Kódelmélet

Wettl Ferenc

V0.150214

Tartalomjegyzék

Jelölések

$\mathrm{GF}(q)$, $\mathbb{F}_q$	q elemű véges test
$\mathbb{F}_q[x]$	$\mathbb{F}_q$ feletti polinomok gyűrűje
$\mathbb{F}_q[x]_n$	n-nél kisebb fokú $\mathbb{F}_q$ feletti polinomok
$\mathrm{d_H}$	Hamming-távolság
$\mathrm{w_H}$	Hamming-súly (a 0-szótól való távolság)
$\mathrm{S}_{r,q}$	r paraméterű $\mathbb{F}_q$ feletti szimplex kód
$\mathrm{H}_{r,q}$	r paraméterű $\mathbb{F}_q$ feletti Hamming-kód
$\mathrm{EH}_{r,q}$	kiegészített Hamming-kód
$\mathrm{RS}_{??}$	Reed–Solomon-kód
$\mathrm{RM}_{??}$	Reed–Müller-kód

1. Zajmentes csatorna, forráskód

1.1. Entrópia = információ mennyisége = bizonytalanság mértéke

Entrópia

Legyen az X valószínűségi változó eloszlása $\{p_1, p_2, \dots, p_n\}$, ahol $p_i = p(x_i) := \mathbb{P}(X = x_i)$. Az x_i információtartalmát vagy bizonytalanságát megadó függvény nő, ha p_i csökken, és ez a bizonytalanság csak p_i-től függ, jelölje ezt $I(p_i)$. Pl. $I(1) = 0$, hisz az 1 valószínűségű kimenetel bizonytalansága 0, $I(0) = \infty$, és legyen $I(\frac{1}{2}) = 1$, azaz az $1/2$ valószínűségű esemény bizonytalanságát válasszuk egységnek (1 bit vagy 1 Shannon). Legyen

$$I(p) = \log \frac{1}{p} = -\log p.$$

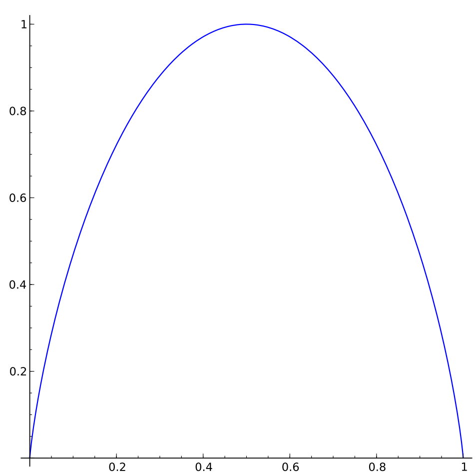
Egy valószínűségi változó entrópiáján bizonytalanságának várható értékét értjük. Ezt $H(X)$ vagy $H(p_1, p_2, \dots, p_n)$ jelöli, azaz

$$\begin{aligned} H(X) = H(p_1, p_2, \dots, p_n) &= \mathbb{E}(I(X)) = \mathbb{E}(-\log(p(X)) \\ &= \sum_{i=1}^{n} p_i \log \frac{1}{p_i} = -\sum_{i=1}^{n} p_i \log p_i. \end{aligned} \tag{1}$$

A bizonytalanság nagyságát méri az az információ, mely az eloszlatásához szükséges. A bizonytalanság, és így az információ leggyakrabban használt mértékegysége a bit (= Shannon).

A fenti képlet úgy értendő, hogy $0 \log 0 = 0$ (miért?).

A $H(p, 1-p)$ függvényre használatos a $h(p)$ jelölés is.



1. ábra. A $h(p) = H(p, 1-p) = -p \log p - (1-p) \log(1-p)$ függvény grafikonja.

1.1. feladat. Konkrét példákon gondoljuk végig, hogy az alábbi tulajdonságok joggal elvárhatók egy bizonytalanságot kifejező függvénytől.

1. Az X valószínűségi változó „bizonytalansága” nem függ mástól, mint az X valószínűségeloszlásától, és nem függ a p_i értékek sorrendjétől sem, azaz H **szimmetrikus**;
2. $H(p_1, p_2, \dots, p_n) \ge 0$, és pontosan akkor 0, ha valamely i-re $p_i = 1$;
3. H **folytonos**;
4. $H(p_1, p_2, \dots, p_n, 0) = H(p_1, p_2, \dots, p_n)$;
5. $H(p_1, p_2, \dots, p_n) \le H(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n})$;
6. $H(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n}) \le H(\frac{1}{n+1}, \frac{1}{n+1}, \dots, \frac{1}{n+1})$;
7. $H(\frac{1}{mn}, \frac{1}{mn}, \dots, \frac{1}{mn}) = H(\frac{1}{m}, \dots, \frac{1}{m}) + H(\frac{1}{n}, \dots, \frac{1}{n})$;
8. Ha $p = p_1 + \cdots + p_n$, $q = q_1 + \cdots + q_m$ és $p + q = 1$, akkor $H(p_1, \dots, p_n, q_1, \dots, q_m) = H(p, q) + pH(p_1/p, \dots, p_n/p) + qH(q_1/q, \dots, q_m/q)$ (**additivitás**).

Belátható a következő tétel:

1.2. tétel. *Ha $p_i \ge 0$ $(i = 1, \dots, n)$, és $\sum_{i=1}^{n} p_i = 1$, akkor a fenti 8 feltételt kielégítő függvény alakja*

$$H(p_1, p_2, \dots, p_n) = -c \sum_{i=1}^{n} p_i \log p_i,$$

ahol c egy tetszőleges pozitív konstans.

1.3. házi feladat. Az entrópia tulajdonságai. Mutassuk meg, hogy

1. ha az X valószínűségi változó értékkészlete n elemű, akkor $0 \le H(X) \le \log n$, és a bal oldalon egyenlőség akkor és csak akkor áll fenn, ha az X valváltozó 1 valószínűséggel konstans, míg a jobb oldalon akkor és csak akkor áll egyenlőség, ha X egyenletes eloszlású.
2. $H(X, Y) \le H(X) + H(Y)$, és egyenlőség akkor és csak akkor áll fenn, ha X és Y függetlenek.

1.4. példa. Adva van n érme, melyek közül lehet, hogy az egyik hamis, és akkor a súlya különbözik a többiétől (könnyebb vagy nehezebb). Van egy kétkarú mérlegünk, mellyel k mérést végzünk, hogy megtaláljuk a hamis érmét, és hogy megmondjuk azt is, hogy könnyebb vagy nehezebb a többinél, vagy hogy bizonyítsuk, nincs az érmék közt hamis. A mérésekkel szerezhető információ felhasználásával adjunk n-re felső becslést. (ld. még a 4.6. példát)

Megoldás. $2n+1$ lehetőség van: az n érme valamelyike nehezebb a többinél, az n érme valamelyike könnyebb a többinél, vagy mind egyforma nehéz. A feladat alapján minden esetet egyformán valószínűnek kell tekintenünk, mivel semmi információnk az eloszlásra, azaz az entrópia $\log(2n+1)$. Az egy méréssel megszerezhető információ legföljebb $\log 3$, hisz minden mérésnek 3 eredménye lehet, a mérleg balra billen, jobbra billen, egyensúlyban marad. Így k, a mérések száma minimum $\log(2n+1)/\log 3$. Innen $n \le (3^k-1)/2$.

Elemi okoskodással is megkapható ez az eredmény: minden mérésnek 3 eredménye lehet, így k méréssel 3^k különböző „állapot" különböztethető meg, így $2n+1 \le 3^k$, ami ugyancsak a fenti eredményt adja. □

1.2. Feltételes entrópia

Egy kommunikációs csatorna mindkét végén megjelenik egy valváltozó: a bemenetit jelölje X, a kimenetit Y. Kettőjük viszonyát fejezik ki a következő fogalmak. Az X, ill. Y értelmezési tartományát jelölje $\mathcal{X}$, illetve $\mathcal{Y}$.

Az $(Y|X=x)$ feltételes valószínűségi változó eloszlása

$$\mathbb{P}(Y=y|X=x) = p(y|x) = \frac{p(x,y)}{p(x)}, \quad y \in \mathcal{Y}$$

Az $(Y|X=x)$ entrópiája

$$H(Y|X=x) = -\sum_{y\in\mathcal{Y}} p(y|x)\log p(y|x).$$

A $H(Y|X)$ feltételes entrópia definíciója:

$$\begin{aligned} H(Y|X) &= \sum_{x\in\mathcal{X}} p(x) H(Y|X=x) \\ &= -\sum_{x\in\mathcal{X}} p(x) \sum_{y\in\mathcal{Y}} p(y|x)\log p(y|x) \\ &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(y|x) \end{aligned}$$

1.5. házi feladat. Mutassuk meg, hogy

1. $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$.
2. $0 \le H(X|Y) \le H(X)$, és a bal oldalon egyenlőség csak akkor áll fenn, ha 1 valószínűséggel függvénye X az Y-nak, míg a jobb oldalon csak akkor áll egyenlőség, ha X és Y függetlenek.

Az X és Y valváltozók **kölcsönös információján** az

$$I(X,Y) = H(X) + H(Y) - H(X,Y)$$

mennyiséget értjük.

1.6. házi feladat. A kölcsönös információ tulajdonságai. Mutassuk meg, hogy

1. $I(X,Y) = \sum_{x,y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}$
2. $I(X,Y) \ge 0$,
3. $I(X,Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$, azaz X bizonytalansága $I(X,Y)$-nal csökken, ha ismerjük Y-t,
4. $I(X,Y) \le H(X)$, $I(X,Y) \le H(Y)$.

1.3. Egyértelmű dekódolhatóság

A következőkben a forrásábécé legyen a véges $\mathcal{X}$, a kódábécé a véges $\mathcal{Y}$ halmaz. A kódszavak az $\mathcal{Y}^*$ elemei, azaz az $\mathcal{Y}$ elemeiből álló véges hosszú sorozatok.

Egy $f: \mathcal{X} \to \mathcal{Y}^*$ függvényt **kódnak** nevezünk, az $\mathcal{X}^*$ elemeit **üzeneteknek**. Az $f: \mathcal{X} \to \mathcal{Y}^*$ kód egyértelműen dekódolható, ha bármely két $\mathbf{u} \ne \mathbf{v}$ üzenet esetén $f(u_1)f(u_2)\dots f(u_k) \ne f(v_1)f(v_2)\dots f(v_m)$. Az f kód **prefix**, ha egyik kódszó sem folytatása egy másiknak. Egy prefix kód egyértelműen dekódolható. Az $f(x)$ kódszó hosszát $|f(x)|$ jelöli.

1.7. tétel (McMillan)**.** *Minden egyértelműen dekódolható $f: \mathcal{X} \to \mathcal{Y}^*$ kódra*

$$\sum_{i=1}^{n} s^{-|f(x_i)|} \le 1,$$

ahol $n = |\mathcal{X}|$ és $s = |\mathcal{Y}|$.

Bizonyítás. Mivel

$$\begin{aligned} \left(\sum_{i=1}^{n} s^{-|f(x_i)|}\right)^N &= \sum_{i_1=1}^{n}\cdots\sum_{i_N=1}^{n} s^{-|f(x_{i_1}|-\dots-|f(x_{i_N}|} \\ &= \sum_{l=1}^{NL} A_l s^{-l}, \end{aligned}$$

ahol $L = \max_{1\le i\le n}|f(x_i)|$, és A_l az összes olyan l-hosszú kódbetűsorozatok száma, melyek N kódszó egymás után írásával keletkeztek. Az összes ilyen sorozat különböző az egyértelmű dekódolhatóság miatt, ezért $A_l \le s^l$. Így

$$\left(\sum_{i=1}^{n} s^{-|f(x_i)|}\right)^N \le NL,$$

azaz

$$\sum_{i=1}^{n} s^{-|f(x_i)|} \le \sqrt[N]{NL} \to 1,$$

ami bizonyítja az állítást. □

1.8. tétel (Kraft)**.** *Ha az $l_1, l_2, \dots, l_n$ pozitív egészekre*

$$\sum_{i=1}^{n} s^{-l_i} \le 1,$$

akkor létezik olyan f prefix kód, hogy $|f(x_i)| = l_i$, ahol $i = 1,\dots,n$.

1.4. Zajmentes kódolási tétel

1.9. tétel (Zajmentes kódolási tétel)**.** *Legyen X diszkrét valószínűségi változó. Ekkor létezik olyan $E: \mathcal{X} \to \{0,1\}^*$ és $D: \{0,1\}^* \to \mathcal{X}$ függvény, hogy minden $x \in \mathcal{X}$ elemre $D(E(x)) = x$, továbbá*

$$\mathop{\mathbb{E}}_{x\in\mathcal{X}}(|E(x)|) \in [H(X), H(X)+1].$$

2. Zajos csatorna, hibajavítás

2.1. Példák

2.1. definíció. Legyen $x, y \in \mathcal{Y}^n$ két kódszó. Hamming-távolságuk

$$\mathrm{d_H}(x, y) = |\{i : x_i \neq y_i,\ 1 \leq i \leq n\}|$$

Könnyen igazolható, hogy $\mathrm{d_H}$ valóban távolság, azaz metrika:

(1) $\mathrm{d_H}(x, y) \geq 0$,

(2) $\mathrm{d_H}(x, y) = 0 \iff x = y$,

(3) $\mathrm{d_H}(x, y) = \mathrm{d_H}(y, x)$ (szimmetria),

(4) $\mathrm{d_H}(x, y) + \mathrm{d_H}(y, z) \geq \mathrm{d_H}(x, z)$ (háromszög-egyenlőtlenség).

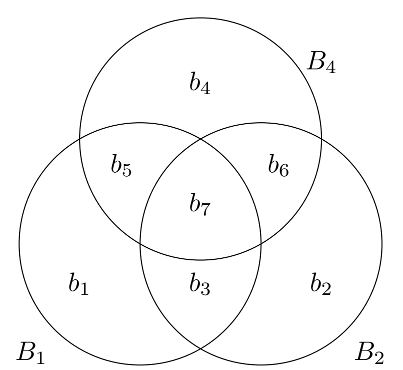
Például $\mathrm{d_H}(1022011, 1012012) = 2$.

2.2. példa (Alappéldák)**.** Az alábbi öt példára többször fogunk hivatkozni.

(a) Ismétlő kód. $a \in \mathcal{X} \mapsto aa\dots a \in \mathcal{X}^n$. Legföljebb $n-1$ hibát jelez, és $\lfloor \frac{n-1}{2} \rfloor$ hibát javít (hogyan?).

(b) Paritásellenőrző kód, nullösszegű kód. $(b_1, \dots, b_{n-1}) \in \mathbb{F}_2^{n-1} \mapsto (b_1, \dots, b_{n-1}, b_1 + \dots + b_{n-1}) \in \mathbb{F}_2^n$. A kód utolsó bitjét szokás paritásbitnek nevezni. Hibát javítani e kód nem tud, de egy hibát jelez (valójában páratlan sokat). Általánosítása a nullösszegű kódolás: $(a_1, \dots, a_{n-1}) \in \mathbb{F}_q^{n-1} \mapsto (a_1, \dots, a_{n-1}, -\sum_{i=1}^{n-1} a_i) \in \mathbb{F}_q^n$. E kódolásoknál pontosan azok a kódszavak, melyek koordinátáinak összege 0.

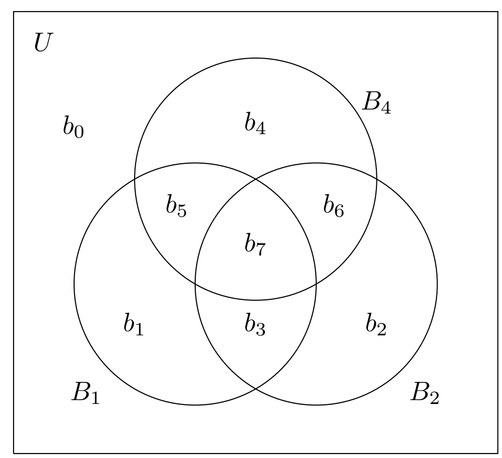
(c) Bináris $[7, 4, 3]_2$ **Hamming-kód.** $\mathbb{F}_2^4 \to \mathbb{F}_2^7 : (b_3, b_5, b_6, b_7) \mapsto (b_1, \dots, b_7)$, ahol $b_1 = b_3 + b_5 + b_7$, $b_2 = b_3 + b_6 + b_7$, $b_4 = b_5 + b_6 + b_7$. A biteket Venn-diagramban ábrázolhatjuk. Legyen B_1, B_2, B_4 három halmaz. B_{2^k} pontosan akkor tartalmazza a b_i bitet, ha i bináris alakjában a k-adik bit 1 (ld. a 2.2. ábrát). Innen



2. ábra. Hamming-kód konstrukciója

könnyen látható, hogy egy $(b_1, \dots, b_7)$ bitsorozat pontosan akkor kódszó, ha a B_j ($j = 1, 2, 4$) halmazok mindegyikében páros sok bit egyes. Ami még érdekesebb, az is igaz, hogy bármely $\mathbb{F}_2^7$-beli vektor vagy kódszó, vagy egyértelműen kódszóvá változtatható egyetlen bit megváltoztatásával, azaz e kód képes egy bithibát javítani. Pl. ha a B_2 halmazban páratlan sok bit egyes, akkor a $\bar{B}_1 \cap B_2 \cap \bar{B}_4 = b_2$ bitet kell megváltoztatni, ha a B_2 és a B_4 halmazokban is páratlan sok bit egyes, akkor a $\bar{B}_1 \cap B_2 \cap B_4 = b_6$ bitet. Ebből az is adódik, hogy bármely két kódszó Hamming-távolsága legalább 3, így e kód képes legföljebb 2 hiba jelzésére is! Innen kitalálható, hogy mit jelentenek a számok a $[7, 4, 3]$ jelölésben. Állítsuk elő e kód összes kódszavát!

(d) Kiegészített bináris $[8, 4, 4]_2$ **Hamming-kód.** $\mathbb{F}_2^4 \to \mathbb{F}_2^8 : (b_3, b_5, b_6, b_7) \mapsto (b_0, \dots, b_7)$, ahol a Hamming-kódbeli b_1, b_2, b_4 bitek mellett még egy b_0 paritásellenőrző bitet is csatolunk, azaz $b_0 = \sum_i b_i = b_3 + b_5 + b_6$. A kiegészített Hamming-kód is ábrázolható Venn-diagrammal: az U univerzumban van még egy bit, b_0, amely a B_j halmazokon kívül van, és egy vektor pontosan akkor kódszó, ha U, B_1, B_2 és B_4 mindegyikében páros sok bit egyes. Igazoljuk,



3. ábra. Kiegészített Hamming-kód konstrukciója

hogy itt bármely két kódszó Hamming-távolsága legalább 4, így e kód képes legföljebb 3 hiba jelzésére! Vagy képes egy hibát javítani és két hibát jelezni.

(e) Ternér $\mathrm{H}_{2,3}$ **Hamming-kód.** $\mathbb{F}_3^2 \to \mathbb{F}_3^4 : (a, b) \mapsto (a, b, a + b, a + 2b)$. Írjuk fel a kód összes kódszavát, és adjunk meg egy 1 hibát kijavító eljárást! Igazoljuk, hogy bármely két kódszó Hamming-távolsága legalább 3.

2.3. feladat. A magyar személyi szám 11-jegyű szám. Első jegye s_1 a tulajdonos nemét adja meg. Ezután következik a születési dátuma ($s_2 \dots s_7$), majd az egy napon születettek megkülönböztetését szolgáló véletlenszerűen generált 3-jegyű szám ($s_8 s_9 s_{10}$), végül egy ellenőrző szám (s_{11}). Ennek képzési szabálya:

$$s_{11} = \sum_{i=1}^{10} i s_i \bmod 11.$$

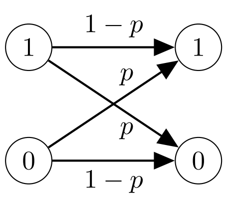
Az $s_8s_9s_{10}$ kódot úgy választják ki, hogy s_{11} ne lehessen 10, így az is egyjegyű. Mutassuk meg, hogy e kód jelzi, ha a személyi számban egy jegy hibás (1-hibajelző), és jelzi két szomszédos szám fölcserélését is. (Hasonló volt az ISBN régi 10-jegyű kódja is, ahol a 10-es maradékot X-szel, a római tízessel jelölték).

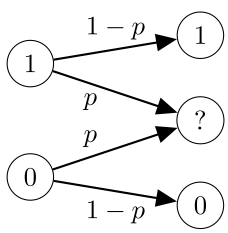
2.4. feladat. 7 halálraítélt körben ül, mindegyikük fején egy véletlenül kiválasztott piros vagy fekete sapka. Mindenki látja a többiek sapkáját, de senki se látja a sajátját. Semmi módon nem kommunikálhatnak egymással. Egy idő után egyszerre mindegyiküknek tippelnie kell a saját sapkája színére. Három válasz lehetséges: „nem tudom”, „fekete”, „piros”. Ha senki nem találja el, vagy csak egy is akad, aki téved, mind meghalnak, egyébként mind megmenekülnek. Tudunk-e számukra olyan eljárást javasolni, ami 1/2-nél nagyobb valószínűséggel megmenekíti őket. Mi a legnagyobb valószínűség, amit el tudunk érni?

2.2. Csatornamodellek

Diszkrét memóriamentes csatorna (DMC: discrete memoriless channel)

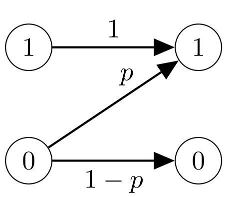
1. bináris szimmetrikus csatorna (BSC: binary symmetric channel)





2. bináris törléses csatorna (binary erasure channel)

3. z-csatorna.



2.3. Blokk-kódok

2.5. definíció. Legyen $\mathcal{Y}$ egy véges halmaz, n egy pozitív egész. A $\mathcal{C} \subseteq \mathcal{Y}^n$ halmazt $\mathcal{Y}$ fölötti (n, M)-kódnak, vagy **blokk-kód**nak nevezzük, ahol $M = |\mathcal{C}|$. Egy kölcsönösen egyértelmű $\mathcal{X} \to \mathcal{C}$ leképezést kódolásnak nevezünk. Elnevezések: $\mathcal{Y}$ a **kódábécé**, $q = |\mathcal{Y}|$ a kódábécé mérete, n a **kódhossz**, $M = |\mathcal{C}|$ a **kódméret**, $k = \log_{|\mathcal{Y}|} M = \log_q M$ a dimenzió vagy az üzenet hossza, $R = \log M/n = \frac{k}{n}\log q$ a **kódsebesség** (information rate, coding rate), $r = n - k$ a **redundancia**.

Ha a k üzenethossz egész szám, a $\mathcal{C}$ kódra az (n, M) jelölés helyett az (n, k) jelölés is használatos, illetve a kódábécé méretét is megadva $(n, k)_q$.

$\mathcal{Y}$ gyakran a q-elemű véges test, azaz $\mathcal{Y} = \mathbb{F}_q = \mathrm{GF}(q)$.

2.6. definíció (Kódtávolság, minimális távolság)**.** $d = \min_{x,y\in\mathcal{C}} \mathrm{d_H}(x, y)$. A d kódtávolságú (n, M)-, illetve (n, k)-kódot (n, M, d)-kódnak, illetve (n, k, d)-kódnak is mondjuk.

- Ha egy kód e hibát tud jelezni, akkor $d = e + 1$.
- Ha egy kód t hibát tud javítani, akkor $d = 2t + 1$ vagy $d = 2t + 2$.
- Fordítva, a d kódtávolságú kód $t = \lfloor \frac{d-1}{2} \rfloor$ hibát tud javítani és $e = d - 1$ hibát jelezni, illetve $e = d - 1$ **törléses hibát** tud javítani.

2.7. példa (Kódok paraméterei)**.**
Ismétlő kód: $k = 1$, $R = 1/n$, $d = n$.
Paritáskód, nullösszegű kód: $k = n-1$, $R = 1-1/n$, $d = 2$.
Bináris $[7, 4, 3]$ Hamming-kód: $k = 4$, $R = 4/7$, $d = 3$.
Bináris kiegészített $[8, 4, 4]$ Hamming-kód: $k = 4$, $R = 1/2$, $d = 4$.
Ternér $[4, 2, 3]$ Hamming-kód: $k = 2$, $R = 1/2$, $d = 3$.

2.4. Dekódolás, hibajavítás

A dekódolásnak kiemeljük azt a részét, amelyben a zajos csatornán átjutott c kódszó megváltozik, helyette egy x szót kapunk, melyből megpróbáljuk c-t kitalálni.

A **maximum likelihood** vagy ML-döntés az, amikor x-hez úgy választunk c-t, hogy a

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

maximális legyen.

2.8. állítás (ML dekódolás BSC-re)**.** *Mivel*

$$\mathbb{P}(x \mid c) = \prod_{i=1}^{n} \begin{cases} 1-p, & \text{ha } x_i = c_i, \\ p, & \text{ha } x_i \neq c_i. \end{cases} = (1-p)^n \left(\frac{p}{1-p}\right)^{d(x,c)}$$

ami annál nagyobb, minél kisebb $d(x, c)$, tehát az x-hez legközelebbi kódszó keresendő.

A **MAP-dekódolás** vagy MAP-döntés (maximum a posteriori – **a posteriori** = a tapasztalatból származó, **a priori** = a tapasztalatot megelőző tudás) az, amikor x-hez úgy választunk c-t, hogy a

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

maximális legyen. Ekkor legkisebb a hiba valószínűsége. Ha minden kódszó egyformán valószínű, akkor így ugyanazt kapjuk, mint ML-döntés esetén, mert

$$\mathbb{P}(c \mid x) = \frac{\mathbb{P}(x \mid c)\mathbb{P}(c)}{\mathbb{P}(x)}.$$

2.5. Csatornakódolási tétel

Egy DMC **kapacitása**

$$C = \sup_X I(X,Y).$$

Ez az X bizonytalanságának maximális csökkenése, amit Y ismerete okoz, ha az X összes lehetséges valószínűség-eloszlásaira nézzük. C csak a csatornastatisztikától függ, amelynek mátrixa $P = [p_{ij}]$, ahol $p_{ij} = \mathbb{P}(y_j \mid x_i)$. Ez sorsztochasztikus mátrix, mert

$$\sum_{j=1}^{m} p_{ij} = 1.$$

2.9. példa (Zajtalan bináris DMC kapacitása)**.** Zajtalan bináris DMC esetén a lehetséges két bemenet (0 és 1) változás nélkül jelenik meg a kimeneten, így a csatornastatisztika $P = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Határozzuk meg kapacitását!

Megoldás. A feltételek szerint $\mathbb{P}(0|0) = \mathbb{P}(1|1) = 1$. Ha $\mathbb{P}(X = 0) = p$, $\mathbb{P}(X = 1) = 1 - p$, akkor $H(X|Y = 0) = -\mathbb{P}(0|0)\log\mathbb{P}(0|0) - \mathbb{P}(1|0)\log\mathbb{P}(1|0) = 0$, hasonlóképp $H(X|Y = 1) = 0$, tehát $H(X|Y) = 0$, vagyis $I(X,Y) = H(X) - H(X|Y) = H(X) = H(p)$. Így

$$C = \sup_{p\in[0,1]} H(p) = H(\frac{1}{2}) = 1.$$

Azaz a zajtalan bináris DMC csatorna kapacitása $C = 1$. □

2.10. feladat. Mutassuk meg, hogy p valószínűségű bináris szimmetrikus csatorna (BSC) kapacitása $1 - H(p)$. (Útmutatás: a csatornastatisztika $\left[\begin{smallmatrix} p & 1-p \\ 1-p & p \end{smallmatrix}\right]$.)

2.11. feladat. Tekintsük azt a diszkrét memóriamentes csatornát, melynek csatornastatisztikája az $m \times m$-es

$$\begin{bmatrix} p & \frac{1-p}{m-1} & \cdots & \frac{1-p}{m-1} \\ \frac{1-p}{m-1} & p & \cdots & \frac{1-p}{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1-p}{m-1} & \frac{1-p}{m-1} & \cdots & p \end{bmatrix}.$$

mátrix. Mutassuk meg, hogy kapacitása

$$C = \log m + p\log p + (1-p)\log\frac{1-p}{m-1}.$$

2.12. tétel (Shannon csatornakódolási tétele)**.** *Az elérhető R kódsebességek szuprémuma egy diszkrét memóriamentes csatornán egyenlő a csatornakapacitással, tehát bármely, a csatornakapacitásnál kisebb kódsebesség tetszőlegesen nagy biztonság mellett megvalósítható, míg a csatornakapacitásnál nagyobb kódsebesség nem.*

2.13. tétel (Shannon csatornakódolási tétele BSC$_p$-re)**.** *Minden $0 \le p < \frac{1}{2}$ és $0 < \varepsilon < \frac{1}{2} - p$ számhoz van olyan $\delta > 0$ szám és egy olyan kód, melynek kódsebessége $\frac{k}{n} = 1 - H(p+\varepsilon)$, kódoló és dekódoló függvényei $E : \{0,1\}^k \to \{0,1\}^n$ és $D : \{0,1\}^n \to \{0,1\}^k$, hogy minden $m \in \{0,1\}^k$ üzenetre*

$$\mathbb{P}(D(E(m) + \mathit{zaj}) \ne m) \le 2^{-\delta n},$$

ahol zaj a BSC$_p$-ből származó zaj.

2.6. Korlátok kód méretére

2.14. tétel (Singleton-korlát)**.** *Ha $\mathcal{C}$ egy (n,k,d)-kód, akkor*

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

Ha $M = q^k$, akkor a korlát alakja $d \le n - k + 1$.

Bizonyítás. Ha d a kódtávolság, akkor nincs két kódszó, mely az első $n-d+1$ jelen megegyezne, így a szavak száma legföljebb q^{n-d+1}. Ha $M = q^k$, akkor $k \le n - d + 1$, azaz $d \le n - k + 1$. □

Azokat a kódokat, amelyekre a Singleton-korlátban egyenlőség áll **MDS-kód**oknak nevezzük (maximum distance separable). A ternér $[4,2,3]$ Hamming-kód MDS-kód. Lásd még a Reed-Solomon-kódokat.

2.15. tétel (Hamming-korlát)**.** *A d távolságú $\mathcal{C} \subseteq \mathcal{Y}^n$ ($|\mathcal{Y}| = q$) kódra*

$$|\mathcal{C}| \le \frac{q^n}{V_q(t,n)}, \quad \textit{ahol} \quad V_q(j,n) = \sum_{i=0}^{j} \binom{n}{i}(q-1)^i,$$

és $t = \lfloor\frac{d-1}{2}\rfloor$.

Bizonyítás. Ha d a kódtávolság, akkor két $t = \lfloor\frac{d-1}{2}\rfloor$-sugarú gömb nem metszheti egymást. Egy ilyen gömb „térfogata" – azaz kódszavainak száma – $V_q(t,n)$, és az egymást nem metsző gömbök számának maximuma a kódszavak számára is felső becslést ad. □

Azokat a kódokat, amelyekben itt egyenlőség áll **perfekt kód**oknak nevezzük. A bináris $[7,4,3]$ Hamming-kód perfekt kód. Minden $\mathbb{F}_q$ feletti perfekt kód (n,k,d) paraméterhármasa megegyezik az alábbiak valamelyikével:

$$\left(\frac{q^r-1}{q-1}, q^{n-r}, 3\right)_q,$$

ezek az 1-hibajavító kódok, közéjük tartoznak a Hamming-kódok, valamint

$$(23,12,7)_2 \text{ és } (11,6,5)_3,$$

ez utóbbiak neve bináris, illetve ternér Golay-kód. A ternért valójában Golay előtt 2 évvel, 1947-ben Virtakallio publikálta a Veikaaja című fociújságban.

3. Lineáris kód

3.1. Alapfogalmak

3.1. definíció. Az $\mathbb{F}_q$ test fölött értelmezett $\mathcal{C} \subseteq \mathbb{F}_q^n$ kódot **lineáris** (n,k)-kódnak nevezzük, ha $\mathcal{C}$ az $\mathbb{F}_q^n$ vektortér egy k-dimenziós altere. A lineáris kódra $(n,k)_q$ helyett az $[n,k]_q$, illetve az $[n,k,d]_q$ jelölés is használatos. Az $\mathcal{X} \to \mathcal{C}$ kódolásban általában $\mathcal{X} = \mathbb{F}_q^k$.

A definícióból következően a zérus kódszó minden lineáris kódnak eleme, és kódszavak minden lineáris kombinációja is kódszó.

A 2.2. példa kódjainak mindegyike lineáris.

3.2. feladat. Mutassuk meg a 2.2. példa kódjairól, hogy az ismétlő kód $[n,1,n]$-kód, a paritásellenőrző kód $[n,n-1,2]_2$-kód, a nullösszegű kód $[n,n-1,2]_q$-kód, a bináris Hamming-kód $[7,4,3]_2$-kód, a bináris kiegészített Hamming-kód $[8,4,4]_2$-kód, a ternér Hamming-kód $[4,2,3]_3$-kód.

Egy $c \in \mathcal{C}$ kódszó **Hamming súly**án (weight) a nemnulla komponenseinek $\mathrm{w_H}(c)$ számát értjük, azaz $\mathrm{w_H}(c) = |\{i : c_i \neq 0,\ i = 1,\dots,n\}|$. A $\mathcal{C}$ kód **minimális súlya** a legkisebb Hamming súlyú nemnulla kódszó w súlya, azaz $w = \min_{c\in\mathcal{C}, c\neq 0} \mathrm{w_H}(c)$.

3.3. tétel. *Egy lineáris $\mathcal{C}$ kód kódtávolsága megegyezik minimális súlyával, azaz $d = w$.*

Bizonyítás. Mivel $\mathcal{C}$ lineáris, ezért kódszavainak bármely lineáris kombinációja is kódszó, így, ha $x, y \in \mathcal{C}$, akkor $x - y \in \mathcal{C}$. A távolság kiszámítása így a 0-tól való távolság számításává változtatható:

$$\begin{aligned} d &= \min_{x,y\in\mathcal{C},\ x\neq y} \mathrm{d_H}(x,y) = \min_{x,y\in\mathcal{C},\ x\neq y} \mathrm{d_H}(x-y, y-y) \\ &= \min_{c\in\mathcal{C},\ c\neq 0} \mathrm{w_H}(c) = w. \end{aligned}$$

□

3.4. tétel (súlyeloszlás = távolságeloszlás)**.** *Bármely lineáris kódban a szavak súlyeloszlása megegyezik a távolságok eloszlásával.*

Bizonyítás. Legyen a $\mathcal{C}$ kódban a w súlyú kódszavak száma A_w. Ha $c \in \mathcal{C}$ egy tetszőleges kódszó, akkor az M^2 számú rendezett (c', c'') kódszó-pár között pontosan M olyan van, ahol $c' - c'' = c$. Így a w távolságú szópárok száma MA_w. □

3.2. Generátormátrix

Az, hogy $\mathcal{C}$ lineáris altér, egy egyszerű $\mathbb{F}_q^k \to \mathbb{F}_q^n$ kódolási eljárást tesz lehetővé. Legyen $g_1, g_2, \dots, g_k$ a $\mathcal{C}$ egy bázisa. Egy tetszőleges $x \in \mathbb{F}_q^k$ vektor (üzenet) $c \in \mathcal{C}$ kódja legyen $c = x_1g_1 + x_2g_2 + \cdots + x_kg_k$. Ez egy egyszerű mátrixszorzással is előállítható:

$$c = xG,$$

ahol a $k \times n$-es G mátrix – az úgynevezett **generátormátrix** – sorvektorai $\mathcal{C}$ bázisának elemei. (A kódelméletben a kódszavakat inkább sorvektorokkal szokás reprezentálni.)

3.5. példa. Írjuk fel a 2.2. példa kódjainak generátormátrixait!

(a) Ismétlő kód.
Természetesen feltesszük, hogy $\mathcal{Y} = \mathbb{F}_q$. Ekkor $\mathcal{C}$ az $(1,1,\dots,1)$ kódszó által generál egydimenziós altér $\mathbb{F}_q^n$-ben. Így $G = [1\ 1\ \dots\ 1]$.

(b) Paritásellenőrző kód, nullösszegű kód.
Az $(a_1,\dots,a_{n-1}) \in \mathbb{F}_q^{n-1} \mapsto (a_1,\dots,a_{n-1},\sum_{i=1}^{n-1} a_i) \in \mathbb{F}_q^n$ leképezés mátrixa

$$G = \begin{bmatrix} 1 & 0 & \dots & 0 & -1 \\ 0 & 1 & \dots & 0 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -1 \end{bmatrix}$$

(c) Bináris $[7,4,3]_2$ Hamming-kód.
Az $\mathbb{F}_2^4 \to \mathbb{F}_2^7 : (b_3,b_5,b_6,b_7) \mapsto (b_1,\dots,b_7)$, ahol $b_1 = b_3 + b_5 + b_7$, $b_2 = b_3 + b_6 + b_7$, $b_4 = b_5 + b_6 + b_7$ leképezés mátrixa

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{2}$$

Például az $x = (0,1,1,0)$ üzenet kódja

$$\begin{aligned} c = xG &= \begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \end{aligned}$$

(d) Kiegészített bináris $[8,4,4]_2$ Hamming-kód.
Az előző generátormátrixot itt csak egy nulladik oszloppal kell kiegészíteni a $b_0 = b_3 + b_5 + b_6$ összefüggésnek megfelelően:

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(e) Ternér $[4,2,3]_3$ Hamming-kód.
A $\mathbb{F}_3^2 \to \mathbb{F}_3^4 : (a,b) \mapsto (a, b, a+b, 2a+b)$ leképezés mátrixa

$$G = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Világos, hogy a generátormátrix nem egyértelmű, hisz a kódban maga a $\mathcal{C}$ altér fontos, az $\mathbb{F}_q^k$-nak erre való bijektív leképezése nem. Az altérnek több bázisa van, és egy bázis is többféleképp sorolható fel. Tudjuk, hogy G elemi sorműveletekkel redukált lépcsős alakra hozható, ami egyértelmű, és hogy ennek sorvektorai ugyanazt a teret generálják, mint az eredeti mátrix. A vezető egyesek oszlopait kiemelve egy egységmátrixot kapunk, így ezeken a helyeken megjelenik az üzenetvektor.

Azt mondjuk, hogy az $\mathbb{F}_q^k \to \mathcal{C}$ kódolás **szisztematikus** az $i_1,\ldots,\ i_k$ helyeken, ha az üzenet k jegye megjelenik a kódszó i_1-edik,..., i_k-adik helyein. Például a 2.2. példában megadott Hamming-kódolás szisztematikus a 3-, 5-, 6-, 7-dik helyeken.

3.6. feladat. A $\mathcal{C}$ kódnak pontosan akkor van $\mathbb{F}_q^k \to \mathcal{C}$ szisztematikus kódolása az $i_1,\ldots,\ i_k$ helyeken, ha a G mátrix i_1-edik,..., i_k-adik oszlopai lineárisan függetlenek. Ekkor elemi sorműveletekkel G mindig átalakítható olyan G' mátrixszá, mely ugyancsak $\mathcal{C}$ generátormátrixa, és a vele való kódolás szisztematikus az $i_1,\ldots,\ i_k$ helyeken.

Ha azt mondjuk, hogy egy kódolás szisztematikus, de nem adjuk meg hogy mely helyeken, akkor az azt jelenti, hogy az első k helyen. Ilyenkor a generátormátrix alakja

$$G = \left[\ I_k \ \middle|\ A_{k\times n-k}\ \right]$$

Ezt nevezzük a generátormátrix **standard alak**jának. Ekkor bármely x üzenethez tartozó $c = xG$ kódszó $c = [x|xA_{k\times n-k}]$ alakú.

Azokat a koordinátákat, ahol a kódolás szisztematikus **üzenetszegmens**nek (information set), a maradék $n-k$ koordinátából álló részt **ellenőrző szegmens**nek (vagy **paritásszegmens**nek) nevezzük, hisz ezek valóban az üzenetszegmens koordinátáinak bizonyos „ellenőrző lineáris kombinációi”.

3.3. Kódok ekvivalenciája

Elemi sorműveletekkel nem mindig érhető el, hogy egy kódolás az első k helyen szisztematikus legyen, de a koordináták permutációjával igen. Két lineáris kódot **permutációekvivalensnek** vagy egyszerűen **ekvivalensnek** nevezünk, ha a koordinátáknak egy adott permutációja erejéig megegyeznek, azaz $\mathcal{C}$ pontosan akkor ekvivalens $\mathcal{C}'$-vel ha létezik egy P permutációmátrix, hogy $c \in \mathcal{C} \iff cP \in \mathcal{C}'$. Ha G a $\mathcal{C}$ generátormátrixa, akkor $G' = GP$ a $\mathcal{C}'$-é.

Például a 2.2. példában megadott Hamming-kódolás és kiegészített Hamming-kódolás egy vele permutációekvivalens szisztematikus változatának generátormátrixa:

$$\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix},\quad \begin{bmatrix}1&0&0&0&0&1&1&1\\0&1&0&0&1&0&1&1\\0&0&1&0&1&1&0&1\\0&0&0&1&1&1&1&0\end{bmatrix}$$

A permutációk: (1745263), illetve (184)(2763)(5), a permutációmátrixok:

$$\begin{bmatrix}0&0&0&0&0&0&1\\0&0&0&0&0&1&0\\1&0&0&0&0&0&0\\0&0&0&0&1&0&0\\0&1&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&1&0&0&0\end{bmatrix} \text{ és } \begin{bmatrix}0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\\0&1&0&0&0&0&0&0\\1&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&1&0&0&0&0\end{bmatrix}$$

A $\mathcal{C}$ és $\mathcal{C}'$ kódok diagonálisan ekvivalensek, ha létezik egy olyan D diagonális mátrix, hogy $c \in \mathcal{C} \iff cD \in \mathcal{C}'$. E két ekvivalencia egyesítése a monomiális ekvivalencia, ahol $c \in \mathcal{C} \iff cM \in \mathcal{C}'$, és M monomiális mátrix, azaz minden sorában és oszlopában egyetlen nemnulla elem áll. Itt is fennáll a $G' = GD$, illetve a $G' = GM$ összefüggés.

3.7. feladat. Hány elemű a $[7,4,3]$-paraméterű Hamming-kód automorfizmuscsoportja, azaz azoknak a permutációknak a csoportja, melyek a kódszavak halmazát önmagába viszik?

3.8. feladat. Írjuk fel egy olyan monomiális mátrixot, mely ....

3.4. Ellenőrző mátrix

3.9. definíció. A $\mathcal{C}$ kód **duálisán** a

$$\mathcal{C}^\perp = \{\, v \in \mathbb{F}_q^n : v\cdot c = 0 \text{ minden } c \in \mathcal{C} \text{ kódszóra}\,\}$$

kódot értjük, mely egy lineáris kód. A $\mathcal{C}^\perp$ kód H generátormátrixát a $\mathcal{C}$ kód **ellenőrző mátrix**ának nevezzük. (Használatos még a **paritásmátrix** vagy a paritásellenőrző mátrix elnevezés is, bár paritásról csak a $q = 2$ esetben van szó.)

Azonnal látszik, hogy az ismétlő kód és a nullösszegű kód egymás duálisa, valamint hogy az ismétlő kód generátormátrixa a nullösszegű kód ellenőrző mátrixa és fordítva.

3.10. tétel. *Ha $\mathcal{C}$ egy lineáris $[n,k]$-kód, akkor*

(1) $\mathcal{C}^\perp = \{\, v \in \mathbb{F}_q^n : vG^T = 0\,\}$,

(2) $\mathcal{C}^\perp$ *egy* $[n, n-k]$*-kód,*

(3) $\mathcal{C}^{\perp\perp} := (\mathcal{C}^\perp)^\perp = \mathcal{C}$,

(4) $\mathcal{C} = \{\, c \in \mathbb{F}_q^n : cH^T = 0\,\}$,

(5) $GH^T = O_{k\times n-k}$, $HG^T = O_{n-k\times k}$,

(6) ha $G = [I_k|A]$ *a* $\mathcal{C}$ *kód standard alakú generátormátrixa, akkor ellenőrző mátrixa* $H = [-A^T|I_{n-k}]$.

Bizonyítás. (1) világos a duális kód definíciójából. Másként fogalmazva a $\mathcal{C}^\perp$ kód megegyezik G^T bal magterével. Mivel a magtér dimenziójának és a mátrix rangjának összege megegyezik a sorok számával, ezért $\dim(\mathcal{C}^\perp)+k = n$, azaz $\dim(\mathcal{C}^\perp) = n-k$, ami bizonyítja *(2)*-t. Ezt az érvelést megismételve $\mathcal{C}^{\perp\perp}$-re kapjuk, hogy $\mathcal{C}^{\perp\perp}$ egy $[n,k]$-kód. E kód tartalmazza $\mathcal{C}$-t, és dimenziójuk megegyezik, így $\mathcal{C}^{\perp\perp} = \mathcal{C}$, azaz fennáll *(3)* is. Ezután *(1)* bizonyítja *(4)*-et. Mivel minden $x \in \mathbb{F}_q^k$ vektorra $xG \in \mathcal{C}$, azaz $xGH^T = 0$, ezért GH^T csak a zérusleképezés lehet, ami bizonyítja *(5)*-öt. A *(6)*-ban megadott G és H mátrixokra a blokkmátrixok szorzási szabálya szerint $GH^T = O$, így bármely $c = xG$ kódszóra $cH^T = xGH^T = xO = 0$, tehát *(4)* szerint H valóban ellenőrző mátrix, feltéve, hogy sorai lineárisan függetlenek, ami meg nyilvánvaló. $\square$

3.11. tétel ($\mathcal{C}$ kódtávolsága – H oszlopai)**.** *Legyen H a $\mathcal{C}$ lineáris kód egy tetszőleges ellenőrző mátrixa, és $s > 0$ egész. A $\mathcal{C}$ kód kódtávolsága pontosan akkor nagyobb s-nél, ha H bármely s különböző oszlopa lineárisan független. Következésképp a $\mathcal{C}$ kód d minimális távolsága megegyezik a H mátrix lineárisan összefüggő oszlopai minimális számával.*

Bizonyítás. Megmutatjuk, hogy a H mátrix s különböző (i_1-edik,… i_s-edik) oszlopa pontosan akkor lineárisan összefüggő, ha van olyan nem nulla c kódszó, melyben a nem nulla koordináták indexei az $\{i_1, \dots, i_s\}$ halmazba esnek.

A $c \in \mathcal{C}$ kódszó súlya legyen s. Mivel $Hc^T = 0^T$, ezért H-nak van s oszlopa, melyek lineárisan összefüggők. Fordítva, ha H-nak van s lineárisan összefüggő oszlopa, akkor az ezek közti $c_{i_1}h_{i_1} + \dots + c_{i_s}h_{i_s} = 0$ lineáris összefüggést mátrixalakba írva egy olyan nem nulla, és legfeljebb s súlyú c vektorhoz jutunk, melyre $Hc^T = 0^T$, azaz amely benne van $\mathcal{C}$-ben. Tehát pontosan akkor van $\mathcal{C}$-ben legfeljebb s súlyú kódszó, ha H-ban van s lineárisan összefüggő oszlop. Ez azt jelenti, hogy ha $\mathcal{C}$ kódtávolsága d, akkor H-nak minden $d-1$ oszlopa lineárisan független, de van d lineárisan összefüggő oszlopa. □

Ezzel – kihasználva, hogy H rangja $n-k$ – a lineáris kódok esetére egy új bizonyítást adtunk a Singleton-korlátra.

3.12. tétel (Singleton-korlát lineáris kódra)**.** *Tetszőleges $\mathcal{C}$ lineáris $[n, k, d]$ kódra*

$$d \le n - k + 1.$$

A 3.11. tétel átfogalmazható a H mátrix nélkül is a $\mathcal{C}^\perp$ kódra való hivatkozással.

3.13. lemma. *A k-dimenziós $\mathcal{C} \le \mathbb{F}_q^n$ altér generátormátrixának valamely t oszlopa pontosan akkor lineárisan független, ha e koordinátapozíciókon $\mathcal{C}$-ben minden lehetséges t-hosszú vektor ugyanannyiszor, nevezetesen q^{k-t}-szer fordul elő.*

Bizonyítás. Nyilvánvaló, hisz ha az adott t oszlop lineárisan összefüggő, akkor nem állhat elő minden vektor e koordinátapozíciókon, ha pedig e t oszlop független, található $\mathcal{C}$-nek olyan bázisa, mely e pozíciókban standard, így minden t-es épp q^{k-t}-szer áll elő. □

Egy $\mathcal{C}$ kód **szilárdságán** (strength) azt a legnagyobb t számot értjük, amelyre igaz, hogy bármely t pozíción minden t-es ugyanannyiszor fordul elő. Az ilyen kód szavaiból, mint sorvektorokból képzett mátrixot t-szilárdságú **ortogonális tömbnek** (orthogonal array) nevezzük. Szokásos jelölése $\mathrm{OA}_\lambda(t, n, q)$, ha minden t-es λ-szor fordul elő.

3.14. tétel (Dualitás elve)**.** *Bármely $\mathcal{C}$ lineáris kódra*

$$d(\mathcal{C}) = t(\mathcal{C}^\perp) + 1.$$

Egy kódnak és duálisának szisztematikussága összefügg.

3.15. tétel. *A $\mathcal{C}$ kódnak pontosan akkor van szisztematikus kódolása adott k helyen, ha a $\mathcal{C}^\perp$ kódnak van a maradék $n-k$ helyen.*

Bizonyítás. Feltehető, hogy $\mathcal{C}$-nek az első k helyen van szisztematikus kódolása. Legyen $\mathcal{C}$ ellenőrző mátrixa H. Meg kell mutatni, hogy H utolsó $n-k$ oszlopa lineárisan független. Indirekt módon tegyük fel, hogy lineárisan összefüggők, azaz van olyan $0 \ne y = (0, \dots, 0, y_{k+1}, \dots, y_n)$ vektor, hogy $yH^T = 0$. Ekkor $y \in \mathcal{C}$, ami ellentmondásra vezet, hisz $\mathcal{C}$-nek van $G = [I|A]$ alakú generátormátrixa, így $y = [x|\dots]$ alakú, ahol $x = 0$, így $y = xG = 0G = 0$, ami ellentmond az $y \ne 0$ kikötésnek. Megmutattuk tehát, hogy ha $\mathcal{C}$-nek van szisztematikus kódolása valamely k helyen, akkor $\mathcal{C}^\perp$-nek van a többi $n-k$ helyen. Ezt a duális kódra is alkalmazva kapjuk a tétel állítását. □

3.16. példa. Írjuk fel a 3.5. példabeli generátormátrixokhoz tartozó ellenőrző mátrixokat egy esetleges koordinátapermutáció után a 3.10. tételbeli $H = [-A^T|I_{n-k}]$ képlettel.

(a) Ismétlő kód. A generátormátrix $[1|1\dots1]$ alakú, így

$$H = \begin{bmatrix} -1 & 1 & 0 & \dots & 0 \\ -1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \dots & 1 \end{bmatrix}$$

(b) Paritásellenőrző kód, nullösszegű kód. Itt $H = [1\dots1]$, ahol az utolsó 1-es egy 1×1-es egységmátrix.

(c) Bináris $[7,4,3]_2$ Hamming-kód. A (2) generátormátrix a (34) permutációval $[A|I]$ alakot ölt, amelyhez az $[I|-A^T]$ ellenőrző mátrix tartozik. Ezen a (34) permutáció inverze – ami önmaga – a következő mátrixot adja:

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{3}$$

(d) Kiegészített bináris $[8,4,4]_2$ Hamming-kód. Az előzőhöz hasonlóan:

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

(e) Ternér $[4,2,3]_3$ Hamming-kód. $-1 = 2$ és $-2 = 1$ felhasználásával

$$H = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix}$$

Egy $\mathcal{C}$ lineáris kód **önortogonális**, ha $\mathcal{C}^\perp \ge \mathcal{C}$, és **önduális**, ha $\mathcal{C}^\perp = \mathcal{C}$.

3.17. feladat. Egy lineáris kód generátormátrixa

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Írjuk fel generátormátrixának standard és ellenőrző mátrixának standard alakját és a kód paramétereit! Önduális-e a kód?

Megoldás. A generátormátrix elemi sorműveletekkel megkapható, hisz azok nem változtatják a mátrix sorterét:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

A standard alakból származó ellenőrző mátrixból hasonlóképp származik az ellenőrzőmátrix standard alakja:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

A kódszavak listája: 000000, 111100, 101111, 010011, 011110, 100010, 110001, 001101. Így a minimális távolság 2, a kód egy $[6,3,2]_2$-kód. Nem lehet önortogonális, mert vannak páratlan súlyú kódszavak, így önduális sem lehet. □

3.18. feladat. A páros hosszú bináris ismétlő kód és a $[7,4]$ Hamming-kód duálisa önortogonális, míg a kiegészített $[8,4]_2$ és a $[4,2]_3$ Hamming-kódok önduálisak is.

3.19. feladat. Mutassuk meg, hogy egy önduális bináris kód minden kódszava páros súlyú, egy önduális ternér kód minden kódszavának 3-mal osztható a súlya. Mutassuk meg továbbá, hogy ha egy önduális bináris kódnak van olyan bázisa, amelyben minden kódszó súlya osztható 4-gyel, akkor minden kódszó súlya osztható 4-gyel.

3.20. feladat. A SET® nevű játék 81 olyan kártyából áll, melyek rajzolatán négy különböző tulajdonság 3-3 változata különböztethető meg. A négy tulajdonság: az ábra színe (piros, zöld, lila), a figurák száma (1, 2, 3), alakja (káró, kör, pikk), és a színezés telítettsége (üres, csíkos, teli). A négy tulajdonságot egy vektor 4 koordinátájának gondolva, a kártyák mindegyikének megfelel $\mathbb{F}_3^4$ egy eleme. A játék célja kártyák egy halmazából minél több ún. SET-et kiválasztani. A SET három olyan kártya, melyek minden tulajdonság szerint vagy azonosak, vagy különbözők. Például az alábbi öt kártya között két SET is található. A kártyák alatt az $\mathbb{F}_3^4$-be való kódolásukat is megadjuk:

A	B	C	D	E
piros	piros	zöld	lila	lila
1	3	1	1	2
káró	kör	kör	pikk	kör
üres	csíkos	teli	csíkos	üres
0000	0211	1012	2021	2110

SET-et alkotnak az ACD és a BCE kártyahármasok. Például az ACD kártyák különböző színűek, azonos figuraszámúak, különböző figurák vannak rajtuk, és különböző a telítettségük is.

Megmutatható, hogy ki lehet választani a 81-ből 20 kártyát úgy, hogy ne legyen köztük SET, de 21-et már nem. Például az alábbi mátrix 20 oszlopa 20 ilyen kártya kódja:

$$M = \begin{bmatrix} 0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&2&2 \\ 0&0&0&1&1&1&2&2&2&0&0&0&1&1&1&2&2&2&1&1 \\ 0&0&1&1&1&2&0&0&1&0&1&1&0&0&2&0&1&1&0&1 \\ 0&2&1&0&2&1&0&2&1&1&0&2&0&2&1&1&0&2&1&1 \end{bmatrix}$$

Konstruáljunk e táblázat felhasználásával egy $[20,15,4]_3$ kódot!

Megoldás. Három $\mathbb{F}_3^4$-beli vektor pontosan akkor alkot SET-et, ha összegük a nullvektor, ugyanis $0+1+2=0$, $a+a+a=0$ $(a=0,1,2)$, és más számhármas összege nem 0. Az M mátrixnak tehát nincs három oszlopa, melynek összege 0 lenne. Ez még nem jelenti, hogy bármely három oszlop független, de ha kiegészítjük M-et egy csupa-1-sorral, akkor semmilyen 3 oszlopvektor lineáris kombinációja nem lesz a 0-vektor, így az ezzel az 5×20-as mátrixszal, mint ellenőrző mátrixszal képzett lineáris kód $[20,15,4]_3$ kód lesz. □

3.5. Dekódolás, szindróma

Tegyük fel, hogy egy $c \in \mathcal{C}$ kódszó helyett egy $v = c + e$ érkezik, ahol e az ún. **hibavektor**. Mivel $cH^T = 0$, ezért

$$vH^T = (c+e)H^T = cH^T + eH^T = eH^T,$$

vagyis vH^T csak a hibavektortól függ, így e vektor jelzi a hibát, orvosi hasonlattal élve olyan, mint a szindróma, mely jelzi a betegséget. Az

$$s = vH^T$$

vektort **szindrómának** nevezzük. A szindróma arra is lehetőséget ad, hogy segítségével megbecsüljük a hibavektort, és így tippeljünk az üzenetre. A ML becslésnél a minimális távolságú kódszóra tippelünk. Ha több kódszó is azonos távolságra van, véletlenül választunk közülük. A dekódolás módját egy táblázatba is foglalhatjuk, amit **standard elrendezési táblázatnak** nevezünk. Ennek első sorába a $\mathcal{C}$ kódszavai vannak írva, és minden sorába $\mathcal{C}$ egy mellékosztálya, azaz valamely e vektorral való eltoltja. Arra kell csak ügyelni, hogy minden sorban a legkisebb súlyú vektorok valamelyikét válasszuk e-nek. Világos, hogy egy mellékosztályhoz egyetlen szindróma tartozik, hisz bármely két $c_1, c_2 \in \mathcal{C}$ kódszóra $(c_1+e)H^T = (c_2+e)H^T = eH^T = s$. Így a táblázatnak q^{n-k} sora van, vagyis ennyi hibamintát tudunk javítani.

szindróma	hiba			
$s_0 = 0$	$e_0 = c_0 = 0$	c_1	$\dots$	c_{q^k-1}
s_1	e_1	$c_1 + e_1$	$\dots$	$c_{q^k-1} + e_1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$s_{q^{n-k}-1}$	$e_{q^{n-k}-1}$	$c_1 + e_{q^{n-k}-1}$	$\dots$	$c_{q^k-1} + e_{q^{n-k}-1}$

3.21. példa (Táblázatos dekódolás)**.** Tekintsük azt a kódot, melynek ellenőrző mátrixa

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Adjuk meg egy standard elrendezési táblázatát. Hány ilyen különböző táblázat létezik, azaz hány különböző dekódolás?

(1) Írjuk fel a táblázat első sorába $\mathcal{C} \subseteq \mathbb{F}_q^n$ kódszavait, elsőnek a 0-szót.

(2) Válasszunk ki az $\mathbb{F}_q^n$ megmaradt szavai közül a legkisebb súlyú e szót, és írjuk a hibaoszlopba. Adjuk ezt hozzá mindegyik kódszóhoz, és a $c + e$ összeget írjuk c oszlopába.

(3) Ismételjük meg az előző lépést, amíg $\mathbb{F}_q^n$ vektorai el nem fogynak.

(4) Írjuk minden sor fejlécébe a sorhoz tartozó szindrómát.

szindróma	hiba			
000	**00000**	11110	10101	01011
100	**10000**	01110	00101	11011
010	**01000**	10110	11101	00011
001	**00100**	11010	10001	01111
111	**00010**	11100	10111	01001
101	**00001**	11111	10100	01010
110	**11000**	**00110**	01101	10011
011	**01100**	**10010**	11001	00111

A táblázatban félkövéren szedtük azokat a vektorokat, melyeket egy adott lépésben hibavektornak választhatunk. Így e kódnak 4 különböző ML-dekódolása lehetséges.

A standard elrendezési táblázat tulajdonságai tehát a következők:

(1) A táblázat az $\mathbb{F}_q^n$ vektortér q^n elemét tartalmazza, ezek q^k oszlopba és q^{n-k} sorba vannak rendezve. Minden sor fejlécébe az adott sorhoz tartozó szindróma kerül.

(2) A táblázat minden sora a $\mathcal{C}$ egy mellékosztálya, így az egy sorban lévő két vektor különbsége mindig kódvektor. Különböző sorok különböző mellékosztályok, amik így diszjunktak, de egy sorban sem lehet két azonos vektor, hisz $c_i + e_l = c_j + e_l$ esetén $c_i = c_j$ lenne, ami $i \neq j$ miatt nem lehetséges.

(3) Minden sorban az első elem a legkisebb lehetséges súlyú, így e sorba azok a vektorok kerültek, amelyeket ezzel a vektorral, mint hibavektorral javítunk.

A táblázattal való dekódoláshoz valójában elég a fenti hibaoszlopa és a szindrómák oszlopa, ezt nevezzük szindrómatáblázatnak. Ekkor ugyanis egy tetszőleges v vektorra a táblázatból kikeressük az $s = vH^T$ szindrómához tartozó e hibavektort, és a $c = v - e$ kódszóra tippelünk.

Például a fenti kód szindrómatáblázata szindróma szerint rendezve:

szindróma	hiba
000	00000
001	00100
010	01000
011	01100
100	10000
101	00001
110	11000
111	00010

3.22. feladat. Határozzuk meg a 2.2. példabeli $[4, 2, 3]_3$ paraméterű Hamming-kód szindrómatáblázatát! Dekódoljuk a 2112 és az 1101 vektorokat!

4. Hamming kód

4.1. A Hamming kód tulajdonságai

4.1. példa. Keressünk olyan 1-hibajavító lineáris $\mathbb{F}_q$ feletti kódot, melyre k a lehető legnagyobb, ha a javításra használható jegyek $r = n - k$ száma, azaz a redundancia rögzítve van! Mutassuk meg, hogy e kód perfekt!

Megoldás. E kód H ellenőrző mátrixa $r \times n$-es, a H^T mátrix i-edik sorvektorát jelölje h_i. Legfeljebb 1 hiba esetén az e hibavektor Hamming-súlya legföljebb 1, így az $s = eH^T$ szindróma vagy a 0-vektor, vagy $e_i h_i$ valamely i-re, ahol e_i az e vektor egyetlen nem-0 koordinátája. Mivel e kód minimális távolsága 3, ezért a 3.11. tétel szerint H-nak bármely 1 és bármely 2 oszlopa lineárisan független (azaz nincs köztük a 0-vektor, és egyik sem konstansszorosa a másiknak). Rögzített $r = n - k$ mellett k maximális, ha n maximális, és n maximális értéke $(q^r - 1)/(q - 1)$. Fogalmazhatunk úgy is, hogy e feltételeknek megfelelő H mátrixot úgy kapunk, ha az $\mathbb{F}_q$ feletti $r - 1$-dimenziós projektív tér pontjainak koordinátás alakját írjuk H oszlopaiba. Ha h_i első nem-0 koordinátája mindig 1, akkor az $s = e_i h_i$ szindróma első nem-0 koordinátája épp e_i, vagyis a szindrómából az e hibavektor azonnal leolvasható.

E kód perfekt, mert $n = (q^r - 1)/(q - 1)$, azaz $1 + n(q - 1) = q^{n-k}$, tehát a Hamming-korlátban egyenlőség áll. □

4.2. definíció. Vegyünk egy olyan H mátrixot, melynek oszlopai között $\mathbb{F}_q^r$ minden nemnulla vektorának pontosan egy nem nulla konstansszorosa szerepel. (Például ilyen az a mátrix, mely az összes olyan nemnulla oszlopvektorból áll, melynek utolsó nemnulla koordinátája 1.) Azt a kódot, melynek a H mátrix az ellenőrző mátrixa, r paraméterű $\mathbb{F}_q$ feletti $\mathrm{H}_{r,q}$ **Hamming-kódnak**, duálisát $\mathrm{S}_{r,q}$ **szimplex kódnak** nevezzük. (Rögzített r és q esetén minden $\mathrm{H}_{r,q}$ kód monomiálisan ekvivalens, hasonlóképp a szimplex kódok.)

4.3. tétel. *A $\mathrm{H}_{r,q}$ Hamming-kód*

$$\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1}-r, 3\right]_q$$

paraméterű perfekt kód, a $\mathrm{H}_{2,q}$ kód $q>2$ esetén $[n, n-2, 3]_q$ paraméterű MDS-kód.

Bizonyítás. A Hamming-kód paraméterei a definícióból adódnak, $d=3$, mert H-ban bármely két oszlop független, de van három összefüggő. A kód perfektségét beláttuk a 4.1. példában. Az $r=2$ esetben a Singleton-korlát szerint $d \leq n-k+1=3$, másrészt $d=3$, így itt egyenlőség áll. □

4.4. példa. Írjuk fel a $\mathrm{H}_{2,3}$ és $\mathrm{H}_{2,4}$ kódok ellenőrző és generátormátrixát!

Megoldás. A $q=3$ esetben (felhasználva, hogy $-1=2$ és $-2=1$)

$$H=\left[\begin{array}{cc|cc}1&1&1&0\\1&2&0&1\end{array}\right] \qquad G=\left[\begin{array}{cc|cc}1&0&2&2\\0&1&2&1\end{array}\right]$$

A $q=4$ esetben legyenek a test elemei 0, 1, α, $\alpha+1$, ahol az $\mathbb{F}_2$ fölött irreducibilis $\alpha^2+\alpha+1$ polinommal végezzük a testbővítést.

$$H=\left[\begin{array}{ccc|cc}1&1&1&1&0\\1&\alpha&\alpha+1&0&1\end{array}\right] \qquad G=\left[\begin{array}{ccc|cc}1&0&0&1&1\\0&1&0&1&\alpha\\0&0&1&1&\alpha+1\end{array}\right]$$

□

4.5. feladat. Dekódoljuk a fogadott 1212121212121 szót, ha a kód ellenőrző mátrixa

$$\begin{bmatrix}1&0&1&2&0&1&2&0&1&2&0&1&2\\0&1&1&1&0&0&0&1&1&1&2&2&2\\0&0&0&0&1&1&1&1&1&1&1&1&1\end{bmatrix}.$$

4.6. példa. Az 1.4. példában n érme közül k méréssel kerestünk egy hamisat. Mi lenne a mérések sorozata az $n=12$, $k=3$ esetben?

Megoldás. Írjuk fel a számokat 1-től 12-ig a 3-as számrendszerben a $\{-1,0,1\}$ jegyeket használva. Írjuk e számokat egy táblázatba:

	1	2	3	4	5	6	7	8	9	10	11	12	Σ
3^0	1	-1	0	1	-1	0	1	-1	0	1	-1	0	0
3^1	0	1	1	1	-1	-1	-1	0	0	0	1	1	2
3^2	0	0	0	0	1	1	1	1	1	1	1	1	8

E táblázat a $\mathrm{H}_{3,3}$ ternér Hamming-kód ellenőrző mátrixának első 12 oszlopa (egy jegycsere után). Sorösszegei nem nullák, de például a 8-, 9-, 10-, 12-dik oszlopok előjelét ellenkezőjére változtatva ez is elérhető:

	1	2	3	4	5	6	7	8	9	10	11	12	Σ
3^0	1	-1	0	1	-1	0	1	1	0	-1	-1	0	0
3^1	0	1	1	1	-1	-1	-1	0	0	0	1	-1	0
3^2	0	0	0	0	1	1	1	-1	-1	-1	1	-1	0

Ezután megsorszámozzuk az érméket, és az i-edik mérés során a j-edik érmét aszerint kezeljük, hogy mi áll a táblázat i-edik sorának j-edik oszlopában. Ha ott

- 1 áll, a jobb serpenyőbe,
- -1 áll, a bal serpenyőbe,
- 0 áll, félre

tesszük. Ha nincs az érmék közt hamis, mindhárom mérés egyensúlyt mutat. Ha pl. az 5. érme nehezebb a többinél, az 1. és 2. mérésnél balra, a harmadiknál jobbra billen a mérleg, azaz egy $(-1,-1,1)$ vektort kapunk, ami épp a táblázat 5. oszlopa. Ha a három eredmény: balra–egyensúly–jobbra, azaz a mérés eredménye $(-1,0,1)$, akkor a 8. érme hamis, és könnyebb a többinél, mert a 8. oszlopban e vektor -1-szerese szerepel.

Az 1.4. példabeli $n \leq (3^k-1)/2$ becslésből $k=3$ esetén $n \leq 13$ jön ki. Vajon 13 érméből is ki tudjuk választani a hamisat? Igen, ha mindazt a lehetőséget kihasználjuk, amit a bizonyítás nem zárt ki, például hogy egy érmét ketté vágjunk, vagy felhasználjunk egy további szabályos érmét. Keressünk ilyen megoldást! Viszont **nem** a válasz, ha a fentihez hasonló megoldást keresünk. □

4.2. A szimplex kód tulajdonságai

A szimplex kód elnevezés onnan származik, hogy – mint a szimplex csúcsi – a kódszavak egyenlő távolságra vannak egymástól. Ez a távolság q^{r-1}. A 3.4. tétel szerint ezzel ekvivalens, hogy bármely nem nulla szó súlya q^{r-1}.

4.7. tétel (A szimplex kód egyenlő súlyú)**.** *Egy $\mathcal{C} \in \mathrm{S}_{r,q}$ szimplex kód minden nemnulla kódszavának q^{r-1} a súlya.*

Bizonyítás. Legyen G a $\mathcal{C} \in \mathrm{S}_{r,q}$ egy generátormátrixa. Tegyük fel, hogy van olyan szó, amelynek súlya $> q^{r-1}$. Válasszunk olyan G-t a kódhoz, melynek első sorába ezt a kódszót írjuk, majd G minden oszlopát osszuk el az oszlop legfölső elemével, ha az nem 0 vagy 1. Így egy ekvivalens kódot kapunk, melyben a skatulyaelv miatt van két azonos oszlop, hisz, $r-1$ sorba legfeljebb q^{r-1} különböző vektor írható. Ez ellentmond annak, hogy e mátrixnak bármely két oszlopa lineárisan független, hisz a Hamming-kód minimális távolsága 3.

Tegyük fel, hogy van olyan szó, amelynek súlya $< q^{r-1}$. Az előzőekhez hasonlóan egy generátormátrix első sorába ezt e vektort írva, majd minden 0-kezdetű oszlopot leosztva az első nem nulla koordinátával, $(q^r-1)/(q-1) - q^{r-1} = q^{r-2}+\cdots+q+1$ darabnál több 0-kezdetű vektort kapunk, így ismét a skatulyaelv miatt van olyan i szám, hogy a pontosan i darab 0-val kezdődő vektorból q^{r-1-i}-nél több van, vagyis van köztük két azonos. □

4.8. következmény. $\mathrm{S}_{r,q}$ *paraméterei*

$$\left[\frac{q^r-1}{q-1}, r, q^{r-1}\right]_q.$$

4.9. feladat (Bináris Hamming kód dekódolása)**.** A bináris Hamming-kód H ellenőrző mátrixát lexikografikusnak nevezzük, ha i-edik oszlopában az i szám bináris alakja szerepel (a legkisebb helyiértékű bittel az első sorban). Például $\mathrm{H}_{3,2}$ lexikografikus ellenőrző mátrixa (3). Hogyan egyszerűsödik a szindróma dekódolás?

4.10. feladat (Kódtömörítés)**.** Tegyük fel, hogy egy 40 jeles szavakból álló ternér kódot használunk, melyben mind a 3^{40} szó előfordulhat üzenetként, és ha az üzenet továbbításában egy jelhiba történik, azt a szövegkörnyezetet felhasználva még ki tudjuk javítani. Hogyan tudnánk ezt felhasználva információveszteség nélkül tömöríteni az üzenetet?

4.3. Bővített bináris Hamming-kód

A bináris Hamming-kódból egy ellenőrző összeg hozzáadásával konstruált kódot **bővített bináris Hamming-kódnak** nevezzük. Jele $\mathrm{EH}_{r,2}$.

4.11. tétel. *Az $\mathrm{EH}_{r,2}$ kód paraméterei $[2^r, 2^r - r - 1, 4]$. Ha egy bináris Hamming-kód ellenőrző mátrixa H, akkor az ellenőrző összeg első helyre írásával kapott bővített kód egyik ellenőrző mátrixa*

$$\bar{H} = \left[\begin{array}{c|c} 1 & 11\dots1 \\ \hline 0 & \\ \vdots & H \\ 0 & \end{array}\right]$$

Bizonyítás. A bővítés eggyel növeli n értékét, k pedig nem változik. A d érték is nő, mivel a minimális 3-súlyú szavak mindegyikéből 4-súlyú lesz. Így e kód paraméterei

$$[2^r, 2^r - r - 1, 4].$$

Legyen H egy bináris Hamming-kód egy tetszőleges ellenőrző mátrixa. Mivel H $r \times n$-es, ezért a paraméterekből következően egy $(r+1) \times (n+1)$-es mátrix lesz a bővített kód ellenőrző mátrixa. Elég tehát megmutatnunk, hogy $\bar{H}$ sorai lineárisan függetlenek (ez nyilvánvaló), másrészt ha $c = (c_1, \dots, c_n)$ egy Hamming kódszó, azaz $cH^T = 0$, akkor a $\bar{c} = (\sum_{i=1}^n c_i, c_1, \dots, c_n)$ szóra $\bar{c}\bar{H}^T = 0$. Ez is nyilvánvaló, a $\bar{c}$-nak a $\bar{H}$ sorvektoraival való szorzatára vagy a $cH^T = 0$ összefüggés vagy a $\sum_{i=1}^n c_i + c_1 + \dots + c_n = 0$ összefüggés használható. $\square$

Például $\mathrm{EH}_{1,2}$, $\mathrm{EH}_{2,2}$, $\mathrm{EH}_{3,2}$, $\mathrm{EH}_{4,2}$ egy-egy ellenőrző mátrixa a Hamming-kód lexikografikus ellenőrző mátrixból konstruálva:

$$\left[\begin{array}{c|c} 1 & 1 \\ \hline 0 & 1 \end{array}\right] \left[\begin{array}{c|ccc} 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right] \left[\begin{array}{c|ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$
$$\left[\begin{array}{c|ccccccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right] \tag{4}$$

4.4. Elsőrendű bináris Reed–Muller-kód

A bővített bináris $\mathrm{EH}_{m,2}$ Hamming-kód duálisát elsőrendű **Reed–Muller-kódnak** nevezzük, jelölése $\mathrm{RM}_{1,m}$. (Mivel itt az m paraméter már nem a redundanciát jelenti, nem az r betűt használjuk.) Kis m-ek esetei: $\mathrm{RM}_{1,1} = \mathbb{F}_2^2$, $\mathrm{RM}_{1,2} =$ a 4-hosszú paritásellenőrző kód, $\mathrm{RM}_{1,3} = EH_{3,2}$, mert önduális. Az $\mathrm{RM}_{1,5}$ kód érdekessége, hogy 1969-ben ezt használta a Mariner 6 és 7 a Marsról készült képek továbbításánál.

A (4) mátrixai tehát generátormátrixai e kódoknak. Ezek rekurzív tulajdonsága leolvasható e mátrixokról, ha másként blokkosítjuk:

$$\left[\begin{array}{c|c} 1 & 1 \\ \hline 0 & 1 \end{array}\right] \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 \end{array}\right] \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] \tag{5}$$
$$\left[\begin{array}{cccccccc|cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

A rekurzív összefüggés tehát:

$$H_0 = [1], \quad H_m = \left[\begin{array}{c|c} H_{m-1} & H_{m-1} \\ \hline 00\dots0 & 11\dots1 \end{array}\right]$$

4.12. tétel. *Az $\mathrm{RM}_{1,m}$ kód bináris $[2^m, m+1, 2^{m-1}]_2$-kód.*

Bizonyítás. Az $n = 2^m$, $k = m+1$ világos a definícióból. Az $\mathrm{RM}_{1,m}$ kód generátormátrixának konstrukciójából következik, hogy az $\mathrm{S}_{m,2}$ kód kódszavai egy vezető 0-val, valamint ezek komplementerei (az $111\dots1$ vektorral való összeg miatt) mind kódszavak, ezzel viszont meg is kaptuk mind a 2^{m+1} kódszót. E szavak súlya a $000\dots0$ és az $111\dots1$ kódszavakat kivéve 2^{m-1}. $\square$

Az $\mathrm{RM}_{1,m}$ kód is ekvidisztáns, hisz – a komplementer vektorpárokat kivéve – bármely két szó távolsága 2^{m-1}.

4.5. Hadamard dekódolás

Végezzük el az $\mathrm{RM}_{1,m}$ kód szavain az alábbi $\mathbb{F}_2 \to \mathbb{R}$ jelcserét: $0 \mapsto 1$, $1 \mapsto -1$. A c kódszó képét jelölje $c^{\pm} \in \{1, -1\}^n$, az így kapott kódot $\mathrm{RM}_{1,m}^{\pm}$.

4.13. lemma. $\mathrm{RM}^{\pm}_{1,m}$ *kódszavaira igazak az alábbiak:*

1. *Ha* $c^{\pm} \in \mathrm{RM}^{\pm}_{1,m}$*, akkor* $-c^{\pm} \in \mathrm{RM}^{\pm}_{1,m}$*, így a kód* 2^{m+1} *szava indexelhető úgy, hogy* $c^{\pm}_i = -c^{\pm}_j$*, ha* $|j-i| = 2^m$.

2. *Ha* $c^{\pm}_i, c^{\pm}_j \in \mathrm{RM}^{\pm}_{1,m}$*, akkor*

$$c^{\pm}_i \cdot c^{\pm}_j = \begin{cases} 2^m & \text{ha } c^{\pm}_i = c^{\pm}_j \\ -2^m & \text{ha } c^{\pm}_i = -c^{\pm}_j \\ 0 & \text{ha } c^{\pm}_i \neq \pm c^{\pm}_j. \end{cases}$$

Bizonyítás. A csupa-1 kódszóra $(1+c)^{\pm} = -c^{\pm}$, ami igazolja az első állítást.

Ha $x^{\pm}, y^{\pm} \in \{1,-1\}^n$ két tetszőleges ± 1-vektor, akkor $x^{\pm} \cdot y^{\pm} = n - 2\,\mathrm{d_H}(x^{\pm}, y^{\pm})$, ugyanis a skaláris szorzat megegyezik azon koordináták száma, ahol a két kód megegyezik $(n - \mathrm{d_H}(x^{\pm}, y^{\pm}))$, mínusz azon koordináták száma, ahol különböznek $(\mathrm{d_H}(x^{\pm}, y^{\pm}))$. Az $x^{\pm} = c^{\pm}_i$, $y^{\pm} = c^{\pm}_j$, $c^{\pm}_i \neq c^{\pm}_j$, $c^{\pm}_i \neq -c^{\pm}_j$ esetben $\mathrm{d_H}(x^{\pm}, y^{\pm}) = n/2$, ami bizonyítja a második állítást. □

A lemma szerinti indexeléssel készítsünk egy M mátrixot az $\mathrm{RM}^{\pm}_{1,m}$ kód első 2^m szavából. Például az $\mathrm{RM}^{\pm}_{1,2}$ kódnál az (5)-beli generátormátrixából kiindulva, és az 1-vektor helyett a 0-vektort használva:

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \Longrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \Longrightarrow$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \Longrightarrow M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Mivel így egyik kódszó ellentettje sem szerepel e mátrix soraiban, ezért fennáll az $MM^T = nI$ összefüggés.

Azokat az $n \times n$-es ± 1-mátrixokat, melyek eleget tesznek az

$$MM^T = nI_n \tag{6}$$

összefüggésnek, n-edrendű **Hadamard-mátrixoknak** nevezzük.

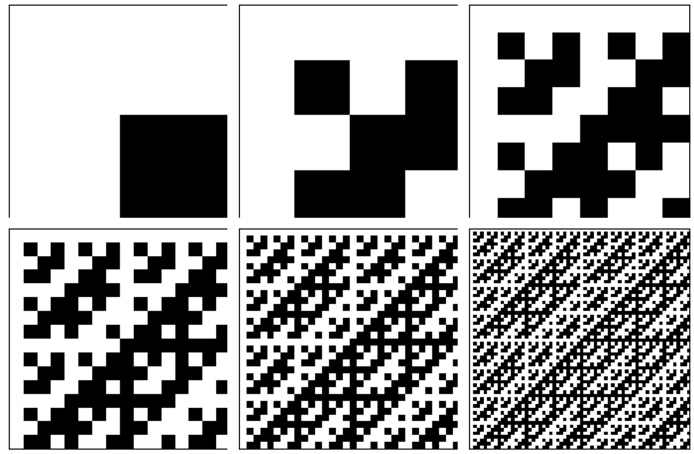
4.14. feladat. Ha M_n egy n-edrendű Hadamard mátrixot jelöl, akkor

1. $n = 1$, $n = 2$ vagy $n \equiv 0 \pmod 4$.

2. $M_n \otimes M_m$ egy nm-rendű Hadamard-mátrix ($\otimes$ a Kronecker-szorzatot jelöli).

3. Ha $M_2 = \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$, akkor a rekurzív $M_{2^n} = M_2 \otimes M_{2^{n-1}}$ összefüggés Hadamard-mátrixokat ad (ld. a 4. ábrát).

Az mindmáig nyitott kérdés, hogy milyen n-ekre létezik n-edrendű Hadamard-mátrix. Sejtés, hogy minden 4-gyel osztható értékre létezik. 1000 alatti eldöntetlen értékek: 668, 716, 892.



4. ábra. A 4.14. feladatban konstruált Hadamard mátrixok ábrázolása az $1 \mapsto$ fehér, $-1 \mapsto$ fekete megfeleletéssel.

Mivel $x^{\pm} \cdot y^{\pm} = n - 2\,\mathrm{d_H}(x^{\pm}, y^{\pm})$, ezért a ML-dekódolás azzal ekvivalens, hogy egy fogadott x szó ahhoz az c kódszóhoz van legközelebb, mellyel vett skaláris szorzata maximális abszolút értékű. A Hadamard-dekódolás az az eljárás, melyben a fogadott x szóhoz az M mátrixnak azt a sorát választjuk, amellyel vett skaláris szorzata maximális abszolút értékű, azaz amely az Mx^T legnagyobb abszolút értékű koordinátájához tartozik.

Például legyen a fogadott vektor $x = (-1,-1,-1,1,1,1,-1,-1)$. Ekkor az $M_8 x^T$ legnagyobb abszolút értékű koordinátája a 7-dik, és negatív előjelű:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} -1 \\ -1 \\ -1 \\ 1 \\ 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = \begin{bmatrix} -2 \\ -2 \\ 2 \\ 2 \\ -2 \\ -2 \\ -6 \\ 2 \end{bmatrix}$$

Ezért az M 7-dik sorvektorának -1-szerese lesz x Hadamard-dekódoltja, azaz a

$$c_{7+8} = c_{15} = (-1,-1,1,1,1,1,-1,-1)$$

kódszó. E módszer lágy dekódolásnál is ugyanúgy használható (azaz amikor nem a dekóder által meghatározott jelet, hanem a demodulátor által nyújtott, bizonytalanabb értéket kapjuk vissza). Például ha az $y = (-1.3, 0.1, 0, 0.6, 1.6, -1.1, 0.2, 0.1)$ vektort mérjük a csatornán, az $My^T = (0.2, 0.8, -1.6, 1.8, -1.4, -4.8, -2.0, -3.4)$ alapján a 6-dik sor ellentettje a legvalószínűbb üzenet.

4.15. feladat. Az r-edrendű $\mathrm{RM}_{r,m}$ Reed-Muller-kód.....

5. Ciklikus kód

5.1. Alapfogalmak

5.1. definíció. A $\mathcal{C}$ lineáris kód **ciklikus**, ha bármely $c = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$ esetén $\vec{c} = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.

Könnyen ellenőrizhető, hogy az ismétlő kód és a nullösszegű kód ciklikus, és hogy a $\mathrm{H}_{3,2}$ Hamming kód megfelelő koordinátacserével ciklikussá tehető.

A ciklikusság és a linearitás független egymástól. Például a $\{000, 110, 101, 011, 111\}$ kódban minden szó ciklikus eltoltja is kódszó, de e kód nem lineáris.

Használjuk a kölcsönösen egyértelmű

$$a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n \leftrightarrow a(x) = a_0 + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]_n$$

megfeleltetést. Az $a(x)$ az a vektorhoz (szóhoz) rendelt polinom, a az $a(x)$ polinomhoz rendelt szó. A $c \leftrightarrow c(x)$ hozzárendeléssel azonosítjuk a kódszavak e két megadását, amit a $c(x) \in \mathcal{C}$ jelöléssel is kifejezünk.

Ha $\vec{c} = (c_{n-1}, c_0, \ldots, c_{n-2})$, akkor a hozzárendelt polinom $\vec{c}(x) = c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1} = xc(x) - c_{n-1}(x^n - 1)$ azaz

$$\vec{c}(x) = xc(x) \bmod (x^n - 1).$$

Ennek alapján tetszőleges $f(x) \in \mathbb{F}_q[x]$ polinomra $f(x) \in \mathcal{C} \pmod{x^n - 1}$ azt jelöli, hogy $f(x) \bmod (x^n - 1)$ hozzárendelt kódszava $\mathcal{C}$-ben van. Elegánsabb, ha úgy tekintünk a kódra, hogy $\mathcal{C} \subseteq \mathbb{F}_q[x]/(x^n - 1)$. Például a bináris $\mathcal{C} = \{000, 110, 101, 011, 111\}$ kódra $1 + x^4 \in \mathcal{C} \pmod{x^3 - 1}$, mert $1 + x^4 = 1 + x \bmod (x^3 - 1)$, amihez az 110 szó tartozik.

5.2. tétel. *Legyen $\mathcal{C} \neq \{0\}$ egy $\mathbb{F}_q$ fölötti n-hosszú ciklikus kód.*

1. *Egyetlen minimális fokú $g(x) \in \mathcal{C}$ főpolinom létezik, és erre*
$$\mathcal{C} = \{f(x)g(x) : f(x) \in \mathbb{F}_q[x]_{n-r}\},$$
ahol $r = \deg g(x)$.

2. *$k = n - r$.*

3. *$g(x) \mid x^n - 1$ az $\mathbb{F}_q[x]$-ben, azaz van olyan $h(x) \in \mathbb{F}_q[x]_n$, hogy $g(x)h(x) = x^n - 1$.*

Bizonyítás. Először belátjuk, hogy $\bmod (x^n - 1)$ polinomok ideált alkotnak: $\mathcal{C}$ ciklikus $\rightsquigarrow x^ic(x) \in \mathcal{C} \pmod{x^n - 1}$, $\mathcal{C}$ lineáris $\rightsquigarrow \sum a_ix^ic(x) \in \mathcal{C} \pmod{x^n - 1}$, $\rightsquigarrow \forall a(x) \in \mathbb{F}_q[x]$: $a(x)c(x) \in \mathcal{C} \pmod{x^n - 1}$.

Mivel $\mathcal{C} \neq \{0\}$, van (legalább) egy minimális fokú 1-főegyütthatójú kódpolinom, legyen egy ilyen $g(x)$, foka legyen r. Az előzőek szerint minden $f(x) \in \mathbb{F}_q[x]_{n-r}$ polinomra $f(x)g(x) \in \mathcal{C}$. Megmutatjuk egyrészt, hogy g egyértelmű, másrészt, hogy minden $c(x) \in \mathcal{C}$ polinomhoz van olyan $f(x) \in \mathbb{F}_q[x]_{n-r}$, hogy $f(x)g(x) = c(x)$.

$g(x)$ egyértelmű, hisz ha létezne egy $g'(x) \neq g(x)$ főpolinom is, akkor $g(x) - g'(x) \neq 0$ kisebb fokú lenne, ami ellentmondás. (Tudjuk, az $\mathbb{F}[x]$ polinomgyűrű főideálgyűrű.)

Legyen $c(x) \in \mathcal{C}$. Ekkor létezik olyan $f(x)$ és $s(x)$ polinom, hogy $c(x) = f(x)g(x) + s(x)$, és $\deg s(x) < \deg g(x) = r$. Mivel $s(x) = c(x) - f(x)g(x)$ és a jobb oldal $\mathcal{C}$-beli, ezért $s(x)$ is, ami csak akkor lehet, ha $s(x) = 0$ és $c(x) = f(x)g(x)$.

A $\mathcal{C}$ ideál altér is, melynek dimenziója a konstrukcióból leolvasható: $n - r$.

A fentihez hasonló érveléssel: egyértelműen létezik olyan $h(x)$ és $s(x)$ polinom, hogy $\deg s(x) < \deg g(x)$, és $x^n - 1 = h(x)g(x) + s(x)$. Ekkor $s(x) \equiv (-h(x))g(x) \pmod{x^n - 1}$, azaz $s(x) \in \mathcal{C}$, ami a fokszáma miatt csak $s(x) = 0$ esetén lehetséges. □

A tételbeli $g(x)$ polinomot a $\mathcal{C}$ lineáris ciklikus kód **generátorpolinomjának**, a $h(x)$ polinomot **ellenőrző polinomjának** nevezzük.

A fenti tétel kiterjeszthető a nullvektorból álló $\mathcal{C} = \{0\}$ kódra is azzal a megállapodással, hogy ekkor $x^n - 1$ a generátorpolinom.

5.3. példa. Soroljuk fel az összes 4- és 7-hosszú bináris, ciklikus kódot!

Megoldás. A 4-hosszú kódok generátorpolinomjai osztói az $x^4 - 1 = x^4 + 1 = (x + 1)^4$ polinomnak.

$g(x)$	$\|\mathcal{C}\|$	kód
1	16	$\mathbb{F}_2^4$
$x + 1$	8	$\{1100^*, 1010^*, 0000, 1111\}$
$x^2 + 1$	4	$\{1010^*, 0000, 1111\}$
$x^3 + x^2 + x + 1$	2	$\{1111, 0000\}$
$x^4 + 1$	1	$\{0000\}$

A 7-hosszú kódok generátorpolinomjai osztói az $x^7 - 1 = x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ polinomnak.

$g(x)$	$\|\mathcal{C}\|$	kód
1	128	$\mathbb{F}_2^7$
$x + 1$	64	paritásellenőrző kód
$x^3 + x + 1$	16	$[7, 4]$ Hamming-kód
$x^3 + x^2 + 1$	16	$[7, 4]$ Hamming-kód
$x^4 + x^3 + x^2 + 1$	8	$[7, 3]$ sziplex kód
$x^4 + x^2 + x + 1$	8	$[7, 3]$ sziplex kód
$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	2	ismétlő kód
$x^7 + 1$	1	$\{0000000\}$

□

5.4. tétel. *Ha $\mathcal{C}$ egy ciklikus n-hosszú kód, akkor*

$$\mathcal{C} = \{c(x) \in \mathbb{F}_q[x]_n : c(x)h(x) \equiv 0 \pmod{x^n - 1}\}.$$

Bizonyítás. $\subseteq$: $c(x) \in \mathcal{C} \iff \exists f(x) : c(x) = f(x)g(x) \rightsquigarrow c(x)h(x) = f(x)g(x)h(x) = f(x)(x^n - 1) \equiv 0 \pmod{x^n - 1}$.

$\supseteq$: $c(x) \in \mathbb{F}_q[x]_n \rightsquigarrow c(x)h(x) = f(x)(x^n - 1) = f(x)g(x)h(x) \rightsquigarrow (c(x) - f(x)g(x))\,h(x) = 0$, de $h(x) \neq 0$ $\rightsquigarrow c(x) = f(x)g(x)$. □

5.5. feladat. Egy ciklikus kódra szindróma a következőképp is definiálható: mivel a $\mathcal{C}$ kódhoz tartozó kódpolinomok pontosan azok, amelyek a $g(x)$ generátorpolinom többszörösei, ezért egy tetszőleges $p(x)$ polinom $s(x)$ szindromája lehet a $g(x)$-szel való osztási maradéka, azaz

$$p(x) = f(x)g(x) + s(x), \quad \text{ahol } \deg s < \deg g,$$

hisz $s(x)$ pontosan akkor 0, ha $p(x)$ kódpolinom. A $p(x)$ szindrómapolinomját jelölje $s(x)$, az eltoltjához, azaz a $\vec{p}(x)$ polinomhoz tartozó szindrómát jelölje $s_1(x)$. Mutassuk meg, hogy $s_1(x)$ az $xs(x)$ polinom $g(x)$-szel való osztási maradéka. (Másként fogalmazva mutassuk meg, hogy a $p(x)$ eltoltja modulo $x^n - 1$ polinom szindrómája a $p(x)$ szindrómájának eltoltja modulo $g(x)$.)

5.2. Generátormátrixok

Világos, hogy a $g(x) = g_0 + \cdots + g_r x^r$ generátorpolinomú kód generátormátrixa

$$\begin{bmatrix} g_0 & g_1 & \dots & g_{r-1} & g_r & 0 & \dots & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_{r-1} & g_r & 0 \\ 0 & \dots & \dots & 0 & g_0 & g_1 & \dots & g_{r-1} & g_r \end{bmatrix} \tag{7}$$

ugyanis e mátrix valóban $n-k$ rangú, hisz $g_r = 1$, $(n-k)\times n$-es, és sorvektorai kódszavak. Ezt nevezik **ciklikus generátormátrixnak**. Sorlépcsős alakú a főátlóban nemnulla elemekkel, ugyanis $g(x)h(x) = x^n - 1$ miatt $g_0 h_0 = g(0)h(0) = 0^n - 1 = -1$, így $g_0 \neq 0$.

Például az $x^3 + x^2 + 1$ generátorpolinomú $[7,4]$-kód és az $x^4 + x^2 + x + 1$ generátorpolinomú $[7,3]$-kód generátormátrixai:

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \tag{8}$$

A ciklikus kódok másik szép tulajdonsága, hogy a ciklikus mátrix sorlépcsős alakú, így első k oszlopa lineárisan független, azaz a kódhoz van szisztematikus kódolás, és így standard alakú generátormátrix is.

5.6. tétel. *Egy $\mathcal{C}$ ciklikus lineáris kód*

$$m = (m_0, \dots, m_{k-1}) \mapsto (m_0, \dots, m_{k-1}, -s_0, \dots, -s_{r-1})$$

standard kódolásának maradék r koordinátája az $x^r m(x)$ polinom $g(x)$-szel való maradékos osztásából kapott $s(x) = \sum_{i=0}^{r-1} s_i x^i$ maradék együtthatóiból áll.

Bizonyítás. A maradékos osztás legyen $x^r m(x) = f(x)g(x) + s(x)$, ahol $\deg s(x) < r$. Ebből

$$f(x)g(x) = x^r m(x) - s(x) \leftrightarrow (-s_0, \dots, -s_{r-1}, m_0, \dots, m_{k-1})$$

ami $\mathcal{C}$-beli, és ennek k-szoros ciklikus eltoltja, ami ugyancsak $\mathcal{C}$-beli, épp az m üzenet keresett szisztematikus kódolása. □

5.7. példa. Határozzuk meg az x^3+x^2+1 generátorpolinomú $[7,4]$-kód és az $x^4+x^2+x+1 = (x+1)(x^3+x^2+1)$ generátorpolinomú $[7,3]$-kód standard generátormátrixát, majd bizonyítsuk, hogy a kódok egymás duálisai.

1. megoldás. A (8) generátormátrixaiból elemi sorműveletekkel megkapható a standard generátormátrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Ha a második kódot az utolsó három oszlopra szisztematizáljuk, akkor a

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

mátrixot kapjuk, ami bizonyítja, hogy az $x^3 + x^2 + 1$ generátorpolinomú és az $x^4+x^2+x+1 = (x+1)(x^3+x^2+1)$ generátorpolinomú kódok duálisai egymásnak. (Ez meglepő, mert talán azt várnánk, hogy ha $g(x)h(x) = x^n - 1$, akkor a $g(x)$ és $h(x)$ generátorpolinomú kódok legyenek egymás duálisai, de ez a sejtés nem teljesül.)

2. megoldás. A standard generátormátrix sorai megkaphatók a standard bázis kódolásával. Ezt az 5.6. tétel szerint az $x^r x^i$ $(i = 0, \dots, k-1)$ polinomok $g(x)$-szel való osztási maradékából kapjuk. Például az x^3+x^2+1 generátormátrixának harmadik sorában a 0010 üzenet, azaz az x^2 üzenetpolinom kódja szerepel. Az $x^3x^2 = (x^3+x^2+1)(x^2+x+1)+(x+1)$ maradékos osztás maradéka $x + 1$, azaz a maradék koordináták 110, így a mátrix harmadik sora 0010110. □

5.8. feladat. Mutassuk meg, hogy ha $g(x)$ egy n-hosszú bináris ciklikus kód generátorpolinomja, és

(1) $x + 1$ osztója $g(x)$-nek, akkor a kód minden kódszava páros súlyú,

(2) ha $x + 1$ nem osztója $g(x)$-nek és n páratlan, akkor a csupa 1-esből álló szó kódszó,

(3) ha az n-nél kisebb pozitív m egészekre $g(x)$ nem osztója $x^m - 1$-nek, akkor a kód minimális súlya legalább 3.

5.9. feladat. Igazoljuk, hogy ha $g(x)$ egy ciklikus $[n,k,d]$-kód generátorpolinomja, akkor $g(x^m)$ egy ciklikus $[mn, mk, d]$-kódot generál.

5.3. Fordított kód

Ciklikus kóddal ekvivalens kód nem szükségképp ciklikus. Pl. a 70 darab $[7,4]$ Hamming-kódból csak kettő ciklikus, és ezek a kódszavak megfordításával kaphatók meg egymásból.

A $\mathcal{C}$ kódból a koordináták sorrendjének megfordításával kapott $\mathcal{C}^-$ kódot **fordított kódnak** nevezzük. Ez olyan koordinátapermutáció, amely ciklikus kódot ciklikusba visz.

Egy tetszőleges m-edfokú $a(x)$ polinom fordítottján az

$$a^-(x) = \sum_{i=0}^{m} a_{m-i}x^i = x^m a(x^{-1})$$

polinomot értjük. Így ha a $c = (c_0, \dots, c_{n-1}) \in \mathcal{C}$ szóhoz rendelt polinom $c(x)$, akkor a $c^- = (c_{n-1}, \dots, c_0) \in \mathcal{C}^-$ fordított szóhoz rendelt polinom

$$c^-(x) = \sum_{i=0}^{n-1} c_{n-1-i}x^i = x^{n-1}c(x^{-1}).$$

5.10. állítás. *Ha a ciklikus $\mathcal{C}$ kód egy generátorpolinomja $g(x)$, akkor a $g_0^{-1}g^-(x)$ polinom a $\mathcal{C}^-$ kódot generálja.*

Bizonyítás. A (7) ciklikus generátormátrixból a sorok nemnulla részének megfordításával kapott alábbi mátrix a $\mathcal{C}^-$ generátormátrixa:

$$\frac{1}{g_0}\begin{bmatrix} g_r & g_{r-1} & \dots & g_1 & g_0 & 0 & \dots & \dots & 0 \\ 0 & g_r & g_{r-1} & \dots & g_1 & g_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & g_r & g_{r-1} & \dots & g_1 & g_0 & 0 \\ 0 & \dots & \dots & 0 & g_r & g_{r-1} & \dots & g_1 & g_0 \end{bmatrix}$$

Mivel $g_r = 1$, ezért e mátrix sorai függetlenek, mindegyikük a $\mathcal{C}^-$ kódból való, és a sorok száma a kód dimenziójával megegyezik, így e mátrix valóban a $g_0^{-1}g^-(x)$ főpolinomhoz tartozó generátormátrix. □

5.4. Ciklikus kód duálisa

Jellemezzük ciklikus kód duálisát. Ehhez a fordított kódot használjuk.

5.11. tétel. *Ciklikus kód duálisa ciklikus. Ha az n-hosszú $\mathcal{C}$ ciklikus kód ellenőrző polinomja $h(x)$, akkor $\mathcal{C}^\perp$ generátorpolinomja $h_0^{-1}h^-(x)$.*

Bizonyítás. A duális kód ciklikussága triviális. Legyen $g(x)$ és $h(x)$ a $\mathcal{C}$ kód generátor- és ellenőrző polinomja (tehát $g(x)h(x) = x^n - 1$), és legyen a $h(x)$ által generált kód $\mathcal{D}$. Így

$$\mathcal{C} = \{a(x)g(x) : a(x) \in \mathbb{F}_q[x]_{n-r}\},$$
$$\mathcal{D} = \{b(x)h(x) : b(x) \in \mathbb{F}_q[x]_r\}.$$

Legyen $c \in \mathcal{C}$, $d \in \mathcal{D}$ két kódszó, és a hozzájuk rendelt polinomok $c(x) = a(x)g(x)$, $d(x) = b(x)h(x)$. Ekkor $c(x)d(x) = a(x)g(x)b(x)h(x) = a(x)b(x)(x^n - 1)$. Mivel $\deg a(x) \le n-r-1$ és $\deg b(x) \le r-1$, ezért $\deg(a(x)b(x)) \le n-r-1+r-1 = n-2$, így $c(x)d(x)$-ben x^{n-1} együtthatója 0, azaz

$$0 = \sum_{i=0}^{n-1} c_i d_{n-1-i} \quad = (c_0, \dots, c_{n-1}) \cdot (d_{n-1}, \dots, d_0) = c \cdot d^-$$

Eszerint $\mathcal{C}$ minden kódszava merőleges $\mathcal{D}^-$ minden kódszavára, tehát $\mathcal{D}^- \subseteq \mathcal{C}^\perp$. Másrészt $\dim \mathcal{C}^\perp = r = \deg h^-(x) = \dim \mathcal{D}^-$, tehát $\mathcal{C}^\perp = \mathcal{D}^-$. □

Az 5.7. példa duális kódjainak generátorpolinomjai a $g(x) = x^4+x^2+x+1 = (x+1)(x^3+x^2+1)$ és $h(x) = x^3+x+1$ jelölésekkel $g(x)$ és $h^-(x) = x^3h(x^{-1}) = x^3(x^{-3}+x^{-1}+1) = 1 + x^2 + x^3$.

6. Súlyfüggvény

Távolság- és súlyfüggvény

6.1. definíció. Legyen $\mathcal{C}$ egy tetszőleges n-hosszú kód. **Távolságeloszlása**

$$A_i = \frac{1}{|\mathcal{C}|}\left|\{(c, c') \mid c, c' \in \mathcal{C},\ d(c, c') = i\}\right| \quad i = 1, 2, \dots, n.$$

A $\mathcal{C}$ **távolságpolinomja**:

$$W_{\mathcal{C}}(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i.$$

Lineáris kód esetén a távolságeloszlás és a távolságpolinom megegyezik a kód **súlyeloszlásával**, illetve **súlypolinomjával**, amelyben

$$A_i = \left|\{c \mid \mathrm{w_H}(c) = i\}\right|.$$

Duális kód súlyfüggvénye

6.2. tétel (MacWilliams-formula). *Ha $\mathcal{C}$ egy $\mathbb{F}_q$ fölötti n-hosszú lineáris kód, akkor $\mathcal{C}^\perp$ súlyfüggvénye*

$$W_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x + (q-1)y, x - y).$$

Bizonyítás. (Chang–Wolf, 1980)

Tekintsük $\mathbb{F}_q^n$-et eseménytérnek, elemeit egy üzenet elküldésekor keletkező hibavektornak. Ha egy karakter hibájának valószínűsége p, akkor egy $x \in \mathbb{F}_q^n$ vektor valószínűsége

$$\mathbb{P}(x) = \left(\frac{p}{q-1}\right)^{\mathrm{w_H}(x)} (1-p)^{n-\mathrm{w_H}(x)}$$

Egy $S \subseteq \mathbb{F}_q^n$ valószínűsége $\mathbb{P}(S) = \sum_{x \in S} \mathbb{P}(x)$. Annak valószínűsége, hogy egy vektor épp kódszó:

$$\mathbb{P}(\mathcal{C}) = \sum_{i=0}^{n} A_i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i} = W_{\mathcal{C}}(1-p, \frac{p}{q-1}).$$

$\mathbb{P}(\mathcal{C})$ értékét másként is kiszámoljuk (kettős leszámlálás). Tekintsük az összes olyan (c, c') vektorpárt, ahol $c \cdot c' \neq 0$ és $c' \in \mathcal{C}^\perp$. Ekkor

$$\sum_{(c,c')} \mathbb{P}(c) = (1 - \mathbb{P}(\mathcal{C}))(q^{n-k} - q^{n-k-1}),$$

ugyanis $c \notin \mathcal{C}$ és a c-re merőleges vektorok $\mathcal{C}^\perp$-ből egy $n-k-1$-dimenziós alteret vágnak ki. Ezután rögzítsünk egy $c' \in \mathcal{C}^\perp$ szót, és számoljuk össze, mennyivel járul hozzá a fönti összeghez! A c' súlya legyen w. Jelölje $f(j)$ azoknak a j-eseknek a számát, amelyek csupa nemnulla elemből állnak és összegük sem nulla. Látható, hogy $f(1) = q-1$ és $f(j) = (q-1)^j - f(j-1)$, amiből $f(j) = \frac{q-1}{q}((q-1)^j - (-1)^j)$. Így c' hozzájárulása

$$\sum_{j=1}^{w} (1-p)^{w-j} \left(\frac{p}{q-1}\right)^j f(j) = \frac{q-1}{q}\left(1 - \left(1 - \frac{pq}{q-1}\right)^w\right).$$

Innen összegzés után $\mathbb{P}(\mathcal{C})$ kifejezhető:

$$\begin{aligned}\mathbb{P}(\mathcal{C}) &= 1 - \frac{1}{q^{n-k} - q^{n-k-1}} \sum_{c' \in \mathcal{C}^\perp} \frac{q-1}{q}\left(1 - \left(1 - \frac{pq}{q-1}\right)^w\right) \\ &= \frac{1}{q^{n-k}} \sum_i A'_i \left(1 - \frac{pq}{q-1}\right)^i \\ &= \frac{1}{|\mathcal{C}^\perp|} W_{\mathcal{C}^\perp}(1, 1 - \frac{pq}{q-1})\end{aligned}$$

Végül kaptuk, hogy

$$W_{\mathcal{C}}(1-p, \frac{p}{q-1}) = \frac{1}{|\mathcal{C}^\perp|} W_{\mathcal{C}^\perp}(1, 1 - \frac{pq}{q-1})$$

Ez az $x = 1-p$, és $y = p/(q-1)$ helyettesítéssel, a $\mathcal{C}$ és duálisának fölcserélésével a bizonyítandó képletet adja. □

6.3. feladat. Egyváltozós súlypolinomnak az

$$A_{\mathcal{C}}(z) = W(1, z) = \sum_i A_i z^i$$

polinomot nevezzük. Igazoljuk, hogy

$$A_{\mathcal{C}^\perp} = q^{-k}(1 + (q-1)z)^n A_{\mathcal{C}}\left(\frac{1-z}{1+(q-1)z}\right).$$

6.4. feladat. Határozzuk meg a $[7,4,3]_2$ Hamming-kód súlypolinomját, és ellenőrizzük duálisának súlypolinomját a MacWilliams-tétellel.

7. BCH-kód

Bose, Ray-Chaudhuri és Hocquenghem (BCH) által konstruált kód:

7.1. definíció. Egy n-hosszú, $\mathbb{F}_q$ fölötti, legalább t hibát javító kódot konstruálunk:

- Meghatározzuk azt a legkisebb m egészt, melyre $\mathbb{F}_{q^m}$-nek van egy a primitív n-edik egységgyöke.
- Választunk egy nemnegatív b egészt.
- Meghatározzuk a következő $2t$ elem mindegyikének minimálpolinomját: a^b, a^{b+1},…, a^{b+2t-1}.
- A generátorpolinom ezek legkisebb közös többszöröse.

E kód neve **BCH-kód**. Ezt **szűkebb értelemben vett BCH-kódnak** nevezzük, ha $b = 1$, és **primitívnek**, ha $n = q^m - 1$.

7.2. tétel (A BCH-korlát)**.** *Legyen $\mathcal{C}$ egy ciklikus $[n,k]_q$-kód a g generátorpolinommal. Legyen $\mathbb{F}_{q^m}$ az $\mathbb{F}_q$ legkisebb olyan testbővítése, melyben van primitív n-edik egységgyök, jelölje ezt a. Legyen g minimális fokú olyan polinom, melynek az egymást követő $2t$ darab a^b, a^{b+1},…, a^{b+2t-1} hatvány mindegyike gyöke. Ekkor $d \geqslant 2t+1$.*

A becslés nem mindig éles.

Bizonyítás. Könnyen fölírható a kód ellenőrző mátrixa: mivel minden kódpolinom $c(x) = m(x)g(x)$ alakú és $c(a^i) = m(a^i)g(a^i) = m(a^i)0 = 0$, ahol $i = b, b+1, \dots, b+2t-1$. Ezért ha $c(x) = \sum_i c_i x^i$, akkor $c(a^i) = (c_0, c_1, c_2, \dots, c_{n-1}) \cdot (1, a^i, a^{2i}, \dots, a^{(n-1)i}) = 0$, ahol $i = b, b+1, \dots, b+2t-1$. Innen

$$H = \begin{bmatrix} 1 & a^b & a^{2b} & \dots & a^{(n-1)b} \\ 1 & a^{b+1} & a^{2(b+1)} & \dots & a^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a^{b+2t-1} & a^{2(b+2t-1)} & \dots & a^{(n-1)(b+2t-1)} \end{bmatrix}$$

Ha volna $2t+1$-nél kisebb súlyú c szó, akkor $Hc^T = 0$ miatt kiválasztva H-ból a c nemnulla koordinátáinak megfelelő oszlopokat és ugyanannyi sort, egy olyan négyzetes mátrixot kapnánk, melynek determinánsa egyrészt 0, hisz oszlopai lineárisan összefüggők a c elemeivel vett lineáris kombinációk miatt, másrészt nem lehet 0, mivel determinánsa Vandermonde-determináns különböző elemekkel. □

8. Általánosított Reed–Solomon-kód

Reed és Solomon 1960-ban definiálta.

8.1. definíció. Legyen $v = (v_1, v_2, \dots, v_n) \in \mathbb{F}^n$ nemnulla elemű, $a = (a_1, a_2, \dots, a_n) \in \mathbb{F}^n$ csupa különböző elemből álló vektor ($n \leqslant |\mathbb{F}|$), és legyen $0 \leqslant k \leqslant n$ egész. Ekkor a

$$\mathrm{GRS}_{n,k}(a, v) = \{\, (v_1 c(a_1), v_2 c(a_2), \dots, v_n c(a_n)) \mid c(x) \in \mathbb{F}[x]_k \,\}$$

kódot **általánosított Reed–Solomon-kódnak** nevezzük. Itt a $c(x)$ polinomhoz tartozó kódszót fogjuk c-vel jelölni. (A $v = (1, 1, \dots, 1)$ esetben e kódot **Reed–Solomon-kódnak** nevezzük.)

8.2. tétel. $\mathrm{GRS}_{n,k}(a,v)$ *lineáris* $[n,k,n-k+1]$*-kód, tehát MDS-kód.*

Bizonyítás. A linearitás nyilvánvaló a definícióból, ugyanis a $c_1 \leftrightarrow c_1(x)$ és a $c_2 \leftrightarrow c_2(x)$ megfeleletetésekből $sc_1 + c_2 \leftrightarrow sc_1(x) + c_2(x)$ adódik tetszőleges s konstansra.

Legyen $c_1(x), c_2(x) \in \mathbb{F}[x]_k$ két különböző polinom. Ekkor $c_3(x) = c_2(x) - c_1(x) \neq 0$ és k-nál kisebb fokú, továbbá $c_3 = c_2 - c_1$ és $\mathrm{w_H}(c_3) = \mathrm{d_H}(c_1, c_2)$. c_3-nak is legföljebb $k-1$ zérushelye van, ezért $\mathrm{w_H}(c_3) \geqslant n-(k-1)$, de ez a korlát el is érhető, ha $c_3(x) = \prod_{i=1}^{k-1}(x-a_i)$, tehát e kódra a Singleton korlát éles, azaz MDS-kód. □

8.3. tétel. *Legyen* $u = (u_1, u_2, \dots, u_n)$*. Ekkor*

$$\mathrm{GRS}_{n,k}(a,v)^\perp = \mathrm{GRS}_{n,n-k}(a,u), \text{ ahol } L_i(x) = \prod_{\substack{j=1\\ j\neq i}}^{n}(x-a_j),$$

és $u_i^{-1} = v_i L_i(a_i)$*.*

Bizonyítás. Legyen $c \in \mathrm{GRS}_{n,k}(a,v)$, $d \in \mathrm{GRS}_{n,n-k}(a,u)$. Elég megmutatnunk, hogy merőlegesek. Mivel $c(x)$ foka kisebb, mint k, $d(x)$ foka kisebb, mint $n-k$, ezért $c(x)d(x)$ foka kisebb, mint $n-1$, azaz az x^{n-1} együtthatója 0. A $c(x)d(x)$ Lagrange-féle interpolációs polinomja

$$c(x)d(x) = \sum_{i=1}^{n} \frac{L_i(x)}{L_i(a_i)} c(a_i)d(a_i),$$

ezért az x^{n-1} együtthatója

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \frac{1}{L_i(a_i)} c(a_i)d(a_i) \\ &= \sum_{i=1}^{n} (v_i c(a_i)) \left(\frac{1}{v_i L_i(a_i)} d(a_i) \right) \\ &= \sum_{i=1}^{n} (v_i c(a_i))(u_i d(a_i)) = c \cdot d. \end{aligned}$$

□

9. Kódok konstrukciója kódokból

Egy kód módosítása az n, k vagy r valamelyike értékének rögzítése mellett az 1. táblázatban felsorolt hat módon lehetséges.

9.1. példa (Általánosított Reed–Solomon-kódok)**.** Kódnöveléssel, illetve részkódképzéssel származtathatók egymásból az általánosított Reed–Solomon-kódok, ugyanis

$$\mathrm{GRS}_{n,k}(a,v) \geqslant \mathrm{GRS}_{n,k-1}(a,v).$$

9.2. példa (Résztest részkód)**.** Legyen $\mathbb{F}_q \leqslant \mathbb{F}_{q^m}$ két test, és legyen $\mathcal{C}$ egy $\mathbb{F}_{q^m}$ fölötti lineáris kód. Ekkor a $\mathcal{C}$ kód $\mathbb{F}_q$ fölötti szavai részkódot alkotnak.

	n	k	r	Megjegyzés, példa
Kódnövelés (augmenting)	=	↑	↓	új kódszavak hozzávétele
Részkódképzés (expurgating)	=	↓	↑	kódszavak törlése
Kódbővítés kiegészítés (extending)	↑	=	↑	új ellenőrző összeg (új oszlop a generátormátrixban)
Kipontozás (puncturing)	↓	=	↓	redundáns koordináták (oszlopok generátormátrixból) törlése
Nyújtás (lengthening)	↑	↑	=	a generátormátrix keretezése (bordering), azaz oszlopok és azonos számú sorok hozzáadása
Rövidítés (shortening)	↓	↓	=	generátormátrixból sorok törlése, majd a 0-oszlopok lehagyása

1. táblázat. Kód módosításai

9.3. feladat. Igazoljuk, hogy egy d kódtávolságú kód t törléses hibát és e hibát tud javítani, ha $t + 2e + 1 \leqslant d$.

9.4. példa (Kódbővítés jellemzése)**.** Legyen $\mathcal{C}$ egy $[n,k]_q$ kód. $\mathcal{C}$ minden egy koordinátával való kódbővítése megkapható úgy, hogy választunk egy $g \notin \mathcal{C}^\perp$ vektort (vagy ami ezzel ekvivalens: egy $\mathcal{C}_0 \leqslant \mathcal{C}$ lineáris $[n,k-1]_q$ kódot, hogy $g \in \mathcal{C}_0^\perp \setminus \mathcal{C}^\perp$), és minden c kódszóhoz hozzáadjuk a $g \cdot c$ skalárt $(n+1)$-edik koordinátaként. Ha G_0 a $\mathcal{C}_0$ generátormátrixa, akkor a kiegészített kód generátormátrixa

$$\left[\begin{array}{c|c} G_0 & 0 \\ \hline c' & g \cdot c' \end{array}\right]$$

ahol $c' \in \mathcal{C} \setminus \mathcal{C}_0$ egy kódszó. Ugyanehhez a kódbővítéshez jutunk, ha g-t bármely másik $g + \mathcal{C}^\perp$ vektorral helyettesítjük.

9.5. példa (Hamming-kód rövidítése)**.** A $[7,4,3]$ Hamming-kód egy $[5,2,3]$-kóddá rövidíthető, ha a szisztematikus generátormátrixból töröljük az első két sort és oszlopot:

$$\begin{bmatrix} 1&0&0&0&0&1&1\\ 0&1&0&0&1&0&1\\ 0&0&1&0&1&1&0\\ 0&0&0&1&1&1&1 \end{bmatrix} \Longrightarrow \begin{bmatrix} 1&0&1&1&0\\ 0&1&1&1&1 \end{bmatrix}.$$

E kód szavai: 00000, 10110, 01111, 11001. Hasonlóképp, ha az $[n,k]$ paraméterű kód generátormátrixa $[I|A]$, akkor annak első i sorát és oszlopát törölve egy $[n-i, k-i]$ kód generátormátrixát kapjuk.

9.6. feladat. Igazoljuk, hogy a $\mathrm{GRS}_{n,k}(a,v)$ kód rövidítésével (pl. a 0-ra végződő kódszavak megtartásával, majd az utolsó koordináta törlésével) egy $\mathrm{GRS}_{n-1,k-1}(b,u)$ kódot kapunk. Fejezzük ki a b és u vektorokat a és v segítségével.

9.1. Kaszkád kód

Tekintsük az $\mathbb{F}_q$ és a $\mathbb{F}_{q^m}$ testeket, és legyen $\{e_1, e_2, \ldots, e_m\}$ egy bázisa $\mathbb{F}_{q^m}$-nek, mint egy $\mathbb{F}_q$ feletti vektortérnek. A következő jelölést használjuk:

$$\varphi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m; c = c_1e_1+\ldots+c_me_m \mapsto \varphi(c) = \hat{c} = (c_1, \ldots, c_m)$$

9.7. definíció (Kaszkád kód)**.** Legyen $\mathcal{C}$ egy $[n, k, d]_{q^K}$-kód, $\mathcal{C}'$ pedig egy $[N, K, D]_q$-kód. Jelölje $\hat{\mathcal{C}}$ azt az $\mathbb{F}_q$ feletti kódot, melyben a kK-hosszú üzenetszegmenst K-hosszú szegmensekre osztjuk, ezeket $\mathcal{C}'$-beli kódszavaknak tekintjük, majd φ^{-1}-zel $\mathcal{C}$-beli jelekké konvertáljuk, e k-hosszú üzenetet kódoljuk, az n-hosszú kódszóból φ egy nK-hosszú üzenetet ad, melyet $\mathcal{C}'$-ben kódolva egy nN-kódszót kapunk.

9.8. állítás. *A $\hat{\mathcal{C}}$ egy $[nN, kK, \geqslant dD]$-kód.*

9.9. definíció. Egy $[n, k, d]_{q^m}$ paraméterű $\mathcal{C}$ kód **kiterjesztésen** (expansion) olyan $\hat{\mathcal{C}}$ kaszkád kódot értünk, melyben $\mathcal{C}'$ egyszerűen az $[m, m, 1]_q$ kód.

E kódban tehát egyszerűen a $\mathcal{C}$ szavainak minden c jelét $\hat{c}$-ra cseréljük. E kód paraméterei $[nm, km, \geqslant d]$. Bár ebben a definícióban sem látszik, a kódkiterjesztés $\mathcal{C}$-n kívül a φ leképezéstől is függ.

9.10. definíció. Egy hibát f-hosszú **csomós hibának** (burst) hívunk, ha a hibavektorban legföljebb f egymás melletti nem nulla jel hibás. Például 0001101101000000 egy 7-hosszú (8-, 9-…16-hosszú) csomós hiba.

9.11. állítás. *Ha $\mathcal{C}$ képes f-hosszú csomós hibát javítani, akkor $\hat{\mathcal{C}}$ ki tud javítani bármely $(f-1)m+1$ csomós hibát.*

9.12. feladat. Az űrtávközlésben, tömegtárolásban használt egyik népszerű Reed–Solomon kód egy $\mathbb{F}_{2^8}$ fölötti $\mathrm{GRS}_{255,223}(a, 1)$-kód, ahol a koordinátái a test összes nem nulla elemét kiadják, 1 pedig itt a csupa egyesből álló vektor. Hány hibát és hány csomós hibát tud javítani?

Megoldás. A kiterjesztett bináris kód tehát $8 \cdot 255 = 2040$-hosszú, $8 \cdot 223 = 1784$-dimenziós kód. E Reed–Solomon-kód 16-hibajavító, mivel MDS-kód, és így kódtávolsága $d = 255 - 223 + 1 = 33$. Eszerint a kiterjesztett kód 16 hibát, ill. $(16-1)8 + 1 = 121$ csomós hibát tud javítani. □

9.2. Kódok szorzata

9.13. definíció. Legyen $\mathcal{C}_1$ egy $[n_1, k_1, d_1]$-kód $\mathcal{C}_2$ egy $[n_2, k_2, d_2]$-kód egy $\mathbb{F}$ test fölött. A két kód szorzatán azt a $\mathcal{C}_1 \times \mathcal{C}_2$-vel jelölt kódot értjük, melynek kódszavai olyan $n_1 \times n_2$ méretű mátrixok, ahol az oszlopvektorok $\mathcal{C}_1$, a sorvektorok a $\mathcal{C}_2$ kódhoz tartoznak.

Ilyen kód könnyen készíthető. Legyen mindkét kód szisztematikus. Az üzenetszegmens legyen a kódmátrix bal felső $k_1 \times k_2$-es részmátrixa. Az oszlopokat kiegészítjük a $\mathcal{C}_1$, a sorokat a $\mathcal{C}_2$ ellenőrző szegmenseivel, majd a mátrix jobb alsó blokkját valamelyik előbb kiszámolt ellenőrző szegmens ellenőrző szegmensével. Ha a generátormátrixok $[I|A_1]$, illetve $[I|A_2]$, akkor az M üzenethez tartozó kódmátrix:

$$\left[\begin{array}{c|c} M & MA_2 \\ \hline A_1^TM & A_1^TMA_2 \end{array}\right]$$

Ebből nyilvánvaló, hogy a jobb alsó sarok kiszámítása bármelyik mellékátlóbeli blokkból számolható.

10. Golay-kódok

Az előzőekben tanult kódkiterjesztő eljárás egyik gyönyörű alkalmazásával jutunk el a Golay-kódokhoz.

Tekintsük az $\mathbb{F}_3$ és $\mathbb{F}_9$ testeket, utóbbi elemeit az x^2+1 polinom szerinti $\mathbb{F}_3$ fölötti polinomok maradékaival reprezentálva. Jelölje i e polinom egyik gyökét. A természetes megfeleltetés legyen $a = a_0+a_1i \mapsto \hat{a} = (a_0, a_1)$. A konjugálás itt a komplexekhez hasonlóan épp az $a_0+a_1i \mapsto a_0-a_1i$ leképezés.

Legyen A egy unitér mátrix ($A\bar{A}^T = I$), és $a \in \mathbb{F}_9$ olyan elem, melyre $a\bar{a} = -1$. Például legyen

$$A = \begin{bmatrix} 1+i & i & i \\ i & 1+i & i \\ i & i & 1+i \end{bmatrix}$$

és $a = 1 - i$. Képezzük azt az $\mathbb{F}_9$ fölötti kódot, melynek generátormátrixa

$$G = [I|aA] = \begin{bmatrix} 1 & 0 & 0 & -1 & 1+i & 1+i \\ 0 & 1 & 0 & 1+i & -1 & 1+i \\ 0 & 0 & 1 & 1+i & 1+i & -1 \end{bmatrix}.$$

Könnyen ellenőrizhető, hogy e kód ellenőrző mátrixa $H = \bar{G}$, ugyanis $G\bar{G}^T = I + a\bar{a}A\bar{A} = I - I = O$. Tehát $\mathcal{C}^\perp = \bar{\mathcal{C}}$. Egy másik ellenőrző mátrix $[-aA^T|I]$, ahonnan egy másik generátormátrix $[-\bar{a}\bar{A}^T|I]$. Könnyen látható, hogy e $\mathcal{C}$ kód minimális távolsága 4: ha volna 3- vagy annál kisebb súlyú kódszó, akkor annak egyik fele legföljebb 1-súlyú lenne, akkor az pedig csak a fenti két generátormátrix valamelyike egy sorának konstansszorosa lehet, aminek 4 a súlya. Így ez egy $[6, 3, 4]_9$-kód, tehát e kód MDS-kód.

10.1. definíció. E $\mathcal{C}$ kód $\hat{\mathcal{C}}$ kiterjesztését **kiegészített ternér Golay-kódnak** nevezzük. Egy tetszőleges koordinátahelyének kipontozásával kapott kód a **ternér Golay-kód**.

10.2. tétel. *A kiegészített ternér Golay-kód önduális $[12, 6, 6]_3$-kód, a ternér Golay-kód perfekt $[11, 6, 5]_3$-kód, azaz 2-hibajavító.*

Bizonyítás. Legyen $c, d \in \mathbb{F}_9^6$ két $\mathcal{C}$-beli kódvektor, koordinátáik $c_j = c_j' + ic_j''$, $d_j = d_j' + id_j''$, tehát

$$\begin{aligned} c \cdot \bar{d} &= (c_1' + ic_1'', \ldots, c_6' + ic_6'') \cdot (d_1' - id_1'', \ldots, d_6' - id_6'') \\ &= (c_1', c_1'', \ldots, c_6', c_6'') \cdot (d_1', d_1'', \ldots, d_6', d_6'') + zi \\ &= \hat{c} \cdot \hat{d} + zi, \end{aligned}$$

ahol $c'_j, c''_j, d'_j, d''_j, z \in \mathbb{F}_3$. Így ha $c \cdot \bar{d} = 0$, akkor $\hat{c} \cdot \hat{d} = 0$. Ha $d \in \mathcal{C}$, akkor $\bar{d} \in \bar{\mathcal{C}} = \mathcal{C}^{\perp}$, tehát c és $\bar{d}$ merőlegesek. Ebből következik, hogy a kiegészített Golay-kód önduális $[12, 6]$-kód. Mivel a 3.19 feladat szerint önduális ternér kód minden kódszava 3-mal osztható. A korábbiak szerint $\mathcal{C}$ minimális súlya 4, így $\hat{\mathcal{C}}$ minimális súlya legalább 4, másrészt a Singleton-korlát szerint a minimális súly legföljebb $12 - 6 + 1 = 7$, ezért $\hat{\mathcal{C}}$ minimális súlya csak 6 lehet, tehát a kiegészített Golay-kód önduális $[12, 6, 6]$-kód.

E kódot kipontozva egy perfekt $[11, 6, 5]$-kódot kapunk, mert a kód konstrukciójában megadott két generátormátrixból látható, hogy a kiterjesztett kód bármely koordinátahelyét kipontozva lesz legalább egy 5-súlyú kódszó. Ez azt jelenti, hogy e kód 2-hibajavító. A Hamming-korlát e kódra éles, hisz 3^6 darab 2-sugarú gömb épp kiadja a tér 3^{11} pontját:

$$3^6 \left(\sum_{j=0}^{2} \binom{11}{j} 2^j \right) = 3^6(1 + 22 + 220) = 3^{11}.$$

Ez bizonyítja a kód perfektségét! □

A. Függelék: Véges testek

Véges test Ha egy $\mathbb{F}$ testnek véges sok eleme van, **véges testnek** nevezzük. Ekkor létezik egy legkisebb pozitív p egész, hogy p darab 1-es összege 0, ezt a p számot nevezzük a test **karakterisztikájának**. Véges test karakterisztikája prímszám. A test p különböző eleme előáll az 1 ismételt összeadásával: $0, 1, 2 = 1 + 1, \ldots, p - 1 = 1 + \cdots + 1$. Ezek az elemek az $\mathbb{F}$ test egy résztestét alkotják, mely izomorf a modulo p maradékosztálytesttel, és amelyet a test prímtestének nevezünk, és $\mathbb{F}_p$-vel jelölünk. $\mathbb{F}$ egyúttal egy $\mathbb{F}_p$ fölötti végesdimenziós vektortér is, így elemeinek száma $q = p^r$ valamilyen pozitív egész r-re. q elemű test izomorfia erejéig csak egy van, ezt $\mathbb{F}_q$ jelöli.

Véges test additív és multiplikatív csoportja $\mathbb{F}_q$ additív csoportja az előbbiek szerint p-csoport (minden elem additív rendje p), a test multiplikatív $\mathbb{F}_q^*$ csoportja $q-1$-edrendű ciklikus. Az $\mathbb{F}_q^*$ csoport generátorelemeit, azaz $q-1$-edrendű elemeit a test **primitív elemeinek** nevezzük. Ha g egy primitív elem, akkor

$$\mathbb{F}_q = \{0, 1 = g^0, g, g^2, \ldots, g^{q-2}\}.$$

Egy $e \in \mathbb{F}_q$ elemet n-edik egységgyöknek nevezünk, ha $e^n = 1$ és **primitív n-edik egységgyöknek**, ha $e^m \neq 1$ semmilyen $m < n$ esetén. $\mathbb{F}_q$-ban pontosan akkor van primitív n-edik egységgyök, ha $n \mid q - 1$. Egyik ilyen egységgyök $g^{(q-1)/n}$, ahol g primitív elem.

Egy $\alpha \in \mathbb{F}_q$ elem rendje az a legkisebb pozitív n egész, melyre $\alpha^n = 1$. Jele $\operatorname{ord}(\alpha)$.

Az $\mathbb{F}_q$ test bármely α elemére $\operatorname{ord}(\alpha) \mid q - 1$, és ha valamely $m > 0$ egészre $\alpha^m = 1$, akkor $\operatorname{ord}(\alpha) \mid m$. Például ha g jelöli $\mathbb{F}_{16}$ egy primitív elemét, akkor $\alpha = g^6$ rendje 5, mert $\alpha^2 = g^{12}$, $\alpha^3 = g^{6\cdot 3} = g^3$, $\alpha^4 = g^{24} = g^9$, és végül $\alpha^5 = g^{30} = 1$. E testben másodrendű elem nincs, mert $2 \nmid 15$.

Ha $m \mid q - 1$, akkor az m-edrendű elemek száma $\mathbb{F}_q$-ban $\varphi(m)$, speciálisan a primitív elemek száma $\varphi(q - 1)$.

Az $\mathbb{F}_q[x]$ polinomgyűrű Az $\mathbb{F}_q[x]$ polinomgyűrű euklideszi gyűrű, mert létezik rajta egy euklideszi norma, azaz egy olyan φ függvény, hogy bármely két $a(x), b(x) \in \mathbb{F}_q[x]$ polinomhoz van olyan $q(x)$ és $r(x)$ polinom, hogy $a(x) = b(x)q(x) + r(x)$, ahol $\varphi(r(x)) < \varphi(b(x))$. Itt φ a polinom foka. Az $f(x) \in \mathbb{F}_q[x]$ polinomot **irreducibilisnek** nevezzük, ha nincs nemtriviális $\mathbb{F}_q[x]$-beli tényezőkre bontása, azaz nem konstans, és nem bomlik fel alacsonyabb fokú polinomok szorzatára. Minden euklideszi gyűrű, főideálgyűrű, ezért $\mathbb{F}_q[x]$ is, tehát minden ideált egyetlen polinom generál. Az $f(x)$ polinom által generált ideált $(f(x))$ jelöli. Főideálgyűrűkben igaz a számelmélet alaptétele, tehát $\mathbb{F}_q[x]$ minden polinomja skalárszorzótól és sorrendtől eltekintve egyértelműen előáll irreducibilis polinomok szorzataként. Polinom irreducibilitásának eldöntésére vannak hatékony algoritmusok. Az elsőfokú polinom mindig irreducibilis, a másod- és harmadfokú pontosan akkor irreducibilis, ha nincs gyöke.

Euklideszi algoritmus Az $\mathbb{F}_q[x]$ gyűrűben bármely két $a(x)$, $b(x)$ polinomnak egyértelműen létezik az $(a(x), b(x))$ kitüntetett közös osztója, mely az a főpolinom, amely közös osztó, és minden közös osztónak többszöröse. A legnagyobb közös osztó elnevezés is használatos, mivel nincs ennél nagyobb fokú közös osztó. A kitüntetett közös osztó meghatározására az euklideszi algoritmus használható, mellyel azok az $s(x)$, $t(x)$ polinomok is meghatározhatók, melyre

$$a(x)s(x) + b(x)t(x) = (a(x), b(x)).$$

Véges test konstrukciója $\mathbb{F}_p$ a modulo p maradékosztálytest. Legyen

$$a(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0 \in \mathbb{F}_p[x].$$

Az $\mathbb{F}_p[x]/(a(x))$ faktorgyűrű (maradékosztály-gyűrű) pontosan akkor test, ha $a(x)$ irreducibilis polinom, és ekkor megegyezik az $\mathbb{F}_q$ testtel, ahol $q = p^r$. Jelölje α az $x + (a(x))$ maradékosztályt. Erre $a(\alpha) = 0$ az $\mathbb{F}_p[x]/(a(x))$ maradékosztálytestben. Így a test elemeit az r-nél kisebb fokú $b_{r-1}\alpha^{r-1} + \cdots + b_1\alpha + b_0$ alakú polinomok reprezentálják. Az összeadás köztük a szokásos, a szorzás a polinomszorzat modulo $a(\alpha)$, amit a gyakorlatban az $\alpha^r = -a_{r-1}\alpha^{r-1} - \cdots - a_1\alpha - a_0$ helyettesítéssel érhetünk el. Az elemek egy másik reprezentációjában $\mathbb{F}_q$-t $\mathbb{F}_p$ fölötti r-dimenziós vektortérként kezeljük, melynek bázisa $\{\alpha^{r-1}, \ldots, \alpha, 1\}$, és amelyben a $b_{r-1}\alpha^{r-1} + \cdots + b_1\alpha + b_0$ polinomot a $b_{r-1} \ldots b_1 b_0$ vektorral reprezentáljuk. Test konstrukciójához gyakran választunk

primitív polinomot, amelynél a fenti α elem rendje $q-1$, tehát α hatványai kiadják a test nemnulla elemeit. Például $x^3+x+1 \in \mathbb{F}_2[x]$ primitív polinom, a vele megkonstruált $\mathbb{F}_8$ elemei három reprezentációban:

0	0	000
α^0	1	001
α	α	010
α^2	α^2	100
α^3	$\alpha+1$	011
α^4	$\alpha^2+\alpha$	110
α^5	$\alpha^2+\alpha+1$	111
α^6	α^2+1	101

A fenti konstrukció tetszőleges $\mathbb{F}_q$ testből kiindulva is elvégezhető, például $\mathbb{F}_{16}$ megkapható az $\mathbb{F}_2[x]/(x^4+x+1)$ vagy az $\mathbb{F}_4[x]/(x^2+x+\beta)$ faktorstruktúrából is, ahol $\mathbb{F}_4$ pedig az $\mathbb{F}_2[x]/(x^2+x+1)$ test.

	$\mathbb{F}_2[x]/(x^4+x+1)$			$\mathbb{F}_4[x]/(x^2+x+\beta)$	
α^i	$\mathbb{F}_2(\alpha)$	$\mathbb{F}_2^4$	$\mathbb{F}_2(\beta)$	$\mathbb{F}_4(\alpha)$	$\mathbb{F}_4^2$
0	0	0000	0	0	00
α^0	1	0001	1	1	01
α	α	0010		α	10
α^2	α^2	0100		$\alpha+\beta$	1β
α^3	α^3	1000		$\bar{\beta}\alpha+\beta$	$\bar{\beta}\beta$
α^4	$\alpha+1$	0011		$\alpha+1$	11
α^5	$\alpha^2+\alpha$	0110	β	β	0β
α^6	$\alpha^3+\alpha^2$	1100		$\beta\alpha$	$\beta 0$
α^7	$\alpha^3+\alpha+1$	1011		$\beta\alpha+\bar{\beta}$	$\beta\bar{\beta}$
α^8	α^2+1	0101		$\alpha+\bar{\beta}$	$1\bar{\beta}$
α^9	$\alpha^3+\alpha$	1010		$\beta\alpha+\beta$	$\beta\beta$
α^{10}	$\alpha^2+\alpha+1$	0111	$\beta+1$	$\bar{\beta}$	$0\bar{\beta}$
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110		$\bar{\beta}\alpha$	$\bar{\beta}0$
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111		$\bar{\beta}\alpha+1$	$\bar{\beta}1$
α^{13}	$\alpha^3+\alpha^2+1$	1101		$\beta\alpha+1$	$\beta 1$
α^{14}	α^3+1	1001		$\bar{\beta}\alpha+\bar{\beta}$	$\bar{\beta}\bar{\beta}$

2. táblázat. $\mathbb{F}_{16}$ elemeinek különböző reprezentációi, ahol α a test egy primitív elemét jelöli.

Résztestek Ha K és L két test, $K \le L$ és $\alpha_1,\dots,\alpha_k \in L$, akkor $K(\alpha_1,\dots,\alpha_k)$ azt a legszűkebb testet jelöli, mely K-t és az $\alpha_1,\dots,\ \alpha_k$ elemeket is tartalmazza. Ha pedig egy $f(x) \in K[x]$ polinom összes gyöke L-beli, azaz $f(x) = c(x-\alpha_1)\dots(x-\alpha_k)$, ahol $\alpha_i \in L$, akkor $K(\alpha_1,\dots,\alpha_k)$ az $f(x)$ polinom **felbontási teste**.

Mivel a test bármely nemnulla a elemére $a^{q-1}=1$, ezért $\mathbb{F}_q$ elemei mind gyökei az $x^q - x \in \mathbb{F}_p[x]$ polinomnak. Az $\mathbb{F}_q$ $(q=p^r)$ test az $x^q-x \in \mathbb{F}_p[x]$ polinom felbontási teste. Ha m pozitív egész, akkor $\mathbb{F}_{p^r}$-nek pontosan akkor létezik p^m-elemű részteste, ha $m \mid r$. Ez a K résztest egyértelmű, és $\mathbb{F}_q$ azon elemeiből áll, melyek gyökei az $x^{p^m}-x$ polinomnak, azaz $K = \{\beta \mid \beta^{p^m} - \beta = 0\}$. Ha $\mathbb{F}_{p^r}$-nek α egy primitív eleme, akkor a K test multiplikatív csoportjának α^t egy generátora lesz, ahol $t = (p^r-1)/(p^m-1)$. Így $K = \{0, 1, \alpha^t, \alpha^{2t}, \dots, \alpha^{(p^m-2)t}\}$.

Testautomorfizmusok p-karakterisztikájú test bármely két β, γ elemére $(\beta+\gamma)^p = \beta^p + \gamma^p$, ami a binomiális tétellel könnyen igazolható. Mivel $(\beta\gamma)^p = \beta^p\gamma^p$ is fennáll, ezért az $\phi_p : x \mapsto x^p$ leképezés a test egy automorfizmusa. Ezt nevezzük **Frobenius** (vagy **Galois**) **automorfizmusnak**. Az $\mathbb{F}_{p^r}$ test $\mathrm{Gal}(\mathbb{F}_{p^r})$ teljes automorfizmuscsoportja r-elemű ciklikus csoport, melyet ϕ_p generál. Ebből adódik, hogy bármely p-karakterisztikájú testben bármely $m \ge 0$ egészre $(\beta+\gamma)^{p^m} = \beta^{p^m} + \gamma^{p^m}$.

Ha $m \mid r$, és $K \le \mathbb{F}_{p^r}$ egy p^m-elemű résztest, akkor K a ϕ_p^m leképezés fix elemeiből áll. A K-t fixen hagyó automorfizmusok egy r/m-edrendű ciklikus csoportot alkotnak, melyet ϕ_p^m generál. E csoportot $\mathrm{Gal}(\mathbb{F}_{p^r} : K)$ jelöli.

Konjugált elemek Mivel

$$f(x)^q = \left(\sum_{i=0}^{k} f_i x^i\right)^q = \sum_{i=0}^{k} f_i^q x^{iq},$$

ezért ha $f(x) \in \mathbb{F}_q[x]$, akkor $f^q(x) = f(x^q)$. Eszerint ha γ az $f(x)$ egy gyöke $\mathbb{F}_q$ egy testbővítésében, akkor γ^q, γ^{q^2}, γ^{q^3},..., is, azaz minden $n \ge 0$ esetén γ^{q^n} is. Ez vezet a következő definícióhoz: ha $\gamma \in \mathbb{F}_{q^k}$, akkor a γ, γ^q, γ^{q^2}, γ^{q^3},... elemeket a γ elem $\mathbb{F}_q$ szerinti **konjugáltjainak** nevezzük (ezek közt nyilván csak véges sok különböző van). A γ elemmel konjugált elemek halmazát a γ elemhez tartozó, vagy az általa generált $\mathbb{F}_q$ szerinti **konjugálttosztálynak** nevezzük. Például az $\mathbb{F}_{16}$ test $\mathbb{F}_2$ szerinti konjugáltosztályai (α az $\mathbb{F}_{16}$ test 2. táblázat szerinti primitív elemét jelöli): $\{0\}$, $\{1\}$, $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$, $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$, $\{\alpha^5, \alpha^{10}\}$, $\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$. Az $\mathbb{F}_4$ szerinti mellékosztályok pedig $\{0\}$, $\{1\}$, $\{\alpha^5\}$, $\{\alpha^{10}\}$, $\{\alpha, \alpha^4\}$, $\{\alpha^2, \alpha^8\}$, $\{\alpha^3, \alpha^{12}\}$, $\{\alpha^6, \alpha^9\}$, $\{\alpha^7, \alpha^{13}\}$, $\{\alpha^{11}, \alpha^{14}\}$.

Azt a legkisebb pozitív d egész számot, melyre $n \mid q^d - 1$, a q **multiplikatív rendjének** nevezzük modulo n. Például a „2 multiplikatív rendje modulo 5” értéke az $5 \nmid 2-1$, $5 \nmid 2^2-1$, $5 \nmid 2^3-1$, $5 \mid 2^4-1$ oszthatóságok miatt 4-nek adódik, míg a „4 multiplikatív rendje modulo 5” az $5 \nmid 4-1$, $5 \mid 4^2-1$ oszthatóságok miatt 2.

Ha $\gamma \in \mathbb{F}_{q^k}$ és γ rendje n, valamint d a q multiplikatív rendje modulo n, akkor $\gamma^{q^d} = \gamma$, és a γ, γ^q, γ^{q^2},... $\gamma^{q^{d-1}}$ számok mind különbözőek. A γ elemet tartalmazó konjugáltosztály mérete tehát q multiplikatív rendje modulo $\mathrm{ord}(\gamma)$. Például $\mathbb{F}_{16}$-ban az α^3 elem rendje 5, így az őt tartalmazó $\mathbb{F}_2$ szerinti konjugáltosztály mérete 4, míg az $\mathbb{F}_4$ szerinti mérete 2.

Minimálpolinom A $\gamma \in \mathbb{F}_{q^k}$ elem $\mathbb{F}_q$ szerinti **minimálpolinomja** az a legkisebb fokú nemnulla $m(x) \in \mathbb{F}_q[x]$ főpolinom, melynek γ gyöke, azaz melyre $m(\gamma) = 0$. Ilyen polinom mindig létezik, hisz a γ-ban eltűnő nemnulla polinomok halmaza nem üres (pl. $x^{q^k} - x$ benne van). A γ-ban eltűnő polinomok ideált alkotnak $\mathbb{F}_q[x]$-ben, amely főideál, így egyetlen polinom generálja, a minimálpolinom, mely így egyértelmű. A minimálpolinom legfontosabb tulajdonságai:

(1) egyértelmű,

(2) minden γ-ban eltűnő polinomnak osztója,

(3) irreducibilis,

(4) osztója az $x^{q^k} - x$ polinomnak,

(5) foka osztója k-nak,

(6) $m(x) = \prod_{i=0}^{d-1}(x - \gamma^{q^i})$, vagyis $m(x)$ gyökei pontosan γ konjugáltjai, ahol d a q multiplikatív rendje modulo $\mathrm{ord}(\gamma)$.

Tehát minden minimálpolinomnak egy konjugáltosztály elemei a gyökei. A 3. táblázat két kis testre megadja a konjugáltosztályokat és a minimálpolinomokat.

test	konjugáltosztály	minimálpolinom $(m(x))$
$\mathbb{F}_8$	$\{0\}$	x
	$\{1\}$	$x+1$
	$\{\alpha, \alpha^2, \alpha^4\}$	x^3+x+1
	$\{\alpha^3, \alpha^6, \alpha^5\}$	x^3+x^2+1
$\mathbb{F}_{16}$	$\{0\}$	x
	$\{1\}$	$x+1$
	$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$	x^4+x+1
	$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$	$x^4+x^3+x^2+x+1$
	$\{\alpha^5, \alpha^{10}\}$	x^2+x+1
	$\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$	x^4+x^3+1

3. táblázat. $\mathbb{F}_8$ és $\mathbb{F}_{16}$ minimálpolinomjai a $\prod_{i=0}^{d-1}(x - \alpha^{q^i})$ képlettel a konjugáltosztályokból kiszámolva.

Az $x^{q^k-1} - 1$ polinom gyökei az $\mathbb{F}^*_{q^k}$ elemei, így e polinom felbomlik a minimálpolinomok szorzatára. Például $\mathbb{F}^*_{16}$-ra

$$x^{15} - 1 = (x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)\times (x^2+x+1)(x^4+x^3+1)$$