Diszkrét matematika 2

13. előadás
Kódelmélet

Mérai László
merai@inf.elte.hu
https://sites.google.com/view/laszlomerai

Komputeralgebra Tanszék

2023 ősz

Lineáris kódok – emlékeztető

- Legyen $\mathcal{C}$ egy lineáris (n, k) kód, azaz $\mathcal{C}$ egy k dimenziós altér $\mathbb{F}_q^n$-ben.
- Ekkor $\mathcal{C}$-nek létezik generátormátrixa és $\mathbf{u} \mapsto G\mathbf{u}$ egy kódolás
- A $\mathcal{C}$ kód ellenőrző mátrixa H, ha $\mathbf{w} \in \mathcal{C} \iff H\mathbf{w} = 0$

Példa

- n-szeres ismétléses kód ellenőrző mátrixa: $H = (\mathbf{I}_{n-1}, -\mathbf{1}) \in \mathbb{F}_q^{(n-1)\times n}$
- A paritásbit ellenőrző mátrixa: $H = \mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_2^{1\times(k+1)}$
- Reed-Solomon kód:
  - kódolandó szavak: $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1}) \in \mathbb{F}_q^k$
  - $\mathbf{u} \leftrightarrow u(x) = u_0 + u_1 x + \cdots + u_{k-1}x^{k-1} \in \mathbb{F}_q[x]$, $\deg u(x) < k$
  - kódolás: $u(x) \mapsto (u(\alpha_0), \ldots, u(\alpha_{k-1}))$, $\alpha_0, \ldots, \alpha_{k-1} \in \mathbb{F}_q$ különböző elemek
  - Reed-Solomon kódok MDS kódok: $d = n - k + 1$.

Ciklikus kódok

A ciklikus kódok egy másik népszerű kódcsalád.

Definíció

Egy $\mathbf{c} = (c_0, \ldots, c_{n-1})$ szó ciklikus eltoltja az $S\mathbf{c} = (c_{n-1}, c_0, \ldots, c_{n-2})$. Egy $\mathcal{C}$ kód ciklikus kód, ha minden $\mathbf{c} \in \mathcal{C}$ kódszóra, $S\mathbf{c} \in \mathcal{C}$.

Példa

- A $\mathcal{C} = \{101, 110, 011, 111\} \subset \mathbb{F}_2^3$ kód ciklikus (de nem lineáris).
- Az ismétléses kód ciklikus. $b \mapsto (bbb)$. A kódszavak $\{000, 111\}$.
- A paritásbit kód ciklikus. $(c_1, c_2, c_3) \mapsto (c_1, c_2, c_3, c_1 + c_2 + c_3)$. Kódszavak:

0000 0011 0101 0110
1001 1010 1100 1111

Ciklikus kódok

A ciklikus kódok egy másik népszerű kódcsalád.

Definíció

Egy $\mathbf{c} = (c_0, \ldots, c_{n-1})$ szó ciklikus eltoltja az $S\mathbf{c} = (c_{n-1}, c_0, \ldots, c_{n-2})$. Egy $\mathcal{C}$ kód ciklikus kód, ha minden $\mathbf{c} \in \mathcal{C}$ kódszóra, $S\mathbf{c} \in \mathcal{C}$.

Példa

- A $\mathcal{C} = \{101, 110, 011, 111\} \subset \mathbb{F}_2^3$ kód ciklikus (de nem lineáris).
- Az ismétléses kód ciklikus.
- A paritásbit kód ciklikus.

Tétel

Legyen $\mathcal{C}$ egy ciklikus kód és $\mathbf{c} = (c_0, \ldots, c_{n-1}) \leftrightarrow c(x) = c_0 + \cdots + c_{n-1}x^{n-1}$. Ekkor a $\mathbf{c}$ kódszó $S\mathbf{c}$ eltoltjához rendelt $\hat{c}(x)$ polinom: $\hat{c}(x) \equiv xc(x) \mod x^n - 1$.

Bizonyítás. $xc(x) = c_{n-1}(x^n - 1) + \hat{c}(x)$. □

Ciklikus kódok, generátorpolinom

Tétel

Legyen $\mathcal{C} \subset \mathbb{F}_q[x]$ egy (n, k) paraméterű lineáris, ciklikus kód. Ekkor egyértelműen létezik olyan $g(x) \in \mathcal{C}$ polinom, melynek főegyütthatója 1, $\deg g(x) = n - k$ és

$$c(x) \in \mathcal{C} \quad \Leftrightarrow \quad g(x) \mid c(x),$$

azaz minden $c(x) \in \mathcal{C}$ kódpolinomhoz létezik olyan $u(x) \in \mathbb{F}_q[x]$, melyre $c(x) = u(x)g(x)$.

Bizonyítás 1/3. (g konstrukciója)

- Legyen $q(x) = c_0 + c_1 x + \cdots + c_s x^s \in \mathcal{C} \setminus \{0\}$ egy legkisebb fokú kódpolinom.
- Mivel $\mathcal{C}$ lineáris, így $c_s^{-1} q(x) = g(x)$ szintén kódszó: $g(x) \in \mathcal{C}$.
- Egyértelműség: ha $\tilde{g}(x) \in \mathcal{C}$ szintén ilyen polinom, akkor a linearitás miatt $g(x) - \tilde{g}(x) \in \mathcal{C}$. De $\deg(g(x) - \tilde{g}(x)) < s$, így a minimalitás miatt $g(x) = \hat{g}(x)$.

($s = \deg g(x) = n - k$ bizonyítása a 3/3 részben!)

Ciklikus kódok, generátorpolinom

Tétel

Legyen $\mathcal{C} \subset \mathbb{F}_q[x]$ egy (n, k) paraméterű lineáris, ciklikus kód. Ekkor egyértelműen létezik olyan $g(x) \in \mathcal{C}$ polinom, melynek főegyütthatója 1, $\deg g(x) = n - k$ és

$$c(x) \in \mathcal{C} \quad \Leftrightarrow \quad g(x) \mid c(x),$$

azaz minden $c(x) \in \mathcal{C}$ kódpolinomhoz létezik olyan $u(x) \in \mathbb{F}_q[x]$, melyre $c(x) = u(x)g(x)$.

Bizonyítás 2/3. ($\Leftrightarrow$ bizonyítása) Legyen $s = \deg g(x)$.

- $\Leftarrow$: A ciklikusság miatt $g(x), xg(x), x^2g(x), \ldots, x^{n-s-1}g(x) \in \mathcal{C}$, és a linearitás miatt $u(x)g(x) = u_0g(x) + u_1xg(x) + u_2x^2g(x) + \cdots + u_{n-s-1}x^{n-s-1}g(x) \in \mathcal{C}$.

- $\Rightarrow$: Legyen $c(x) \in \mathcal{C}$. Osszuk el maradékosan $c(x)$-et, $g(x)$-szel: $c(x) = q(x)g(x) + r(x)$, $\deg r(x) < s$. A "$\Leftarrow$" miatt $q(x)g(x) \in \mathcal{C}$, a linearitás miatt $r(x) = c(x) - q(x)g(x) \in \mathcal{C}$. A $s = \deg g(x)$ minimalitása miatt $r(x) = 0$, azaz $c(x) = q(x)g(x)$.

Ciklikus kódok, generátorpolinom

Tétel

Legyen $\mathcal{C} \subset \mathbb{F}_q[x]$ egy (n,k) paraméterű lineáris, ciklikus kód. Ekkor egyértelműen létezik olyan $g(x) \in \mathcal{C}$ polinom, melynek főegyütthatója 1, $\deg g(x) = n-k$ és

$$c(x) \in \mathcal{C} \quad \Leftrightarrow \quad g(x) \mid c(x),$$

azaz minden $c(x) \in \mathcal{C}$ kódpolinomhoz létezik olyan $u(x) \in \mathbb{F}_q[x]$, melyre $c(x) = u(x)g(x)$.

Bizonyítás 3/3. ($\deg g(x) = n-k$ bizonyítása)

- Minden $c(x) \in \mathcal{C}$ kódpolinom előáll $c(x) = u(x)g(x) = u_0 g(x) + u_1 x g(x) + u_2 x^2 g(x) + \cdots + u_{n-s-1} x^{n-s-1} g(x)$ alakban.
- Ilyen $c(x)$ (ill. $u(x)$) polinomból q^{n-s} darab van.
- A $\mathcal{C}$ kód (n,k) lineáris kód, azaz $\dim \mathcal{C} = k \Rightarrow q^k = \#\mathcal{C} = q^{n-s} \Rightarrow \deg g(x) = s = n-k$. □

A $g(x)$ polinomot a kód generátorpolinomjának nevezzük.

Ciklikus kódok konstrukciója

Tétel

Minden $\mathcal{C}$ ciklikus, lineáris kód $g(x)$ generátorpolinomjára $g(x) \mid x^n - 1$.
Megfordítva, ha $g(x) \mid x^n - 1$, akkor létezik olyan ciklikus, lineáris kód, melynek generátorpolinomja $g(x)$.

Bizonyítás. Legyen $\deg g = n - k$.
$\Rightarrow$:Mivel a kód ciklikus, $x^{k-1}g(x) \in \mathcal{C}$, $\deg x^{k-1}g(x) = n - 1$. Mivel $g(x)$ főegyüttható 1, $x^k g(x) - (x^n - 1) \in \mathcal{C}$. Azaz $x^k g(x) - (x^n - 1) = a(x)g(x)$, így a kettő különbsége ($= x^n - 1$) osztható $g(x)$-szel.
$\Leftarrow$: Legyen $\mathcal{C} = \{c(x) = a(x)g(x) : \deg a(x) < k\}$. Megmutatjuk, hogy ez ciklikus, azaz $a(x)$, $\deg a(x) < k$ polinomhoz létezik $b(x)$, $\deg b(x) < k$ polinom, hogy $xc(x) = xa(x)g(x) \equiv b(x)g(x) \mod x^n - 1$.
Ehhez, ha $\deg a(x) < k - 1$, legyen $b(x) = xa(x)$. Ha $\deg a(x) = k - 1$, legyen a_{k-1} az $a(x)$ főegyüttható.Ekkor $xc(x) = xa(x)g(x) = a_{k-1}(x^n - 1) + r(x)$, ahol $\deg r(x) < n$. Mivel $g(x)$ osztja a bal oldalt, ill. $x^n - 1$-et, osztja $r(x)$-et: $r(x) = b(x)g(x)$. □

Ciklikus kódok generálása

A ciklikus kódok előnye, hogy sokféleképpen lehet a kódszavakat generálni:

- Generálás generátorpolinommal: $u(x) \mapsto u(x)g(x) \bmod x^n - 1$.
- Generálás generátormátrixszal: legyen $g(x) = x^{n-k} + g_{n-k-1}x^{n-k-1} + \cdots + g_0$. Ekkor a $G \in \mathbb{F}_q^{n \times k}$ a kód generátormátrixa:

$$G = \begin{pmatrix} g_0 & 0 & \dots & 0 & 0 \\ g_1 & g_0 & \dots & 0 & 0 \\ g_2 & g_1 & \dots & 0 & 0 \\ \vdots & & \dots & \vdots & \vdots \\ g_{n-k-1} & g_{n-k-2} & \cdots & g_1 & g_0 \\ 1 & g_{n-k-1} & \cdots & g_2 & g_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \dots & 1 & g_{n-k-1} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Ciklikus kódok generálása

A ciklikus kódok előnye, hogy sokféleképpen lehet a kódszavakat generálni:

- Generálás generátorpolinommal: $u(x) \mapsto u(x)g(x) \bmod x^n - 1$.
- Generálás generátormátrixszal.

A szisztematikus kódolás egy praktikus módja:

- Legyen $u(x) \in \mathbb{F}_q[x]$, $\deg u(x) < k$ egy üzenetpolinom.
- Ekkor $c(x) = u(x)x^{n-k} - (u(x)x^{n-k} \bmod g(x))$ egy kódszó.
- Továbbá, ez szisztematikus kódolás: $\geq n - k$ fokú tagok adják az $u(x)$ polinomot.

Ciklikus kód ellenőrzőmátrixa

Ciklikus kód ellenőrzőmátrixa is leírható polinomokkal.

Tétel

Legyen $\mathcal{C}$ egy (n, k) paraméterű lineáris, ciklikus kód $g(x) \in \mathbb{F}_q[x]$ generátorpolinommal. Ekkor a $h(x) = \dfrac{x^n - 1}{g(x)}$ a kód ellenőrzőpolinomja, azaz

$$c(x) \in \mathcal{C} \iff c(x)h(x) \equiv 0 \mod x^n - 1.$$

Bizonyítás. Mivel $g(x) \mid x^n - 1$, ezért a definíció értelmes.

Legyen $c(x)$ egy szó. Ekkor $c(x) \in \mathcal{C} \iff c(x) = a(x)g(x) \iff$
$c(x)h(x) = a(x)g(x)h(x) = a(x)(x^n - 1) \equiv 0 \mod x^n - 1.$ □

Példa ciklikus kódokra

Legyen $q = 2$ és $n = 7$. Ekkor $g(x) \mid x^7 - 1$.

Az $x^7 - 1$ irreducibilis faktorizációja: $x^7 - 1 = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

Ekkor $g(x)$ generátorpolinomra a következő lehetőségeink vannak:

- $g(x) = x - 1$.Ekkor $\mathcal{C}$ egy $(7, 6)$ kód: $h = x^6 + x^5 + \cdots + x + 1 \rightarrow$ paritásbit kód.
- $g(x) = x^6 + x^5 + \cdots + x + 1$. Ekkor $\mathcal{C}$ egy $(7, 1)$ kód: $h = x - 1 \rightarrow$ 7-szeres ismétléses kód.
- $g(x) = x^3 + x + 1$. Ekkor $\mathcal{C}$ egy $(7, 4)$ kód.

Ciklikus kódok alkalmazása

- A ciklikus kódok a leghosszabb múlttal rendelkező kódok.
- Gyakran CRC (Cyclic Redundancy Check) kódoknak hívják.
- Felhasználásuk: visszacsatolással rendelkező zajos csatornán. Hiba észlelése esetén újraküldés: ARQ (Automatic Repeat reQuest).
- CITT: bináris ciklikus kód $g(x) = x^{16} + x^{12} + x^5 + 1$ generátorpolinommal. Használatuk integrált áramkörökben: SNC 2653, INTEL 82586, INTEL 8274, Signetics 2652