C Cyklické kódy

Ať C je $[n,k]_q$ kód takový, že pro každé $(u_1,\ldots,u_n)\in C$ je také $(u_2,\ldots,u_n,u_1)\in C$. Jinými slovy, kódová slova jsou uzavřena na cyklické posuny. Je přirozené takový kód nazvat **cyklický**.

Strukturu cyklických kódu lze osvětlit, pokud kódová slova budeme chápat jako polynomy. Pro komutativní těleso F ať $F[x]_n$ značí množinu všech $a\in F[x]$ stupně menšího než n. Pro $a=\sum a_i x^i\in F[x]$ definujeme $b=\pi_n(a)\in F[x]_n$, $b=b_0+b_1x+\ldots+b_{n-1}x^{n-1}$ tak, že $b_j=\sum_{r\geq 0}a_{j+rn}$. Je snadné vidět, že $\pi_n(a)$ je rovno zbytku po dělení polynomu a polynomem x^n-1.

Definujeme-li na $F[x]_n$ sčítání a násobení jako

$$\begin{aligned} a+b &= \pi_n(a+b)\\ a\cdot b &= \pi_n(a\cdot b)\end{aligned}$$

stane se z $F[x]_n$ okruh izomorfní s okruhy $F[x]/(x^n-1)$.

Každý ideál $F[x]$, který obsahuje ideál x^n-1, je roven nějakému (g), kde g je jednoznačně určený monický polynom dělící x^n-1.

Ideály v $F[x]_n$ mají tvar $\pi_n(gF[x])$. Je-li $x^n-1=gh$, vyjádříme $a\in F[x]$ jako $c\cdot h+b$, kde $\deg b<\deg h$. Pak $\pi_n(ga)=\pi_n(ghc+gb)=\pi_n(gb)=gb$. Proto můžeme vyslovit:

Tvrzení C.1. *Buď F komutativní těleso a $n\geq 1$. Pro každý monický dělitel g polynomu x^n-1 je množina $C(g)=\{ga;\ a\in F[x],\deg(a)<n-\deg(g)\}$ ideálem okruhu $F[x]_n$ a každý ideál $F[x]_n$ lze takto jednoznačně vyjádřit.*

□

V dalším budeme prvky $\mathbb{F}_q^n$ ztotožňovat s prvky $F_q[x]_n$ tak, aby vektoru $(u_0,u_1,\ldots,u_{n-1})$ odpovídal polynom $u_0+u_1x+u_{n-1}x^{n-1}$. Kódy $C\subseteq\mathbb{F}_q^n$ tedy dále chápeme (také) jako podmnožiny $\mathbb{F}_q[x]_n$.

Tvrzení C.2. *Cyklické lineární q-ární kódy délky n se shodují s množinami $C(g)$, kde g probíhá všechny dělitele $x^n-1\in\mathbb{F}_q[x]$.*

Důkaz. Ať $C\subseteq\mathbb{F}_q[x]_n$ je cyklický lineární kód. Potom je C lineární podprostor $\mathbb{F}_q[x]_n$ a pro každé $u\in C$ je $\pi_n(xu)\in C$. Indukcí dostáváme $\pi_n n(x^iu)\in C$ pro všechna $i\geq 0$, takže $\pi_n(au)=\sum a_i\pi_n(x^iu)\in C$ pro každé $a=\sum a_ix^i\in\mathbb{F}_q[x]$. Vidíme, že C je ideál, a proto lze použít Tvrzení C.1. Naopak je zřejmé, že každý ideál $\mathbb{F}_q[x]_n$ poskytuje lineární cyklický kód. □

Tvrzení C.3. *Ať $x^n-1=gh\in\mathbb{F}_q[x]$, kde g, h jsou monické polynomy a ať $k=\deg h\geq 1$. Potom $C(g)$ je cyklický $[n,k]_q$ kód. Dále pro $k'=n-k=\deg(g)$ a polynomy*

$$\begin{aligned} g &= g_{k'}x^{k'}+g_{k'-1}x^{k'-1}+\ldots+g_1x+g_0\\ h &= h_kx^k+h_{k-1}x^{k-1}+\ldots+h_1x+h_0\end{aligned}$$

jsou matice

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

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \dots & 0 \\ 0 & 0 & h_k & \cdots & \cdots & h_1 & h_0 & \dots & 0 \\ \vdots & & & \ddots & \ddots & \ddots & & & \vdots \\ 0 & 0 & \dots & 0 & h_k & \dots & \dots & h_1 & h_0 \end{pmatrix}$$

po řadě generující a prověrková matice $C(g)$.

Důkaz. Řádky matice G odpovídají polynomům g, xg, …, $x^{k-1}g$, takže pro $ga \in C(G)$, kde $\deg a < k$ a $a = \sum a_i x^i$, je $ga = a_0 g + a_1 xg + \cdots + a_{k-1}x^{k-1}g$. Z definice $C(g)$ vyplývá, že G je opravdu jeho generující maticí. Zbývá ověřit, že bodový součin libovolných řádků obou matic dává nulu. Řádky matice H odpovídají polynomům f, xf, …, $x^{k'-1}f$, kde $f = h_k + h_{k-1}x + \cdots + h_1 x^{k-1} + h_0 x^k$. Bodový součin $x^a g$ a $x^b h$ je v případě $b \geq a$ shodný s bodovým součinem g a $x^\delta h$, kde $b - a = \delta \leq k - 1$, a ten je roven $\sum g_i h_{k-\delta-i}$. V případě $a > b$ je bodový sočin $x^a g$ a $x^b h$ roven bodovému součinu $x^\sigma g$ a h, kde $a - b = \sigma \leq k' - 1$, a ten je roven $\sum h_{k-i} g_{i+\sigma}$. Máme $1 \leq k - \delta \leq k$ a $k < k + \sigma \leq k + k' - 1 = n - 1$. Hodnota $\sum_{i+j=r} g_i h_j$ se shoduje s koeficientem x^r v polynomu $x^n - 1 = gh$. Ve všech výše uvažovaných případech je $1 \leq r \leq n - 1$, takže příslušná hodnota je vždy nulová. □

Vidíme, že pro určení struktury cyklických kódů je rozhodující umět rozkládat polynomy $x^n - 1 \in F[x]$, kde F je konečné těleso.

Obecně pro komutativní těleso F máme $x^n - 1 = (x^m - 1)^{p^k}$, pokud $p > 0$ je charakteristika tělesa F a $n = m \cdot p^k$, kde p nedělí m. Stačí se tedy zabývat rozklady $x^n - 1$, kde $\operatorname{char} F$ nedělí n.

Tvrzení C.4. *Ať F je komutativní těleso s prvotělesem P. Pro každé $d \geq 1$, kde $char(F)$ nedělí d, existuje jednoznačně určený polynom $t_d \in P[x]$, závislý pouze na charakteristice F takový, že pro všechna $n \geq 1$, kde $charF$ nedělí n, je $x^n - 1 = \prod_{d|n} t_d$. Pokud se $x^n - 1$ rozkládá v tělese $K \supseteq F$ na kořenové činitele, tak $t_n = \prod(x - \zeta)$, kde $\zeta \in K$ probíhá všechny kořeny $x^n - 1$, které jsou řádu n. Přitom t_n je monický polynom stupně $\varphi(n)$, kde φ označuje Eulerovu funkci.*

Důkaz. Dle definice je $t_1 = x - 1$. Vidíme, že pro $n = 1$ tvrzení platí. Postupujme indukcí. Ať $n > 1$. Protože derivace $x^n - 1$ je rovna $nx^{n-1} \neq 0$, nemá $x^n - 1$ v K vícenásobné kořeny. Množina R všech kořenů $x^n - 1$ v K je konečná podgrupa K^*, a proto je cyklická. V cyklické grupě řádu n je právě $\varphi(d)$ prvků

řádu d, pro každé $d|n$. Podle indukčního předpokladu je $\prod(x-\xi)$, kde $\xi \in R$ probíhá všechny kořeny řádu $< n$, rovno $\prod_{d|n,d<n} t_d$. Označme tento polynom r. Označme s polynom $\prod(x-\zeta)$, kde $\zeta \in R$ probíhá kořeny řádu n. Máme $x^n - 1 = rs$, přičemž $r \in F[x]$ je monický. Polynom $s \in K[x]$ se získá tak, že $x^n - 1 \in P[x]$ vydělíme polynomem $r \in P[x]$. Ze znalosti algoritmu dělení plyne, že všechny koeficienty s leží v P. Proto $s = t_n \in P[x]$. □

Polynomy t_n se nazývají *cyklotomické* nebo též *kruhové*. Pro $n = p$ prvočíslo je $t_p = 1 + x + \cdots + x^{p-1}$.

Tvrzení C.5. *Buď $x^n - 1 \in \mathbb{F}_q[x]$, kde q a n jsou nesoudělné. Polynom $x^n - 1$ se rozkládá v $\mathbb{F}_{q^s}[x]$ na kořenové činitele právě když $q^s \equiv 1$ mod n, tedy když s je násobkem řádu q v $\mathbb{Z}_n^*$. Toto nastane právě když $t_n \in \mathbb{F}_q[x]$ má v $\mathbb{F}_{q^s}$ alespoň jeden kořen.*

Důkaz. Podmínka je nutná, neboť v tělese, kde se $x^n - 1$ rozkládá na kořenové činitele, existuje podgrupa řádu n. Ta tam existuje i v případě, kdy t_n má alespoň jeden kořen. Proto platí, že když má t_n alespoň jeden kořen, tak už se rozkládá na kořenové činitele. Pak n dělí $q^s - 1 = |\mathbb{F}_{q^s}^*|$, což lze jinak vyjádřit jako $q^s \equiv 1 \bmod n$. Polynom $x^{q^s-1} - 1$ se v $\mathbb{F}_{q^s}[x]$ rozkládá na kořenové činitele a $x^n - 1$ ho dělí, pokud n dělí $q^s - 1$. Jde tedy i o podmínku dostačující. □

Tvrzení C.6. *Ať $x^n - 1 \in \mathbb{F}_q[x]$, kde q a n jsou nesoudělné. Buď s řád q v $\mathbb{Z}_n^*$. Pak t_n se rozkládá na součin $\varphi(n)/s$ ireducibilních polynomů stupně s.*

Důkaz. Ať S je množina všech kořenů $x^n - 1 \in \mathbb{F}_{q^s}[x]$, které jsou řádu n. Víme, že $t_n = \prod(x-\zeta)$, kde $\zeta \in S$. Je-li a monický ireducibilní dělitel polynomu t_n a $\zeta \in S$ je kořen a, tak minimální polynom $m_\zeta \in \mathbb{F}_q[x]$ dělí a, a je mu tedy roven. Stačí ukázat, že stupeň m_ζ je s. Stupeň m_ζ je roven $[\mathbb{F}_q[\zeta] : \mathbb{F}_q]$, což je rovno s právě když $\mathbb{F}_q[\zeta] = K$. Poslední rovnost platí, neboť s je nejmenší číslo takové, že t_n má v $\mathbb{F}_{q^s}$ alespoň jeden kořen. □

Prvek ζ komutativního tělesa se nazývá **n-tá odmocnina z jedné**, pokud $\zeta^n = 1$. Je-li ζ řádu n, hovoříme o **primitivní n-té odmocnině z jedné**. Cyklotomický polynom t_n, kde $\operatorname{char} F$ nedělí n, lze tudíž zapsat jako $\prod(x-\zeta)$, kde ζ probíhá (ve vhodném rozšíření) všechny primitivní n-té odmocniny z jedné. Ireducibilní polynomy dělící $x^n - 1 \in \mathbb{F}_q[x]$ jsou tedy právě všechny minimální polynomy m_ζ, kde ζ probíhá primitivní n-té odmocniny z jedné.

Lemma C.7. *Buďte f a g dva dělitelé polynomu $x^n - 1 \in \mathbb{F}_q[x]$. Pak $C(f) \subseteq C(g)$ právě když g dělí f. Dále $C(f) \cap C(g) = C(NSN(f,g))$ a $C(NSD(f,g))$ je nejmenší cyklický kód, který obsahuje $C(f)$ i $C(g)$, tedy $C(NSD(f,g)) = C(f) + C(g)$.*

Důkaz. Struktura ideálů $\mathbb{F}_q[x]_n$ souhlasí se strukturou ideálů $\mathbb{F}_q[x]$, které obsahují ideál $(x^n - 1)$. Stačí si tedy uvědomit, že je-li F komutativní těleso, tak pro všechna $f, g \in F[x]$ platí $(f) + (g) = (\mathrm{NSD}(f,g))$ a $(f) \cap (g) = (\mathrm{NSN}(f,g))$. □

Lemma C.8. *Ať $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$. Položme $u = u_1 + u_2x + \ldots + u_nx^{n-1}$. Nejmenší cyklický kód délky n nad $\mathbb{F}_q$, který obsahuje $(u_1, \ldots, u_n)$, je roven $C(NSD(u, x^n - 1))$.*

Důkaz. Jde o nalezení ideálu $\mathbb{F}_q[x]_n$, který obsahuje polynom u. Jinak vyjádřeno, hledáme nejmenší ideál $\mathbb{F}_q[x]$, který obsahuje $(u) + (x^n - 1) = \mathrm{NSD}(u, x^n - 1)$. □

Lemma C.9. *Ať C je cyklický $[n, k]_q$ kód. Buď j, $j' \in \{0, 1, \ldots, n-1\}$ taková, že $jj' \equiv 1 \bmod n$. Sestrojme C' jako množinu všech $\pi_n\left(u\left(x^j\right)\right)$, kde $u(x) = u$ probíhá všechna kódová slova kódu $C \subseteq \mathbb{F}_q[x]_n$. Potom C' je cyklický kód stejné dimenze jako C a je mu permutačně ekvivalentní. Je-li $C = C(f)$, kde f dělí $x^n - 1$, tak $C' = C(NSD(f(x^j), x^n - 1)$.*

Důkaz. Pro C platí, že z $u \in C$ plyne $\pi_n(xu) \in C$. Tudíž z $\pi_n(u(x^j)) \in C'$ plyne $\pi_n(x^j u(x^j)) \in C'$. Rotací o j pozic se tedy z kódového slova C' opět stane kódové slovo C'. Pokud se tato rotace opakuje j'-krát, dostaneme rotaci pouze o jednu pozici, neboť $1 \equiv jj' \bmod n$. Proto je C' uzavřené na cyklické posuny. Je-li $(u_0, u_1, \ldots, u_{n-1}) \in C$, tak $(u_{0j'}, u_{1j'}, \ldots, u_{(n-1)j'}) \in C'$, neboť při počítání indexů a exponentů modulo n máme $u_{ij'}x^i = u_{ij'}x^{ij'j} = u_{ij'}(x^j)^{j'i}$, takže $\sum u_{ij'}x^i = \sum u_{ij'}(x^j)^{j'i} = \sum u_i(x^j)^i = u(x^j)$. Vidíme, že C' je kód permutačně ekvivalentní kódu C, a proto musí mít i stejnou dimenzi.

Ať $C = C(g)$. Každý prvek C je sumou lineárních kombinací cyklických posunů g. Tudíž C' je sumou lineárních kombinací cyklicých posunů $g(x^j)$. Jde tedy o ideál $\mathbb{F}_q[x]_n$ generovaný polynomem $g(x^j)$, a proto lze použít Lemma C.8. □

Důsledek C.10. *Uvažme $m_\zeta \in \mathbb{F}_q[x]$, kde ζ je primitivní n-tá odmocnina z jedné a $NSD(n, q) = 1$. Je-li pro $j > 1$ prvek $\zeta' = \zeta^j$ jiná primitivní odmocnina z jedné a je-li $jj' \equiv 1 \mod n$, tak*

$$m_{\zeta'} = NSD\left(x^n - 1,\, m_\zeta(x^{j'})\right).$$

Důkaz. Z Tvrzení C.4 víme, že m_ζ a $m_{\zeta'}$ jsou stejného stupně. Z Lemmatu C.9 plyne, že takového stupně je i $\mathrm{NSD}(x^n - 1, m_\zeta(x^{j'}))$. Samozřejmě platí, že $m_{\zeta'}$ tento polynom dělí, neboť $(\zeta')^{j'} = \zeta$. □

Důsledek C.11. *Ať $f, g \in \mathbb{F}_q[x]$ jsou dva ireducibilní dělitelé t_n a ať $NSD(q, n) = 1$. Pak $C(f)$ a $C(g)$ jsou permutačně ekvivalentní.*

Důkaz. Podle Důsledku C.10 máme $f = m_{\zeta'}$ a $g = m_\zeta$ pro vhodná ζ a ζ'. □

Je dobré si uvědomit, že pokud $f | t_n$, $\mathrm{NSD}(f, q) = 1$ je ireducibilní a $f(\zeta) = 0$, tak $\zeta^q, \ldots, \zeta^{q^{s-1}}$ jsou také kořeny f. Hodnotu s volíme jako řád q modulo n. Kořeny f jsou tak tvořeny prvky automorfismu $x \mapsto x^q$. Předpoklad $1 = \mathrm{NSD}(n, q)$ je nutný pro to, aby t_n byl polynom bez vícenásobných kořenů. Značná část teorie cyklických kódů předpokladá splnění uvedené podmínky nesoudělnosti.

Podle Lemmatu C.7 je $C(f) + C(g) = C(\mathrm{NSD}(f, g))$. Pokud $C(f) \cap C(g) = 0$, tak je $C(\mathrm{NSD}(f, g)) = C(f) \oplus C(g)$. Ovšem $C(f) \cap C(g) = 0$, pokud $x^n - 1 = \mathrm{NSN}(f, g)$. Poslední uvedená podmínka v případě $\mathrm{NSD}(n, q) = 1$ znamená, že kořeny f a kořeny g pokrývají všechny n-té odmocniny z jedné. Rozšířením na více sčítanců pak dostáváme, že $C(\mathrm{NSD}(f_1, \ldots, f_r)) = C(f_1) \oplus \ldots \oplus C(f_r)$, jestliže pro každé $1 \leq j \leq r$ platí, že každá n-tá odmocnina z jedná je kořenem f_j nebo kořenem všechny zbylých f_i, $i \neq j$. Jsou-li $g_1, \ldots, g_r$ všechny ireducibilní polynomy, které dělí $x^n - 1$, tak tato podmínka bude splněna, pokud položíme $f_i = (x^n - 1)/g_i$, $1 \leq i \leq r$. Můžeme proto vyslovit:

Tvrzení C.12. *Ať NSD$(n, q) = 1$ a ať $x^n - 1 = g_1 \cdot \ldots \cdot g_r$ je rozklad na ireducibilní polynomy. Položme $f_i = (x^n - 1)/g_i$. Pak $\mathbb{F}_q^n = C(f_1) \oplus \ldots \oplus C(f_r)$. Současně platí, že $C(f_1), \ldots, C(f_r)$ jsou právě všechny minimální cyklické q-ární kódy délky n a $C(g_1), \ldots, C(g_r)$ jsou právě všechny maximální q-ární cyklické kódy délky n.*

□

Tvrzení C.13. *Ať NSD$(n, q) = 1$ a ať $C \subseteq \mathbb{F}_q[x]_n$ je cyklický kód. Ať komutativní těleso $K \supseteq \mathbb{F}_q$ obsahuje $\mathbb{F}_{q^s}$, kde s je řádu q v $\mathbb{Z}_n^*$. Pak C je plně určeno množinou M včech $\zeta \in K^*$, $a(\zeta) = 0$ pro každé $a \in C$. Přitom $C = C(f)$, kde $f = \prod_{\zeta \in M}(x - \zeta)$, a $\zeta \in M$ právě když m_ζ dělí f.*

Důkaz. Kód C je roven nějakému $C(f)$. Pokud $\zeta \in M$, tak m_ζ dělí každé $a \in C$, takže m_ζ dělí f. Je-li naopak f dělitelné m_ζ, tak $C(f) \subseteq C(m_\zeta)$, a tedy $\zeta \in M$. Vidíme, že M splývá jak s množinou kořenů f, tak s množinou takových $\zeta \in K$, že m_ζ dělí f. Podmínka $\mathrm{NSD}(n, q) = 1$ je potřebná k tomu, aby M určovalo f jednoznačně. □

Tvrzení C.14. *Ať se v komutativním tělese $K \supseteq \mathbb{F}_q$ rozkládá $x^n - 1$ na kořenové činitele. Ať $\xi_1, \ldots, \xi_r \in K$ jsou nějaké n-té odmocniny z jedné. Definujme C jako množinu všech $a \in \mathbb{F} - q[x]$. že $a(\xi_1) = \cdots = a(\xi_r) = 0$. Pak C je cyklický kód a $C = \bigcap(C(m_{\xi_i}); 1 \leq i \leq r) = C(NSN(m_{\xi_1}, m_{\xi_2}, \ldots, m_{\xi_r}))$.*

Důkaz. Pokud $a \in C$, tak m_{ξ_i} dělí a pro každé i, $1 \leq i \leq r$. Proto $C \supseteq C(f)$, kde $f = \mathrm{NSN}(m_{\xi_1}, m_{\xi_2}, \ldots, m_{\xi_r})$. Je-li naopak $a \in C(f)$, tak z $m_{\xi_i} | a$ plyne $a(\xi_i) = 0$. □