2. kolokvij iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

Ljubljana, 1. junij 2009

1. (35 točk) Sporočilo oblike $a_1a_2a_3a_4a_5a_6a_7 \in \mathrm{GF}(11)^7$ kodiramo v kodno besedo $c_1c_2c_3c_4c_5c_6c_7c_8 \in \mathrm{GF}(11)^8$ na naslednji način: $c_i = a_i$ za $i = 1, \ldots, 7$, c_8 pa določimo tako, da je
$$\sum_{i=1}^{8} (9-i)\, c_i \equiv 0 \pmod{11}.$$
Pokažite, da je dobljeni kod linearen. Določite generatorsko in kontrolno matriko za ta kod. Kolikšna je njegova minimalna razdalja? Koliko napak odkrije in koliko napak popravi?

   Opomba: tako je sestavljena slovenska davčna številka, pri čemer so dovoljeni kodni simboli samo števila med 0 in 9.

2. (35 točk) Z uporabo Gilbert-Varshamove meje preverite, ali lahko obstaja linearen $[8, 4, 4]$-kod nad obsegom $\mathrm{GF}(2)$. Če obstaja, sestavite nadzorno matriko za takšen kod.

3. (30 točk) Linearni kod $\mathcal{C}$ nad $\mathrm{GF}(2)$ je podan z nadzorno matriko
$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$
Prejeli smo besedo $y_1 = 011111$. Katera kodna beseda je bila poslana? Katere kodne besede so najboljši kandidati za poslano besedo, če smo prejeli besedo $y_2 = 010010$. Dekodirajte z uporabo sindromov.

Odgovore na vsa vprašanja je potrebno utemeljiti!