ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ
ΣΗΜΕΙΩΣΕΙΣ $\#2$

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

1. Ο συμβολισμος $O(\cdot)$

Ας δούμε αρχικά τον ορισμό.

Ορισμός 1.1. Έστω συναρτήσεις $f, g : \mathbb{N} \to \mathbb{R}$. Τότε ορίζουμε το σύνολο $O(g)$

$$f \in O(g) \iff \exists c > 0\ \exists n_0 \in \mathbb{N}\ \forall n \geq n_0, |f(n)| \leq c|g(n)|.$$

Εμείς θα έχουμε μόνο περιπτώσεις όπου οι f και g είναι μη αρνητικές για κάθε φυσικό, εκτός ίσως από κάποιους αρχικούς όρους. Οπότε στον παραπάνω ορισμό δεν είναι απαραίτητες οι απόλυτες τιμές. Ακόμη, συχνά αντί για $f \in O(g)$ θα γράφουμε $f = O(g)$ ή και $f \ll g$.

Βλέπουμε ότι ο ορισμός μάς δίνει ένα σύντομο τρόπο γραφής ενός πάνω φράγματος, μέχρι πολλαπλασιαστικής σταθεράς, μιας συνάρτησης, για «μεγάλα» n. Ας δούμε μερικά παραδείγματα.

Παραδείγματα 1.2. (1) Τετριμμένα ισχύει: $n^a = O(n^b)$ για $a \leq b$.

(2) Αν $f = O(g)$ και $g = O(h)$ τότε $f = O(h)$. Πραγματικά υπάρχουν σταθερές $c_1, c_2 > 0$ και φυσικοι n_1, n_2 τέτοιοι ώστε

$$f(n) \leq c_1 g(n) \quad \text{για} \quad n \geq n_1$$

και

$$g(n) \leq c_2 h(n) \quad \text{για} \quad n \geq n_2.$$

Τότε με $n_0 = \max\{n_1, n_2\}$ και $c = c_1 c_2$ έχουμε

$$f(n) \leq c h(n) \quad \text{για} \quad n \geq n_0.$$

(3) Όμοια βλέπουμε οτι αν $f_1 = O(g)$ και $f_2 = O(g)$ τότε $f_1 + f_2 = O(g)$.

(4) Αν $f(n) = a_d n^d + \cdots + a_1 n + a_0$ με $a_d > 0$, τότε $f(n) = O(n^d)$. Πραγματικά, κάθε όρος $a_i n^i$, $i = 0, \ldots, d$ είναι στο $O(n^d)$, και έχουμε σταθερό πλήθος όρων (ανεξάρτητο του n), οπότε το αποτέλεσμα προκύπτει από το προηγούμενο παράδειγμα.

(5) Ισχύει $n^d = O(e^n)$ για οποιοδήποτε φυσικό d. Αυτό μπορούμε να το δούμε για παράδειγμα από το ανάπτυγμα Taylor της e^x γύρω απο το 0. Για $x = n$, όλοι οι όροι του αναπτυγματος είναι θετικοί, άρα $e^n \geq n^d/d!$. Σε συνδοιασμό με το προηγούμενο παράδειγμα βλέπουμε ότι για κάθε πολυώνυμο f ισχύει $f(n) = O(e^n)$.

(6) Με τον ίδιο τρόπο δείχνουμε ότι $n = O(e^{n^\epsilon})$ για οποιοδήποτε $\epsilon > 0$. Πραγματικά, από το ανάπτυγμα Taylor της εκθετικής γύρω από το 0, έχουμε $e^x \geq x^d/d!$ για κάθε $x \geq 0$ και για κάθε φυσικό d. Για $x = n^\epsilon$ και $d = \lfloor 1/\epsilon \rfloor + 1$ έχουμε $e^{n^\epsilon} \geq n^{\epsilon d}/d! \geq n/d!$. Το παράδειγμα αυτό είναι ενδιαφέρον για $0 < \epsilon < 1$. Για παράδειγμα, για $\epsilon = 1/2$ έχουμε, $n = O(e^{\sqrt{n}})$.

(7) Ισχύει $\log n = O(n^\epsilon)$ για οποιοδήποτε $\epsilon > 0$. Στο προηγούμενο παράδειγμα δείξαμε ότι

$$e^{n^\epsilon} \geq \frac{n^{\epsilon d}}{d!}$$

όπου $d = \lfloor 1/\epsilon \rfloor + 1 > 1/\epsilon$, άρα $\epsilon d > 1$ και έχουμε

$$e^{n^\epsilon} \geq \frac{n^{\epsilon d}}{d!} \geq n$$

για $n \geq n_0 = \lfloor (d!)^{1/(\epsilon d - 1)} \rfloor$. Λογαριθμίζοντας παίρνουμε το ζητούμενο.

(8) Προσέξτε ότι *δεν* ισχύει $e^n = O(e^{n/2})$ (γιατι;).

Παρατηρήστε ότι είναι δυνατό να συμβαίνει $f = O(g)$ και $g = O(f)$ για δύο διαφορετικές συναρτήσεις f και g (βρείτε παραδείγματα). Τότε θα λέμε ότι οι f και g έχουν ίδια τάξη μεγέθους.

Αν για μια συνάρτηση $f : \mathbb{N} \to \mathbb{R}$ υπάρχει πολυωνυμική συνάρτηση $p : \mathbb{N} \to \mathbb{R}$ τέτοια ώστε $f = O(p)$, θα λέμε ότι η f είναι πολυωνυμικά φραγμένη.

2. Ο Συμβολισμος $o(\cdot)$

Ορισμός 2.1. Έστω συναρτήσεις $f, g : \mathbb{N} \to \mathbb{R}$. Τότε ορίζουμε το σύνολο $o(g)$

$$f \in o(g) \quad \Longleftrightarrow \quad \forall c > 0 \; \exists n_0 \in \mathbb{N} \; \forall n \geq n_0, |f(n)| \leq c|g(n)|.$$

Παρατηρήστε ότι, εάν $g(n) \neq 0$, έχουμε την ισοδυναμία

$$f \in o(g) \Longleftrightarrow \lim_{n\to\infty} \frac{f(n)}{g(n)} = 0.$$

Δείτε επίσης ότι $f = o(g) \Rightarrow f = O(g)$. Το αντίστροφο δεν ισχύει. (Δώστε παράδειγμα.) Εξετάστε σε ποια από τα παραπάνω παραδείγματα μπορούμε να αντικαταστήσουμε το $O()$ με $o()$.

3. Πολυπλοκοτητα αλγοριθμου

Όλοι έχουμε μια διαισθητική αντίληψη της έννοιας του αλγόριθμου. Έστω ένας αλγόριθμος $\mathcal{A}$ που έχει είσοδο μήκους n. Δηλαδή το πλήθος των συμβόλων που χρειάζονται για την καταγραφή της εισόδου είναι n. Για παράδειγμα για να γράψουμε τον φυσικό αριθμό N σε δεκαδικό σύστημα χρειαζόμαστε $\lfloor \log_{10} N \rfloor + 1$ δεκαδικά ψηφία – δηλαδή $O(\log N)$ ψηφία. Για να παραστήσουμε

ένα πολυώνυμο βαθμού d με συντελεστες ακεραίους με απόλυτη τιμή το πολύ N χρειαζόμαστε $O(d \log N)$ ψηφία.

Η πολυπλοκότητα του αλγόριθμου $\mathcal{A}$ είναι ο αριθμός των βημάτων που χρειάζεται ο αλγόριθμος για να τερματίσει και δίνεται ως συνάρτηση του μήκους της εισόδου.

Για παράδειγμα, ας δουμε τον αλγόριθμο της πρόσθεσης φυσικών αριθμών. Αν η είσοδος είναι δύο φυσικοί a και b, ο αλγόριθμος προσθέτει ψηφίο προς ψηφίο. Το πλήθος των βημάτων είναι $O(\max\{\log a, \log b\})$. Ο «σχολικός» πολλαπλασιασμός ακεραίων a και b έχει πολυπλοκότητα $O(\log a \log b)$. Επίσεις η διαίρεση με υπόλοιπο του a με το b γίνεται σε χρόνο $O(\log a \log b)$.

Συχνά θα μετράμε την πολυπλοκότητα ενός αλγόριθμου ως αριθμό κάποιων μη στοιχειωδών βημάτων (π.χ. αριθμητικών πράξεων). Για παράδειγμα, αν έχουμε δύο $m \times m$ πίνακες $A, B \in \mathrm{Mat}_m(\mathbb{Z})$, τότε το άθροισμα τους μπορεί να υπολογιστεί με m^2 προσθέσεις ακεραίων. Εάν οι ακέραιοι που εμφανίζονται στους πίνακες είναι κατ' απόλυτη τιμή το πολύ N, τότε η πολυπλοκότητα του αλγόριθμου είναι $O(m^2 \log N)$. Βρείτε προσεκτικά πόσες προσθέσεις και πόσους πολλαπλασιασμούς ακεραίων χρειάζεται ο «κλασικος» αλγόριθμος πολλαπλασιασμού πινάκων για να υπολογίσει τον $A \cdot B$. Προσέξτε ότι αν $A = (a_{ij})$ και $B = (b_{ij})$ και $|a_{ij}| \leq N$ και $|b_{ij}| \leq N$ για $1 \leq i, j \leq m$ τότε τα γινόμενα $a_{ik}b_{kj}$ που θα εμφανιστούν μπορεί να έχουν τιμή έως και N^2. Δηλαδή οι προσθέσεις θα είναι μεταξύ αριθμών μεγαλύτερου μεγέθους. Αυτό βέβαια δε θα επηρρεάσει τελικά τα πράγματα, αφού το κόστος μιας πρόσθεσης δύο ακεραίων μεγέθους το πολύ N^2 είναι στο $O(\log N^2) = O(\log N)$.