

1) Adott egy nem rövidített, ciklikus RS kód a következő generátorpolinommal a GF(8) felett  $g(x) = x^2 + y^4x + y^3$

a) Mik a kód paraméterei? (5p)

$$GF(8) \Rightarrow q=8 \text{ és } n=q-1=8-1=7$$

$$\deg(g(x)) = n - k = 2 \Leftrightarrow 7-k=2 \Leftrightarrow k=5 \Rightarrow C(7, 5)$$

b) Hány hibát tud javítani a kód? (5p)

$$\text{Általánosan: } t = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor \text{ és } d_{\min} \leq n-k+1$$

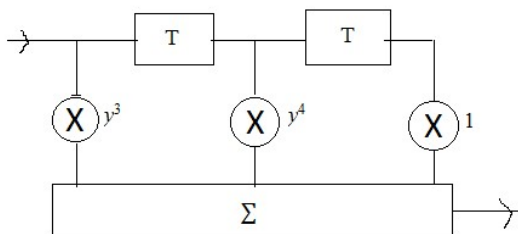
$$RS \Rightarrow MDS \Rightarrow d_{\min} = n-k+1 \Rightarrow t = \left\lfloor \frac{n-k}{2} \right\rfloor = \left\lfloor \frac{2}{2} \right\rfloor = 1$$

c) Hányad fokú a paritásellenőrző polinom? (5p)

$$\deg(h(x)) = k = 5 \quad (\text{mert } h(x) = \prod_{i=n-k+1}^n (x - \alpha^i), \text{ ahol } \alpha \text{ primitív elem})$$

d) Milyen HW architektúrával valósítható meg a kódolás? (5p)

Előrecsatolt shiftregiszter



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

a) Egy  $C(n, k)$  paraméterű ciklikus kód generátorpolinomja ~~nem~~ osztja az  $x^n-1$  polinomot

**b) Két azonos szindrómavektorhoz tartozó hibavektorból arra érdemes detektálni, amelynek kisebb a súlya**

**c) Egy  $C(7, 4)$  paraméterű kód lehet Hamming kód**

Kiegyenlíti a  $2^{n-k} = n+1$  egyenletet.

d) A szisztematikus kódok paritásellenőrző mátrixának az utolsó  $k \times k$ -s szegmense egységmátrix. ( $[n-k] \times [n-k]$ )

**e) Két polinom szorzatát előrecsatolt shiftregisztereken lehet implementálni.**

3) Adott egy emlékezet nélküli forrás a következő eloszlással:  $p_1=0.7$ ;  $p_2=0.2$ ;  $p_3=0.1$

a) Adja meg a tömöríthetőség elvi alsó határát! (4p)

$$H(x) \leq L \Rightarrow H(x) = \sum_{\forall x} p(x) \log_2 \frac{1}{p(x)} = 0.7 * 0.515 + 0.2 * 2.322 + 0.1 * 3.322 = 1.16$$

b) Tömörítse a forrást Huffman kóddal: adja meg a kódot és az átlagos kódszóhosszat! (4p)

$$\begin{array}{l} p_1=0.7 \quad - \quad 0.7 \quad - \quad 1 \quad \quad \quad \cdot \quad - \quad c_1=(1) \\ p_2=0.2 \quad - \quad 0.3 \quad / \quad \quad \quad \backslash \quad - \quad c_2=(01) \\ p_3=0.1 \quad / \quad \quad \quad \quad \quad \quad \quad \quad \backslash \quad c_3=(00) \end{array}$$

$$L = \sum_{\forall x} p(x) l(x) = 0.7 * 1 + 0.2 * 2 + 0.1 * 3 = 1.3$$

c) Mi lenne az átlagos kódszóhossz, ha Shannon Fano kóddal akarnánk tömöríteni? (4p)

$$L^{SF} = \sum_{\forall x} p(x) \left\lceil \log_2 \frac{1}{p(x)} \right\rceil = 0.7 * 1 + 0.2 * 3 + 0.1 * 4 = 1.7$$

d) Milyen hosszú blokkokban kell a forrást kódolni, ha az elvi alsó határt  $\epsilon=0.02$ -al akarnánk megközelíteni (4p)

$$H(X) + \epsilon = H(X) + 1/K \Leftrightarrow \epsilon = 1/K \Leftrightarrow K = \lceil 1/\epsilon \rceil = \lceil 1/0.02 \rceil = 50$$

e) Mekkora lesz így a kódtábla mérete (hány sort fog tartalmazni)? (4p)

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

4) Csak egy számmal adja meg a válaszokat (minden helyes válasz 4p)!

a) Milyen min. és max. érték közé esik egy 4 darab szimbólummal rendelkező forrás entrópiája?

$$0 \leq H(x) \leq \log_2(N) = \log_2(4) = 2$$

b) Egy 8 szimbólumot tartalmazó egyenletes eloszlású forrás esetén hány bitek lesznek az optimális kódhosszak?

$$\text{Egyenletes eloszlású} \Rightarrow \text{entrópia max., továbbá } H(x) \leq L \text{ és } L \text{ min. (mert optimális)} \Rightarrow L = \log_2(N) = 3$$

c) Egy 5 szimbólummal és az  $l_1=2; l_2=2; l_3=2; l_4=3$  kódhosszakkal rendelkező forrás esetén legalább milyen hosszú legyen az ötödik szimbólumhoz tartozó kódszó hossza, ha az egyértelmű dekódolhatóság a cél?

*Egyértelmű dekódolhatóság: prefixmentes kód kell! A kód prefixmentes, ha teljesíti a  $\sum_{\forall x} 2^{-l(x)} \leq 1$  (Kraft-McMillan) egyenlőtlenséget.  $l_5=2$ -re nem teljesül, de  $l_5=3$ -ra már igen.*

d) Adott két független egyenletes eloszlású bináris forrás. Mekkora az együttes entrópiájuk?

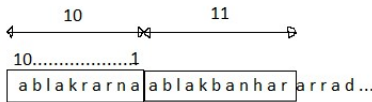
$$\text{Bináris} \Rightarrow N=2 \Rightarrow H(x), H(y) = \log_2(N) = 1$$

$$\text{Flen.} \Rightarrow H(x, y) = H(x) + H(y) = 1+1 = 2$$

e) Hány darab prím szám kell az RSA algoritmus kulcsának generálásához egy adott felhasználó esetén?

$$p_1, p_2 \Rightarrow 2 \text{ darab}$$

5) Adott egy LZ77 kódoló a következő architektúrával:



a) Adja meg a fenti ábrán látható szövegálláshoz tartozó kimeneti adathármas, ha az első buffer hossza 10 és (ahogy az ábra is mutatja) az első buffernél, balról a legelső betű felett helyezkedik el a 10-es koordináta, valamint a második buffer hossza 11.

A betűk kódolására az f() jelet használjuk (pl. a „b” betű kódját „f(b)” jelöli). (15p)

$$\langle 10, 5, f(b) \rangle$$

b) Adja meg a szöveg jelenlegi állásához tartozó kimeneti adathármas teljes bináris hosszát, ha 32 db karakterből álló szöveget tömörítünk. (5p)

$$\langle p, l, n \rangle \longrightarrow \lceil \log h_s \rceil + \lceil \log h_l \rceil + \lceil \log \chi \rceil = \text{Output, ahol } h_s \text{ az első, } h_l \text{ második buffer mérete, és } X \text{ a karakterek száma.} \Rightarrow \text{Output} = 4+4+5 = 13$$