2. kolokvij iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 4. junij 2013

1. ($4 + 8 + 3 + 5 = 20$ točk) Linearen $[n, k, d]$-kod $\mathcal{C}_1$ nad GF(5) je podan z nadzorno matriko

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 4 & 3 & 2 & 1 \end{bmatrix}.$$

   (a) Poiščite parametre $[n, k, d]$ za kod $\mathcal{C}_1$. Koliko napak lahko popravi kod $\mathcal{C}_1$?

   (b) Ali je kod $\mathcal{C}_1$ popoln?

   (c) S pomočjo sindromov dekodirajte prejeto besedo $y = 101131$ in poiščite pripadajoče sporočilo.

   (d) Kodne besede pošiljamo po dvojiškem simetričnem kanalu z verjetnostjo napake $p = 0.1$. Kolikšna je verjetnost, da bo prejeta beseda pravilno odkodirana? Kolikšna je verjetnost, da prejete besede ne bomo znali odkodirati (čeprav nepravilno)? Pri dekodiranju uporabimo pravilo najbližjega soseda.

2. ($4+3+3+5+5 = 20$ točk) Kod $\mathcal{C}_2$ nad obsegom GF(2) vsebuje vse ciklične pomike besede 10101 in ničelno besedo.

   (a) Poiščite parametre (n, M, d) za kod $\mathcal{C}_2$.

   (b) Ali je kod $\mathcal{C}_2$ linearen?

   (c) Ali je kod $\mathcal{C}_2$ cikličen?

   (d) Poiščite najmanjši cikličen kod, ki vsebuje kod $\mathcal{C}_2$.

   (e) Poiščite najmanjši linearen kod, ki vsebuje kod $\mathcal{C}_2$ (lahko ga podate z generatorsko ali nadzorno matriko). Kakšni so njegovi parametri?

   Opomba: nad GF(2) je faktorizacija x^5-1 enaka $x^5-1 = (x+1)(x^4+x^3+x^2+x+1)$.

Odgovore na vsa vprašanja je potrebno utemeljiti!