

## Ülesanded

**Ül.1.** Olgu  $A \leftarrow \{0, \dots, 5\}$  ja  $B \leftarrow \{0, \dots, 5\}$  sõltumatud ühtlase jaotusega juhuslikud suurused. Kas suurused

$$\begin{aligned} X_0 &= A \cdot 0 + B \pmod{6}, \\ X_1 &= A \cdot 1 + B \pmod{6}, \\ &\dots \\ X_5 &= A \cdot 5 + B \pmod{6} \end{aligned}$$

on ühtlase jaotusega? Kas  $X_0, \dots, X_5$  on paarikaupa sõltumatud?

**Ül.2.** 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

**Ül.3.** Olgu  $\mathcal{D}_1$  ja  $\mathcal{D}_2$  tõenäosusjaotused hulgal  $S$ . Defineerime jaotuste  $\mathcal{D}_1$  ja  $\mathcal{D}_2$  vahelise kauguse kui summa:

$$\partial(\mathcal{D}_1, \mathcal{D}_2) = \frac{1}{2} \sum_{x \in S} \left| \Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x] \right| .$$

Tõesta, et iga eristava vastase  $A$  edukus

$$\delta_A = \left| \Pr[X_1 \leftarrow \mathcal{D}_1 : A(X_1) = 1] - \Pr[X_2 \leftarrow \mathcal{D}_2 : A(X_2) = 1] \right| \leq \partial(\mathcal{D}_1, \mathcal{D}_2) .$$

**Ül.4.** Juhuarvude generaator  $g: \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$  on *turvaline mitteühtlases polünomiaalses mudelis*, kui iga polünomiaalse Turingi masina  $A$  ja iga polünomiaalse pikkusega nõuannete jada  $a = (a_n)_{n \in \mathbb{N}}$  korral:

$$\left| \Pr[A(g(X), a_n) = 1] - \Pr[A(Z, a_n) = 1] \right| = n^{-\omega(1)} ,$$

kus  $X \leftarrow \{0, 1\}^n$  ja  $Z \leftarrow \{0, 1\}^{\ell(n)}$  on ühtlase jaotusega sõltumatud juhuslikud suurused. Tõesta järgmine väide:

**Teoreem:** Kui leiduvad mitteühtlases polünoomiaalses mudelis turvalised juhuarvude generaatorid, siis  $\mathbf{BPP} \subseteq \bigcap_{\gamma > 0} \mathbf{DTIME}(2^{n^\gamma})$ , kus  $\mathbf{DTIME}(f(n))$  tähendab kõigi  $O(f(n))$ -ajas (deterministliku Turingi masinaga) tuvastatavate keelte klassi.

## Lahendused

**Ül.1.** Suurused  $X_i$  on ühtlase jaotusega, sest võrrandil  $a \cdot i + b \equiv \alpha \pmod{6}$  on iga  $\alpha \in \{0, \dots, 5\}$  korral täpselt 6 lahendit ja seega  $\Pr[X_i = \alpha] = \frac{6}{6^2} = \frac{1}{6}$ . Suurused  $X_i$  ei ole paarikaupa sõltumatud, sest näiteks

$$\Pr[X_0 = 0, X_2 = 0] \neq \Pr[X_0 = 0] \cdot \Pr[X_2 = 0] = \frac{1}{6^2} .$$

Tõepoolest, võrrandisüsteemil  $\begin{cases} 0a + b \equiv 0 \pmod{6} \\ 2a + b \equiv 0 \pmod{6} \end{cases}$  on täpselt kaks lahendit  $(0, 0)$  (st  $a = b = 0$ ) ja  $(3, 0)$  (st  $a = 3$  ja  $b = 0$ ), mistõttu

$$\Pr[X_0 = 0, X_2 = 0] = \frac{2}{6^2} \neq \frac{1}{6^2} .$$

**Ül.2.** 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

$$\Pr[X = x_i, Y = y_j] = \Pr[X = x_i] \cdot \Pr[Y = y_j] . \quad (1)$$

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 (1), saame et see alati kehtib ja seega on  $X$  ja  $Y$  sõltumatud.

Ü1.3.

$$\begin{aligned}
\delta_A &= \left| \sum_x \Pr_{\mathcal{D}_1}[x][A(x) = 1] - \sum_x \Pr_{\mathcal{D}_2}[x][A(x) = 1] \right| \\
&= \frac{1}{2} \left| \sum_x (\Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x])[A(x) = 1] + \sum_x (\Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x])[A(x) = 1] \right| \\
&= \frac{1}{2} \left| \sum_x (\Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x])[A(x) = 1] + \sum_x (\Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x])(1 - [A(x) \neq 1]) \right| \\
&= \frac{1}{2} \left| \sum_x (\Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x])[A(x) = 1] - \sum_x (\Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x])[A(x) \neq 1] \right. \\
&\quad \left. + \underbrace{\sum_x (\Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x])}_{=0} \right| \\
&= \frac{1}{2} \left| \sum_x (\Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x])[A(x) = 1] - \sum_x (\Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x])[A(x) \neq 1] \right| \\
&\leq \frac{1}{2} \sum_x \left| \Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x] \right| = \partial(\mathcal{D}_1, \mathcal{D}_2) .
\end{aligned}$$

Ü1.4. Olgu  $L \in \mathbf{BPP}$ . Vastavalt definitsioonile leidub Turingi masin  $M$  tööajaga  $t(n) = n^{O(1)}$  nii et iga  $n$  ja  $x \in \{0, 1\}^n$  korral:

$$\begin{aligned}
x \in L &\Rightarrow \Pr[M(x, Z) = 1] > \frac{3}{4} \\
x \notin L &\Rightarrow \Pr[M(x, Z) = 1] < \frac{1}{4} ,
\end{aligned}$$

kus  $Z \leftarrow \{0, 1\}^{t(n)}$ . Olgu  $\gamma > 0$  mingi konstant,  $\epsilon = 0.9\gamma$  ja  $g_m: \{0, 1\}^m \rightarrow \{0, 1\}^{t(m^{\frac{1}{\epsilon}})}$  mingi mitteühtlases polünoomiaalses mudelis turvaline juhuarvude generaator.

Asendame ehtsa juhuarvu  $Z$  generaatori  $g$  sobiva pikkusega väljundiga. Võtame  $m = n^\epsilon$  ja  $K \leftarrow \{0, 1\}^{n^\epsilon}$ . Ütleme, et  $x \in \{0, 1\}^n$  on *halb*, kui kas:

- $x \in L$  ja  $\Pr[M(x, g_m(K)) = 1] \leq \frac{1}{2}$ , või

- $x \notin L$  ja  $\Pr[M(x, g_m(K)) = 1] > \frac{1}{2}$ ,

st  $x$  on halb kui tavaline hääletusalgoritm ei väljasta tõeväärtust  $[x \in L]$ .

Kui oleks olemas lõpmata palju halbu sisendeid  $x$ , siis leiduks ka lõpmatult paljude  $n$ -de korral sisend  $x_n$  nii et:

$$| \Pr_Z[M(x_n, Z) = 1] - \Pr_K[M(x_n, g(K)) = 1] | \geq \frac{1}{4} ,$$

mis oleks vastuolus generaatori  $g$  turvalisusega. Järelikult eksisteerib vaid lõplik hulk  $\mathcal{L} = \{x_1, \dots, x_\ell\}$  halbu sisendeid.

Seega saab defineerida järgmise deterministliku masina  $P$ , mis sisendi  $x \in \{0, 1\}^n$  korral toimib järgmiselt:

- Kui  $x \in \mathcal{L}$ , siis  $P$  väljastab  $[x \in L]$  (vastus sisaldub  $P$  programmis).
- Võtab  $m = \lceil n^\epsilon \rceil$ .
- Iga  $k \in \{0, 1\}^m$  korral arvutab  $b_k = M(x, g(k))$ .
- Kui  $\sum_k b_k \geq \frac{2^m}{2}$ , siis  $P$  väljastab 1;
- Kui  $\sum_k b_k < \frac{2^m}{2}$ , siis  $P$  väljastab 0.

On selge, et  $P(x) = [x \in L]$  kõikide sisendite  $x$  korral ja  $P$  töötab ajas  $O(t(n) \cdot 2^{n^\epsilon}) = O(2^{n^\gamma})$ .