Kódtech levlist kérdések válaszok pótzéhára

Q *error trapping algorithm Ezt tudja valaki mi? a burst hibas dolog (kodatfuzes?)*

A *ennek az a lényege, hogy: u(x)-et hozzáadjuk g(x)-hez egy balra shiftelő shiftregiszteres architektúrán (picit bonyolultabb IRL), átküldjük a csatornán, majd vételi oldalon egy jobbra shiftelő shiftregiszteres architektúra kiköpi e(x)-et egy az egybe, amit mod2-vel hozzáadsz g(x)hez, és megkapod u(x)-et.*

Q *Sziasztok! Az lenne a kérdésem, hogy az RS kód valóban olyan-e, hogy ha aszondják, h csináljam GF(q)-ban, akkor zseniálisan generátormátrixolok a maximális primitívelem hatványaival, ha meg aszondják h GF(2^m), akkor ciklikus mivoltából az irreducibilis polival betolok egy laza generátorpolinomot? A kérdés konkrétan arra irányul, hogy ezek teljesen ugyanolyan RS-kódok-e, nincs specializáló nevük, akármi, ami a testen kívül megkülönbözteti őket?*

A *ha az a mondás, hogy GF(8)-ban okoskodj össze egy RS kódot (mondjuk n = 7 és k = 5 esetén), akkor ezt használhatod:*

$$g(x) = \prod_{i=1}^{n-k(2)} (x-y^i)$$

$$h(x) = \prod_{i=n-k+1(3)}^{7} (x-y^i)$$

Q ***LZ77***, ***LZ78*** *igen,* ***LZW*** *nem, Sima / Adaptív, Huffman / Shannon szerintem lehet, ha csak elméleti kérdés szintjén is. Ezek mik?*

A http://en.wikipedia.org/wiki/LZ77_and_LZ78 ***LZ78*** *példa van a múlt órán megoldott példafeladatok közt.* ***LZ77****-et szerintem nem csináltunk gyakorlatban. Elég sok a különbség, a* ***LZ77*** *az előre meg hátra bufferelős móka, míg a* ***LZ78*** *a szótárazós. http://www.crysys.hu/courses/kodolastechnika/bscinfkod.pdf -> 177. oldal* ***LZ77*** *kódra példa*

Q *Szeretnem megkerdezni, hogy ebben a feladatsorban(1.oldalon) hogy szamolodnak ki a Es-k, illetve a csoportvezeto? Illetve hogy szamitunk hibajavito kepesseget? link: http://neural.hit.bme.hu/kodtech/fileok/Kodtech.ppt*

A *Íme:*

1, *kiszámoljuk az összes c kódszóvektort*

2, *Intuitive (H oszlopainak lin. kombinációjával) meghatározzuk azt az e vektort,ami a megadott szindrómavektort adja. Itt például a 00001 jó mert,az a H oszlopai közül csak utolsó engedi ki, és abból lesz így (0,1)*

3, *ehhez hozzáadjuk az összes c kódszót,ebből lesz Es,(úgye e elem Es, és e+ c is eleme Es) a megkapott vektorok közül, a legkisebb súlyú a vezető,azaz önmaga*

Egy hibacsoportba annyi kódszó tartozik, ahány hibavektor van

Q *A http://www.crysys.hu/courses/kodolastechnika/zh071130.pdf dolgozat 1. feladatának d) és e) része hogy jön ki?*

A *Miután meghatároztad a szindróma táblázatot, abból kijön a groupleader.(e), annak a súlya w(e) Annak a hibavalószínűsége = $p^{w(e)}*(1-p)^{(n-w(e)}$ A detektációs valószínűség pedig szerintem: Korábban kijött dmin,abból minusz egy a detektálható hibák száma,és arra egy Binomiális eloszlásfüggvénye kell és kész.*

Q2 *Ezt értem is, csak azt nem, hogy az egyes tényezők együtthatója miért pont annyi, amennyi: 5, 2, ill 1. Pl. a hibadetektálásnál mintha abból akarná kihozni, hogy a kódoláscsak 2 hibát tud jelezni, ezért összeadta azokat a valószínűségeket, amikor 3 vagy 4 hiba keletkezik: $2*p^3*(1-p)^2 + p^4*(1-p)$. De az előbbit miért szorozza 2-vel, utóbbit meg csak 1-gyel? Illetve nem kéne még a p^5-t is hozzávenni, vagyis amikor 5 hiba van?*

A2 *mert 5 db van abbol a tipusbol, 2 a masikbol stb, nezd meg a szindroma tablazatot.*
Az e) resz meg ugy van, hogy akkor nem tudunk detektalni egy hibat, ha olyan a hiba, hogy a vett vektor egy kodszovektor lesz. De ekkor a hibavektor vagy csupa 0 (ekkor ugy nincs is hiba, ezt nem kell belevenni) vagy egy kodszovektor, hiszen a kodunk linearis ket kodszo osszege is kodszo. Tehat a hibavektor most eppen haromfele lehet, mert harom nem csupanulla kodszavunk van, ezeket adja ossze (peldaul 2 db 3 sulyu kodszo van es egy db 4 sulyu).

Q *a http://neural.hit.bme.hu/kodtech/fileok/Kodtech.ppt dia utolsó oldalán a v=1100101 vektor azért nem lehet kódszó, mert ennek előállításához a generátormátrix első két sorát kéne összeadni, de így meg 1100010 jönne ki, vagyis az utolsó 3 paritásbit nem egyezik?*
A feladat a megoldást máshogy csinálta: kiszámolta az ehhez tartozó szindrómavektort: 111. Ebből meg azt kéne ugye észrevenni, hogy ennek csupanullavektornak kéne lenni, akkor lehetne csak a v vett vektor kódszó?

A *A leírt megoldás szerint s valóban (111), és (000) kellene legyen ahhoz, hogy v kódszó legyen szerintem is.*

Q *$g(x) = y^3 * x^4 + y^2 * x^3 + y^6 * x^2 + x + 1$ Lehet-e ez egy **BCH**-kód generátor polinomja?*

A *Nem, mert azért nem, mert a BCH kód-nak együtthatói csak 0 és 1-ek lehetnek. Itt a megoldás: https://wiki.sch.bme.hu/pub/Infoalap/KodTech/kodtech_08-12-16_pzh.pdf*

Q *ez a feladat:*
$G =$
10110
01101
d.) Adja meg a szindróma dekódolási táblázatát.

a megoldás:
szindróma hibavektor

```
000 00000
001 00001
011 00011
100 00100
101 01000
110 10000
111 10001
```
hogy jön ez ki?

A *úgy kaptad meg a táblázatot, hogy a H mátrixot beszoroztad valamivel, hogy a 000, 001... jöjjön ki. Látszik hogy melyik az az 5 jegyű vektor, mellyel beszorozva megkapod a szindrómát. a 000-nál értelemszerűen a 00000 a hibavektor, a 001-nél csak az utolsó számjegy legyen egyes, tehát 00001 (mátrix utolsó oszlopa). 010-nál csak a második számjegy legyen egyes, tehát akkor a H mátrixban keress olyan oszlopot, ami kiadja neked a 010 kombinációt (utolsó előtti), tehát akkor szorzod 00010-al. 011-nél 00011, aztán 100-nál látszik hogy a mátrix 3. oszlopa kiadja ezt a vektort, tehát 00100-al kell megszorozni, és így tovább, valami hasonló logika alapján. Remélem érthető volt nagyjából.*

A2 *Hát én bruteforce-al meg tudom csinálni :)* (by Koczka)
> `G =`
> `10110`
> `01101`
Akkor n = 5, k = 2
Beszorzod, 00, 01, 10, 11-gyel, kijönnek a kódszavak: 00000, 01101, 10110, 11011
Szindrómákat pedig, veszed a hibavektorokat így sorban: 00000 (ez igazából nem hiba), 00001, 00010, 00100, 01000, 10000, 00011, 00101, ...
Összeszorzod a H-val és akkor kijön a szindróma és annak megfelelő sorba felírod. Hozzáadod az összes kódszót fentebbről. Amikor a következő hibavektorral próbálkoznál akkor meg már vigyázol, hogy ha már a táblázatban benne van, akkor ne is szorozgassad, mert felesleges, úgyis azt a szindrómát adná ki. H-t persze a szokásos, transzponálós módszerrel felírod...

Q *hogyan határozzuk meg a csoportvezetőt?*

A *legkisebb súlyú (lehet több is)*

Q *egy **GF(7)** RS kódnál, ahol nincs meghatározva, hogy melyik primitívet vegyük alapul, mindegy, hogy mivel számolunk, vagy pedig a legnagyobbat KELL választani (ez esetben 5öst)?*

A *legnagyobbat, íme egy példa:*
Szerintem GF(p), most p = 7 esetén fogod és 6tól 2ig mész lefele, amíg jót nem találsz.
Jó akkor lesz, ha csak akkor ad 1-et, ha (p - 1)dikre emeled (tehát p - 1 nél kisebb értékre nem).

*A hatványozást pedig érdemes lépésenként, mindig modulust véve **p**-vel elvégezni.*
Példa:
*6*6 = 36 mod 7 = 1 <-- $6^2 = 1$, $2 \neq 7 - 1$*
*5*5 = 25 mod 7 = 4*
*4*5 = 20 mod 7 = 6*
*6*5 = 30 mod 7 = 2*
*2*5 = 10 mod 7 = 3*
*3*5 = 15 mod 7 = 1 <-- $5^6 = 1$ 6 = 7 - 1, tehát jó az **5***
*4, 3, 2-re nyilván nem nézzük meg, ha a legnagyobbat kerestük, ami az **5***

Q *ez alapján akkor mi a **GF(8)**-nak a primitív eleme? (lásd előző kérdés)*

A *itt nem működik a brute force, mert 8 nem prímszám - egy pdf: http://www.math.uic.edu/~leon/mcs425-s08/handouts/field.pdf sztem itt látszik h a **7** primitiv elem*
A2 *Ellenben prímhatvány, amikor ez az egész máshogy működik. Ott fel kell írni egyenletes formába és nem primitív elem lesz, hanem irreducibilis polinom, ami amúgy a $x^3 + x + 1$ lesz. Én így tudom, de ez a polinomos móka még nekem se kristály tiszta teljesen, szóval hülyeséget nem akarok írni.*
A3 *ajánlom a jegyzet **26-28-adik** oldalait*

Q *a kódtech zh 2008 12 04-es 5. feladatában a 4-es az mér lett y^2??*

A *ott a hatványtábla. a 4 binárisan:* `100` *ebből az 1-esek "választják ki" hogy a polinomokból mi "kell" : $y^2 + y + 1$ és ha összeveted a* `100`*-al marad y^2*

Q *a GF testeken belüli elemek szorzását értem, de mikor SHR-be kell pakolni, hogy kell felírni azt az alfa0*y + $alfa_1$*y^1 + $alfa_2$*y^2 cuccot? mármint mi alapján? évközben előadáson felírtuk hogy 2*alfa hogy jön ki meg 4*alfa. alfa a GF beli primitív elemet jelenti ez esetben? vagy csak úgy jelölte a szorzat másik tényezőjét éppen..? ha "csak úgy" akkor viszont az alfákat nem tudom mi alapján írjuk fel:/*

A *Az az **ALFA** mindig a primitív elemet jelenti az adott testen belül.*
*A2 a SHR-es implementációnál mindig felírjuk általános alakban a szorzatot: (a_0 + a_1*x^1 + ... + a_n*x^n) * konstans, ahol a zárójelben (ami eddig mindig **alpha** volt) az adott test irreducibilis polinomja áll a_0,a_1....a_n együtthatókkal, ezek lesznek az egyes SHR-ek kezdeti értékei. Az konstans pedig a konkrét szám, amivel megszorzod az "**alpha**"-t. Ezt a számot meg át kell írni a "testnek megfelelő" alakba.*

---

simple help, no question:

Egy korábbi előadáson felírtuk a **GF(7)** hatványtábláját,és onnan jöttünk rá a max. primitív elemre

elem	1	2	3	4	5	6	rend	
1	1	1	1	1	1	1	1	
2	2	4	1				3	
3	3	2	6	4	5	1	6 <-	primitív elem
4	4	2	1				3	
5	5	4	6	2	3	1	6 <-	primitív elem
6	6	1					2	

Azt, hogy a rendek miért így jönnek ki,és azok miért primitív elemek, azt a bsz2 tárgyalta.
A szorzások persze mod 7 -ben történnek.

Q *Ha lehet kimerítő kulcskeresni, akkor megfejthető-e a nyílt szöveg? Hogyan?*

A *A nyílt üzenet szerintem megfejthető, ha megjegyzed az egészet, és tetszőleges n. blokk visszafejthető, ha n+1 és n+2 blokkot összeadod. (Persze a végéről kell kezdeni rekurzívan.)*

A kérdések és válaszok összeállítása a Ti kérdéseitek és segítőkész válaszaitok alapján állt össze. A lista az első ZH előtti napok lázas készülései alatt gyűlt össze, én a pótZH előtt foglaltam pdf-be☺. Mivel a ZH-m 2-es lett (nem véletlenül készülök a pótZH-ra), ezért a legjobb tudásom szerint igyekeztem összevágni a lista tartalmát (info2008), de sok helyen véthettem hibákat, vagy felejthettem el javítani.