8 Kořeny cyklických kódů, BCH-kódy

Generující kořeny cyklických kódů

Nechť K je cyklický kód délky n nad $\mathbb{Z}_p$ s generujícím polynomem $g(z)$. Chceme najít rozšíření T tělesa $\mathbb{Z}_p$, tedy nějaké těleso $GF(p^k)$, ve kterém by měl polynom $g(x)$ stupně m celkem m různých kořenů. Pokud se mám to podaří, budou tyto kořeny společné všem kódovým polynomům a kód K jimi bude jednoznačně určen.

8.1 Příklad Uvažujme těleso $GF(8)$, $T = \mathbb{Z}_2[x]/x^3+x+1$, aneb $T = \{a\alpha^2+b\alpha+c,\, a,b,c \in \mathbb{Z}_2,\, \alpha^3 = \alpha+1\}$. Víme z předchozí kapitoly, že α je primitivní prvek tělesa T a že má minimální polynom $m_\alpha(x) = x^3+x+1$. Dále víme, že x^7-1 se nad $\mathbb{Z}_2$ rozkládá na ireducibilní polynomy takto: $x^7-1 = (x+1)(x^3+x^2+1)(x^3+x+1)$.

1) Lze tedy sestrojit cyklický kód K délky 7 nad $\mathbb{Z}_2$ s generujícím polynomem $g(z) = z^3+z+1$. Přitom $v(z) \in K$ právě, když $g(z) \,|\, v(z)$. Ale $g(z) = m_\alpha(z)$ a $v(z)$ je dělitelný minimálním polynomem $m_\alpha(z)$ s kořenem α právě, když $v(z)$ má také kořen α. Cyklický kód K je jednoznačně určen kořenem α: $K = \{v(z) \in \mathbb{Z}_2^{(7)}, v(\alpha) = 0\}$.

Kořene α lze využít ke kontrole - pokud $v(\alpha) \neq 0$ v tělese T, tak polynom $v(z)$ je chybný.
Z podmínky $v(\alpha) = 0$ odvodíme kontrolní matici kódu K. Slova převádíme na polynomy takto:

$$\bar{v} = (v_1, v_2, \ldots, v_6, v_7) \;\leftrightarrow\; v(z) = v_1 z^6 + v_2 z^5 + \ldots + v_6 z + v_7$$

Odtud

$$v(\alpha) = v_1\alpha^6 + v_2\alpha^5 + \ldots + v_6\alpha + v_7 = (\alpha^6\, \alpha^5\, \ldots\, \alpha\, 1)\cdot \bar{v}^T = 0$$

a kontrolní matice nad tělesem T pro kód K je $\mathbb{H} = (\alpha^6\, \alpha^5\, \ldots\, \alpha\, 1)$. Rozepíšeme-li mocniny prvku α na polynomy stupně nejvýše 2 (prvky tělesa T), získáme homogenní soustavu nad $\mathbb{Z}_2$ pro kódová slova:

$$v(\alpha) = v_1(\alpha^2+1) + v_2(\alpha^2+\alpha+1) + \ldots + v_6\alpha + v_7 = 0$$

právě, když (první rovnice následující soustavy je pro koeficienty u α^2, druhá u α, třetí u 1)

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \cdot \bar{v}^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Matice této soustavy je kontrolní maticí $\mathbb{H}$ nad $\mathbb{Z}_2$ pro kód K.
Sloupec $\alpha^i = a\alpha^2 + b\alpha + c$ v matici $\mathbb{H}$ nad T odpovídá sloupci $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ v matici $\mathbb{H}$ nad $\mathbb{Z}_2$.

Všimněme si, že kontrolní matice $\mathbb{H}$ má za sloupce všechny nenulové trojice nad $\mathbb{Z}_2$ (protože α byl primitivní prvek a vygeneroval všechny nenulové prvky tělesa T). Náš kód K je tedy cyklický Hammingův kód se třemi kontrolními znaky.
Tudíž opravuje 1 chybu a opravování lze také dělat pomocí kořene α. V případě jedné chyby je $w(z) = v(z) + a\, z^i = v(z) + z^i$ (neboť $a \in \mathbb{Z}_2$), pro nějaký $v(z) \in K$. Pak $w(\alpha) =$ "polynom v α stupně nejvýše 2"$= 0 + \alpha^i$, přičemž mocnina primitivního prvku α^i je určena jednoznačně, tudíž chyba je v i-té mocnině.

2) Analogicky lze sestrojit cyklický kód K' délky 7 nad $\mathbb{Z}_2$ s generujícím polynomem $g(z) = (z+1)(z^3+z+1)$. Přitom $v(z) \in K'$ právě, když $g(z) \,|\, v(z)$. Ale $g(z) = m_1(z)m_\alpha(z)$ a $v(z)$ je dělitelný oběma minimálními (a tudíž ireducibilními) polynomy $m_1(z)$ i $m_\alpha(z)$ právě, když $v(z)$ má kořeny α a 1 v tělese T. Cyklický kód K je jednoznačně určen kořeny α, 1: $K = \{v(z) \in \mathbb{Z}_2^7, v(\alpha) = 0$ a $v(1) = 0\}$.
Kontrolní matice pro kód K' bude

$$\mathbb{H} = \begin{pmatrix} \alpha^6 & \alpha^5 & \ldots & \alpha & 1 \\ 1^6 & 1^5 & \ldots & 1 & 1 \end{pmatrix} \text{ nad } T \;\leftrightarrow\; \mathbb{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ nad } \mathbb{Z}_2\,.$$

8.2 Definice *Generující kořeny* cyklického kódu K délky n nad $\mathbb{Z}_p$ jsou takové prvky $c_1, c_2, \ldots, c_m$ nějakého tělesa $GF(p^k)$, že pro každý $v(z) \in \mathbb{Z}_p^{(n)}$ je $v(z) \in K$ právě, když $v(z)$ má kořeny $c_1, c_2, \ldots, c_m$ v tělese $GF(p^k)$.

8.3 Poznámka Generující kořeny nejsou určeny jednoznačně, protože kódové polynomy jsou celočíselné polynomy nad $\mathbb{Z}_p$ a mají v tělese charakteristiky p s kořenem c automaticky také kořeny c^p, $c^{(p^2)}$, atd. Například kód K délky 7 nad $\mathbb{Z}_2$ s generujícím polynomem $g(z) = z^3+z+1$ z prvního příkladu má v tělese $T = \mathbb{Z}_2[x]/x^3+x+1$ generující kořen α, ale také má generující kořeny α, α^2 a $\alpha^4 = \alpha^2 + \alpha$. Stejně tak je generujícím kořenem kódu K prvek α^2.

8.4 Tvrzení *Cyklický kód K délky n nad $\mathbb{Z}_p$ má v tělese $GF(p^k)$ generující kořeny právě, když má jeho generující polynom $g(z)$ v tělese T tolik navzájem různých kořenů, kolik je jeho stupeň.*

Důkaz Nechť $g(z)$ je stupně m a má v tělese T celkem m různých kořenů $c_1, c_2, \ldots, c_m$. Kódové polynomy jsou násobky generujícího polynomu, $v(z) \in K$ právě, když $v(z) = a(z)g(z)$. Tudíž $c_1, c_2, \ldots, c_m$ jsou též kořeny každého kódového polynomu. Naopak, protože kořeny jsou různé, tak každý polynom s kořeny $c_1, c_2, \ldots, c_m$ je dělitelný $\prod_{i=1}^{m}(z - c_i)$, ale polynom $g(z) = \prod_{i=1}^{m}(z - c_i)$, neboť $\mathrm{st}(g) = m$ a $c_1, c_2, \ldots, c_m$ jsou jeho kořeny (můžeme předpokládat, že generující polynom je monický). Takže každý polynom s kořeny $c_1, c_2, \ldots, c_m$ je kódovým polynomem.
Má-li $g(z)$ v tělese T méně než m různých kořenů, pak existují polynomy, které tyto kořeny mají také a přesto nejsou dělitelné polynomem $g(z)$, aneb nejsou to kódové polynomy. ⊠

8.5 Příklad Polynom $x^5 - 1$ se nad $\mathbb{Z}_5$ rozkládá na ireducibilní polynomy takto: $x^5 - 1 = (x - 1)^5$. Lze tedy sestrojit cyklický kód K délky 5 nad $\mathbb{Z}_5$ s generujícím polynomem $g(z) = (z - 1)^2$. Každý kódový polynom je dělitelný polynomem $g(z)$, má tedy kořen 1 v $\mathbb{Z}_5$. Ale ne každý polynom s kořenem 1 je kódový, neboť kořen 1 může být jen jednonásobný. Vlastnost $v(1) = 0$ necharakterizuje jednoznačně kód K.

8.6 Cyklický kód K délky n nad $\mathbb{Z}_p$ je svými generujícími kořeny v tělese $GF(p^k)$ (označme je T) jednoznačně určen. Z generujících kořenů spočteme generující polynom i kontrolní matici.

Generující polynom je nenulový kódový polynom nejmenšího stupně, aneb nenulový polynom nad $\mathbb{Z}_p$ nejmenšího stupně s danými kořeny v tělese. Je-li generujícím kořenem jeden prvek c, jedná se o minimální polynom pro tento prvek, tj. $g(z) = m_c(z)$. Jsou-li generujícími kořeny prvky $c_1, c_2, \ldots, c_m$, jedná se o součin minimálních polynomů pro ty prvky, které mají různé minimální polynomy (aneb které splňují $c_i \neq c_j^{(p^l)}$):

$$g(z) = \mathrm{lcm}(m_{c_1}(z), \ldots, m_{c_l}(z)) = \prod_{\text{přes různé polynomy}} m_{c_i}(z)$$

Kontrolní matice cyklického kódu K délky n s generujícím kořenem c je odvozena ze vztahu $v(c) = 0$, což je vlastně homogenní "soustava", kterou musí splňovat kódové polynomy. Matice této soustavy je $\mathbb{H} = \begin{pmatrix} c^{n-1} & c^{n-2} & \ldots & c & 1 \end{pmatrix}$ nad tělesem T. Nahradíme-li každé c^i = "polynom stupně nejvýše k v tělese T" sloupcem jeho koeficientů, získáme matici $\mathbb{H}$ o k řádcích nad $\mathbb{Z}_p$. Jsou-li v této matici některé řádky lineární kombinací ostatních, můžeme je vyškrtnout (a získáme matici pro ekvivalentní homogenní soustavu rovnic).
Kontrolní matice kódu K délky n s generujícími kořeny $c_1, c_2, \ldots, c_m$ se získá analogicky z matice

$$\mathbb{H} = \begin{pmatrix} c_1^{n-1} & c_1^{n-2} & \ldots & c_1 & 1 \\ c_2^{n-1} & c_2^{n-2} & \ldots & c_2 & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ c_m^{n-1} & c_m^{n-2} & \ldots & c_m & 1 \end{pmatrix} \text{ nad } T\,.$$

Opravování jedné chyby: Cyklický kód nad $\mathbb{Z}_p$ s jedním generujícím kořenem pro $p > 2$ většinou neopravuje jednu chybu. V případě jedné chyby je $w(z) = v(z) + a\,z^i$ pro $v(z) \in K$. Například nad $\mathbb{Z}_3$ mohou být dvě možnosti, jak vyjádřit "syndrom" ve tvaru $a\,c^i$, neboť může být $w(c) = 1\,c^i$ ale taky $w(c) = 2\,c^j$. Nevíme tedy, zda chybový polynom je $e(z) = 1\,z^i$ nebo $e(z) = 2\,z^j$, a neumíme chybu opravit.
Cyklický kód nad $\mathbb{Z}_p$ s více generujícími kořeny jednu chybu už opravovat může a lze to udělat pomocí kořenů. Vyjádříme syndrom pro každý kořen c_k všemi možnostmi jako $w(c_k) = a\,(c_k)^i$ (pro různá $a \in \mathbb{Z}_p$ a různá $0 \leq i \leq n-1$) a je-li pouze jediná možnost společná všem kořenům, pak tato možnost určuje chybový polynom.

8.7 Otázka č.1 Máme těleso T o p^k prvcích a v něm vybereme prvky $c_1, c_2, \ldots, c_m$. Chceme, aby tyto prvky byly generujícími kořeny cyklického kódu nad $\mathbb{Z}_p$. Pro jakou délku n kódových slov je to možné?

Víme, že generující polynom cyklického kódu délky n musí dělit $x^n - 1$ v $\mathbb{Z}_p[x]$. $g(z) = \mathrm{lcm}(m_{c_1}(z), \ldots, m_{c_l}(z))$, takže každý minimální polynom $m_{c_i}(x)$ musí dělit $x^n - 1$. Ale $m_{c_i}(x) \mid x^n - 1$ právě, když c_i je kořen $x^n - 1$, aneb když $c_i^n = 1$. Dostáváme podmínku, že řád každého kořene c_i musí dělit n. Délka cyklického kódu s generujícími kořeny $c_1, c_2, \ldots, c_m$ je $n = l \cdot \mathrm{lcm}(\mathrm{r}(c_1), \ldots, \mathrm{r}(c_m))$ pro libovolné $l \in \mathbb{N}$.

8.8 Příklad Je dáno těleso komplexních čísel nad $\mathbb{Z}_3$, $T = \mathbb{Z}_3[x]/x^2 + 1 = \{ai + b, a, b \in \mathbb{Z}_3,\ i^2 = -1\}$.
a) Cyklický kód s generujícím kořenem i v tělese T má nejmenší možnou délku $n = \mathrm{r}(i) = 4$. Jeho generující polynom je $g(z) = m_i(z) = z^2 + 1$. Jeho kontrolní matice je $\mathbb{H} = (i^3\ i^2\ i\ 1)$ nad tělesem T, což odpovídá matici $\mathbb{H} = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{pmatrix}$ nad $\mathbb{Z}_3$.
b) Cyklický kód s generujícími kořeny i a $i+1$ v tělese T má nejmenší délku $n = \mathrm{lcm}(\mathrm{r}(i), \mathrm{r}(i+1)) = 8$. Jeho generující polynom je $g(z) = m_i(z)m_{i+1}(z) = (z^2+1)(z^2+z+2) = z^4 + z^3 + z + 2$. Jeho kontrolní matice je

$$\mathbb{H} = \begin{pmatrix} (i+1)^7 & (i+1)^6 & (i+1)^5 & \ldots & (i+1) & 1 \\ i^7 & i^6 & i^5 & \ldots & i & 1 \end{pmatrix} \longleftrightarrow \mathbb{H} = \begin{pmatrix} 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\ 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \\ 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 \end{pmatrix}.$$

Opravíme ještě jednu chybu ve slově $\bar{w} = (1\ 1\ 0\ 0\ 0\ 0\ 2\ 1)$ pomocí dosazování kořenů.
$w(i) = i^7 + i^6 + 2i + 1 = 2i + 2 + 2i + 1 = i = a\ i^j = 1\ i^1 = 1\ i^5 = 2\ i^3 = 2\ i^7$
$w(i+1) = (i+1)^7 + (i+1)^6 + 2(i+1) + 1 = (i+2) + i + 2(i+1) + 1 = i + 2 = a\ (i+1)^j = 1\ (i+1)^7 = 2\ (i+1)^3$
Chybový polynom je určen jednoznačně, jediná možnost odpovídající oběma kořenům je $e(z) = 2\ z^3$. Opravíme $v(z) = w(z) - e(z)$, tedy $\bar{v} = (1\ 1\ 0\ 0\ 1\ 0\ 2\ 1)$.

8.9 Otázka č. 2. Máme cyklický kód K délky n nad $\mathbb{Z}_p$. V jakém tělese T lze najít jeho generující kořeny? Musí takové těleso vždy existovat?

Hledáme tedy rozšíření T tělesa $\mathbb{Z}_p$, ve kterém by měl generující polynom $g(x)$ stupně m celkem m různých kořenů. Víme, že generující polynom $g(x)$ je dělitelem polynomu $x^n - 1$ nad $\mathbb{Z}_p$. Pokusíme se tedy najít těleso T charakteristiky p, tedy nějaké $GF(p^k)$, nad kterým by se polynom $x^n - 1$ rozkládal na kořenové činitele (s jednonásobnými kořeny).

V tělese T o p^k prvcích má polynom $x^n - 1$ celkem n různých kořenů právě, když je n dělitelem počtu prvků cyklické grupy T^*, tedy když $n \mid p^k - 1$. Kořeny jsou pak všechny prvky n-prvkové podgrupy generované prvkem β řádu n a mají tvar β^i pro $1 \leq i \leq n$. Hledáme tedy k tak, aby $n \mid p^k - 1$. Přitom

$$n \mid p^k - 1 \qquad \text{iff} \qquad p^k - 1 = 0 \ \text{ v } \ \mathbb{Z}_n \qquad \text{iff} \qquad p^k = 1 \ \text{ v } \ \mathbb{Z}_n$$

Takové k lze najít jenom, když p není dělitelem čísla n. Z rovnosti $p^k = 1$ lze totiž spočítat inverzní prvek k prvku p, konkrétně $p^{-1} = p^{k-1}$ v $\mathbb{Z}_n$. Víme, že v $\mathbb{Z}_n$ jsou invertibilní pouze prvky nesoudělné s n, takže p musí být nesoudělné s n, což pro prvočíslo p nastane právě, když $p \nmid n$.

Dostáváme podmínku $p \nmid n$, bez níž bychom nemohli vyřešit naši úlohu - nemohli bychom najít těleso těleso T o p^k prvcích, v němž má polynom $x^n - 1$ celkem n různých kořenů. Podíváme-li se na to z druhé strany, tak pro $n = mp$ lze v tělese T charakteristiky p rozložit polynom $x^n - 1 = x^{mp} - 1 = (x^m - 1)^p$. Tudíž všechny jeho kořeny budou aspoň p-násobné a nebude n různých kořenů.

Pokud $p \nmid n$, pak naši úlohu skutečně vyřešíme. Euler-Fermatova věta tvrdí:

$$\text{Když } \ p \nmid n, \ \text{ pak } \ p^{\varphi(n)} = 1 \ \text{ v } \ \mathbb{Z}_n.$$

Můžeme tedy volit $k = \varphi(n)$, pak v tělese $GF(p^{\varphi(n)})$ bude mít polynom $x^n - 1$ celkem n různých kořenů.
Mohou ale existovat i menší tělesa, která řeší naši úlohu. To nejmenší k, které splňuje $p^k = 1$ v grupě invertibilních prvků $\mathbb{Z}_n^*$, je vlastně řád prvku p v této grupě, $k = \mathrm{r}(p)$ v $\mathbb{Z}_n^*$. Dokonce víme:

$$p^k = 1 \ \text{ v } \ \mathbb{Z}_n^* \quad \text{právě, když} \quad \mathrm{r}(p) \mid k$$

Těles $GF(p^k)$, v nichž má polynom $x^n - 1$ celkem n různých kořenů, je tedy nekonečně mnoho (za předpokladu, že $p \nmid n$).

Shrňme naše úvahy do následujícího tvrzení:

8.10 Tvrzení *Nechť K je cyklický kód délky n nad $\mathbb{Z}_p$ s generujícím polynomem $g(z)$ stupně m a nechť $p \nmid n$. Položme $k = \varphi(n)$ (anebo $k = \mathrm{r}(p)$ v grupě $\mathbb{Z}_n^*$). Pak v tělese $GF(p^k)$ má generující polynom $g(z)$ právě m různých kořenů tvaru $\beta^{i_1}, \beta^{i_2}, \ldots, \beta^{i_m}$ pro nějaký prvek β řádu n v tělese $GF(p^k)$ (aneb nalezneme je mezi kořeny polynomu $x^n - 1$). Tyto kořeny jsou generujícími kořeny cyklického kódu K.*

8.11 Příklad Cyklický kód K délky 4 nad $\mathbb{Z}_7$ má generující polynom $g(z) = z^2 + 1$. Jeho generující kořeny budeme hledat v tělese $GF(7^k)$, kde $k = \varphi(4) = 2$. Zkonstruujeme těleso $GF(49)$, $T = \mathbb{Z}_7[x]/q(x)$, kde $q(x)$ bude ireducibilní nad $\mathbb{Z}_7$ stupně 2. Najdeme jeho primitivní prvek (označme ho α, aneb $\mathrm{r}(\alpha) = 48$) a dopočteme prvek řádu $n = 4$ (označme ho $\beta = \alpha^{12}$). Generující kořeny kódu K budou dva z prvků β, β^2, β^3 a $\beta^4 = 1$, určíme je dosazováním.

BCH-kódy

Pokud budeme volit kořeny "šikovně", můžeme zaručit opravování předem daného množství chyb. Následující konstrukci vymysleli pánové Bose a Ray-Chaudhuri a nezávisle na nich pan Hocquenghem.

8.12 Definice *BCH-kód* délky n nad $\mathbb{Z}_p$ ($p \nmid n$) *s plánovanou vzdáleností* d ($d \leq n$) je cyklický kód s generujícími kořeny $\beta, \beta^2, \beta^3, \ldots, \beta^{d-1}$, kde β je prvek řádu n v nějakém tělese $GF(p^k)$.

8.13 Tvrzení *BCH-kód K délky n nad $\mathbb{Z}_p$ s plánovanou vzdáleností d má skutečnou Hammingovu vzdálenost kódu $d_H(K) \geq d$.*

Tudíž BCH-kód s plánovanou vzdáleností d objevuje $(d-1)$ chyb a opravuje $[\frac{d-1}{2}]$ chyb.

8.14 Poznámka Pro vytvoření BCH-kódu nad $\mathbb{Z}_p$ s plánovanou vzdáleností d není vždy nutné vyžadovat všechny kořeny $\beta, \beta^2, \ldots, \beta^{d-1}$. Kódové polynomy jsou polynomy nad $\mathbb{Z}_p$ a tudíž musí mít v tělese charakteristiky p s kořenem c, také kořeny c^p, $c^{(p^2)}$, atd. Speciálně pro BCH-kódy nad $\mathbb{Z}_2$ s (lichou) plánovanou vzdáleností d stačí požadovat kořeny $\beta, \beta^3, \beta^5, \ldots, \beta^{d-2}$, neboť potom prvky $\beta^2, \beta^4, \beta^6, \ldots, \beta^{d-1}$ budou také kořeny daného kódu.

8.15 BCH-kódy nad $\mathbb{Z}_p$ délky $n = p^k - 1$: Má-li BCH-kód nad $\mathbb{Z}_p$ délku $n = p^k - 1$, pak je kořen β primitivním prvkem v tělese $GF(p^k)$ (kde $p^k = n + 1$). Vždy lze zvolit ireducibilní polynom $q(x)$ stupně k tak, aby kořen α tohoto polynomu byl primitivním prvkem tělesa $T = \mathbb{Z}_p[x]/q(x)$, jehož prvky zapisujeme jako polynomy stupně nejvýše $k-1$ v proměnné α. Provedeme-li takovouto konstrukci tělesa $GF(p^k)$, pak volíme za kořen $\beta = \alpha$.

BCH-kódy nad $\mathbb{Z}_p$ délky $n = p^k - 1$ s jediným generujícím kořenem α v tomto tělese budou mít generující polynom $g(z) = m_\alpha(z) = q(z)$ a jejich kontrolní matice $\mathbb{H} = \begin{pmatrix} \alpha^{n-1} & \alpha^{n-2} & \ldots & \alpha & 1 \end{pmatrix}$ nad T obsahuje všechny nenulové prvky tělesa T. Tudíž kontrolní matice $\mathbb{H}$ nad $\mathbb{Z}_p$ má ve sloupcích všechny nenulové k-tice nad $\mathbb{Z}_p$. Každé dva sloupce matice $\mathbb{H}$ jsou lineárně nezávislé právě, když pracujeme nad $\mathbb{Z}_2$ (neboť nad $\mathbb{Z}_p$, $p > 2$, jsou v $\mathbb{H}$ sloupce S a $2S$, které jsou různé, ale lineárně závislé). Tedy BCH-kódy nad $\mathbb{Z}_2$ opravují jednu chybu a mají Hammingovu vzdálenost $d_H(K) = 3$. Ale to není překvapující, neboť kódové polynomy nad $\mathbb{Z}_2$ mají v tělese charakteristiky 2 s kořenem α také kořen α^2 (a α^4, atd.), tedy dvě po sobě jdoucí mocniny prvku α, a jsou to vlastně BCH-kódy s plánovanou vzdáleností $d = 3$. BCH-kód nad $\mathbb{Z}_2$ délky $n = 2^k - 1$ s jedním kořenem je tudíž **cyklický Hammnigův kód** o k kontrolních znacích.

BCH-kódy nad $\mathbb{Z}_2$ délky $n = p^k - 1$ s generujícími kořeny $\alpha, \alpha^3, \alpha^5, \ldots, \alpha^{2t-1}$ ve výše zkonstruovaném tělese, jsou podprostory Hammingových kódů. Opravují t chyb a mají velmi dobrý informační poměr ("relativně malou" redundanci). Jsou pro ně také vypracovány metody, jak opravovat vícenásobné chyby pomocí kořenů.

8.16 Příklad Cyklický kód délky $n = 7$ opravující dvě chyby má Hammingovu vzdálenost $d_H(K) = 5$. Vyrobíme BCH-kód s plánovanou vzdáleností $d = 5$. Použijeme těleso $GF(2^3) = GF(8)$, například těleso $T = \mathbb{Z}_2[x]/x^3 + x + 1 = \{a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}_2,\ \alpha^3 = \alpha + 1\}$, které má primitivní prvek α. Za kořeny volíme prvky α a $\alpha^3 = \alpha + 1$.

Kontrolní matice nad T, resp. nad $\mathbb{Z}_2$ je

$$\mathbb{H} = \begin{pmatrix} \alpha^6 & \alpha^5 & \dots & \alpha & 1 \\ (\alpha+1)^6 & (\alpha+1)^5 & \dots & (\alpha+1) & 1 \end{pmatrix} \longleftrightarrow \mathbb{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Generující polynom je (viz předchozí kapitola)

$$g(z) = m_\alpha(z) m_{\alpha+1}(z) = (z^3 + z + 1)(z^3 + z^2 + 1) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1.$$

Jde o opakovací kód délky 7 a jeho skutečná Hammingova vzdálenost je $d_H(K) = 7$, tedy větší než plánovaná vzdálenost $d = 5$.

8.17 BCH-kódy nad $\mathbb{Z}_p$ délky $n \neq p^k - 1$: Má-li BCH-kód nad $\mathbb{Z}_p$ délku $n \neq p^k - 1$, pak je β prvkem řádu n v tělese $GF(p^k)$, kde volíme $k = \varphi(n)$ (anebo $k = \mathrm{r}(p)$ v grupě $\mathbb{Z}_n^*$). Tato volba zafunguje kdykoli $p \nmid n$ (viz odpověď na otázku č.2).

8.18 Příklad BCH-kód délky $n = 9$ nad $\mathbb{Z}_2$ s plánovanou vzdáleností $d = 3$ bude mít za kořen prvek β řádu $\mathrm{r}(\beta) = 9$ v tělese $GF(2^{\varphi(9)}) = GF(2^6) = GF(64)$. Menší těleso $GF(2^k)$ obsahující prvek řádu 9 nenajdeme, protože $\mathrm{r}(2) = 6$ v grupě $\mathbb{Z}_9^*$. Toto těleso sestrojíme jako $\mathbb{Z}_2[x]/q(x)$, kde $q(x)$ bude polynom šestého stupně ireducibilní nad $\mathbb{Z}_2$. Prvky tělesa budou polynomy nejvýše pátého stupně zapsané v proměnné α a přepisovací pravidla budou dána vztahem $q(\alpha) = 0$. V tělese najdeme primitivní prvek, při šikovné volbě ireducibilního polynomu $q(x)$ bude primitivním prvkem přímo prvek α a $\mathrm{r}(\alpha) = 63$. Potom generujícím kořenem našeho BCH-kódu bude prvek $\beta = \alpha^7$, neboť $\mathrm{r}(\beta) = \mathrm{r}(\alpha^7) = 9$.