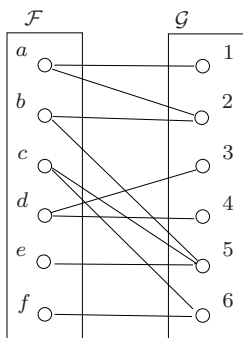


# Ülesanded

## I töö

Ü1.I-1. Kas järgneval graafil alustega  $\mathcal{F}$  ja  $\mathcal{G}$  on  $(\frac{1}{2}, \frac{1}{2})$ -laiendus?



Ü1.I-2. Kas  $\frac{15n^4+2n^2+5}{n} = O(n^3)$ ? Põhjenda!

## II töö

Ü1.II-1. Kas juhuslik suurus  $X$  võimalike väärtustega  $\{x_1, x_2, x_3, x_4\}$  ja suurus  $Y$  väärtustega  $\{y_1, y_2, y_3, y_4\}$  on sõltumatud, kui on teada allolev tabel tõenäosustega  $\Pr[x_i, y_j] = \Pr[X = x_i, Y = y_j]$ . Põhjenda!

	$x_1$	$x_2$	$x_3$	$x_4$
$y_1$	0.02	0.04	0.06	0.08
$y_2$	0.01	0.02	0.03	0.04
$y_3$	0.04	0.08	0.12	0.16
$y_4$	0.03	0.06	0.09	0.12

Ü1.II-2. Olgu  $g_1: \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$  ja  $g_2: \{0, 1\}^{n+1} \rightarrow \{0, 1\}^{n+2}$  pseudo-juhuarvude generaatorid, kusjuures  $g_2(T)$  on (iga  $T \in \{0, 1\}^{n+1}$  korral) arvutatav ajaga  $t_2(n)$ . Näita, et kui  $g_1$  ja  $g_2$  on eristamatud, siis ka nende kompositsioon  $g_2 \circ g_1$  on eristamatu. Täpsemini, kui leidub kompositsiooni eristav vastane  $A$  tööajaga  $t(n)$  ja edukusega

$$\delta(n) = |\Pr_X[A(g_2(g_1(X))) = 1] - \Pr_Z[A(Z) = 1]|, \quad (1)$$

kus  $X \in \{0, 1\}^n$  ja  $Z \in \{0, 1\}^{n+2}$  on ühtlase jaotusega sõltumatud juhuslikud suurused; siis leidub vähemalt üks järgmistest vastastest:

- (a) generaatorit  $g_1$  eristav vastane tööajaga  $t(n) + t_2(n)$  ja edukusega  $\frac{\delta(n)}{2}$
- (b) generaatorit  $g_2$  eristav vastane tööajaga  $t(n)$  ja edukusega  $\frac{\delta(n)}{2}$ .

## Lahendused

**Ü1.I-1.** Olgu  $X \in \mathcal{F}$  ja  $Y \in \mathcal{G}$  ühtlase jaotusega juhuslikud suurused. Võtame  $F = \{c, e, f\}$ , saame et  $\Pr[X \in F] = \frac{1}{2}$ . Samas  $E(F) = \{5, 6\}$  ja seega  $\Pr[Y \in E(F)] = \frac{2}{6} = \frac{1}{3} < 1 - \frac{1}{2}$ . Seega ei kehti laienduse tingimus iga alamhulga  $F \subseteq \mathcal{F}$  korral, millest järeldub, et antud graafil  $(\frac{1}{2}, \frac{1}{2})$ -laiendus puudub.

**Ü1.I-2.** Võttes  $c = 16$  ja  $n_0 = 2$ , saame et iga  $n > n_0 = 2$  korral  $\frac{5}{n} \leq 2$  ja samuti  $2n + 2 \leq n^3$  ja seega:

$$f(n) = 15n^3 + 2n + \frac{5}{n} \leq 15n^3 + 2n + 2 \leq 15n^3 + n^3 = 16n^3 = c \cdot n^3 .$$

**Ü1.II-1.** Sõltumatuse näitamiseks piisab kui tõestada, et iga väärtuse  $x_i \in \{x_1, x_2, x_3, x_4\}$  ja iga  $y_j \in \{y_1, y_2, y_3, y_4\}$  korral kehtib seos

$$\Pr[X = x_i, Y = y_j] = \Pr[X = x_i] \cdot \Pr[Y = y_j] . \quad (2)$$

Selle seose kontrollimiseks tuleb arvutada tõenäosused:

$$\begin{aligned} \Pr[X = x_i] &= \sum_j \Pr[X = x_i, Y = y_j] \\ \Pr[Y = y_j] &= \sum_i \Pr[X = x_i, Y = y_j] . \end{aligned}$$

Nii arvatud tõenäosused tulevad:  $\Pr[X = x_1] = 0.1$ ,  $\Pr[X = x_2] = 0.2$ ,  $\Pr[X = x_3] = 0.3$ ,  $\Pr[X = x_4] = 0.4$ ,  $\Pr[Y = y_1] = 0.2$ ,  $\Pr[Y = y_2] = 0.1$ ,  $\Pr[Y = y_3] = 0.4$  ja  $\Pr[Y = y_4] = 0.3$ . Kontrollides 16 erineva väärtuste kombinatsiooni korral valemit (2), saame et see alati kehtib ja seega on  $X$  ja  $Y$  sõltumatud.

**Ü1.II-2.** Olgu  $T \leftarrow \{0, 1\}^{n+1}$  ühtlase jaotusega juhuslik suurus. Liites ja lahutades vastase  $A$  edukuse avaldises (1) absoluutväärtuse märgi all

tõenäosuse  $\Pr[A(g_2(T))=1]$ , ja defineerides  $A_1(y) := A(g_2(y))$  (iga  $y \in \{0, 1\}^{n+1}$  korral) saame

$$\begin{aligned}
\delta(n) &= |\Pr_X[A(g_2 g_1(X))=1] - \Pr_T[A(g_2(T))=1] + \Pr_T[A(g_2(T))=1] - \Pr_Z[A(Z)=1]| \\
&= |\Pr_X[A_1(g_1(X))=1] - \Pr_T[A_1(T)=1] + \Pr_T[A(g_2(T))=1] - \Pr_Z[A(Z)=1]| \\
&\leq \underbrace{|\Pr_X[A_1(g_1(X))=1] - \Pr_T[A_1(T)=1]|}_{\delta_1(n)} + \underbrace{|\Pr_T[A(g_2(T))=1] - \Pr_Z[A(Z)=1]|}_{\delta_2(n)} \\
&= \delta_1(n) + \delta_2(n) .
\end{aligned}$$

Seega kas  $\delta_1(n) \geq \frac{\delta(n)}{2}$ , millest järelduks, et vastane  $A_1 = A \circ g_2$  tööajaga  $t(n) + t_1(n)$  eristab generaatori  $g_1$  väljundit edukusega vähemalt  $\frac{\delta(n)}{2}$ ; või siis  $\delta_2(n) \geq \frac{\delta(n)}{2}$ , millest järelduks, et vastane  $A$  tööajaga  $t(n)$  eristab generaatori  $g_2$  väljundit edukusega vähemalt  $\frac{\delta(n)}{2}$ .