

# Hibajavító kódolás

(előadásvázlat, 2008. május 14.)

Maróti Miklós

Ennek az előadásnak a megértéséhez a következő fogalmakat kell tudni: **test**, **monoid**, **vektortér**, **dimenzió**, **mátrixok**.

Az előadáshoz ajánlott jegyzet:

- Kiss Emil: Bevezetés az algebra, Typotex Kiadó, Budapest, 2007.
- Czédli Gábor: *Boole-függvények*, Polygon Kiadó, Szeged, 1995.

**1. Definíció.** Az információ tároló vagy továbbító rendszerek a következő öt részre bonthatók:

- (1) **információ forrás**, pl. szöveges (TXT) vagy zenei (WAV) adat
- (2) **kódoló**, pl. tömörítő vagy CD író program
- (3) **kommunikációs csatorna**, pl. internet vagy kompakt diszk
- (4) **dekódoló**, pl. kitömörítő vagy CD lejátszó program
- (5) **információ felhasználás**, pl. szöveges (TXT) vagy zenei (WAV) adat

A továbbítandó információ általában diszkrét egységekre bontható (szöveges adat esetén karakterek sorozatára, mono zenei adat esetén 16-bites előjeles számok sorozatára), melyeket **üzeneteknek** nevezük. A **kódolás** egy  $\varphi : M \rightarrow C$  bijektív leképezés, ahol  $M$  az üzenetek, illetve  $C$  a **kódszavak** halmaza. Magát a  $C$  halmazt nevezük **kódnak**. Mi csak olyan kódolásokkal fogunk foglalkozni, ahol mind  $M$ , mind  $C$  a  $K = \{0, 1, \dots, k-1\}$  **szimbólumok** ( $k = 2$  esetben **bitek**) feletti szavakból áll, azaz  $M, C \subseteq K^*$ , ahol

$$K^* = \{a_0 a_1 \cdots a_{n-1} : n \geq 0, a_0, \dots, a_{n-1} \in K\}.$$

A **dekódolás** egy  $\psi : K^* \rightarrow M$  parciális leképezés. Többfajta kódolás létezik (titkosítás, tömörítés, stb.), de mi csak olyanokat vizsgálunk, melynek célja a hibajelzés és hibajavítás.

**2. Definíció.** A  $C \subseteq K^*$  kód **blokk-kód**, ha minden kódszava ugyanolyan hosszú. A kódszavak közös  $n \in \mathbb{N}$  hosszát a  $C$  kód **hosszának** nevezük. Ekkor természetesen  $C \subseteq K^n$ .

**3. Definíció.** A  $C \subseteq K^n$  blokk-kód elemeit ideális esetben  $\log_{|K|} |C|$  hosszúságú szavakkal is meg tudnánk különböztetni, de mi  $n$ -hosszú szavakat használunk. Tehát a  $C$  blokk-kód **információs rátája** (gazdaságossági együtthatója)

$$\frac{\log_{|K|} |C|}{n}.$$

**4. Példa.** A  $C = \{000, 111\} \subseteq \mathbb{Z}_2^3$  kód információs rátája  $\frac{\log_2 2}{3} = \frac{1}{3}$ , ami durván azt jelenti, hogy egy bitnyi kódolt adat csak  $\frac{1}{3}$  bitnyi információt hordoz.

**5. Definíció.** A kommunikációs csatornát **szimmetrikusnak** nevezük, ha

- (1) a kódszavak hosszát nem változtatja meg, azaz a csatornán bemenő és kijövő szimbólumok száma ugyanaz,
- (2) minden szimbólumot egymástól független módon, sorrendben, azonos  $p > \frac{1}{2}$  valószínűséggel helyesen továbbít, vagy  $1 - p$  valószínűséggel elront, és
- (3) az elrontott szimbólumok azonos eséllyel kerülnek ki a helytelen szimbólumok közül.

**6. Példa.** A  $K = \{0, 1, 2\}$  és  $p = 80\%$  paraméterek esetén a szimmetrikus kommunikációs csatorna az 1 szimbólumot 10% valószínűséggel továbbítja 0-ként, 80% valószínűséggel 1-ként, és szintén 10% valószínűséggel továbbítja 2-ként. Ezt a bejövő szimbólumok mind-egyikére hasonlóan, egymástól függetlenül végzi el.

**7. Definíció.** Az  $u = u_1 \dots u_n$  és  $v = v_1 \dots v_n \in K^n$  szavak **Hamming-távolsága** azoknak az  $1 \leq i \leq n$  koordinátáknak a száma, ahol  $u$  és  $v$  eltér:

$$d(u, v) = |\{1 \leq i \leq n : u_i \neq v_i\}|.$$

**8. Tétel.** Legyen  $C \subseteq K^n$  blokk-kód és  $v \in C$  szimmetrikus kommunikációs csatornából kijövő szó. Ekkor a legnagyobb valószínűséggel azt az  $u \in C$  kódszót alakította át a csatorna, amelynek Hamming-távolsága minimális  $v$ -től. Ha több ilyen van, akkor azok mindegyike egyenlő valószínűséggel lehetett a bemenő kódszó.

**9. Példa.** Ha a  $C = \{000, 111\}$  kód esetén a szimmetrikus kommunikációs csatornából kijövő szó  $v = 010$ , akkor annak a legnagyobb a valószínűsége, hogy az  $u = 000$  kódszó ment be a csatornába.

**10. Definíció.** Legyen  $C \subseteq K^n$  blokk-kód. Ha ismert a  $\varphi : M \rightarrow C$  kódolás, akkor a  $\psi : K^n \rightarrow M$  dekódoláshoz elég megadni azt a  $\tau : K^n \rightarrow C$  parciális leképezést, amelyre  $\tau = \psi\varphi$ . Ha minden  $v \in K^n$  beérkező szóra

$$v\tau = \begin{cases} u, & \text{ha } u \in C \text{ a } v \text{ szóhoz legközelebbi kódszó, és} \\ - & \text{(nem definiált), ha több kódszó van legközelebb } v\text{-hez,} \end{cases}$$

akkor a kapott dekódolást a **standard hibajavító dekódolásnak** nevezzük.

**11. Példa.** Legyen  $C = \{101, 111, 011\}$  és  $v = 100$  a kommunikációs csatornából kijövő szó. Ekkor  $d(101, 100) = 1$ ,  $d(111, 100) = 2$ ,  $d(011, 100) = 3$ , tehát a standard hibajavító dekódolás a  $v$  szót az 101 kódszóra javítja. Ha  $v = 001$ , akkor  $d(101, 001) = 1$  és  $d(011, 001) = 1$ , tehát a standard hibajavító dekódolás a  $v$  szót hibásnak jelzi.

**12. Definíció.** Legyen  $t \geq 0$  és  $C \subseteq K^n$ . A  $C$  kód  **$t$ -hibajelző**, ha bármely kódszót legfeljebb  $t$  helyen megváltoztatva az eredmény nem lehet az eredetitől különböző kódszó. A  $C$  kód  **$t$ -hibajavító**, ha bárhogy is veszünk két  $u \neq v$  kódszót, és azokat legfeljebb  $t$  helyen (külön-külön) megváltoztatjuk, akkor a kapott  $u', v' \in K^n$  szavak különbözők.

**13. Példa.** A  $C = \{000, 111\}$  kód 2-hibajelző, de nem 3-hibajelző, és 1-hibajavító, de nem 2-hibajavító.

**14. Definíció.** A  $C \subseteq K^n$  blokk-kód **minimális távolságán** a

$$d(C) = \min\{d(u, v) : u, v \in C, u \neq v\}$$

számot értjük.

**15. Példa.** A  $C = \{000, 111\}$  kód minimális távolsága 3. A  $C = \{000, 011, 101, 110\}$  kód minimális távolsága 2.

**16. Definíció.** Tetszőleges  $C$  blokk-kód  $d(C) - 1$ -hibajelző, és  $\lfloor \frac{d(C)-1}{2} \rfloor$ -hibajavító. Ezek a számok a lehető legnagyobbak, azaz  $C$  nem  $d(C)$ -hibajelző, és nem  $\lfloor \frac{d(C)+1}{2} \rfloor$ -hibajavító.

**17. Példa.** A  $C = \{000, 111\}$  kód  $3 - 1 = 2$ -hibajelző és  $2/2 = 1$ -hibajavító. A  $C = \{000, 011, 101, 110\}$  kód  $2 - 1 = 1$ -hibajelző és  $\lfloor 1/2 \rfloor = 0$ -hibajavító.

**18. Tétel (Hamming-korlát).** Ha a  $C \subseteq K^n$  kód  $t$ -hibajavító, akkor

$$|K|^n \geq |C| \cdot \sum_{i=0}^t \binom{n}{i} (|K| - 1)^i.$$

**19. Példa.** Kiszámoljuk, hogy maximum hány kódszót tartalmazhat egy 7-hosszú 1-hibajavító bináris kód. Tehát  $|K| = 2$ ,  $n = 7$ ,  $t = 1$ , és

$$\sum_{i=0}^t \binom{n}{i} (|K| - 1)^i = \binom{7}{0} + \binom{7}{1} = 8.$$

Ez azt jelenti, hogy minden kódszó körüli 1-sugarú gömb pontosan 8 szót tartalmaz, és ezek páronként diszjunktak. Azt kaptuk, hogy  $2^7 = 128 \geq |C| \cdot 8$ , azaz  $|C| \leq 16$ . Ebből azt is megállapíthatjuk, hogy  $C$  információs rátája legfeljebb  $4/7$  lehet.

**20. Definíció.** A  $t$ -hibajavító  $C \subseteq K^n$  kód **tökéletes**, ha minden  $v \in K^n$  szóhoz van tőle legfeljebb  $t$  Hamming-távolságra levő kódszó (azaz a kód eléri a Hamming-korlátját).

**21. Példa.** A  $C = \{000, 111\}$  kód tökéletes 1-hibajavító kód, mert  $2^3 = 2 \cdot (1 + 3)$ .

**22. Definíció.** Ha  $K$  test és  $C \subseteq K^n$  altere a  $K$  feletti  $K^n$  vektortérnek, akkor  $C$ -t **lineáris kódnak** nevezzük.

**23. Tétel.** Legyen  $C \leq K^n$  lineáris kód. Ekkor

- (1)  $|C| = |K|^r$  valamely  $r$  egészre, tehát lineáris kódok esetében feltehető, hogy  $M = K^r$ ;
- (2) létezik olyan  $\varphi : K^r \rightarrow C$  kódolás, amely lineáris leképezés,
- (3)  $C$  információs rátája  $\frac{r}{n}$ .

**24. Definíció.** Legyen  $C \leq K^n$   $r$ -dimenziós lineáris kód. A  $G \in K^{r \times n}$  mátrixot a  $C$  kód **generátormátrixának** nevezzük, ha  $G$  sorainak rendszere a  $C$  vektortér bázisát alkotja. Ekkor az  $u \in K^r$  üzenet  **$G$ -szerinti kódolása** az  $uG \in C$  kódszó.

**25. Példa.** A  $C = \{000, 111\}$  kód generátormátrixa  $G = (1 \ 1 \ 1) \in \mathbb{Z}_2^{1 \times 3}$ .

**26. Definíció.** A  $C$  lineáris kód **szisztematikus**, ha van olyan generátormátrixa, amelyben az első  $r$  oszlop az egységmátrixot alkotja, azaz  $G = [E \ H]$  valamely  $H \in K^{r \times (n-r)}$  mátrixra.

**27. Példa.** A  $C = \{0000, 1010, 0111, 1101\}$  kód szisztematikus, mivel  $C$  egy generátormátrixa  $G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{Z}_2^{2 \times 4}$ . Ekkor  $H = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ .

**28. Definíció.** A  $C, D \leq K^n$  lineáris kódok **ekvivalensek**, ha létezik olyan  $\pi \in S_n$  permutáció, amelyre

$$a_1 a_2 \dots a_n \in C \iff a_{1\pi} a_{2\pi} \dots a_{n\pi} \in D.$$

**29. Példa.** A  $C = \{0000, 1010, 0111, 1101\}$  és  $D = \{0000, 1100, 0111, 1011\}$  kódok ekvivalensek, mert minden kódszóban a második és harmadik szimbólumot felcserélve ( $\pi = (2 \ 3)$ ) egymásba vihetők.

**30. Tétel.** Minden lineáris kód ekvivalens egy szisztematikus lineáris kóddal.

**31. Tétel.** A  $C \leq K^n$  lineáris kód minimális távolsága éppen

$$\min\{d(u, 0) : u \in C \setminus \{0\}\}.$$

**32. Definíció.** Legyen  $C \leq K^n$   $r$ -dimenziós lineáris kód. A  $P \in K^{n \times (n-r)}$  mátrixot a  $C$  kód **ellenőrző mátrixának** nevezzük, ha  $u \in K^n$  akkor és csak akkor kódszó, ha  $uP = 0$ .

**33. Tétel.** Minden lineáris kódnak van ellenőrző mátrixa, ami egyértelműen meghatározza a kódot. A  $P \in K^{n \times (n-r)}$  mátrix akkor és csak akkor ellenőrző mátrixa a  $G \in K^{r \times n}$  generátormátrixú lineáris kódnak, ha oszlopvektorai lineárisan függetlenek és  $GP = 0$ . Ha a kód szisztematikus a  $G = [E \ H]$  generátormátrixal, akkor a kód egy ellenőrző mátrixa

$$P = \begin{bmatrix} -H \\ E \end{bmatrix}.$$

**34. Példa.** A  $C = \{0000, 1010, 0111, 1101\}$  szisztematikus kód generátormátrixa

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

Tehát a kód ellenőrző mátrixa

$$P = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

**35. Definíció.** Legyen  $K$  tetszőleges véges test,  $r \geq 2$ ,

$$n = \frac{|K|^r - 1}{|K| - 1},$$

és legyen  $P \in K^{n \times r}$  olyan mátrix, melynek sorai a  $K^r$  vektortér páronként lineárisan független nemzérő vektorait tartalmazzák (pl. azon nemzérő vektorok, melyeknek az első nemnulla komponense 1). Azt a  $C \leq K^n$  lineáris kódot, melynek  $P$  az ellenőrző mátrixa, **Hamming-kódnak** nevezzük, melynek dimenziója  $n - r$ .

**36. Példa.** Megadjuk a  $K = \mathbb{Z}_2$  test feletti (azaz bináris)  $\frac{2^2-1}{2-1} = 3$ -hosszú Hamming-kódot. A kód egy lehetséges ellenőrzőmátrixa

$$P = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

tehát  $H = (1 \ 1)$  és a kód generátormátrixa

$$G = (1 \ 1 \ 1),$$

azaz  $C = \{000, 111\}$ .

**37. Példa.** Megadjuk a  $K = \mathbb{Z}_3$  test feletti  $\frac{3^2-1}{3-1} = 4$ -hosszú Hamming-kódot. A  $K^2$  vektortér azon nemzérő vektorai, melynek az első nemnulla komponense 1, pontosan a  $(1, 0)$ ,  $(1, 1)$ ,  $(1, 2)$  és  $(0, 1)$  vektorok. Tehát a kód egy lehetséges ellenőrzőmátrixa

$$P = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

és a kód generátormátrixa

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

Ezért a kód 2-dimenziós, kilenc eleme van, mégpedig

$$C = \{0000, 1022, 2011, 0121, 1110, 2102, 0212, 1201, 2220\}.$$

A kód minimális távolsága 3 (elég megnézni a nemzérő vektorok zérótól való távolságát), tehát  $C$  2-hibajelző és 1-hibajavító, és információs rátája  $\frac{2}{4} = \frac{1}{2}$ .

**38. Példa.** Megadjuk a  $2^3 - 1 = 7$ -hosszú, bináris Hamming-kódot. A kód egy lehetséges ellenőrzőmátrixa

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

tehát a kód generátormátrixa

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

A kód 4-dimenziós, 16 eleme van, és információs rátája  $\frac{4}{7}$ .

**39. Tétel.** Tetszőleges  $K$  test fölött a Hamming-kód tökéletes, 1-hibajavító és 2-hibajelző.

**40. Definíció.** A  $C \subseteq K^n$  blokk-kódot **ciklikusnak** nevezzük, ha minden  $a_1 a_2 \dots a_n$  kódszóra az  $a_2 \dots a_n a_1$  szó szintén kódszó.

**41. Megjegyzés.** Legyen  $K$  tetszőleges test. Az  $a_1 a_2 \dots a_n \in K^n$  szavakat azonosítjuk az  $a_1 + a_2 x + \dots + a_n x^{n-1}$  polinommal.

**42. Tétel.** Legyen  $C \leq K^n$  nemtriviális (azaz  $C \neq \{0\}$ ) ciklikus lineáris kód és  $g \in C$  minimális fokszámú főpolinom kódszó. Ekkor

- (1)  $g$  egyértelműen meghatározott,
- (2) minden  $h \in K^n$  szóra  $h \in C \iff g \mid h$ ,
- (3)  $g$  valódi osztója az  $x^n - 1$  polinomnak,
- (4)  $C$  dimenziója pontosan  $n - \deg(g)$ .

**43. Definíció.** A  $C \leq K^n$  ciklikus lineáris kódban egyértelműen meghatározott minimális fokszámú főpolinomot a  $C$  kód **generátorpolinomjának** nevezzük.

**44. Tétel.** Ha  $g$  a  $C \leq K^n$  ciklikus lineáris kód generátorpolinomja, és  $r = n - \deg(g)$ , akkor a  $C$  kód egy generátormátrixa

$$G = \begin{pmatrix} g \\ xg \\ x^2g \\ \vdots \\ x^{r-1}g \end{pmatrix}.$$

**45. Példa.** Tekintsük a  $C = \{0000, 1010, 0101, 1111\}$  ciklikus lineáris kódot. Ekkor a generátorpolinom az 1010 szóhoz tartozó  $g = 1 + x^2 \in \mathbb{Z}_2[x]$  polinom, és  $C$  egy generátormátrixa

$$G = \begin{pmatrix} g \\ xg \end{pmatrix} = \begin{pmatrix} 1010 \\ 0101 \end{pmatrix}.$$

**46. Tétel.** Ha a  $g \in K[x]$  polinom valódi osztója az  $x^n - 1$  polinomnak, akkor a  $g$  által generált  $C = \{h \in K^n : g \mid h\}$  kód ciklikus, lineáris, és  $g$  a generátorpolinomja.

**47. Példa.** Meghatározzuk az összes 3-hosszú nemtriviális ciklikus lineáris bináris kódot. Az  $x^3 - 1 \in \mathbb{Z}_2[x]$  polinom irreducibilis felbontása  $x^3 - 1 = (x + 1)(x^2 + x + 1)$ . Tehát  $x^3 - 1$ -nek pontosan három valódi osztója van:  $g_1 = x + 1$ ,  $g_2 = x^2 + x + 1$  és  $g_3 = 1$ . Ezen generátorpolinomokhoz tartozó kódok rendje a  $C_1 = \{000, 110, 011, 101\}$ ,  $C_2 = \{000, 111\}$  és  $C = \mathbb{Z}_2^3$  ciklikus lineáris kódok.

**48. Tétel.** Legyen  $f \in K[x]$   $n$ -edfokú irreducibilis polinom,  $\beta$  a  $K[x]/\langle f \rangle$  test primitív eleme, és  $g \in K[x]$  a  $\beta$  elem minimálpolinomja. Ekkor  $g$  generátorpolinomja egy  $\frac{|K|^n - 1}{|K| - 1}$ -hosszú ciklikus Hamming-kódnak.

**49. Példa.** Legyen  $K = \mathbb{Z}_2$ ,  $f = 1 + x + x^3 \in \mathbb{Z}_2[x]$  és  $\beta = \overline{x + 1} \in \mathbb{Z}_2[x]/\langle f \rangle$ . Ekkor

$$\begin{aligned} \beta^2 &= \overline{(x + 1)^2} = \overline{x^2 + 1}, \\ \beta^3 &= \overline{(x + 1)(x^2 + 1)} = \overline{x^3 + x^2 + x + 1} = \overline{x^2}, \end{aligned}$$

azaz  $\beta^3 + \beta^2 + 1 = \overline{x^2 + (x^2 + 1) + 1} = 0$  és ezért  $\beta$  minimálpolinomja  $g = x^3 + x^2 + 1$ . Tehát a Hamming-kód hossza  $2^3 - 1 = 7$ , és generátormátrixa

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

**50. Definíció.** Legyen  $f \in K[x]$   $r$ -edfokú irreducibilis polinom,  $\alpha$  a  $K[x]/\langle f \rangle$  test legalább  $n$ -edrendű eleme,  $d \leq n$ , és  $g \in K[x]$  az  $\alpha, \alpha^2, \dots, \alpha^{d-1}$  elemek minimálpolinomjainak legkisebb közös többszöröse. Ekkor a  $g$  által generált  $n$ -hosszú ciklikus lineáris kódot **BCH-kódnak** nevezzük, ahol  $d$  a kód **tervezett távolsága**.

**51. Tétel (Bose, Ray-Chaudhuri, Hocquenghem).** Legyen  $C$  az előző definícióban megadott BCH-kód. Ekkor  $C$

- (1) hossza  $n$  és  $n \leq |K|^r - 1$ ,
- (2) minimális távolsága legalább  $d$ ,
- (3) dimenziója legalább  $n - r(d - 1)$ .

**52. Példa.** Tervezzünk bináris 1-hibajavító BCH-kódot. Mivel a kód 1-hibajavító, ezért a minimális távolságának 3-nak kell lennie. Olyan véges testet kell tehát keresnünk, amelyben van legalább harmadrendű elem. Tudjuk, hogy a  $\text{GF}(2^k)$  testben van primitív, azaz  $2^k - 1$ -rendű elem, tehát a  $k = 2$  jó választás. A  $\text{GF}(2^2)$  testet az  $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$  irreducibilis polinommal állítjuk elő. A  $\mathbb{Z}_2[x]/\langle f \rangle$  testben könnyen leellenőrizhető, hogy az  $\alpha = \bar{x}$  elem rendje éppen 3, mert

$$\begin{aligned}\alpha^2 &= \overline{x^2} = \overline{x + 1}, \\ \alpha^3 &= \overline{x(x + 1)} = \overline{x^2 + x} = 1.\end{aligned}$$

Ebből azt is látjuk, hogy  $1 + \alpha + \alpha^2 = 0$ , azaz  $\alpha$  minimálpolinomja  $g = 1 + x + x^2$ , és  $1 + \alpha^2 + (\alpha^2)^2 = 1 + \alpha^2 + \alpha = 1$ , azaz  $\alpha^2$  minimálpolinomja szintén  $g = 1 + x + x^2$ . Tehát  $\alpha$  és  $\alpha^2$  minimálpolinomjainak legkisebb közös többszöröse  $g = 1 + x + x^2$ , így a keresett kód generátormátrixa

$$G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix},$$

azaz  $C = \{000, 111\}$ .

**53. Tétel.** A 3-minimális távolságú BCH-kódok éppen a ciklikus Hamming-kódok.

**54. Tétel.** A  $\text{GF}(2^k)$  test tetszőleges  $\alpha$  elemére  $\alpha$  és  $\alpha^2$  minimálpolinomjai megegyezik.

**55. Példa.** Tervezzünk bináris 2-hibajavító kódot. A  $d$  minimális távolságnak most 5-nek kell lennie. Legalább ötödrendű  $\alpha$  elemet kell keresnünk és ilyen van a  $\text{GF}(2^3)$  testben. Válasszuk az  $f = x^3 + x + 1 \in \mathbb{Z}_2[x]$  irreducibilis polinomot. Tudjuk, hogy a  $\mathbb{Z}_2[x]/\langle f \rangle$  test minden nemzéró elemének rendje osztója  $2^3 - 1 = 7$ -nek, azaz a 0-tól és 1-től különböző elemek hetedrendűek. Legyen tehát  $\alpha = \bar{x}$  és  $n = 7$ . Ki kell számolnunk az  $\alpha, \alpha^2, \alpha^3$  és  $\alpha^4$  elemek minimálpolinomját, amihez  $\alpha$  hatványaira van szükségünk:

$$\begin{aligned}\alpha^1 &= \bar{x}, \\ \alpha^2 &= \overline{x^2}, \\ \alpha^3 &= \overline{x^3} = \overline{x + 1}, \\ \alpha^4 &= \overline{x(x + 1)} = \overline{x^2 + x}, \\ \alpha^5 &= \overline{x(x^2 + x)} = \overline{x^3 + x^2} = \overline{x^2 + x + 1}, \\ \alpha^6 &= \overline{x(x^2 + x + 1)} = \overline{x^3 + x^2 + x} = \overline{x^2 + 1}, \\ \alpha^7 &= \overline{x(x^2 + 1)} = \overline{x^3 + x} = \bar{1}.\end{aligned}$$

Tehát  $\alpha^3 + \alpha + 1 = 0$ , azaz  $\alpha$  minimálpolinomja  $x^3 + x + 1$ , és az előző tétel szerint ugyan ez a minimálpolinomja az  $\alpha^2$  és  $\alpha^4$  elemeknek is. Az  $\alpha^3$  minimálpolinomja  $x^3 + x^2 + 1$ , mivel  $\alpha^9 + \alpha^6 + 1 = \alpha^2 + \alpha^6 + 1 = 0$ . A minimálpolinomok legkisebb közös többszöröse  $g = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ , így a keresett kód generátormátrixa  $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$ . Ennek a kódnak a minimális távolsága 7, jobb mint a tervezett, de nem valami érdekes, mert dimenziója csak 1, információs rátája pedig csak 1/7. A probléma abból adódik, hogy túl kicsi testben számoltunk.

**56. Példa.** Megint bináris 2-hibajavító kódot tervezünk, de most az  $f = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$  irreducibilis polinomot és a  $\mathbb{Z}_2[x]/\langle f \rangle$  testet használva. Vegyünk az  $\alpha = \bar{x} = \overline{0100}$  elemet, és számoljuk ki hatványait (a polinomok és szavak azonosítását felhasználva)

$$\begin{aligned} \alpha^1 &= \overline{0100}, & \alpha^2 &= \overline{0010}, & \alpha^3 &= \overline{0001}, & \alpha^4 &= \overline{1001}, & \alpha^5 &= \overline{1101}, \\ \alpha^6 &= \overline{1111}, & \alpha^7 &= \overline{1110}, & \alpha^8 &= \overline{0111}, & \alpha^9 &= \overline{1010}, & \alpha^{10} &= \overline{0101}, \\ \alpha^{11} &= \overline{1011}, & \alpha^{12} &= \overline{1100}, & \alpha^{13} &= \overline{0110}, & \alpha^{14} &= \overline{0011}, & \alpha^{15} &= \overline{1000}. \end{aligned}$$

Látjuk, hogy  $\alpha$  rendje 15, azaz  $\alpha$  primitív, és ezért  $n$  tetszőlegesen választható  $d = 5$  és  $o(\alpha) = 15$  között. Az is leolvasható, hogy  $\alpha$  minimálpolinomja  $x^4 + x^3 + 1$ ,  $\alpha^2$  és  $\alpha^4$  minimálpolinomja szintén ez az előző tétel szerint, és  $\alpha^3$  minimálpolinomja  $x^4 + x^3 + x^2 + x + 1$ . Tehát a kód generátorpolinomja  $g = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^4 + x^2 + x + 1$ . Ha maximális dimenziójú kódot keresünk, akkor legyen  $n = 15$ . Így a kód generátormátrixa

$$P = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

dimenziója  $n - \deg g = 15 - 8 = 7$ , és információs rátája  $\frac{7}{15}$ .

**57. Definíció.** Ha a BCH-kód definíciójában  $\alpha \in K$ , akkor  $\alpha$  hatványainak minimálpolinomjai mind elsőfokúak, azaz  $g = (x - \alpha)(x - \alpha^2) \dots (x - \alpha^{d-1})$ . A kapott kódot **Reed-Solomon** kódnak nevezzük, melynek dimenziója  $n - d + 1$ .

**58. Példa.** Legyen  $K = \text{GF}(2^3)$  a nyolcelemű test és  $\alpha \in K$  a 55 példában használt hetedrendű elem, melyről tudjuk, hogy  $\alpha^7 = 1$  és  $\alpha^3 + \alpha + 1 = 0$ . Tervezzünk maximális információs rátájú 2-hibajavító kódot, azaz legyen  $d = 5$  és  $n = 7$ . Az  $f \in K[x]$  hetedrendű irreducibilis polinomot meg sem kell határoznunk, mert minket csak  $g$  érdekel. Tehát

$$g = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4).$$

Mivel  $K$  karakterisztikája 2, ezért tetszőleges  $a \in K$  elemre  $a = -a$ , azaz

$$g = (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4).$$

Ezt kifejtve és felhasználva az  $\alpha^7 = 1$  és  $\alpha^3 + \alpha + 1 = 0$  azonosságokat

$$\begin{aligned} g &= x^4 + (\alpha + \alpha^2 + \alpha^3 + \alpha^4)x^3 + (\alpha\alpha^2 + \alpha\alpha^3 + \alpha\alpha^4 + \alpha^2\alpha^3 + \alpha^2\alpha^4 + \alpha^3\alpha^4)x^2 \\ &\quad + (\alpha\alpha^2\alpha^3 + \alpha\alpha^2\alpha^4 + \alpha\alpha^3\alpha^4 + \alpha^2\alpha^3\alpha^4)x + \alpha\alpha^2\alpha^3\alpha^4 \\ &= x^4 + (\alpha + \alpha^2 + \alpha^3 + \alpha^4)x^3 + (\alpha^3 + \alpha^4 + \alpha^5 + \alpha^5 + \alpha^6 + \alpha^7)x^2 \\ &\quad + (\alpha^6 + \alpha^7 + \alpha^8 + \alpha^9)x + \alpha^{10} \\ &= x^4 + (\alpha^3 + \alpha(1 + \alpha + \alpha^3))x^3 + (1 + \alpha^3(1 + \alpha + \alpha^3))x^2 + (\alpha + \alpha^6(1 + \alpha + \alpha^3))x + \alpha^3 \\ &= x^4 + \alpha^3x^3 + x^2 + \alpha x + \alpha^3. \end{aligned}$$

Tehát a kapott Reed-Solomon kód generátor mátrixa

$$G = \begin{pmatrix} \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 & 0 \\ 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 \\ 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 \end{pmatrix} \in K^{3 \times 7},$$

dimenziója 3, információs rátája  $\frac{3}{7}$  és pontosan  $8^3 = 512$  kódszót tartalmaz.