LA COLUMNA DE MATEMÁTICA COMPUTACIONAL

Sección a cargo de

Tomás Recio

LA COLUMNA

El objetivo de esta columna es presentar de manera sucinta, en cada uno de los números de *La Gaceta*, alguna cuestión matemática en la que los cálculos, en un sentido muy amplio, tengan un papel destacado. Para cumplir este objetivo el editor de la columna (sin otros méritos que su interés y sin otros recursos que su mejor voluntad) quisiera contar con la colaboración de los lectores, a los que anima a remitirle (a la dirección que se indica al final de esta columna) los trabajos y sugerencias que consideren oportunos.

EL NÚMERO DE RAÍCES REALES DE UN POLINOMIO

Determinar el número de raíces reales de un polinomio de grado n, $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, es un problema clásico al que uno puede aproximarse de diversas formas. Supongamos, para restringir la temática, que el polinomio $f(x)$ tiene coeficientes enteros, que podemos manipular tales números sin problemas de precisión y que buscamos algoritmos *exactos* cuyo resultado sea el número de raíces reales de $f(x)$.

En tal caso el algoritmo de Sturm es, posiblemente, el más conocido. Procede dividendo, al modo euclídeo, el polinomio dado $f(x)$ (que renombraremos $f(x) = f_0(x)$) por su polinomio derivado $f'(x) = f_1(x)$; tomando, luego, el resto de esta división multiplicado por -1, digamos $f_2(x) = f(x) - f'(x)q(x)$ y continuando con este proceso mediante la división sucesiva de f_{i-1} por f_i, etc... Se calcula el signo en $-\infty$ y en $+\infty$ de cada uno de los polinomios de la sucesión $\{f_0, f_1, f_2, \ldots, f_r\}$ así obtenida. Sean estas dos sucesiones de signos $\{f_0, f_1, f_2, \ldots, f_r\}_{-\infty}$ y $\{f_0, f_1, f_2, \ldots, f_r\}_{+\infty}$, respectivamente. Entonces el número de raíces reales distintas de $f(x)$ es exactamente la diferencia entre el número de alternancias de signo (también llamadas *variaciones* de signo) presentes en $\{f_0, f_1, f_2, \ldots, f_r\}_{-\infty}$ y el número de alternancias de signo de $\{f_0, f_1, f_2, \ldots, f_r\}_{+\infty}$. Es decir:

$$Var\{f_0, f_1, f_2, \ldots, f_r\}_{-\infty} - Var\{f_0, f_1, f_2, \ldots, f_r\}_{+\infty}$$

EJEMPLO

El siguiente ejemplo de cálculo de la sucesion de Sturm está realizado mediante un pequeño programa de Maple V (Release 2), sin utilizar, para mejor comprensión del proceso, la llamada a la función *sturmseq* de Maple, que daría directamente la sucesión L. La ultima instrucción trata de obtener el output en forma Latex.

```
> P_(0):=subs(a=-5, b=0, c=1, x^4+a*x^2+b*x+c):
  P_(1):=diff(P_(0),x): L:=[P_(0),P_(1)]:

          for j from 2 to 4
                         do
                P_(j):=-rem(P_(j-2),P_(j-1),x):
                L:=[op(L),P_(j)]:
           od:
          latex(L);
```

$$[x^4 - 5\,x^2 + 1, 4\,x^3 - 10\,x, \frac{5\,x^2}{2} - 1, \frac{42\,x}{5}, 1]$$

Obviamente, la lista L de polinomios tiene los signos $[+,-,+,-,+]$ en $-\infty$ y los signos $[+,+,+,+,+]$ en $+\infty$, luego tiene 4 y 0 variaciones de signo, respectivamente. Así pues, tendremos $4-0=4$ raíces reales para el polinomio $x^4 - 5\,x^2 + 1$.

EL PROBLEMA DE LA ESPECIALIZACIÓN

El método que acabamos de esbozar tiene algunos inconvenientes. Uno de ellos (entre otros) es que no es *especializable*. Expliquemos esto. Por ejemplo, un polinomio de grado dos $x^2 + bx + c$ tiene dos raíces reales si $b^2 - 4c > 0$; o una sóla raíz real si $b^2 - 4c = 0$. Tenemos en ambos casos una fórmula que vale, tras sustitución de las letras $\{b, c\}$ por los coeficientes correspondientes (la *especilización* de la fórmula), para cualquier polinomio de grado dos. Análogamente, sería muy deseable que el cálculo del número de raíces reales de cualquier polinomio de un grado fijo n pudiese hacerse del mismo modo, calculando la sucesión de Sturm para un sólo polinomio *genérico* de grado n, con coeficientes indeterminados, y luego asignando a dichas indeterminadas, en cada polinomio de la sucesión, los valores concretos de los coeficientes de cada polinomio específico. Calculemos, como en el ejemplo anterior, la sucesión de Sturm para el polinomio genérico de grado 4, $x^4 + ax^2 + bx + c$, en el que mediante una pequeña transformación hemos eliminado el término de grado 3.

$$[x^4 + ax^2 + bx + c, 4\,x^3 + 2\,ax + b, -\frac{ax^2}{2} - \frac{3\,bx}{4} - c,$$

$$-\frac{(-8\,ac + 9\,b^2 + 2\,a^3)\,x}{a^2} - \frac{b\,(12\,c + a^2)}{a^2},$$

$$\frac{a^2\,(256\,c^3 - 128\,a^2c^2 + 144\,acb^2 + 16\,a^4c - 27\,b^4 - 4\,b^2a^3)}{4\,(-8\,ac + 9\,b^2 + 2\,a^3)^2}]$$

Desgraciadamente, salvo casos como el de grado dos, la sucesión de Sturm no es especializable, pues la división de polinomios procede verificando si ciertos coeficientes del divisor son o no son cero (y la respuesta a esta comprobación será diversa para valores concretos de los coeficientes de diversos polinomios). Por ejemplo, en el cálculo precedente es claro que no se puede sustituir el valor $a = 0$ en la sucesión obtenida.

EL MÉTODO DE HERMITE

Una solución clásica a este problema de especialización consiste en determinar el número de raíces reales de otro modo, como la signatura de una forma cuadrática peculiar que se construye a partir del polinomio dado. Brevemente, se considera la matriz simétrica cuya primera fila está formada por las sumas de Newton $N_0, N_1, \ldots, N_{d-1}$ de las raíces del polinomio, cuya segunda fila tiene la sumas $N_1, N_1, \ldots, N_d$, etc. . . y cuya fila d-ésima tiene las sumas $N_{d-1}, N_1, \ldots, N_{2d-2}$. Las sumas de Newton N_i se definen como las sumas de las potencias i-ésimas de las raíces (reales o complejas) del polinomio; como son unas funciones simétricas en estas raíces, se pueden expresar en términos de los coeficientes del polinomio dado. Por ejemplo, en el caso del polinomio genérico de grado 4 descrito arriba,

$$N_0 = 4, \quad N_1 = 0, \quad N_2 = -2a, \quad N_3 = -3b, \quad N_4 = 2a^2 - 4c,$$

$$N_5 = 5ab, \quad N_6 = -2a^3 + 6ac + 3b^2$$

Consideraríamos, pues, la matriz,

$$\begin{bmatrix} 4 & 0 & -2\,a & -3\,b \\ 0 & -2\,a & -3\,b & 2\,a^2 - 4\,c \\ -2\,a & -3\,b & 2\,a^2 - 4\,c & 5\,ab \\ -3\,b & 2\,a^2 - 4\,c & 5\,ab & -2\,a^3 + 6\,ac + 3\,b^2 \end{bmatrix}$$

y hallaríamos su signatura (la diferencia entre el número de raíces positivas y negativas de su polinomio característico) en función de los parámetros $\{a, b, c\}$, por ejemplo, como la diferencia entre el número de permanencias y de variaciones de signo de la sucesión de menores principales de la matriz (añadiendo un término constante igual a 1 al comienzo de esta sucesión):

$$\delta_0 = 1, \delta_1 = 4, \delta_2 = -8\,a, \delta_3 = -8\,a^3 + 32\,ac - 36\,b^2$$

$$\delta_4 = 16\,a^4c - 4\,a^3b^2 - 128\,a^2c^2 + 144\,acb^2 - 27\,b^4 = 256\,c^3$$

Naturalmente, este proceso matricial es bastante especializable, puesto que las funciones simétricas se especializan bien y lo mismo ocurre con el cálculo de determinantes. Para el ejemplo con los valores $a = -5, b = 0, c = 1$ si repetimos el proceso de hallar las sumas de Newton obtendríamos la matriz

$$\begin{bmatrix} 4 & 0 & 10 & 0 \\ 0 & 10 & 0 & 46 \\ 10 & 0 & 46 & 0 \\ 0 & 46 & 0 & 220 \end{bmatrix}$$

y la sucesión de menores $\{1, 4, 40, 840, 7056\}$, que tiene cuatro permanencias de signo y ninguna variación, lo que confirma la existencia de cuatro raíces reales conocida previamente a través del método de Sturm. Compruébese que la misma sucesión $\{1, 4, 40, 840, 7056\}$ se obtiene directamente sustituyendo los valores elegidos en cada una de las expresiones simbólicas δ_i de los menores principales calculadas arriba. Una referencia que puede ser útil para más detalles sobre este método y para la gran cantidad de desarrollos actuales relacionados con él (polinomios subresultantes, sucesión de Sturm-Habicht, etc...) es [3].

LA ESPECIALIZACIÓN DE LA FÓRMULA

Con el método de Hermite acabamos de observar que el recuento del número de raíces reales puede realizarse a través de una *única sucesión de polinomios* en ciertos parámetros, dando valores concretos a los mismos. Pero ocurre ahora que el cálculo de las permanencias y las variaciones de signo de una sucesión presenta problemas de especialización. Veamos un caso: es obvio que el polinomio genérico de grado cuatro tiene cuatro raíces reales si $\delta_1 > 0, \delta_2 > 0, \delta_3 > 0, \delta_4 > 0$ (pues es la única forma de obtener cuatro permanencias de signo y ninguna variación, dado que $\delta_0 = 1$ siempre). Pero, ¿cómo debemos acomodar esta conjunción de desigualdades estrictas de modo que represente el conjunto de valores concretos de los coeficientes $\{a, b, c\}$ tales que el polinomio de grado cuatro correspondiente tenga todas sus raíces reales (esto es, que sea un polinomio hiperbólico)? Resulta que el conjunto de R^3 formado por los coeficientes de los polinomios hiperbólicos de grado cuatro es cerrado (en la topología euclídea) y definible a través de desigualdades polinómicas (usando alguno de los métodos esbozados arriba), luego puede escribirse con sólo desigualdades $\geq$ (por el denominado Teorema de Finitud, ver [5], [1]) ¿Será igual al conjunto $\delta_1 \geq 0, \delta_2 \geq 0, \delta_3 \geq 0, \delta_4 \geq 0$? Ahora bien, cuando $a = 0, b = 0, c = 1$ tenemos $\delta_1 = 4, \delta_2 = 0, \delta_3 = 0, \delta_4 = 256$, pero el polinomio $x^4 + 1$ no tiene ninguna raíz real, luego esta forma "evidente"de especializar la fórmula no es correcta.

Del mismo modo, cualquier combinación (conjunción y disyunción) de signos *estrictos* de los polinomios δ_i que exprese la existencia de raíz real para el polinomio genérico va requerir el estudio específico de los casos en los que alguno de ellos se anula. Aunque el conjunto de coeficientes que corresponden a polinomios de grado cuatro con alguna raíz real es cerrado, los signos de la fórmula genérica obtenida vía Hermite no son especializables mediante la simple regla de sustituir las desigualdades estrictas $>$ por desigualdades laxas $\geq$. En el caso de polinomios de grado cuatro, como los que estamos tratando, hay dos raíces reales si $\delta_2 < 0, \delta_3 < 0, \delta_4 < 0$ (por ejemplo, si $a = 1, b = -1, c = -1$); pero no hay ninguna raíz real si $\delta_2 < 0, \delta_3 = 0, \delta_4 = 0$ (por ejemplo, si $a = 1, b = 0, c = 1/4$). Este problema, bien conocido desde hace tiempo, se debe a que el cálculo de la signatura como diferencia entre permanencias y variaciones de signo de la sucesión de menores principales no funciona correctamente cuando hay ceros intermedios en la misma, aunque puede resolverse asignando mediante cierto convenio un signo *ficticio* a los ceros intermedios (veáse [2]). Por ejemplo, puede establecerse que no hay ninguna raíz real si y sólo si los coeficientes verifican

$$\{\delta_2 \leq 0 \wedge \delta_4 > 0\} \vee \{\delta_2 < 0 \wedge \delta_3 = 0\} \vee \{\delta_2 > 0 \wedge \delta_3 < 0 \wedge \delta_4 > 0\}$$

mientras que la fórmula genérica se reduce a

$$\{\delta_2 < 0 \wedge \delta_4 > 0\} \vee \{\delta_2 > 0 \wedge \delta_3 < 0 \wedge \delta_4 > 0\}.$$

EL TAMAÑO DE LA FÓRMULA

El lector puede pensar, llegado a este punto, que así quedaría resuelto el problema de determinar el número de raíces reales para cada polinomio de un grado dado con un sólo cálculo para cada grado, considerando coeficientes genéricos, el método de Hermite (u otros métodos especializables) y utilizando el recurso a esos signos ficticios a los que acabamos de hacer referencia.

Pero esta solución, en cualquier caso, requiere escribir la fórmula que exprese el número de raíces reales con muchas más disyunciones de signos (positivo, cero o negativo) sobre los polinomios δ_i que en el caso genérico, pues precisa abrir una nueva disyunción, en principio, para cada posible anulación de uno de estos polinomios. Naturalmente, si deseamos tener esa fórmula precalculada para utilizarla muchas veces con cada polinomio específico, deberíamos preocuparnos del coste computacional de evaluarla. Se pueden plantear, pues, cuestiones del siguiente tipo:

- ¿Habrá algún otro procedimiento algorímico cuyo resultado sea, digamos, una fórmula genérica que exprese la existencia de raíz real, pero de modo que esta se especialice mediante la simple sustitución de los signos $>$ por $\geq$?

- ¿Habrá una fórmula (expresando la existencia de raíz real) válida para todos los polinomios de grado cuatro que no necesite disyunciones o sólo muy pocas?

Obviamente, podemos formular preguntas similares para polinomios de otros grados o para la determinación de un número concreto de raíces reales, etc... La respuesta a la primera pregunta es afirmativa: es posible construir algorímicamente, a partir de una fórmula genérica, otra descripción de la misma (como unión e intersección de desigualdades estrictas con otros polinomios) tal que la clausura topolólogica se obtenga por el simple procedimiento de relajar las desigualdades estrictas a desigualdades laxas en esta nueva descripción. El argumento utilizado se basa en un lema de R. Thom (véase [1]) y no es totalmente trivial. El nuevo problema que surge es que el número de los polinomios que aparecen en la nueva forma de escribir la fórmula genérica a la Thom es muy elevado (siguiendo el método que se conoce hoy día; tal vez haya otro mejor...): hay que añadir, para empezar, los polinomios involucrados en la descripción de partida y todas sus derivadas,...

La respuesta a la segunda pregunta es negativa y sirve para ejemplificar otro aspecto interesante del problema de la especialización. Si pudieramos expresar el conjunto

$$\{(a,b,c) \in R^3 / \exists r \in R, r^4 + ar^2 + br + c = 0\}$$

como una intersección de desigualdades e igualdades polinómicas, entonces podríamos aplicar esta expresión al polinomio $(x^2+t_1)(x^2+t_2)$ que tiene alguna raíz real si y sólo si $\{t_1 \leq 0\} \vee \{t_2 \leq 0\}$. Ahora bien, este conjunto no es expresable mediante una simple intersección de condiciones de signo: es necesario introducir alguna disyunción (veáse [4]).

Naturalmente, ambas preguntas son casos muy sencillos de la verdadera cuestión de fondo: hallar una forma de expresar la existencia de de raíz real, que sea válida por sustitución para todos los polinomios de un grado dado y que sea la *mas simple* de evaluar, donde la simplicidad debe medirse en algún modelo de computación adecuado (árboles de computación, straight line programs, etc. . .). Un problema básico en este contexto es, para empezar, la determinación de algunas cotas inferiores al tamaño de la fórmula. Se sabe muy poco acerca de ello: los escasos resultados obtenidos en algunas de las referencias [4], apuntan a que una tal fórmula debe crecer al menos linealmente con el grado del polinomio, pero las cotas superiores conocidas (usando alguno de los métodos expuestos aquí) son exponenciales en dicho grado!

Referencias

[1] BOCHNAK, J.; COSTE, M. Y ROY, M.F.: *Géométrie Algebrique Réelle.* Ergebnisse, Folge 3, Band 12. Springer, 1987.

[2] GANTMACHER, F.: *Théorie des Matrices*, Dunod, Paris, 1966.

[3] RECIO, T.; GONZÁLEZ, L.; ROY, M.F. Y LOMBARDI, H.: *Sturm-Habicht Sequences, Determinants and Real Roots of Univariate Polynomials.* In: Quantifier Elimination and Cylindrical Algebraic Decomposition. Bob Caviness and Jeremy Johnson Eds. Series: Texts and Monographs in Symbolic Computation Publisher: Springer-Verlag, Wien, New York. 1998. ISBN: 3-211-82794-3

[4] MONTAÑA, J. L.; PARDO, L.M. Y RECIO,T.: *A note on Rabin's width of a complete proof.* Computational Complexity (1994), 12-36.

[5] RECIO, T.: Una descomposición de un conjunto semialgebraico. Actas V Reunión Matemáticos de Expresión Latina, Mallorca, 1978.

Tomás Recio. Departamento de Matemáticas. Facultad de Ciencias. Univ. de Cantabria. 39071 Santander. Dirección electrónica: recio@matesco.unican.es