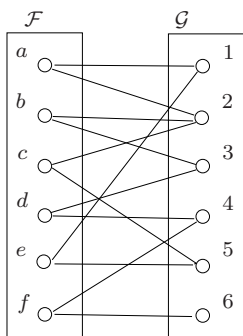


Ülesanded

I töö

Ü1.I-1. Kas järgneval graafil alustega \mathcal{F} ja \mathcal{G} on $(\frac{1}{3}, \frac{1}{3})$ -laiendus?



Ü1.I-2. Kas $n^4 = O(n^3 \log^2 n)$? Põhjenda!

II töö

Ü1.II-1. Juhuslike suuruste X (võimalike väärtustega $\{x_1, x_2, x_3, x_4\}$, kus $x_i = i$ iga $i = 1..4$ korral) ja Y (väärtustega $\{1, 2, 3, 4\}$) kohta on teada allolev tabel tõenäosustega $\Pr[i, j] = \Pr[X = i, Y = j]$, kusjuures tabel on mõnevõrra ebatäielik, sest kõrvaldiagonaali väärtused ei ole teada. Kas on võimalik täita kõrvaldiagonaal nii, et $\text{cov}(X, Y) = 0$? Kas on võimalik täitmine nii, et $\text{cov}(X, Y) \neq 0$?

	x_1	x_2	x_3	x_4
1	0.02	0.04	0.06	
2	0.01	0.02		0.04
3	0.04		0.12	0.16
4		0.06	0.09	0.12

Ü1.II-2. Olgu $g_1: \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ ja $g_2: \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ pseudojuhuarvude generaatorid, mis on defineeritud valemitega $g_1(X) = X \| Z \odot X$ ja $g_2(X) = X \| h(X)$, kus \odot tähistab skalaarkorrutist mooduliga 2 ja $h(X)$ tähistab 1-bittide arvu (n -bitises) argumendis X mooduliga 2. Kas g_1 ja g_2 on head pseudojuhuarvude generaatorid? Leida võimalikult efektiivsed eristavad vastased A_1 ja A_2 .

Lahendused

Ül.I-1. Graafil puudub $(\frac{1}{3}, \frac{1}{3})$ -laiendus, sest võttes näiteks $F = \{a, b\}$ (seega $\Pr[X \in F] = \frac{2}{6} = \frac{1}{3}$) saame, et $E(F) = \{1, 2, 3\}$, millest järeldub, et $\Pr[Y \in E(F)] = \frac{3}{6} = \frac{1}{2} < \frac{2}{3} = 1 - \frac{1}{3}$. Saime vastuolu laienduse tingimusega.

Ül.I-2. Õige vastus on $n^4 \neq O(n^3 \log^2 n)$, sest oletades vastupidist peak-sid leiduma konstandid c ja n_0 , nii et $n^4 \leq cn^3 \log^2 n$ (ehk $n \leq c \log^2 n$) iga $n > n_0$ korral. Kasutame matemaatilisest analüüsist teada fakti, et $\lim_{n \rightarrow \infty} \frac{\log^2 n}{n} = 0$, st iga $\epsilon > 0$ korral leidub N , nii et $\log^2 n/n < \epsilon$ iga $n > N$ korral. Võttes $\epsilon = \frac{1}{c}$ saame siit et iga c ja iga n_0 korral leidub $n > n_0$, nii et $\log^2 n/n < \frac{1}{c}$, st $n > c \log^2 n$, mis on vastuolus lausega $n = O(\log^2 n)$ (kui lause $n^4 \neq O(n^3 \log^2 n)$ järeldusega).

Ül.II-1. Tähistame $a = \Pr[X = x_1, Y = 4]$, $b = \Pr[X = x_2, Y = 3]$, $c = \Pr[X = x_3, Y = 2]$ ja $d = \Pr[X = x_4, Y = 1]$. Esitame tõenäosuste tabeli abstraktsel kujul:

	x_1	x_2	x_3	x_4
1	0.02	0.04	0.06	d
2	0.01	0.02	c	0.04
3	0.04	b	0.12	0.16
4	a	0.06	0.09	0.12

Selleks, et tabel esitaks tõenäosusi, peavad kehtima järgmised (tarvilikud ja piisavad!) tingimused:

$$a + b + c + d = 0.22$$

$$0 \leq a \leq 0.73$$

$$0 \leq b \leq 0.68$$

$$0 \leq c \leq 0.73$$

$$0 \leq d \leq 0.68$$

Lihtne on näha, et nende tingimuste süsteemil on lõpmata palju lahend-
deid, kusjuures lahendite hulk moodustab teatud 3-mõõtmelise piirkonna
4-mõõtmelises (a, b, c, d) -ruumis. Tähistame seda piirkonda \mathcal{P} .

Ülesande jõumeetodil lahendamiseks tuleks nüüd kovariatsioon

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

esitada polünoomina muutujatest b, c, d . Muutujat a ei ole vaja, sest esimese tingimuse tõttu on tema väärtus üheselt määratud muutujate b, c ja d väärtustega: $a = 0.22 - b - c - d$.

Avaldame kovariatsiooni definitsioonis esinevad keskvaartused, saame:

$$\begin{aligned} E[X] &= 2.4 + a + 2b + 3c + 4d \\ E[Y] &= 2.3 + d + 2c + 3b + 4a \\ E[XY] &= 7.03 + 4a + 6b + 6c + 4d \end{aligned}$$

Siit on lihtne näha, et $\text{cov}(X, Y)$ on 4 muutuja ruutpolünoom, mis ei võrdu samaselt nulliga. Seega järeldub siit sellise lahendi (a, b, c, d) olemasolu piirkonnas \mathcal{P} , mille korral $\text{cov}(X, Y) \neq 0$, sest iga polünoom, mis võrdub nulliga mingis mittetriviaalses ruumiosas (st mitteloenduv arvus punktides) on samaselt võrdne nulliga.

Nullkoha olemasolu piirkonnas \mathcal{P} saaks muidugi ka otsesel viisil tuletada kovariatsiooni üldavaldisest, kuid see oleks võrdlemisi töömahukas ülesanne. Kasutame siin asjaolu, et lihtsam on näidata, et sobivalt valitud (a, b, c, d) korral on X ja Y sõltumatud, millest tuleneb ka $\text{cov}(X, Y) = 0$.

Vaatleme esialgu suuruse d valikut. Selleks, et X ja Y oleksid sõltumatud peab kehtima $d = \Pr[X = x_4, Y = 1] = \Pr[X = x_4] \cdot \Pr[Y = 1] = (0.12 + d)(0.32 + d)$. Saadud ruutvõrrandil $d^2 - 0.56d + 0.0384$ on kaks lahendit: 0.48 ja 0.08. Esimene lahend ei sobi tingimuse $d \leq 0.22$ tõttu. Seega sõltumatuse eelduse korral peaks $d = 0.08$.

Toimides analoogiliselt suurusega c , saame c jaoks ruutvõrrandi $c^2 - 0.66c + 0.0189 = 0$, mille lahendid on 0.63 ja 0.03, millest vaid teine sobib tingimuse $c \leq 0.22$ tõttu. Seega $c = 0.03$.

Jääb üle teha sedasama suurusega b . Saame, et $b = 0.08$ ja seega $a = 0.22 - 0.08 - 0.03 - 0.08 = 0.03$. Seega saame järgmise tõenäosuste tabeli:

	x_1	x_2	x_3	x_4
1	0.02	0.04	0.06	0.08
2	0.01	0.02	0.03	0.04
3	0.04	0.08	0.12	0.16
4	0.03	0.06	0.09	0.12

Vahetu kontroll näitab, et antud tabeli põhjal on X ja Y tõepoolest sõltumatud, millest järeldub ka $\text{cov}(X, Y) = 0$.

Ü1.II-2. Generaatorit g_1 murdev vastane A_1 töötab järgmiselt. Sisendi $Y \in \{0, 1\}^{n+1} = Y' \| b$ korral väljastab 1 kui $Z \oplus Y' = b$ ja 0 vastupidisel

juhul. Kui sisend Y on ühtlaselt valitud juhuslik suurus $Z \leftarrow \{0, 1\}^{n+1}$, siis $\Pr[A_1(Z) = 1] = \frac{1}{2}$. Kui aga sisendiks on genetaarori g_1 väljund $g_1(X)$, siis $\Pr[A_1(g_1(X)) = 1] = 1$. Seega on vastase A_1 edukus

$$|\Pr[A_1(g_1(X)) = 1] - \Pr[A_1(Z) = 1]| = \frac{1}{2},$$

mis on väga suur (kaugel kaduvväiksest suurusel!). Seetõttu tuleb järeldada, et generaator g_1 on väga nõrk. Analoogilise arutelu saab läbi viia ka ganaraator g_2 korral.