Notación Asintótica

por Marcos Kiwi

Muchas veces, al analizar algoritmos es conveniente expresar los costos computacionales asociados con una precisión de hasta un factor constante. En general no se requiere determinar el costo exacto del algoritmo sino que cómo crecen estos costos en términos del tamaño de la entrada. En otras palabras, basta conocer la *razón de crecimiento*. Por ejemplo, la forma usual de multiplicar dos matrices de $n \times n$, decimos es un algoritmo que requiere *orden* n^3 multiplicaciones. Esto significa que si $f(n)$ es el número de multiplicaciones requeridas, entonces existe una constante c tal que $f(n) \leq cn^3$ para todo n suficientemente grande. La noción de razón de crecimiento puede formalizarse a través de la notación asintótica. Esta maravillosa convención notacional para análisis asintótico fue introducida por Paul Bachmann en 1894 y popularizada más tarde por Edmund Landau y otros.

Definición 1 *Una función parcial $f : \mathbb{N} \to \mathbb{R}$ es una que no necesariamente esta definida para todo $n \in \mathbb{N}$.*

Definición 2 (O-grande) *Sea g una función parcial. Denotamos por $O(g)$ al conjunto de funciones f parciales para las que existe $c > 0$ y $n_0 \in \mathbb{N}$ tales que $f(n)$ y $g(n)$ están definidas y $|f(n)| \leq c|g(n)|$ para todo $n \geq n_0$.*

La belleza de la O-notación radica en que obvía los detalles irrelevantes y permite concentrarse en los puntos importantes: Por ejemplo, $O(f)$ donde $f(n) = 1/n$ para $n \geq 1$, es despreciablemente pequeña, si múltiplos constantes de $1/n$ no tienen importancia. Otro ejemplo; $H_n = \ln(n)+\gamma+O(1/n)$ significa que $|H_n - \ln(n) - \gamma| \leq C/n$ — la constante C no está especificada, pero aun si desconocemos su valor sabemos que la cantidad $H_n - \ln(n) - \gamma$ será arbitrariamente pequeña si n es grande.

Si $f(n)$ denota el costo de multiplicar matrices de $n \times n$ más arriba mencionado entonces escribimos $f = O(n^3)$ para denotar que $f \in O(g))$ donde $g(n) = n^3$. La igualdad pasa a tener propiedades curiosas; si $g(n) = n^3$ y $h(n) = n^4$, entonces $g = O(h)$ y $h = O(h)$, pero no queremos concluir que $g = h$.

También es usual abusar la notación y escribir $O(f(n))$ para denotar $O(f)$ a pesar de que $f(n)$ es sólo un número y la O-notación tiene sentido para una función. A lo que uno se refiere es a f como función de la variable n. Otro abuso es que suele escribirse $n^3 = O(n^4)$ a pesar de que n^3 es sólo un número. Lo que se quiere decir es que $g = O(n^4)$ donde $g(n) = n^3$.

Otro uso de la notación asintótica es cuando uno escribe $h = O(1)$ para una función parcial h, queriendo decir que h está uniformemente acotada por una constante cuando está definida. Si se quiere explicitar la variable n de la que h se considera función se escribe $h = O(n^0)$.

Cuando $O(g)$ aparece en la mitad de una fórmula representa una función específica $f \in O(g)$. Los valores precisos de f son desconocidos, pero sabemos no son demasiado grandes (al menos en comparación con g). Es así que podemos escribir

$$\frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = \frac{1}{3}n^3 + \frac{1}{2}n^2 + O(n)\,,$$

o

$$\frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = \frac{1}{3}n^3 + O(n^2)\,.$$

Observar que también es cierto que

$$\frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = O(n^{10})\,,$$

Nada en la O-notación asintótica obliga a escribir la mejor cota posible.

También tiene sentido escribir una cadena de igualdades que involucren la O-notación, como por ejemplo,

$$\frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = \frac{1}{3}n^3 + O(n^2) = O(n^3)\,.$$

Aquí la primera igualdad indica pertenencia y la segunda inclusión de conjuntos. La primera expresión corresponde a una función y las dos restantes a conjuntos de funciones (al conjunto de funciones de la forma $n^3/3 + f(n)$ y $g(n)$ con $f(n) \in O(n^2)$ y $g(n) \in O(n^3)$ respectivamente). Siempre usamos la convención que el lado izquierdo de una ecuación no da más información que el lado derecho. Es así que cuando uno trabaja con notación asintótica, dependiendo del contexto, una función particular f a veces representa el conjunto $\{f\}$.

Si S y T son dos conjuntos de funciones, se denota por $S + T$ al conjunto de todas las funciones $f + g$ donde $f \in S$ y $g \in T$. Otras expresiones como $S - T$, ST, S/T, $\sqrt{S}$, e^S, $\ln(S)$ se definen de manera similar. Además, la O-notación puede manipularse algebráicamente. Por ejemplo, las siguientes identidades se cumplen:

- $c \cdot O(f) = O(f)$ para todo $c \in \mathbb{R}$, $c > 0$,
- $O(f) + O(g) = O(f + g) = O(\max\{f, g\})$,
- $O(f)O(g) = O(fg) = fO(g)$,
- $O(f)^m = O((f)^m)$, para todo $m \in \mathbb{N}$, $m > 0$,
- $O(O(f)) = O(f)$.

¿Por que usar '=' en vez de '$\subseteq$'? Primero, por tradición, la O-notación comenzó a usarse en teoría de números, y la práctica prendió. Ya está demasiado establecida como para hacer que la comunidad matemática cambie. En segundo lugar, por tradición. Científicos de la computación están demasiado acostumbrados a abusar del signo '=' a través de asignaciones como '$n = n + 1$'. Otro nuevo abuso no es como para alterarse. Tercero, por tradición. Muchas veces leemos '=' como *es*. Por ejemplo leemos $H_n = O(\log n)$ como *H sub n es O grande de* $\log n$, y en castellano el *es* tiene dirección (decimos que un pájaro es un animal, pero no que un animal es un pájaro).

Un punto de suma importancia es que las identidades que involucran notación asintótica no son reversibles. Tiene sentido decir que $n^2 = O(n^3)$ (pues $n^2 \in O(n^3)$) pero no tiene sentido decir que $O(n^3) = n^2$.

Otro punto a tener presente es que cada aparición de la O-notación involucra una constante distinta, así, no es cierto que

$$\underbrace{O(n) + O(n) + \ldots + O(n)}_{n \text{ veces}} = O(n^2)\,,$$

puesto que a pesar que $n = O(n), 2n = O(n), 3n = O(n), \ldots$, se tiene que

$$n + 2n + 3n + \ldots + n^2 = O(n^3)\,.$$

Observar que al usar logaritmos en la O-notación sin explicitar la base de los mismos, como por ejemplo al decir $O(\log^k n)$, es irrelevante cual es la base. Se asume que es 2 o e según convenga. Por otro lado, hay que tener cierta cautela al usar la O-notación en exponentes. Podría parecer que $e^{O(f)} = O(e^f)$, pero $e^{2n} \in e^{O(n)}$ y sin embargo $e^{2n} = (e^n)^2 \notin O(e^n)$. La constante que se esconde dentro de la O-notación influencia la razón de crecimiento cuando ocurre en un exponente.

Otra sutileza de la O-notación es que si hay más de una variable presente, la O-notación representa conjuntos de funciones en todas las variables presentes. El dominio de cada función es sobre el conjunto en que cada variable es "libre" de moverse. Por ello, se debe prestar atención a las partes de una ecuación sobre las cuales está definida una variable cuando hay sumatorias de operadores similares involucrados. Por ejemplo, consideremos la ecuación

$$\sum_{k=0}^{n}(k^2 + O(k)) \quad = \quad \frac{1}{3}n^3 + O(n^2)\,. \tag{1}$$

La expresión $k^2+O(k)$ representa el conjunto de funciones sobre dos variables de la forma $k^2+f(k,n)$ tal que existe una constante C y un $n_0 \in \mathbb{N}$ tal que $|f(k,n)| \leq Ck$ para $0 \leq k \leq n$ y $n \geq n_0$. Como

$$\sum_{k=0}^{n}(k^2 + f(k,n)) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n + f(0,n) + f(1,n) + \ldots + f(n,n)\,,$$

y $f(0,n) + f(1,n) + \ldots + f(n,n) \leq C \cdot 0 + C \cdot 1 + \ldots + C \cdot n = Cn(n+1)/2 < (C+1)n^2$, entonces se satisface (1).

La O-notación también se usa frecuentemente con funciones de una variable x perteneciente a un intervalo $[a,b]$ particular. En este caso $O(f(x))$ representa cualquier $g : \mathbb{R} \to \mathbb{R}$ tal que $|g(x)| \leq C|f(x)|$ cuando $a \leq x \leq b$. (Como siempre, C es una constante no especificada.) Por ejemplo, sea $g(x) = \sum_{k\geq 0} a_k x^k$ con $|x| \leq r$ tal que $g(x) = \sum_{k\geq 0} |a_k x^k|$ existe cuando $|x| \leq r$. Entonces, podemos escribir

$$g(x) = a_0 + a_1 x + \ldots + a_m x^m + O(x^{m+1})\,, \quad |x| \leq r\,.$$

Análogamente, también tienen sentido las siguientes expresiones:

$$\begin{aligned} e^x &= 1 + x + \frac{1}{2!}x^2 + \ldots + \frac{1}{m!}x^m + O(x^{m+1})\,, \quad |x| \leq r, \quad r \text{ fijo;} \\ \ln(1+x) &= x - \frac{1}{2}x^2 + \ldots + \frac{(-1)^{m+1}}{m}x^m + O(x^{m+1}), \quad |x| \leq r, \quad r < 1 \text{ fijo.} \end{aligned}$$

El requerimiento de que r este "fijo" implica que r debe tomar un valor específico cuando la O-notación se use — claramente tenemos que $e^x = O(1)$ cuando $|x| \leq r$, dado que $e^x \leq e^r$ si $|x| \leq r$, pero la constante C implícita en la O-notación depende de r.

En algunos casos la O-notación todavía acarrea demasiada información. Por ejemplo, el algoritmo rápido de multiplicación de dos enteros de n bits requiere $O(n \log n \log\log n)$ operaciones binarias, por lo que, salvo factores logarítmicos, es esencialmente un algoritmo lineal como el algoritmo de suma de dos enteros de n bits. Cuando los factores logarítmicos son irrelevantes, preferimos escribir $\widetilde{O}(n)$. En general, si $poly(m) = m^{O(1)}$ en vez de $O(f(n)poly(\log(n)))$ escribimos $\widetilde{O}(f(n))$.

Otras extensiones usuales de la notación asintótica, están dadas por:

- **Ω-grande:** Denotamos por $\Omega(g)$ al conjunto de funciones parciales para las que existe $c > 0$ y $n_0 \in \mathbb{N}$ tales que $f(n)$ y $g(n)$ están definidas y $|f(n)| \geq c|g(n)|$ para todo $n \geq n_0$.
- **o-chica:** Denotamos por $o(g)$ al conjunto de funciones f en $O(g)$ tales que $f(n)/g(n) \to 0$ cuando $n \to \infty$.
- **ω-chica:** Denotamos por $\omega(g)$ al conjunto de funciones f en $\Omega(g)$ tales que $f(n)/g(n) \to \infty$ cuando $n \to \infty$.
- **Θ:** Denotamos por $\Theta(g)$ al conjunto de funciones f tales que existen $c, c' > 0$ y $n_0 \in \mathbb{N}$ tales que $c'|g(n)| \leq |f(n)| \leq c|g(n)|$ para todo $n \geq n_0$.

Observar que de las relaciones sobre el conjunto de funciones parciales definidas por $f = \Theta(g)$, $f = O(g)$, $f = \Omega(g)$, $f = o(g)$ y $f = \omega(g)$, todas son transitivas, las tres primeras son reflejas y sólo la primera es simétrica. Notar finalmente que:

- $\Theta(f) = O(f) \cap \Omega(f)$,
- $f = O(g)$ si y sólo si $g = \Omega(f)$,
- $f = o(g)$ si y sólo si $g = \omega(f)$.