KÓDOLÁSTECHNIKA ZH

2006. december 14.

1. Hibakontroll kódolást tekintünk. Egy C bináris (nemlineáris) blokk kódban csak két kódszó van: 101101 és 011110.
a.) Adja meg a kód n, k, d paramétereit! (2 p)
b.) Legyen p a bithibázás valószínűsége az emlékezetnélküli BSC(p) csatornán. Adja meg detekciós célú C kód hibavalószínűségét! (3 p)
c.) Tekintsük a legkisebb méretű C* bináris lineáris kódot, amely tartalmazza C kódszavait. Adja meg C* kód

c1.) kódszavait (3 p)

c2.) G* szisztematikus generátormátrixát és H* szisztematikus paritásellenőrző mátrixát. (4 p)

d.) Definiálja az perfekt kód fogalmát. (2 p)
e.) Perfekt-e a C kód? (4 p)
f..) Adja meg a C* kód szindróma dekódolási táblázatának első 8 szindróma-hibavektor pár bejegyzését a hibavektor súlya szerint monoton növekvően. (4p)

2. Definiálja a következőket:
a.) MDS tulajdonságú kód (2 p)
b.) lineáris ciklikus bináris blokk kód (2 p)
c.) CRC (3 p)
d.) átfűzéses kód (3 p)

3. Tekintsük a következő rejtjelezést. A nyílt szövegek, a rejtett szövegek halmaza, illetve a kulcsok halmaza rendre {a,b}, {1,2,3,4}, illetve {k1,k2,k3,k4}. A kódolás az alábbi táblázat szerinti (pl. Ek3(a)=3).

	a	b
k1	1	2
k2	2	4
k3	3	1
k4	4	3

A {k1,k2,k3,k4} kulcsokat a P_k= {2/5, 1/5, 1/5, 1/5} eloszlás szerint sorsoljuk, továbbá P(a)=P(b)=1/2.
a.) Mekkora a valószínűsége, hogy egy rejtjelezett üzenet páros szám? (2 p)
b.) Mikor tökéletes egy rejtjelezés? Tökéletes-e az adott rejtjelezés? (8 p)

4.) Tömören, formálisan fejtse ki :
a.) Nyilvános kulcsú rejtjelezés elve. (2 p)
b.) A kulcstanúsítvány és biztonsági szerepe. (3 p)
c.) Kihívás és válaszvárás elve (egy példaprotokollon bemutatva) (5 p)

5. a.) Adja meg az alábbi sorozat LZW kódoltját és a felépített szótár: aaaaabbbbb (8 p)
b.) 64 karaktert tartalmaz a forrás abc, 256 a maximalizált szótárméret. Hány %-ra tömörítettük a megadott sorozatot? (bináris méreteket vessen egybe) (2p)

6. Tömören, formálisan fejtse ki:
a.) egyértelműen dekódolható adattömörítő kód (2 p)
b.) felső korlát az átlagos betűnkénti kódszóhosszra Shannon-Fano kód esetén (3 p)
c.) Max-Lloyd feltételek (3 p)

Pontozás: 1: <=24 2:25- 34 3: 35 - 45 4: 45- 54 5: 55– 70

Kódolástechnika ZH eredmények

2006. december 14.

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

Név: .....

Neptun kód:
.....

1.

a.) (2 p) n= k = d= b.) (3 p) Pe=

c.) (3p) C* kódszavai:

(4p) G* = H* =

d.) (2p) Perfekt kód:

e.) (3p) Perfektség (C kód): igen nem indoklás

f..) (5p) C* kód szindróma dekódolási táblázatának első 8 szindróma-hibavektor pár bejegyzése

s	e
0	
1	
2	
3	
4	
5	
6	
7	

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

3. (2p) a.) P=

b.) (8p) Tökéletes rejtjelezés:

Tökéletes-e az adott rejtjelezés: igen nem

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

5. (8p) a.) LZW kódszó:
Szótár:

b.) tömörítés = %

6. a. b. c. (karikázza be, amire válaszolt)

Kódolástechnika ZH megoldások

2006. december 14.

1.

a.) (2 p) n=6 k =1 d= 4

b.) (3 p) $Pe=p^4(1-p)^2$

c.) (3p) C* kódszavai: 000000 , 101101 , 011110, 110011

(4p) $G^* = \begin{matrix} 101101 \\ 011110 \end{matrix}$ $H^* = \begin{matrix} 111000 \\ 110100 \\ 010010 \\ 100001 \end{matrix}$

d.)

e.) (3p) Perfektség (C kód): igen <u>nem</u> indoklás: $1+ n (= 7) < 2^{n-k} (=32)$

f..) (5p) C* kód szindróma dekódolási táblázatának első 8 szindróma-hibavektor pár bejegyzése

	<u>s</u>	<u>e</u>
0	0000	000000
1	0001	000001
2	0010	000010
3	0100	000100
4	1000	001000
5	1110	010000
6	1101	100000
7	0011	000011

3. (2p) a.) P= 1/2 (1/5+1/5) + 1/2 (2/5 + 1/5) =1/2

b.) (8p) Tökéletes rejtjelezés:

Tökéletes-e az adott rejtjelezés: igen <u>nem:</u> pl. P(1|a) > P(1|b)

5. LZW kódszó: 1 3 3 2 6 6
Szótár:
1 a
2 b
3 aa
4 aaa
5 aab
6 bb
7 bbb
b.) tömörítés: 6*8 / 10*6 → 80%

2. Definiálja a következőket:
a.) MDS tulajdonságú kód (2p)

Egyenlőséggel teljesül a Singleton korlát: d=n-k+1
Pl. Reed-Solomon kód

b.) lineáris ciklikus bináris blokk kód (2 p)
bináris lineáris: zárt a kódszavak összeadására
ciklikus: zárt a ciklikus forgatásra

c.) CRC (3 p)
hibadetekciós eljárás,

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

CRC a következő kódszót generálja (polinom alakban):
$c(x)= x^m u(x)$ - CRCC, ahol
$CRCC= x^m u(x) \bmod g(x)$

d.) átfűzéses kód (3 p)
C kód m-szeres kódátfűzésével eredményeképp kapott kódszó generálása:
C m kódszavát soronként mátrixba rendezzük, majd oszloponként olvassuk a csatornába
alkalmazás: hibacsomó javítás

4.) Tömören, formálisan fejtse ki :
a.) Nyilvános kulcsú rejtjelezés elve.
Egy B felhasználó egy saját kulcspárt kap, amelynek egyik elem nyilvános a résztvevő titkos kulcsa. Az adott nyilvános kulccsal bárki küldhet rejtjelezett üzenetet B-nek, amit csak B tud dekódolni.

b.) A kulcstanúsítvány és biztonsági szerepe.
A kulcstanúsítvány lényege a nyilvános kulcs tulajdonosa azonosítójának és a nyilvános kulcsnak a biztonságos összekapcsolása, amit digitális aláírással képezünk. A digitális aláírást egy megbízható harmadik fél (CA) adja.
Pl. Egy támadó nem képes saját nyilvános kulcsát másénak elhitetni, hogy ezáltal egy másnak szánt üzenet ő dekódolhasson.

c.) Kihívás és válaszvárás elve (egy példaprotokollon bemutatva)
Lásd elektronikus jegyzet 120 oldal alján (parnerhitelesítés)

6. Tömören, formálisan fejtse ki:
a.) egyértelműen dekódolható adattömörítő kód
Lásd elektronikus jegyzet 142 oldal 4.1.def.

b.) felső korlát az átlagos betűnkénti kódszóhosszra Shannon-Fano kód esetén
Lásd elektronikus jegyzet 142 oldal 4.3. tétel

c.) Max-Lloyd feltételek
Lásd elektronikus jegyzet 186 oldal