A tárgyról ...

Alkalmazások

- "térbeli" kommunikáció (katonai, űrkutatás, internet, molbil telefon)
- "időbeli" kommunikáció (adattárolás)
- kriptográfia
- algoritmikus bonyolultságelmélet

Matematikai apparátus

- valszám, információelmélet, statisztika, sztochasztikus folyamatok
- algebra, számelmélet, algebrai geometria
- geometria (rácsok, gömbkitöltések)
- gráfok, halmazrendszerek
- stb.

Bevezető példák

- ismétlő kód: $b \mapsto (b, \ldots, b)$ (n-szer)
  $\leq n-1$ hiba esetén jelez, vagy
  $\leq \lfloor (n-1)/2 \rfloor$ hibát javít ("többségi szavazás")
- paritásbit: $(b_1, \ldots b_{n-1}) \mapsto (b_1 \ldots b_{n-1}, b_1 + \ldots + b_{n-1})$
  1 (pontosabban: páratlan sok) hiba esetén jelez
- Hamming $[7, 4, 3]$: $(b_1, b_2, b_3, b_4) \mapsto$
  $(b_1, b_2, b_3, b_4, b_1 + b_2 + b_4, b_1 + b_3 + b_4, b_2 + b_3 + b_4)$
  ≤ 2 hiba esetén jelez vagy
  1 hibát javít
  Miért? Két különböző kódszó ≥ 3 bitben tér el egymástól $\Leftrightarrow$ a két kódszó összege ≥ 3 1-est tartalmaz. Mik a két különböző kódszó összegeként előálló szavak? A linearitás miatt ezek éppen a nem 0 kódszavak.
  Feladat: Biz. be, hogy minden 7 bites szóhoz pontosan egy olyan kódszó tartozik, mely legfeljebb 1 bitben tér el.
- kiegészített Hamming $[8, 4, 4]$: $(b_1, b_2, b_3, b_4) \mapsto$
  $(b_1, b_2, b_3, b_4, b_1 + b_2 + b_4, b_1 + b_3 + b_4, b_2 + b_3 + b_4, b_1 + b_2 + b_3)$
  ≤ 3 hiba esetén jelez vagy
  1 hibát javít (és két hibát jelez)
  Miért? Az előző példa kódszavait kiegészítettük a paritásbitjükkel. Így a 3 bites kódszavai 4 bitesek lesznek.

1. Bevezetés

1.1. Kommunikációs modell

Ábra

A fizikai csatorna lehet:

- rádió
- kábel (elektromos v. optikai)
- memória
- mágnesszalag, mágneslemez, optikai lemez
- vonalkód
- stb.

1.2. A legfontosabb csatorna- illetve hibamodellek

Általános diszkrét csatorna véletlen hibával.

BSC (emlékezetnélküli) bináris szimmetrikus.

Nagyobb ábécé feletti szimmetrikus.

Additív hiba.

Törléses csatorna.

AWGN (Gauß-csatorna). Additive White Gaussian Noise. Csak megemlítve.

Csomósodó hiba.

1.3. Blokk-kódok és alapvető paramétereik

Blokk kód. (n, M)-kód F fölött:

$$C \subseteq F^n$$

- F=kódábécé
- $n =$ **kódhoszz**
- $M = |C| =$**kódméret**
- $k = \log_{|F|} M =$"dimenzió", "információ-hossz"
- $R = k/n =$**kódsebesség** (coding rate,information rate), n/k=(relatív) redundancia

Hamming-távolság. F^n-ben:

$$d(x, y) = \#\{i | 1 \leq i \leq n, x_i \neq y_i\}$$

tényleg távolság:

- $d(x, y) \geq$
- $d(x, y) = 0 \Leftrightarrow x = y$
- $d(x, y) = d(y, x)$ - Szimmetria
- $d(x, z) \leq d(x, y) + d(y, z)$ - Háromszög-egyenlőtlenség

kódtávolság. (minimum distance, minimális távolság) $d = \min_{x,y \in C} d(x, y) \longrightarrow (n, M, d)$-kód.

Példák

- ismétlő kód: $k = 1, R = 1/n, d = n$
- paritásbit: $k = n - 1, R = 1 - 1/n, d = 2$
- Hamming $[7, 4, 3]$: $k = 4, R = 4/7, d = 3$
- kiegészített Hamming $[8, 4, 4]$: $k = 4, R = 1/2, d = 4$

1.4. Kódolás

általában nem nehéz.

1.5. Dekódolás

legfontosabb részfeladat:

$$D : F'^n \to C$$

($F' =$ output ábécé, gyakran $F' = F$.)

ML-dekódolás. (maximum likelihood decision) $D(x) =$ azon c kódszó, amely maximalizálja a

$$P(\text{kimenet} = x | \text{bemenet} = c)$$

(röviden $P(x|c)$) feltételes valószínűséget.

ML-dekódolás BSC-re.

$$P(x|c) = \prod_{i=1}^{n} \begin{cases} 1-p & \text{ha } x_i = c_i \\ p & \text{ha } x_i \neq c_i \end{cases} = (1-p)^n (p/(1-p))^{d(x,c)}$$

annál nagyobb, minél kisebb $d(x,c)$. Tehát a szabály szerint x-hez a Hamming-távolság szerinti (egyik) **legközelebbi kódszót** kell választani.

MAP-dekódolás. (maximum a posteriori decision) $D(x)$ = azon c kódszó, amely maximalizálja a

$$P(\text{bemenet} = c | \text{kimenet} = x)$$

(röviden $P(c|x)$) feltételes valószínűséget. Ekkor lesz a legkisebb a hiba valószínűsége. Ha minden kódszó egyforma valószínűséggel fordul elő, ugyanazt adja, mint a ML, mert $P(c|x) = P(x|c)P(c)/P(x)$.

"szuboptimális" dekódolások. Cél: "elég sok" esetben legyen jó.

dekódolás korlátos távolságra. (bounded distance decoding) Adott t-re $D(x)$ =az x-től $\leq t$ távolságra levő kódszó, ha van egy egyértelmű ilyen. Egyébként $D(x)$ = "hiba".

t **hiba javítása.** (t-error correction) $t \leq \lfloor (d-1)/2 \rfloor$-re a fenti. (Tipikusan $t = \lfloor (d-1)/2 \rfloor$.)

hibajelzés. (error detection) Itt $t = 0$, tehát $D(x) = x$, ha $x \in C$ és $D(x) =$ hiba, ha $x \notin C$. Ez egy $d-1$-hibajelző dekódolás.

Feladat:. (Hibajavítás és hibajelzés egyszerre) Egy C (n, M, d)-kód esetén milyen t, t' $(t < t')$ számpárokra tudunk olyan dekódoló módszert csinálni, amely $\leq t$ hiba esetén a kódszót helyreállítja, t-nél több, de t'-nél nem több hiba esetén pedig hibát jelez? (Tehát olyan D dekódoló függvényt szeretnénk, amelyre az igaz, hogy tetszőleges $c \in C$ kódszó esetén $D(x) = c$, ha $d(x,c) \leq t$, és $D(x) =$ "hiba", ha $t < d(x,c) \leq t'$.

2. Lineáris kódok

Konvenció:. F^n elemeit sorvektorokként írjuk. (A kódelmélet irodalmában többnyire így van.)

Definíció:. C egy lineáris $[n,k,d]$-kód (vagy $[n,k]$-kód) az $F = GF(q)$ véges test felett, ha

$$C \leq F^n \quad \text{(lineáris altér)},$$

ahol $k = \dim_F C$ és d a C $(n, |F|^k)$-kód távolsága.

2.1. Hamming-súly:

$w(x) = \#\{i | 1 \leq i \leq n, x_i \neq 0\}$.

Állítás:. $d(x,y) = w(x-y)$. Egy $C \leq F^n$ lineáris kód minimális távolsága a C-beli nem 0 vektorok minimális súlya.

2.2. Generátormátrixok

Definíció:. C egy generátormátrixa egy olyan G $k \times n$-es mátrix, amelynek sorai C egy bázisát alkotjuk.

Bázistranszformáció:. G és G' ugyanannak a kódnak generátormátrixai $\Leftrightarrow G' = BG$, ahol B egy $k \times k$ méretű reguláris mátrix ($B \in GL_n(F)$).

Egy lehetséges kódolás:. $x \in F^k \to xG \in F^n$. (Más szóval: $C = \operatorname{Im} G$.)

Példák generátormátrixokra:

- Ismétlő kód

$$(1 \dots 1)$$

- Paritásbit

$$\begin{pmatrix} 1 & & & -1 \\ & 1 & & -1 \\ & & \ddots & \vdots \\ & & 1 & -1 \end{pmatrix}$$

- Hamming $[7,4,3]_2$

$$\begin{pmatrix} 1 & & & & 1 & 1 & \\ & 1 & & & 1 & & 1 \\ & & 1 & & & 1 & 1 \\ & & & 1 & 1 & 1 & 1 \end{pmatrix}$$

Szisztematikus kódok

Szisztematikus kódolás:. Legyen $i_1, \dots, i_k$ k darab különböző koordinátapozíció. Egy kódolást az $i_1, \dots, i_k$ helyeken szisztematikusnak nevezünk, ha az üzenet jegyei a megfelelő kódszó $i_1, \dots, i_k$ helyein megjelennek:

$$(x_1, \dots, x_k) \mapsto (?, ?, x_1, ?, ?, x_2, ?, ?, x_k, ?, ?)$$

Definíció:. A C lineáris $[n,k]$-kód **szisztematikus** az $i_1, \dots, i_k$ helyeken, ha C szavait ezekre a koordinátákra levetítve minden F^k-beli szó előadódik.

Világos, hogy ha létezik C-hez az $i_1, \dots, i_k$ helyeken szisztematikus kódolás, akkor C szisztematikus ezeken a helyeken. Belátjuk, hogy ez elegendő is.

Állítás:. Legyen G a C lineáris $[n,k]$-kód egy tetszőleges generátormátrixa. Ekkor C az $i_1, \dots, i_k$ helyeken szisztematikus $\Leftrightarrow$ G-nek az i_1-edik, ..., i_k-adik oszlopai lineárisan függetlenek.

Biz.: Feltehető, hogy $i_1 = 1, \dots, i_k = k$. Legyen $G = (G_0|G_1)$ alakú, ahol G_0 az első k oszlopból álló részmátrix. Ekkor $C = \{xG|x \in F^k\} = \{(xG_0|xG_1)|x \in F^k\}$, tehát C szavai levetítve az első k helyre a G_0 mátrix képterét adját. Ez nyilván akkor és csak akkor a teljes F^k, ha G_0 reguláris.

Következmény:. A C lineáris kódnak akkor és csak akkor van szisztematikus kódolása az $i_1, \dots, i_k$ helyeken, ha C szisztematikus ezeken a helyeken.

Biz.: $\Rightarrow$: Világos.
$\Leftarrow$: Feltehető, hogy $i_1 = 1, \dots, i_k = k$. Az előző állítás alapján C egy tetszőleges G generátormátrixa $(G_0|G_1)$ alakú, ahol G_0 reguláris $k \times k$-as. Ekkor az $x \mapsto xG_0^{-1}G$ kódolás szisztematikus.

Kódok ekvivalenciája:

Ekvivalens kódokat eredményező transzformációk:
Szűkebb értelemben: a koordináták felcserélése: $x \mapsto xP$, ahol P egy $n \times n$-es permutációmátrix.
Lineáris kódokra még szokás: a koordináták szorzása F^*-beli elemekkel: $x \mapsto xD$, ahol D egy $n \times n$-es reguláris diagonális mátrix.
Tágabb értelemben (a fenti 2 féle együtt): $x \mapsto xM$, ahol M egy $n \times n$-es monomiális mátrix. (Minden sorban és minden oszlopban pont 1 nem nulla elem.)
Generátormátrixra: a G és a BGM mátrixok ekvivalens kódokat generálnak,
ahol $B \in GL_k(F)$ (bázistranszformáció, a kódot nem változtatja); M egy $n \times n$-es monomiális mátrix (ekvivalens kódot ad).

2.3. Ellenőrző (paritásellenőrző) mátrixok:

C egy lehetséges másik megadása egyenletekkel.

Definíció:. C egy **ellenőrző mátrixa** egy olyan H $(n-k) \times n$-es mátrix, amelyre $C = \operatorname{Ker} H^T$, azaz:

$$x \in C \Leftrightarrow xH^T = 0.$$

Kapcsolat a duális kóddal

skalárszozat F^n-ben:. $(x,y) = xy^t = \sum_{i=1}^{n}(x_i, y_i)$. Ez egy nemelfajuló szimmetrikus bilineáris függvény.

duális kód:. $C^\perp = \{y \in F^n | (x,y) = 0 \text{ minden } x \in C\text{-re}\}$. **alaptulajdonságok:** $\dim C^\perp = n-k$, $(C^\perp)^\perp = C$.

Állítás:. H C-nek egy ellenőrző mátrixa $\Leftrightarrow$ H $C^\perp$-nek egy generátormátrixa.

Biz.: $\Rightarrow$: Világos, hogy H minden sora merőleges C-re. Ugyanakkor H rangja $n-k$, hiszen különben H^T magja nagyobb lenne C-nél. Tehát H sorai $C^\perp$-nek $n-k$ lineárisan független elemét, azaz $C^\perp$ egy bázisát adják. (Felhasználtuk, hogy $\dim C + \dim C^\perp = n$.)
$\Leftarrow$: Ha H sorai $C^\perp$-nek egy bázisát alkotják, akkor H^T egy olyan $n-k$ rangú mátrix, amelynek magjában C nyilván benne van. A rangfeltétel miatt H^T magja k dimenziós, tehát nem lehet nagyobb C-nél.

Példák:.

- Ismétlő kód
$$\begin{pmatrix} -1 & 1 & & & \\ -1 & & 1 & & \\ \vdots & & & \ddots & \\ -1 & & & & 1 \end{pmatrix}$$
- Paritásbit
$$(1 \dots 1)$$
- Hamming $[7,4,3]_2$
$$\begin{pmatrix} 1 & 1 & & 1 & 1 & & \\ 1 & & 1 & 1 & & 1 & \\ & 1 & 1 & 1 & & & 1 \end{pmatrix}$$

Ekvivalencia ellenőrő mátrixra:.
$$H \mapsto B'HM',$$
ahol $B' \in GL_{n-k}(F)$ (bázistranszformáció, a kódot nem változtatja); M' egy $n \times n$-es monomiális mátrix (ekvivalens kódot ad). (A generátormátrixos M-mel "összhangban" levő M'-re: $MM'^T = I_n$.)

Állítás:. Ha C szisztematikus az $i_1, \dots, i_k$ helyeken, akkor $C^\perp$ szisztematikus a maradék helyeken.

Biz.: Feltehető, hogy $i_1 = 1, \dots, i_k = k$. Legyen H $C^\perp$ egy generátormátrixa. Be kell látni, hogy H utolsó $n-k$ oszlopa lineárisan független. Tegyük fel, hogy ezen oszlopok valamely lineáris kombinációja (együtthatók: $x_{n-k+1}, \dots, x_n$) nulla. Ekkor a $z = (0, \dots, 0, x_{n-k+1}, \dots, x_n)$ vektorra $zH^T = 0$, tehát $z \in C$, mivel H C-nek egy ellenőrző mátrixa. C szisztematikussága miatt C egy G generátormátrixa $G = (G_0|G_1)$ alakú, ahol G_0 reguláris. Következésképpen C elemei $yG = (yG_0, yG_1)$ alakúak ($y \in F^k$). G_0 regularitása miatt yG_0 csak akkor 0, ha $y = 0$, következésképpen $yG = 0$. Tehát $z = 0$, speciálisan az $x_{n-k+1}, \dots, x_n$ együtthatók is nullák. Tehát H hátsó oszlopai tényleg lineárisan függetlenek.

Mivel $C^{\perp\perp} = C$, valójában:

Következmény:. C akkor és csak akkor szisztematikus az $i_1, \dots, i_k$ helyeken, ha $C^\perp$ szisztematikus a maradék helyeken.

Megjegyzések:.
1. Mivel G rangja k, mindig választhatók olyan $i_1, \dots, i_k$ helyek, ahol C szisztematikus.
2. A fentiek értelmében tetszőleges C lineáris $[n,k]$ kódhoz, amely az $i_1, \dots, i_k$ helyeken szisztematikus, választható egyszerre olyan G generátormátrix és H ellenőrző mátrix, hogy G-nek az $i_1, \dots, i_k$ oszlopaiból, H-nak meg a maradék $n-k$ oszlopaiból álló almátrixa $k \times k$-as, illetve $(n-k)\times(n-k)$-as egységmátrixok. Ekvivalencia erejéig feltehető, hogy $i_1 = 1, \dots, i_k = k$. Ekkor a G szerinti szisztematikus kódolás az üzenethez (a k darab úgynevezett **információs jegyhegy** $n-k$ darab úgynevezett **ellenőrző jegy** hozzárakását jelenti, a H sorai pedig lényegében az ellenőrző jegyeket fejezik ki az információs jegyekből.

Állítás:. Legyen H a C lin. kód egy tetszőleges ellenőrző mátrixa és $s > 0$ egész. A C kód távolsága akkor és csak akkor nagyobb s-nél, ha H bármely s különböző oszlopa lineárisan független.

Biz.: Legyen x egy $t > 0$ súlyú kódszó, amelynek nem 0 jegyei $x_{i_1}, \dots, x_{i_t}$. Ekkor az $xH^T = 0$ feltétel H-nak az i_1-edik, ..., i_t-edik oszlopai között egy $x_{i_1}, \dots, x_{i_t}$ együtthatós lineáris összefüggést ad. Fordítva, ha van H-nak az i_1-edik, ..., i_t-edik oszlopai között egy $x_{i_1} \neq 0, \dots, x_{i_t} \neq 0$ együtthatós lineáris összefüggés, abból egy t súlyú olyan x szó nyerhető, amire $xH^T = 0$, azaz $x \in C$. Tehát akkor és csak akkor van legfeljebb s súlyú kódszó, ha van H-ban s lineárisan összefüggő oszlop.

Mivel H rangja $n-k$,

Következmény (Singleton-korlát lineáris kódokra):. Tetszőleges C lineáris $[n,k,d]$-kódra:
$$d \leq n - k + 1.$$

2.4. Hamming-kódok

$Hamming_q(m)$ ellenőrző mátrixának oszlopai: $GF(q)^m$-ből a lehető legtöbb páronként lineárisan független vektor ($\sim$ a $GF(q)$ feletti $m-1$ dimenziós projektív tér pontjai.) A kód paraméterei:

$$[n = \frac{q^m-1}{q-1}, k = \frac{q^m-1}{q-1} - m, d = 3].$$

A kontrukció miatt $d \geq 3$. A $d \leq 3$ közvetlenül is belátható lenne, de a következő gondolatmenet jobban mutatja a Hamming-kódok egy fontos tulajdonságát. A $Hamming_q(m)$ minden kódszavára tekintsük $GF(q)^n$ azon pontjait, amelyek az adott kódszótól legfeljebb 1 távolságra vannak, kapunk kódszavanként $1+n(q-1) = q^m$ pontot. Összesen $q^k q^m = q^{m+k} = q^n$ pontot kapunk, melyek $d \geq 3$ miatt, mind különbözőek. Azaz a kódszavak köré írt 1 sugarú "gömbökkel" lefedtük az egész $GF(q)^n$ teret: minden egyes x ponthoz **pontosan egy** $y \in Hamming_q(m)$ kódszó tartozik, melyre $d(x,y) \leq 1$. A fenti gondolatmenet általánosítható:

Tétel (Hamming- avagy gömbkitöltési korlát):. Legyen C egy (nem feltétlenül lineáris) (n, M, d)-kód a q elmű F ábécé fölött. Ekkor

$$M \leq q^n / V_q(n, \lfloor \frac{d-1}{2} \rfloor),$$

ahol

$$V_q(n,t) = \sum_{j=0}^{t} \binom{n}{j} (q-1)^j,$$

az F^n-beli t Hamming-sugarú gömb "térfogata" (pontjainak a száma).

Biz.: C minden pontja köré írjuk $t = \lfloor \frac{d-1}{2} \rfloor$ sugarú Hamming-gömböt. Ezek páronként diszjunktak, tehát $q^n = |F^n| \geq M \cdot V_q(n,t)$.

Definíció:. Az olyan C kódokat, amelyekre egyenlőség van – tehát a gömbök hézagmentesen lefedik az F^n teret, **perfekt** kódoknak nevezzük.

A Hamming-kódok a fentiek szerint perfektek.

Alkalmazás:

IBM memória (70-es évek) [J. D. Key 14.3]

Paritásbittel kiegészített Hamming-kódok:. $Hamming_2^+(m)$ úgy kapható $Hamming_2(m)$-ből, hogy a utóbbi kódszavait kiegészítjük a paritásbitjükkel. A paraméterek:

$$[n = 2^m, k = 2^m - m - 1, d = 4].$$

A használt kód:. Vegyük a $Hamming_2^+(6)$ kódot. A paraméterek:

$$n = 64, k = 57, d = 4.$$

A "hasznos" bitek száma 57, ebből 32 bitet szoktak hasznosítani (egy gépi szóhoz). A kóddal 1 hibát javítani, kettőt pedig jelezni lehet.

2.5. Szimplex kódok

Olyan (nem feltétlenül lineáris) kódok, melyekben bármely két kódszó távolsága állandó.

Bináris Hamming-kódok duális kódja. Legyen C egy a q elemű F test felett egy $[n = \frac{q^m-1}{q-1}, k = \frac{q^m-1}{q-1} - m, d = 3]$ paraméterű kód. Ekkor C egy tetszőleges H ellenőrző mátrixának bármely két oszlopa lineárisan független, tehát H oszlopai nem egymás skalárszorosai, és a passzoló paraméterek miatt valójában az F^m tér összes 0-n átmenő egyeneséből tartalmaz egy-egy nemnulla pontot. Legyen $v \in C^\perp \setminus \{0\}$ tetszőleges. Ekkor létezik C-nek olyan H ellenőrző mátrixa, amelynek v az első sora. A 0-n átmenő $\frac{q^m-1}{q-1}$ egyenes közül $\frac{q^{m-1}-1}{q-1}$ olyan van, amelynek minden pontjának az első koordinátája 0, a maradék q^{m-1} egyenes semelyik nem 0 pontjának az első koordinátája nem lesz 0. Ezért v súlya q^{m-1}. Tehát $C^\perp$ egy szimplex kód.

2.6. Dekódolás standard táblázattal/szindrómák alapján

Standard táblázat:. Sorai: C mellékosztályai (eltoltjai), soron belül a mellékosztály elemei a Hamming-súlyuk szerint nem csökkenő sorrendben rendezve. A sorok első (legkisebb súlyú) elemeit a mellékosztályok **vezérelemeinek** (coset leaders) nevezik.

A legközelebbi kódszó:. $x \mapsto c_x \in C$, ahol $w(x - c_x)$ (az egyik) lehető legkisebb. Legyen $e_x = x - c_x$ ("hibavektor"). Ekkor e_x az $x + C$ mellékosztály (egyik) legkisebb súlyú eleme, tehát választható a vezérelemnek. Ha $x + C = y + C$ (azaz $x - y = C$), akkor x-hez és y-hoz ugyanaz(ok) az e-k tartoznak.

2.7. Szindrómák

Szindróma:. xH^T. $x + C = y + C \Leftrightarrow xH^T = yH^T$. Tehát az e_x hibavektor(oka)t az xH^T szindróma egyértelműen meghatározza. Tehát elég egy $q^{n-k} \times n$ méretű táblázat.

Példa:. Létezik egy $[32, 17, 8]$ paraméterű bináris kód (a Cheng-Sloane–kód). Ezzel egy 32 bites szóban (17 helyett) 16 bites információt tárolhatunk, 3 bitnyi hibát javító (és 4 bit hibát jelző) képességgel. A szindrómák 15 bitesek, tehát a kódot egy 2^{15} darab 32 bites szóból álló, azaz egy 128 kilobájtos táblázat segítségével dekódolni tudjuk. A triviális dekódoló táblázat 8 gibagájtba fér cak el.

3. Általánosított Reed-Solomon–kódok

3.1. Maximális távolságú (MDS-) kódok

Állítás (Singleton-korlát nemlineáris kódokra):. Egy tetszőleges q-elemű ábécé feletti (n, M, d)-kódra:

$$M \leq q^{n-d+1}.$$

Biz.: Legyen C a kód. Töröljük el C kódszavaiból az utolsó $d-1$ jegyet. Mivel C-ben a kódtávolság d, nincs olyan különböző két kódszó C-ben, amelyek megegyeznek az első $n-d+1$ koordinátájukban. Tehát a fenti törlő művelet egy injektív leképezés C-ből F^{n-d+1}-be. Következésképpen $M = |C| \leq |F^{m-d+1}| = q^{n-d+1}$.

Megjegyzés:. A bizonyításban használt műveletet (egy koordináta törlése a kódszavakból) **lyukasztásnak** (puncturing) hívjuk. Általában csökkenti a kódhosszat és a kódtávolságot, a dimenziót pedig változatlanul hagyja (amíg az eredeti kódtávolság 1-nél nagyobb volt).

Definíció:. Egy C lineáris $[n, k, d]$-kód **maximális távolságú**, ha $d = n - k + 1$. Szokás még a ilyen kódokat optimális kódoknak vagy MDS-kódoknak nevezni. (MDS=maximum distance separable, ahol a separable jelző a szisztematikusságra, azaz arra utal, hogy a kódszavak szétválaszthatók információs és ellenőrző részekre. Mégpedig, mint az alábbi állítás mutatja, tetszőleges módon.)

Állítás:. Legyen H a C lineáris $[n, k]$-kód egy tetszőleges ellenőrző mátrixa. Ekkor C maximális távolságú $\Leftrightarrow$ H bármely k oszlopa lineárisan független. (Más szóval, a C kód tetszőleges k darab helyén szisztematikus.)

Biz.: Az ellenőrző mátrix szerkezete és a kódtávolság közötti kapcsolatról szóló tétel alapján nyilvánvaló.

A C és $C^\perp$ szisztematikussága közötti kapcsolatról szóló állítás alapján:

Következmény:. Egy C lineáris kód akkor és csak akkor maximális távolságú, ha $C^\perp$ maximális távolságú.

3.2. Lagrange-interpoláció

Legyen $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in F^n$, amelyre $i \neq j$ esetén $\alpha_i \neq \alpha_j$. Ekkor a $V_{\underline{\alpha}} : F[x] \to F^n$ leképezés, ahol

$$V_{\underline{\alpha}}(f) = (f(\alpha_1), \ldots, f(\alpha_n))$$

egy lineáris leképezés.

Tény:. Legyen $\underline{\alpha}$ mint fent, továbbá legyenek $a_1, \ldots, a_n \in F$ teszőleges elemek. Ekkor pontosan egy olyan legfeljebb $n-1$-ed fokú $f \in F[x]$ polinom létezik, amelyre $f(\alpha_1) = a_1, \ldots, f(\alpha_n) = a_n$. Más szóval, $V_{\underline{\alpha}}$ megszorítása az n-nél alacsonyabb fokú polinomok terére egy reguláris lineáris transzformáció.

Valójában:. $V_{\underline{\alpha}} : F[x] \to F^n$ egy gyűrű-homomorfizmus, ahol F^n-ben a szorzás is koordinátánként értendő. $V_{\underline{\alpha}}$ magja a $p_{\underline{\alpha}}(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ polinom által generált ideál. Ennek megfelelően $V_{\underline{\alpha}}$ egy (szintén $V_{\underline{\alpha}}$-val jelölt) izomorfizmust indukál az $F[x]/(p_{\underline{\alpha}}(x))$ maradékosztálygyűrű és az F^n gyűrű között.

Megjegyzés:. A $V_{\underline{\alpha}}$ transzformáció és az inverze $O(n^2)$ F-beli alapművelettel számolható. Előbbi kézenfekvő, utóbbi a Lagrange-alappolinomok segítségével:

$$l_i(x) = \prod_{j \neq i} \frac{x - \alpha_j}{\alpha_i - \alpha_j}$$

$$l_i(\alpha_j) = \begin{cases} 1 & \text{ha } i = j \\ 0 & \text{ha } i \neq j \end{cases}$$

Speciális $\alpha_1, \ldots, \alpha_n$ elemekre még gyorsabban mennek (pl. $O(n \log n)$ művelet).

3.3. Általánosított Reed-Solomon–kódok

Előbbiek értelmében, ha egy k-nál alacsonyabb fokú polinomot $n \geq k$ különböző helyen való behelyettesítéssel kódolunk, a polinom visszanyerhető (interpolálható) az n hely közül bármely k helyen felvett értékéből. Más szóval, egy $n-k+1$, azaz maximális távolságú kódot kapunk.

Definíció:. Legyen $\underline{\alpha}$ mint fenn és $\underline{v} = (v_1, \ldots, v_n) \in F^n$, amelynek egyik v_i koordinátája sem 0. Ezekkel a paramérerekkel:

$$\begin{aligned} GRS_k(\underline{\alpha}, \underline{v}) &= \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) | f \in F[x], \deg f < k\} \\ &= \{\underline{v} \cdot V_{\underline{\alpha}}(f) | f \in F[x], \deg f < k\} \end{aligned}$$

A "természetes" kódolás mátrixa, tehát egy generátormátrix:

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix} . \begin{pmatrix} v_1 & & & & \\ & v_2 & & & \\ & & v_3 & & \\ & & & \ddots & \\ & & & & v_n \end{pmatrix}$$

A $GRS_k(\underline{\alpha}, \underline{v})$ kód tágabb értelemben ekvivalens a $GRS_k(\underline{\alpha}, \underline{1})$ kóddal, a $\underline{v}$ paraméterű kódok bevezetésének – többek közt – a következő miatt van értelme:

Tétel:. Van olyan $\underline{v}' = (v_1', \ldots, v_n') \in F^n$ vektor (semelyik $v_i' \neq 0$), melyre:

$$GRS_k(\underline{\alpha}, \underline{v})^\perp = GRS_{n-k}(\underline{\alpha}, \underline{v}').$$

Más szóval, $GRS_k(\underline{\alpha}, \underline{v})$ egy paritásellenőrző mátrixa

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \ldots & \alpha_n^{n-k-1} \end{pmatrix} . \begin{pmatrix} v_1' & & & & \\ & v_2' & & & \\ & & v_3' & & \\ & & & \ddots & \\ & & & & v_n' \end{pmatrix}$$

Biz.: $GRS_{n-1}(\underline{\alpha}, \underline{v})^\perp$ 1-dimenziós maximális, azaz $n-1+1$, azaz n távolságú kód. Tehát ha $\underline{v}' = (v_1', \ldots, v_n') \in GRS_{n-1}(\underline{\alpha}, \underline{v})^\perp \setminus \{0\}$, akkor semelyik $v_i' \neq 0$. Továbbá minden $0 \leq j < n-1$-re

$$0 = (\underline{v}', \underline{v} \cdot V_{\underline{\alpha}}(x^j)) = \sum_{i=1}^{n} v_i v_i' \alpha_i^j.$$

Ezért

$$(\underline{v}' \cdot V_{\underline{\alpha}}(x^s), \underline{v} \cdot V_{\underline{\alpha}}(x^t)) = \sum_{i=1}^{n} v_i v_i' \alpha_i^{s+t} = 0$$

ha $s+t < n-1$, például ha $s \leq n-k-1$ és $t \leq k-1$. Ez pedig éppen azt mondja, hogy $GRS_{n-k}(\underline{\alpha}, \underline{v}')$ egy bázisa merőleges $GRS_k(\underline{\alpha}, \underline{v})$ egy bázisára.

3.4. Hagyományos Reed-Solomon–kódok

Legyen α egy primitív n-edik egységgyök az $F = GF(q)$ testben. (Ilyen pontosan akkor van, ha $n|(q-1)$.) A $GRS_k(1, \alpha, \ldots, \alpha^{n-1}, \underline{1})$ kódot **szűk értelemben vett Reed-Solomon–kódnak** nevezzük.

Feladat:. Milyen $\underline{v}'$ vektorokra lesz $GRS_k(1, \alpha, \ldots, \alpha^{n-1}, \underline{1}) \perp GRS_{n-k}(1, \alpha, \ldots, \alpha^{n-1}, \underline{v}')$

3.5. Alkalmazás: hivajavítás CD-n

Forrás: http://www.univ-tln.fr/ zanotti/enseignement/divers/chapter3.html

Itt a CD-re írt adatok védelmére használt módszerek egy alapvető részletét vázoljuk. A kódolás elnevezése: CIRC=*cross interleaved Reed-Solomon code*. Erre a CD-n opcionálisan még számos hibajelző/hibajavító kód rakódhat rá.

A kiindulás egy $[255, 251, 5]$ paraméterű Reed-Solomon–kód az $F = GF(2^8)$ test fölött. Ebből két kódot csinálunk az úgynevezett rövidítés (shortening) műveletével:

Kódok rövidítése:. Legyen C egy lineáris $[n, k, d]$-kód és legyen $i_1, \ldots, i_l$ l különböző koordinátapozíció. Álljon C_0 C azon szavaiból, amelyek 0-k ezeken a helyeken. Ezek után töröljük C_0 szavaiból a (fölösleges, hiszen azonosan 0) i_1-edik, ..., i_l-edik koordinátákat. A kapott C' (rövidített) kód hossza $n - l$ lesz, a távolsága legalább d, a dimenziója legalább $n - l$. C' egy ellenőrző mátrixa úgy kapható C-nek egy ellenőrző mátrixából, hogy töröljük az i_1-edik, ..., i_l-edik oszlopokat, majd (esetleg) törlünk néhány redundánssá vált sort is.

A $[255, 251, 5]$ paraméterű RS-kódból rövidítéssel egy C_1 $[28, 24, 5]$-kódot és egy C_2 $[32, 28, 5]$-kódot csinálunk. Mindkét kódnál (az első 24 illetve az első 28 bájt szerinti) szisztematikus kódolást használunk.

Az első kódoló az üzenet 24 bájtos blokkjaiból 28 bájtosakat csinál, amelyeket a következő, késleltetésesen összefésült (átfűzött, interleaved) módon ad át a második kódolónak. Képzeljük el, hogy a kódszavakat egy 28 sorból álló táblázat 4 meredekségű átlóiba írjuk fel:

Ábra

Az első kódszó bájtai (sorrendben) tehát a táblázat $(1, 1), (2, 5), \ldots, (i, 4(i-1)+1), \ldots, (28, 119)$-edik pozícióiban helyezkedenek el. A második kódszó elhelyezkedése: $(1, 2), (2, 6), \ldots, (i, 4(i-1)+2), \ldots, (28, 120)$, és így tovább, esetleg ciklikusan modulo a táblázat hosszúsága.

A második kódoló a táblázat oszlopait kapja egymás utáni sorrenben, ellátja őket oszloponként további 4 ellenőrző bájttal, majd ezeket (további átfűzéseket alkalmazva) írjuk ki a lemezre.

A szisztematikus kódolás a dekódoló számára elég nagy szabadságot biztosít. Elképzelhető, hogy az ellenőrző bájtokat egyáltalán nem használjuk, vagy csak a C_2 kód ellenőrző bájtjait hsználjuk vagy mindkettőét.

Alább egy lehetséges (és szokásos) dekódolási eljárást elemzünk a hibacsomókkal szembeni védekezés szempontjából. A C_2 kód távolsága 5, ezt 1 hiba javítására és 1-nél több hiba jelzésére használjuk föl. Ha 1-nél több hibát érzékelünk (azaz nincs 0 vagy 1 távolságra kódszó), az olvasott szó összes bájtját töröltnek nyilvánítjuk.

Feladat:. Tegyük fel, hogy a C_2 kód egy 32 bájtos blokkja "durván" meghibásodott: a hiba ereményként a lehetséges 256^{32} vektor egyenletes valószínűséggel fordul elő. Mutassuk meg, hogy annak a valószínűsége, hogy a fenti eljárás nem jelez hibát < 0.000002.

A C_1-dekódolót ezek után a törlések javítására használjuk fel. Mivel a kódtávolság 5, egy blokkon belül akár 4 törlést is ki tudunk javítani. Ebbe belefér az, hogy a C_2 kódnak 15 vagy kevesebb egymást követő blokkja, azaz 480 bájtja hibásodik meg. Tehát egy ekkora hibacsomót ki tudunk javítani. Ez egy körülbelül egy 2.5 mm-es "rossz irányú" karcolásnak felel meg.

3.6. Egy egyszerű dekódoló algoritmus

A "kódtávolságon belül": t hiba, ahol $2t+1 \leq d = n-k+1$. Az egyszerűség kedvéért feltesszük, hogy $\underline{v} = \underline{1}$. Az általános eset kezelése az alábbi vázolt módszertől egyszerű részletekben tér csak el.

Tegyük fel, hogy a csatornára a $c = V_{\underline{\alpha}}(f) = (f(\alpha_1), \ldots, f(\alpha_n))$ kódszót küldték, ahol $\deg f < k$, valamint azt, hogy legfeljebb t hiba történt az (ismeretlen) $i_1, \ldots, i_t$ helyeken, azaz a beérkezett sorozat

$$u = c + e = c + (0, \ldots, 0, e_{i_1}, 0, \ldots, 0, e_{i_t}, 0, \ldots, 0).$$

(Itt megengedjük, hogy bizonyos e_{i_j}-k nullák legyenenk.) Legyen $h(x) = (x - \alpha_{i_1}) \cdots (x - \alpha_{i_t})$ és $l(x) = f(x)h(x)$. Ekkor $\deg h = t$ és $\deg l = \deg f + \deg h < k + t$. $V_{\underline{\alpha}}(h) \cdot e = 0$ mivel $V_{\underline{\alpha}}(h)$ 0 azokon a helyeken, ahol e nem. Így $V_{\underline{\alpha}}(h) \cdot u = V_{\underline{\alpha}}(h) \cdot c = V_{\underline{\alpha}}(h) \cdot V_{\underline{\alpha}}(f) = V_{\underline{\alpha}}(hf) = V_{\underline{\alpha}}(l)$. Tehát h és l között a

$$V_{\underline{\alpha}}(h) \cdot u = V_{\underline{\alpha}}(l)$$

összefüggést nyerjük. Azaz léteznek olyan $y \in GRS_{t+1}(\underline{\alpha}, \underline{1})$ illetve $z \in GRS_{k+t}(\underline{\alpha}, \underline{1})$, amelyekre

$$y \cdot u = z.$$

Ez y és z koordinátáiban kifejezve egy homogén lineáris egyenletrendszer (n egyenlet $2n$ ismeretelennel) ekvivalens. További $n-(t+1)+n-k-t < 2n$ egyenlettel (ellenőrző mátrixok) kifejezhető az is, hogy $y \in GRS_{t+1}(\underline{\alpha}, \underline{1})$ és $z \in GRS_{k+t}(\underline{\alpha}, \underline{1})$ legyen.

Tétel:. Legyen $2t+1 \leq n-k+1$. Tegyük fel, hogy $u \in F^n$, $c \in GRS_k(\underline{\alpha}, \underline{1})$, melyrekre $d(u,c) \leq t$. Ekkor van olyan $0 \neq y \in GRS_{t+1}(\underline{\alpha}, \underline{1})$ és $z = y \cdot u \in GRS_{k+t}(\underline{\alpha}, \underline{1})$, Tetszőleges ilyen y-ra $y \cdot c = y \cdot u$ (következésképpen $c_i = u_i$ azokon az i helyeken, ahol $y_i \neq 0$).

Biz.: Az első állítást már beláttuk. A második állítás abból következik, hogy $y \cdot c$ is egy GRS_{k+t}-beli kódszó, következésképpen $y \cdot (u-c) \in GRS_{k+t}$. Ugyanakkor $w(y \cdot (u-c)) \leq w(u-c) \leq t \leq n-k-t$, ami csak úgy lehet, hogy $y \cdot (u-c) = 0$ hiszen GRS_{k+t} kódtávolsága $n-k-t+1$.

Ennek megfelelően y-ból c-t (és a megfelelő f-et) úgy próbálhatjuk meg visszanyerni, hogy interpoláljuk f-et az α_i-k közül k olyan helyen, ahol $y_i \neq 0$, majd visszahelyettesítéssel kiszámítjuk $c_i = f(\alpha_i)$-t. Ellenőrzésképpen meg kell nézni, hogy c_i megegyezik-e u_i-vel az összes olyan i helyen, ahol $y_i \neq 0$. Ha nem, akkor nincsen u-tól t távolságon belül kódszó.

Megjegyzések:.

- A módszer általánosítható az úgynevezett algebrai geometriai kódok (Goppa-kódok) dekódolására.
- Lényegében ezen az alapelven, de sokkal finomabb részleteket is (pl. a szindrómákat) figyelembe véve működnek a leghatékonyabb dekódoló módszerek. Ezek közül nevezetes az $O(n^2)$ idejű, hardwerrel igen jól támogatható Berlekamp-Massey–algoritmus. Az ismert leggyorsabb módszer $O(n \log^2 n \log\log n)$ futási idejű.

3.7. Reed-Solomon kódok

$n|q-1$, α primitív n-edik egységgyök,

$$\underline{\alpha} = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$$

Ekkor az általánosított Reed-Solomon–kódok dualitásáról szóló tétel alapján (a bizonyítás módszerét konkrétan alkalmazva):

$$GRS_k(\underline{\alpha}, \underline{1})^{\perp} = GRS_k(\underline{\alpha}, (1, \alpha, \alpha^2 \ldots, \alpha^{n-1})).$$

Azaz $GRS_k(\underline{\alpha}, \underline{1})$ egy ellenőrző mátrixa:

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{n-k-1} & \alpha^{2(n-k-1)} & \ldots & \alpha^{(n-k-1)(n-1)} \end{pmatrix} \cdot \begin{pmatrix} 1 & & & & \\ & \alpha & & & \\ & & \alpha^2 & & \\ & & & \ddots & \\ & & & & \alpha^{n-1} \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \ldots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \ldots & \alpha^{(n-k)(n-1)} \end{pmatrix}$$

Így $GRS_k(\underline{\alpha}, \underline{1})$ $(a_0, \ldots, a_{n-1})$ kódszavait az

$$a_0 + a_1\alpha^{i\cdot 1} + \ldots + a_{n-1}\alpha^{i\cdot(n-1)} = 0 \;\; (i = 1, \ldots, n-k)$$

egyenletrendszer írja le. Ha az $(a_0, \ldots, a_{n-1})$ vektort polinomként, nevezetesen az $a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ polinomként értelmezzük, a fenti feltételek a következőképpen fogalmazhatók meg:

$$a(\alpha) = a(\alpha^2) = \ldots = a(\alpha^{n-k}) = 0,$$

vagy másképpen:

$$(x-\alpha)\cdots(x-\alpha^{n-k}) | a(x).$$

Tehát polinommként interpretálva $GRS_k(\underline{\alpha}, \underline{1})$ az $(x-\alpha)\cdots(x-\alpha^{n-k})$ polinom n-nél alacsonyabb fokú többszöröseiből áll.

Hasonlóképpen, a $C = GRS_k(\underline{\alpha}, *) = GRS_{n-k}(\underline{\alpha}, (1, \alpha^t, \alpha^{2t}, \ldots, \alpha^{(n-1)t})^{\perp}$ GRS-kódot. A C kód $(a_0, \ldots, a_{n-1})$ szavait az

$$a_0 + a_1\alpha^{t+i} + \alpha^{2t+2i} + \ldots + \alpha^{(n-1)t+(n-1)i} = 0 \;\; (i = 0, \ldots, n-k-1)$$

egyenletek írják le. Polinomos interpretációban a C kód tehát azon $a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ polinomokból áll, amelyekre

$$a(\alpha^t) = a(\alpha^{t+1}) = \ldots = a(\alpha^{t+n-k-1}) = 0,$$

azaz az $(x-\alpha^t)(x-\alpha^{t+1})\cdots(x-\alpha^{t+n-k-1})$ polinom n-nél alacsonyabb fokú többszöröseiből. Ezeket a kódokat hívjuk Reed-Solomon–kódoknak ($RS(n,k)$-kódoknak):

Definíció: Reed-Solomon kódok. polinomos értelmezésben: Legyen $n|q-1$ és $\alpha \in F = GF(q)$-ban egy primitív n-edik egységgyök és $0 \leq t < n$. Legyen továbbá

$$g(x) = (x-\alpha^t)(x-\alpha^{t+1})\cdots(x-\alpha^{t+n-k-1}).$$

A

$$C = \{f(x) \cdot g(x) | f(x) \in F[x],\ \deg f(x) < k\}$$

kód (pontosabban: ezen polinomok együthatóvektoraiból álló kódot) egy $RS(n,k)$-kód. Mivel egy C egy $GRS_k(*,*)$-kód, C maximális távolságú, tehát a paraméterek: $[n, k, n-k+1]$.

3.8. Kódok résztestek fölötti kódként

Legyen $F \leq F'$ (résztest), $(F' : F) = m$ és $C \subseteq F'^n$ egy n hosszú kód. F' elemeit F feletti m hosszú vektorokként tekinthetjük (számos módon, függ attól, hogy F'-ben milyen F-bázist veszünk). Így tekintve C egy $m \cdot n$ hosszú kód, és egy lineáris $[n, k, d]$-kód F' egy lineáris $[mn, mk, \geq d]$-kód lesz F fölött. A relatív kódtávolságra általában nem tudunk jobbat mondani, mint azt, hogy $\frac{d}{n}$-ről $\frac{1}{m} \cdot \frac{d}{n}$-nél kisebbre nem csökken. Viszont a konstrukció alkalmazható hibacsomók elleni védekezésre: ha C-ben h hosszú (F'-beli) hibacsomót ki tudunk javítani, akkor F feletti kódként tekintve $(h-1)m+1$ hosszú hibacsomót is ki tudunk javítani.

4. BCH-kódok

4.1. Résztest-kód

Legyen $F \leq F'$ (résztest), $(F' : F) = m$ és $C \subseteq F'^n$ egy n hosszú kód. C **résztest-kódja:** $C_{|F} = C \cap F^n$. $C_{|F}$ tehát C azon szavaiból áll, melyeknek minden jegye F-beli. Világos, hogy ha $C_{|F}$ távolsága nem lehet kisebb C távolságánál. Nyilvánvaló az is, hogy ha C lineáris, akkor $C_{|F}$ is az.

Állítás:. Legyen C lineáris kód F' felett. Vegyük F' elemeinek egy rögzített ábrázolását F feletti m hosszú (oszlop-)vektorokként: $\alpha \leftrightarrow (\alpha^1, \ldots, \alpha^m)^T$. Ennek megfelelően egy F'^n-beli x vektorhoz m darab $x^1, \ldots, x^m$ F^m-beli vektor tartozik, ahol $x^i = (x_1^i, \ldots, x_n^i)$. Ekkor F^m-ben

$$C_{|F}^{\perp} = \langle y^i | x \in C^{\perp},\ 1 \leq i \leq m \rangle.$$

Másképpen: Ha C-nek H egy ellenőrző mátrixa, akkor $C_{|F}$-nak egy ellenőrző mátrixa úgy kapható, hogy H elemeit helyettesítjük a megfelelő m hosszú oszlopvektorokkal, majd esetleg kitörlünk néhány, a többitől lineárisan függő sort.

Biz.: Legyen $x \in F^m$. Tekintsük x-et mint F'^n-beli vektort. Legyen $y \in F'^m$. Ekkor az (x, y) skalárszorzatra, mint m hosszú vektorra $(x, y)^j = (\sum_{i=1}^n x_i y_i)^j = \sum_{i=1}^n (x_i y_i)^j = \sum_{i=1}^n (x_i y_i^j) = (x, y^j)$. Következésképpen $(x, y) = 0 \Leftrightarrow (x, y^i) = 0$ minden i-re. Innen az állítás nyilvánvaló.

Következmény:. Ha C egy $[n, k, d]_{F'}$-kód, akkor $C_{|F}$ egy $[n, k_0, d_0]_F$-kód, ahol $d \leq d_0$, $n - m(n-k) \leq k_0 \leq k$.

4.2. Alternáns-kódok

GRS-kódok résztest-kódjai.

4.3. BCH-kódok

Legyen $F = GF(q) \leq F' = GF(q^m)$, ahol $n | q^m - 1$, α egy primitív n-edik egységgyök F'-ben.
Egy BCH-kód egy Reed-Solomon–kód résztest-kódja:

$$C = \{f(x) | f(x) \in F[x],\ \deg f(x) < n,\ (x - \alpha^t)(x - \alpha^{t+1}) \cdots (x - \alpha^{t+\delta-2}) \text{ osztója } f(x)\text{-nek } F'[x]\text{-ben}\}.$$

A Reed-Solomon kód paraméterei: $[n, n-\delta+1, \delta]$. A C BCH-kód távolsága: $d \geq \delta$, dimenziója $n - m(\delta-1) \leq k \leq n-\delta+1$. (Elnevezés: δ a kód **tervezett távolsága** (designed distance).)

Szokásos dekódolás:. A "tervezett távolságon belül" (pontosabban $\lfloor (\delta-1)/2 \rfloor$ hibát javítva): F' felett dolgozva, a Reed-Solomon–kód dekódolási eljárását végrehajtva.

Előismeret:. F'-ben $\Phi : a \mapsto a^q$ egy test-automorfizmus. Φ fixpontjai éppen F elemei. Φ rendje m. (Háttér: az $(F'|F)$ bővítés Galois-bővítés és $Gal(F'|F)$ a Φ által generált ciklikus csoport.)

Állítás:. Legyen $\beta \in F'$. Ha $f(x) \in F[x] = GF(q)[x]$ és $f(\beta) = 0$ akkor $f(\beta^q) = 0$.
Biz.: $f(\beta^q) = f(\beta)^q$ alapján nyilvánvaló.

Jelölés:. $K(\beta) = \{\beta^{q^i} | (\text{i}=0,\ldots,\text{m-1})\} - \beta$ konjugáltjai.

Következmény/elnevezés:. $m_\beta(x) = \prod_{\gamma \in K(\beta)} (x - \gamma) \in F[x]$. Ez a legalacsonyabb fokú $F[x]$-beli 1 főegyütthatós polinom, aminek β gyöke. Elnevezés: β minimálpolinomja.

Következmény:. Az $\alpha^t, \alpha^{t+1}, \alpha^{t+\delta-2}$ elemekhez fabrikált BCH-kód

$$\{f(x) \in F[x] | \deg f(x) < n,\ g(x) \text{ osztója } f(x)\text{-nek}\},$$

ahol $g(x)$ az $\alpha^t, \alpha^{t+1}, \alpha^{t+\delta-2}$ elemek minimálpolinomjainak legkisebb közös többszöröse.

Példa - bináris Hamming-kódok. Legyen $F = GF(2), F' = GF(2^m), n = 2^m - 1$, továbbá α egy primitív n-edik egységgyök (azaz az F' test egy primitív eleme). A $C = GRS_{n-1}((1, \alpha, \alpha^2, \ldots, \alpha^{n-1}), \underline{1})$ ellenőrző mátrixa

$$(1, \alpha, \ldots, \alpha^{n-1}),$$

tehát – polinomos értelmezésben – C azon polinomokból áll, melyeknek gyöke az α elem. A megfelelő BCH-, azaz résztest kódot kétféleképpen nézhetjük meg:
(1) A C kód ellenőrző mátrixának elemei helyébe a megfelelő m hosszú bináris vektorokat írva a résztest-kód elenőrző mátrixaként azt a mátrixot kapjuk, melynek oszlopai az m hosszú bináris vektorok. Ez a Hamming-kód szokásos definíciója.
(2) α konjugáltjai: $\alpha, \alpha^2, \alpha^4, \ldots, \alpha^{2^{m-1}}$. Tehát a BCH-kód a $g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)\cdots(x-\alpha^{2^{m-1}})$ bináris polinom n-nél alacsonyabb fokú többszöröseiből áll, a dimenzió tehát $n - m = 2^m - m - 1$. A kódszavak gyökei közt van α is és α^2 is, tehát a kód valójában megegyezik az α, α^2 paraméterekhez gyártott BCH-kóddal, így a kódtávolság legalább 3.

Megjegyzés. Legyenek F, F', n, m, α mint fent, $t < n/m$. Ekkor az $\alpha, \alpha^2, \ldots, \alpha^{2t}$ elemekhez tartozó C bináris BCH-kód dimenziója legalább $n - tm$, a távolsága pedig legalább $\delta = 2t+1$, azaz t hibát ki tud javítani. Ehhez legfeljebb $tm = t \log_2 n$ ellenőrző bitet használ fel. Megmutatható, hogy a C kód tartalmaz 2δ-nál kisebb súlyú elemet tehát a kódtávolság legfeljebb kétszerese a "tervezettnek".

5. Ciklikus kódok

Definíció:. Egy C lineáris $[n,k]$-kód ciklikus, ha zárt a kódszavak ciklikus léptetésére, azaz ha $(v_1, \ldots, v_n) \in C$, akkor $(v_n, v_1, \ldots, v_{n-1}) \in C$.

Az F^n elemeit n-nél alacsonyabb fokú polinomokkal azonosítjuk (együtthatósorozatok). Kényelmes lesz ezeket a poliomokat a modulo $x^n - 1$ redukált polinomoknak, azaz az $F[x]/(x^n - 1)$ gyűrű elemeinek tekinteni.

Észrevétel:. A ciklikus léptetés az x-szel való szorzásnak felel meg (modulo $x^n - 1$).

Tétel:. A $C \subseteq F[x]/(x^n - 1)$ lineáris kód ciklikus $\Leftrightarrow$ C ideál az $F[x]/(x^n - 1)$ gyűrűben.

Biz.: $\Leftarrow$: C zárt a (modulo $x^n - 1$ vett) beszorzásra x-szel, ezért minden t-re az x^t-vel való szorzásra is. Mivel C zárt az összeadásra, az előbbiekből az következik, hogy zárt a polinomokkal való beszorzásra is. $\Rightarrow$: egyszerű.

Tétel:. A $C \subseteq F[x]/(x^n - 1)$ lineáris kód ciklikus $\Leftrightarrow$

$$C = \{g(x) \text{ } n\text{-nél alacsonyabb fokú többszörösei}\}$$

$x^n - 1$ valamely $g(x) \in F[x]$ osztójára.

Biz.: $\Leftarrow$: Legyen I a C ideál teljes inverz képe a $\phi : F[x] \to F[x]/(x^n - 1)$ természetes homomorfizmusnál (a modulo $x^n - 1$ vett maradékképzésnél). Ekkor I egy olyan ideál $F[x]$-ben, amely tartalmazza az $(x^n - 1)$ polinomot. Mivel $F[x]$ főideálgyűrű, $I = (g(x))$ (azaz I a $g(x)$ polinom többszöröseiből áll). Mivel $(x^n - 1) \in \ker\phi \subseteq I$, $g(x)$ valóban osztója $x^n - 1$-nek. Az állítás fennmaradó része egyszerű dimenzió-megfontolással adódik. (Világos, hogy $g(x)$ n-nél alacsonyabb fokú többszörösei tényleg C-ben vannak. Ez egy $n - \deg g$ dimenziós $V \leq C$ altér. Tekintsük a $\deg g$-nél alacsonyabb fokú polinomok W alterét. Világos, hogy $V \cap W = (0)$ és $\dim V + \dim W = n$. Egy $0 \neq w(x) \in W$ vektor teljes inverz képe $\phi^{-1}(\{w(x)\}) = \{w(x) + f(x)(x^n - 1) | f(x) \in F[x]\}$, $g(x)$-szel (az osztás maradéka éppen w(x)). Ezért $W \cap C = (0)$ is teljesül, következésképpen $\dim C \leq n - \dim W = n - \deg g = \dim V$, ami a $V \subseteq C$ tartalmazással összevetve a $V = C$ egyenlőséget adja.) $\Rightarrow$: Egyszerű.

Általában feltesszük:. $(n, q) = 1$. (Különben nincs primitív n-edik egységgyök és az $F[x]/(x^n - 1)$ gyűrű "csúnya". Például $q = 2$, $n = 2^m$-re a gyűrű összes ideálja: az $1, (x-1), (x-1)^2, \ldots, (x-1)^n$.)

Következmény:. A BCH-kódok (és speciálisan a Reed-Solomon-kódok) ciklikusak.

Elnevezés:. A tételbeli $g(x)$-et C **generátorpolinomjának** hívjuk. Ha $\dim C = k$, akkor $\deg g(x) = n - k$: $g(x) = g_0 + g_1 x + \ldots + g_{n-k} x^{n-k}$ A $g(x)$-hez tartozó természetes generátormátrix:

$$\begin{pmatrix} g_0 & g_1 & g_2 & \ldots & g_{n-k} & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_{n-k-1} & g_{n-k} & 0 & \ldots & 0 \\ 0 & 0 & g_0 & \ldots & g_{n-k-2} & g_{n-k-1} & g_{n-k} & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & g_0 & g_1 & g_2 & \ldots & g_{n-k} \end{pmatrix}.$$

Ellenőrző polinom:. $h(x) = (x^n - 1)/g(x)$. Ellenőrző mátrix:

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & h_k & h_{k-1} & \dots & h_1 & h_0 \\ 0 & 0 & \dots & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 \\ \vdots & \vdots & & & & & & & \vdots & \\ \vdots & \vdots & & & & & & & \vdots & \\ \vdots & \vdots & & & & & & & \vdots & \\ h_k & h_{k-1} & \dots & h_2 & h_1 & h_0 & 0 & \dots & 0 & \end{pmatrix}.$$

Biz.: feladat. (Útmutatás: igazoljuk, hogy az első mártix i-edik sorának a második mátrix j-edik sorával vett skalárszorzata $x^{n-i-j+1}$ együtthtatója a gh polinomban.)

Megjegyzés:. A duális kód (általában) tehát nem a $h(x)$, hanem a "fordított", $x^k h(x^{-1})$ "fordított" poliom által generált ciklikus kód. Ekvivalens, de nem mindig azonos a $h(x)$ által generált kóddal.

Egy szokásos szisztematikus kódolás:. $f(x) \mapsto x^{n-k}f(x) - u(x)$, ahol $u(x) = x^{n-k}f(x)$ modulo $g(x)$.

Tétel (BCH-korlát):. Legyen a C lineáris kódnak a generátorpolinomja $g(x)$. Tegyük fel, hogy van olyan α primitív n-edik egységgyök (F alkalmas bővítéséből), amelyre $\alpha^s, \alpha^{s+1}, \dots, \alpha^{s+t-1}$ mind gyöke $g(x)$-nek (azaz a C kód minden elemének). Ekkor a C kód távolsága legalább $t+1$.

Biz.: A feltételek mellett C részkódja a megfelelő BCH-kódnak.

Sift-regiszterek:. A polinomokkal való szorzásra/osztásra használt eszközök, ld. majd a konvolúciós kódoknál.

5.1. CRC-kódok (cyclic redundancy check)

$g(x) \in F[x]$ négyzetmentes, $g(0) \neq 0$.

$$CRC_{g,n} = \{f(x) \in F(x) | \deg f(x) \leq n,\ f(x) \text{ osztható } g(x)\text{-szel}\}$$

Ha $N \geq n$, hogy $g(x) | x^N - 1$, akkor $CRC_{g,n}$ a $CRC_{g,N}$ ciklikus kód rövidítése, tehát $CRC_{g,n}$ kódtávolsága legalább akkora, mint $CRC_{g,N}$ kódtávolsága. A fenti szisztematikus kódolást alkalmazzák, az ellenőrző jegyeket általában hibajelzésre használják.

Feladat:. Tegyük fel, hogy $\deg g(x) = k$. Bizonyítsuk be, hogy ekkor $CRC_{g,?}$ egy $\leq k$ hosszú hibacsomót jelezni tud.

Példa: CRC-32. (IEEE 802.3 szabvány) a

$$g(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

$\in GF_2[x]$ polinomra $CRC_{g,n}$ kódtávolsága ≥ 5, ha $n \leq 3000$, ≥ 4, ha $n \leq 12000$.

5.2. Feladatsor: a bináris Golay-kódok

$F = GF(2)$, $n = 23$. Legyen α egy primitív 23-adik egységgyök F egy alkalmas F' bővítésében (látjuk mindjárt, hogy $F' = GF(2^{11})$ egy jó választás). α konjugáltjai:

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32} = \alpha^9, \alpha^{18}, \alpha^{36} = \alpha^{13}, \alpha^{26} = \alpha^3, \alpha^6, \alpha^{12},$$

tehát α minimiálpolinomja F felett egy 11-edfokú $g(x)$ polinom. Látjuk, hogy $\alpha^{-1} = \alpha^{22}$ nem konjugáltja α-nak, annak egy másik, szintén 11-edfokú minimálplinomja van, a "fordított" $x^{11} \cdot g(x^{-1})$ polinom. Valóban,

$$x^{23} - 1 = (x-1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1),$$

tehát – α megválasztásától függően – $g(x) = (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)$ vagy $g(x) = (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$. Feltehető, hogy az előbbi áll fenn.

$$G_{23} = \{g(x)\text{-nek legfeljebb 22 fokú többszörösei}\}.$$

G_{24} G_{23}-ból paritásbittel kiegészítéssel kapható: csapjuk minden egyes G_{23} beli kódszóhoz 24-edik bitként a paritását.

1. feladat:. Mutassuk meg, hogy G_{23} kódtávolsága legalább 5. (Ajánlás: BCH-korlát.)

2. feladat:. Bizonyítsuk be, hogy $G_{23}^{\perp}$ G_{23}-nak egy 1 kodimenziós altere. (Ajánlás: $G_{23}^{\perp}$ generátorpolinomja az $(x^{23}-1)/g(x)$ polinom megfordítottja, azaz az $(x-1)g(x)$ polinom.)

3. feladat:. Mutassuk meg, hogy $G_{24}^{\perp} = G_{24}$. (Ajánlás a $\subseteq$ tartalmazáshoz: előző feladat.)

4. feladat:. Bizonyítsuk be, hogy G_{24}-ben minden kódszó súlya 4-gyel osztható. (Ajánlás: igazoljuk és használjuk fel, hogy ha egy bináris lineáris $C \subseteq C^{\perp}$ kódban egy bázis minden elemének a súlya 4-gyel osztható, akkor ez igaz marad minden C-beli kódszóra.)

5. feladat:. Mutassuk meg, hogy G_{24} kódtávolsága 8.

6. feladat:. Igazoljuk, hogy G_{23} távolsága 7 és így G_{23} perfekt.

Elnevezések:. G_{23} a **perfekt bináris Golay-kód**, G_{24} a **kiegészített bináris Golay-kód**.

6. (Bináris) Reed-Muller–kódok

A Reed-Solomon–kódokhoz hasonló prezentáció.

Megállapodás/Jelölések:. $F = GF(2)$, $K = F^m = \{0,1\}^m$ m-dimenziós hiperkocka

Kiértékelés a kocka pontjain:. $V : F[x_1, \ldots, x_m] \to F^K$

Tény:. $\ker V = (x_1^2 - x_1, \ldots, x_m^2 - x_m)$ (generált ideál.)

Reprezentánsrendszer. modulo $\ker V$: **multilineáris polinomok:**

$$\{f(x_1, \ldots, x_m) | \deg_{x_i} f \leq 1 \ (i = 1, \ldots, m)\}.$$

Köv.:. V izomorfizmust indukál a multilineárs polinomok tere és az F^K tér között.

Definíció:. $RM_{m,k} = \{V(f) | f \text{ multilineáris és } \deg f \leq k\}$

Nyilvánvaló:. $0 \leq k < m$-ra $RM_{m,k}$ lineáris, $\dim RM_{m,k} = \sum_{j=0}^{k} \binom{m}{j}$.

Tétel:. $RM_{m,k}$ kódtávolsága 2^{m-k}.

Biz.: $\leq$: A $V(x_1 \cdots x_k)$ kódszó súlya, tehát azon K-beli pontok száma, amelyeken az $x_1 \cdots x_k$ polinom nem 0 értéket vesz fel éppen 2^{m-k}. (Ezek azok a potok, amelyeknek az első k koordinátájuk 1.)
$\geq$: Azt kell bizonyítani, hogy tetszőleges $RM_{m,k}$-beli nemnulla kódszó legalább 2^{m-k} helyen nem 0, azaz egy nem azonosan 0, legfeljebb k-adfokú m változós multilineáris polinomhoz van legalább 2^{m-k} pont a $\{0,1\}^m$ hiperkockán, ahol a polinom értéke nem 0. Ezt k és m szerinti indukcióval bizonyítjuk. Az állítás $k = 0$-ra és tetszőleges m-re nyilvánvaló: egy nem 0 kosntans polinom sehol sem lehet 0. Tegyük fel, hogy k-nál alacsonyabb fokú vagy m-nél kevesebb változós polinomokra az állítást már beláttuk és legyen f egy k-adfokú multilineáris polinom. Írjuk fel f-et $x_m g_1(x_1, \ldots, x_{m-1}) - g_0(x_1, \ldots, x_{m-1})$ alakban, ahol $\deg g_1 \leq k-1$ és $\deg g_0 \leq k$. Ha g_0 azonosan 0, akkor g_1 nem azonosan 0, és az indukciós feltevés miatt van legalább $2^{m-1-(k-1)} = 2^{m-k}$ olyan $(a_1, \ldots, a_{m-1}) \in \{0,1\}^{m-1}$ vektor, amelyekre $g(a_1, \ldots, a_{m-1}) \neq 0$. Ezeket kiegészítve az utolsó koordinátában egy-egy 1-essel, ugyanennyi $\{0,1\}^m$-beli vektort nyerünk, amelyekre f értéke nem 0. Hasonlóan, ha $g_1 - g_0$ azonosan 0, akkor $f = (x_m - 1)g_1$ alakú, ahol és ebben az esetben a g_1-ben nem nullát adó $(a_1, \ldots, a_{m-1})$ vektorokat 0-val kell kiegészíteni. Maradt tehát azon esetek kezelése, amikor sem g_0 sem $g_1 - g_0$ nem azonosan 0. Ekkor az $x_m = 0$ ágon a $-g_0$, az $x_m = 1$ ágon pedig a $g_1 - g_0$ $m-1$-változós polinomokra alkalmazva legalább $2^{m-1-k} + 2^{m-1-k} = 2^{m-k}$ helyet kapunk, ahol f nem 0.

Tétel:. $RM_{m,k}^{\perp} = RM_{m,m-k-1}$ $(0 \leq k < m)$

Biz.: $RM_{m,k}$, illetve $RM_{m,m-k-1}$ bázisát alkotják az $u = V(x_{i_1} \cdots x_{i_s})$ $(s \leq k)$ illetve a $v = V(x_{j_1} \cdots x_{j_t})$ $(t \leq m-k-1)$ alakú vektorok. Azon (K-beli) helyek, ahol mind u, mind v értéke 1:

$$\{(a_1, \ldots, a_m) \in K | a_{i_1} = \ldots = a_{i_s} = a_{j_1} = \ldots = a_{j_t} = 1\},$$

ez 2^{m-z} hely, ahol z az $\{i_1, \ldots, i_s\} \cup \{j_1, \ldots, j_t\}$ halmaz számossága. A z szám legfeljebb $s + t \leq m - 1$ lehet, ezért a kérdéses helyek száma páros. Az (u, v) skalárszozat azonban éppen ezen szám paritása, azaz 0. Tehát $RM_{m,k}$ merőleges $RM_{m,m-k-1}$-re, következésképpen $RM_{m,k}^{\perp} \leq RM_{m,m-k-1}$. Az egyenlőség innen már a dimenziókból adódik.

Példa:. $RM_{m,m-2}$ egy $[2^m, 2^m - m - 1, 4]$-kód. Lyukasszuk ki: dobjuk el a $(0, \ldots, 0)$-nak megfelelő értéket! Kapunk egy $[2^m - 1, 2^m - m - 1, \geq 3]$-kódot. A kód ellenőrző mátrixa $m \times 2^m - 1$-es. A kódtávolság ellenőrző mátrixos jellemzése alapján bármely két oszlop lineárisan független $GF(2)$ fölött (azaz: különböző, egyik sem 0). Tehát az ellenőrző mátrix oszlopai éppen a $2^m - 1$ darab m hosszú nem 0 vektor, azaz a kód ekvivalens a bináris Hamming-kóddal. ($RM_{m,m-2}$ pedig a paritásbittel kiegészített Hamming-kóddal ekvivalens.)

Példa:. $RM_{m,1} = RM_{m,m-2}^{\perp}$ egy $[2^m, m+1, 2^{m-1}]$-kód. Ebből csak azokat a kódszavakat vegyük, amelyek a $(0, \ldots, 0)$ helyen nullák (azaz: a homogén lineáris polinomok értékeit nézzük). Kaptunk egy $[2^m, m, 2^{m-1}]$ paraméterű lineáris kódot, a szimplex kódot. (Valójában az egyik koordináta "fölösleges", ott mindig 0 van.) Mivel egy nem azonosan 0 homogén lineáris polinom zérushelyei hipersíkot alkotnak, a nem 0 kódszavak súlya mindig 2^{m-1}. Ennek megfelelően bármely két különböző kódszó távolsága 2^{m-1}. Átírva a 0-kat $+1$-re, az 1-eket -1-re, a vektorokat egy mátrix soraiba írva egy olyan négyzetes ± 1 elemű mátrixot kapunk, melynek bármely két sora merőleges egymásra. Az ilyen mátrixokat **Hadamard-mátrixoknak** hívjuk. Egy $n \times n$-es Hadamard-mátrix sorai egy (általában nemlineáris) (n,n,n/2)-kódot alkotnak a ± 1 ábécé fölött. A fenti konstrukció a legegyszerűbb, az úgynevezett Sylvester-féle Hadamard-mátrix (vagy Walsh-Hadamard–mátrix, – lényegében a Z_2^m csoport Fourier-transzformációjának a mátrixa). Egy más jellegű (Paley-féle) konstrukció $n = q + 1$-re, ahol q egy $4k - 1$ alakú prímhatvány: legyen $P_{a,b}$ $+1$ vagy -1 aszerint, hogy létezik-e nemnulla $\sqrt{a - b}$ a $GF(q)$ testben vagy sem. Az Hadamard-mátrixot úgy kapjuk, hogy P-hez még hozzáadunk egy-egy csupa egyesből álló sort illetve oszlopot. (Biz.: hf.)

7. Aszimptotikusan jó kódok

Definíció:. Egy rögzített F ábécé feletti kódoknak egy (végtelen) családja **jó**, ha létezik olyan végtelen $\{C_1, C_2, \ldots\}$ részcsaládja, melyre $d_i/n_i >= \delta$, $k_i/n_i >= \kappa$ valamely $\delta > 0, \kappa > 0$ számokra, ahol n_i a C_i kód hossza, k_i a dimenziója ($k_i = [\log_q |C_i|]$), d_i pedig a C_i kód távolsága.

Tétel:. A primítív BCH-kódok ($n = q^m - 1$) családja rossz. Az alternáns kódok családja jó.
Nem bizonyítjuk.

7.1. Véletlen kódok - a Gilbert-Varshamov–korlát

Tétel:. Tegyük fel, hogy a q elemű F ábécé feletti n hosszú k dimenziós lineáris kódok egy X családjára igaz az, hogy a nemnulla w szavakra a w-t tartalmazó X-beli kódok száma független w-től (azaz $\exists c = c(X)$, melyre bármely $0 \neq w \in F^n$ esetén $|\{C \in X | w \in C\}| = c$). Ekkor

$$\sum_{i=1}^{d-1} \binom{n}{i} (q-1)^i < q^{n-k}$$

esetén létezik X-ben $\geq d$ távolságú kód, sőt, az X-beli kódok legalább

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

része ilyen.

Biz.: Számoljuk meg kétféleképpen a (w, C) párokat, melyekre $0 \neq w \in C \in X$. Kapjuk, hogy $c(q^n - 1) = |X|(q^k - 1)$. Innen $c = \frac{q^k-1}{q^n-1}|X| \leq q^{k-n}|X|$. Azon X-beli kódok száma, melyekben van d-nél rövidebb nemnulla kódszó legfeljebb

$$c \cdot (V_q(n, d-1) - 1) = c \cdot \sum_{i=1}^{d-1} \binom{n}{i} (q-1)^i \leq |X| q^{k-n} \sum_{i=1}^{d-1} \binom{n}{i} (q-1)^i$$

($V_q(n, d-1) - 1$ a d-nél rövidebb nemnulla n hosszú szavak száma).

Következmény:. Annak esélye, hogy egy véletlenül választott k-dimenziós n hosszú kód távolsága $\geq d$, legalább

$$1 - q^{k-n} \sum_{i=1}^{d-1} \binom{n}{i} (q-1)^i.$$

Biz. Legyen $X = \{C \leq F^n, \dim C = k\}$. Nyilvánvaló, hogy azon k-dimenziós alterek száma, amelyek egy rögzített $w \neq 0$ vektort tartalmaznak, nem függ a w választásától.

Megjegyzések:.

- A Gilbert-Varshamov–féle alsó korlát d-ben, a kódtávolságban nézve körülbelül fele a Hamming-féle felső korlátnak.
- Nem ismert polinomidejű általános dekódolási eljárás, sőt, a kódtávolság kiszámítása (még közelítőleg is) nehéz (kb. NP-nehéz). Tehát az összes lineáris kódokból történő véletlen választás nem igazán eredményez praktikusan használható kódokat.

Lemma:. $\delta \leq \frac{q-1}{q}$ esetén

$$\lim_{n\to\infty} \frac{1}{n} \log_q V_q(n, [n\delta]) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta) \log_q(1-\delta) =: H_q(\delta)$$

(entrópia).

Biz.: $\frac{\binom{n}{i}(q-1)^i}{\binom{n}{i-1}(q-1)^{i-1}} = \frac{n-i+1}{i}(q-1) \geq 1$ minden $0 < i \leq \frac{q-1}{q}$ egészre, ezért $V_q(n, n\delta)$ legnagyobb tagja $\binom{n}{[n\delta]}(q-1)^{[n\delta]}$, és így $V_q(n, n\delta) \leq (n\delta + 1)\binom{n}{[n\delta]}(q-1)^{[n\delta]}$. Innen $\frac{1}{n}\log_q V_q(n, n\delta) \leq \frac{1}{n}\log_q(n\delta+1) + \frac{1}{n}\log_q \binom{n}{[n\delta]} + \delta \log_q(q-1) + o(1) = \log_q n - \log_q e - \delta \log_q n\delta + \delta \log_q e - (1-\delta)\log_q n(1-\delta) + (1-\delta)\log_q e + \delta \log_q(q-1) + o(1) = -\delta \log_q \delta - (1-\delta)\log_q(1-\delta) + \delta \log_q(q-1) + o(1)$. (A $\log \binom{n}{n\delta}$ becslésére a Stirling-formulát használtuk: $\log_q x! = x \log_q x - x \log_q e + o(x)$.) Az alsó becslés a $V_q(n, n\delta) \geq \binom{n}{[n\delta]}(q-1)^{[n\delta]}$ egyenlőtlenségből, hasonló számolással adódik.

Következmény (aszimptotikus Gilbert-Varshamov–korlát):. Tegyük fel, hogy $\delta < \frac{q-1}{q}$ és

$$R < 1 - H_q(\delta).$$

Ekkor elég nagy n-re létezik n hosszú $\geq R$ sebességű, $\geq [\delta n]$ távolságú lineáris kód. Sőt, elég nagy n-re egy véletlenül választott $\lceil Rn \rceil$ dimenziós kód ilyen.

Aszimptotikus Hamming-korlát:. Legyen a C kód hossza n, sebessége (relatív dimenziója) R: ($R = \frac{1}{n}\log_q |C|$)), relatív távolsága δ. Ekkor

$$R \leq 1 - H_q(\frac{\delta}{2}) + o(1).$$

7.2. Justesen-kódok

Ebben a fejezetben $F = GF(2)$.

7.2.1. Egy érdekes kódcsalád (1/2 sebességű Wozencraft-család)

Legyen $F' = GF(2^m)$. Adott $\alpha \in F'^*$-ra legyen

$$C_\alpha = \{(x, \alpha x) | x \in F'\},$$

F feletti kódként értlemezve. Tehát a kódhossz $2m$, a kódsebesség pedig $\frac{1}{2}$.

Következmény:. Tegyük fel, hogy $H_2(\delta) < \frac{1}{2}$. Ekkor elég nagy m-re a $\{C_\alpha | \alpha \in F'^*\}$ családból egy véletlen kód nagy valószínűséggel legalább δ relatív távolságú.

Biz. Egészítsük ki a családot a $C_0 = \{(x, 0) | x \in F'\}$ és a $C_\infty = \{(0, x) | x \in F'\}$ kódokkal. A kiegészített családból minden $(x, y) \neq (0, 0)$ párra pontosan egy (x, y)-t tartalmazó kód található. Alkalmazható tehát a tétel.

7.2.2. Forney-féle konkatenált kódok

Egy csatornát körbevéve egy kódolással majd a megfelelő dekódolással felfoghatunk egy – az eredetinél jó esetben "biztonságosabb" – csatornának. Az így keletkezett csatornát, az úgynevezett szupercsatornát további kódolási/dekódolási eljárásokkal vehetjük körbe. Az eredményül kapott kódot konkatenált kódnak hívjuk. Az ötlettel találkoztunk már a CD-ket védő CIRC kódoknál.

Itt egy speciális konkatenálási eljárást mutatunk be. A C_1 "belső" kód egy $[n, k, d]$ paraméterű lineáris bináris kód, a C_2 "külső" kód pedig egy $[N, K, D]$ paraméterű lineáris kód a $GF(2^k)$ test fölött. A konkatenált kód úgy kapható, hogy a C_2 kód szavait k hosszú bináris vektorként értlemezve a C_1 kód egy (alkalmas) kódolási eljárásának vetjük alá. Az eredmény egy $[Nn, Kk, \geq Dd]$ paraméterű lineáris bináris kód lesz. (Miért? $\longrightarrow$ feladat.)

Példa:. Legyen C_1 a fenti Wozencraft-család egy "jó" tagja. A paraméterek: $[2m, m, m\delta]$, C_2 pedig egy $GF(2^m)$ feletti S sebességű ($(2^m - 1)S$ dimenziós) primitív ($2^m - 1$ hosszú) Reed-Solomon–kód. A konkatenált kód paraméterei:

$$[2m(2^m - 1), m(2^m - 1)S, \geq m\delta(2^m - (2^m - 1)S)].$$

A relatív paraméterek: kódsebesség$\geq\approx \frac{S}{2}$, relatív távolság: $\approx (1 - S)\delta$. A belső kód dekódolása simán exponenciális idejű m-ben (azaz $2^{O(m)}$), ami polinomiális a konkatenált kód hosszában. (Ugyanez igaz a legjobb C_1 kód kikeresésére is – hála annak, hogy a Wozenkraft-család viszonylag "kicsi".) Mivel a külső kód Reed-Solomon, annak a dekódolása is polinomiális. Ha például $S = \frac{1}{2}$, akkor egy $\approx \frac{1}{4}$ sebességű és $\approx \frac{\delta}{2}$ relatív távolságú, tehát "jó" kódot nyertünk.

7.2.3. Justesen-kódok

Az első jó "explicit" kódcsalád.

Ötlet ("derandomizálás"). Az előbbi konkatenált konstrukcióban cseréljük ki a belső C_1 kódot m-esenként a Wozencraft-család különböző tagjaira. Tehát most C_1 információs blokkmérete $m(2^m - 1)$ és a kódolás

$$(x_1, \ldots, x_{2^m-1}) \mapsto (x_1, \alpha_1 x_1, x_2, \alpha_2 x_2, \ldots, x_{2^m-1}, \alpha_{2^m-1} x_{2^m-1})$$

ahol x_i az információ i-edik m bites darabja $GF(2^m)$ elemeként értelmezve és az α_i elemek befutják $GF(2^m)^*$-ot. A külső kód legyen továbbra is egy $GF(2^m)$ feletti $2^m - 1$ hosszú S sebességű Reed–Solomon-kód.

Tétel:. A kapott kód sebessége $\approx \frac{S}{2}$, relatív távolsága pedig $\geq\sim 1 - S\delta$.

Biz.: A sebesség nyilvánvalóan $\approx \frac{S}{2}$. Legyen $y = (x_1, \alpha_1 x_1, \ldots, x_{2^m-1}, \alpha_{2^m-1} x_{2^m-1})$ egy nemnulla kódszó. Mivel az $(x_1, \ldots, x_m)$ vektor a C_2 Reed-Solomon–kód eleme, $x_i \neq 0$ – és így persze $(x_i, \alpha_i x_i) \neq 0$ – az i indexek legalább $(1 - S)$ részére. Legyen $\epsilon > 0$. Ha m elég nagy, az olyan i indexek száma, melyekre $(x_i, \alpha_i x_i) \neq 0$, de (x_i, α_i) súlya $2\delta m$-nél kisebb, legfeljebb $\epsilon(2^m - 1)$. Így az i indexek legalább $1 - S - \epsilon$ részére (x_i, α_i) súlya legalább δ, tehát y súlya legalább $(1 - S)\delta - \epsilon\delta$.

Megjegyzések.

- "Explicit" $GF(2^m)$: $m = 2 \cdot 3^l$ alakú számokra $x^m + x^{m/2} + 1$ irreducibilis, $GF(2^m) = GF(2)[x]/(x^m + x^{m/2} + 1)$.
- Csak a konstrukció alapötletét mutattuk be. Igazából különböző "hangolási" eljárásokkal többféle és jobb kódok nyerhetők. Például a Wozencraft-családból lyukasztással $\frac{1}{2}$-nél sűrűbb, hasonló kódok kaphatók (persze akkor δ kisebb lesz).