

Harjutustund 1: Keerukusteooria alused

Ahto Buldas

Ülesanded.

Ülesanne 1: Leia üksühene vastavus hulkade \mathbb{N} ja $\{0, 1\}^*$ vahel.

Ülesanne 2: Näita, et $3n^2 + 6n + 7 = O(n^2)$.

Ülesanne 3: Näita, et $2n^3 + 6n^2 + 6n + 1 = O(n^3)$.

Ülesanne 4: Näita, et $n^3 \neq O(n^2)$.

Ülesanne 5: Näita, et $n! \neq O(2^n)$.

Ülesanne 6: Leia funktsioonid f ja g , nii et $f(n) = O(g(n))$, $g(n) \neq O(f(n))$ ja $f(n) \neq o(g(n))$.

Ülesanne 7: Näita, et (a) kui $\varepsilon(n) = 2^{-n^{O(1)}}$, siis $\text{BPP}_\varepsilon = \text{BPP}$; ja (b) kui $\varepsilon = n^{-O(1)}$, siis $\text{BPP}_{\frac{1}{2}-\varepsilon} = \text{BPP}$.

Ülesanne 1: lahendus

Tavaline binaaresitus ($0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 10$, $3 \mapsto 11$, jne.) ei ole üksühene, sest tühistring ja nulliga algavad järjendid (peale 0) ei kodeeri ühtegi naturaalarvu.

Sobiliku vastavuse $\varphi: \mathbb{N} \rightarrow \{0, 1\}^*$ saame aga, kui defineerime $\varphi(n)$, kui arvu $n + 1$ binaaresituse, mille algusest on ära võetud 1. Näiteks $0 \mapsto \square$, $1 \mapsto 0$, $2 \mapsto 1$, $3 \mapsto 00$, jne.

Ülesanne 2: lahendus

Tuleb näidata, et leiduvad konstandid c ja n_0 , nii et iga $n \geq n_0$ korral:

$$3n^2 + 6n + 7 \leq c \cdot n^2 .$$

Võttes $c = 4$, saame viimase võrratuse asemel ruutvõrratuse

$$f(n) = n^2 - 6n - 7 \geq 0 ,$$

mille nullkohad x_1 ja x_2 (kus $x_1 \leq x_2$) saaksime täpselt leida ja valida n_0 neist suuremana. Samas ei ole nullkohtade täpne leidmine antud ülesande korral tähtis ja saab teha lihtsamalt. Oluline on tähelepanek, et $f(n)$ on positiivne kui kas $n \leq x_1$ või $n \geq x_2$. Piisab seega, kui valida n_0 nii, et $x_2 \leq n_0$, sest siis on $f(n) \geq 0$ iga $n \geq n_0$ korral.

Piirkondade $n \leq x_1$ ja $n \geq x_2$ eristamiseks on kasulik tähelepanek, et esimeses piirkonnas $f(x)$ kahaneb ja teises kasvab. Seega, teise piirkonda

kuulumise tingimus on

$$\frac{d}{dn}(n^2 - 6n - 7) = 2n - 6 \geq 0 .$$

Võttes näiteks $n_0 = 100$ on selge, et $f(n_0) > 0$ ja $\frac{d}{dn}f(n_0) > 0$ ja seega $f(n) \geq 0$ iga $n \geq n_0$ korral.

Ülesanne 3: lahendus

Näitame, et $2n^3 + 6n^2 + 6n + 1 \leq 3 \cdot n^3$ iga $n \geq n_0$, kus n_0 on piisavalt suur konstant. Lihtsustades saame, et võrratus on samaväärne kuupvõrratusega:

$$f(n) = n^3 - 6n^2 - 6n - 1 \geq 0 .$$

Olgu x_1 , x_2 ja x_3 polünoomi f nullkohad, kusjuures $x_1 \leq x_2 \leq x_3$. Konstant n_0 tuleb valida nii et $x_3 \leq n_0$. On lihtne veenduda, et n_0 kuulub piirkonda $[x_3 \dots \infty)$ parajasti siis, kui $f(n_0) \geq 0$ (f on positiivne), $\frac{d}{dn}f(n_0) \geq 0$ (f kasvab) ja $\frac{d^2}{dn^2}f(n_0) \geq 0$ (f on kumer*). Võttes $n_0 = 100$ on ilmselt kõik kolm tingimust rahuldatud.

*Matemaatikute kumeruse ja nõgususe mõisted on vastavate üldkeeles mõistete vastandid, st kumera funktsiooni graafik meenutab kaussi, ja nõgusa funktsiooni graafik mäge.

Ülesanne 4: lahendus

$n^3 \neq O(n^2)$ tõestamiseks tuleb näidata, et iga c ja n_0 korral leidub $n \geq n_0$, nii et

$$n^3 > c \cdot n^2 .$$

Et see võrratus on $n \neq 0$ korral samaväärne võrratusega $n > c$, siis piisab, kui võtta $n = \max\{c, n_0\}$.

Ülesanne 5: lahendus

Et võrratus $n! > c \cdot 2^n$ on samaväärne võrratusega $\frac{n!}{c \cdot 2^n} > 1$, analüüsime suhet

$$\frac{n!}{c \cdot 2^n} = \frac{1}{c} \cdot \frac{1}{2} \cdot \underbrace{\frac{2}{2} \cdot \frac{3}{2} \cdots \frac{n-1}{2}}_{>1} \cdot \frac{n}{2}.$$

On näha, et võrratuse $n! > c \cdot 2^n$ kehtivuseks piisab, kui valida n nii, et $\frac{1}{2c} \cdot \frac{n}{2} \geq 1$, st $n \geq 4c$ ja seega võrratuseks $n! \neq O(2^n)$ on piisav kui valida $n = \max\{n_0, 4c\}$.

Ülesanne 6: lahendus

Kui valida näiteks $f(n) = n^2$ ja $g(n) = n^3$, siis on $f(n) = O(g(n))$ ja $g(n) \neq O(f(n))$ (vt. Ül.4) täidetud, kuid $f(n) = o(g(n))$, sest

$$\lim_{n \rightarrow \infty} \frac{n^2}{n^3} = \lim_{n \rightarrow \infty} \frac{1}{n} = 0 .$$

Kui aga võtta $f(n) = n^2$ ja

$$g(n) = \begin{cases} n^3 & \text{kui } n \text{ on paaris,} \\ n^2 & \text{kui } n \text{ on paaritu.} \end{cases}$$

saamegi otsitavad funktsioonid, sest:

- $f(n) = O(g(n))$ võrratuse $f(n) \leq g(n)$ tõttu.

- $g(n) \neq O(f(n))$, sest $g(n) = n^3$ paarisarvuliste n -de korral ja seega iga c ja n_0 korral saab valida $n = 2 \cdot \max\{n_0, c\}$, mille korral kehtib seega $g(n) > c \cdot f(n)$.
- $f(n) \neq o(g(n))$, sest jagatisel $\frac{f(n)}{g(n)}$ puudub piirväärtus piirprotsessis $n \rightarrow \infty$ – tema väärtus "pendeldab" 1 ja $\frac{1}{n}$ vahel.

Ülesanne 7: Lahendus

Kasutame hääletusalgoritmi.

(a) näitamiseks kasutame BPP algoritmi parandamiseks kasutatava hääletusalgoritmi veahinnangut:

$$\Pr \left[\sum_{i=1}^m x_i \geq \frac{m}{2} \right] \leq e^{-\frac{m}{12}} .$$

Piisab, kui leida m , nii et $e^{-\frac{m}{12}} \leq e^{-n^{O(1)}} < 2^{-n^{O(1)}}$, s.t. $m = n^{O(1)}$ ja seega piisab polünomiaalses ajas töötavast hääletusalgoritmist.

(b) näitamiseks kasutame Tšernovi tõket: Olgu x_1, \dots, x_m sõltumatud juhuslikud suurused, mille väärtus on kas 1 või 0 vastavalt tõenäosustega p ja $1 - p$. Siis iga $0 \leq \Theta \leq 1$ korral

$$\Pr \left[\sum_{i=1}^m x_i \geq (1 + \Theta)pm \right] \leq e^{-\frac{\Theta^2}{3}pm} .$$

võttes $p = \frac{1}{2} - \epsilon$. Tõenäosuse all sobiliku parema poole $m/2$ saamiseks lahendame võrrandi:

$$(1 + \Theta) \left(\frac{1}{2} - \epsilon \right) m = \frac{m}{2} , \text{ s.t. } (1 + \Theta) \left(\frac{1}{2} - \epsilon \right) = \frac{1}{2} ,$$

ja saame $\Theta = \frac{\epsilon}{\frac{1}{2} - \epsilon}$. Tingimusest $\Theta \leq 1$ saame, et lahend on mõttekas tingimusel, et $\epsilon \leq \frac{1}{4}$. Seega on m katse korral olemas hääletusvea ülemtõke:

$$\Pr \left[\sum_{i=1}^m x_i \geq \frac{m}{2} \right] \leq e^{-\frac{\epsilon^2}{3(\frac{1}{2} - \epsilon)^2} \left(\frac{1}{2} - \epsilon \right) m} .$$

Sobiliku katsete arvu m leidmiseks tuleb lahendada võrrand

$$e^{-\frac{\epsilon^2}{3(\frac{1}{2}-\epsilon)^2} \left(\frac{1}{2}-\epsilon\right)^m} \leq \frac{1}{4},$$

et tagada **BPP** definitsioonis nõutud veapiir $\frac{1}{4}$, s.t. piisab kui leida m nii et:

$$\frac{\epsilon^2}{3 \left(\frac{1}{2} - \epsilon\right)^2} \left(\frac{1}{2} - \epsilon\right)^m \geq 2,$$

kusjuures kerge on veenduda, et kui $\epsilon = n^{-O(1)}$, siis $m = n^{O(1)}$, st hääletusalgoritm on polünomiaalse tööajaga.