- 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 tetején lévő táblázatban azt a feladatot, amelyet nem oldott meg!
- Minden lapon olvashatóan szerepeljen a neve és a NEPTUN kódja!
- AZ 1-ES, 3-AS, 4-ES ÉS 5-ÖS FELADATOK MEGOLDÁSA MELLÉ INDOKLÁST IS KÉRÜNK! ÖNMAGÁBAN CSAK A HELYES VÉGEREDMÉNY NEM ÉRTÉKELHETŐ, A MEGOLDÁS GONDOLATMENETÉRŐL A JAVÍTÓKNAK MEG KELL GYŐZŐDNIÜK.

1. Adott egy digitális csatorna az alábbi állapot-átmeneti mátrixszal:

$$\mathbf{P}=\begin{pmatrix} 0.5 & 0.125 & 0.25 & 0.125 \\ 0.125 & 0.5 & 0.125 & 0.25 \\ 0.25 & 0.125 & 0.5 & 0.125 \\ 0.125 & 0.25 & 0.125 & 0.5 \end{pmatrix}$$

a) Mekkora a forrás szimbólum készlete? *(5p)*
b) A $k=10$ szimbólumhosszú üzeneteket milyen n hosszúságú kódszavakra kell kiegészíteni a megbízható kommunikációhoz? *(15p)*

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

A. Csak a $C\left(2^m-1, 2^m-m-1\right)$ kódok (ahol $m=1,2,\ldots$) lehetnek Hamming kódok.
B. Az LZ77 tömörítési algoritmus nem igényli a forráseloszlást.
C. Egy szisztematikus kódnál az üzenet kódszóból történő detekciójához egy visszacsatolt shift regiszterre van szükség.
D. Az RSA algoritmushoz kell az adó és vevő közti kulcscsere.
E. Az entrópia egyenletes forráseloszlás esetén minimális.

3. Adott egy emlékezetnélküli forrás a következő eloszlással: $p_1=0.25;\ p_2=0.25;\ p_3=0.25;\ p_4=0.125;\ p_5=0.125$

a) Adja meg az tömöríthetőség elvi alsó határát! *(5p)*
b) Kódolja ezt a forrást Shannon-Fano-Elias kóddal! Mekkora az átlagos kódszóhossz? *(5p)*
c) Kódolja ezt a forrást Shannon-Fano kóddal! Mekkora az átlagos kódszóhossz? *(5p)*
d) Kódolja ezt a forrást Huffmann kóddal! Mekkora az átlagos kódszóhossz? *(5p)*

4 Ahol nincs indokláskérés ott csak egy számmal, vagy IGEN/NEM adja meg a válaszokat (mindegyik helyes válasz 5p)!

a) Mekkora egy emlékezetnélküli 8-állapotú egyenletes eloszlású bináris forrás 3 hosszúságú blokkjainak az entrópiája?
b) Egy C(7,3) Reed Solomon kód esetén adja meg q értékét és a javítható hibák számát!
c) Hány darab hibacsoport van egy C(15,11) lineáris, bináris kód esetén?
d) Lehet-e 12 felhasználónak 12 dimenziós Walsh Hadamard kódokat adni? (Indokolja válaszát!)

5 Egy 4 szimbólumkészletű forrás kódolására adaptív Huffmann kódot használunk. Rajzolja fel az állapotgráf változását szimbólumról szimbólumra, és adja meg a kódszavakat, ha a megfigyelt szimbólumsorozat a következő: $x_3, x_4, x_3, x_2, \ldots$

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

2014. 01. 12

Infokód

Vizsga ZH mo.

I.) Adott egy digitális csatorna az alábbi állapot-átmeneti mátrixxal:

$$P = \begin{bmatrix} 0,5 & 0,125 & 0,25 & 0,125 \\ 0,125 & 0,5 & 0,125 & 0,25 \\ 0,25 & 0,125 & 0,5 & 0,125 \\ 0,125 & 0,125 & 0,125 & 0,5 \end{bmatrix}$$

a.) Mekkora a forrás szimbólum készlete? (5p)

az állapot-átmeneti mátrix mindig négyzetes

$P_{4\times4} \rightarrow \underline{\underline{n=4}} \rightarrow$ akkora a forrás szimbólum készlete

b.) A $k=10$ szimbólumhosszú üzeneteket milyen n hosszúságú kódszavakra kell kiegészíteni a megbízható kommunikációhoz? (15p)

1. lépés: megvizsgálni, hogy szimmetrikus-e a mátrix.
(megj.: egy mátrix akkor szimm., ha az oszlopok egymás permutációi)

$\Rightarrow$ ha szimmetrikus, akkor:

2. lépés: csatorna kapacitásának számolása

$\hookrightarrow C = ld(N) - H(\pi)$

π: egy tetszőleges oszlop

$\rightarrow H(x) = \sum_x p(x) \cdot ld \frac{1}{p(x)} \rightarrow$ entrópia

$$C = ld(4) - 0,125 \cdot ld \frac{1}{0,125} \cdot 2 - 0,25 \cdot 2 - 0,5 \cdot 1 = 0,25$$

$$n = \frac{k}{C} = \frac{10}{0,25} = \underline{\underline{40}}$$

II.) Igaz - Hamis

a.) Csak a $C(2^m-1; 2^m-m-1)$ kódok (ahol $m=1,2\dots$) lehetnek Hamming kódok.

→ a Hamming kód az perfekt kód és MDS is.

$$d_{min} = n-k+1$$

$$n+1 = 2^{n-k}$$

vagy

$$\sum_{0}^{t} \binom{n}{i} = 2^{n-k}$$

$$(2^m-1)+1 = 2^m$$

$$2^{n-k} = 2^{(2^m-\cancel{1})-(\cancel{2^m}-m-\cancel{1})} = 2^m$$

⇒ ezek lehetnek Hamming kódok, viszont NEM CSAK ezek. Ellenpéldát nem találtam !!

b.) Az LZ77 tömörítési algoritmus nem igényli a forráseloszlást.

→ valóban nem, mivel adaptív.

adaptív kódolások:

- adaptív Huffmann
- LZ77
- LZ78
- LZW → ezt nem vettük

nem kell neki forrás elo, feltételezi, hogy egyenletes

Entrópia alapú:

- SF
- SFE
- Huffmann

ezeknek kell tudni a forrás elo-t

c.) egy szisztematikus kódnál az üzenet kódszóból történő detektálásához egy visszacsatolt shift regiszterre van szükség.

az, hogy szisztematikus, azt jelenti, hogy a G eleje egységmátrix, amit csak csonkítani kell.
visszacsatolt shift regiszter pedig nem értelmezhető kell.

d.) Az RSA algoritmushoz kell az adó és a vevő közti kulcscsere.

Hamis, mivel az RSA-nál 2 kulcs van

<u>privát kulcs</u>: ezzel tudod kibontani az üzeneteket

<u>publikus kulcs</u>: titkosítja az üzenetet

e.) Az entrópia egyenletes forrás elo. esetén minimális.

Hamis! akkor lesz maximális.
ha ez 0, akkor nincs értelmes információ.

egyenletes elo.: $H(x) = ld(N)$

kül.: $H(x) \leq ld(N)$

III.) Adott egy emlékezetnélküli forrás a köv. elo-val:

$p_1 = 0{,}25$; $p_2 = 0{,}25$; $p_3 = 0{,}25$; $p_4 = 0{,}125$; $p_5 = 0{,}125$

a.) Adja meg a <u>tömöríthetőség elvi alsó határát</u>! (5p)

ez az entrópia

$$H(x) = \sum_x p(x) \cdot ld \frac{1}{p(x)} = 0{,}25 \cdot \underbrace{ld \frac{1}{0{,}25}}_{2} \cdot 3 + 0{,}125 \cdot \underbrace{ld \frac{1}{0{,}125}}_{3} \cdot 2 =$$

$ld \frac{1}{0,25} = \log_2 \frac{1}{2^{-2}} = \log_2 2^2 = 2$

$\boxed{\text{Ell: } H(x) \leq ld(N)}$

$ld \frac{1}{0,125} = \log_2 2^3 = 3$

$H(x) = 1,5 + 0,75 = \underline{\underline{2,25}}$

b.) Kódolja ezt a forrást Shannon-Fano-Elias kóddal! Mekkora az átlagos kódszó hossz? (5p)

átlagos kódszó hossz:

$L = \sum_x p(x) \cdot l(x) = 0,25 \left(\left\lceil ld \frac{1}{0,25} \right\rceil + 1 \right) \cdot 3 +$

$l(x) = \left\lceil ld \frac{1}{p(x)} \right\rceil + 1$

$+ 0,125 \left(\left\lceil ld \frac{1}{0,125} \right\rceil + 1 \right) \cdot 2 = 2,25 + 1 = \underline{\underline{3,25}}$

SFE kódolás: $\bar{F} = \sum_{a<x} p(a) + \frac{p(x)}{2} = F - \frac{p(x)}{2}$

$\bar{F}(1) = \frac{p(x)}{2} = \frac{0,25}{2} = 0,125 \rightarrow 0,\underbrace{001}$

$\bar{F}(2) = p_1 + \frac{p_2}{2} = 0,25 + \frac{0,25}{2} = 0,375 \rightarrow 0,\underbrace{011}$

$\bar{F}(3) = p_1 + p_2 + \frac{p_3}{2} = 0,25 + 0,25 + \frac{0,25}{2} = 0,675 \rightarrow 0,\underbrace{101}001\ldots$

$\bar{F}(4) = p_1 + p_2 + p_3 + \frac{p_4}{2} = 0,25 \cdot 3 + \frac{0,125}{2} = 0,8125 \rightarrow 0,\underbrace{1101}$

$\bar{F}(5) = p_1 + p_2 + p_3 + p_4 + \frac{p_5}{2} = 3 \cdot 0,25 + 0,125 + \frac{0,125}{2} = 0,9375 \rightarrow 0,\underbrace{1111}$

$\bar{F}(1) = 0,\underbrace{001}$ 3 bitet hagyunk, mert $\left\lceil ld \frac{1}{p(x)} \right\rceil + 1 = 3$

a többit elhagyjuk. ha nincs annyi, akkor 0-val pótoljuk.

c) Kódolja ezt a forrást Shannon-Fano kóddal! Mekkora az átlagos kódszó hossz?

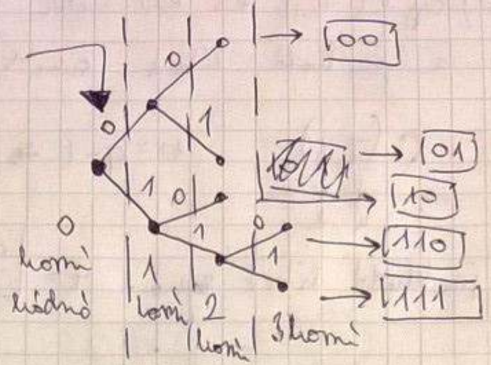
átlagos kódszó hossz: SFE − 1 = <u>2,25</u>

SF kódolás: 1. lépés: $l(x)$-ek kiszámítása az SFE − 1 szerint

$l_1 = 2$ $l_4 = 3$

$l_2 = 2$ $l_5 = 3$

$l_3 = 2$

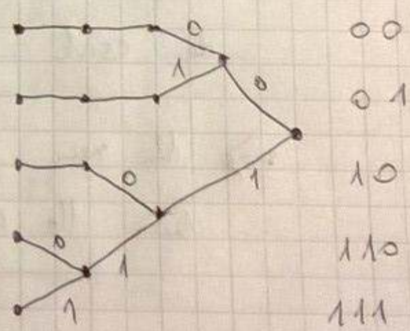


d) Kódolja ezt a forrást Huffmann kóddal! Mekkora az átlagos kódszó hossz?

átlagos kódszó hossz: $L = p(x) \cdot l(x) = 0{,}25 \cdot 2 \cdot 3 + 0{,}125 \cdot 3 \cdot 2 = \underline{2{,}25}$

Huffmann: 1. lépés: sorba kell tenni a szimbólumokat valószínűség szerint.

P1	0,25	0,25	0,25	0,5
P2	0,25	0,25	0,25	0,5
P3	0,25	0,25	0,5	
P4	0,125	0,25		
P5	0,125			



IV.)

a.) Mekkora egy emlékezetnélküli 8-állapotú egyenletes eloszlású bináris forrás 3 hosszú blokkjainak az entrópiája? (5p)

$$2^3 = 8 \qquad H(x) = 8 \cdot \frac{1}{8} \cdot \mathrm{ld}\,\frac{1}{\frac{1}{8}} = 3$$

b.) Egy $C(7,3)$ RS kód esetén adja meg q értékét és a javítható hibák számát! (5p)

$C(7,3)$: $n = 7$, $k = 3$

$$n = q-1 \Rightarrow n+1 = \underline{\underline{q = 8}} \Rightarrow 2^3$$

javítható hibák száma: $t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor = \left\lfloor \frac{7-3}{2} \right\rfloor = \underline{\underline{2}}$

c.) Hány db hibacsoport van $C(15,11)$ lineáris, bináris kód esetén? (5p)

2^{n-k} db hibacsoport van $\Rightarrow 2^{15-11} \Rightarrow 2^4 = \underline{\underline{16}}$

d.) Lehet-e 12 felhasználónak 12 dimenziós Walsh Hadamard kódokat adni? (Indoklással) (5p)

es a kód olyan $k \times k$-s mátrixokat állít elő, melynek sorai vagy oszlopai ortogonálisak

de csak $2^4 = k$ lehet (k-nak 2 hatványnak kell lennie!)

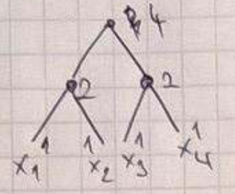
$\Rightarrow$ 12 nem 2 hatványa így nem lehet.

min 16 dimenziósat lehet kiosztani.

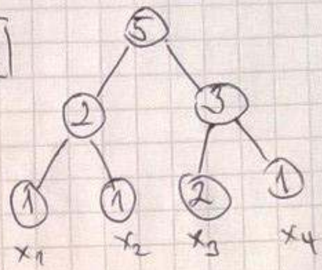
V. Egy 4 szimbólumkészletű forrás kódolására adaptív Huffman kódot használunk. Rajzolja fel az állapot gráf változásait szimbólumról szimbólumra, és adja meg a kódszavakat, ha a megfigyelt szimbólum sorozat a köv: x_3, x_4, x_3, x_2 ---

1 lépés: feltételezzük, hogy egyenletes elo.-van.

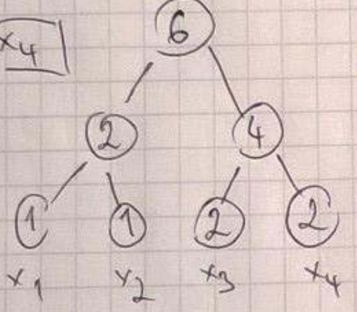
1



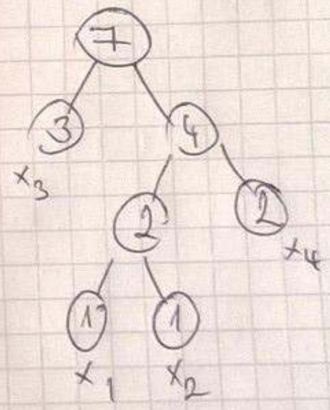
2 $\boxed{x_3}$



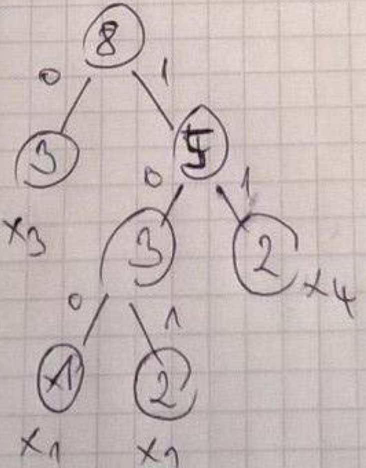
3 $\boxed{x_4}$



4 $\boxed{x_3}$



5 $\boxed{x_2}$



x_3: 0

x_1: 100

x_2: 101

x_4: 11