Name/Code:

1. (20p)	**2.** (20 p)	**3.** (20 p)	**4.** (20 p)	**5.** (20 p)	**Total (100p)**	**Grade**

IMPORTANT

- **Apart from the test questions (where each correct answer must be indicated by a tick) each problem must be worked out on a separate sheet on which your name and code must be clearly indicated!**
- **The notations and conventions you use must be conform with the ones used in the lecture series !**
- **Each solution requires a compact reasoning. Without this reasoning the answer is not considered to be valid even though the final result is correct.**

IMPORTANT

1) Given a linear binary code with generator matrix $\mathbf{G}=\begin{pmatrix}1&0&0&0&1\\0&1&0&1&0\\0&0&1&1&1\end{pmatrix}$!

a.) Give the type of the code (n,k) !
b.) Can this be a Hamming code?
c.) How many errors can be detected and corrected by this code!
d.) Can the error vectors $\mathbf{e}_1=(10000)$ and $\mathbf{e}_2=(00001)$ be distinguished? Can these error vectors be group leaders?
e.) If this code operates over a BSC with error probability $p=0.2$ then what is the probability of these two error vectors occurring?
f.) What is the error group belonging to the syndrome vector $\mathbf{s}=(10)$?
g.) What is the detected error vector?

---

a) n=5, k=3
b) No, because the Hamming bound is not achieved, $n+1\neq 2^{n-k}$
c) the codewords are:

$$(000)\mathbf{G}=(00000);\ (001)\mathbf{G}=(00111);\ (010)\mathbf{G}=(01010);\ (011)\mathbf{G}=(01101);$$

$$(100)\mathbf{G}=(10001);\ (101)\mathbf{G}=(10110);\ (110)\mathbf{G}=(11011);\ (111)\mathbf{G}=(11100)$$

$$w_{\min}=d_{\min}=2$$

$$l=d_{\min}-1=1\quad t=\left\lfloor\frac{d_{\min}-1}{2}\right\rfloor=0$$

d) first to compute the syndrome vectors, we need the parity check matrix:

$\mathbf{H}=\begin{pmatrix}0&1&1&1&0\\1&0&1&0&1\end{pmatrix}$, then we calculate the syndrome vectors as: $\mathbf{s^T}=\mathbf{H}\mathbf{e}^T$

With $\mathbf{e}_1=(10000)$ and $\mathbf{e}_2=(00001)$ we come to the syndrome vector $\mathbf{s^T}=\mathbf{H}\mathbf{e}_1^T=\mathbf{H}\mathbf{e}_2^T=\begin{pmatrix}0\\1\end{pmatrix}$, so the two error vector <u>cannot</u> be distinguished.

e)

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

f) Error group for $\mathbf{s} = (10)$

$$\begin{pmatrix}1\\0\end{pmatrix} = \mathbf{s}^T = \mathbf{He}^T = \begin{pmatrix}0&1&1&1&0\\1&0&1&0&1\end{pmatrix} \cdot \begin{pmatrix}?\\?\\?\\?\\?\end{pmatrix}$$

$$\mathbf{e}^T \in \left\{ \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}1\\0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\1\\1\end{pmatrix} \right\}$$

g) the detected error vector is the first or the second element of the above mentioned error group

---

2) Given an RS code over GF(8) capable of correcting every single error.

a.) What are the parameters of the code?
b.) Give the generator polynomial!
c.) What is the degree of the parity check polynomial?
d.) What HW architecture can implement the encoding?

---

a) The parameters of the code are:
$C(n,k)$
$n = q-1 = 8-1 = 7$, RS codes are MDS, so $d_{\min} - 1 = n - k$, and $t = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$, so

$$1 = \left\lfloor \frac{7-k}{2} \right\rfloor, k = 5$$

b) $g(x) = (x-y)(x-y^2) = x^2 + (y+y^2)x + y \cdot y^2 = x^2 + y^4 x + y^3$

c) The degree of the parity check polynomial is always *k*, since $h(x) = \prod_{i=n-k+1}^{n} (x - y^i)$

d) The encoding can be performed with a LFFSR, since the coding is performed by multiplying the message polynomial with the generator polynomial, $c(x) = u(x)g(x)$, and this operation can be carried out by convolving their coefficients with each other. So a linear filter can carry out the polynomial multiplication

---

3) Determine the value of the following determinant over GF(8)!

$$\det \begin{bmatrix}2&1&2\\1&1&2\\1&0&1\end{bmatrix} = ?$$

The power table over $GF(2^3)$:

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

One can use the power table like $a, b \in GF(2^3), a \mapsto y^m, b \mapsto y^n \quad a \cdot b \mapsto y^{m+n}$

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

$$\det\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = aei - afh - \left(bdi - bfg\right) + cdh - ceg =$$

$$= 2\cdot1\cdot1 - 0 - (1 - 1\cdot2\cdot1) + 0 - 2\cdot1\cdot1 =$$

$$= y\cdot1\cdot1 - 0 - (1 - 1\cdot y\cdot1) + 0 - y\cdot1\cdot1 = y = 2$$

---

4) Given a memoryless source with the following distribution $p_1 = 0.55;\ p_2 = 0.2;\ p_3 = 0.25$.

a.) What is the theoretical limit of compression!

b.) Compress the source by Huffman coding: give the code and the average codelength !

c.) What is the average code-length if we compress the source by Shannon-Fano coding?

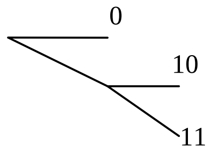
d.) What block length should be chosen if the theoretical lower bound is to be achieved with $\varepsilon = 0.002$. What is then the size of the code table?

---

a) $$H(X) = \mathbb{E}\, I(x) = \sum_x p(x)\, ld\left(\frac{1}{p(x)}\right) = 0.55\cdot ld\left(\frac{1}{0.55}\right) + 0.2\cdot ld\left(\frac{1}{0.2}\right) + 0.35\cdot ld\left(\frac{1}{0.35}\right) =$$

$$= 1.46886$$

b)
0.55 0.55 1
0.25 0.45
0.2



The average codelength is $L = 0.55\cdot1 + 0.35\cdot2 + 0.2\cdot2 = 1.65$

c) the average codelength using SF coding is

$$L = 0.55\cdot\left\lceil ld\left(\frac{1}{0.55}\right)\right\rceil + 0.35\cdot\left\lceil ld\left(\frac{1}{0.35}\right)\right\rceil + 0.2\cdot\left\lceil ld\left(\frac{1}{0.2}\right)\right\rceil = 1.85$$

d)

5) Indicate the correct statements! Justify your answer!

- ☐ Having two error vectors belonging to the same syndrome vector, we must decide on the one which has smaller weight than the other. **T**
- ☐ The mutual information of two independent random variables is zero. **T**
- ☐ Between 0 and 4 values bound the entropy of a source containing 4 symbols. **F** $0 \le H(x) \le ld(N)$

  $$H(x) = ld(N),\ \text{if}\ p(x) = \frac{1}{N}, \forall x$$
- ☐ The Hamming codes are MDS codes **F**
- ☐ The irreducible polynomial can be factorized into the product of two other polynomials. **F**

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