La Columna de Matemática Computacional

Sección a cargo de

Tomás Recio

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 pie de página*[1]*) los trabajos y sugerencias que consideren oportunos.*

En este número...

Para este número de *La Gaceta* hemos solicitado la colaboración del joven ayudante de la Universidad Pública de Navarra, Mikel Aldaz Zaragüeta, que realiza su tesis doctoral con los profesores J. L. Montaña (U.P.Na.) y L.M. Pardo (U. Cantabria), en el seno del grupo multinacional de investigación TERA que coordina el profesor J. Heintz (U. Buenos Aires y U. Cantabria).

En este artículo Aldaz presenta, con un enfoque eminentemente divulgativo, un problema de planteamiento sencillo pero de gran trascendencia en la teoría de la complejidad computacional algebraica: la evaluación de polinomios. Tras una introducción elemental se aborda una nueva y sorprendente técnica, debida a Aldaz et al., para estimar la dificultad de evaluar ciertos tipos de polinomios, con una curiosa aplicación al establecimiento de nuevas familias de series trascendentes.

[1]Tomás Recio. Departamento de Matemáticas. Facultad de Ciencias. Universidad de Cantabria. 39071 Santander. recio@matesco.unican.es

Un método combinatorio para la obtención de polinomios difíciles de evaluar y series trascendentes

por

Mikel Aldaz Zaragüeta

INTRODUCCIÓN

La regla de Horner muestra que todo polinomio univariado de grado d, $F := a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0$, puede ser evaluado en un valor numérico cualquiera x empleando para ello no más de d sumas y d productos. El cálculo de $F(x)$ está basado en la fórmula

$$F(x) = (\ldots(((a_d \cdot x + a_{d-1}) \cdot x + a_{d-2}) \cdot x + a_{d-3})\ldots) \cdot x + a_0 \ ,$$

y se desarrolla en $d+1$ pasos de la siguiente manera:

- paso inicial: $u_0 := a_d$,
- paso de iteración: $u_i := u_{i-1} \cdot x + a_{d-i}$, con $1 \leq i \leq d$.

Sin embargo, existen polinomios –familias de polinomios– para los que es posible encontrar esquemas de evaluación que empleen un número de sumas y productos sustancialmente menor al requerido por la regla de Horner. El ejemplo más sencillo que se nos ocurre es el del polinomio X^d para cuya evaluación son necesarios a lo sumo $2\lceil \log_2 d \rceil - 1$ productos y ninguna suma/sustracción[2]. Otros ejemplos de polinomios cuya evaluación requiere un número de operaciones considerablemente menor que el empleado por la regla de Horner son los de la familia

$$\Big(\sum_{0 \leq j \leq d} X^j \Big)_{d \in \mathbb{N}} \ ,$$

o los de la familia

$$\Big(\sum_{0 \leq j \leq d} f_j X^j \Big)_{d \in \mathbb{N}} \ ,$$

[2]El procedimiento se basa en la idea siguiente:

$$\begin{aligned} X^d &= (X^2)^{d/2} && \text{si } d \text{ es par,} \\ X^d &= X \cdot X^{d-1} && \text{si } d \text{ es impar.} \end{aligned}$$

Empleando un algoritmo recursivo que proceda según lo anterior es fácil ver que el número de multiplicaciones necesarias para calcular X^d es exactamente la parte entera del logaritmo en base 2 del grado d más el número de dígitos no nulos que aparecen en la representación binaria de d, todo ello menos 1.

donde f_j representa el j-ésimo término de la sucesión de Fibonacci. En ambos casos, si se tienen en cuenta las identidades

$$\sum_{0\le j\le d} X^j = \frac{X^{d+1}-1}{X-1},$$

$$\sum_{0\le j\le d} f_j X^j = X\cdot\frac{f_d X^{d+1}+f_{d+1}X^d-1}{X^2+X-1},$$

la evaluación de tales polinomios se consigue empleando una división, más un número de sumas/sustracciones constante, más un número de productos del orden[3] de $O(\log_2 d)$.

Las evaluaciones anteriores se pueden considerar óptimas, puesto que el llamado *Teorema del Grado* establece que el logaritmo en base 2 del grado de un polinomio es una *cota inferior universal*, válida para todo polinomio, para el número de productos necesarios para evaluar el polinomio. Por esta razón, a las familias de polinomios anteriores las llamaremos *fáciles de computar*, ya que la evaluación del polinomio de grado d de una de esas familias se puede hacer con un número total de operaciones del orden de $(\log_2 d)^{O(1)}$. Por contra, llamaremos *difíciles de computar* a aquellas familias para las que la evaluación del polinomio de grado d requiera, independientemente del esquema de evaluación que se emplee, un número total de operaciones de orden al menos $d^{\Omega(1)}$ –cercano, por lo tanto, a la *cota superior universal* proporcionada por la regla de Horner–.

Encontrar ejemplos de familias de polinomios fáciles de computar no resulta complicado –basta, por ejemplo, que los coeficientes del polinomio pertenezcan a una progresión linealmente recurrente de orden positivo y estén dispuestos en el orden en el que aparecen en la progresión, como ocurre en los ejemplos mostrados–. Mayor interés tiene presentar familias de polinomios difíciles de computar, tanto por lo arduas que resultan las demostraciones correspondientes como por las consecuencias teóricas que conllevaría conseguir tales demostraciones para ciertas familias.

Un ejemplo de este tipo de consecuencias lo da un teorema de R. J. Lipton (véase [Li92]) que afirma que si la familia de polinomios de Pochhammer

$$\Big(\prod_{0\le j<d}(X-j)\Big)_{d\in\mathbb{N}},$$

[3] A lo largo de esta exposición se empleará notación asintótica para dar idea del crecimiento de ciertas funciones enteras. En el caso de querer acotar por arriba este crecimiento se empleará notación O, y se dirá que una función f es a lo sumo de orden $O(g)$, con g otra función, cuando existan una constante $c>0$ y un valor x_0 tales que para todo x mayor que x_0 se verifica $f(x)\le c\cdot g(x)$. En el caso de que lo que interese resaltar sea un crecimiento mínimo se empleará notación Ω, y se dirá que la función f es al menos de orden $\Omega(h)$, con h una función, si existen una constante $c'>0$ y un valor x_0' tales que para todo x mayor que x_0' se verifica $f(x)\ge c'\cdot h(x)$.

es fácil de computar, entonces existe un algoritmo que factoriza completamente cualquier número entero n en tiempo $(\log_2 n)^{O(1)}$. Recuérdese que, por ejemplo, ciertos códigos criptográficos empleados para salvaguardar el secreto en la comunicación de datos –el popular sistema RSA de clave pública es uno de ellos– basan su seguridad en la hipótesis de que la factorización de enteros es un problema computacionalmente difícil, es decir, que en general se necesita tiempo $n^{\Omega(1)}$ para factorizar completamente un entero n.

Otro ejemplo, debido a J. Heintz y J. Morgenstern ([HeMo93]), muestra la importancia que esta misma familia tiene en la resolución de sistemas de ecuaciones polinomiales. Si consideramos el siguiente sistema de ecuaciones en las variables $Y_0, \ldots, Y_{n-1}, X$:

$$Y_0^2 - Y_0 = 0, \ldots, Y_{n-1}^2 - Y_{n-1} = 0, \sum_{0 \le i < n} 2^i Y_i = X \ ,$$

entonces la fórmula

$$\prod_{0 \le j < 2^n} (X - j) = 0$$

expresa una condición necesaria y suficiente para que el sistema tenga solución. Si se demostrara que el polinomio de Pochhammer de grado d requiere del orden de $d^{\Omega(1)}$ operaciones para ser evaluado, entonces al menos un problema –bastante natural– de la resolución de sistemas de ecuaciones polinomiales requeriría un número de operaciones exponencial con respecto al tamaño del sistema. En consecuencia, la teoría de la eliminación podría considerarse computacionalmente intratable.

En este artículo se va a presentar una nueva técnica para obtener cotas inferiores de complejidad en problemas de evaluación de polinomios y funciones racionales. En la sección siguiente se comienza por definir un modelo teórico de computación que nos permita analizar y discutir cuestiones de complejidad computacional en un contexto algebraico. A continuación, se describe la naturaleza combinatoria de la nueva técnica y se muestran dos ejemplos de familias de polinomios para los que esta técnica consigue dar cotas inferiores de complejidad significativas. Para terminar, y como una evidencia más de que todos los campos de la matemática están en relación, se mostrará la forma de emplear el método expuesto como un nuevo criterio de trascendencia para series de potencias formales.

En lo que sigue, K representará un cuerpo algebraicamente cerrado de característica cero y X una indeterminada sobre el cuerpo K. Además, se utilizará la denominación *escalar* para referirse a los elementos del cuerpo K y *no escalar* para referirse a los elementos de $K(X) \setminus K$.

ESQUEMAS DE EVALUACIÓN

El modelo de computación más extensamente empleado en la búsqueda de cotas inferiores de complejidad para problemas de evaluación de polinomios y

funciones racionales es el modelo llamado *esquema de evaluación –straight-line program* es su expresión en idioma inglés–.

En su forma más general, un esquema de evaluación de *longitud* L es una secuencia $\beta := (u_0, \ldots, u_L)$ en la cual el primer elemento es igual a la indeterminada X y cada uno de los restantes elementos es el resultado de aplicar una operación de las del conjunto $\{+, -, \cdot, \div\}$ bien a dos elementos cualquiera de los que le preceden en la secuencia, bien a uno de los elementos precedentes y a un escalar del cuerpo K.

Se dice que un esquema de evaluación de longitud L *computa* la función racional F de $K(X)$ si el último elemento u_L de la secuencia es igual a F.

El siguiente es un ejemplo de esquema de evaluación en el que se computa el polinomio $X^4 - 4X^3 + 5X^2 - 12X + 17$ de acuerdo a la regla de Horner:

$$u_0 := X, \quad u_1 := u_0 - 4, \quad u_2 := u_1 \cdot u_0, \quad u_3 := u_2 + 5,$$
$$u_4 := u_3 \cdot u_0, \quad u_5 := u_4 - 12, \quad u_6 := u_5 \cdot u_0, \quad u_7 := u_6 + 17.$$

Para cada elemento F del cuerpo de funciones racionales $K(X)$ se define la *complejidad total de evaluación* de F, y se representa por $L(F)$, como el mínimo de las longitudes de los esquemas de evaluación que computan F, esto es,

$$L(F) := \min\Big\{\text{longitud de } \beta : \beta \text{ computa } F\Big\} \ .$$

Definamos una operación como *no escalar* si es, o bien un producto de elementos no escalares, o bien un cociente con denominador no escalar –excluimos de la definición las operaciones de adición y sustracción aun cuando sus operandos no sean escalares–.

Entonces, como cota inferior de la complejidad total sirve la *complejidad no escalar*, que del total de operaciones necesarias para evaluar un polinomio o función racional sólo tiene en cuenta las operaciones no escalares. En la definición del modelo de computación correspondiente a este tipo de complejidad, las operaciones aditivas y los productos por escalares se condensan formando combinaciones lineales de resultados no escalares tal como se describe en la siguiente definición.

Definición 1 *Un* esquema de evaluación de longitud no escalar L *es una secuencia* β, $\beta := (Q_{-1}, Q_0, \ldots, Q_L, R_L)$, *de elementos tomados del modo siguiente:*

- $Q_{-1} := 1$.
- $Q_0 := X$.
- *Para cada paso no escalar* ρ, *con* $1 \le \rho \le L$, *el correspondiente resultado intermedio* Q_ρ *tiene la forma*

$$Q_\rho := \Big(\sum_{-1 \le j < \rho} a_{\rho,j} Q_j\Big) \cdot \Big(d_\rho \Big(\sum_{-1 \le j < \rho} b_{\rho,j} Q_j\Big) + (1 - d_\rho)\Big(\sum_{-1 \le j < \rho} b_{\rho,j} Q_j\Big)^{-1}\Big) \ ,$$

donde $d_\rho \in \{0, 1\}$, *y los* $a_{\rho,j}$, $b_{\rho,j}$, *con* $-1 \le j < \rho$, *son escalares del cuerpo* K.

- *El resultado final R_L es de la forma $R_L := \sum_{-1 \le l \le L} c_l Q_l$, donde los c_l son escalares tomados del cuerpo K.*

Diremos que un esquema de evaluación de longitud no escalar L *computa* un elemento F de $K(X)$ si se verifica que el resultado final R_L es igual a F.

La *complejidad no escalar* de una función racional F se define como el mínimo de las longitudes no escalares de esquemas de evaluación que computan F, esto es,

$$L_{ns}(F) := \min\Big\{\text{longitud no escalar de } \beta : \beta \text{ computa } F\Big\} \ .$$

Si los escalares $a_{\rho,j}$, $b_{\rho,j}$, d_ρ y c_l, con $-1 \le j < \rho$, $1 \le \rho \le L$ y $-1 \le l \le L$, se consideran como *parámetros* del esquema de evaluación, se consigue que el esquema de evaluación de la Definición 1 represente una computación *genérica* dependiente sólo de la longitud no escalar L. En particular, cada parámetro d_ρ nos permite elegir la operación aritmética –no escalar– a realizar en el paso ρ correspondiente: el valor asignado al parámetro d_ρ será 1 si queremos que la operación a realizar sea una multiplicación y 0 si queremos que sea una división. El número total de parámetros del esquema de evaluación genérico de longitud no escalar L está acotado superiormente por el valor $(L+1)(L+4)$.

El resultado final R_L –también los resultados intermedios $Q_1, \ldots, Q_L$– del esquema de evaluación genérico es una función racional sobre K de los parámetros del esquema y de la indeterminada X. Para poder obtener una cota inferior de la complejidad no escalar de R_L interesa cuantificar la forma de tal dependencia. Con este fin, se utiliza una idea que se debe a V. Strassen ([St74]) y que se plasma en la siguiente herramienta técnica llamada *Teorema de Representación de funciones racionales.*

Se recuerda que la *altura* de un polinomio P con coeficientes enteros de define como el máximo del valor absoluto de sus coeficientes, y su *peso* se define como la suma de los valores absolutos de esos mismos coeficientes. Obsérvese que el peso de un polinomio es subaditivo y submultiplicativo.

Teorema 2 *Sea L un número natural y defínase $N := (L+1)(L+4)$. Existe una familia de polinomios $(P_{L,j})_{j \in \mathbb{N}}$, $P_{L,j} \in \mathbb{Z}[Z_1, \ldots, Z_N]$, con cotas de grado*

$$\text{grado } P_{L,j} \le j(2L-1)+2$$

y peso

$$\text{peso } P_{L,j} \le 2^{3((j+1)^L-1)} \ ,$$

tales que, para cada α del cuerpo K y para cada función racional F de $K(X)$ definida en α que se pueda computar mediante un esquema de evaluación de longitud no escalar L, existe un punto z_α del espacio afín K^N tal que el desarrollo de Taylor de F alrededor del punto α, $i_\alpha(F)$ en notación, verifica

$$i_\alpha(F) = \sum_{j \in \mathbb{N}} P_{L,j}(z_\alpha) \cdot (X-\alpha)^j .$$

El espacio afín K^N que aparece en el Teorema de Representación es el espacio afín de los parámetros del esquema de evaluación genérico de longitud no escalar L, y el punto z_a perteneciente a tal espacio afín es un conjunto de escalares del cuerpo K tales que, al sustituirlos en los parámetros del esquema de evaluación genérico, la computación resultante produce como resultado final la función racional F.

J. Heintz y M. Sieveking ([HeSi80]) hacen la siguiente interpretación geométrica del Teorema de Representación. Los polinomios del Teorema de Representación permiten definir una familia de morfismos: para d y L números naturales, sea

$$\Phi_{d,L} : K^N \longrightarrow K^{d+1}$$

el morfismo de espacios afines definido para cada punto z del espacio afín de parámetros K^N de la forma siguiente:

$$\Phi_{d,L}(z) := (P_{L,0}(z), \ldots, P_{L,d}(z)) \ .$$

Denotemos por $W_{d,L}$ la variedad de K^{d+1} obtenida como clausura Zariski sobre $\mathbb{Q}$ de la imagen del morfismo $\Phi_{d,L}$, esto es,

$$W_{d,L} := \overline{im\, \Phi_{d,L}} \ .$$

Si ahora identificamos cada polinomio $\sum_{0 \le j \le d} f_j X^j$ de grado d del anillo $K[X]$ con su vector de coeficientes $(f_0, \ldots, f_d)$ y consideramos a éste como un punto del espacio afín K^{d+1}, resulta que, de acuerdo al Teorema de Representación, a la variedad $W_{d,L}$ pertenecen los puntos formados por los coeficientes de los segmentos iniciales de grado d de los desarrollos de Taylor de aquellas funciones racionales de $K(X)$ que se pueden evaluar con un número de operaciones no escalares menor o igual a L.

MÉTODO COMBINATORIO

Sea A un anillo arbitrario. Para cada subconjunto finito Γ del anillo A representemos por $\prod(\Gamma)$ el conjunto de todos los valores que se obtienen como producto de elementos distintos de Γ:

$$\prod(\Gamma) := \left\{ \prod_{f \in S} f : S \subseteq \Gamma \right\} \ .$$

Mediante sumas, se define del mismo modo el conjunto $\sum(\Gamma)$ para todo subconjunto finito Γ de elementos del anillo A:

$$\sum(\Gamma) := \left\{ \sum_{f \in S} f : S \subseteq \Gamma \right\} \ .$$

Definamos $\mu(\Gamma)$, para cada subconjunto finito Γ del anillo A, como el cardinal del conjunto formado por todas las sumas de todos los productos de elementos de Γ. En términos de la notación introducida,

$$\mu(\Gamma) := \#\sum\left(\prod(\Gamma)\right).$$

Ahora tomemos como A el anillo de polinomios en las N indeterminadas $Z_1, \ldots, Z_N$ con coeficientes enteros, esto es, hagamos $A := \mathbb{Z}[Z_1, \ldots, Z_N]$, con N un número natural mayor que cero. Asimismo, tomemos como Γ un subconjunto de $d+1$ elementos de $\mathbb{Z}[Z_1, \ldots, Z_N]$, con d un número natural mayor que cero. Si se conocen cotas para el grado y el peso de los polinomios que forman Γ no resulta difícil obtener una cota superior del valor $\mu(\Gamma)$. Sean D y W tales cotas de grado y peso:

$$\max\left\{\text{grado } P : P \in \Gamma\right\} \leq D,$$
$$\max\left\{\text{peso } P : P \in \Gamma\right\} \leq W.$$

Entonces las siguientes desigualdades nos dan cotas válidas para el grado y la altura de los polinomios del conjunto $\sum(\prod(\Gamma))$:

$$\max\left\{\text{grado } P : P \in \sum(\prod(\Gamma))\right\} \leq (d+1)D,$$
$$\max\left\{\text{altura } P : P \in \sum(\prod(\Gamma))\right\} \leq (2W)^{d+1}.$$

El número de monomios de un polinomio de grado menor o igual que $(d+1)D$ en N variables está acotado superiormente por

$$\binom{(d+1)D+N}{N} \leq ((d+1)D+1)^N.$$

Si cada uno de estos monomios va acompañado por un coeficiente entero cuyo valor absoluto está acotado por $(2W)^{d+1}$, resulta que el número total de polinomios del conjunto $\sum(\prod(\Gamma))$ es menor o igual que $(2(2W)^{d+1}+1)^{((d+1)D+1)^N}$, esto es,

$$\mu(\Gamma) \leq (2(2W)^{d+1}+1)^{((d+1)D+1)^N}.$$

Para cada punto z del espacio afín K^N, representemos mediante Γ_z el subconjunto de K formado por los valores de la evaluación en z de los polinomios de Γ,

$$\Gamma_z := \left\{P(z) : P \in \Gamma\right\}.$$

Entonces, dado que el cardinal del conjunto Γ es cota superior para el cardinal del conjunto Γ_z, se concluye

$$\mu(\Gamma_z) \leq \mu(\Gamma) \leq (2(2W)^{d+1}+1)^{((d+1)D+1)^N}.$$

Apliquemos ahora, para d y L números naturales dados, la acotación anterior al conjunto formado por los $d+1$ primeros polinomios del Teorema de Representación. Bastará con hacer $N := (L+1)(L+4)$, $D := 2(Ld+1)$ y $W := 2^{4(d+1)^L}$ para obtener de manera casi inmediata el resultado siguiente[4].

Lema 3 *Existe una constante universal $c > 0$ tal que para cada par de números naturales d y L, y para cada polinomio F de grado d de $K[X]$ perteneciente a la variedad algebraica $W_{d,L}$, es válida la siguiente desigualdad*

$$\mu(F) \leq 2^{(d+1)^{cL^2}} .$$

El Lema 3 permite obtener fácilmente una condición suficiente para decir si un polinomio con coeficientes enteros es difícil de computar. Para ello, basta con ver que para todo conjunto finito Γ de números enteros y para todo número primo p se verifica que el cardinal de Γ es siempre mayor o igual que el cardinal del conjunto $\{\nu_p(f) : f \in \Gamma\}$, donde $\nu_p(f)$ denota la multiplicidad del primo p en la descomposición en factores primos del número entero f. De lo anterior no es difícil concluir que $\#\sum(\Gamma) \geq 2^b$, con con $b = \#\{\nu_p(f) : f \in \Gamma\}$, lo que nos lleva al siguiente resultado.

Teorema 4 *Existe una constante universal $c > 0$ con la propiedad siguiente. Sean d y L números enteros. Sea $F := \sum_{0 \leq j \leq d} f_j X^j$ un polinomio de grado d con coeficientes enteros tal que el vector de coeficientes de F pertenece a la variedad algebraica $W_{d,L}$. Entonces para todo número primo p se tiene*

$$L^2 \geq c \cdot \frac{\log_2\Big(\#\Big\{\nu_p(f) : f \in \prod(F)\Big\}\Big)}{\log_2 d} .$$

Ejemplos de Familias de Polinomios Difíciles de Computar

Los siguientes son dos ejemplos de familias de polinomios con coeficientes enteros para las que el Teorema 4 permite afirmar que son difíciles de computar. En estos ejemplos, L representa la complejidad no escalar de evaluación del polinomio correspondiente: los polinomios de las familias

$$\sum_{0 \leq j \leq d} 2^{2^{\lfloor \sqrt[n]{j} \rfloor}} X^j \quad \text{y} \quad \sum_{0 \leq j \leq d} 2^{\lfloor \sqrt[n]{j} \rfloor !} X^j ,$$

verifican la cota de complejidad no escalar $L^2 = \Omega\Big(\frac{\sqrt[n]{d}}{\log_2 d}\Big)$, para todo número natural $n \geq 1$.

---

[4] En lo sucesivo, el operador μ se aplicará sobre elementos del espacio afín K^{d+1}. En este caso, el sentido que habrá de darse a la expresión $\mu(F)$, siendo F un punto del espacio afín K^{d+1}, será el de cardinal del conjunto formado por todas las sumas de todos los productos de *coordenadas* del punto F.

El lector interesado en obtener la cota inferior dada para el polinomio $\sum_{0\le j\le d} 2^{2^{\lfloor \sqrt[3]{j} \rfloor}} X^j$ sólo habrá de observar

$$\begin{aligned} \#\Big\{\nu_2\Big(\prod_{j\in S} 2^{2^{\lfloor \sqrt[3]{j} \rfloor}}\Big) : S \subseteq \{0,\ldots,d\}\Big\} &= \#\Big\{\sum_{j\in S} 2^{\lfloor \sqrt[3]{j} \rfloor} : S \subseteq \{0,\ldots,d\}\Big\} \\ &\ge \#\Big\{\sum_{j\in S} 2^{j} : S \subseteq \{0,\ldots,\lfloor \sqrt[3]{d} \rfloor\}\Big\} \\ &= 2^{\lfloor \sqrt[3]{d} \rfloor + 1}\ , \end{aligned}$$

y a continuación aplicar el Teorema 4 con $p = 2$ para obtener

$$L^2 \ge c \cdot \frac{\log_2\Big(\#\Big\{\nu_2\Big(\prod_{j\in S} 2^{2^{\lfloor \sqrt[3]{j} \rfloor}}\Big) : S \subseteq \{0,\ldots,d\}\Big\}\Big)}{\log_2 d} \ge c \cdot \frac{\lfloor \sqrt[3]{d} \rfloor + 1}{\log_2 d}\ .$$

La cota de complejidad para el otro polinomio se obtiene de forma similar.

El ejemplo anterior evidencia la limitación de la que adolece el método expuesto. Para que la desigualdad $\mu(F) \le 2^{(d+1)^{cL^2}}$ del Lema 3 produzca una cota inferior significativa para la complejidad no escalar L del polinomio F de grado d es necesario que $\mu(F)$ sea un valor de orden mayor que una exponencial en $d^{O(1)}$. Esto sólo es posible si los coeficientes del polinomio F tienen un crecimiento doblemente exponencial, como los dados en el ejemplo, o cercano a ese orden. Polinomios cuyos coeficientes tienen un crecimiento menor, como es el caso del polinomio de Pochhammer, quedan a la espera de nuevas ideas.

NUEVAS SERIES TRASCENDENTES

El método de complejidad algebraica descrito puede ser aplicado a cuestiones clásicas de trascendencia en geometría y teoría de números, actuando los resultados de convergencia del algoritmo de Newton-Hensel como conexión entre la teoría de la trascendencia y la complejidad algebraica.

En esta sección, cuando σ designe una serie de potencias formales de $K[[X]]$ se denotará por σ^α, para cada elemento α del cuerpo K, el desarrollo formal de Taylor de σ en el punto α, esto es,

$$\sigma^\alpha := \sum_{j\in\mathbb{N}} \frac{\sigma^{(j)}(\alpha)}{j!}(X-\alpha)^j.$$

También se empleará la notación σ^α_k, con k un número natural cualquiera, para designar el polinomio formado por los 2^k primeros términos del desarrollo σ^α,

esto es,

$$\sigma_k^\alpha := \sum_{0 \le j < 2^k} \frac{\sigma^{(j)}(\alpha)}{j!}(X-\alpha)^j \ .$$

El segmento inicial de grado $2^k - 1$ de la propia serie σ se denotará como σ_k.

Teorema 5 *Sea σ una serie de potencias formales del anillo $K[[X]]$. Si existe un valor $\epsilon > 0$ tal que para todo número natural k la complejidad no escalar del polinomio σ_k es mayor que $k^{1+\epsilon}$, esto es, si se verifica*

$$\sigma_k \notin W_{2^k-1,k^{1+\epsilon}} \ ,$$

entonces la serie σ es trascendente sobre $K(X)$.

La demostración del teorema se basa en los conocidos resultados de convergencia del algoritmo de Newton-Hensel. Sea $\sigma \in K[[X]]$ una serie algebraica raíz del polinomio irreducible $P \in K[X][Y]$, y sea α un escalar del cuerpo K tal que $\sigma(\alpha)$ es una raíz simple del polinomio $P(\alpha, Y) \in K[Y]$. Entonces al comenzar la iteración de Newton-Hensel en el punto $\sigma(\alpha)$ y tras realizar k iteraciones, la función racional obtenida es una aproximación de orden 2^k a la serie σ en el anillo $K[[X-\alpha]]$, esto es, los 2^k primeros términos de σ^α y del desarrollo de Taylor en α de la función racional obtenida coinciden[5]. Dado que el número de operaciones no escalares a realizar en cada iteración es constante, el algoritmo de Newton-Hensel permite obtener una aproximación de orden 2^k al desarrollo σ^α empleando un número de operaciones no escalares proporcional a k.

De acuerdo con lo anterior, si la serie σ es algebraica existe una constante c tal que, para infinitos valores α del cuerpo K, la condición Zariski cerrada

$$\sigma_k^\alpha \in W_{2^k-1,ck}$$

es válida para todo natural k. Esto es incompatible, por razones de continuidad en la topología del espacio afín K^{2^k} que contiene al cerrado Zariski $W_{2^k-1,ck}$, con la condición expresada en el enunciado del Teorema 5, lo que permite concluir que toda serie que verifique tal condición será trascendente.

Combinando los resultados del Lema 3 y del Teorema 5 se obtiene como corolario el siguiente criterio de trascendencia.

---

[5] El algoritmo de Newton-Hensel procede de la siguiente manera:

- paso inicial: $\xi_0 := \sigma(\alpha)$,
- paso de iteración: $\xi_{k+1} := \xi_k - \frac{P(X,\xi_k)}{\frac{\partial P}{\partial Y}(X,\xi_k)}$.

El número de operaciones no escalares que se realizan en cada paso de iteración es igual al número de operaciones necesarias para evaluar en Y la función racional $Y - \frac{P}{\frac{\partial P}{\partial Y}}$, y esto sólo depende del polinomio P y no de la iteración a realizar. En el contexto algebraico en el que se presenta, el algoritmo de Newton-Hensel siempre converge.

Corolario 6 *Sea σ una serie de potencias formales del anillo $K[[X]]$. Si existe un valor $\epsilon > 0$ tal que para todo número natural k se verifica*

$$\mu(\sigma_k) > 2^{2^{k^{3+\epsilon}}}$$

entonces la serie σ es trascendente sobre $K(X)$.

Los siguientes son ejemplos de series de potencias formales cuya trascendencia sobre $\mathbb{C}(X)$ se puede probar mediante el criterio del Corolario 6.

1. $\sum_{j\in\mathbb{N}} \frac{1}{2^{2^{\lfloor \sqrt[n]{j} \rfloor}}} X^j$ y $\sum_{j\in\mathbb{N}} \frac{1}{2^{\lfloor \sqrt[n]{j!} \rfloor}} X^j$, para todo número natural $n \geq 1$.

2. $\sum_{j\in\mathbb{N}} \frac{1}{2^{2^{\varphi(j)}}} X^j$ y $\sum_{j\in\mathbb{N}} \frac{1}{2^{\varphi(j!)}} X^j$, con φ la función de Euler.

3. $\sum_{j\in\mathbb{N}} \frac{1}{2^{2^{\pi(j)}}} X^j$ y $\sum_{j\in\mathbb{N}} \frac{1}{2^{\pi(j!)}} X^j$, con $\pi(j)$ el número de primos menores o iguales que j.

4. $\sum_{j\in\mathbb{N}} \frac{1}{2^{f_j}} X^j$ y $\sum_{j\in\mathbb{N}} \frac{1}{f_{2^j}} X^j$, con f_j el j-ésimo número de Fibonacci.

5. $\sum_{j\in\mathbb{N}} \frac{1}{2^{\lfloor (\log_2(j+1))^n \rfloor}} X^j$, para todo número natural $n \geq 4$.

NOTAS BIBLIOGRÁFICAS

La teoría de la complejidad algebraica, en lo concerniente a la obtención de cotas inferiores para problemas del álgebra numérica, es una de las ramas más antiguas de la Informática Teórica.

Los estudios actuales tienen su origen en un trabajo ([Os54]) que A. M. Ostrowski publica en el año 1954 tras haberse interesado por la optimalidad de la regla de Horner para la evaluación de polinomios. Ostrowski conjeturó que todo esquema de evaluación general –que sirva para cualquier polinomio, sin aprovecharse de la particular forma de éste– necesita realizar d productos/divisiones –escalares y no escalares– para evaluar un polinomio univariado de grado d, independientemente del número de adiciones o sustracciones usadas. Su conjetura fue probada doce años después por V. Ya. Pan ([Pan66]), demostrando con ello que la regla de Horner es el único algoritmo óptimo para el problema de evaluación de polinomios.

Los estudios en complejidad algebraica continuaron durante toda la década de los sesenta y a comienzos de la siguiente se disponía ya de un coherente cuerpo de resultados teóricos –el Teorema del Grado es uno de ellos–. Sin

embargo, no fue hasta el año 1974 cuando V. Strassen ([St74]) presentó los primeras familias de polinomios difíciles de computar en un trabajo en el que también nos legó la principal herramienta usada hasta el momento en la búsqueda de cotas inferiores de complejidad para problemas de evaluación de polinomios, el Teorema de Representación. Siguiendo la línea del anterior, C. P. Schnorr ([Sc78]) simplificó las técnicas usadas por Strassen y mejoró sus resultados. J. Heintz y M. Sieveking ([HeSi80]) fueron pioneros en realizar una interpretación geométrica del Teorema de Representación para después introducir un método nuevo, y más adaptable, que hace uso del concepto de grado de una variedad y de la desigualdad de Bézout. En [HeMo93], J. Heintz y J. Morgenstern adaptan el método anterior al caso de polinomios dados por sus raices. El método combinatorio explicado en estas páginas puede encontrarse en [AlHeMaMoPa98].

La relación entre la complejidad no escalar de evaluación del polinomio de Pochhammer y la factorización de enteros aparece en [Li92]. En [HeMo93] se puede encontrar también la comentada relación entre el polinomio de Pochhammer y la complejidad de la resolución de sistemas de ecuaciones polinomiales. Para comprender el efecto que en la teoría de la eliminación tienen tanto la complejidad de evaluación de polinomios como la complejidad de codificación de números enteros, puede consultarse el *survey* [Par95] de L. M. Pardo sobre este particular.

Por último, el artículo [KuTr78] de H. T. Kung y J. F. Traub es un completo estudio de la convergencia de diferentes métodos numéricos de aproximación empleados en un contexto puramente algebraico. Sus resultados, y las sugerencias de L. M. Pardo, inspiraron los que aparecen aquí en la parte dedicada a trascendencia de series formales.

Bibliografía

[AlHeMaMoPa98] ALDAZ, M., HEINTZ, J., MATERA, G., MONTAÑA, J. L., PARDO, L. M.: *Combinatorial hardness proofs for polynomial evaluation.* En Proceedings 23rd International Symposium MFCS'98, Brno, volumen 1450 de la colección Lecture Notes in Computer Science, Springer, 1998, 167–175.

[HeMo93] HEINTZ, J., MORGENSTERN, J.: *On the intrinsic complexity of elimination theory.* Journal of Complexity **9**, 1993, 471–498.

[HeSi80] HEINTZ, H., SIEVEKING, M.: *Lower bounds for polynomials with algebraic coefficients.* Theoretical Computer Science **11**, 1980, 321–330.

[KuTr78] KUNG, H. T., TRAUB, J. F.: *All algebraic functions can be computed fast.* Journal of the ACM **25**(2), 1978, 245–260.

[Li92] LIPTON, R. J.: *Straight-line complexity and integer factorization.* En Proceedings First International Symposium ANTS-I, Ithaca, volumen 877 de la colección Lecture Notes in Computer Science, Springer, 1994, 71–79.

[Os54] OSTROWSKI, A. M.: *On two problems in abstract algebra connected with Horner's rule.* En Studies in Mathematics and Mechanics presented to Richard Von Mises, Academic Press, New York, 1954, 40–48.

[Pan66] PAN, V. YA.: *Methods of computing values of polynomials.* Russian Mathematical Surveys **21**(1), 1966, 105–136.

[Par95] PARDO, L. M.: *How lower and upper complexity bounds meet in elimination theory.* En Proceedings 11th International Symposium AAECC-11, Paris, volumen 948 de la colección Lecture Notes in Computer Science, Springer, 1995, 33–69.

[Sc78] SCHNORR, C. P.: *Improved lower bounds on the number of multiplications/divisions which are necessary to evaluate polynomials.* Theoretical Computer Science **7**(3), 1978, 251–261.

[St74] STRASSEN, V.: *Polynomials with rational coefficients which are hard to compute.* SIAM Journal of Computing **3**, 1974, 128–149.

Agradecimientos

El autor agradece al profesor Tomás Recio su invitación a colaborar en este número de La Gaceta.

Mikel Aldaz Zaragüeta, Departamento de Matemática e Informática,
Universidad Pública de Navarra, Campus de Arrosadía s/n. 31006 Pamplona
e-mail: mikaldaz@upna.es