Kryptografia z elementami algebry, ćwiczenia 1

Maciej Grześkowiak

20 października 2020

Kryptografia, złożoność obliczeniowa

Notacja wielkie-O

Definicja Niech $f, g : \mathbb{N} \mapsto \mathbb{R}$. Mówimy, że

$$f(n) = O(g(n))$$

jeśli istnieje stała $c > 0$ taka, że dla każdego $n \geq n_0$ mamy

$$|f(n)| \leq cg(n).$$

Własności:
Niech $f(n) = O(g(n))$, $u(n) = O(w(n))$, to

1. $f(n) \pm u(n) = O(g(n) + w(n))$,
2. $f(n)u(n) = O(g(n)w(n))$.

Notacja wielkie-O, przykłady

Zadanie: Niech $LB(n)$ oznacza liczbę bitów n, dla $n \in \mathbb{N}$. Za pomocą notacji wielkie-O oszacuj funkcję $LB(n)$.

Rozwiązanie:
Niech

$$n = (b_{k-1} b_{k-2} \dots b_0)_2, \quad b_{k-1} = 1.$$

Stąd,

$$2^{k-1} \leq n < 2^k,$$

oraz

$$LB(n) = [\log_2 n] + 1 = [\frac{\log n}{\log 2}] + 1 = O(\log n).$$

Operacje elementarne na bitach

p	0	0	0	0	1	1	1	1
r_1	0	0	1	1	0	0	1	1
r_2	0	1	0	1	0	1	0	1
w	0	1	1	0	1	0	0	1
np	0	0	0	1	0	1	1	1

Operacje elementarne na bitach, przykład

Zadanie: Niech $a, b \in \mathbb{N}$, gdzie $a \geq b$. Ile elementarnych operacji na bitach potrzeba do obliczenia $S(a, b) = a + b$?

Zadanie: Niech $a, b \in \mathbb{N}$, gdzie $a \geq b$. Ile elementarnych operacji na bitach potrzeba do obliczenia $I(a, b) = ab$?

Operacje elementarne na bitach, przykład

Przykład: Niech $a = (1011)_2, b = (1001)_2$, to

$$\begin{array}{cccccc} & 1 & 0 & 1 & 1 \\ + & 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 \end{array}$$

Stąd, wykonujemy $O(\log a)$ operacji elementarnych na bitach.

Operacje elementarne na bitach, przykład

Przykład: Niech $a = (1011)_2, b = (1001)_2$, to

$$
\begin{array}{cccccccc}
 & & & & 1 & 0 & 1 & 1 \\
 & & & * & 1 & 0 & 0 & 1 \\
\hline
 & & & & 1 & 0 & 1 & 1 \\
 & & & 0 & 0 & 0 & 0 & \\
 & & 0 & 0 & 0 & 0 & & \\
+ & 1 & 0 & 1 & 1 & & & \\
\hline
\end{array}
$$

Stąd, wykonujemy $O(\log a)O(\log b) = O(\log^2 a)$ operacji elementarnych na bitach.

Notacja wielkie-O, przykłady

Zadanie: Zabadaj czy $f(n) = O(g(n))$ lub $g(n) = O(f(n))$, gdzie

$$f(n) = n^2 + n + 1, \quad g(n) = 50n + 30.$$

Rozwiązanie:
Istnieje $n_0 = 10$ oraz $c = 6$ takie, że dla każdego $n \geq n_0$ zachodzi

$$|50n_0 + 30| \leq c(n_0^2 + n_0 + 1)$$

Stąd, $50n + 30 = O(n^2 + n + 1)$.
Ustalmy $c > 0$. Istnieje n_0 takie, że dla każdego $n \geq n_0$ zachodzi

$$|n_0^2 + n_0 + 1| \geq c(50n_0 + 30)$$

Rozszerzony algorytm Euklidesa, idea

Dane: $x = 10, N = 13,\ x < N,$
Wynik: (u, v, d) takie, że $xu + vN = d$ oraz $(x, N) = d$.

$$13 = 1 \cdot 10 + 3$$
$$10 = 3 \cdot 3 + 1$$
$$3 = 1 \cdot 3 + 0$$

$$13 = 13 \cdot 1 + 0 \cdot 10$$
$$10 = 13 \cdot 0 + 1 \cdot 10$$
$$3 = 13 \cdot 1 - 1 \cdot 10$$
$$1 = 13 \cdot (-3) + 4 \cdot 10$$

Rozszerzony algorytm Euklidesa, implementacja

Dane: x, N, $x < N$,
Wynik: (u, v, d) takie, że $xu + vN = d$ oraz $(x, N) = d$.

1. $A = N$; $B = x$; $U = 0$; $V = 1$;
2. **repeat**
3. $q = A \text{ div } B$
4. $$\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \begin{bmatrix} A \\ B \end{bmatrix}$$
5. $$\begin{bmatrix} U \\ V \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \begin{bmatrix} U \\ V \end{bmatrix}$$
6. **until** $B == 0$
7. $d = A$, $u = U$, $v = (d - xu)/N$
8. **return** (u, v, d)

Notacja wielkie-O, przykłady

Zadanie 1: Zabadaj czy $f(n) = O(g(n))$ lub $g(n) = O(f(n))$, gdzie

1. $f(n) = n^3 + 1$, $g(n) = 1000n^2 + 60n$,
2. $f(n) = n + 1$, $g(n) = 5\log(n)$,
3. $f(n) = n^2 + n + 1$, $g(n) = 5n^2 + 7$.