

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. Leida juhuslike suuruste $X \in \{x_1, x_2, x_3\}$ ja suurus $Y \in \{y_1, y_2, y_3\}$ kovariatsioon $\text{cov}(X, Y)$, kui on teada allolev tabel tõenäosustega $\Pr[x_i, y_j] = \Pr[X = x_i, Y = y_j]$.

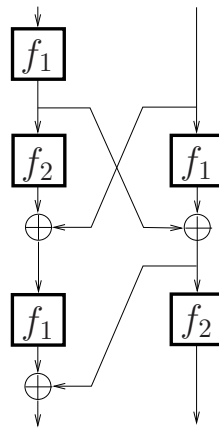
| | x_1 | x_2 | x_3 |
|-------|-------|-------|-------|
| y_1 | 0.01 | 0.03 | 0.06 |
| y_2 | 0.03 | 0.09 | 0.18 |
| y_3 | 0.06 | 0.18 | 0.36 |

Ü1.5. Olgu $K \leftarrow \{0, 1, \dots, 14\}$ ühtlase jaotusega juhuslik suurus. Suuruse K abil defineerime juhuslikud suurused:

$$\begin{aligned} X &= K \bmod 4 \in \{0, 1, \dots, 3\}, \\ Y &= K \bmod 8 \in \{0, 1, \dots, 7\}, \\ Z &= (K \bmod 3, K \bmod 5) \in \{0, \dots, 2\} \times \{0, \dots, 4\} . \end{aligned}$$

Leia tingimuslik kovariatsioon $\text{cov}(X, Y \mid Z)$.

Ü1.6. Olgu f_1 ja f_2 juhuslikud funktsioonid tüüpi $\{0, 1\}^n \rightarrow \{0, 1\}^n$. Näita, et järgneval joonisel kujutatud funktsioon $F^{f_1 f_2}: \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$ ei ole pseudojuhuslik.



Ü1.7. Olgu Z ühtlase jaotusega juhuslik suurus väärtustega $\{0, \dots, 10\}$ ja X ühtlase jaotusega juhuslik suurus väärtustega $\{0, \dots, 7\}$. Juhuslik suurus Y arvutatakse suurusest X funktsiooni

$$Y = g(X) = 16 \cdot X \bmod 11$$

järgi. Kas leidub algoritm A , mis eristab suurusi Z ja Y edukusega

$$\delta = |\Pr[A(g(X)) = 1] - \Pr[A(Z) = 1]| \geq 0.4 ?$$

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 arvutatud 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. Lihtne on veenduda, et X ja Y on sõltumatud, st $\Pr[X = x_i, Y = y_j] = \Pr[X = x_i] \cdot \Pr[Y = y_j]$. Seetõttu $\text{cov}(X, Y) = 0$.

Ü1.5. Kerge on näha, et kui suuruse Z väärtus on teada, siis on üheselt teada K väärtus ja seega ka suuruste X ja Y väärtus, mistõttu

$$\text{cov}(X, Y \mid Z) = 0 .$$

Ü1.6. Joonisel toodud konstruktsioon:

$$F^{f_1 f_2}(x, y) = (f_1(y \oplus f_2 f_1(x)) \oplus f_1(x) \oplus f_1(y), f_2(f_1(x) \oplus f_1(y)))$$

ei ole pseudojuhuslik, sest

$$F^{f_1 f_2}(x, x) = (f_1(x \oplus f_2 f_1(x)), f_2(0))$$

ja seega arvutades F väärtuse kahe sisendi (x_1, x_1) ja (x_2, x_2) (kus $x_1 \neq x_2$) korral saame, et F väljundi teine komponent jääb samaks tõenäosusega 1. Täiesti juhusliku funktsiooni korral oleks see tõenäosus aga 2^{-n} .

Ül.7. Teame, et iga eristusalgoritmi A korral kehtib

$$| \Pr[A(g(X)) = 1] - \Pr[A(Z) = 1] | \leq \partial(\mathcal{D}_1, \mathcal{D}_2) .$$

Arvutus näitab, et

$$\partial(\mathcal{D}_1, \mathcal{D}_2) = \frac{1}{2} \sum_y | \Pr[g(X) = y] - \Pr[Z = y] | = \frac{3}{11} < 0.4 ,$$

ja seega võib järeldada, et nimetatud omadustega algoritmi A ei eksisteeri.