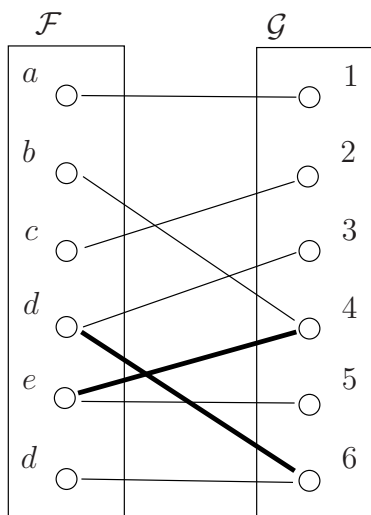


Ülesanded

I töö

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



Ül.I-2. Kas $\frac{19n^5+2n+7}{n} = O(n^4)$? Põhjenda!

II töö

Ül.II-1. Juhuslik suurus X võimalike väärtustega $\{x_1, x_2, x_3, x_4\}$ ja suurus Y väärtustega $\{y_1, y_2, y_3, y_4\}$. Järgmine tabel annab tõenäosused $\Pr[x_i, y_j] = \Pr[X = x_i, Y = y_j]$. Leia kovariatsioon $\text{cov}(X, Y)$ eeldades, et $x_i = y_i = i$ (iga $i \in \{1, \dots, 4\}$ korral).

	x_1	x_2	x_3	x_4
y_1	0.08	0.1	0.02	0.05
y_2	0.02	0.07	0.03	0.18
y_3	0.10	0	0.20	0
y_4	0.05	0.05	0	0.05

Ül.II-2. Olgu $g: \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$ mingi pseudojuhuarvude generaator. Ütleme, et g on *eristamatu kahe katsega*, kui iga vastase A korral tööajaga $T(n)$ ja edukusega

$$\delta(n) = | \Pr[A(g(X_1), g(X_2)) = 1] - \Pr[A(Z_1, Z_2) = 1] |$$

kehtib $\frac{T(n)}{\delta(n)} \geq S(n)$, kus $X_1, X_2 \leftarrow \{0, 1\}^n$ ja $Z_1, Z_2 \leftarrow \{0, 1\}^{\ell(n)}$ on sõltumatud ühtlase jaotusega juhuslikud suurused. Tõesta, et kui g on eristamatu tavalises mõttes, siis on ta eristamatu ka kahe katsega, kusjuures reduktsioon on seejuures lineaarne.

Lahendused

Ül.I-1. Kui esialgselt graafist servade hulgaga E eemaldada servad $(d, 6)$ ja $(e, 4)$ (joonisel paksud), siis kujutavad ülejäänud servad üksühelst vastavust aluste \mathcal{F} ja \mathcal{G} vahel, mistõttu uues graafis servade hulgaga E' iga alamhulga $F \subseteq \mathcal{F}$ korral kehtib $|E'(F)| = |F|$. Et $E(F) \supseteq E'(F)$, siis ühtlase jaotusega valitud $X \in \mathcal{F}$ ja $Y \in \mathcal{G}$ korral kehtib järelikult

$$\Pr[X \in F] \geq \frac{1}{2} \quad \Rightarrow \quad \Pr[Y \in E(F)] \geq \Pr[Y \in E'(F)] \geq \frac{1}{2} = 1 - \frac{1}{2} ,$$

mistõttu definitsiooni järgi on vaadeldaval graafil $(\frac{1}{2}, \frac{1}{2})$ -laiendus.

Ül.I-2. Et $f(n) = \frac{19n^5 + 2n + 7}{n} = 19n^4 + 2 + \frac{7}{n}$. Võttes $c = 20$ ja $n_0 = 2$, saame et iga $n \geq n_0$ korral

$$f(n) \leq 19n^4 + 6 \leq 19n^4 + 2^4 \leq 19n^4 + n^4 = 20n^4 .$$

Seega, $f(n) = O(n^4)$.

Ül.II-1. Arvutame iga i ja j korral tõenäosused $\Pr[x_i] = \sum_j \Pr[x_i, y_j]$ ja $\Pr[y_j] = \sum_i \Pr[x_i, y_j]$. Saame $\Pr[x_1] = 0.25$, $\Pr[x_2] = 0.22$, $\Pr[x_3] = 0.25$, $\Pr[x_4] = 0.28$, $\Pr[y_1] = 0.25$, $\Pr[y_2] = 0.3$, $\Pr[y_3] = 0.3$ ja $\Pr[y_4] = 0.15$. Kovariatsiooni leidmisel kasutame valemit:

$$\text{cov}(X, Y) = E[XY] - E[X] \cdot E[Y] .$$

Arvutades suuruse XY erinevate väärtuste tõenäosused ja esitades need tabelina, saame:

XY	1	2	3	4	6	8	9	16
$\Pr[XY]$	0.08	0.12	0.12	0.17	0.03	0.23	0.2	0.05

Seega $E[XY] = 0.08 + 0.24 + 0.36 + 0.68 + 0.18 + 1.84 + 1.8 + 0.8 = 5.98$,
 $E[X] = 2.56$ ja $E[Y] = 2.35$. Seega $\text{cov}(X, Y) = -0.036$.

Ül.II-2. Defineerime eristava vastase A' järgmiselt. Sisendi $Y \in \{0, 1\}^{\ell(n)}$ korral vastane A' :

1. Genereerib ühtlase jaotusega $Z' \leftarrow \{0, 1\}^{\ell}$ ja $X' \leftarrow \{0, 1\}^n$.
2. Valib juhuslikult ja ühtlaselt $i \leftarrow \{1, 2\}$ ja:
 - (a) Kui $i = 1$, siis tagastab $A(Y, Z')$.
 - (b) Kui $i = 2$, siis tagastab $A(g(X'), Y)$.

Tõenäosus ühtöaselt valitud $X, X_1, X_2 \leftarrow \{0, 1\}^n$ ja $Z, Z_1, Z_2 \leftarrow \{0, 1\}^{\ell}$ korral

$$\Pr_X[A'(g(X_2)) = 1] = \frac{1}{2} \Pr_{Z_2, X_1}[A(g(X_1), Z_2) = 1] + \frac{1}{2} \Pr_{X_1, X_2}[A(g(X_1), g(X_2)) = 1]$$

ja

$$\Pr_Z[A'(Z) = 1] = \frac{1}{2} \Pr_{Z_1, Z_2}[A(Z_1, Z_2) = 1] + \frac{1}{2} \Pr_{Z_2, X_1}[A(g(X_1), Z_2) = 1] .$$

Seega on A' eristab g väljundit edukusega:

$$\begin{aligned} \delta'(n) &= | \Pr_X[A'(g(X_2)) = 1] - \Pr_Z[A'(Z) = 1] | \\ &= \frac{1}{2} | \Pr[A(g(X_1), g(X_2)) = 1] - \Pr[A(Z_1, Z_2) = 1] | \\ &= \frac{\delta(n)}{2} . \end{aligned}$$