Kódtech ZH Vizsga Összefoglalás

Emlékezet nélküli stacionárius forrás:

$P(X(k)=x_i \mid X(k-1)=x_j \ldots X(0)=x_m) = P(X(k)=x_i) =$

$= P_i(k)$: hogy a forrás a "k"-adik időpillanatban éppen az x_i minta-

at generálja magától (nem függ az időtől)

mintaelem : $X \to x_1, x_2 \ldots x_n$

mintaelemhez tartozó valószínűség : $p_1, p_2 \ldots p_n \to P(X)$

minden mintaelemhez egy kódszó : $c(X) \to c_1, c_2 \ldots c_n$

mintaelemhez tartozó kódhossz : $l(X) \to l_1, l_2 \ldots l_n$

Átlagos kódszóhossz: $L = E(l(X)) = \sum_X P(X) \cdot l(X)$

Adatátviteli sebesség: $f_s \cdot L$

↑ időben egymás után milyen gyakran generálódik egy mintaelem a forrásból

C_{opt} : $\min_C L \Rightarrow$ min. adatátviteli sebesség

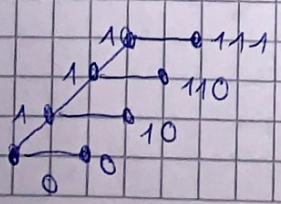
$f_s \geq 2B$ B: a jel sávszélessége

Egyértelműen dekódolhatóság:

- prefixmentes kód esetén: egyik kódszó sem előtagja a másiknak

$(\bar{c}_i \neq \bar{c}_j \; \forall i,j = 1,2 \ldots m, \; i \neq j$

Bináris fa:



Nem megírható levelek száma: $2^{L-l(X)}$

Kraft egyenlőtlenség: $\sum_X 2^{-l(X)} \leq 1$ (prefixmentesség feltétele)

Információ: $I(x) = \log_2\left(\frac{1}{P(x)}\right)$

Entrópia (átlagos információ): $H(x) = E(I(x)) = \sum_x P(x) \cdot \log_2\left(\frac{1}{P(x)}\right)$

$0 \leq H(x) \leq \log_2 n$ n: a forrás minőlunk lehetséges száma

Forráskódolási tétel:

$\boxed{H(x) \leq L}$

→ Tanúsítlehetőség elvi alsó határa az entrópia: $H(x)$

Shannon - Faro kód:

$$l(x) = \left\lceil \log_2\left(\frac{1}{P(x)}\right) \right\rceil$$

Algoritmus: Adott $P(x)$

1, Kódszóhossz kiszámítására

2, Bináris fa konstrukció

3, Átlagos kódszóhossz

4, Entrópia kiszámolására

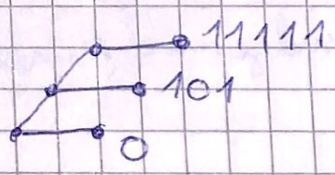
5, Hatékonyság kiszámítására

Példa megoldás: $P_1 = 0,8$ $P_2 = 0,15$ $P_3 = 0,05$

① $l_1 = \left\lceil \log_2 \frac{1}{0,8} \right\rceil = \lceil 0,32 \rceil = 1$

$l_2 = \left\lceil \log_2 \frac{1}{0,15} \right\rceil = \lceil 2,73 \rceil = 3$

$l_3 = \left\lceil \log_2 \frac{1}{0,05} \right\rceil = \lceil 4,32 \rceil = 5$

② 

③ $L = 1 \cdot 0,8 + 3 \cdot 0,15 + 5 \cdot 0,05 = \underline{\underline{1,5}}$

④ $H(x) = 0,32 \cdot 0,8 + 2,73 \cdot 0,15 + 4,32 \cdot 0,05 = \underline{\underline{0,88}}$

⑤ Hatékonyság $= \frac{H(x)}{L} = \frac{0,88}{1,5} = 0,59 = \underline{\underline{59\%}}$

Huffman-kód (Optimális kód)

Kritériumok: 1, $P(x) > P(y) \rightarrow \ell(x) < \ell(y)$

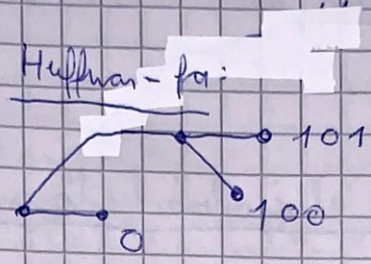
2, $P_1 > P_2 > \ldots > P_{n-1} > P_n \Rightarrow \ell_{n-1} = \ell_n$

Előző példa Huffmanal:

$P_1 = 0{,}8$ — 0,8

$P_2 = 0{,}15$ — 0,2

$P_3 = 0{,}05$



$L_{HUFF} = 1 \cdot 0{,}8 + 2 \cdot 0{,}15 + 2 \cdot 0{,}05 = 1{,}2$ Tegyük fel $f_S = 1{,}6 \cdot 10^8$

$L_{SF} = 1{,}5$ Adatátviteli sebesség: $R = f_S \cdot L$

$R_{HUFF} = 192$ Mbps

$R_{SF} = 240$ Mbps

} Huffman kód esetén majd 50 Mbps-t nyerünk

$\rightarrow \sum_x P(x) \cdot$ milyen mélyen van a fában

Blokk kódok: Képes arra, hogy $H(X) \leq L \leq H(X) + \varepsilon$

$H(X,Y) = H(X) + H(Y)$ (ha X, Y függetlenek egymástól)

$H(X_1, X_2, \ldots, X_M) = \sum_{i=1}^{M} H(X_i)$ (ha $X_1, \ldots, X_M$ függetlenek)

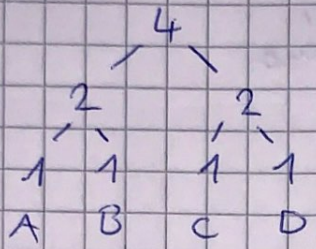
$= M \cdot H(X)$ (ha azonos eloszlásúak)

$X_1 = \ldots = X_M$

Adaptív Huffman-kódok:

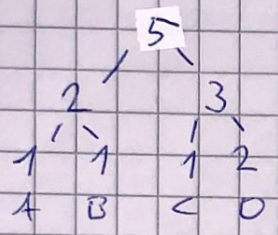
- manóban nem csalódnak
- a levelek száma megegyezik a csomópont számával akárhogy bővülhet

Példa:

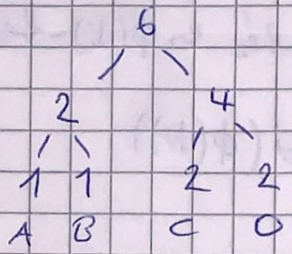


A fenti dolgot tudjuk bővíteni: DCDA

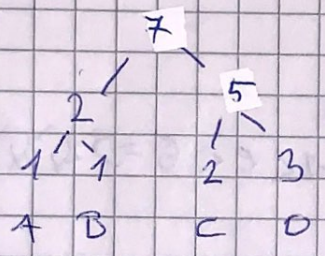
D:



C:

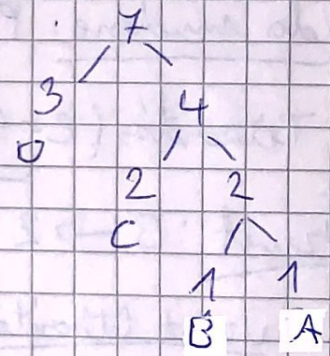


D:

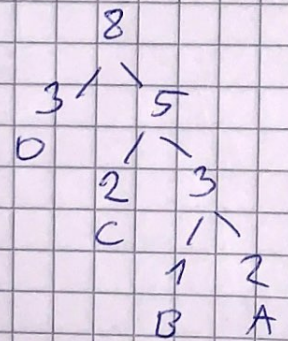


(manóban nem csalódnak, ezért: újra bővítgetem a fát)

=>



A:



RSA titkosítás:

Hogyan válasszuk paramétereket?:

1, P, q prím számok — P, q titkos

N, e nyilvános

2, $N = P \cdot q$

3, $\phi(N) = (P-1)\cdot(q-1)$

4, e $\begin{cases} 1 < e < \phi(N) \\ \text{relatív prím } N\text{-hez és } \phi(N)\text{-hez} \end{cases}$

5, d: $d \cdot e = 1 \mod(\phi(N))$

Példa mindenre: $P = 2 \quad q = 7$

Titkosítás ($e = 5$, $N = 14$) (nyilvánosak)

$1 < e < 6 \Rightarrow 2, 3, 4, 5$

Üzenet: B → 2 (számmá írjuk)

Üzenet titkosítása: $2^5 \mod(14) = 4 \rightarrow D$

$(y = x^e \mod(N))$

Titkosított üzenet: D → 4

Visszatitkosítás: $(\overset{d}{11}, 14)$

$4^{11} \mod(14) = 2 \rightarrow B$

$d \cdot e = 1 \mod(\phi(N))$

$\phi = 6$

$e = 5$ ⟶ $5d = 1 \mod(6)$

$d = 11 \Rightarrow 5 \cdot 11 = 1 \mod(6)$