2. kolokvij iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 4. junij 2010

1. (10 točk) Sporočila pošiljamo po dvojiškem simetričnem kanalu, kjer se poleg napak pojavljajo tudi *izbrisi*, torej na nekaterih mestih v prejeti besedi simbolov ne moremo prebrati.

   (a) Kaj pomeni, da bločni kod popravi besedo, pri kateri je prišlo do natančno u izbrisov? Kaj pomeni, da bločni kod popravi u izbrisov? Napišite smiselni definiciji.

   (b) Naj bo $\mathcal{C}$ linearen kod z minimalno razdaljo d. Pokažite, da lahko kod $\mathcal{C}$ popravi $d-1$ izbrisov.

2. (15 točk) Linearen $[n,k,d]$-kod $\mathcal{C}_1$ nad GF(5) z M besedami je podan z generatorsko matriko

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

   Poiščite nadzorno matriko za kod $\mathcal{C}_1$. Poiščite parametre n, k, d in M ter pokažite, da je kod popoln.

3. (15 točk) Linearen $[n,k,d]$-kod $\mathcal{C}_2$ nad GF(2) je podan z nadzorno matriko

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

   Koliko napak in koliko izbrisov lahko popravi kod $\mathcal{C}_2$? Če se da, dekodirajte prejete besede $y_1 = 011111$, $y_2 = 111111$, $y_3 = 1\_01\_1$ in poiščite pripadajoča sporočila.

4. (10 točk) Poiščite generatorski polinom za najmanjši ciklični kod nad GF(2), ki vsebuje besedo 0101100. Kolikšna je dimenzija tega koda?

   Opomba: v GF(2) je $x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3)$.

Odgovore na vsa vprašanja je potrebno utemeljiti!