

Név/Kód:

--	--	--	--	--	--	--

1. (20p)	2. (20 p)	3. (20 p)	4. (20 p)	5. (20 p)	Összesen (100p)	Jegy
----------	-----------	-----------	-----------	-----------	--------------------	------

- Győződjön meg róla, hogy a névsorban elfoglalt helye alapján a megfelelő teremben írja-e a dolgozatot!
- Minden feladatot külön lapon dolgozzon, kivéve a teszt (2.) feladatot, amelyet a nyomtatott oldalon töltsön ki bekarikázással jelezve a helyes választ!
- Egy vízszintes vonallal jelezze a nyomtatott lap tetjén lévő táblázatban azt a feladatot, amelyet nem oldott meg!
- Minden lapon olvashatóan szerepeljen a neve és a NEPTUN kódja!
- A diákigazolványa legyen előkészítve!
- AZ 1-ES, 3-AS ÉS 5-ÖS FELADATOK MEGOLDÁSA MELLÉ INDOKLÁST IS KÉRÜNK! ÖNMAGÁBAN CSAK A HELYES VÉGEREDMÉNY NEM ÉRTÉKELHETŐ.

F
O
N
T
O
S
!!!

1. Adott egy bináris lineáris kód a $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ generátormátrix-al.

- a) Szisztematikus-e a kód (indokolja választát) (4p)
- b) Adja meg a kódszavakat (4p)
- c) Hány hibát tud javítani a kód? (4p)
- d) Adja meg a paritásellenőrző mátrixot! (4p)
- e) Adja meg azon hibavektorok csoportját, amelyek a csupa egyesből álló hibavektorhoz tartoznak! (4p)

Megoldás:

a) Szisztematikus a kód, mert a G 2×5 -es egységmátrix-al kezdődik.

$$b) \mathbf{c} = \mathbf{uG} = (u_1, u_2) \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \rightarrow \mathbf{c}^{(0)} = (00000); \mathbf{c}^{(1)} = (01111); \mathbf{c}^{(2)} = (10110); \mathbf{c}^{(3)} = (11001)$$

$$c) t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = \left\lfloor \frac{w_{\min} - 1}{2} \right\rfloor = \left\lfloor \frac{3 - 1}{2} \right\rfloor = 1$$

$$d) \mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$e) \mathbf{s}^T = \mathbf{He}^T = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}; E_{(111)} = \{ \mathbf{e} : \mathbf{He}^T = \mathbf{s}^T \} = \{ (11111), (11111) + \mathbf{c}^{(0)}, (11111) + \mathbf{c}^{(2)}, (11111) + \mathbf{c}^{(3)} \} = \{ (11111); (10000); (01100); (00110) \}$$

2. Karikázza be a helyes állításokat az alábbi listán (csak akkor adható rá 20p, ha minden állításról helyesen döntött, különben 0 pont).

- a) Egy $C(8,5)$ kód lehet bináris Hamming kód.
- b) A Reed Solomon kód csak egy hibát tud javítani.
- c) Egy bináris lineáris kódnál, azonos szindrómavektorhoz tartozó hibavektorok csak azonos súlyúak lehetnek.
- d) Egy $C(n, k)$ ciklikus kód generátorpolinomja osztja az $x^n - 1$ polinomot.**
- e) A Reed Solomon kódnak létezik shiftregiszteres implementációja**

3. Adott egy emlékezetnélküli forrás a következő eloszlással $p_1 = 0.8; p_2 = 0.15; p_3 = 0.05$

- a) Adja meg az tömöríthetőség elvi alsó határát! (4p)
- b) Mi lenne az átlagos kódszóhossz, ha Shannon-Elias kóddal akarnánk tömöríteni? (4p)
- c) Mi a lenne az átlagos kódszóhossz ha Shannon-Fano kóddal akarnánk tömöríteni? (4p)
- d) Milyen hosszúságú blokkokban kell a forrást kódolni, ha az elvi alsó határt $\epsilon = 0.02$ -al akarnánk megközelíteni. (4p)
- e) Mekkora lesz így a kódtábla mérete? (4p)

Megoldás:

Elégtelen	Elégséges	Közepes	Jó	Jeles
0-39 pont	40-53 pont	54-67 pont	68-81 pont	82-100 pont

$$a) \text{ld}\left(\frac{1}{p_1}\right) = \text{ld}(1.25) = 0.322; \text{ld}\left(\frac{1}{p_2}\right) = 2,736; \text{ld}\left(\frac{1}{p_3}\right) = 4.322;$$

$$H(X) = p_1 \text{ld}\left(\frac{1}{p_1}\right) + p_2 \text{ld}\left(\frac{1}{p_2}\right) + p_3 \text{ld}\left(\frac{1}{p_3}\right) = 0.2575 + 0.4104 + 0.2161 = 0.884$$

$$b) L_{SFE} = l_1 p_1 + l_2 p_2 + l_3 p_3 + l_4 p_4 = \left(\left\lceil \text{ld}\left(\frac{1}{p_1}\right) \right\rceil + 1 \right) p_1 + \left(\left\lceil \text{ld}\left(\frac{1}{p_2}\right) \right\rceil + 1 \right) p_2 + \left(\left\lceil \text{ld}\left(\frac{1}{p_3}\right) \right\rceil + 1 \right) p_3 =$$

$$= 0.8 * 2 + 0.15 * 4 + 0.05 * 6 = 2.5$$

$$c) L_{SF} = l_1 p_1 + l_2 p_2 + l_3 p_3 + l_4 p_4 = \left\lceil \text{ld}\left(\frac{1}{p_1}\right) \right\rceil p_1 + \left\lceil \text{ld}\left(\frac{1}{p_2}\right) \right\rceil p_2 + \left\lceil \text{ld}\left(\frac{1}{p_3}\right) \right\rceil p_3 =$$

$$= 0.8 * 1 + 0.15 * 3 + 0.05 * 5 = 1.5$$

$$d) H(X) = 1.5023 \leq L_{fajlagos}^{blokk} \leq H(X) + 1/K = H(X) + 0.02 \rightarrow K = \frac{1}{0.02} = 50$$

$$e) \text{Compl} : O(3^{50})$$

- 4 Ahol nincs indoklás kérés ott csak egy számmal, vagy IGEN/NEM adja meg a válaszokat (mindegyik helyes válasz 4p) !
- a) Mekkora egy emlékezetnélküli 8-állapotú egyenletes eloszlású bináris forrás 3 hosszúságú blokkjainak az entrópiája ?
 $H(X_{k-2}, X_{k-1}, X_k) = H(X_{k-2}) + H(X_{k-1}) + H(X_k) = 3 + 3 + 3 = 9$
- b) Egy C(7,3) Reed Solomon kód esetén adja meg q értékét és a javítható hibák számát. ($q=8, t=2$)
- c) Mekkora egy C(5,2) lineáris bináris kód adott szindrómavektorhoz tartozó hibacsoportjaiban szereplő hibavektorok száma ? (4 db)
- d) Hányadfokú a generátorpolinomja egy C(7,3) lineáris ciklikus kódnak ? ($7-3=4$)

- 5 a) Ha egy példa RSA algoritmusnál $p_1 = 3, p_2 = 5$ és $e = 7$ mennyi d ? (10p)
- Megoldás: $\Phi(m) = (p_1 - 1)(p_2 - 1) = 2 * 4 = 8, d = e^{-1} \bmod \Phi(m) \rightarrow d = 7 \rightarrow de = 7 * 7 = 6 * 8 + 1$
- b) Adja meg egy C(7,5) Reed Solomon kód generátor polinomjának standard alakját ! (10p)
- A hatványtábla GF(8) felett a következő
- | | | | | |
|-----------|-------|----|----|----|
| 1 | 1 | 7 | 14 | 21 |
| y | y | 8 | 15 | 22 |
| y^2 | y^2 | 9 | 16 | 23 |
| $y+1$ | y^3 | 10 | 17 | 24 |
| y^2+y | y^4 | 11 | 18 | 25 |
| y^2+y+1 | y^5 | 12 | 19 | 26 |
| y^2+1 | y^6 | 13 | 20 | 27 |

$$\text{Megoldás: } g(x) = \prod_{i=1}^{n-k} (x - y^i) = (x + y)(x + y^2) = x^2 + (y + y^2)x + y^3 = x^2 + y^4 x + y^3$$

Elégtelen	Elégséges	Közepes	Jó	Jeles
0-39 pont	40-53 pont	54-67 pont	68-81 pont	82-100 pont