

Valik ülesandeid aines “Sissejuhatus andmeturbesse”

29.märts, 2005

1 Ülesanded

Ülesanne 1. Olgu meil jadasiffer, mis algvõtmest $K = K_0 \dots K_5 \in \{0, 1\}^6$ genereerib võtmejada $z_0 z_1 z_2 \dots z_n \dots$, mis on genereeritud järgmiselt:

$$\begin{aligned}z_0 &= K_0 \\z_1 &= K_1 \\z_2 &= K_2 \\z_{k+1} &= K_5 \cdot z_k + K_4 \cdot z_{k-1} + K_3 \cdot z_{k-2} \pmod{2} \quad (\text{kui } k > 2) .\end{aligned}$$

Krüpteerimine toimub eeskirja $y_i = x_i \oplus z_i$ järgi, kus \oplus tähistab liitmist mooduliga 2. On teada, et $Y = y_3 y_4 \dots y_8 = 010110$ ja $X = x_3 x_4 \dots x_8 = 101111$. Leia algvõti $K = K_0 K_1 \dots K_5$.

Ülesanne 2. Olgu X juhuslik suurus väärtuste hulgaga $\{x_1, \dots, x_n\}$ ja vastavate tõenäosustega p_1, \dots, p_n , kus $p_i = \mathbf{P}[X = x_i]$. Nimetame suuruse X *ennustajaks* mis tahes algoritmi \mathbf{E} , mis sisendi $(x_1, \dots, x_n; p_1, \dots, p_n)$ korral väljastab elemendi $\tilde{x} \in \{x_1, \dots, x_n\}$. Märgime, et \mathbf{E} võib kasutada oma töös ka juhuarve. Ennustaja eesmärgiks on ennustada juhusliku suuruse X väärtus x , mis saadakse eelnevatest katsetest sõltumatu katses $x \leftarrow X$. Ennustaja \mathbf{E} *edukuseks* suuruse X ennustamisel nimetatakse tõenäosust

$$\delta = \delta(\mathbf{E}, X) = \mathbf{P}[x = \tilde{x}]$$

eeldusel, et $x \leftarrow X$ ja $\tilde{x} \leftarrow \mathbf{E}(x_1, \dots, x_n; p_1, \dots, p_n)$ on sõltumatud katsed. Suuruse X *ennustatavuseks* $\Delta(X)$ nimetatakse edukuse δ maksimumi (üle

kõikvõimalike algoritmide \mathbf{E}). Ekvivalentne oleks defineerida $\Delta(X)$ kui δ väärtus *parima ennustaja* \mathbf{E} korral.

Millise väljundjaotusega \tilde{X} on parim ennustaja? Leia lõplikud juhuslikud suurused X ja Y , nii et $H[X] < H[Y]$, kuid Y on paremini ennustatav kui X , st $\Delta(Y) > \Delta(X)$.

2 Lahendused

Ülesanne 1. Esmalt leiame vastava võtmejada lõigu $Z = z_3 z_4 \dots z_8 = X \oplus Y = 010110 \oplus 101111 = 111001$, st $z_3 = z_4 = z_5 = z_8 = 1$ ja $z_6 = z_7 = 0$. See teadmine võimaldab välja kirjutada võrrandisüsteemi võtmete K_3 , K_4 ja K_5 leidmiseks:

$$\begin{cases} z_7 \cdot K_5 + z_6 \cdot K_4 + z_5 \cdot K_3 = z_8 \\ z_6 \cdot K_5 + z_5 \cdot K_4 + z_4 \cdot K_3 = z_7 \\ z_5 \cdot K_5 + z_4 \cdot K_4 + z_3 \cdot K_3 = z_6 \end{cases} \sim \begin{cases} 0 \cdot K_5 + 0 \cdot K_4 + 1 \cdot K_3 = 1 \\ 0 \cdot K_5 + 1 \cdot K_4 + 1 \cdot K_3 = 0 \\ 1 \cdot K_5 + 1 \cdot K_4 + 1 \cdot K_3 = 0 \end{cases},$$

mida lahendades saame $K_3 = 1$, $K_4 = 1$ ja $K_5 = 0$. Edasi saab aga tuletada võrrandisüsteemi K_0 , K_1 ja K_2 leidmiseks:

$$\begin{cases} z_4 \cdot K_5 + z_3 \cdot K_4 + z_2 \cdot K_3 = z_5 \\ z_3 \cdot K_5 + z_2 \cdot K_4 + z_1 \cdot K_3 = z_4 \\ z_2 \cdot K_5 + z_1 \cdot K_4 + z_0 \cdot K_3 = z_3 \end{cases} \sim \begin{cases} 1 \cdot 0 + 1 \cdot 1 + K_2 \cdot 1 = 1 \\ 1 \cdot 0 + K_2 \cdot 1 + K_1 \cdot 1 = 1 \\ K_2 \cdot 0 + K_1 \cdot 1 + K_0 \cdot 1 = 1 \end{cases},$$

mille ainus lahend on $K_0 = 0$, $K_1 = 1$ ja $K_2 = 0$. Seega $K = K_0 \dots K_6 = 0101110$.

Ülesanne 2. Parim ennustaja \mathbf{E}_{\max} töötab järgmiselt:

- Leia (minimaalne) m nii et $p_m = \max\{p_1, \dots, p_n\}$.
- Väljasta x_m .

Ennustaja \mathbf{E}_{\max} väljundjaotust \tilde{X} iseloomustavad võrdused

$$\tilde{p}_i = P[\tilde{X} = x_i] = \begin{cases} 1 & \text{kui } i = m \\ 0 & \text{kui } i \neq m \end{cases}.$$

On selge, et selle ennustaja edukus on p_m . Tõestamiseks, et \mathbf{E}_{\max} on tõepoolest *parim* ennustaja, paneme esmalt tähele, et kui $\{\tilde{p}_1, \dots, \tilde{p}_n\}$ on mingi (mitte tingimata parima) ennustaja väljundjaotus, siis

$$\delta(\mathbf{E}, X) = p_1 \tilde{p}_1 + p_2 \tilde{p}_2 + \dots + p_n \tilde{p}_n.$$

Kasutame induktsiooni n järgi, näidates et $\delta(\mathbf{E}, X) \leq \max\{p_1, \dots, p_n\}$ iga n korral. Lihtsuse mõttes eeldame, et $p_n \geq p_{n-1} \geq \dots \geq p_1$ ja seega $\max\{p_1, \dots, p_n\} = p_n$.

On selge, et teoreemi väide kehtib $n = 1$ korral, sest siis on tõenäosusruum $\{\tilde{p}_1, \dots, \tilde{p}_n\}$ triviaalne. Induktsioonisammu tõestamiseks eeldame, et võrratus

$$p_1q_1 + p_2q_2 + \dots + p_{n-1}q_{n-1} \leq p_{n-1}$$

kehtib iga tõenäosusjaotuse $\{q_1, \dots, q_{n-1}\}$ korral (seejuures $p_{n-1} \geq \dots \geq p_1$ võivad olla suvalised positiivsed reaalarvud) ja näitame, et siis kehtib ka võrratus

$$p_1\tilde{p}_1 + p_2\tilde{p}_2 + \dots + p_n\tilde{p}_n \leq p_n \quad (1)$$

iga tõenäosusjaotuse $\{\tilde{p}_1, \dots, \tilde{p}_n\}$ korral (ja suvaliste reaalarvude $p_n \geq \dots \geq p_1$ korral).

Olgu $\tilde{X}: \tilde{p}_1, \dots, \tilde{p}_n$ mingi tõenäosusjaotus. Defineerime uue tõenäosusjaotuse $Y: q_1, \dots, q_{n-1}$ järgmiselt:

$$q_i = \frac{\tilde{p}_i}{1 - \tilde{p}_n}.$$

On selge, et $\sum_i q_i = 1$, mistõttu Y on tõepoolest tõenäosusjaotus. Seega, vastavalt induktsiooni eeldusele:

$$p_1q_1 + p_2q_2 + \dots + p_{n-1}q_{n-1} \leq p_{n-1} \leq p_n .$$

Korrutades võrratuse mõlemat poolt suurusega $1 - \tilde{p}_n$, saame

$$p_1\tilde{p}_1 + p_2\tilde{p}_2 + \dots + p_{n-1}\tilde{p}_{n-1} \leq p_n - p_n\tilde{p}_n,$$

millest aga tulenebki võrratus (1). Järelikult tõepoolest iga juhusliku suuruse X korral $\Delta(X) = \max\{p_1, \dots, p_n\}$.

Kui võtta juhuslikud suurused jaotustega $X: \frac{1}{3}, \frac{1}{3}, \frac{1}{3}$ ja $Y: \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{2}$. Saame, et

$$\begin{aligned} \Delta(X) &= \frac{1}{3} < \frac{1}{2} = \Delta(Y) \\ \mathbf{H}[Y] &= 2 > \log_2 3 = \mathbf{H}[X] . \end{aligned}$$