

Ülesanded

Ül.1.(40p) Olgu $K \leftarrow \{0, 1, \dots, 14\}$ ühtlase jaotusega juhuslik suurus. Suuruse K abil defineerime juhuslikud suurused:

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

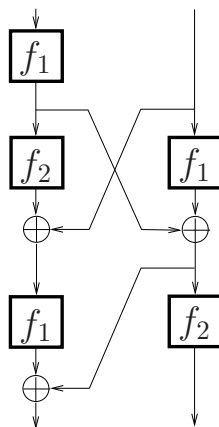
Leia tingimuslik kovariatsioon $\text{cov}(X, Y \mid Z)$.

Ül.2.(40p) Olgu $A \leftarrow \{0, \dots, 5\}$ ja $B \leftarrow \{0, \dots, 5\}$ sõltumatud ühtlase jaotusega juhuslikud suurused. Kas suurused

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

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

Ül.3.(40p) 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.



Lahendused

Ül.1. 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

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

Ül.2. 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.3. 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 pseudojhuslik, 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 jhusliku funktsiooni korral oleks see tõenäosus aga 2^{-n} .