

## KOODAUSTEORIA

kesätentti 21.6.2010

1. Koodataan viesti  $\mathbf{m} = x_1x_2x_3 \in \mathbb{F}_2^3$  koodisanaksi  $\mathbf{c} = x_1x_2x_3x_4x_5x_6 \in \mathbb{F}_2^6$ , missä  $x_4 = x_1 + x_2 + x_3$ ,  $x_5 = x_1 + x_3$  ja  $x_6 = x_2 + x_3$ . Osoita, että näin saatu koodi  $C$  on lineaarinen. Määrää koodin  $C$  generoijamatriisi ja minimietäisyys.
2. Määrittele alkion  $\alpha \in \mathbb{F}_q$  minimipolynomi  $m_\alpha(x)$  kunnan  $\mathbb{F}_q$  suhteen. Osoita seuraavat tulokset:
  - a)  $m_\alpha(x)$  on jaoton,
  - b) jos  $f \in \mathbb{F}_q[x]$  ja  $f(\alpha) = 0$ , niin  $m_\alpha \mid f$ .

3. Määrittele kunnan  $\mathbb{F}_q$ ,  $q = p^m$ , kanoninen additiivinen karakteri  $\chi$ . Osoita, että

$$\sum_{x \in \mathbb{F}_q} \chi(ax) = 0, \quad \text{kun } a \neq 0.$$

Olkkoon lopuksi  $p = 2$ ,  $m = 3$  ja  $\alpha \in \mathbb{F}_8$ ,  $\alpha^3 + \alpha + 1 = 0$ . Laske  $\chi(1 + \alpha^2)$ .

4. Määrittele syklinen koodi.

Olkkoon  $\mathbb{F}_q$  äärellinen kunta ja  $n \in \mathbb{Z}_+$  ehdon  $\text{synt}(n, q) = 1$  toteuttava kokonaisluku. Osoita, että renkaan  $R_n = \mathbb{F}_q[x]/\langle x^n - 1 \rangle$  ideaali  $I$  on syklinen koodi.

Osoita edelleen, että jos  $g(x) \mid (x^n - 1)$  renkaassa  $\mathbb{F}_q[x]$  ja  $\deg g = n - k$ , niin koodin  $\langle g(x) \rangle$  pituus on  $n$  ja dimensio  $k$ .

5. Käytetään [7, 3, 5]-RS-koodia ja kunnan  $\mathbb{F}_8$  primitiivialkiota  $\alpha$ , jolle  $\alpha^3 + \alpha + 1 = 0$ . Dekoodaa saatu sana

$$\mathbf{u} = (\alpha, 1, 0, 0, *, \alpha, 1),$$

missä  $*$  tarkoittaa pyyhkiytymää.