5 Cyklické kódy

5.1 Definice Lineární kód K délky n nad $\mathbb{Z}_p$ je *cyklický*, pokud je množina kódových slov uzavřená na cyklické posuny, tj. pokud pro každé $\bar{v} = (v_1 v_2 \dots v_n) \in K$ je také $c(\bar{v}) = (v_2 \dots v_n v_1) \in K$.

5.2 Příklad Opakovací kód délky n nad $\mathbb{Z}_p$ je zřejmě cyklický.
Binární kód kontroly parity délky n je cyklický, protože obsahuje právě všechna slova délky n o sudém počtu jedniček a cyklické otáčení počet jedniček nezmění.

5.3 U cyklických kódů se vyplatí chápat kódová slova délky n jako polynomy stupně nejvýše $(n-1)$. Cyklický posun je pak realizován vynásobením proměnnou z podle pravidla $z^n = 1$. Tedy

$$\begin{array}{lcrcl} \bar{v} = (v_1 \dots v_{n-1} v_n) & \leftrightarrow & v(z) & = & v_1 z^{n-1} + \dots + v_{n-1} z + v_n \\ c(\bar{v}) = (v_2 \dots v_n v_1) & \leftrightarrow & z \cdot v(z) & = & v_1 z^n + v_2 z^{n-1} + \dots + v_{n-1} z^2 + v_n z \\ & & & = & v_2 z^{n-1} + \dots + v_{n-1} z^2 + v_n z + v_1 \end{array}$$

Jakožto lineární prostory nad $\mathbb{Z}_p$ se prostor $\mathbb{Z}_p^n$ všech slov nad $\mathbb{Z}_p$ délky n a prostor všech polynomů nad $\mathbb{Z}_p$ stupně nejvýše $(n-1)$ shodují (sčítání a násobení konstantou ze $\mathbb{Z}_p$ je v nich realizováno stejně). Proto budeme prostor polynomů nad $\mathbb{Z}_p$ stupně nejvýše $(n-1)$ značit $\mathbb{Z}_p^{(n)}$.
Na množině všech polynomů nad $\mathbb{Z}_p$ stupně nejvýše $(n-1)$ máme však navíc operaci násobení - umíme vynásobit dva polynomy nad $\mathbb{Z}_p$ a použít přepisovací pravidlo $z^n = 1$ (a další odvozená pravidla $z^{n+1} = z$, $z^{n+2} = z^2$ atd.), takže výsledkem bude opět polynom stupně nejvýše $(n-1)$. Takto definované násobení odpovídá násobení ve faktorovém okruhu $\mathbb{Z}_p[x]/(x^n - 1)$, aneb $\mathbb{Z}_p^{(n)}$ tvoří komutativní okruh s jednotkou.

5.4 Definice Nechť $(R, +, \cdot)$ je komutativní okruh. Podmnožina $I \subset R$ se nazývá *ideál* okruhu R, jestliže $(I, +)$ je podgrupa grupy $(R, +)$ a jestliže pro všechny $r \in R$ a všechny $i \in I$ je $r \cdot i \in I$.

5.5 Tvrzení *Cyklický kód K délky n nad $\mathbb{Z}_p$ je ideál v okruhu $\mathbb{Z}_p^{(n)}$.*

Důkaz Cyklický kód K je lineární, tvoří lineární podprostor v $\mathbb{Z}_p^{(n)}$, a je tudíž podgrupou vůči sčítání. Zbývá dokázat uzavřenost kódu K na násobení libovolným polynomem ze $\mathbb{Z}_p^{(n)}$.
K je cyklický kód, tudíž pro $v(z) \in K$ je $z \cdot v(z) \in K$, a tudíž je také $z^2 \cdot v(z) \in K$ a libovolné $z^i \cdot v(z) \in K$.
Buď $a(z) = \sum_{i=1}^{s} a_i z^i \in \mathbb{Z}_p^{(n)}$, pak $a(z) \cdot v(z) = \sum_{i=1}^{s} a_i (z^i \cdot v(z))$ je lineární kombinací kódových polynomů, ale K je lineární kód, tudíž $a(z) \cdot v(z) \in K$. ⊠

5.6 Definice *Generující polynom* cyklického kódu K nad $\mathbb{Z}_p$ je takový kódový polynom $g(z) \in K$, že každý kódový polynom je jeho polynomiálním násobkem, tj.

$$v(z) \in K \quad \text{iff} \quad v(z) = a(z) \cdot g(z) \quad \text{pro nějaký } a(z) \in \mathbb{Z}_p^{(n)}.$$

5.7 Tvrzení *Každý cyklický kód K délky n nad $\mathbb{Z}_p$ má generující polynom.*

Důkaz Zvolme jako $g(z)$ nějaký nenulový kódový polynom nejmenšího stupně. Dokážeme, že libovolný kódový polynom $v(z) \in K$ je jeho násobkem. Podle věty o dělení polynomů nad $\mathbb{Z}_p$ je $v(z) = a(z) \cdot g(z) + r(z)$, kde $\mathrm{st}(r) < st(g)$. Avšak polynom $r(z) = v(z) - a(z) \cdot g(z)$ je také kódový, neboť K je ideál v $\mathbb{Z}_p^{(n)}$. Protože $g(z)$ má nejmenší stupeň mezi nenulovými kódovými polynomy, musí být $r(z) = 0$. ⊠

5.8 Důkaz předchozího tvrzení nám dává návod, jak najít generující polynom $g(z)$ cyklického kódu K. Je jím jakýkolikv nenulový kódový polynom nejmenšího stupně. Takových polynomů bude právě $(p-1)$ a budou se lišit o vynásobení nenulovou konstantou ze $\mathbb{Z}_p$ (budou to navzájem asociované polynomy).

Dále je z důkazu patrné, že každý kódový polynom je tvaru $v(z) = a(z) \cdot g(z)$, kde $n - 1 \geq \mathrm{st}(v) = \mathrm{st}(a) + \mathrm{st}(g)$ (protože $a(z)$ vznikl dělením), aneb při násobení $a(z) \cdot g(z)$ se nepoužívá přepisovací pravidlo $z^n = 1$ a jde o obyčejné násobení polynomů nad $\mathbb{Z}_p$. Pro různé polynomy $a(z)$ tedy vzniknou různé kódové polynomy $v(z)$ (neboť okruh polynomů nad $\mathbb{Z}_p$ nemá dělitele nuly) a každé kódové slovo vznikne tímto způsobem, tj. vynásobením polynomu $g(z)$ nějakým polynomem $a(z)$ stupně nejvýše $(n - 1 - \mathrm{st}(g))$. Jde o vzájemně jednoznačné přiřazení mezi polynomy $a(z)$ a kódovými polynomy $v(z)$, které určuje kódování informace délky $k = n - \mathrm{st}(g)$.

5.9 Kódování pomocí generujícího polynomu: Nechť K je cyklický (n,k)-kód s generujícím polynomem $g(z)$, tedy $\mathrm{st}(g) = n-k$. Kódování informace délky k probíhá takto: Informačnímu slovu přiřadíme informační polynom stupně nejvýše $(k-1)$, ten vynásobíme generujícím polynomem $g(z)$ a vzniklý kódový polynom stupně nejvýše $(n-1)$ opět přepíšeme na kódové slovo.

$$\begin{array}{rcll} \bar{a} = (a_1 \dots a_{k-1} a_k) & \leftrightarrow & a(z) = a_1\, z^{k-1} + \dots + a_{k-1}\, z + a_k & \\ a(z) & \longrightarrow & v(z) = a(z) \cdot g(z) & \\ & & v(z) = v_1\, z^{n-1} + \dots + v_{n-1}\, z + v_n & \leftrightarrow \quad \bar{v} = (v_1 \dots v_{n-1} v_n) \end{array}$$

Dekódování: Kódový polynom $v(z) \in K$ vydělíme generujícím polynomem $g(z)$ nad $\mathbb{Z}_p$ a získáme informační polynom $a(z) = v(z) : g(z)$.

5.10 Tvrzení *Je-li $g(z)$ generující polynom cyklického (n,k)-kódu K nad $\mathbb{Z}_p$, pak*
1) množina $\{g(z), z\,g(z), z^2\,g(z), \dots, z^{k-1}\,g(z)\}$ tvoří bázi podprostoru K (bázi získáme otáčením slova $\bar{g}$, které odpovídá generujícímu polynomu $g(z)$).
2) Generující matice $\mathbb{G} = \begin{pmatrix} c^{k-1}(\bar{g}) \\ \vdots \\ c(\bar{g}) \\ \bar{g} \end{pmatrix}$ *určuje stejné kódování jako generující polynom $g(z)$.*

Důkaz $v(z) \in K$ iff $v(z) = a(z) \cdot g(z) = \sum_{i=1}^{k} a_i\,(z^i \cdot g(z))$, přitom polynomy $g(z), z\,g(z), \dots, z^{k-1}\,g(z)$ jsou lineárně nezávislé (neboť násobení probíhá v okruhu polynomů nad $\mathbb{Z}_p$), tvoří tedy bázi podprostoru K.
Zapíšeme-li lineární kombinaci maticově, a pak přepíšeme do kódových slov, získáme kódování pomocí matice $\mathbb{G}$.

$$v(z) = a(z) \cdot g(z) = \bar{a} \cdot \begin{pmatrix} z^{k-1} \cdot g(z) \\ \vdots \\ z \cdot g(z) \\ g(z) \end{pmatrix} \leftrightarrow \bar{v} = \bar{a} \cdot \begin{pmatrix} c^{k-1}(\bar{g}) \\ \vdots \\ c(\bar{g}) \\ \bar{g} \end{pmatrix} = \bar{a} \cdot \mathbb{G}$$

⊠

5.11 Příklad Binární kód kontroly parity délky 3 má kódová slova $K = \{(0\,0\,0), (0\,1\,1), (1\,0\,1), (1\,1\,0)\}$ a kódové polynomy $K = \{0, z+1, z^2+1, z^2+z\}$. Generujícím polynomem je $g(z) = z+1$ a určuje toto kódování:

$$\begin{array}{rcll} \bar{a} = (0\,0) & \longrightarrow & v(z) = 0 \cdot g(z) = 0 & \leftrightarrow \quad \bar{v} = (0\,0\,0) \\ \bar{a} = (0\,1) & \longrightarrow & v(z) = 1 \cdot g(z) = z+1 & \leftrightarrow \quad \bar{v} = (0\,1\,1) \\ \bar{a} = (1\,0) & \longrightarrow & v(z) = z \cdot g(z) = z^2+z & \leftrightarrow \quad \bar{v} = (1\,1\,0) \\ \bar{a} = (1\,1) & \longrightarrow & v(z) = (z+1) \cdot g(z) = z^2+1 & \leftrightarrow \quad \bar{v} = (1\,0\,1) \end{array}$$

Stejné kódování určuje matice $\mathbb{G} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \leftrightarrow \begin{pmatrix} z \cdot g(z) \\ g(z) \end{pmatrix}$.

5.12 Systematické kódování pro cyklický (n,k)-kód K lze také provádět pomocí generujícího polynomu $g(z)$. Nejprve informačnímu slovu přiřadíme polynom stupně $(n-1)$ tak, že informační znaky napíšeme na začátek (od nejvyšších mocnin):

$$\bar{a} = (a_1 \dots a_k) \longrightarrow u(z) = a_1\, z^{n-1} + a_2\, z^{n-2} + \dots + a_k\, z^{n-k}$$

Polynom $u(z)$ vydělíme generujícím polynomem $g(z)$ a dostaneme:

$$u(z) = f(z)\, g(z) + r(z), \quad \text{kde} \quad st(r) < st(g) = n-k$$

Polynom $v(z) = u(z) - r(z) = f(z)\, g(z)$ je kódový polynom z K, neboť je násobkem generujícího polynomu. Navíc odečítání zbytkového polynomu nezasáhlo do informačních znaků:

$$v(z) = u(z) - r(z) = a_1\, z^{n-1} + a_2\, z^{n-2} + \dots + a_k\, z^{n-k} - r_{n-k-1}\, z^{n-k-1} - \dots - r_1\, z - r_0$$

Přiřadíme-li informačnímu slovu $\bar{a}$ kódové slovo $\bar{v} \leftrightarrow v(z)$, bude toto přiřazení určovat systematické kódování.

5.13 Tvrzení *Generující polynom $g(z)$ cyklického kód K délky n nad $\mathbb{Z}_p$ dělí beze zbytku polynom $x^n - 1$ v polynomech nad $\mathbb{Z}_p$.*

Důkaz Podle věty o dělení polynomů je $x^n - 1 = h(x) \cdot g(x) + r(x)$, kde $\mathrm{st}(r) < \mathrm{st}(g)$ v $\mathbb{Z}_p[x]$. Potom v okruhu $\mathbb{Z}_p^{(n)} = \mathbb{Z}_p[x]/x^n - 1$ je $0 = h(z) \cdot g(z) + r(z)$, odkud $r(z) = -h(z) \cdot g(z) \in K$, neboť K je ideál v $\mathbb{Z}_p^{(n)}$. Protože má generující polynom nejnižší stupeň mezi nenulovými kódovými polynomy, musí být $r(z) = 0$. ⊠

5.14 Důsledek *Každý rozklad polynomu $x^n - 1 = h(x) \cdot g(x)$ v polynomech nad $\mathbb{Z}_p$ určuje cyklický kód délky n nad $\mathbb{Z}_p$. Je tedy tolik cyklických kódů délky n nad $\mathbb{Z}_p$, kolik je monických dělitelů polynomu $x^n - 1$ v $\mathbb{Z}_p[x]$.*

5.15 Příklad V $\mathbb{Z}_2[x]$ je $x^3 - 1 = (x+1)(x^2 + x + 1)$ rozklad na ireducibilní polynomy, existují tedy pouze dva binární cyklické kódy délky 3. Je to opakovací kód s $g(z) = z^2 + z + 1$ a kód kontroly parity s $g(z) = z + 1$.

5.16 Definice *Kontrolní polynom* cyklického kódu K délky n nad $\mathbb{Z}_p$ je takový polynom $h(z) \in \mathbb{Z}_p^{(n)}$, že pro každý polynom $v(z) \in \mathbb{Z}_p^{(n)}$ platí:

$$v(z) \in K \quad \text{iff} \quad v(z) \cdot h(z) = 0 \quad \text{v okruhu} \quad \mathbb{Z}_p^{(n)} = \mathbb{Z}_p[x]/x^n - 1$$

aneb násobení je podle pravidla $z^n = 1$.

5.17 Tvrzení *Každý cyklický kód K délky n nad $\mathbb{Z}_p$ má kontrolní polynom.*

Důkaz Položme $h(x) = (x^n - 1) : g(x)$ v $\mathbb{Z}_p[x]$, kde dělení je beze zbytku dle předchozího tvrzení. Víme, že $v(z) \in K$ právě, když $v(z) = a(z) \cdot g(z)$, což nastane právě, když $v(z) \cdot h(z) = a(z) \cdot g(z) \cdot h(z) = a(z) \cdot (z^n - 1) = 0$, počítáme-li podle pravidla $z^n = 1$. ⊠

Poznámka Pro cyklický (n, k)-kód K nad $\mathbb{Z}_p$ je $\mathrm{st}(h) = k$, protože $h(x) \cdot g(x) = x^n - 1$ v $\mathbb{Z}_p[x]$ a už víme, že $\mathrm{st}(g) = n - k$.

5.18 Tvrzení *Nechť $h(z) = h_k\, z^k + \ldots + h_1\, z + h_0$ je kontrolní polynom cyklického (n, k)-kódu K nad $\mathbb{Z}_p$. Pak kontrolní matice kódu K má tvar*

$$\mathbb{H} = \begin{pmatrix} 0 & \ldots & & 0 & h_0 & h_1 & \ldots & h_k \\ & & & \vdots & & & & \\ 0 & h_0 & h_1 & \ldots & h_k & 0 & \ldots & 0 \\ h_0 & h_1 & \ldots & h_k & 0 & & \ldots & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} z^{n-k-1} \cdot h(z)^{op} \\ \vdots \\ z \cdot h(z)^{op} \\ h(z)^{op} \end{pmatrix},$$

kde $h(z)^{op}$ znamená, že koeficienty polynomu se do slova délky n vypisují v opačném pořadí, tedy od nejnižších mocnin.

Důkaz Při kontrole slova $\bar{w}$ touto maticí $\mathbb{H}$ vznikají v syndromu $\bar{s}^T = \mathbb{H}\, \bar{w}^T$ koeficienty polynomu $h(z) \cdot w(z)$, kontrolou tedy projde slovo $\bar{w}$ právě, když projde polynom $w(z)$. Konkrétně

$$\bar{s}^T = \mathbb{H}\, \bar{w}^T = \begin{pmatrix} s_k \\ \vdots \\ s_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{iff} \quad h(z) \cdot w(z) = s_{n-1}\, z^{n-1} + \ldots + s_k\, z^k + \ldots + s_0 = 0.$$

⊠

5.19 Opravování chyb Pokud je v přijatém polynomu jedna chyba, pak $w(z) = v(z) + a\, z^i$, kde $v(z) \in K$. Při vynásobení kontrolním polynomem vznikne syndrom $w(z) \cdot h(z) = 0 + a\, z^i \cdot h(z)$. Určíme-li jednoznačně a a z^i, pak můžeme chybu opravit: $v(z) = w(z) - a\, z^i$. Ale pozor, násobení jsme prováděli podle pravidla $z^n = 1$, nelze tedy jednoduše podělit syndromový polynom polynomem $h(z)$ jakožto polynomy nad $\mathbb{Z}_p$.

K opravování chyb budeme raději používat kontrolní matici.