6. Minimálpolinomok GF(2^m) felett és BCH kódok

Kódolástechnika

Előkészületek

Legyen $q = p^m$ és $n = q - 1$ (p prímszám, $m \geq 2$). GF(q) primitív eleme y, így

$$GF(q) = \{0, 1, y, y^2, \ldots, y^{n-1}\}.$$

Korábbról tudjuk, hogy $x^n - 1$ gyökei kiadják GF(q) összes nemnulla elemét, vagyis

$$x^n - 1 = (x - 1)(x - y)(x - y^2)\ldots(x - y^{n-1}).$$

Előkészületek

Legyen $q = p^m$ és $n = q - 1$ (p prímszám, $m \geq 2$). GF(q) primitív eleme y, így

$$GF(q) = \{0, 1, y, y^2, \ldots, y^{n-1}\}.$$

Korábbról tudjuk, hogy $x^n - 1$ gyökei kiadják GF(q) összes nemnulla elemét, vagyis

$$x^n - 1 = (x - 1)(x - y)(x - y^2) \ldots (x - y^{n-1}).$$

$x^n - 1$ azonban tekinthető egy GF(p) polinomként is, és felbontható GF(p) felett irreducibilis polinomok szorzatára:

$$x^n - 1 = p_1(x)p_2(x) \ldots p_L(x).$$

Előkészületek

Minden egyes $p_\ell(x)$ $(\ell = 1, \ldots, L)$ polinom irreducibilis GF(p) felett, de GF(q) felett gyöktényezőkre bontható.

GF(q) elemeit a $p_\ell(x)$-ek szerint csoportosítjuk. Ezeket konjugált csoportoknak hívjuk.

Példa. GF(8) esetén $(q = 8, p = 2, m = 3, n = 7)$

$$x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) =$$

Előkészületek

Minden egyes $p_\ell(x)$ $(\ell = 1, \ldots, L)$ polinom irreducibilis GF(p) felett, de GF(q) felett gyöktényezőkre bontható.

GF(q) elemeit a $p_\ell(x)$-ek szerint csoportosítjuk. Ezeket konjugált csoportoknak hívjuk.

Példa. GF(8) esetén $(q = 8, p = 2, m = 3, n = 7)$

$$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) =$$
$$= (x-1) \cdot \underbrace{(x^3 + x + 1)}_{(x-y)(x-y^2)(x-y^4)} \cdot \underbrace{(x^3 + x^2 + 1)}_{(x-y^3)(x-y^5)(x-y^6)},$$

Előkészületek

Minden egyes $p_\ell(x)$ $(\ell = 1, \ldots, L)$ polinom irreducibilis GF(p) felett, de GF(q) felett gyöktényezőkre bontható.

GF(q) elemeit a $p_\ell(x)$-ek szerint csoportosítjuk. Ezeket konjugált csoportoknak hívjuk.

Példa. GF(8) esetén $(q = 8, p = 2, m = 3, n = 7)$

$$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) =$$
$$= (x-1) \cdot \underbrace{(x^3 + x + 1)}_{(x-y)(x-y^2)(x-y^4)} \cdot \underbrace{(x^3 + x^2 + 1)}_{(x-y^3)(x-y^5)(x-y^6)},$$

Tehát GF(8) felett a konjugált csoportok és a megfelelő minimálpolinomok

$$\{1\} \to x - 1$$
$$\{y, y^2, y^4\} \to x^3 + x + 1$$
$$\{y^3, y^5, y^6\} \to x^3 + x^2 + 1$$

BCH kódok

Egy lineáris ciklikus kód BCH kód GF(q) felett, ha a $g(x)$ generátorpolinomjának $y^1, y^2, \ldots, y^{2t}$ gyökei. A kód t hiba kijavítására képes.

Megjegyzések.

- minden BCH kódra $n = q - 1$.
- k értéke nincs előírva, t-től fog függni.
- $g(x)$-nek lehetnek további gyökei $y^1, y^2, \ldots, y^{2t}$-n kívül.
- $g(x)$ gyökei teljes konjugált csoportokat tartalmaznak; $g(x)$ a megfelelő minimálpolinomok szorzata.

1. feladat

(a) Határozzuk meg a konjugált gyököket GF(4) felett.

(b) Határozzuk meg a megfelelő minimálpolinomot.

(c) Adjuk meg a GF(4) feletti, 1 hibát javító BCH kód generátorpolinomját.

(d) Ábrázoljuk a megfelelő eltolás regiszter architektúrát és jelöljük az együtthatókat.

(GF(4) feletti hatványtábla: $y^0 = 1, y^1 = y, y^2 = y + 1, y^3 = 1$.)

1. feladat

(a) Határozzuk meg a konjugált gyököket GF(4) felett.

(b) Határozzuk meg a megfelelő minimálpolinomot.

(c) Adjuk meg a GF(4) feletti, 1 hibát javító BCH kód generátorpolinomját.

(d) Ábrázoljuk a megfelelő eltolás regiszter architektúrát és jelöljük az együtthatókat.

(GF(4) feletti hatványtábla: $y^0 = 1, y^1 = y, y^2 = y + 1, y^3 = 1$.)

Megoldás.

(a)

$$x^3 - 1 = (x - 1)(x^2 + x + 1) = (x - 1)(x - y)(x - y^2),$$

tehát a konjugált gyökök y, y^2.

1. feladat

(a) Határozzuk meg a konjugált gyököket GF(4) felett.

(b) Határozzuk meg a megfelelő minimálpolinomot.

(c) Adjuk meg a GF(4) feletti, 1 hibát javító BCH kód generátorpolinomját.

(d) Ábrázoljuk a megfelelő eltolás regiszter architektúrát és jelöljük az együtthatókat.

(GF(4) feletti hatványtábla: $y^0 = 1, y^1 = y, y^2 = y + 1, y^3 = 1$.)

Megoldás.

(a)

$$x^3 - 1 = (x - 1)(x^2 + x + 1) = (x - 1)(x - y)(x - y^2),$$

tehát a konjugált gyökök y, y^2.

(b) $\Phi(x) = (x - y)(x - y^2) = x^2 + x + 1$.

1. feladat

(a) Határozzuk meg a konjugált gyököket GF(4) felett.

(b) Határozzuk meg a megfelelő minimálpolinomot.

(c) Adjuk meg a GF(4) feletti, 1 hibát javító BCH kód generátorpolinomját.

(d) Ábrázoljuk a megfelelő eltolás regiszter architektúrát és jelöljük az együtthatókat.

(GF(4) feletti hatványtábla: $y^0 = 1, y^1 = y, y^2 = y + 1, y^3 = 1$.)

Megoldás.

(a)

$$x^3 - 1 = (x - 1)(x^2 + x + 1) = (x - 1)(x - y)(x - y^2),$$

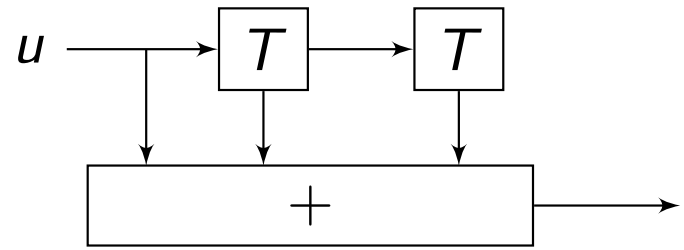
tehát a konjugált gyökök y, y^2.

(b) $\Phi(x) = (x - y)(x - y^2) = x^2 + x + 1$.

(c) y és y^2 muszáj, hogy szerepeljen $g(x)$ gyökei között. Mivel egy konjugált csoporthoz tartoznak, ezért elegendőek is, és $g(x) = (x - y)(x - y^2) = x^2 + x + 1$.

1. feladat

(d)



Megjegyzés: minden szorzás egy galvanikus kapcsolattal van megvalósítva (a minimálpolinomok tulajdonságai miatt). Emiatt GF(2^m) felett nincs szükség bonyolult „rész eltolás architektúrákra” a szorzásokhoz.

2. feladat

Lehet-e a következő polinom egy GF(8) feletti BCH kód generátorpolinomja?

$$g(x) = x^4 + yx^3 + y^3x^2 + yx + 1$$

2. feladat

Lehet-e a következő polinom egy GF(8) feletti BCH kód generátorpolinomja?

$$g(x) = x^4 + yx^3 + y^3x^2 + yx + 1$$

Megoldás. Nem, mivel egy GF(8) feletti BCH kód generátorpolinomjának minden együtthatója GF(2)-beli kell legyen, vagyis minden együttható csak 0 vagy 1 lehet.

3. feladat

Adjuk meg a GF(8) feletti, 1 hibát javító BCH kód generátorpolinomját.

3. feladat

Adjuk meg a GF(8) feletti, 1 hibát javító BCH kód generátorpolinomját.

Megoldás. A GF(8) feletti konjugált csoportok és a megfelelő minimálpolinomok

$$\{1\} \to x - 1$$
$$\{y, y^2, y^4\} \to x^3 + x + 1$$
$$\{y^3, y^5, y^6\} \to x^3 + x^2 + 1$$

Ahhoz, hogy $t = 1$ hibát javítson a kód, $g(x)$ gyökei között kell szerepeljen y és y^2 a teljes konjugált csoportjukkal, így

$$g(x) = x^3 + x + 1.$$

4. feladat

(a) Számítsuk ki a GF(8) feletti, 2 hibát javító BCH kód paramétereit.

(b) Adjuk meg a generátorpolinomot.

(c) Számítsuk ki a csupa 7-es üzenetvektorhoz tartozó kódszót.

4. feladat

(a) Számítsuk ki a GF(8) feletti, 2 hibát javító BCH kód paramétereit.

(b) Adjuk meg a generátorpolinomot.

(c) Számítsuk ki a csupa 7-es üzenetvektorhoz tartozó kódszót.

Megoldás.

(a) $t = 2$ miatt a generátorpolinom gyökei között y, y^2, y^3, y^4 biztosan szerepel. Viszont akkor be kell vennünk a teljes konjugált csoportokat is:

$$\{y, y^2, y^4\} \to x^3 + x + 1$$
$$\{y^3, y^5, y^6\} \to x^3 + x^2 + 1$$

és így

$$g(x) = (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1.$$

4. feladat

(a) $g(x)$ foka $n - k = 6 \rightarrow n = 7, k = 1$, ez egy C(7,1) kód.

($g(x)$-nek egyébként $y^1, \ldots, y^6$ is mind gyöke, így ez a kód igazából 3 hibát is képes javítani, nemcsak 2-t.)

4. feladat

(a) $g(x)$ foka $n-k=6 \;\rightarrow\; n=7, k=1$, ez egy C(7,1) kód.

($g(x)$-nek egyébként $y^1, \ldots, y^6$ is mind gyöke, így ez a kód igazából 3 hibát is képes javítani, nemcsak 2-t.)

(b) $g(x) = (x^3+x+1)(x^3+^2x+1) = x^6+x^5+x^4+x^3+x^2+x+1.$

4. feladat

(a) $g(x)$ foka $n-k=6 \;\rightarrow\; n=7, k=1$, ez egy C(7,1) kód.

($g(x)$-nek egyébként $y^1, \ldots, y^6$ is mind gyöke, így ez a kód igazából 3 hibát is képes javítani, nemcsak 2-t.)

(b) $g(x) = (x^3+x+1)(x^3+^2x+1) = x^6+x^5+x^4+x^3+x^2+x+1.$

Ez a kód az $u(x) = u$ üzenetpolinomhoz a

$$c(x) = u(x)g(x) = u + ux + \cdots + ux^6$$

kódpolinomot rendeli. Az $u \rightarrow c$ kódszó hozzárendelés kiolvasható az együtthatókból:

$$u \quad \rightarrow \quad (u\,u\,u\,u\,u\,u\,u);$$

igazából ez ugyanaz a triviális kód, amit ismerünk korábbról.

4. feladat

(a) $g(x)$ foka $n-k=6 \;\rightarrow\; n=7, k=1$, ez egy C(7,1) kód.

($g(x)$-nek egyébként $y^1, \ldots, y^6$ is mind gyöke, így ez a kód igazából 3 hibát is képes javítani, nemcsak 2-t.)

(b) $g(x) = (x^3+x+1)(x^3+^2x+1) = x^6+x^5+x^4+x^3+x^2+x+1.$

Ez a kód az $u(x) = u$ üzenetpolinomhoz a

$$c(x) = u(x)g(x) = u + ux + \cdots + ux^6$$

kódpolinomot rendeli. Az $u \rightarrow c$ kódszó hozzárendelés kiolvasható az együtthatókból:

$$u \quad \rightarrow \quad (u\,u\,u\,u\,u\,u\,u);$$

igazából ez ugyanaz a triviális kód, amit ismerünk korábbról.

(c) $u = (7) \;\rightarrow\; c = (7\,7\,7\,7\,7\,7\,7)$