

## 4. Műveletek $GF(q)$ felett, Reed–Solomon kódok, ciklikus lineáris kódok

Kódolástechnika

# GF(q) axiómái

GF(q) a q elemű Galois test (véges test).

## Test axiómák

Összeadás “+”

$$\alpha, \beta \in GF(q) \rightarrow \alpha + \beta \in GF(q)$$

$$\alpha + \beta = \beta + \alpha$$

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$

$$\exists 0 : \forall \alpha \in GF(q) : \alpha + 0 = \alpha$$

$$\forall \alpha \in GF(q) \exists \beta : \alpha + \beta = 0;$$

$$\beta = \alpha_a^{-1} = -\alpha$$

Szorzás “\*”

$$\alpha, \beta \in GF(q) \rightarrow \alpha * \beta \in GF(q)$$

$$\alpha * \beta = \beta * \alpha$$

$$(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$$

$$\exists 1 : \forall \alpha \in GF(q) : \alpha * 1 = \alpha$$

$$\forall \alpha \in GF(q) \setminus \{0\} : \exists \beta : \alpha * \beta = 1;$$

$$\beta = \alpha_m^{-1} = \alpha^{-1}$$

$$\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma$$

“+” és “\*” bármilyen lehet, amíg teljesítik a fenti axiómákat.

## Példák $GF(q)$ -ra

$q$  lehet prímszám vagy prímszámhatvány ( $p^m$ , ahol  $p$  prímszám és  $m \geq 2$ ).

**Egyelőre a  $q$  prímszám esettel foglalkozunk.** Ha  $q$  prímszám, akkor  $GF(q)$ -ban a műveletek mod  $q$  értendők:

$$GF(q) = \{0, 1, \dots, q - 1\},$$

és

$$\alpha + \beta = \alpha + \beta \pmod{q},$$

$$\alpha * \beta = \alpha \cdot \beta \pmod{q}.$$

Például  $GF(7)$ -ben:

$$6 + 5 = 4 \pmod{7} \qquad (6 + 5 = 11 = 4 \pmod{7})$$

$$6 * 5 = 2 \pmod{7} \qquad (6 \cdot 5 = 30 = 2 \pmod{7})$$

$$4_a^{-1} = 3 \pmod{7} \qquad (4 + 3 = 7 = 0 \pmod{7})$$

$$4_m^{-1} = 2 \pmod{7} \qquad (4 \cdot 2 = 8 = 1 \pmod{7})$$

# Hatványtábla

Alap tulajdonság:  $\forall \alpha \in GF(q) \setminus \{0\} : \alpha^{q-1} = 1$ .

Egy  $\alpha$  elem rendje az a legkisebb pozitív  $m$ , amire  $\alpha^m = 1$ . Ha  $m = q - 1$ , akkor  $\alpha$ -t primitív elemnek nevezzük.

# Hatványtábla

Alap tulajdonság:  $\forall \alpha \in GF(q) \setminus \{0\} : \alpha^{q-1} = 1$ .

Egy  $\alpha$  elem rendje az a legkisebb pozitív  $m$ , amire  $\alpha^m = 1$ . Ha  $m = q - 1$ , akkor  $\alpha$ -t primitív elemnek nevezzük.

elem $\alpha$	hatványok						rend $m$
	$\alpha^1$	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$	
1	1						1
2	2	4	1				3
3	3	2	6	4	5	1	6
4	4	2	1				3
5	5	4	6	2	3	1	6
6	6	1					2

– primitív elem

– primitív elem

# Hatványtábla

Alap tulajdonság:  $\forall \alpha \in GF(q) \setminus \{0\} : \alpha^{q-1} = 1$ .

Egy  $\alpha$  elem rendje az a legkisebb pozitív  $m$ , amire  $\alpha^m = 1$ . Ha  $m = q - 1$ , akkor  $\alpha$ -t primitív elemnek nevezzük.

elem $\alpha$	hatványok						rend $m$
	$\alpha^1$	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$	
1	1						1
2	2	4	1				3
3	3	2	6	4	5	1	6
4	4	2	1				3
5	5	4	6	2	3	1	6
6	6	1					2

– primitív elem

– primitív elem

Egy primitív elem hatványai kiadják a  $GF(q)$  összes nemnulla elemét.

## Polinomok $GF(q)$ felett

$$\alpha(x) = \alpha_0 + \alpha_1x + \alpha_2x^2 + \cdots + \alpha_mx^m; \alpha_0, \alpha_1, \alpha_2, \dots, \alpha_m \in GF(q)$$

Gyökök:  $x_1, \dots, x_m$ :  $\alpha(x_i) = 0, i = 1, \dots, m$

A gyökök száma  $\leq \deg(\alpha(x)) = m$ .

Ha  $\alpha(x)$ -nek  $\deg(\alpha(x)) = m$  gyöke van,  $x_1, \dots, x_m$ , akkor

$$\alpha(x) = \alpha_m \prod_{i=1}^m (x - x_i).$$

Polinomosztás: adott  $\alpha(x)$  és  $d(x)$  esetén, ahol  $\deg(\alpha(x)) = m > \deg(d(x)) = k$ ,

$$\exists q(x), r(x) : \alpha(x) = q(x)d(x) + r(x); \quad \deg(r(x)) < k.$$

$a(x), d(x) \rightarrow$  Euklideszi algoritmus  $\rightarrow q(x), r(x)$   
 $m - k$  lépés

# 1. feladat

Mi a 2 additív inverze  $GF(5)$ -ben?



# 1. feladat

Mi a 2 additív inverze GF(5)-ben?

Megoldás.  $2 + 3 = 1 \cdot 5 + 0$ , tehát a 2 additív inverze (ellentettje) GF(5)-ben

$$-2 = 2_a^{-1} = 3.$$

## 2. feladat

Mi a 2 multiplikatív inverze  $GF(5)$ -ben?

## 2. feladat

Mi a 2 multiplikatív inverze GF(5)-ben?

Megoldás.  $2 \cdot 3 = 1 \cdot 5 + 1$ , azaz

$$2 * 3 = 1 \pmod{5},$$

tehát a 2 multiplikatív inverze (reciproka) GF(5)-ben

$$2^{-1} = 2_m^{-1} = 3.$$

### 3. feladat

Mi az 5 additív inverze  $GF(11)$ -ben?

### 3. feladat

Mi az 5 additív inverze GF(11)-ben?

Megoldás.  $5 + 6 = 1 \cdot 11 + 0$ , tehát az 5 additív inverze GF(11)-ben

$$-5 = 5_a^{-1} = 6.$$

## 4. feladat

Mi  $\text{GF}(11)$ -ben a 7 multiplikatív inverze?

## 4. feladat

Mi  $\text{GF}(11)$ -ben a 7 multiplikatív inverze?

Megoldás.  $7 \cdot 8 = 5 \cdot 11 + 1$ , azaz

$$7 * 8 = 1 \pmod{11},$$

így a 7 multiplikatív inverze  $\text{GF}(11)$ -ben

$$7^{-1} = 7_m^{-1} = 8.$$

## 5. feladat

Oldjuk meg a  $6x + 5 = 2$  egyenletet  $GF(7)$  felett.



## 5. feladat

Oldjuk meg a  $6x + 5 = 2$  egyenletet  $GF(7)$  felett.

Megoldás.

$$6x + 5 = 2$$

$$6x = 2 - 5$$

$$6x = -3$$

$$6x = 4$$

$$x = 6^{-1} * 4$$

$$x = 6 * 4$$

$$x = 24$$

$$x = 3$$

## Reed–Solomon kódok

Legyen  $n = q - 1$  és  $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$  különböző nemnulla elemek  $\text{GF}(q)$ -ből.

Az ezeknek megfelelő  $C(n, k)$  Reed-Solomon kód egy  $\text{GF}(q)$  feletti lineáris kód, melynek generátor mátrixa

$$G = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} \\ \vdots & & & \ddots & \vdots \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_{n-1}^{k-1} \end{bmatrix}$$

## Reed–Solomon kódok

Legyen  $n = q - 1$  és  $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$  különböző nemnulla elemek  $\text{GF}(q)$ -ből.

Az ezeknek megfelelő  $C(n, k)$  Reed-Solomon kód egy  $\text{GF}(q)$  feletti lineáris kód, melynek generátor mátrixa

$$G = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} \\ \vdots & & & \ddots & \vdots \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_{n-1}^{k-1} \end{bmatrix}$$

Az RS kódokra teljesül az MDS tulajdonság:

$$d_{\min} = n - k + 1,$$

azaz a kód képes

- ▶  $n - k$  hibát detektálni, és
- ▶  $\lfloor \frac{n-k}{2} \rfloor$  hibát javítani.

## Reed-Solomon kódok

Speciális eset: egy  $\alpha$  primitív elem által generált RS kód. Ha az előbbi konstrukcióban  $\alpha_i = \alpha^i$ , akkor

$$G = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ \vdots & & & \ddots & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \dots & \alpha^{(n-1)(k-1)} \end{bmatrix},$$

és a paritás ellenőrző mátrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & & & \ddots & \vdots \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \dots & \alpha^{(n-k)(n-1)} \end{bmatrix}.$$

## 6. feladat

Tervezzünk egy RS kódot  $GF(7)$  felett, ami képes 2 hiba javítására.

## 6. feladat

Tervezzünk egy RS kódot  $GF(7)$  felett, ami képes 2 hiba javítására.

Megoldás. Először az  $(n, k)$  paramétereket számítjuk ki.

## 6. feladat

Tervezzünk egy RS kódot  $GF(7)$  felett, ami képes 2 hiba javítására.

Megoldás. Először az  $(n, k)$  paramétereket számítjuk ki.

$$n = q - 1 = 6,$$

és a hibajavító képesség

$$t = \left\lfloor \frac{n - k}{2} \right\rfloor = 2 \quad \rightarrow \quad n - k = 4,$$

így

$$(n, k) = (6, 2).$$

## 6. feladat

Bármely  $GF(7)$  feletti  $C(6,2)$  RS kód megfelelő; például, ha az 5 primitív elem által generált Reed-Solomon kódot vesszük, akkor

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix}$$

és

$$H = \begin{bmatrix} 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{bmatrix}.$$



## 7. feladat

Kódoljuk az előbbi kóddal a következő kódszavakat:  $u = (4, 4)$ ,  
 $u = (3, 5)$  és  $u = (5, 1)$ .

## 7. feladat

Kódoljuk az előbbi kóddal a következő kódszavakat:  $u = (4, 4)$ ,  
 $u = (3, 5)$  és  $u = (5, 1)$ .

Megoldás.

$$(44) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} = (136052)$$

## 7. feladat

Kódoljuk az előbbi kóddal a következő kódszavakat:  $u = (4, 4)$ ,  
 $u = (3, 5)$  és  $u = (5, 1)$ .

Megoldás.

$$(44) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} = (136052)$$

$$(35) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} = (102564)$$

## 7. feladat

Kódoljuk az előbbi kóddal a következő kódszavakat:  $u = (4, 4)$ ,  
 $u = (3, 5)$  és  $u = (5, 1)$ .

Megoldás.

$$(44) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} = (136052)$$

$$(35) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} = (102564)$$

$$(51) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} = (632401)$$

## 8. feladat

Adjuk meg a  $GF(5)$  feletti, a 2 primitív elem által generált, 1 hiba javítására képes RS kód generátor mátrixát és paritás ellenőrző mátrixát.

## 8. feladat

Adjuk meg a  $GF(5)$  feletti, a 2 primitív elem által generált, 1 hiba javítására képes RS kód generátor mátrixát és paritás ellenőrző mátrixát.

Megoldás. A hibajavító képesség alapján

$$t = \left\lfloor \frac{n - k}{2} \right\rfloor = 1 \quad \rightarrow \quad n - k = 2.$$

## 8. feladat

Adjuk meg a  $GF(5)$  feletti, a 2 primitív elem által generált, 1 hiba javítására képes RS kód generátor mátrixát és paritás ellenőrző mátrixát.

Megoldás. A hibajavító képesség alapján

$$t = \left\lfloor \frac{n-k}{2} \right\rfloor = 1 \quad \rightarrow \quad n-k = 2.$$

$q = 5$  miatt  $n = q - 1 = 4$ , így  $(n, k) = (4, 2)$ , és

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \end{bmatrix} \quad H = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \end{bmatrix}.$$

## 9. feladat

Egy GF(11) feletti C(10,4) RS kód generátor mátrixa

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 6 & 3 & 7 & 9 & 10 & 5 & 8 & 4 & 2 \\ 1 & 3 & 9 & 5 & 4 & 1 & 3 & 9 & 5 & 4 \\ 1 & 7 & 5 & 2 & 3 & 10 & 4 & 6 & 9 & 8 \end{bmatrix}$$

- (a) Mennyi hibát képes a kód javítani?
- (b) Milyen primitív elem segítségével generáltuk a kódot?
- (c) Adjuk meg a  $H$  paritás ellenőrző mátrixot.



## 9. feladat

Megoldás.

(a) Ez egy RS kód, tehát  $\lfloor \frac{n-k}{2} \rfloor = 3$  hibát képes javítani.

## 9. feladat

Megoldás.

- (a) Ez egy RS kód, tehát  $\lfloor \frac{n-k}{2} \rfloor = 3$  hibát képes javítani.
- (b) A 6 primitív elem segítségével generáltuk:

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 6 & 3 & 7 & 9 & 10 & 5 & 8 & 4 & 2 \\ 1 & 3 & 9 & 5 & 4 & 1 & 3 & 9 & 5 & 4 \\ 1 & 7 & 5 & 2 & 3 & 10 & 4 & 6 & 9 & 8 \end{bmatrix}$$

## 9. feladat

Megoldás.

- (a) Ez egy RS kód, tehát  $\lfloor \frac{n-k}{2} \rfloor = 3$  hibát képes javítani.  
(b) A 6 primitív elem segítségével generáltuk:

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 6 & 3 & 7 & 9 & 10 & 5 & 8 & 4 & 2 \\ 1 & 3 & 9 & 5 & 4 & 1 & 3 & 9 & 5 & 4 \\ 1 & 7 & 5 & 2 & 3 & 10 & 4 & 6 & 9 & 8 \end{bmatrix}$$

(c)

$$H = \begin{bmatrix} 1 & 6 & 3 & 7 & 9 & 10 & 5 & 8 & 4 & 2 \\ 1 & 3 & 9 & 5 & 4 & 1 & 3 & 9 & 5 & 4 \\ 1 & 7 & 5 & 2 & 3 & 10 & 4 & 6 & 9 & 8 \\ 1 & 9 & 4 & 3 & 5 & 1 & 9 & 4 & 3 & 5 \\ 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 \\ 1 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \end{bmatrix}$$

## 10. feladat

Egy GF(7) feletti RS kód paritás ellenőrző mátrixa

$$H = \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$

- (a) Mi a kód típusa (azaz az  $n$  és  $k$  paraméterek értéke)?
- (a) Hány hiba javítására képes a kód?
- (c) Adjuk meg a csupa 2-esből álló üzenethez tartozó kódszót.

## 10. feladat

Megoldás.

- (a) A  $H$  paritás ellenőrző mátrix mérete egy  $C(n, k)$  RS kód esetén  $(n - k) \times n$ . Jelen esetben  $H$   $4 \times 6$ -os, tehát  $(n, k) = (6, 2)$ .

## 10. feladat

Megoldás.

- (a) A  $H$  paritás ellenőrző mátrix mérete egy  $C(n, k)$  RS kód esetén  $(n - k) \times n$ . Jelen esetben  $H$   $4 \times 6$ -os, tehát  $(n, k) = (6, 2)$ .
- (b) Egy RS kódra a hibajavítási képesség  $\lfloor \frac{n-k}{2} \rfloor = 2$ .

## 10. feladat

Megoldás.

- (a) A  $H$  paritás ellenőrző mátrix mérete egy  $C(n, k)$  RS kód esetén  $(n - k) \times n$ . Jelen esetben  $H$   $4 \times 6$ -os, tehát  $(n, k) = (6, 2)$ .
- (b) Egy RS kódra a hibajavítási képesség  $\lfloor \frac{n-k}{2} \rfloor = 2$ .
- (c) A kódot a 3 primitív elem generálja, tehát

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{bmatrix},$$

és

$$c = uG = (22) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{bmatrix} = (416035).$$

## 11. feladat

Egy  $C(6,3)$  RS kódot a véges test legnagyobb primitív eleme generál.

- (a) Adjuk meg a  $G$  generátor mátrixot.
- (b) Adjuk meg a  $H$  paritás ellenőrző mátrixot.
- (c) Hány hibát képes a kód detektálni? Hány hibát képes javítani?



## 11. feladat

Megoldás.

- (a)  $q$  értéke közvetlenül ugyan nincs megadva, de  $n = q - 1$ , ahonnan  $q = 7$ .  $\text{GF}(7)$ -ben a legnagyobb primitív elem az 5, így

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$

## 11. feladat

Megoldás.

- (a)  $q$  értéke közvetlenül ugyan nincs megadva, de  $n = q - 1$ , ahonnan  $q = 7$ .  $GF(7)$ -ben a legnagyobb primitív elem az 5, így

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$

- (b)

$$H = \begin{bmatrix} 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \end{bmatrix}$$

## 11. feladat

Megoldás.

- (a)  $q$  értéke közvetlenül ugyan nincs megadva, de  $n = q - 1$ , ahonnan  $q = 7$ .  $GF(7)$ -ben a legnagyobb primitív elem az 5, így

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$

- (b)

$$H = \begin{bmatrix} 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \end{bmatrix}$$

- (c) A kód képes

- ▶  $n - k = 3$  hibát detektálni, és
- ▶  $\lfloor \frac{n-k}{2} \rfloor = 1$  hibát javítani.

# Lineáris ciklikus kódok

Egy kód ciklikus, ha bármely

$$c = (c_0 \ c_1 \ c_2 \ \dots \ c_{n-1}),$$

kódszó esetén a ciklikus eltolója:

$$Sc = (c_{n-1} \ c_0 \ c_1 \ \dots \ c_{n-2})$$

szintén kódszó.  $S$  a ciklikus eltolás operátor.

# Lineáris ciklikus kódok

Egy kód ciklikus, ha bármely

$$c = (c_0 \ c_1 \ c_2 \ \dots \ c_{n-1}),$$

kódszó esetén a ciklikus eltolója:

$$Sc = (c_{n-1} \ c_0 \ c_1 \ \dots \ c_{n-2})$$

szintén kódszó.  $S$  a ciklikus eltolás operátor.

Egy  $\alpha$  primitív elem által generált Reed-Solomon kód egyúttal ciklikus lineáris kód is.

## Lineáris ciklikus kódok

Példa. A  $GF(5)$  feletti, 2 primitív elem által generált  $C(4,2)$  RS kód kódszavai:

$(00) \rightarrow (00\ 00)$	$(23) \rightarrow (0\ 3\ 4\ 1)$
$(01) \rightarrow (12\ 43)$	$(24) \rightarrow (1\ 0\ 3\ 4)$
$(02) \rightarrow (24\ 31)$	$(30) \rightarrow (3\ 3\ 3\ 3)$
$(03) \rightarrow (31\ 24)$	$(31) \rightarrow (4\ 0\ 2\ 1)$
$(04) \rightarrow (43\ 12)$	$(32) \rightarrow (0\ 2\ 14)$
$(10) \rightarrow (11\ 11)$	$(33) \rightarrow (1\ 4\ 0\ 2)$
$(11) \rightarrow (23\ 04)$	$(34) \rightarrow (2\ 14\ 0)$
$(12) \rightarrow (30\ 42)$	$(40) \rightarrow (4\ 4\ 4\ 4)$
$(13) \rightarrow (42\ 30)$	$(41) \rightarrow (0\ 13\ 2)$
$(14) \rightarrow (04\ 23)$	$(42) \rightarrow (1\ 3\ 2\ 0)$
$(20) \rightarrow (22\ 22)$	$(43) \rightarrow (2\ 0\ 13)$
$(21) \rightarrow (34\ 10)$	$(44) \rightarrow (3\ 2\ 0\ 1)$
$(22) \rightarrow (41\ 03)$	

## 12. feladat

Egy  $GF(5)$  feletti  $C(6,2)$  lineáris ciklikus kód 2 hibát tud kijavítani.  
A  $(6,0,3,5,4,1)$  szerepel a kódszavak között.

- (a) Kódszó-e az  $(5,4,1,6,0,3)$ ?
- (b) Kódszó-e az  $(1,0,4,2,3,6)$ ?
- (c) Kódszó-e az  $(1,0,4,3,5,2)$ ?

## 12. feladat

Egy  $GF(5)$  feletti  $C(6,2)$  lineáris ciklikus kód 2 hibát tud kijavítani.  
A  $(6,0,3,5,4,1)$  szerepel a kódszavak között.

- (a) Kódszó-e az  $(5,4,1,6,0,3)$ ?
- (b) Kódszó-e az  $(1,0,4,2,3,6)$ ?
- (c) Kódszó-e az  $(1,0,4,3,5,2)$ ?

Megoldás.

- (a) Igen, mert a megadott kódszó ciklikus eltoltja (3-szor kell eltolni).



## 12. feladat

Egy  $GF(5)$  feletti  $C(6,2)$  lineáris ciklikus kód 2 hibát tud kijavítani. A  $(6,0,3,5,4,1)$  szerepel a kódszavak között.

- (a) Kódszó-e az  $(5,4,1,6,0,3)$ ?
- (b) Kódszó-e az  $(1,0,4,2,3,6)$ ?
- (c) Kódszó-e az  $(1,0,4,3,5,2)$ ?

Megoldás.

- (a) Igen, mert a megadott kódszó ciklikus eltoltja (3-szor kell eltolni).
- (b) Igen, mert a megadott kódszó konstansszorososa (6-tal kell szorozni, ez például arról a helyiértékről látszik, ahol az 1-es szerepel).
- (c) Nem, mert a kód 2 hibát képes javítani  $\rightarrow d_{\min} \geq 5$ , viszont a (b) és (c)-beli vektorok Hamming-távolsága csak 3.

## Kódpolinomok

Polinomokat rendelünk a kódszavakhoz:

$$c = (c_0 \ c_1 \ c_2 \ \dots \ c_{n-1}) \quad \rightarrow \quad c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$$

Ekkor az  $Sc$ -hez rendelt polinom

$$c'(x) = [xc(x)] \quad \text{mod } (x^n - 1).$$

Hasonlóan az üzenetekhez, hibavektorhoz stb. is rendelhetünk polinomot.

## Kódpolinomok

Polinomokat rendelünk a kódszavakhoz:

$$c = (c_0 \ c_1 \ c_2 \ \dots \ c_{n-1}) \quad \rightarrow \quad c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$$

Ekkor az  $Sc$ -hez rendelt polinom

$$c'(x) = [xc(x)] \quad \text{mod } (x^n - 1).$$

Hasonlóan az üzenetekhez, hibavektorhoz stb. is rendelhetünk polinomot.

Bármely  $C(n, k)$  ciklikus lineáris kódra létezik egy  $(n - k)$ -adfokú  $g(x)$  kódpolinom, melyre teljesül, hogy minden kódpolinom

$$c(x) = g(x)u(x).$$

alakú.  $g(x)$ -et a kód generátorpolinomjának nevezzük.

# Kódpolinomok

Polinomokat rendelünk a kódszavakhoz:

$$c = (c_0 \ c_1 \ c_2 \ \dots \ c_{n-1}) \quad \rightarrow \quad c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$$

Ekkor az  $Sc$ -hez rendelt polinom

$$c'(x) = [xc(x)] \quad \text{mod } (x^n - 1).$$

Hasonlóan az üzenetekhez, hibavektorhoz stb. is rendelhetünk polinomot.

Bármely  $C(n, k)$  ciklikus lineáris kódra létezik egy  $(n - k)$ -adfokú  $g(x)$  kódpolinom, melyre teljesül, hogy minden kódpolinom

$$c(x) = g(x)u(x).$$

alakú.  $g(x)$ -et a kód generátorpolinomjának nevezzük.

$g(x) \mid x^n - 1$  mindig teljesül, és tetszőleges ilyen  $g(x)$  megfelelő generátorpolinom egy ciklikus lineáris kódhoz.

# Kódpolinomok

Példa. A  $GF(5)$  feletti, 2 primitív elem által generált  $C(4,2)$  RS kód generátorpolinomja

$$g(x) = (x - 2^1)(x - 2^2) = (x - 2)(x - 4).$$

Néhány kódszóhoz tartozó polinom:

$$(1\ 2\ 4\ 3) \rightarrow 1 + 2x + 4x^2 + 3x^3 = (4 + 3x)(x - 2)(x - 4),$$

$$(0\ 3\ 4\ 1) \rightarrow 3x + 4x^2 + x^3 = x(x - 2)(x - 4),$$

$$(4\ 4\ 4\ 4) \rightarrow 4 + 4x + 4x^2 + 4x^3 = (3 + 4x)(x - 2)(x - 4).$$

# Kódpolinomok

$g(x)$  megadja a kódszavak halmazát, de azt nem, hogy hogyan rendeljük hozzá az üzenetekhez a kódszavakat. A lineáris kódokra szokásos  $c = uG$  hozzárendelés egy lehetőség, de polinomok esetén praktikusabb a

$$c(x) = u(x)g(x)$$

képlettel dolgozni. (Ez egy másik hozzárendelést ad meg, mint a  $c = uG$  képlet.)

## Lineáris ciklikus kódok

A  $g(x)$ -hez tartozó paritás ellenőrző polinom

$$h(x) = \frac{x^n - 1}{g(x)}.$$

A  $v(x)$  vett kódszóhoz tartozó szindróma polinom

$$s(x) = v(x) \pmod{g(x)} \iff s(x) = v(x) : g(x)$$

## Lineáris ciklikus kódok

A  $g(x)$ -hez tartozó paritás ellenőrző polinom

$$h(x) = \frac{x^n - 1}{g(x)}.$$

A  $v(x)$  vett kódszóhoz tartozó szindróma polinom

$$s(x) = v(x) \pmod{g(x)} \iff s(x) = v(x) : g(x)$$

Az  $\alpha$  primitív elem által generált Reed-Solomon kód generátor és paritás-ellenőrző polinomja

$$g(x) = \prod_{i=1}^{n-k} (x - \alpha^i), \quad h(x) = \prod_{i=n-k+1}^n (x - \alpha^i).$$



## Lineáris ciklikus kódok

A  $g(x)$ -hez tartozó paritás ellenőrző polinom

$$h(x) = \frac{x^n - 1}{g(x)}.$$

A  $v(x)$  vett kódszóhoz tartozó szindróma polinom

$$s(x) = v(x) \pmod{g(x)} \iff s(x) = v(x) : g(x)$$

Az  $\alpha$  primitív elem által generált Reed-Solomon kód generátor és paritás-ellenőrző polinomja

$$g(x) = \prod_{i=1}^{n-k} (x - \alpha^i), \quad h(x) = \prod_{i=n-k+1}^n (x - \alpha^i).$$

Fontos tulajdonság: a polinom szorzás és osztás hatékonyan kiszámítható.

## 13. feladat

Adjuk meg a  $GF(7)$  feletti, 3 primitív elem által generált, 2 hiba javítására képes ciklikus lineáris RS kód generátor polinomját és paritás ellenőrző polinomját.

## 13. feladat

Adjuk meg a  $GF(7)$  feletti, 3 primitív elem által generált, 2 hiba javítására képes ciklikus lineáris RS kód generátor polinomját és paritás ellenőrző polinomját.

Megoldás.

$$g(x) = \prod_{i=1}^{n-k} (x - \alpha^i) = (x - 3)(x - 3^2)(x - 3^3)(x - 3^4) = \\ (x - 3)(x - 2)(x - 6)(x - 4) = (x^2 + 2x + 6)(x^2 + 4x + 3) = \\ x^4 + 6x^3 + 3x^2 + 2x + 4.$$

$$h(x) = \prod_{i=n-k+1}^n (x - \alpha^i) = (x - 3^5)(x - 3^6) = \\ (x - 5)(x - 1) = x^2 + x + 5.$$

## 14. feladat

Az előző kód segítségével adjuk meg a következő üzenetekhez tartozó kódszavakat: (1 1) és (0 2).

## 14. feladat

Az előző kód segítségével adjuk meg a következő üzenetekhez tartozó kódszavakat: (1 1) és (0 2).

Megoldás.

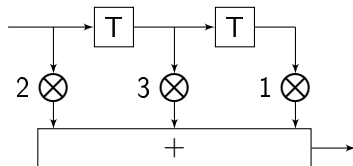
$$c_1(x) = u_1(x)g(x) = (1 + x)(4 + 2x + 3x^2 + 6x^3 + x^4) = 4 + 6x + 5x^2 + 2x^3 + 0 \cdot x^4 + x^5 \rightarrow c_1 = (465201)$$

$$c_2(x) = u_2(x)g(x) = (0 + 2x)(4 + 2x + 3x^2 + 6x^3 + x^4) = 0 + 1 \cdot x + 4x^2 + 6x^3 + 5x^4 + 2x^5 \rightarrow c_2 = (014652)$$

(Egyébként  $c_2 = S^2 c_1$ .)

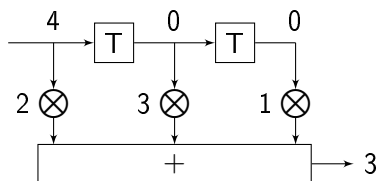
## Polinom szorzás LFSR révén

A  $2 + 3x + x^2$  polinommal való szorzáshoz tartozó Linear FeedForward Shift Register architektúra:



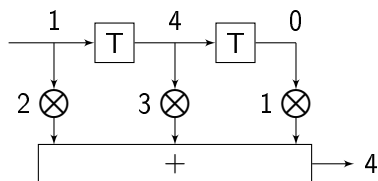
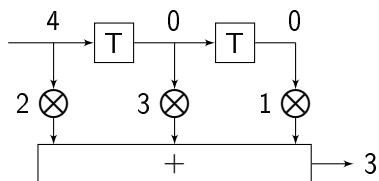
## Polinom szorzás LFSR révén

Számítsuk ki  $(2 + 3x + x^2)(4 + x)$ -et  $GF(5)$  felett:



## Polinom szorzás LFSR révén

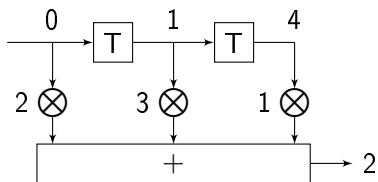
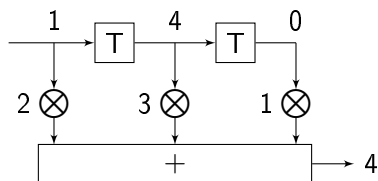
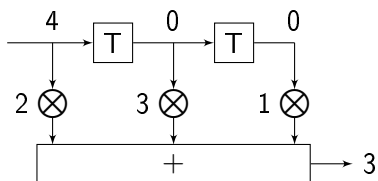
Számítsuk ki  $(2 + 3x + x^2)(4 + x)$ -et  $GF(5)$  felett:





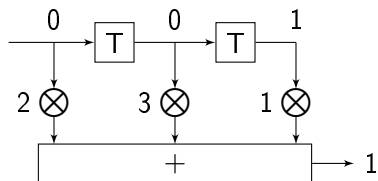
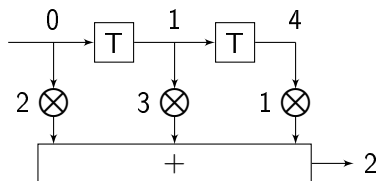
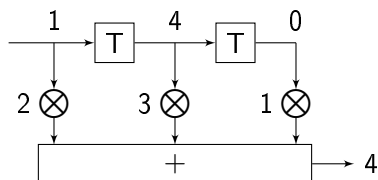
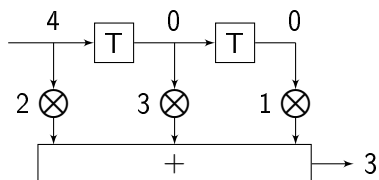
# Polinom szorzás LFSR révén

Számítsuk ki  $(2 + 3x + x^2)(4 + x)$ -et  $GF(5)$  felett:



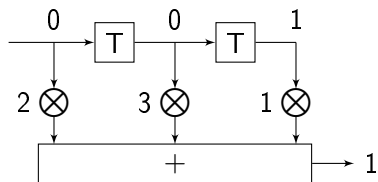
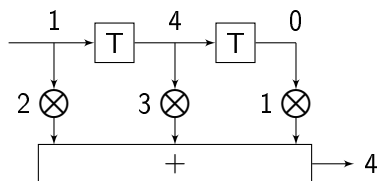
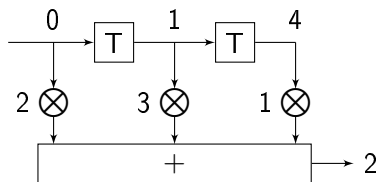
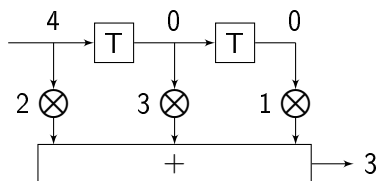
# Polinom szorzás LFSR révén

Számítsuk ki  $(2 + 3x + x^2)(4 + x)$ -et  $GF(5)$  felett:



# Polinom szorzás LFSR révén

Számítsuk ki  $(2 + 3x + x^2)(4 + x)$ -et  $GF(5)$  felett:



$$(3, 4, 2, 1) \longrightarrow 3 + 4x + 2x^2 + x^3$$

## Polinom osztás LFBSR révén

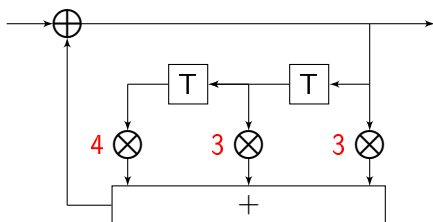
A  $GF(5)$  feletti,  $3 + 2x + x^2$  polinommal való osztáshoz tartozó Linear Feedback Shift Register architektúra. Előkészület: ha az együtthatók

$$a_0 = 3, \quad a_1 = 2, \quad a_2 = 1;$$

akkor a regiszterekbe

$$1 - a_0 = 3, \quad -a_1 = 3, \quad -a_2 = 4$$

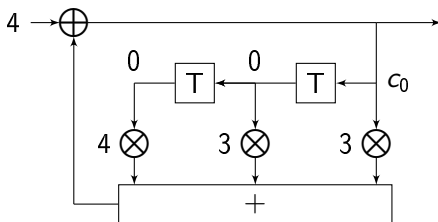
kerül:



## Polinom osztás LFBSR révén

Számítsuk ki  $(4 + 4x + x^3) : (3 + 2x + x^2)$  eredményét  $GF(5)$  felett.

Az LFBSR 2 lépésben működik. Először  $c_0$ -ból indulva megtesz egy teljes kört, ez alapján felír egy lineáris egyenletet  $c_0$ -ra.



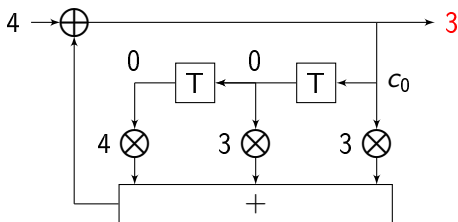
$$4 + 3c_0 = c_0$$

## Polinom osztás LFBSR révén

Számítsuk ki  $(4 + 4x + x^3) : (3 + 2x + x^2)$  eredményét  $GF(5)$  felett.

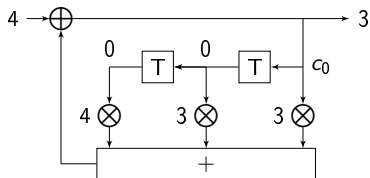
A második lépésben megoldja a lineáris egyenletet  $c_0$ -ra, és a megoldást továbbítja a kimeneten és  $c_0$  helyére is beírja.

$$4 + 3c_0 = c_0 \rightarrow 2c_0 = -4 \rightarrow c_0 = 2^{-1} * 1 = 3 * 1 = 3.$$



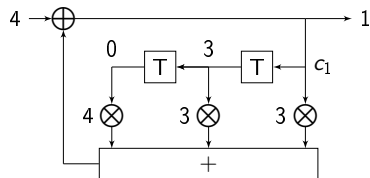
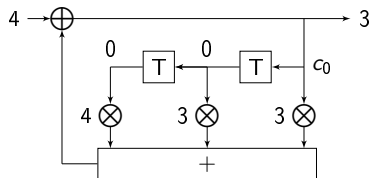
## Polinom osztás LFBSR révén

Számítsuk ki  $(4 + 4x + x^3) : (3 + 2x + x^2)$  eredményét  $GF(5)$  felett.



# Polinom osztás LFBSR révén

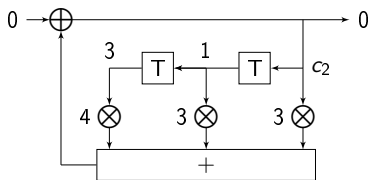
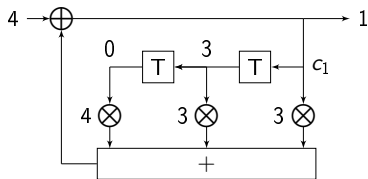
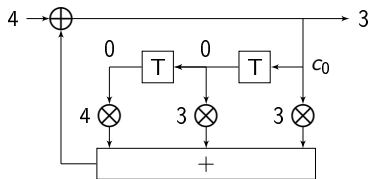
Számítsuk ki  $(4 + 4x + x^3) : (3 + 2x + x^2)$  eredményét  $GF(5)$  felett.





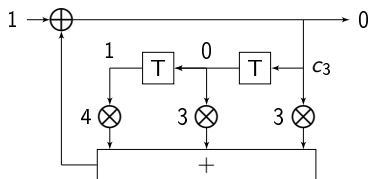
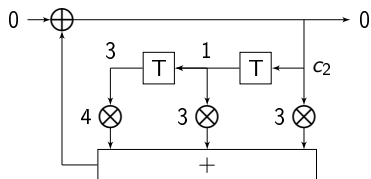
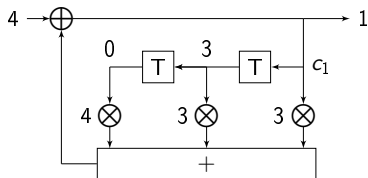
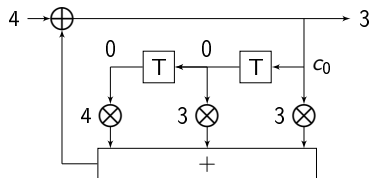
# Polinom osztás LFBSR révén

Számítsuk ki  $(4 + 4x + x^3) : (3 + 2x + x^2)$  eredményét  $GF(5)$  felett.



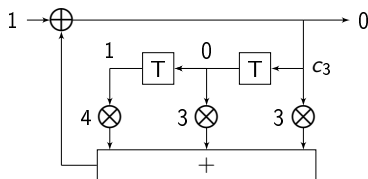
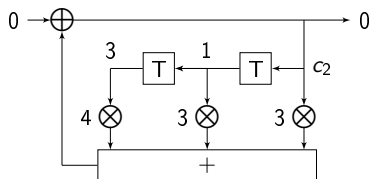
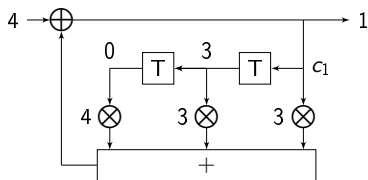
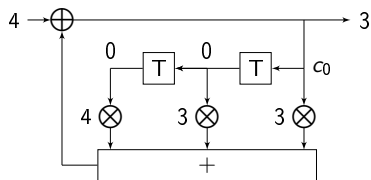
# Polinom osztás LFBSR révén

Számítsuk ki  $(4 + 4x + x^3) : (3 + 2x + x^2)$  eredményét  $GF(5)$  felett.



## Polinom osztás LFBSR révén

Számítsuk ki  $(4 + 4x + x^3) : (3 + 2x + x^2)$  eredményét  $GF(5)$  felett.



$(3, 1, 0, 0)$

$\rightarrow$

$3 + x$

## A kód séma implementálása

A szindróma dekódoló táblázat (a paramétereiktől függően) lehet nagy méretű; viszont a szindróma dekódolás lecserélhető egy gyors, a detektált hibát valós időben kiszámító eljárásra, az Error Trapping Algorithm-re (ETA).

