Ciklične kode

Gre za enega najbolj pomembnih razredov linearnih kod. V splošnem je te kode veliko lažje implementirati, zato imajo izjemen praktičen pomen. Iz algebraičnega vidika pa so prav tako izredno zanimive.

Podprostor S n-razsežnega vektorskega prostora je **cikličen podprostor**, če iz

$$(a_1, a_2, \ldots, a_{n-1}, a_n) \in S \quad \text{sledi} \quad (a_n, a_1, a_2, \ldots, a_n) \in S.$$

Linearna koda C je **ciklična koda**, če je C cikličen podprostor.

Kodni besedi c, podobno kot prej pri sporočilu, priredimo polinom

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

Cikličnemu pomiku potem ustreza polinom $c'(x)$, tj.,

$$c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} = x \cdot c(x) - c_{n-1}(x^n - 1).$$

V kolobarju polinomov $R_n = \mathbb{F}^n[x]/(x^n - 1)$, kjer gledamo polinome po modulu polinoma $x^n - 1$, dobimo ciklični pomik kar z množenjem s polinomom x.

Zato bomo pogosto enačili kodne besede s polinomi po modulu polinoma $x^n - 1$, tj. delali v kolobarju R_n.

Kolobarji in ideali

Bertrand Russell:
"*Matematiko lahko definiramo kot predmet, pri katerem nikoli ne vemo, o čem govorimo niti nikoli ne vemo, ali je tisto, kar pravimo, resnično.*"

Če v neki množici G z binarno operacijo $\circ$, velja:

(G1) $\forall a, b \in G$ je $a \circ b \in G$,
(G2) $\exists e \in G$, tako da za $\forall g \in G$ velja $e \circ g = g \circ e = g$,
(G3) $\forall g \in G \;\; \exists f \in G$, tako da velja $g \circ f = f \circ g = e$,
(G4) $\forall a, b, c \in G$ velja $(a \circ b) \circ c = a \circ (b \circ c)$,

potem pravimo, da je par $(G, \circ)$ **grupa**.

Če za neko množico $\mathcal{K}$ z binarnima operacijam
bomo označili s $+$ in $*$, velja

(K1) par $(\mathcal{K}, +)$ je grupa z enoto 0,
(K2) $\forall a, b, c \in \mathcal{K}$ velja $(a * b) * c = a * (b * c)$
(K3) $\forall a, b \in \mathcal{K}$ velja $a * b = b * a$,
(K4) $\forall a, b, c \in \mathcal{K}$ velja $a * (b + c) = a * b + b$
(K5) $\exists 1 \in \mathcal{K}$, tako da za $\forall a \in \mathcal{K}$ velja $e * g =$

potem imenujemo trojico $(\mathcal{K}, +, *)$ **komut kolobar z enoto**.

Ker bomo imeli opravka samo s komuta kolobarji z enoto, jim bomo rekli kar kolobarji

Primeri:

Množica vseh celih števil z običajnim seštevanjem in množenjem $(\mathbb{Z}, +, *)$, ponavadi označena kar z $\mathbb{Z}$.

Množica celih števil po modulu $n \in \mathbb{N}$, ponavadi označena kar z $\mathbb{Z}_n$.

Množica vseh polinomov (spremenljivke x) s koeficienti iz obsega $\mathbb{F}$, in običajnim seštevanjem in množenjem polinomov, običajna oznaka $\mathbb{F}[x]$.

Za neničelen polinom $f(x) \in \mathbb{F}[x]$ lahko definiramo še kolobar polinomov nad $\mathbb{F}$ po modulu $f(x)$, oznaka $\mathbb{F}[x]/(f(x))$.

Neprazna podmnožica $\mathcal{I}$ kolobarja $(\mathcal{K}, +, *)$ se imenuje ideal kolobarja, če velja

(I1) par $(\mathcal{I}, +)$ je grupa,
(I2) $i * k \in \mathcal{I}$ za $\forall i \in \mathcal{I}$ in za $\forall k \in \mathcal{K}$.

Opišimo preprosto konstrukcijo ideala. Za neničelen element $g \in \mathcal{K}$ vzamemo naslednjo množico

$$\mathcal{I} = \{g * k \mid k \in \mathcal{K}\}.$$

Ni se težko prepričati, da gre za ideal. Pravimo mu ideal generiran z g. Vsakega ideala ne moremo dobiti na ta način, če pa je možno, mu pravimo glavni ideal.

Kolobar v katerem je vsak ideal glavni ideal
(tj. je generiran z enim samim elementom)
imenujemo glavni kolobar.

Izrek: *$\mathbb{F}[x]$ in $\mathbb{F}[x]/(f(x))$ sta glavna kolobarja.*

Izrek: *Neprazna množica S n-razsežnega vektorskega prostora V je cikličen podprostor če in samo če je množica polinomov $\mathcal{I}$, ki ustreza množici S, ideal v kolobarju, ki ustreza prostoru V.*

Izrek: *Naj bo $\mathcal{I} \neq \emptyset$ ideal v $V = \mathbb{F}^n$ in $g(x)$ moničen polinom najmanjše stopnje, ki predstavlja nek razred iz $\mathcal{I}$.*

Potem $[g(x)]$ (ali kar $g(x)$) generira ideal $\mathcal{I}$ in $g(x)$ deli $x^n - 1$.

Izrek: *Obstaja natanko določen moničen p najmanjše stopnje, ki generira ideal $\mathcal{I} \neq \emptyset$ n-razsežnega vektorskega prostora V.*

Izrek: *Naj bo $h(x)$ moničen delitelj polinoma $x^n - 1$. Potem je $h(x)$ generator ideala*

$$\mathcal{I} = \{a(x)h(x) \mid a(x) \in \mathcal{K}\}$$

kolobarja $\mathcal{K} = \mathbb{F}[x]/(x^n - 1)$.

Izrek: *Obstaja bijektivna korespondenca med cikličnimi podprostori vektorskega prostora $\mathbb{F}^n$*
in
moničnimi polinomi $g(x) \in \mathbb{F}[x]$,
ki delijo binom $x^n - 1$.

Izrek 5: *Naj bosta $n, k \in \mathbb{N}$, $n > k$,*
$g(x)$ moničen polinom stopnje $n - k$,
ki deli polinom $x^n - 1$. Potem je

$$S = \{a(x)g(x) \mid \deg(a) < k\}$$

cikličen podprostor vektorskega prostora R_n
in $B = \{g(x), x\,g(x), \dots, x^{k-1}g(x)\}$
baza podprostora S.

Dokaz: Očitno je S podprostor v R_n. Pokažimo, da je S cikličen, tj. za polinom $p(x) := a(x)g(x) \in S$ je

$$p_1(x) := x\,p(x) \mod (x^n - 1) \quad \text{v podprostoru } S.$$

To je očitno, saj je razlika $p_1(x) - x\,p(x)$ deljiva z $x^n - 1$, ki je deljiv z $g(x)$, polinom $p(x)$ pa je tudi deljiv z $g(x)$. Zato je z $g(x)$ deljiv tudi polinom $p_1(x)$.

Prepričajmo se, da je množica B baza podprostora S. Predpostavimo, da je poljubna linearna kombinacija

$$\sum_{i=0}^{k-1} \lambda_i x^i g(x) = 0.$$

Če obstaja največji indeks j, za katerega je $\lambda_j \neq 0$, potem je koeficient ob x^{n-k+j} enak λ_j, kar pomeni, da mora biti $\lambda_j = 0$. Torej je B linearno neodvisna.

Vektorji iz B napenjajo cel podprostor S, saj za poljuben $p(x) \in S$, velja $p(x) = a(x)g(x)$ za nek $a(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$, tj.

$$p(x) = a_0 g(x) + a_1 x g(x) + \dots + a_{k-1}x^{k-1}g(x)$$

je res linearna kombinacija polinomov iz B. ■

Izrek 6: *Naj bo $\mathbb{F}$ končen obseg s q eleme*
in $n := q - 1$. Naj bo k tako število, da ve
$1 \leq k < n$ in $d := n - k + 1$ ter α primitive
element v $\mathbb{F}$.

Koda C_1 naj bo linearna ciklična
generatorskim polinomom

$$g(x) = (x - \alpha)(x - \alpha^2)\dots(x - \alpha^{d-1}$$

koda C_2 pa naj bo RS-koda, pri kateri
$m \in \mathbb{F}^k$ s prirejenim polinomom

$$m(x) = m_0 + m_1x + \dots + m_{k-1}x^{k-}$$

priredimo kodno besedo

$$(m(\alpha), m(\alpha^2), \dots, m(\alpha^n)).$$

Potem kodi C_1 in C_2 sestavljajo iste kodne

Opozorimo, da zgornji izrek ne trdi, da istemu sporočilu v obeh primerih priredimo isto kodno besedo in da izrek velja tudi, če pogoj $n = q - 1$ zamenjamo s $q - 1 \mid n$.

Dokaz: Ker sta kodi C_1 in C_2 linearni in k-razsežni, je dovolj preveriti, da je beseda $c = (c_0, c_1, \dots, c_{n-1})$, katere prirejeni polinom

$$c(x) = c_0 + c_1x + \dots + c_{k-1}x^{k-1}$$

je oblike $c(x) = m(x)g(x)$
(tj. beseda iz kode C_1, ki pripada sporočilu m),
tudi v kodi C_2, tj. $C_1 \subseteq C_2$.

Torej je treba poiskati tak polinom $f(x)$ stopnje $k-1$, da bo $c_i = f(\alpha^i)$ za $i \in \{0, \dots, n-1\}$.

Naj bo $f(x) = f_0 + f_1x + \dots + f_{n-1}x^{n-1}$, tako da velja

$$f_j = \frac{c(\alpha^{-j})}{n}, \quad j = 0, \dots, n-1. \tag{1}$$

Polinom $c(x)$ je deljiv s polinomom $g(x)$,
zato so $\alpha, \alpha^2, \dots, \alpha^{d-1}$ tudi njegove ničle.

Ker je $d - 1 = n - k$, to pomeni, da za
$j \in \{n-1, n-2, \dots, k\}$ velja $c(\alpha^{-j}) = c(\alpha^{n-j}) = 0$
in zato tudi $f_j = 0$.

Torej ima polinom $f(x)$ stopnjo največ $k - 1$.

Izračunajmo še vrednosti $f(\alpha^i)$, $i \in \{0, \dots, n-1\}$.

Iz (1) sledi

$$\begin{aligned} f(\alpha^i) &= \sum_{j=0}^{n-1} \frac{c(\alpha^{-j})}{n} \cdot (\alpha^i)^j = \frac{1}{n}\sum_{j=0}^{n-1}\Big(\sum_{h=0}^{n-1} c_h \alpha^{-jh}\Big)\alpha^{ij} \\ &= \frac{1}{n}\sum_{h=0}^{n-1} c_h \cdot \Big(\sum_{j=0}^{n-1} \alpha^{(i-h)j}\Big) = c_i. \end{aligned}$$

Pri zadnjem enačaju smo upoštevali, da je izraz v zadnjem oklepaju enak n za $h = i$, sicer pa 0.

To vidimo takole: α je primitiven element, zato je $\alpha^n = 1$ in $\alpha \neq 1$, se pravi, da je α ničla polinoma $(x^n - 1)/(x - 1) = 1 + x + x^2 + \dots + x^{n-1}$;

enako velja tudi za vse potence α, ki so različne od 1.
■

Pravkar opisana transformacija, ki preslik
v $f(x)$, je znana kot **(inverzna) Four**
transformacija v končnih obsegih in je d
analog Fourierove transformacije v analizi.

Naj bo $\mathbb{F}$ končen obseg s q elementi in $n := q$
Naj bo k tako število, da velja $1 \leq k$
$d := n - k + 1$.
Naj bo α primitiven element v $\mathbb{F}$ in

$$g(x) = (x - \alpha)(x - \alpha^2)\dots(x - \alpha^{d-1})$$

Obravnavamo odkodiranje pri RS(n, k)-kodi,
generirani s polinomom $g(x)$.

Naj bo $c(x) = a(x)g(x)$ poslana kodna beseda, $r(x)$ pa prejeta beseda. Lahko jo zapišemo v obliki

$$r(x) = c(x) + e(x), \tag{2}$$

kjer je $e(x)$ **polinom napake**.

Če pri prenosu ni prišlo do napake, je $e(x)$ enak nič in je polinom $r(x)$ deljiv z $g(x)$.

Polinom sporočila $a(x)$ dobimo iz $r(x)$ kar z deljenjem s polinomom $g(x)$.

V primeru, da je prišlo do napake, pa bo odkodiranje težje. Najprej bomo odkodiranje prevedli na reševanje sistema linearnih enačb.

Vemo, da obstajata taka polinoma $h(x)$ in $s(x)$, da je

$$\begin{aligned} r(x) &= h(x) \cdot g(x) + s(x), \\ &\quad \text{in } \deg(s(x)) < \deg(g(x)). \end{aligned}$$

$s(x)$ imenujemo **sindrom** prejete besede $r(x)$.
Ker so α, $\alpha^2, \dots, \alpha^{d-1}$ ničle polinoma $g(x)$ in zato tudi polinoma $c(x)$, velja zaradi (2) in zgornje enačbe naslednja zveza:

$$r(\alpha^i) = e(\alpha^i) = s(\alpha^i) \quad \text{za } i = 1, \dots, d-1. \tag{3}$$

Predpostavimo, da pri prenosu ni prišlo do več kot $\ell \leq \lfloor (d-1)/2 \rfloor$ napak, kolikor jih koda največ lahko odpravi.

Naj bodo $a_0, a_1, \dots, a_{\ell-1} \in \{0, \dots, n-1\}$ mesta v kodni besedi, na katerih je prišlo do napake.

Potem lahko polinom $e(x)$ zapišemo v obliki

$$e(x) = \sum_{j=0}^{\ell-1} \lambda_j x^{a_j}.$$

$S_i := s(\alpha^i)$. Eksponenti a_j v potenci α^{a_j} nam povedo položaje napak, zato števila α^{a_j} imenujemo **lokatorji napak**. Vrednosti λ_j pa so **velikosti napak**.

Iz (3) dobimo za $i = \{1, \dots, d-1\}$ sistem enačb

$$S_i = \sum_{j=0}^{\ell-1} \lambda_j (\alpha^i)^{a_j} = \sum_{j=0}^{\ell-1} \lambda_j (\alpha^{a_j})^i, \tag{4}$$

z neznankami λ_j in α^{a_j}, $j = 0, \dots, \ell - 1$.

Z uvedbo oznak $X_j = \alpha^{a_j}$, $j = 0, \dots, \ell - 1$
zapišemo v naslednji obliki

$$\begin{array}{lclclclcl} S_1 &=& \lambda_0 X_0 &+& \lambda_1 X_1 &+& \cdots &+& \lambda_{\ell-} \\ S_2 &=& \lambda_0 X_0^2 &+& \lambda_1 X_1^2 &+& \cdots &+& \lambda_{\ell-} \\ & \vdots & & & & & & & \\ S_{d-1} &=& \lambda_0 X_0^{d-1} &+& \lambda_1 X_1^{d-1} &+& \cdots &+& \lambda_{\ell-} \end{array}$$

Ta sistem $d-1$ enačb z 2ℓ neznankami (λ_j in
v preteklosti pojavil pri reševanju različnih pro

L. 1975 baron de Prony rešuje interpolacijski p

Najprej poiščemo vrednosti X_j, nato pa l
sistema poiščemo še velikosti napak, saj je sistem
za λ_i, $i = 0, \dots, \ell - 1$, linearen.

Naj bo

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 + \cdots + \sigma_\ell x^\ell$$

polinom lokatorjev napake oziroma bolj precizno polinom, ki ima za ničle ravno inverzne vrednosti lokatorjev napak, tj. $\prod_{i=0}^{\ell-1}(1 - X_j x)$. Zato velja:

$$\lambda_j X_j^{\ell+u} \sigma(X_j^{-1}) = 0 \quad \text{za } j = 0, \dots, \ell - 1, \tag{6}$$

kjer je u naravno število manjše ali enako ℓ. Seštejmo enačbe (6), upoštevajmo še sistem in dobimo

$$0 = \sum_{j=0}^{\ell-1} \lambda_j X_j^{\ell+u} \Big(1 + \sum_{i=1}^{\ell} \sigma_i X_j^{-i} \Big)$$

$$= S_{u+\ell} + \sum_{i=1}^{\ell} \sigma_i \sum_{j=0}^{\ell-1} \lambda_j X_j^{\ell+u-i} = S_{u+\ell} + \sum_{i=1}^{\ell} \sigma_i S_{\ell+u-i},$$

To je rekurzivna enačba za zaporedje $\{S_i\}$:

$$\sigma_1 S_{u+\ell-1} + \sigma_2 S_{u+\ell-2} + \cdots + \sigma_\ell S_u = -S_{u+\ell}. \tag{7}$$

Ko u teče od $1, \dots, \ell$, dobimo sistem linearnih enačb za σ_i, $i = 1, \dots \ell$, ki ga lahko zapišemo v matrični obliki

$$\begin{bmatrix} S_1 & S_2 & \dots & S_\ell \\ S_2 & S_3 & \dots & S_{\ell+1} \\ \vdots & \vdots & & \vdots \\ S_\ell & S_{\ell+1} & \dots & S_{2\ell-1} \end{bmatrix} \begin{bmatrix} \sigma_\ell \\ \sigma_{\ell-1} \\ \vdots \\ \sigma_1 \end{bmatrix} = - \begin{bmatrix} S_{\ell+1} \\ S_{\ell+2} \\ \vdots \\ S_{2\ell} \end{bmatrix}. \tag{8}$$

Vnaprej ne poznamo ℓ, zato namesto z ℓ računamo z $\lfloor (d-1)/2 \rfloor$.

Rang matrike sistema je v tem primeru enak številu napak. Ko poznamo število napak, lahko iz sistema izračunamo koeficiente polinoma $\sigma(x)$.

Da dobimo lokatorje napak, moramo poiskati ničle $\sigma(x)$ in njihove inverze. Ker smo v končnem obsegu, ničle lahko poiščemo tudi tako, da kar po vrsti preizkušamo elemente obsega (v praksi namreč obseg nima več kot 32 elementov).

Algoritem za odkodiranje Reed-Solomonovih kod, ki smo ga predstavili zgoraj, je bistveno hitrejši od tistega iz drugega razdelka, saj je polinomski.

Rešimo le dva sistema enačb (8) in (5) velikosti $O(d \times d)$, iščemo inverze ℓ elementov, ki so lahko shranjeni tudi v tabeli, ter vrednosti polinoma $\sigma(x)$ v največ n točkah. Skupna zahtevnost algoritma je v najslabšem primeru enaka $O(n^3)$.

Primer: RS$(15, 9)$-koda nad obsegom GF$(2^4$
Za primitivni element obsega izberemo
polinoma $f(x) = x^4 + x + 1$.

Razdalja kode je enaka $d = 15 - 9 + 1 = 7$
(koda popravi do tri napake).

Stopnja generatorskega polinoma $g(x)$ je n
$15 - 9 = 6$. Z uporabo ZechLog tabele izraču

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)(x - \alpha^5$$
$$= \alpha^6 + \alpha^9 x + \alpha^6 x^2 + \alpha^4 x^3 + \alpha^{14} x^4 + \alpha^{10} x^5$$

Kodiranje je množenje s polinomom $g(x)$. Besedo $m = (0, 0, 1, 0, \alpha^{10}, 0, \alpha^2, 0, 0)$ zakodiramo torej kot

$$\begin{aligned} c(x) &= m(x) \cdot g(x) = \alpha^6 x^2 + \alpha^9 x^3 + \alpha^{11} x^4 + \alpha^{11} x^6 \\ &\quad + \alpha^{11} x^8 + \alpha^9 x^9 + \alpha^8 x^{10} + \alpha^{12} x^{11} + \alpha^2 x^{12} \end{aligned}$$

oziroma

$$c = (0, 0, \alpha^6, \alpha^9, \alpha^{11}, 0, \alpha^{11}, 0, \alpha^{11}, \alpha^9, \alpha^8, \alpha^{12}, \alpha^2, 0, 0).$$

Poglejmo sedaj še, kako poteka odkodiranje.
Če je prirejeni polinom $c(x)$ kodne besede c deljiv s polinomom $g(x)$, potem je polinom sporočila $m(x)$ enak $c(x)/g(x)$.

Poskusimo odkodirati še prejeto besedo r s prirejenim polinomom $r(x) = \alpha^6 x^2 + \alpha^9 x^3 + x^4 + x^5 + x^6 + \alpha^{10} x^7 + \alpha^3 x^8 + \alpha^3 x^9 + \alpha^2 x^{12}$. Polinom $r(x)$ ni deljiv z $g(x)$, saj je ostanek enak

$$s(x) = \alpha^5 + \alpha^{10} x + \alpha x^2 + \alpha^{10} x^3 + \alpha^3 x^4 + \alpha^9 x^5.$$

Izračunamo $S_i = s(\alpha^i)$ za $i = 1, \ldots, 6$ in dobimo naslednje vrednosti

S_1	S_2	S_3	S_4	S_5	S_6
α^{12}	0	α^3	α^2	α^3	1

Sestavimo matriko iz sistema (8).

$$\begin{bmatrix} \alpha^{12} & 0 & \alpha^3 \\ 0 & \alpha^3 & \alpha^2 \\ \alpha^3 & \alpha^2 & \alpha^3 \end{bmatrix} \tag{9}$$

Matriko (9) enostavno prevedemo na zgornje-trikotno obliko. Od tretje vrstice odštejemo prvo, pomnoženo z α^6, in nato še drugo, pomnoženo z α^{14} (ker ima obseg karakteristiko 2, je odštevanje kar enako seštevanju).

Dobimo matriko ranga 2, kar pomeni, da je pri prenosu kodne besede najverjetneje prišlo do dveh napak. Zato je treba rešiti sistem dveh enačb z dvema neznankama

$$\begin{bmatrix} \alpha^{12} & 0 \\ 0 & \alpha^3 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = - \begin{bmatrix} \alpha^3 \\ \alpha^2 \end{bmatrix}, \tag{10}$$

ki nam da rešitev $\sigma_1 = \alpha^{14}$ in $\sigma_2 = \alpha^6$.

Sedaj poznamo polinom $\sigma(x) = 1 + \alpha^{14} x$
Z računanjem njegovih vrednosti v vseh el
obsega GF(2^4) preverimo, da sta njegovi nič
α^5.

Njuna inverza α^{11} in α^{10} nam povesta, da sta
pri prejeti besedi na 10. in 11. mestu.

Preostane nam le še, da izračunamo velik
napak. V našem primeru bo to najenostavn
z reševanjem sistema (5).

Le-ta je predoločen; če nima rešitve,
predpostavka, da je prišlo do največ treh
napačna.

Velikosti napak izračunamo iz prvih dveh enačb

$$\begin{aligned} \alpha^{12} &= \lambda_0 \alpha^{11} + \lambda_1 \alpha^{10} \\ 0 &= \lambda_0 (\alpha^{11})^2 + \lambda_1 (\alpha^{10})^2 \end{aligned} \tag{11}$$

in z deljenjem s polinomom $g(x)$ preverimo, da smo res dobili kodno besedo.

Velikosti napak sta $\lambda_0 = \alpha^{12}$ in $\lambda_1 = \alpha^{14}$.

Polinom poslane kodne besede je potem

$$\begin{aligned} c_1(x) &= \alpha^6 x^2 + \alpha^9 x^3 + x^4 + x^5 + x^6 + \alpha^{10} x^7 \\ &\quad + \alpha^3 x^8 + \alpha^3 x^9 + \alpha^{14} x^{10} + \alpha^{12} x^{11} + \alpha^2 x^{12}. \end{aligned}$$

Ker velja $c_1(x) = g(x) \cdot (x^2 + \alpha^7 x^4 + \alpha^2 x^6)$, je polinom sporočila enak $x^2 + \alpha^7 x^4 + \alpha^2 x^6$, samo sporočilo pa je enako $(0, 0, 1, 0, \alpha^7, 0, \alpha^2, 0, 0)$.