¿CUAN DIFÍCIL ES RESOLVER UN SISTEMA DE ECUACIONES ALGEBRAICAS?

CARLOS A. BERENSTEIN

Prefacio

Todavía recuerdo que al comenzar mi primer curso en el viejo edificio de la calle Perú, el curso de Análisis I, encontré una pizarra anunciando el fallecimiento del Profesor Julio Rey Pastor. Claro que nuestra memoria sólo selecciona (y frecuentemente distorsiona) detalles sobre hechos o personas que han influido en nuestra vida. Como estudiante tuve la suerte de leer un poco varios de los libros de Rey Pastor y aprendí en ellos a valorar la unidad de las matemáticas, algo bastante contrario al espíritu que cundía entre mis contemporáneos en la Facultad. Ya desde el principio éramos algebristas o analistas o lógicos, etc. Es por ello que como pequeña contribución a este volumen dedicado al centenario del nacimiento de Rey Pastor, querría discutir un problema de álgebra que Alain Yger y yo hemos estado estudiando usando métodos analíticos. Es interesante que las ideas de Miguel Herrera sobre la teoría de residuos juegan un papel importante, y que parte de nuestros trabajos ha sido utilizada por Joos Heintz y sus colaboradores del Instituto Argentino de Matemáticas en cuestiones de complejidad. Herrera, yo y todos los matemáticos argentinos hemos sido en espíritu discípulos de Rey Pastor y pienso que él estaría contento de ver que su integrismo sigue siendo fecundo.

El problema a considerar es el siguiente. Sean $p_1, \dots, p_m$ polinomios a coeficientes enteros en n variables, $p_j \in \mathbb{Z}[z]$, queremos decidir si el sistema de ecuaciones algebraicas

$$p_1(z) = \dots = p_m(z) = 0 ,$$

tiene o no una solución en $\mathbb{C}^n$. Decidir significa dar un procedimiento efectivo con ayuda de computadoras, etc., para dar una respuesta afirmativa o negativa. La dificultad mencionada en el título se mide en el número de operaciones aritméticas necesarias para decidir. Recalco que los polinomios tienen coeficientes enteros por dos motivos, uno, no tener necesidad de usar aproximaciones, y otro, evitar cualquier razonamiento de tipo genérico. Además, en este problema no pedimos conocer las soluciones, sólo saber si ellas existen.

Inclusive el caso de polinomios cuadráticos parece tener interés en robótica, en el así llamado problema de la mudanza de pianos. J.Schwartz hizo la siguiente pregunta en una conferencia en Baltimore de la ACM:

Estimar el número de operaciones que se requieren para decidir si un sistema de 10 ecuaciones cuadráticas en 10 variables tiene una solución o no. Dar un algoritmo que tenga ese comportamiento. (Si bien él no lo mencionó, el resultado podría dar diferente si se tratara de decidir si hay soluciones en $\mathbb{R}^{10}$ o en $\mathbb{C}^{10}$).

La dificultad que existe es que el algoritmo de las bases de Groebner, que generaliza el algoritmo euclídeo, tiene una complejidad doble exponencial y el problema de Schwartz podría requerir un orden de magnitud de 10^{300} operaciones aritméticas. Claramente, si este fuera el caso, sería esencialmente indecidible. Veremos más abajo que resultados recientes implican una cota de 10^{30} operaciones y permiten conjeturar que quizá $10^8 - 10^{12}$ es el número más correcto. Notemos que esta conjetura diría que el problema es decidible en minutos, mientras que la cota 10^{30} requiere un tiempo del orden de magnitud de la edad del universo.

Agradezco a la Dra. S. Trione y a la U.M.A. la invitación a participar en este volumen de homenaje a Don Julio Rey Pastor. El texto está basado en una conferencia dada en el IAM en Diciembre de 1987, tomando debida cuenta de un gran número de resultados de los últimos meses.

1. Los trabajos de Brownawell y Kollár

El problema del prefacio es equivalente a poder dar un buen algoritmo que produzca polinomios $q_1, \dots, q_m \in \mathbb{Z}[z]$ y un número $\delta \in \mathbb{Z}^+$ tales que

$$(1) \quad \delta = p_1 q_1 + \dots + p_m q_m,$$

dado que si el algoritmo falla sabríamos que la variedad $V := \{z \in \mathbb{C}^m : p_1(z) = \dots = p_m(z) = 0\}$, no es vacía. Esta ecuación se llama a veces *ecuación de Bezout*.

Cuantificamos el problema introduciendo la notación $D := \max_j \{\text{grado } p_j\}$,

$h(p_j) := \log \max \{\text{valor absoluto de los coeficientes de } p_j\}$, $h := \max \{h(p_j)\}$. En el caso genérico de $V = \emptyset$, $m \geq n$, y los primeros n polinomios no tienen ceros comunes en ∞ , es un resultado de Macaulay que se pueden encontrar q_j que satisfacen la ecuación (1) y

$$(2) \quad \text{grado}(q_j) \leq mD.$$

Una vez que conocemos una tal cota, la ecuación (1) puede escribirse como un sistema de ecuaciones lineales cuyas incógnitas son los coeficientes de los polinomios q_j . La matriz correspondiente es de tamaño aproximado $(mD)^n \times m(mD)^n$. Se deduce que el sistema de ecuaciones lineales tiene por lo menos una solución si y sólo si $V = \emptyset$. Más aún esa solución $q_1, \dots, q_m, \delta$ puede escogerse con las cotas

$$(3) \quad \delta, h(q_j) \leq \kappa D^n (h + \log m),$$

donde $\kappa = \kappa(n)$ es una constante efectiva. El número de operaciones para decidir si hay una solución es también del orden de D^n (olvidando constantes dependientes de n, m).

Hay ejemplos muy sencillos mostrando que la cota (2) no es válida en general. El resultado de Brownawell fue demostrado usando una combinación de álgebra y análisis, y mejorado con respecto a las constantes por Kollár, da la cota optimal siguiente (ver los trabajos [4], [8] por más precisión):

Teorema 1. Si $V = \emptyset$ hay una solución $q_1, \dots, q_m$ de la ecuación de Bezout tal que

$$(4) \quad \text{grado}(q_j) \leq D^n.$$

Como corolario vemos que si consideramos la ecuación de Bezout como un sistema de ecuaciones lineales en el espacio vectorial de polinomios de grado D^n , la matriz correspondiente será de tamaño aproximado $D^{n^2} \times mD^{n^2}$. Nuevamente, esto nos da un método de decisión con aproximadamente D^{n^2} operaciones. Si hay una solución se obtiene en vez de (3)

$$(5) \quad \delta, h(q_j) \leq \kappa D^{n^2} (h + \log m).$$

Notamos que cuando $D = 2, n = 10, D^{n^2} \cong 10^{30}$ como dijimos en el prefacio.

Cuando se llega a este punto es natural preguntarse si un algoritmo más sutil no reduciría el tamaño de los coeficientes de q_j (y automáticamente el de δ), así como el número de operaciones requeridas para decidir si $V = \emptyset$ o no. El algoritmo de Euclides de división de polinomios de una variable tiene un elegante análogo, el algoritmo de Buchberger, generalmente conocido como método de las bases de Groebner [5], (Groebner fue el profesor de Buchberger). Este algoritmo tiene la ventaja que su programación en computadoras es muy simple. Dada una familia finita de polinomios $p_1, \dots, p_m$ se construye la base de Groebner del ideal I engendrado por ellos en $Z[z]$, y conocida esta base todos los problemas típicos de álgebra asociados a un tal ideal son de resolución casi inmediata. En particular, la decisión si $V = \emptyset$ o no. El problema surge de la propia potencia del algoritmo. Es capaz de decidir inmediatamente si un polinomio $f \in I$ o no. Pero hay un ejemplo de Mayr-Meyer [9] que muestra la existencia de polinomios $f_1, \dots, f_{n+1}$ de grado D tales que el polinomio $z_1 \in I(f_1, \dots, f_{n+1})$ pero si $a_j \in Z[z]$ y

$$z_1 = f_1 a_1 + \dots + f_{n+1} a_{n+1}$$

entonces, "grossó modo"

$$\max_j \text{grado}(a_j) \geq D^{2^n}.$$

Es claro que en este caso $V(f_1, \dots, f_{n+1}) \neq \emptyset$. Stillman ha concluido que el proceso de búsqueda de la base de Groebner es en general de complejidad doble exponencial. Claro que podríamos preguntarnos si no es posible modificar este algoritmo de manera de decidir el problema en discusión en complejidad D^n . Hay cuatro o cinco resultados que indican que quizás tal modificación sea posible. Los tres primeros se refieren al ejemplo de Mayr-Meyer.

Teorema 2 (Nullstellensatz) [4], [8]. Sean $f_1, \dots, f_n, f$ polinomios de n variables de grado $\leq D$, f se anula en $V(f_1, \dots, f_n)$. Existe un entero positivo $s \leq D^n$ y polinomios g_j de grado $\leq D^n$ tales que

$$f^s = \sum_{j=1}^n f_j g_j.$$

Este teorema fue demostrado por Brownawell usando una astuta modificación del método de Rabinowitsch para reducirlo al Teorema 1. En particular, quizá sea posible decidir si un polinomio f está en el radical de un ideal I con complejidad a lo sumo D^n o quizá D^n . Un manuscrito de Heintz et al. [6] parecería indicar que D^n es ya posible.

Usando métodos enteramente analíticos sobre el complejo de Koszul hemos demostrado los siguientes dos teoremas que podrían explicar porqué frecuentemente el método de las bases de Groebner funciona a pesar del ejemplo de Mayr-Mayer.

Teorema 3 [3]. Sean $f, f_1, \dots, f_m$ polinomios en C^n de grado a lo sumo $D, f \in I(f_1, \dots, f_m)$ y $V(f_1, \dots, f_m)$ es discreta en C^n . Existen entonces polinomios g_j tales que $f = f_1 g_1 + \dots + g_m$ y

$$\text{grado}(g_j) \leq 3(n+1)D^n.$$

Por métodos algebraicos B. Shiffman a obtenido un resultado similar con la hipótesis adicional de que también la variedad en ∞ de $f_1, \dots, f_m$ sea discreta.

Teorema 4 [3]. *Sea $2 \leq m \leq n-1$, $f, f_1, \dots, f_m$ polinomios de grado a lo sumo D , $f \in I(f_1, \dots, f_m)$ y $\text{diam } V(f_1, \dots, f_m) = n - m$. Existe una constante $\kappa = \kappa(n)$ y polinomios g_j tales que $f = f_1 g_1 + \dots + f_m g_m$ y*

$$\text{grado}(g_j) \leq \kappa D^n.$$

2. La teoría de residuos y fórmulas de división

Sean $f_1, \dots, f_n \in \mathbb{C}[z_1, \dots, z_n]$ que definen una variedad discreta (y finita) en $\mathbb{C}^n$ y R una función racional con polos fuera de V . Se puede definir el residuo

$$(6) \quad \text{Res}_f \text{Rd}\zeta := \langle \bar{\partial} \frac{1}{f}, \text{Rd}\zeta \rangle := \lim_{\substack{\varepsilon_j \rightarrow 0 \\ j=1, \dots, n}} \frac{1}{(2\pi i)^n} \int_{|f_j| \leq \varepsilon_j} \frac{R(\zeta) d\zeta_1 \wedge \dots \wedge d\zeta_n}{f_1(\zeta) \dots f_n(\zeta)}$$

Este residuo se puede también calcular de la siguiente manera. Sea χ una función C^∞ de soporte compacto, $\chi=1$ en un entorno de V . Consideremos la función de una variable compleja λ , holomorfa cuando $\text{Re } \lambda > 1, \mathbb{C}$

$$(7) \quad \lambda \rightarrow \frac{(-1)^{n(n-1)/2}}{(2\pi i)^n} \lambda^n \int_{\mathbb{C}^n} \frac{R(\zeta) \chi(\zeta) |f_1(\zeta) \dots f_n(\zeta)|^{2(\lambda-1)}}{\bar{\partial} f_1(\zeta) \wedge \dots \wedge \bar{\partial} f_n(\zeta) \wedge d\zeta_1 \wedge \dots \wedge d\zeta_n}$$

Esta función tiene una continuación analítica como función meromorfa a todo el plano complejo. Es holomorfa en $\lambda = 0$ y su valor allí coincide con (6) (ver [1]) Esta definición de residuos es válida para toda función R de clase C^∞ , coincidiendo con la definición de Herrera-Coleff [7].

Una variación de esta fórmula también puede ser demostrada. Para ello necesitamos un poco de notación. Si $m \in \mathbb{N}^n$, sea $m+1 = (m_1+1, \dots, m_n+1)$, $m! = \dots m_n!$, $|m| = m_1 + \dots + m_n$, $\bar{f}^m = \bar{f}_1^{m_1} \dots \bar{f}_n^{m_n}$, $\bar{\partial} f = \bar{\partial} f_1 \wedge \dots \wedge \bar{\partial} f_n$, $F = f_1 \dots f_n$, $\|f\|^2 = \sum_{j=1}^n |f_j|^2$. Los polinomios

$\bar{f}_1^{m_1+1}, \dots, \bar{f}_n^{m_n+1}$ definen la misma variedad V y podemos ver que la función

$$(8) \quad \lambda \rightarrow \frac{(-1)^{n(n-1)/2}}{(2\pi i)^n} \lambda^n \int_{\mathbb{C}^n} \frac{|\mathbb{F}|^{2(n+|m|)\lambda}}{\|f\|^{2(n+|m|)}} \bar{f}^m \bar{\partial} f \wedge d\zeta, \quad (\varphi \in \mathcal{D}(\mathbb{C}^n))$$

tiene una continuación analítica cuyo valor en $\lambda = 0$ es

$$(9) \quad \frac{m!}{(n+|m|)!} < \bar{\partial} \frac{1}{f^{m+1}}, \quad \langle \varphi, d\zeta \rangle,$$

donde el residuo (8) es definido por (7) (ó (6) si $\varphi = \chi_R$ como arriba) reemplazando $f_1, \dots, f_n$ por $f_1^{m_1+1}, \dots, f_n^{m_n+1}$.

Definimos n^2 polinomios de $2n$ variables, $g_{j,k}$ como sigue

$$(10) \quad g_{j,k}(z, \zeta) = \frac{f_j(\zeta_1, \dots, \zeta_{k-1}, z_{k+1}, \dots, z_n) - f_j(\zeta_1, \dots, \zeta_k, z_{k+1}, \dots, z_n)}{z_k - \zeta_k}$$

Tenemos que $\text{grado}(g_{j,k}) \leq \text{grado}(f_j)$ y si $f_j \in \mathbb{Z}[z]$, $g_{j,k} \in \mathbb{Z}[z, \zeta]$, $h(g_{j,k}) \leq h(f_j) + 2n \log(\text{grado}(f_j) + 1)$.

Supongamos ahora que si $\|z\| \gg 1$, $\|f(z)\| \geq \gamma \|z\|^\delta$, ($\gamma, \delta > 0$). Sea f_{n+1} un polinomio tal que $V(f_1, \dots, f_n, f_{n+1}) = \emptyset$. Suponiendo que $\max_j \text{grado}(f_j) \leq D$ sea q un entero tal que $\delta q > (n-1)(2D - \delta) + 1$.

Teorema 5 [2]. *Bajo estas condiciones la siguiente identidad es válida en $\mathbb{C}^n$.*

$$(11) \quad \sum_{\substack{m \in \mathbb{N}^n \\ |m| \leq q-n}} < \bar{\partial} \frac{1}{f^{m+1}}, \frac{1}{f_{n+1}} \left| \begin{array}{ccc} g_{1,1}(z, \cdot) & \dots & g_{n+1,1}(z, \cdot) \\ \vdots & & \vdots \\ g_{1,n}(z, \cdot) & \dots & g_{n+1,n}(z, \cdot) \\ f_1(z) - f_1(\cdot) & \dots & f_{n+1}(z) \end{array} \right| d\zeta > f^m(z) = 1.$$

Esta identidad define polinomios G_j , $1 \leq j \leq n+1$, tales que

$$1 = f_1 G_1 + \dots + f_n G_n + f_{n+1} G_{n+1}.$$

Si $f_1, \dots, f_n, f_{n+1} \in \mathbb{Z}[z]$ entonces $G_j \in \mathbb{Q}[z]$.

Esta fórmula nos da una representación explícita de una solución de la ecuación de Bezout, pero requiere usar la variedad V y requiere la condición $\|f(z)\| \geq \gamma \|z\|^{\delta}$ en infinito. De todas maneras forma la base de la sección siguiente.

3. Estimaciones efectivas en la ecuación de Bezout

Retornemos a la situación de la primera sección, es decir, $p_1, \dots, p_m \in \mathbb{Z}[z]$, $\max_j \text{grado}(p_j) \leq D$, $\max_j h(p_j) \leq h$, $V = V(p_1, \dots, p_m) = \{z \in \mathbb{C}^n : p_1(z) = \dots = p_m(z) = 0\} = \emptyset$.

Teorema 6 [2]. *Bajo estas condiciones existe una constante efectiva $\kappa = \kappa(n)$, polinomios $q_j \in \mathbb{Z}[z]$ and $\delta \in \mathbb{Z}^+$ verificando la ecuación de Bezout (1) y tales que*

$$(12) \quad \text{grado}(q_j) \leq 10(n+1)^5 (2D+1)^{2n}$$

$$(13) \quad h(q_j), \log \delta \leq \kappa D^{9n+3} (h + \log m + D \log D).$$

Es decir perdemos un poco en el grado de q_j con respecto a (4), a cambio de ganar en (13) con respecto a (5).

Conjetura. (i) Las constantes 2 y 9 en (12) y (13) no son necesarias. (ii) La complejidad de decidir si $V = \emptyset$ o no es del orden de D^n .

Esbozo de demostración. El primer paso consiste en reemplazar $p_1, \dots, p_m$ por polinomios $P_1, \dots, P_n, f_{n+1}$. (i) $V(P_1, \dots, P_n)$ tiene dimensión cero pero no es vacía. (ii) $V(P_1, \dots, P_n, f_{n+1}) = \emptyset$. (iii) $P_1, \dots, P_n, f_{n+1}$ están en ideal generado por $p_1, \dots, p_m$ con coeficientes no muy grandes. (iv) $\text{grado}(P_j) \leq 2D+1$, $\text{grado}(f_{n+1}) \leq D$. Esta construcción es más o menos standard.

Una desigualdad de Brownawell que se usa en la demostración del Teorema 1 muestra que si $\|z\| \gg 1$

$$(14) \quad \left[\sum_{j=1}^n |P_j(z)|^2 \right]^{1/2} \geq c \|z\|^{-(2D+1)^n} \quad (c > 0).$$

Para poder utilizar el Teorema 5 necesitamos cambiar P_j , sin incrementar mucho el número de puntos de $V(P_1, \dots, P_n)$, o el tamaño de los coeficientes, pero con buenas condiciones en ∞ . El punto crucial es que existen formas lineares $L_1, \dots, L_n$ de coeficientes enteros, $h(L_j) \leq \kappa D^n (h + \log m + D \log D)$ y tales que si $p = 2(n+1)^2 (2D+1)^n + 1$, definiendo $f_1 = L_1^p P_1, \dots, f_n = L_n^p P_n$, entonces

$$\|z\| \gg 1 \Rightarrow \|f(z)\| = \left[\sum_{j=1}^n |f_j(z)|^2 \right]^{1/2} \geq c \|z\|.$$

Esto nos permite usar Teorema 5 y construir polinomios $G_j \in \mathbb{Q}[z]$. Usando las propiedades de residuos mencionadas más arriba, una desigualdad de Philippon [10] y bastante análisis se llega a estimar un denominador común δ de todos los coeficientes de G_j . Multiplicando por éste y con un poco más de trabajo prueban el teorema.

Conclusión Hemos explicado qué métodos analíticos de la teoría de varias variables complejas pueden usarse para obtener resultados algebraicos muy interesantes que, por el momento, no tienen demostraciones algebraicas. Estos indican que el problema de decidir si un sistema de ecuaciones algebraicas tiene solución o no debiera ser de complejidad D^n .

Referencias

- [1] BERENSTEIN, C.A., GAY, R. y YGER, A.Y. *Analytic continuation of currents and division problems*, por aparecer en Forum Math.
- [2] BERENSTEIN, C.A. y YGER, A. *Effective Bezout identities in $\mathbb{Q}[z_1, \dots, z_n]$* , Acta Math.
- [3] BERENSTEIN, C.A. y YGER, A. *Bounds for the degrees in the division problem*, Mich Math. J.
- [4] BROWNAWELL, W.D. *Bounds for the degrees in the Nullstellensatz*, Annals of Math. 126 (1987), 577-592.
- [5] BUCHBERGER, B. *An algorithmic method in polynomial ideal theory*, Multidimensional systems theory (ed. N.K.Bose), Reidel Publ., Dordrecht, 1985.
- [6] CANIGLIA, L., GALLIGO, A. y HEINTZ, J. *Some new effectivity bounds in computational geometry*, manuscrito.
- [7] COLEFF, N. y HERRERA, M. *Les courants résiduels associés a une forme meromorphe*, Lecture Notes in Math 633, Springer, Berlin, 1978.
- [8] KOLLÁR, J. *Sharp effective Nullstellensatz*, manuscrito.
- [9] MAYR, E. y MEYER, A. *The complexity of the word problem for commutative semi groups and polynomial ideals*, Advances in Math. 46 (1982), 305-329.
- [10] PHILIPPON, P. *Inégalités valuatives de type Liouville-Lojasiewicz et théorème des zéros de Hilbert*, manuscrito.
- [11] BERENSTEIN, C.A. y STRUPPA, D.C. *Small degree solutions for the Bezout equation*, Linear Algebra and its Applications 98 (1988), 41-55.

Department of Mathematics
University of Maryland
College Park, MD 20742

Recibido el 16 de mayo de 1989.