2010.12.03. Zh

1

minden egy hiba $\Rightarrow t=1$

RS kód $GF(8) \to q$

$n = q-1$

a) $t = \left\lfloor \frac{n-k}{2} \right\rfloor$ $n = 8-1 = 7$

$2t = n-k$

$2 = 7-k \to k=5$

$C(7,5)$

b) $g(x) = \prod_{i}^{n-k} (x - y^i) = \prod_{i}^{n-k} (x + y^i)$

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

$= x^2 + x(\underbrace{y+y^2}_{y^4}) + y^3$

$y^4 \leftarrow$ hatványtáblából

$g(x) = x^2 + y^4 x + y^3$

c) paritásell. polinom fokszáma

$\deg(h(x)) = k = 5$

d) előrecsatolt shift regiszter

2

~~[illegible]~~

3 $p_1 = 0{,}8 \quad p_2 = 0{,}15 \quad p_3 = 0{,}05$

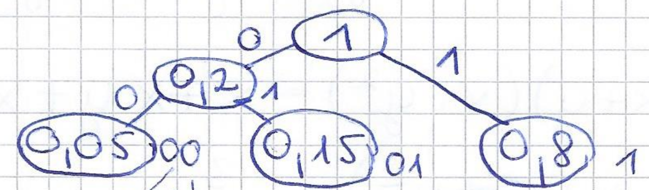
a) ~~$H(x) = \sum_x p(x) \left(\log_2 \frac{1}{p(x)}\right)$~~

$$H(x) = \sum_x p(x) \cdot \left(\log_2 \frac{1}{p(x)}\right)$$

$$H(x) = 0{,}8 \cdot \left(\log_2 \frac{1}{0{,}8}\right) + 0{,}15 \cdot \left(\log_2 \frac{1}{0{,}15}\right) + 0{,}05 \cdot \left(\log_2 \frac{1}{0{,}05}\right) =$$

$$H(x) = 0{,}884$$

b)



$l_3 = 2$ ← ahány db szám van $\quad l_2 = 2 \quad l_1 = 1$

Huffmannál mindig a két legkisebb valószínűség adódik össze.

$$L_H = \sum_x l_x \cdot p(x)$$

$$L_H = 2 \cdot 0{,}05 + 2 \cdot 0{,}15 + 0{,}8 \cdot 1 = 1{,}2$$

c) SF → $L_{SF} = \sum_x p(x) \cdot \left\lceil \log_2 \frac{1}{p(x)} \right\rceil$

$$L_{SF} = 0{,}8 \cdot \underset{(0{,}32 \to 1)}{1} + 0{,}15 \cdot \underset{(2{,}74)}{3} + 0{,}05 \cdot \underset{(4{,}32)}{5} =$$

felfelé kerekítünk mindig

$$L_{SF} = 1{,}5$$

d) $\varepsilon = 0{,}02$

$$H(x) \leqq L \leqq H(x) + \frac{1}{K}$$

$$H(x) \leqq L \leqq H(X) + \varepsilon$$

$$\frac{1}{K} = \varepsilon \rightarrow K = \frac{1}{\varepsilon} = \frac{1}{0{,}02}$$

$$\underline{K = 50}$$

e) 3^{50}

ahány db valószínűség van megadva a feladat növégében

---

(4) a) $0 \leqq H(x) \leqq \log_2 4$

egyenletes eloszlás esetén $H(X) = \log_2 N$

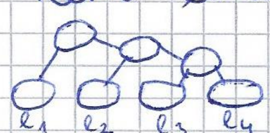
$$H(x) = \log_2 4 = 2$$

b) $H(X_1, X_2) = H(X_1) + H(X_2) = \log_2 N + \log_2 N = 1 + 1 = 2$

($\log_2 N = 1$, mert bináris; összeadom, mert emlékezet nélküli => ftlen egymástól

---

c) nem lehet $\quad \sum_{\forall x} 2^{-l(x)} \leqq 1$



→ így $l_3 = 3$-nak kéne lennie

d)

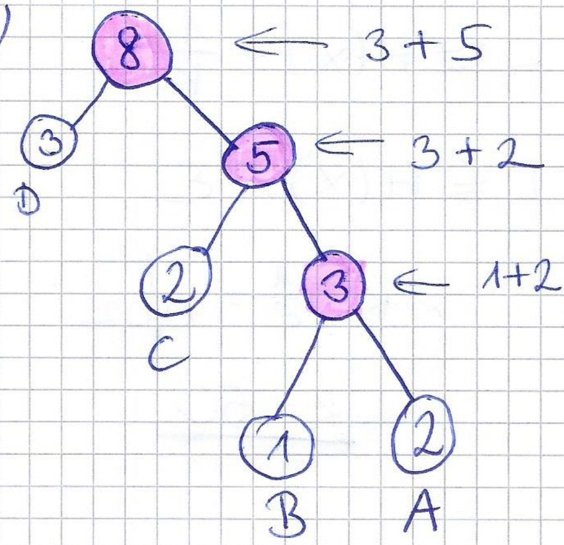
e) 2 elemből áll

p_1 és p_2 (vagy p és q)

(ha titkos lenne, akkor 3)

5

b,



a) $p_1 = 13 \qquad p_2 = 17$

$$\phi(n) = (p_1 - 1)(p_2 - 1)$$

$$\phi(n) = 12 \cdot 16 = \underline{\underline{192}}$$

2 a, Hamis → Haming csak 1 db-ot javít mindig

b, 2^k db-ot → Hamis

c, Hamis

d, $h(x) \cdot g(x) = x^4 - 1 \rightarrow \frac{x^4 - 1}{h(x)} = g(x) \rightarrow$ Igaz

e) Hamis → visszacsatolt shiftr.