2. kolokvij iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 5. junij 2012

1. Po dvojiškem simetričnem kanalu z verjetnostjo napake $p = 0.1$ želimo pošiljati sporočila dolžine k. Ker je verjetnost napake precej velika, pred pošiljanjem sporočilo zakodiramo - uporabimo kod za popravljanje napak s ponavljanjem. Torej vsak bit sporočila ponovimo r-krat za dani r. Prejeto besedo dekodiramo po pravilu najbližjega soseda (uporabimo večinsko pravilo).

   Za dani k označimo z $r(k)$ najmanjšo vrednost r, pri kateri je pri uporabi koda s ponavljanjem, ki vsak bit sporočila ponovi r-krat, verjetnost, da pravilno dekodiramo (celotno) sporočilo, vsaj 0.99.

   (a) Kolikšna je verjetnost, da pravilno dekodiramo besedo, pri kateri vsak bit sporočila ponovimo trikrat za dolžino sporočila $k = 2$?

   (b) Določite $r(1)$ in $r(2)$.

   (c) (dodatna naloga) Pokažite, da je $r(k)$ nepadajoča funkcija k.

2. Linearni $[n, k, d]$-kod $\mathcal{C}$ nad GF(2) je podan z generatorsko matriko

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

   (a) Poiščite parametre koda n, k in d. Koliko napak popravi?

   (b) Prejeli smo besede $y_1 = 0000011111$, $y_2 = 1111000000$, $y_3 = 1010101010$. Katere kodne besede so bile poslane? Dekodirajte z uporabo sindromov.

   (c) (dodatna naloga) Ali obstaja kakšna napaka s težo 2, ki jo kod popravi?

3. Kod $\mathcal{C}$ nad GF_2^4 je podan z nadzorno matriko

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} & \alpha^{-7} & \alpha^{-8} & \alpha^{-9} & \alpha^{-10} & \alpha^{-11} & \alpha^{-12} & \alpha^{-13} & \alpha^{-14} \end{bmatrix},$$

   kjer je α primitiven element obsega $\mathrm{GF}(2^4)$, na primer, α je ničla primitivnega polinoma $f(x) = x^4 + x + 1$. Definirajmo nov kod $\mathcal{D}$ kot $\mathcal{D} = \mathcal{C} \cap \{0, 1\}^{15}$.

   (a) Pokažite, da je kod $\mathcal{D}$ cikličen in poiščite njegov generatorski polinom.

   (b) Kolikšna je dimenzija koda $\mathcal{D}$?

   (c) Kolikšna je razmaknjenost koda $\mathcal{D}$?

   Če naloge ne znate rešiti za kod $\mathcal{D}$, jo rešite vsaj za kod $\mathcal{C}$.

Vse naloge je potrebno ustrezno utemeljiti!