

Kontrolltöö aines “Sissejuhatus andmeturbesse”

21.aprill, 2004

Ülesanne 1. Kas leidub prefiksivaba kood (w_1, \dots, w_7) , nii et $\|w_1\| = \|w_2\| = 2$ ja $\|w_3\| = \|w_4\| = \|w_5\| = \|w_6\| = \|w_7\| = 3$? Põhjenda vastust!

Ülesanne 2. Lahenda kongruentside süsteemid:

$$(a) \begin{cases} 5a + b \equiv 12 \pmod{36} \\ 8a + b \equiv 13 \pmod{36} \end{cases} \quad (b) \begin{cases} 2a + b \equiv 5 \pmod{31} \\ 7a + b \equiv 9 \pmod{31} \end{cases}$$

Ülesanne 3. Leia Huffmani puu ja vastavad koodid järgmisele juhuslikule suurusele X väärtuste hulgaga $\{x_1, \dots, x_6\}$ ja tõenäosustega

$$p_1 = p_2 = 0.25, p_3 = p_4 = p_5 = p_6 = 0.125.$$

Leia keskmine koodi pikkus ℓ ja Shannoni entroopia $H[X]$.

Ülesanne 4. Arv x valitakse juhuslikult (ühtlase jaotusega) hulgast $X = \{0, \dots, 75\}$. Kui suur on tõenäosus, et leiduvad täisarvud α ja β (võivad ka negatiivsed olla), nii et

$$\alpha \cdot x + \beta \cdot 76 = 1.$$

Ülesanne 5. On teada järgmine neljandat järku nihkeregistri (liik teadmata!) poolt moodustatud väljundjada (nullise sisendi korral), milles üks bitt on kustunud (asendatud tärniga):

$$0 \ 1 \ 1 \ * \ 1 \ 1 \ 0 \ 1$$

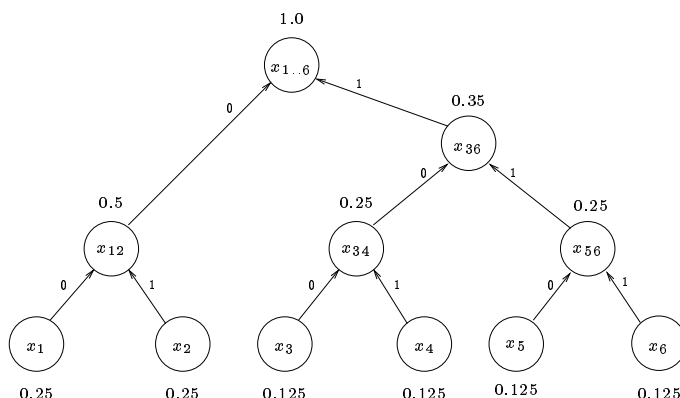
Taasta kustunud bitt ja põhjenda vastust!

Lahendus 1. Iga prefiksivaba kood (w_1, \dots, w_7) peab rahuldama Krafti võrratust $\sum_i 2^{-\|w_i\|} \leq 1$. Antud koodi korral aga see võrratus ei kehti, sest $\sum_i 2^{-\|w_i\|} = 2 \cdot 2^{-2} + 5 \cdot 2^{-3} > 1$. Järelikult sellist prefiksivaba koodi ei leidu.

Lahendus 2. Esimesel süsteemil lahend puudub. Lahutades teisest võrrandist esimese, saame $3a \equiv 1 \pmod{36}$, mis on võimatu, sest 36 jagub 3-ga ja seetõttu puudub jäägil 3 pöördelement arvuvallas \mathbb{Z}_{36} .

Teise süsteemi korrektne lahend on $a = 7$ ja $b = 22$. Lahutame teisest võrrandist esimese ja saame $5a \equiv 4 \pmod{31}$. Et 31 on algarv, siis leidub jäägil 5 ka pöördelement, milleks on $-6 \equiv 25$, sest $31 - 6 \cdot 5 = 1$. Seega $a \equiv 4 \cdot (-6) \equiv -24 \equiv 7 \pmod{31}$. Asendades $a = 7$ esimesse võrrandisse, saame $b \equiv 5 - 2 \cdot 7 \equiv -9 \equiv 22 \pmod{31}$.

Lahendus 3. Huffmani puu tuleb järgmine (see ei ole ainuvõimalik kuju!):



ja vastavad koodid 00, 01, 100, 101, 110, 111. Koodi keskmine pikkus tuleb $\ell = 2 \cdot 0.25 \cdot 2 + 4 \cdot 0.125 \cdot 3 = 2.5$ ja Shannoni entroopia

$$H[X] = 2 \cdot 0.25 \cdot \log_2 \frac{1}{0.25} + 4 \cdot 0.125 \cdot \log_2 \frac{1}{0.125} = 2.5.$$

Lahendus 4. Nimetatud α ja β leiduvad mingi $x \in \{1, \dots, 75\}$ korral parajasti siis, kui $\text{süt}(x, 76) = 1$. Et selliseid elemente x on parasjagu $\phi(76) = \phi(4 \cdot 19) = (4 - 2) \cdot (19 - 1) = 36$, siis otsitav tõenäosus on $\frac{\phi(76)}{76} = \frac{36}{76} = \frac{9}{19}$.

Lahendus 5. Kustunud bitt oli 0. Vastasel korral oleks väljundjadas järjest 5 ühte. Et aga registri järk on 4 ja sisendis on nullid, siis peaksid väljundjadas viiele ühele järgnema kõik ühed. Allesjäänud bittidest selgub, et nii see pole.