

Järeltöö aines “Sissejuhatus andmeturbesse”

12.mai, 2004

Ülesanne 1. Juhuslikule suurusele X väärtuste hulgaga $\{x_1, \dots, x_m\}$ ja vastavate tõenäosustega p_1, \dots, p_m (kus $p_i \neq 0$) on konstrueeritud prefiksivaba kood (w_1, \dots, w_m) , kusjuures koodi keskmine pikkus $\sum_i p_i \cdot \|w_i\|$ langeb kokku suuruse X Shannoni entroopiaga $H[X]$. Tõesta, et iga $i \in \{1, \dots, m\}$ korral leidub naturaalarv $n_i \in \mathbb{N}$, nii et $p_i = 2^{-n_i}$.

Ülesanne 2. Arv x valitakse ühtlaselt ja juhuslikult hulgast $\{0, \dots, 149\}$. Kui suur on tõenäosus, et $\text{süt}(x, 12) = 1 = \text{süt}(25)$?

Ülesanne 3. Leia järgmise kongruentside süsteemi kõik lahendid (a, b) , kus $a, b \in \{0, \dots, 35\}$:

$$\begin{cases} 5a + b \equiv 10 \pmod{36} \\ 8a + b \equiv 13 \pmod{36} \end{cases}$$

Lahendus 1. Teisendame koodi keskmise pikkuse avaldist järgmisel viisil:

$$\sum_i p_i \cdot \|w_i\| = \sum_i p_i \cdot \log_2 2^{\|w_i\|} = \sum_i p_i \cdot \log_2 \frac{1}{2^{-\|w_i\|}}.$$

Seega, vastavalt eeldustele:

$$\sum_i p_i \cdot \|w_i\| - \mathbf{H}[X] = \sum_i p_i \cdot (\log_2 \frac{1}{2^{-\|w_i\|}} + \log_2 p_i) = \sum_i p_i \cdot \log_2 \frac{p_i}{2^{-\|w_i\|}} = 0.$$

Et Krafti võrratuse tõttu $\sum_i 2^{-\|w_i\|} \leq 1$, siis kujutab viimane võrdus endast Kullback-Liebleri võrratuse erijuhtu – täpselt võrdust. See aga saab võimalik olla vaid siis, kui iga i korral $p_i = 2^{-\|w_i\|}$.

Lahendus 2. Et tingimus $\text{süt}(x, 12) = 1$ on samaväärne tingimusega

$$\text{süt}(x, 6) = 1$$

ja $150 = 6 \cdot 25$, siis liittingimus $\text{süt}(x, 12) = 1 = \text{süt}(x, 25) = 1$ on samaväärne tingimusega $\text{süt}(x, 150) = 1$. Selliseid arve x on aga hulgas $\{0, \dots, 149\}$ täpselt $\phi(150) = \phi(2) \cdot \phi(3) \cdot \phi(5^2) = 2 \cdot (25 - 5) = 40$ tükki, millest järeldub, et otsitav tõenäosus on $\frac{40}{150} = \frac{4}{15}$.

Lahendus 3. Lahutades alumisest võrrandist ülemise, saame kongruentsi

$$3a \equiv 3 \pmod{36},$$

millel on täpselt kolm lahendit: $a = 1$, $a = 13$ ja $a = 25$. Põhjenduseks märgime, et kui a on mingi lahend, siis $a + k$ on lahend parajasti siis kui $3k \equiv 0$, st $3k = \ell \cdot 36$ mingi $\ell \in \mathbb{N}$ korral, st kui $k = 12 \cdot \ell$. Et $a = 1$ on ilmselt lahend, siis võttes $k = 0, 1, 2$ saame kõik kolm mainitud lahendit kõik ülejäänud k väärtused ainult kordavad eelnevaid lahendeid. Leides igale a väärtusele vastava b väärtuse, saame $b = 5$, $b = 17$ ja $b = 29$.