Teorija kodiranja – 2. domača naloga

(do petka 5. apr. 2002)

---

1. Naj bo C $[n, M]$-koda z razdaljo d nad abecedo velikosti q in naj bo $e = \lfloor (d-1)/2 \rfloor$.

   (a) Dokaži $M \sum_{i=0}^{e} \binom{n}{i} (q-1)^i \leq q^n$.

   (b) Dakaži $M \leq q^{n-d+1}$.

   (c) Konstruiraj $[8, 4]$-kodo z razdaljo 5 ali pa dokaži, da taka koda ne obstaja.

   (d) Konstruiraj binarno $[8, 8]$-kodo z razdaljo 5 ali pa dokaži, da taka koda ne obstaja.

2. Polinom $f(x) = x^4 + 3x^3 + 5$ je nerazcepen nad $\mathbb{Z}_7$.

   (a) Koliko elementov ima končni obseg $F = \mathbb{Z}_7[x]/(f(x))$?

   (b) Opiši z besedami elemente končnega obsega F.

   (c) Koliko je karakteristika obsega F?

   (d) V končnem obsegu F izračunaj:

   $$(5x^3 + 3x^2 + 6) \ + \ (6x^2 + 6).$$

   (e) Uporabi razširjen Evclidov algoritem za polimone za iskanje (multiplikativnega) inverza elementa $a = 5x^3 + 2x^2 + 3$.

   (f) V končnem obsegu F izračunaj:

   $$(x+1)^7 \cdot (4x^3 + 5x^2 + 6x + 4)^{2400}.$$

3. Naj bo $\alpha \in GF(q)^*$.

   (a) Dokaži, da je α^{-1} natanko določen.

   (b) Dokaži, da je $\alpha^{-1} = \alpha^{q-2}$.
   (Zgornja zveza nam da alternativni algoritem za računanje multiplikativnih inverzov v končnih obsegih).

   (c) Dokaži $\mathrm{red}(\alpha) = \mathrm{red}(\alpha^{-1})$.

4. Naj bo $\alpha \in GF(q)^*$ in $\mathrm{red}(\alpha) = t$.

   (a) Dokaži, da so elementi $\alpha^0, \alpha^1, \ldots, \alpha^{t-1}$ paroma različni.

   (b) Naj bo s celo število. Dokaži, da je $\alpha^s = 1$ samo in samo če t deli s.

5. Najdi nerazcepen polinom stopnje 5 nad $\mathbb{Z}_3$.