

Matematyka dyskretna

© Andrzej Łachwa, UJ, 2017

andrzej.lachwa@uj.edu.pl

3b/15

Notacja O

Notacja O służy do opisu szybkości wzrostu ciągu wartości rzeczywistych. W informatyce jest używana do szacowania czasu wykonania algorytmu dla zmieniającej się liczby danych wejściowych.

Niech f i g to ciągi o wartościach rzeczywistych (w zasadzie interesują nas funkcje o wartościach nieujemnych, jednak wartość bezwzględna zapewnia nam ogólniejszą definicję). A zatem:

Funkcja **asymptotycznie niewiększa** od funkcji $g(n)$ to taka funkcja (ciąg)

$$f: \mathbb{N} \rightarrow \mathbb{R},$$

dla której istnieją $c > 0$ i $n_0 \in \mathbb{N}$, że $|f(n)| \leq c \cdot |g(n)|$ dla wszystkich $n \geq n_0$.

Będziemy też często mówić, że nierówność ta **zachodzi dla prawie wszystkich liczb naturalnych \mathbb{N}** (albo po prostu dla dużych wartości n).

Wśród algorytmów prowadzących do tego samego wyniku jedne są szybsze, inne wolniejsze. Jeżeli czasy liczenia kilku algorytmów z wartością wejściową $n \in \mathbb{N}$ (wykonujących to samo zadanie) zależą wprost proporcjonalnie od liczby n , to dla małych n nie ma zbytniej różnicy, który algorytm wybierzemy. Dla większych n różnica czasu obliczeń może być bardzo duża:

$\log_2 n$	\sqrt{n}	n	n^2	2^n	$n!$	n^n
3,32	3,16	10	100	1,024	$3,63 \cdot 10^6$	10^{10}
6,64	10	100	10 000	$1,27 \cdot 10^{30}$	$9,33 \cdot 10^{157}$	10^{200}
9,97	31,62	1 000	10^6	$1,07 \cdot 10^{301}$	$4,02 \cdot 10^{2567}$	10^{3000}
13,29	100	10 000	10^8	$2,00 \cdot 10^{3010}$	$2,85 \cdot 10^{35659}$	10^{40000}
16,61	316,2	100 000	10^{10}	$1,00 \cdot 10^{30103}$	$2,82 \cdot 10^{456573}$	10^{500000}
19,93	1000	10^6	10^{12}	$9,90 \cdot 10^{301029}$	$8,26 \cdot 10^{5565708}$	$10^{6000000}$
39,86	10^6	10^{12}	10^{24}	duża liczba	większa	jeszcze większa

Źródło: str. 61 podręcznika K.R. Ross, C. R. B. Wright

Zbiór funkcji **asymptotycznie niewiększych** niż $g(n)$ oznaczamy przez $O(g(n))$. Mimo, że poprawnie powinniśmy zapisywać $f \in O(g(n))$, gdy f spełnia warunek podany w definicji, to jednak przyjęło się zapisywać $f(n) = O(g(n))$, co czytamy „ $f(n)$ jest O -duże od $g(n)$ ”, a nie „jest równe”.

- każda funkcja stała jest $O(1)$
- $(-1)^n$ jest $O(1)$
- $1/n$ jest $O(1)$
- $(\log n)/n$ jest $O(1)$
- $15n - 7$ jest $O(n)$
- $3n + 15\log n - 9$ jest $O(n)$
- $-22n^2 - 23n + 4$ jest $O(n^2)$
- $(n(n+1))/2$ jest $O(n^2)$
- $5 \log n - 5$ jest $O(n^2)$, a także jest $O(n)$ i jest $O(\log n)$

W literaturze spotyka się cztery terminy uzupełniające do „ O -duże”.

Wprowadza się mianowicie definicje:

- funkcji asymptotycznie **niemniejszej** od funkcji $g(n)$; zbiór takich funkcji oznacza się przez $\Omega(g(n))$,
- funkcji asymptotycznie **podobnej** do funkcji $g(n)$; zbiór takich funkcji oznacza się przez $\Theta(g(n))$, a także
- funkcji asymptotycznie **mniejszej** od funkcji $g(n)$; zbiór takich funkcji oznacza się przez $\omega(g(n))$ i
- funkcji asymptotycznie **większej** od funkcji $g(n)$; zbiór takich funkcji oznacza się przez $o(g(n))$.

Na przykład, funkcja $f(n)$ jest asymptotycznie **podobna** do funkcji $g(n)$ wtw gdy istnieją $c_0 > 0$, $c_1 > 0$ i $n_0 \in \mathbb{N}$, że $c_0 \cdot |g(n)| \leq |f(n)| \leq c_1 \cdot |g(n)|$ dla **wszystkich $n \geq n_0$** .

Symbole asymptotyczne mogą pojawić się w złożonych wyrażeniach arytmetycznych. Dla przykładu:

$\sum_{i=0}^n i^2 = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$. Możemy teraz napisać $\sum_{i=0}^n i^2 = O(n^3)$, ale także $\sum_{i=0}^n i^2 = \frac{1}{3}n^3 + O(n^2)$, co formalnie oznacza $\sum_{i=0}^n i^2 - \frac{1}{3}n^3 \in O(n^2)$. Co więcej okazuje się, że symbol $=$ może pełnić nie tylko rolę \in , ale czasami także rolę \subseteq . Na przykład wyrażenie

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

ma po obu stronach "równości" zbiory funkcji, przy czym po lewej stronie są to wszystkie funkcje postaci $\frac{1}{3}n^3 + f(n)$ dla $f(n) = O(n^2)$. W tej sytuacji znak $=$ powinien być formalnie rozumiany jako inkluzja \subseteq .

Dla poniższych funkcji z N do R mamy:

- $f(n) = O(f(n))$,
- $f(n) = O(O(g(n)))$ wtedy i tylko wtedy, gdy $f(n) = O(g(n))$,
- $f(n) = O(|g(n)|)$ wtedy i tylko wtedy, gdy $f(n) = O(g(n))$,
- $f(n) = c \cdot O(g(n))$ wtedy i tylko wtedy, gdy $f(n) = O(g(n))$,
- jeśli $f_1(n) = O(g_1(n))$ i $f_2(n) = O(g_2(n))$
to $f_1(n) + f_2(n) = O(g_1(n) + g_2(n))$,
- jeśli $f_1(n) = O(g_1(n))$ i $f_2(n) = O(g_2(n))$
to $f_1(n) \cdot f_2(n) = O(g_1(n)g_2(n))$.

Przykład

$p(n) = a_k n^k + \dots + a_1 n + a_0$ jest wielomianem stopnia k

$$\begin{aligned} |p(n)| &= |a_k n^k + \dots + a_1 n + a_0| \\ &\leq |a_k| n^k + \dots + |a_1| n + |a_0| \\ &= a_k \cdot O(n^k) + \dots + a_1 \cdot O(n) + a_0 \cdot O(1) && \text{bo } n^i = O(n^i) \\ &= O(n^k) + \dots + O(n) + O(1) && \text{bo } c \cdot O(n^i) = O(n^i) \\ &= O(n^k) + \dots + O(n^k) + O(n^k) && \text{bo } O(n^i) = O(n^k), \text{ dla } i \leq k \\ &= O(n^k), && \text{bo } O(n^k) + O(n^k) = O(n^k) \end{aligned}$$

a zatem $p(n) = O(n^k)$

i dalej niech $a = \max(|a_0|, |a_1|, \dots, |a_{k-1}|)$

wtedy dla każdego n większego od pewnego n_0 mamy

$$|a_k| n^k \geq 2kan^{k-1} \geq 2(|a_{k-1}| n^{k-1} + |a_{k-2}| n^{k-2} + \dots + |a_0|)$$

wystarczy więc $n \geq \frac{2ka}{|a_k|}$.

Teraz

$$\begin{aligned} |p(n)| &= |a_k n^k + a_{k-1} n^{k-1} + \dots + a_0| \geq |a_k| n^k - (|a_{k-1}| n^{k-1} + \dots + |a_0|) \\ &\geq |a_k| n^k - kan^{k-1} \geq \frac{|a_k| n^k}{2}, \end{aligned}$$

więc $p(n) = \Omega(n^k)$.

Przykład

Z asymptotycznego punktu widzenia wszystkie funkcje logarytmiczne są podobne tzn. np. $\ln n = \Theta(\lg n)$; $\log n = \Theta(\lg n)$, lub ogólniej:
 $\log_a n = \Theta(\log_b n)$, dla $a, b > 1$.

Jest to po prostu wzór na zamianę podstaw logarytmu:

$$\log_a n = \frac{1}{\log_b a} \cdot \log_b n,$$

gdzie ta sama stała $\frac{1}{\log_b a}$ jest dobra do dolnego i górnego ograniczenia.

Przykład

Dla wielomianów $f(n), g(n)$ mamy:

$f = O(g)$ wtedy i tylko wtedy, gdy $\deg(f) \leq \deg(g)$

Ustala to hierarchię rzędów funkcji: $n, n^2, n^3, n^4, \dots, n^d, n^{d+1}, \dots$

Również dla "stopni" będącymi dowolnymi liczbami dodatnimi mamy:

$n^a = O(n^b)$ wtedy i tylko wtedy, gdy $a \leq b$

Na przykład: $\sqrt{n} \in O(n)$, $\sqrt[3]{n} \in O(\sqrt{n})$.

Lemat

Dla wielomianu dowolnego stopnia d mamy $n^d \in O(a^n)$, o ile tylko $a > 1$.

Przykład

Oczywiście $2^n \leq 3^n$, więc $2^n \in O(3^n)$.

Ale $3^n \notin O(2^n)$. Gdyby bowiem $3^n \leq c \cdot 2^n$ to $\left(\frac{3}{2}\right)^n = \frac{3^n}{2^n} \leq c$,

podczas gdy funkcja wykładnicza $\left(\frac{3}{2}\right)^n$ rośnie do nieskończoności. Nie może zatem być ograniczona przez żadną stałą c .

Lemat

Ogólnie dla $a > 1$, $b > 1$ mamy $a^n \in O(b^n)$ wtedy i tylko wtedy, gdy $a < b$.

Przykład

Mamy $2^n \in O(n!)$ oraz $n! \in O(n^n)$.

Istotnie $2^n \leq 2 \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot n = 2 \cdot n!$, bo każdy czynnik (poza pierwszym) w $n!$ jest równy co najmniej 2.

Podobnie $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n \leq n \cdot n \cdot n \cdot \dots \cdot n = n^n$, bo każdy czynnik w $n!$ jest nie większy niż n .

Przykład

Wykorzystajmy pomysł młodego Gaussa. W wieku 9 lat zaproponował policzenie skończonej sumy początkowych liczb naturalnych (od 1) w następujący sposób:

$$S_n = 1 + 2 + 3 + \dots + (n-1) + n, \text{ ale także } S_n = n + (n-1) + \dots + 3 + 2 + 1.$$

$$\text{Wobec tego } 2 \cdot S_n = (n+1) + (n+1) + (n+1) + \dots + (n+1) = n(n+1).$$

W przypadku $n!$ weźmy:

$$n!^2 = (1 \cdot 2 \cdot 3 \cdot \dots \cdot n) \cdot (n \cdot (n-1) \cdot \dots \cdot 3 \cdot 2 \cdot 1) = \prod_{k=1}^n k \cdot (n+1-k)$$

Wielomian $k \cdot (n+1-k)$ przybiera najmniejszą wartość dla $k=1$, a największą dla $k=\frac{1}{2} \cdot (n+1)$. Zatem $n!^2$ można obustronnie oszacować iloczynami n najmniejszych i n największych czynników wynoszących odpowiednio:

$$n^n \text{ i } (n+1)^{2n}/2^{2n}. \text{ Ostatecznie } n^{n/2} \leq n! \leq (n+1)^n/2^n.$$

Lemat

Oto ciąg funkcji, z których każda jest O -duże od następnej, ale nie od poprzedniej:

$$\frac{1}{n^n}, \frac{1}{n!}, \dots, \frac{1}{3^n}, \frac{1}{2^n}, \dots, \frac{1}{n^3}, \frac{1}{n^2}, \frac{1}{n \lg n}, \frac{1}{n}, \frac{1}{\lg n}, \frac{1}{\sqrt{n}}, \frac{1}{\sqrt[3]{n}}, \dots, \frac{1}{\lg n}, \frac{1}{\lg \lg n}, 1$$

i dalej

$$1, \lg \lg n, \lg n, \dots, \sqrt[3]{n}, \sqrt{n}, \frac{n}{\lg n}, n, n \lg n, n \sqrt{n}, n^2, n^3, \dots, n^{\lg n}, 2^n, 3^n, n!, n^n, 2^{2^n}.$$

Przykład

Nie każde dwie funkcje są porównywalne asymptotycznie.
Na przykład dla funkcji

$$f(n) = \begin{cases} n, & \text{dla } n \text{ parzystych} \\ n^3, & \text{dla } n \text{ nieparzystych} \end{cases}; \quad g(n) = n^2$$

mamy $f(n) \neq \Omega(g(n))$; $f(n) \neq O(g(n))$.

Wykonaj zadania z pliku zad1.pdf