $\mathfrak{C} =: \{U_1 \cap V_1, \ldots, U_r \cap V_r\}$ una descomposición de C como unión finita de conjuntos localmente cerrados irreducibles que satisface:

(1) V_i es una variedad algebraica irreducible en $\mathbb{A}^n(K)$,

(2) U_i es el máximo de los abiertos Zariski $O_i \subseteq \mathbb{A}^n(K)$ tal que $O_i \cap V_i \subseteq C$,

(3) $V_i \neq V_j$.

Definimos el grado de C relativo a esta decomposición como:

$$\deg(C, \mathfrak{C}) := \sum_{i=1}^{r} \deg(V_i).$$

Entonces, definimos el *LCI*-grado de C como:

$$\deg_{\mathrm{lci}}(C) := \text{mín}\{\deg(C, \mathfrak{C}) \ : \ \mathfrak{C} \text{ es una descomposición de } C \text{ como unión finita de conjuntos localmente cerrados irreducibles que satisface (1), (2) y (3)}\}$$

Nueva noción: π-grado

Definición: π-grado de un conjunto constructible

Sea $C \subseteq \mathbb{A}^n(K)$ un conjunto constructible y consideramos la clase de todos los subconjuntos localmente cerrados que se proyectan en C. Es decir, para cada $m \in \mathbb{N}$, $m \geq n$, definimos:

$$\Pi_m(C) := \{V \subseteq \mathbb{A}^m \ : \ V \text{ es localmente cerrado y } \pi(V) = C\}$$

donde $\pi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ es la proyección canónica. Entonces, definimos:

$$\Pi(C) := \bigcup_{m \geq n} \Pi_m(C),$$

y definimos el grado de proyección o π-grado de C como el siguiente mínimo:

$$\deg_\pi(C) := \text{mín}\{\deg(V) \ : \ V \in \Pi(C)\}.$$

Consideramos la hipersuperficie cuadrática:

$$W := \{(x, y, z) \in \mathbb{A}^3(\mathbb{C}) \ : \ xz + (y^2 - 1) = 0\}$$

y el conjunto constructible :

$$C := \pi(W) = \{(x, y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x \neq 0\} \cup \\ \cup \{(x, y) \in \mathbb{A}^2(\mathbb{C}) \ : \ x^2 + y^2 - 1 = 0\}$$

Tenemos que:

- $\deg_z(C) = 1$.
- $\deg_{\mathrm{lci}}(C) = 3$.
- $\deg_\pi(C) = 2$.

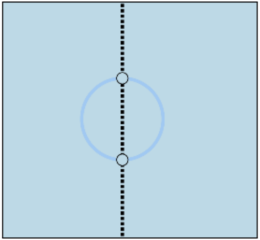

Figura: Conjunto constructible C.

Esto es, cada una de las nociones de grado toma un valor diferente para C:

$$1 = \deg_z(C) < 2 = \deg_\pi(C) < \deg_{\mathrm{lci}}(C) = 3$$

Sean $C,\ D \subseteq \mathbb{A}^n(K)$ dos conjuntos constructibles.

Teorema: (1) Coincide con la noción usual para localmente cerrados

Si C es **localmente cerrado**, entonces:

$$\deg(C) = \deg_z(C) = \deg_\pi(C) = \deg_{\mathrm{lci}}(C)$$

Teorema: (2) Sub-aditividad

Las tres nociones de grado $\deg_z$, $\deg_\pi$ y $\deg_{\mathrm{lci}}$ son funciones **sub–aditivas**:

$$\deg_z(C \cup D) \leq \deg_z(C) + \deg_z(D),$$

$$\deg_\pi(C \cup D) \leq \deg_\pi(C) + \deg_\pi(D) \text{ y}$$

$$\deg_{\mathrm{lci}}(C \cup D) \leq \deg_{\mathrm{lci}}(C) + \deg_{\mathrm{lci}}(D).$$

Propiedades de las nuevas nociones

Teorema: (3) Intersección con variedades lineales

Para cada **variedad lineal afín** $A \subseteq \mathbb{A}^n(K)$, se cumple:

$$\deg_{\mathrm{lci}}(A \cap C) \leq \deg_{\mathrm{lci}}(C), \ \ \deg_{\pi}(A \cap C) \leq \deg_{\pi}(C).$$

Teorema: (3) Producto cartesiano

$$\deg_{\mathrm{lci}}(C \times D) \leq \deg_{\mathrm{lci}}(C) \deg_{\mathrm{lci}}(D), \ \ \deg_{\pi}(C \times D) \leq \deg_{\pi}(C) \deg_{\pi}(D).$$

Teorema: (4) Imágenes de aplicaciones lineales

Sea $\ell : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^m(K)$ una **aplicación lineal**:

- $\deg(\overline{\ell(C)}^z) \leq \deg_{\mathrm{lci}}(C)$
- En general, no es cierto que: $\deg_{\mathrm{lci}}(\ell(C)) \leq \deg_{\mathrm{lci}}(C)$.
- $\deg_z(\ell(C)) \leq \deg_{\pi}(\ell(C)) \leq \deg_{\pi}(C) \leq \deg_{\mathrm{lci}}(C)$.

Teorema: (5) Desigualdad de Bézout para conjuntos constructibles

Sean C, $D \subseteq \mathbb{A}^n(K)$ dos conjuntos constructibles. Se verifica:

$$\deg_{\mathrm{lci}}(C \cap D) \leq \deg_{\mathrm{lci}}(C)\deg_{\mathrm{lci}}(D),$$

$$\deg_{\pi}(C \cap D) \leq \deg_{\pi}(C)\deg_{\pi}(D).$$

La Proposición 2.3. de [HeSc, 82] nos dice que:

$$\deg\left(\bigcap_{i=1}^{s} V_i\right) \leq \deg(V_1)\left(\text{máx}\{\deg(V_i)\ :\ 2 \leq i \leq s\}\right)^{\dim(V_1)}$$

donde V_i son variedades algebraicas.

Proposición: (6) Extensión de la Proposición 2.3. de [HeSc, 82]

Sea $\Omega \subseteq \mathbb{A}^n(K)$ un conjunto constructible y sean $W_1, \ldots, W_s \subseteq \mathbb{A}^n(K)$ una familia de conjuntos localmente cerrados. Entonces, se verifica:

$$\deg_{\mathrm{lci}}\left(\Omega \cap \left(\bigcap_{i=1}^{s} W_i\right)\right) \leq \deg_{\mathrm{lci}}(\Omega)\left(\text{máx}\{\deg_{\mathrm{lci}}(W_i)\ :\ 1 \leq i \leq s\}\right)^{\dim(\Omega)}$$

Proposición: (6) Generalización con el *LCI*-grado para conjuntos constructibles

Sean $C_1, \ldots, C_s$ una familia de conjuntos constructibles. Sea $r := \dim(C_1)$. Entonces,

(1) *Cota superior en el sentido de la Proposición 2.3. de [HeSc, 82]*:

$$\deg_\pi\left(\bigcap_{i=1}^{s} C_i\right) \leq \deg_{\mathrm{lci}}\left(\bigcap_{i=1}^{s} C_i\right) \leq$$

$$\leq \binom{s+r-1}{r} \deg_{\mathrm{lci}}(C_1)\left(\max\{\deg_{\mathrm{lci}}(C_j) \ : \ 2 \leq j \leq s\}\right)^r$$

(2) *Cota superior en términos del "grado medio"*: definimos el "grado medio" de la familia $C_1, \ldots, C_s$ como:

$$\deg_{\mathrm{av}}(C_1, \ldots, C_s) := \frac{1}{s}\sum_{i=1}^{s} \deg_{\mathrm{lci}}(C_i).$$

Entonces, tenemos que:

$$\deg_\pi\left(\bigcap_{i=1}^{s} C_i\right) \leq \deg_{\mathrm{lci}}\left(\bigcap_{i=1}^{s} C_i\right) \leq \deg_{\mathrm{lci}}(C_1)\, s^r \ \left(\deg_{\mathrm{av}}(C_1, \ldots, C_s)\right)^r.$$

Una consecuencia de la Extensión de la Proposición 2.3.

Lema: Variedades evasivas cero-dimensionales para conjuntos constructibles

Sea κ un cuerpo, $Q \subseteq \kappa$ un subconjunto finito y K la clausura algebraica de κ. Sea $C \subseteq \mathbb{A}^n(K)$ un conjunto constructible.

Entonces, el número de puntos de intersección de C y Q^n satisface:

$$\sharp\left(C \cap Q^n\right) \leq \deg_{\text{lci}}(C) \sharp(Q)^{\dim(C)}.$$

Dicho de otra forma,

$$\operatorname*{Prob}_{(x_1,\ldots,x_n)\in Q^n} [x \notin C] \geq 1 - \frac{\deg_{\text{lci}}(C)\sharp(Q)^{\dim(C)}}{\sharp(Q)^n} = 1 - \frac{\deg_{\text{lci}}(C)}{\sharp(Q)^{\operatorname{codim}(C)}}.$$

Si $C = V(f)$ es una hipersuperficie definida por un polinomio f no nulo, el Lema anterior es:

el test de DeMillo–Lipton–Schwartz–Zippel.

Generalizando la noción de conjunto cuestor

Nueva definición

Sea X un conjunto, K un cuerpo y $\mathcal{F}(X) \subseteq K^X$ un subgrupo del grupo abeliano $(K^X, +)$. Sea $m \in \mathbb{N}$ y sea $\Omega \subseteq \mathcal{F}(X)^m$ un conjunto de listas de funciones. Sea $\Sigma \subsetneq \Omega$ un subconjunto propio de Ω, que llamaremos discriminante.

Un conjunto cuestor de longitud L para Ω con discriminante Σ es un conjunto finito de L elementos $\mathbf{Q} := \{x_1, \ldots, x_L\} \subseteq X$ de forma que verifica la siguiente fórmula:

$$\forall f \in \Omega, \quad f(x_1) = \cdots = f(x_L) = 0 \in K^m \Longrightarrow f \in \Sigma.$$

Los conjuntos cuestores son omnipresentes y aparecen bajo distintos nombres en las matemáticas:

- "Identity sequences" en los tests de igualdad de funciones.
- "Norming sets" en el ámbito de las álgebras de Banach.
- "Samples" en el contexto de los Espacios de Hilbert con Núcleo Reproductor.

Sea $(d) := (d_1, \ldots, d_m)$ una lista de grados. Consideramos el conjunto de listas de polinomios:

$$\mathcal{P}_{(d)}^{K} := \mathcal{P}_{(d)}^{K}(X_1, \ldots, X_n) := \prod_{i=1}^{m} \mathcal{P}_{d_i}^{K}(X_1, \ldots, X_n).$$

Proposición: "Maldición de la dimensión" para conjuntos cuestores

Sea $\Omega \subseteq \mathcal{P}_{(d)}^{K}$ un conjunto constructible, $\Sigma \subsetneq \Omega$ un discriminante en Ω y $\mathbf{Q} \subseteq \mathbb{A}^n(K)$ un conjunto cuestor de longitud L para Ω con discriminante Σ. Entonces, tenemos que:

$$\sharp(\mathbf{Q}) = L \geq \mathrm{codim}_{\Omega}(\Sigma) = \dim(\Omega) - \dim(\Sigma).$$

Generalizando el Teorema fundamental de [HeSc, 82]

Teorema

Sean $\Sigma \subsetneq \Omega \subseteq \mathcal{P}_{(d)}^{K}$ conjuntos constructibles con $\mathrm{codim}_{\Omega}(\Sigma) \geq 1$. Supongamos que:

$$\forall f := (f_1, \ldots, f_m) \in \Omega \setminus \Sigma, \ \dim(V(f_1, \ldots, f_m)) = n - m.$$

Sea $C := V(h_1, \ldots, h_r) \subseteq \mathbb{A}^n(K)$ una variedad algebraica de intersección completa de co–dimensión $r \geq (n-m) + m/2 + 1/2$ tal que $\deg(C) \geq \delta^r$, donde $\delta := \min\{\deg(h_1), \ldots, \deg(h_r)\}$. Sea $L \in \mathbb{N}$ y supongamos que se verifican las siguiente propiedades:

- $L \geq 6 \dim(\Omega)$,
- $\log(\delta) \geq \max\{2(1 + \log(d+1)), \frac{2\log(\deg_{\mathrm{lci}}(\Omega))}{\dim(\Omega)}\}$,
- $\max\{\deg(h_1), \ldots, \deg(h_r)\} \leq (1 + \frac{1}{n-m})\delta$.

Sea $R := R(\Omega, \Sigma, C, L)$ el conjunto constructible de todas las listas de puntos $\mathbf{Q} \in C^L$ que son conjuntos cuestores para Ω con discriminante Σ. Entonces, existe un abierto Zariski no vacío $\mathbb{G}(C) \subseteq \mathbb{G}(n, n-r)$ tal que para cada $A \in \mathbb{G}(C)$ la probabilidad de que una lista $\mathbf{Q} \in (C \cap A)^L$ esté en R satisface:

$$\mathrm{Prob}_{(C\cap A)^L}[R] \geq 1 - \frac{1}{\deg_{\mathrm{lci}}(\Omega) e^{\dim(\Omega) + (m-1)L}}$$

En nuestra generalización del Teorema fundamental de [HeSc, 82] hemos añadido la siguiente hipótesis:

$$\forall f := (f_1, \dots, f_m) \in \Omega \setminus \Sigma, \ \dim(V(f_1, \dots, f_m)) = n - m$$

Esta hipótesis generaliza el caso $\Sigma = \{0\}$ e indica que el "asunto" de los conjuntos cuestores es la

dimensión

y no únicamente los test de nulidad.

Definición: Conjunto de Kakeya

Sea $\mathbb{F}_q$ un cuerpo finito de cardinal q. Decimos que subconjunto finito $E \subseteq \mathbb{A}^n(\mathbb{F}_q)$ es un conjunto de Kakeya si se verifica la siguiente propiedad:

Para cada punto proyectivo $v \in \mathbb{P}_{n-1}(\mathbb{F}_q)$, existe $x \in E$ tal que:

$$\rho(x, v) := \{x + tv \ : \ t \in \mathbb{F}_q\} \subseteq E$$

Cota inferior de Z. Dvir [Dv, 09]: si E es un conjunto de Kakeya, entonces:

$$\#(E) \geq \binom{q-1+n}{n}$$

Z. Dvir empleó como herramienta principal: **el Método Polinomial**.

Proposición

Sea $\mathbb{F}_q$ un cuerpo finito de cardinal q y $K := \overline{\mathbb{F}_q}$ su clausura algebraica.

Si $d \leq q-1$ y $E \subseteq \mathbb{A}^n(\mathbb{F}_q)$ es un conjunto de Kakeya, entonces E es un **conjunto cuestor** para P_d^K con discriminante $\Sigma = \{0\}$. En particular, tenemos que:

$$\sharp(E) \geq \dim\left(P_d^K\right) = \binom{d+n}{n}, \ \forall d \leq q-1.$$

¡Los conjuntos de Kakeya son conjuntos cuestores de longitud exponencial!

Proposición

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos y $K := \overline{\mathbb{F}_q}$ su clausura algebraica. Sea $d \in \mathbb{N}$ un grado y $k \in \mathbb{N}$ un entero positivo tal que:

$$d < q^{1-\frac{1}{k}} - 1. \tag{1}$$

Entonces, para $s := k\binom{d+n}{n}$, la probabilidad de que una lista de puntos $\mathbf{Q} \in \mathbb{A}^n(\mathbb{F}_q)^s$ sea un conjunto cuestor para P_d^K con discriminante $\Sigma = \{0\}$ es al menos:

$$1 - \frac{1}{q^{\dim(\Omega)}}.$$

En particular, dados d, k, q y n tales que:

$$k\binom{d+n}{n} < \frac{q^n}{2^n}, \tag{2}$$

y verifican la desigualdad (1), entonces **existen conjuntos cuestores para P_d^K con discriminante $\Sigma = \{0\}$ que no son conjuntos de Kakeya**.

Referencias

Los resultados expuestos en esta charla son parte del trabajo:

L. M. Pardo, D. Sebastián, *A promenade through Correct Test Sequences I: Degree of constructible sets, Bézout's Inequality and density*. To appear in J. of Complexity.

R.A. DeMillo, R.J. Lipton, *A probabilistic remark on algebraic program testing.* Information Processing Letters **7** (1978), 193–195.

Z. Dvir, *On the size of Kakeya sets on finite fields*. J. of the A.M.S. **22** (2009), 1093-1097.

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.

J. Heintz, *Definability and Fast Quantifier Elimination in Algebraically Closed Fields*. Theoret. Comput. Sci. **24** (1983), 239-277.

Referencias

J. Heintz, *Corrigendum: Definability and Fast Quantifier Elimination in Algebraically Closed Fields*. Theoret. Comput. Sci. **39** (1985), 343.

J. P. Schwarz, *Fast Probabilistic Algorithms for Verification of Polynomial Identities*. J. of the A.C.M. **27** (1980), 701-717.

R. Zippel, *Probabilistic Algorithms for Sparse Polynomials*. In *"Symbolic and Algebraic Computation (EUROSAM'79)"*, Lecture Notes in Computer Science **72**, Springer, 1979, 216-266.

¡Gracias!