

## Ülesanded

**Ülesanne I-1 (50 punkti)** Olgu meil juhuslik suurus  $X$  võimalike väärtustega  $\{x_1, x_2, \dots, x_7\}$ , mille tõenäosused on vastavalt:

$$p(x_1) = p(x_2) = \frac{1}{16}, p(x_3) = p(x_5) = p(x_6) = \frac{1}{8}, p(x_4) = p(x_7) = \frac{1}{4} .$$

Leia kombinatoorne entroopia  $H_{\text{comb}}[X]$  ja Shannoni entroopia  $H[X]$ .

**Ülesanne I-2 (50 punkti)** Olgu  $X$  ja  $Y$  juhuslikud suurused vastavalt väärtuste hulkadega  $\{x_1, x_2, x_3\}$  ja  $\{y_1, y_2, y_3\}$ . Nende suuruste kohta on teada tõenäosuste  $p(x_i, y_j) = p(X = x_i, Y = y_j)$  väärtused, mis on esitatud järgnevas tabelis:

$p(x_i, y_j)$	$y_1$	$y_2$	$y_3$
$x_1$	0.06	0.21	0.03
$x_2$	0.04	0.14	0.02
$x_3$	0.10	0.35	0.05

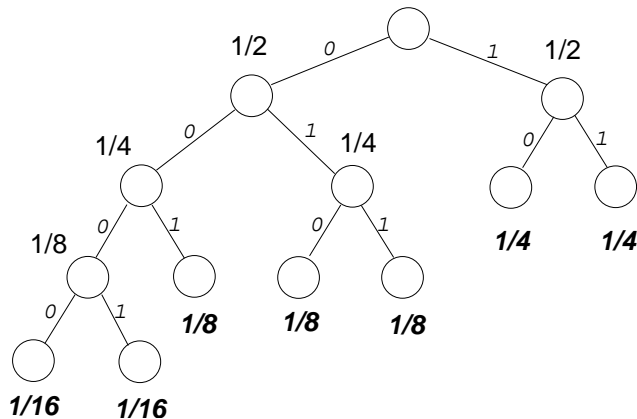
Leia  $H[X | Y] - H[X]$ .

**Ülesanne 1 (60 punkti).** Mitu kuupjuurt on elemendil  $a \neq 0$  ringis  $\mathbb{Z}_{60829}$ ? Põhjenda vastust.

**Ülesanne 2 (40 punkti).** RSA moodul on  $n = 1199021$ . On teada, et  $598963^2 \equiv 1 \pmod{n}$ . Tegurda selle teadmise abil moodul  $n$ .

## Lahendused

**Ülesanne I-1.** Kombinatoorse entroopia leiame kui Huffmani puu:



lehtede kaalutud keskmise kõrguse, st:

$$H_{\text{comb}}[X] = 2 \cdot \frac{4}{16} + 3 \cdot \frac{3}{8} + 2 \cdot \frac{2}{4} = 2.625 .$$

Shannoni entroopia tuleb  $H[X] = 3 \cdot \frac{\log_2 16}{16} + 3 \cdot \frac{\log_2 8}{8} + 2 \cdot \frac{\log_2 4}{4} = 2.625$ .

**Ülesanne I-2.** Arvutades tabelist tõenäosused:

$$p(x_1) = 0.06 + 0.21 + 0.03 = 0.3$$

$$p(x_2) = 0.04 + 0.14 + 0.02 = 0.2$$

$$p(x_3) = 0.10 + 0.35 + 0.05 = 0.5$$

$$p(y_1) = 0.06 + 0.04 + 0.10 = 0.2$$

$$p(y_2) = 0.21 + 0.14 + 0.35 = 0.7$$

$$p(y_3) = 0.03 + 0.02 + 0.05 = 0.1$$

märkame et iga  $i, j = 1..3$  korral kehtib seos  $p(x_i, y_j) = p(x_i) \cdot p(y_j)$ , millest järeldub et suurused  $X$  ja  $Y$  on *sõltumatud* ja seega  $H[X] = H[X | Y]$  ja seega  $H[X | Y] - H[X] = 0$ .

**Ülesanne II-1.** Kuupjuure leidmine elemendile  $a \neq 0$  ringis  $\mathbb{Z}_{60829}$  tähendab võrrandi  $x^3 \equiv a \pmod{60829}$  lahendite arvu leidmist. Et võrrand meenutab

RSA algoritmiga krüpteerimist (standardse astendajaga 3), siis esimene loomulik hüpotees võiks olla see, et arv  $n = 60829$  on kahe algarvu  $p$  ja  $q$  korrutis. Tõepoolest, proovides jagada arvu  $n$  esimeste algarvudega

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59...

märkame, et meie hüpotees peab paika:  $60829 = 59 \cdot 1031$ . Seega  $\phi(n) = (p-1)(q-1) = 58 \cdot 1030 = 59740$  ja kuna  $(3, 59740)$  siis on 3 pööratav element mooduli  $\phi(n)$  järgi. Seega leidub astendaja  $d$ , nii et iga  $x \in \mathbb{Z}_{60829}$  korral kehtib  $(x^3)^d \pmod{60829} = 1$ . Seega on kuupfunktsioon antud tingimustel pööratav ja järelikult on igal arvul  $a \in \mathbb{Z}_{60829}$  täpselt üks kuupjuur.

**Ülesanne II-2.** Mooduli  $n = 1199021$  proovimise teel tegurdamine on ilmselt liiga töömahukas. Teisendame kongruentsi  $598963^2 \equiv 1 \pmod{n}$  järgmisele kujule:

$$598963^2 - 1 \equiv (598963 - 1) \cdot (598963 + 1) \equiv 598962 \cdot 598964 \equiv 0 \pmod{n}.$$

Eeldades, et  $n = pq$ , kus  $p$  ja  $q$  on algarvud, saame et korrutis  $598962 \cdot 598964$  jagub  $n$ -ga kuid kumbki teguritest  $n$ -ga jaguda ei saa sest nad on  $n$ -st rangelt väiksemad. Seega jagub üks tegureist arvuga  $p$  ja teine neist arvuga  $q$ . Seega saame otsitava teguri kätte, kui arvutame suurima ühisteguri:

$$(598962, 1199021) = 1097,$$

mis on algarv. Kontroll näitabki, et  $1199021 = 1097 \cdot 1093$ .