KÓDOLÁSTECHNIKA ZH

2007. november 30.

1. Egy C lineáris bináris kód paritásellenőrző mátrixa:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

a.) Adja meg a kód szisztematikus genenátormátrixát! (2 p)
b.) Adja meg a kód minimalis távolságát! (2 p)
c.) Adja meg a szindróma dekódolási táblázatot! (3 p)
Legyen p a bithibázás valószínűsége az emlékezetnélküli BSC(p) csatornán.
d.) Hibajavító célú C kód hibavalószínűsége (3 p)
e.) Hibadetekciós célú C kód detekciós hibavalószínűsége (3 p)

2. Definiálja a következőket:
a.) perfekt tulajdonságú hibajavító kód (3 p)
b.) hibajavító ciklikus blokk kód paritásellenőrző polinomja definíciója (3 p)
c.) CRC célja, algoritmusa (3 p)
d.) rövidített kód, kódrövidítés (3 p)

3. Tekintsük a következő rejtjelezést. A nyílt szövegek, a rejtett szövegek halmaza, illetve a kulcsok halmaza rendre{A,B}, {a,b,c}, illetve {1,2,3,4}. A kulcsokat egyenletesen véletlenül sorsoljuk. A kódolás az alábbi táblázat szerinti:

k	Ek(A)	Ek(B)
1	a	c
2	c	b
3	c	a
4	b	c

A nyílt szöveg tetszőleges, rögzített bináris eloszlással sorsolt.
a.) Tökéletes rejtjelezés definíciója? (3 p)
b.) Tökéletes-e a rejtjelezés? (4 p)

4.) Tömören, formálisan fejtse ki :
a.) Egyirányú függvény és jelszóbiztonság. Szótáras jelszófejtés (3p)
b.) A nyilvános kulcsú rejtjelezés elve (3p)
c.) Kriptográfia segítségével megvalósítható főbb biztonsági szolgáltatások (3 p)

5.
a.) Az optimális prefix kódok tulajdonságai (3 p)

b.) Legyen $n = 5$ és $p(x1) = 0{,}35$; $p(x2) = 0{,}2$; $p(x3) = 0{,}2$, $p(x4) = 0{,}15$; $p(x5) = 0{,}1$,
b1.) Adja meg a Huffman-kódot. (3p)
b2.) Adja meg az átlagos kódszóhosszat. (2p)
b3.) Viszonyítsa azt az optimumhoz: belül van-e 5%-on az eltérés? (3p)

6. Tömören, formálisan fejtse ki:
a.) egyértelműen dekódolható betűnkénti kódolás (3 p)
b.) alsó és felső korlát betűnkénti kódszóhosszra egyértelműen dekódolható blokk kódok esetén (4 p)
c.) Max-Lloyd feltételek (3 p)

Pontozás: 1: <=22 2:23- 30 3: 31 - 40 4: 41- 50 5: 51-62

Kódolástechnika ZH eredmények

2007. november 30.

(Ügyeljen a pontos fogalomhasználatra, pontos, formális definíciókra, részletes indoklásokra!)

Név:
.....

Neptun kód:
.....

1.

a.) (2p) G=

b.) (2 p) d=

c.) (3p) C kód szindróma dekódolási táblázata

s		e	
0	000		
1	001		
2	010		
3	011		
4	100		
5	101		
6	110		
7	111		

d.)) (3p) Pe_jav =

e.) (3p) Pe_det =

2. (3+3+3+3p) a. b. c. d. (karikázza be, amire válaszolt)

3. (3p) a.)

b.) (4 p) Tökéletes-e az adott rejtjelezés: igen nem

4. (3+3+3p) a. b. c. (karikázza be, amire válaszolt)

5. (3p) a. (karikázza be, ha válaszolt)

b1.) (3p) A kód:

b2.) (2p) átlagos kódszóhossz=

b3.) (3p) igen nem (optimum=)

6. (3+4+3p) a. b. c. (karikázza be, amire válaszolt)

Kódolástechnika ZH megoldások

2006. december 14.

1.

a.) G = $\begin{pmatrix} 10111 \\ 01101 \end{pmatrix}$

b.) C kódszavai: 00000 , 10111 , 01101, 11010

w_min= d_min= 3

c.) C kód szindróma dekódolási táblázata H mátrix alapján

	s		e	
0	000	|	00000	|
1	001	|	00001	|
2	010	|	00010	|
3	011	|	00011	| *
4	100	|	00100	|
5	101	|	01000	|
6	110	|	10001	| *
7	111	|	10000	|

* nem egyértelmű

d.)) Pe_jav = $1-((1-p)^5+5p(1-p)^4+2p^2(1-p)^3)$ (szindróma dek. tábl. alapján)

e.) Pe_det = $2p^3(1-p)^2+p^4(1-p)$ (nemzérus kódszavak halmaza alapján)

2. Definiálja a következőket:

a.) Hibajavító kód perfekt, ha a Hamming korlát egyenlőséggel teljesül.

A Hamming-korlát nembináris esetben a következő alakot ölti:

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^{n-k}$$

(q=2 bináris alakú korlát is elfogadható megoldás)

b.) C(n,k,d) lineáris ciklikus blokk kódot tekintünk, g(x) generátorpolinommal.

2.24. definíció. *Egy $g(x)$ generátorpolinomú lineáris, ciklikus kód esetén a*

$$h(x) = \frac{x^n - 1}{g(x)}$$

polinomot ***paritásellenőrző polinom****nak nevezzük.*

2.18. tétel. *Egy lineáris, ciklikus kódra $c(x)$ akkor és csak akkor kódszópolinom, ha*

$$c(x)h(x) = 0 \mod (x^n - 1)$$

és

$$\deg(c(x)) \leq n - 1.$$

c.) CRC képzés egy hibadetekciós algoritmus, ahol

g(x) CRC polinom, fokszáma m
u(x) üzenetpolinom

a hibadetekciós kód kódszava (polinom alakban):

$c(x)= x^m u(x)$ - CRCC,

ahol

$CRCC= x^m u(x) \bmod g(x)$

d.) rövidített kód (3 p)

Egy $C(n,k)$ kód **rövidítésével** egy $C(n-i,k-i)$, $1 \leq i < k$ kódot kapunk olyan módon, hogy a $C(n,k)$ szisztematikus kód kódszavai közül csak azokat hagyjuk meg, amelyek az első i karakterén zérust tartalmazó üzenetekhez rendeltek. Ekkor a $C(n,k)$ kód i karakterrel történő rövidítéséről beszélünk. Mivel a rövidített kód kódszavai a $C(n,k)$ kód kódszavai is egyben, ezért a rövidített kód minimális távolsága legalább akkora, mint az eredeti kódé volt. Praktikusan természetesen a kódoló és a dekódoló úgy van kiképezve, hogy az első i zérus karaktert nem is továbbítjuk, s a dekóder zérusnak tekinti azokat. A kódrövidítés elsődleges célja a kódhossznak az alkalmazásbeli paraméterekhez való igazítása.

3. a.) Nyílt illetve a rejtett szöveget modellező valószínűségi változók függetlenek.

b.) Tökéletes a rejtjelezés, mivel a rejtett szöveg v.v. független a nyílt szöveg v.v.-tól:
P(y=a | x=A)= P(y=a | x=B)=1/4,
P(y=c | x=A)= P(y=c | x=B)=1/4,
P(y=b | x=A)= P(y=b | x=B)=1/2

4.) Tömören, formálisan fejtse ki

a.) **Egyirányú függvény**, azaz olyan $h(x)$ függvény, hogy x ismeretében $y=h(x)$ *könnyen* számolható, de adott y-hoz a megfelelő x meghatározása *nehéz probléma* (egyik irányban könnyű kiszámolni, a másikban viszont nagyon nehéz).

Szótár alapú támadás: A felhasználók által választott értelmes jelszavak esetén jobb támadás van a brute-force-nál, ugyanis ilyenkor nem is szükséges az összes lehetséges alternatívát végigpróbálgatni, elég egy megfelelően összeállított szótárból vett kifejezéseket vizsgálni. Ha az üzenettér kicsi és predikálható, akkor a támadó előre elkészítheti egy szótárt rejtelezve minden nyílt szöveget

b.) Az ***aszimmetrikus kulcsú titkosításnál*** a kódoláshoz és a dekódoláshoz nem ugyanazt a kulcsot használják, hanem a kódoló és dekódoló kulcs egy kulcspárt alkotnak. A két kulcs szorosan összetartozik (egy kulcsnak pontosan csak egy párja létezik), ám ezek egymásból mégis kiszámíthatatlanok (vagy nagyon nehezen kiszámíthatóak). Ezt a különleges kapcsolatot a kulcspárt létrehozó eljárás garantálja. A kódoló kulccsal kódolt üzenetet a hozzá tartozó dekódoló kulcs segítségével lehet dekódolni.

c.) – bizalmasság
– hitelesség
– sértetlenség
– letagadhatatlanság

5a. jegyzet 4.4. pont, 4.4. tétel

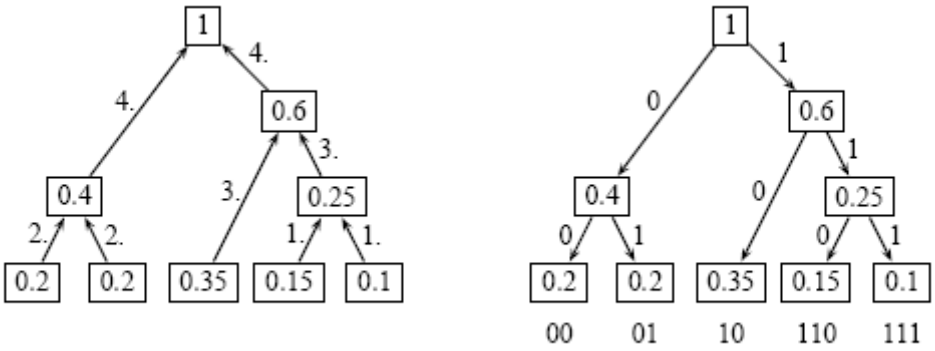
4.4. tétel. *Ha az* $f : \mathcal{X} \to \{0,1\}^*$ *prefix kód optimális, és* $\mathcal{X}$ *elemei úgy vannak indexelve, hogy* $p(x_1) \geq p(x_2) \geq \cdots \geq p(x_{n-1}) \geq p(x_n) > 0$, *akkor feltehető, hogy* f*-re a következő három tulajdonság teljesül:*

a) $|f(x_1)| \leq |f(x_2)| \leq \cdots \leq |f(x_{n-1})| \leq |f(x_n)|$, *vagyis nagyobb valószínűségekhez kisebb kódszóhosszak tartoznak.*

b) $|f(x_{n-1})| = |f(x_n)|$, *vagyis a két legkisebb valószínűségű forrásbetűhöz tartozó kódszó egyenlő hosszú.*

c) *Az* $f(x_{n-1})$ *és az* $f(x_n)$ *kódszavak csak az utolsó bitben különböznek.*

5b.



átlagos kódszóhossz: E(|f(X)|)=2.25
entrópia: H(X)=2.20161
alapján csak 2.2%-kal nagyobb az optimumnál

6. a.)

4.1. definíció. *Az $f : \mathcal{X} \to \mathcal{Y}^*$ kód* ***egyértelműen dekódolható****, ha minden véges kódbetűsorozat legfeljebb egy közlemény kódolásával állhat elő, azaz ha* $\mathbf{u} \in \mathcal{X}^*$, $\mathbf{v} \in \mathcal{X}^*$, $\mathbf{u} = u_1 u_2 \dots u_k$, $\mathbf{v} = v_1 v_2 \dots v_m$, $\mathbf{u} \neq \mathbf{v}$, *akkor* $f(u_1)f(u_2)\dots f(u_k) \neq f(v_1)f(v_2)\dots f(v_m)$. *(Itt az $f(u)f(u')$ a két kódszó egymás után írását [konkatenáció] jelenti.)*

MEGJEGYZÉS:

a) Az egyértelmű dekódolhatóság több, mint az invertálhatóság. Ugyanis legyen $\mathcal{X} = \{a,b,c\}, \mathcal{Y} = \{0,1\}$ és $f(a) = 0, f(b) = 1, f(c) = 01$. Ekkor az $f : \mathcal{X} \to \mathcal{Y}^*$ leképezés invertálható, viszont a 01 kódszót dekódolhatjuk $f(a)f(b) = 01$ szerint *ab*-nek, vagy $f(c) = 01$ szerint *c*-nek is.

b.) (nem triviális) alsó és átlagos korlát betűnkénti kódszóhosszra blokk kódok esetén (3 p)

A betűnkénti átlagos kódszóhossz definíciója értelemszerűen módosul a blokkkódolás esetében: a kódszóhossz várható értékét el kell osztani az egy blokkot alkotó forrásbetűk számával, vagyis a betűnkénti átlagos kódszóhosszon a következő mennyiséget értjük:

$$\frac{1}{m}\mathbf{E}|f(\mathbf{X})| = \frac{1}{m}\sum_{\mathbf{x}\in\mathcal{X}^m} p(\mathbf{x})|f(\mathbf{x})|$$

Értelemszerűen a 4.1. tétel állítása blokk-kódolás esetén is igaz:

$$\frac{1}{m}\mathbf{E}|f(\mathbf{X})| \geq \frac{\frac{1}{m}H(\mathbf{X})}{\log s}.$$

Másrészről a 4.3. tételből következik, hogy a Shannon–Fano-kódra

$$\frac{1}{m}\mathbf{E}|f(\mathbf{X})| \leq \frac{\frac{1}{m}H(\mathbf{X})}{\log s} + \frac{1}{m}.$$

c.) Max-Lloyd feltételek (5 p)

1. Legközelebbi szomszéd feltétel:
   A kvantálási intervallumok határait éppen a kvantálási szintek által kijelölt szakaszok felezőpontjai adják, vagyis

$$y_i = \frac{x_i + x_{i+1}}{2}, \qquad i = 1,2,\ldots,N-1.$$

2. Súlypont feltétel:
   Minden x_i kvantálási szint a $\mathcal{B}_i$ kvantálási intervallumnak a súlypontja, azaz

$$x_i = \frac{\int\limits_{\mathcal{B}_i} x f(x)\,\mathrm{d}x}{\int\limits_{\mathcal{B}_i} f(x)\,\mathrm{d}x}, \qquad i = 1,\ldots,N.$$

A Lloyd–Max-feltételt kielégítő kvantálót Lloyd–Max-kvantálónak nevezzük. Ha egy kvantáló nem elégíti ki a Lloyd–Max-feltétel bármelyik részét, akkor lehetséges egy olyan kvantálót készíteni, amelynek négyzetes torzítása kisebb, tehát egy nem Lloyd–Max-kvantáló nem lehet optimális, de létezik nem optimális Lloyd–Max-kvantáló is.