Domácí úkol č. 7 - Generující kořeny cyklických kódů a BCH kódy

1. Je dáno těleso $GF(25)$, $T = \mathbb{Z}_5[x]/q(x)$, kde $q(x) = x^2+x+1$. Prvky tototo tělesa budeme označovat jako polynomy v proměnné α.

   a) Najděte cyklický kód nejmenší možné délky s generujícím kořenem α v tělese T. Napište jeho generující polynom a jeho kontrolní matici.

   b) Ověřte, že prvek $(\alpha + 2)$ je primitivním prvkem v tělese T. Napište generující polynom pro cyklický kód délky 24 nad $\mathbb{Z}_5$ s generujícím kořenem $(\alpha + 2)$. Opravuje tento kód jednu chybu?

   c) Najděte nějaký BCH kód nad $\mathbb{Z}_5$ délky 24, který opravuje jednu chybu. Napište jeho generující polynom.

2. Je dáno těleso $GF(25)$, $T = \mathbb{Z}_5[x]/q(x)$, kde $q(x) = x^2+x+1$. Prvky tototo tělesa budeme označovat jako polynomy v proměnné α. Prvek $(\alpha + 2)$ je primitivním prvkem v tělese T.

   a) Najděte v tělese T generující kořeny pro cyklický kód K délky 6 nad $\mathbb{Z}_5$ s generujícím polynomem $g(z) = z^3 + 3z^2 + 2z + 4$. (Ověřte, že to jde.)

   b) Dokažte, že tento kód K je BCH kód opravující jednu chybu. Opravte pomocí jeho generujících kořenů chybu ve slově $\bar{w} = (1\,0\,4\,0\,4\,3)$.

3. Najděte nějaký BCH-kód nad $\mathbb{Z}_2$ délky n, který opravuje dvě chyby, pro i) $n = 15$, ii) $n = 9$, iii) $n = 21$.

   a) Jaké těleso $GF(p^s)$ budete používat? Jak najít generující kořeny kódu?

   b) Jakého stupně bude generující polynom? Určete informační poměr $k : n$.

   c) Případně najděte generující polynom.

4. Popište parametry binárních BCH kódů délky $n = 63$.

   Pro plánované vzdálenosti $d = 3, 5, \ldots, 2t + 1 \leq 63$ (tj. pro kódy opravující $1, 2, \ldots, t \leq 31$ chyb) určete počet kontrolních znaků a počet informačních znaků.

Výsledky

1. a), b) viz domácí úkol č. 6

   c) BCH-kód má opravovat 1 chybu, tudíž jeho plánovaná vzdálenost bude $d = 3$ a jeho generující kořeny budou β a β^2, kde $\mathrm{r}(\beta) = n = 24$ v nějakém tělese $GF(5^k)$, tedy stačí $GF(25)$.

   Můžeme použít těleso T a za β vzít jeho primitivní prvek $\alpha + 2$. Pak $\beta^2 = 3\alpha + 3$ a generující polynom $g(z) = m_{\alpha+2}(z)m_{3\alpha+3}(z) = (z^2 + 2z + 3)(z^2 + 2z + 4) = z^4 + 4z^3 + z^2 + 4z + 2$.

2. a) viz domácí úkol č. 6

   b) Generujícími kořeny jsou prvky $-\alpha$, $\alpha + 1 = (-\alpha)^5$ a $1 = (-\alpha)^6$, kde $\mathrm{r}(-\alpha) = 6$, jedná se tedy o BCH kód (v širším smyslu) s plánovanou vzdáleností $d = 3$. Kód tudíž opravuje jednu chybu.

   K opravování použijeme např. kořeny 1 a $-\alpha$ (taktéž lze použít 1 a $\alpha+1$). Tabulka pro mocniny $-\alpha$: $(-\alpha)^1 = -\alpha$, $(-\alpha)^2 = -\alpha - 1$, $(-\alpha)^3 = -1$, $(-\alpha)^4 = \alpha$, $(-\alpha)^5 = \alpha + 1$, $(-\alpha)^6 = 1 = (-\alpha)^0$. Dosazovat je budeme do polynomu $w(z) = z^5 + 4z^3 + 4z + 3$.

   $w(-\alpha) = 2\alpha$, což je na mocniny prvku $-\alpha$ přepsatelné dvěma způsoby: $w(-\alpha) = 2\alpha = 2(-\alpha)^4$ nebo $w(-\alpha) = 3(-\alpha) = 3(-\alpha)^1$.

   $w(1) = 2$, což je na mocniny prvku 1 přepsatelné šesti způsoby: $w(1) = 2 \cdot 1^i$, kde $0 \leq i \leq 5$ (neboť kódové polynomy mají stupeň nejvýše 5).

   Chybový polynom je $e(z) = 2z^4$ (to je jediná společná možnost). Oprava: $v(z) = w(z) - e(z) = z^5 + 3z^4 + 4z^3 + 4z + 3$, tedy poslané slovo je $\bar{v} = (1\,3\,4\,0\,4\,3)$.

3. BCH kód má opravovat 2 chyby, tudíž jeho plánovaná vzdálenost bude $d = 5$ a jeho generující kořeny budou β, β^2, β^3 a β^4, kde $\mathrm{r}(\beta) = n$ v nějakém tělese $GF(2^k)$. Těleso má charakteristiku 2 a kódové polynomy jsou celočíselné nad $\mathbb{Z}_2$, tudíž s kořenem β budou mít automaticky i kořeny β^2 a β^4. Aneb samotné prvky β a β^3 jsou také generujícími kořeny hledaného BCH kódu.

   Musíme najít těleso $GF(2^k)$ tak, aby v něm byl prvek řádu n.

   i) $n = 15 = 2^4 - 1$, stačí vzít těleso $GF(16)$ a za β primitivní prvek v něm.

   Např. $T = \mathbb{Z}_2[x]/(x^4 + x + 1) = \{a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0, a_i \in \mathbb{Z}_2, \alpha^4 = \alpha + 1\}$ je těleso a má primitivní prvek α.

   BCH kód bude mít generující kořeny α, α^3 v tomto tělese. Generující polynom $g(z) = m_\alpha(z)m_{\alpha^3}(z)$, kde $m_\alpha(z) = q(z) = z^4 + z + 1$. Polynom $m_{\alpha^3}(z)$ má v tělese charakteristiky 2 kořeny α^3, α^6, α^{12} a $\alpha^{24} = \alpha^9$ (víc ne, neboť $\alpha^{18} = \alpha^3$), tedy je také stupně 4. (Po pronásobení kořenových činitelů vyjde $m_{\alpha^3}(z) = z^4 + z^3 + z^2 + z + 1$.)

   Odtud $\mathrm{st}(g) = 8$, informační poměr $k : n = 7 : 15$.

   ii) Pro $n = 9$ chceme, aby $9|(2^k - 1)$, aneb aby $2^k = 1$ v $\mathbb{Z}_9$. Položíme $k = \varphi(9) = 6$, menší k neexistuje, neboť $\mathrm{r}(2) = 6$ v grupě $\mathbb{Z}_9^*$. Použijeme tedy nějaké $GF(64)$ a v něm prvek β řádu 9.

   Např. $T = \mathbb{Z}_2[x]/x^6 + x + 1 = \{t(\alpha) \in \mathbb{Z}_2[\alpha], \mathrm{st}(t) \leq 5, \alpha^6 = \alpha + 1\}$ je těleso a má primitivní prvek α (viz domácí úkol č.4).

   Pak generující kořeny v našem tělese jsou $\beta = \alpha^7 = \alpha^2 + \alpha$ a $\beta^3 = \alpha^{21} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$. Generující polynom $g(z) = m_\beta(z)m_{\beta^3}(z)$.

   Prvek β má řád 9 (aneb při umocňování počítáme v exponentu modulo 9), jeho minimální polynom $m_\beta(z)$ má v tělese charakteristiky 2 kořeny β, β^2, β^4, β^8, $\beta^{16} = \beta^7$, $\beta^{32} = \beta^5$ (víc ne, neboť $\beta^{64} = \beta$), je tedy šestého stupně. Dopočítávat ho nebudeme.

   Minimální polynom $m_{\beta^3}(z)$ pro prvek β^3 má kořeny β^3, $(\beta^3)^2 = \beta^6$ (víc ne, neboť $(\beta^3)^4 = \beta^{12} = \beta^3$), je tedy druhého stupně. Lze dopočítat: $m_{\beta^2}(z) = (z - \alpha^{21})(z - \alpha^{42}) = z^2 - (\alpha^{21} + \alpha^{42})z + \alpha^{63} = z^2 + z + 1$, neboť $\alpha^{21} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$ a $\alpha^{42} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha$.

   Odtud $\mathrm{st}(g) = 8$, informační poměr $k : n = 1 : 9$. Sestrojili jsme opakovací kód délky 9 nad $\mathbb{Z}_2$, který opravuje dokonce čtyři chyby.

   iii) Pro $n = 21$ chceme, aby $21|(2^k - 1)$, aneb aby $2^k = 1$ v $\mathbb{Z}_{21}$. Lze volit $k = \varphi(21) = 12$, ale stačí $k = \mathrm{r}(2) = 6$ v grupě $\mathbb{Z}_{21}^*$. Použijeme tedy opět $GF(64)$ jako výše a v něm prvek β řádu 21.

   Generující kořeny jsou $\beta = \alpha^3$ a $\beta^3 = \alpha^9 = \alpha^4 + \alpha^3$. Generující polynom je $g(z) = m_{\alpha^3}(z)m_{\alpha^9}(z)$ má stupeň 9, neboť jeden minimální polynom má stupeň 6 a jeden má stupeň 3 (ověřte si sami). Informační poměr $k : n = 12 : 21$.

4. Jedná se o primitivní BCH kódy, jejich generující kořeny lze najít v $GF(64) = GF(2^6)$.

   Pro $d < 2^{\frac{6}{2}} + 2 = 10$ je počet kontrolních znaků $m = 6 \cdot \frac{d-1}{2}$. (Přitom $\frac{d-1}{2}$ je počet nutných generujících kořenů = lichých mocnin primitivního prvku, tedy počet chyb, které kód opravuje.) Konkrétně BCH kód opravující jednu chybu má $m = 6$ a informační poměr $k : n = 57 : 63$, atd. až BCH kód opravující čtyři chyby má $m = 6 \cdot 4 = 24$ a informační poměr $k : n = 29 : 63$.

   Pro BCH kódy opravující více než čtyři chyby musíme dopočítat stupně minimálních polynomů dalších kořenů. Např. BCH kód opravující pět chyb má generující kořeny β, β^3, β^5, β^7, a β^9, kde β je primitivní prvek v nějakém $GF(2^6)$. Minimální polynomy pro β^i, kde i je liché a $i < 2^{\frac{6}{2}} = 8$ mají stupeň 6. Minimální polynom pro β^9 má další kořeny (v tělese charakteristiky 2) β^{18}, β^{36} (víc ne, neboť $\beta^{72} = \beta^9$), jeho stupeň je tedy 3. BCH kód opravující pět chyb má $m = 6 \cdot 4 + 3 = 27$ kontrolních znaků a informační poměr je $k : n = 26 : 63$.