Uma construção de códigos BCH *

Antonio Aparecido de Andrade†, Tariq Shah e Attiq Qamar‡

Resumo

Um código BCH C (respectivamente, um código BCH C') de comprimento n sobre o anel local $\mathbb{Z}_{p^k}$ (respectivamente, sobre o corpo $\mathbb{Z}_p$) é um ideal no anel $\frac{\mathbb{Z}_{p^k}[X]}{(X^n-1)}$ (respectivamente, no anel $\frac{\mathbb{Z}_p[X]}{(X^n-1)}$), que é gerado por um polinômio mônico que divide X^n-1. Shankar [1] mostrou que as raízes de X^n-1 são as unidades do anel de Galois $GR(p^k,s)$ (respectivamente, corpo de Galois $GF(p,s)$) que é uma extensão do anel $\mathbb{Z}_{p^k}$ (respectivamente, do corpo $\mathbb{Z}_p$), onde s é o grau de um polinômio irredutível $f(X)\in\mathbb{Z}_{p^k}[X]$. Neste estudo, assumimos que para $s_i=b^i$, onde b é um primo e i é um inteiro não negativo tal que $0\leq i\leq t$, existem extensões de anéis de Galois correspondentes $GR(p^k,s_i)$ (respectivamente, extensões do corpo de Galois $GF(p,s_i)$) do anel $\mathbb{Z}_{p^k}$ (respectivamente, do corpo $\mathbb{Z}_p$). Assim, $s_i=b^i$ para $i=2$ ou $s_i=b^i$ para $i>2$. De modo análogo a [1], neste trabalho, apresentamos uma seqüência de códigos BCH $C_0,C_1,\cdots,C_{t-1}C$ sobre $\mathbb{Z}_{p^k}$ de comprimentos $n_0,n_1,\cdots,n_{t-1},n_t$, e uma seqüência de códigos BCH $C'_0,C'_1,\cdots,C'_{t-1},C'$ sobre $\mathbb{Z}_p$ de comprimentos $n_0,n_1,\cdots,n_{t-1},n_t$, onde cada n_i divide $p^{s_i}-1$.

Palavras Chave: Anel de Galois, corpo de Galois, código BCH.

Introdução

É bem conhecido que as estruturas algébricas têm valiosas aplicações na teoria de códigos corretores de erros. Blake [2] obteve códigos cíclicos sobre $\mathbb{Z}_m$, onde m é da forma $\prod_{i=1}^{l}p_i$, e em [3] obteve as matrizes de verificação de paridade para esses códigos. Interlando e Palazzo [4] obteve a estrutura de ideais principais no anel $\frac{\mathbb{Z}_m[X]}{(X^n-1)}$, onde m,n são inteiros positivos. Spiegel [5], obteve códigos cíclicos sobre $\mathbb{Z}_m$, onde $m=\prod_{i=1}^{l}p_i^{k_i}$, a partir de códigos sobre $\mathbb{Z}_{p_i^{k_i}}$, que por sua vez são derivados de códigos sobre o corpo $\mathbb{Z}_{p_i}$, para $i=1,2,\cdots,l$. Posteriormente, Spiegel [6] obteve códigos BCH sobre o anel $\mathbb{Z}_{p^k}$ a partir de códigos BCH sobre corpos p-ádicos e suas classes residuais.

Um código BCH C (respectivamente, um código BCH C') de comprimento n sobre um anel local $\mathbb{Z}_{p^k}$ (respectivamente, sobre o corpo $\mathbb{Z}_p$), onde p e n são primos entre si, é um ideal no anel $\frac{\mathbb{Z}_{p^k}[X]}{(X^n-1)}$ (respectivamente, no anel $\frac{\mathbb{Z}_p[X]}{(X^n-1)}$), que é gerado por um polinômio mônico que divide X^n-1 no anel $\frac{\mathbb{Z}_{p^k}[X]}{(X^n-1)}$ (respectivamente, no

*Os autores agradecem o apoio da Fapesp 2007/56052-8 e 2011/03441-2 e também da Propg - Unesp.

†Departamento de Matemática, Ibilce - Unesp, São José do Rio Preto - SP, Brasil, andrade@ibilce.unesp.br

‡Departamento de Matemática, Universidade de Quaid-i-Azam, Islamabad, Paquistão, stariqshah@gmail.com, qamar.maths@gmail.com.

anel $\frac{\mathbb{Z}_p[X]}{(X^n-1)}$). Shankar [1] mostrou que as raízes de X^n-1 são as unidades do anel de Galois $R = GR(p^k, s)$ (respectivamente, do corpo de Galois $GF(p, s) = \mathbb{K}$) que é uma extensão do anel $\mathbb{Z}_{p^k}$ (respectivamente, do corpo $\mathbb{Z}_p$), onde s é o grau de um polinômio irredutível $f(X) \in \mathbb{Z}_{p^k}[X]$. O conjunto R^* denota o grupo multiplicativo das unidades de R e $\mathbb{K}^*$ o grupo multiplicativo do corpo $\mathbb{K}$. Shankar [1] mostrou que R^* possui um e apenas um subgrupo cíclico G_n de ordem n relativamente primo com p. Além disso, se $r_p(f) = \overline{f}$ gera um subgrupo cíclico de ordem n em $\mathbb{K}^*$, então f gera um subgrupo cíclico de ordem nd em R^*, onde d é um número inteiro maior ou igual a 1 e f^d gera o subgrupo cíclico G_n em R^* [1, Lema 1]. Alem disso, Shankar apresentou um algoritmo para a construção de códigos BCH com símbolos no anel local $\mathbb{Z}_{p^k}$ [1].

O presente trabalho estende a primeira parte de [1] de tal maneira que para $s = b^t$, onde b é um primo e t é um inteiro positivo, existem extensões de anéis de Galois $R_i = GR(p^k, s_i)$, onde $0 \leq i \leq t$ e $s_i = b^i$ (respectivamente, extensões de corpos de Galois $\mathbb{K}_i = GF(p, s_i)$, onde $0 \leq i \leq t$ e $s_i = b^i$), do anel $\mathbb{Z}_{p^k}$ (respectivamente, do corpo $\mathbb{Z}_p$). Para cada i, onde $0 \leq i \leq t$, segue que R_i^* possui um e apenas um subgrupo cíclico G_{n_i} de ordem n_i, que divide $p^{s_i}-1$ e relativamente primo com p [1, Teorema 2]. Além disso, se $\overline{f^i} = r_p(f^i)$ gera um subgrupo cíclico de ordem n_i em $\mathbb{K}_i^*$, então f^i gera um subgrupo cíclico de ordem $n_i d_i$ em R_i^*, onde d_i é um número inteiro maior ou igual a 1, e $(f^i)^{d_i}$ gera um subgrupo cíclico G_{n_i} em R_i^* para cada i [1, Lema 1]. Assim, nesse trabalho, estendemos o algoritmo dado por Shankar [1, p. 482] para a construção de um código BCH com símbolos em um anel local $\mathbb{Z}_{p^k}$ para cada membro de uma cadeia de anéis de Galois e corpos de Galois, respectivamente. Consequentemente, existem duas situações onde $s_i = b^i$ para $i = 2$ ou $s_i = b^i$ para $i > 2$. Assim, de modo semelhante a [1] obtemos uma seqüência de códigos BCH $C_0, C_1, \cdots, C_{t-1}C$ sobre o anel $\mathbb{Z}_{p^k}$ com comprimentos $n_0, n_1, \cdots, n_{t-1}, n_t$, e uma seqüência de códigos BCH $C'_0, C'_1, \cdots, C'_{t-1}, C'$ sobre o corpo $\mathbb{Z}_p$ com comprimentos $n_0, n_1, \cdots, n_{t-1}, n_t$.

1 Cadeias de códigos BCH

Seja o anel local finito $\mathbb{Z}_{p^k}$, onde p é um primo e k um inteiro positivo. Seja $f(X) \in \mathbb{Z}_{p^k}[X]$ um polinômio irredutível com grau $s = b^t$, onde b é um primo e t é um inteiro não negativo. Assim $R = \frac{\mathbb{Z}_{p^k}[X]}{(f(X))} = GR(p^k, s)$ é a extensão de Galois do anel $\mathbb{Z}_{p^k}$ e $\mathbb{K} = \frac{\mathbb{Z}_p[X]}{(f(X))} = GF(p, s) = GF(p^s)$ é a extensão de Galois de $\mathbb{Z}_p$. O próximo lema é muito importante para a construção de uma cadeia de anéis de Galois.

Lema 1 *[7, Lema XVI.7] Um subanel de $GR(p^k, s)$ é um anel de Galois da forma $GR(p^k, s')$, onde s' divide s. Por outro lado, se s' divide s, então $GR(p^k, s)$ possui uma cópia de $GR(p^k, s')$.*

Os elementos $1, b, b^2, \cdots, b^{t-1}, b^t$ são os únicos divisores de s e desse modo tomamos $s_0 = 1, s_1 = b, s_2 = b^2, \cdots, s_t = b^t = s$. Pelo Lema 1 existem polinômios irredutíveis $f_0(X), f_1(X), \cdots, f_t(X)$ com graus $s_0, s_1, \cdots, s_t$, respectivamente, de tal forma que podemos construir anéis de Galois $R_i = \frac{\mathbb{Z}_{p^k}[X]}{(f_i(X))} = GR(p^k, s_i)$, onde $0 \leq i \leq t$. Como s_i divide s_{i+1} para $0 \leq i \leq t$, segue, pelo Lema 1, que existe uma cadeia de anéis de Galois $R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq R_{t-1} \subseteq R$. Analogamente, $\mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_{t-1} \subseteq \mathbb{K}$ é uma cadeia de respectivos corpos de Galois, onde $\mathbb{K}_i = \frac{\mathbb{Z}_p[X]}{(f_i(X))} = GF(p, s_i) = GF(p^{s_i})$, com $0 \leq i \leq t$. Para cada i, onde $0 \leq i \leq t$,

seja R_i^* o grupo das unidades de R_i e $\mathbb{K}_i^*$ os grupos multiplicativos dos corpos $\mathbb{K}_i$. Nosso interesse é no subgrupo cíclico G_{n_i} de R_i^* para cada i, onde $0 \leq i \leq t$, cujos elementos são as raízes do polinômio $X^{n_i} - 1$ para algum inteiro positivo n_i.

Teorema 2 *[7, Lema XVI.7] Seja $\mathbb{Z}_{p^k} = R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq R_{t-1} \subseteq R$ uma sequência de anéis de Galois com correspondente cadeia $\mathbb{Z}_p = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_{t-1} \subseteq \mathbb{K}$ de corpos de Galois. Para cada i, onde $0 \leq i \leq t$, se $f^i(X)$ é um polinômio regular em $R_i[X]$ e que $r_p(f^i(X))$ possui uma raiz simples $\bar{a}^i$ em $\mathbb{K}_i$, então $f^i(X)$ possui uma e apenas uma raiz a^i tal que $r_p(a^i) = \bar{a}^i$.*

Os dois teoremas seguintes servem de base para a construção do subgrupos cíclicos G_{n_i}, para cada i tal que $0 \leq i \leq t$, que proporcionam um método para gerar esses subgrupos cíclicos.

Teorema 3 *[1, Teorema 3] Seja $\mathbb{Z}_{p^k} = R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq R_{t-1} \subseteq R$ uma cadeia de anéis de Galois com correspondente cadeia $\mathbb{Z}_p = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_{t-1} \subseteq \mathbb{K}$ de corpos de Galois. Para cada i, onde $0 \leq i \leq t$, seja ζ^i um gerador da cadeia de subgrupos cíclicos de ordem n_i em R_i^*. Assim, o polinômio $X^{n_i} - 1$ pode ser fatorado como $X^{n_i} - 1 = (X - \zeta^i)(X - (\zeta^i)^2) \cdots (X - (\zeta^i)^{n_i})$ se, e somente se, $\bar{\zeta}^i$ possui ordem n_i em $\mathbb{K}_i^*$.*

Um polinômio $a(X)$ que é um divisor de $X^{n_i} - 1$, onde $0 \leq i \leq t$, pode ser fatorado de modo único sobre $\mathbb{K}_i^*$. Decorre do Teorema 3 que a fatoração de $a(X)$ sobre G_{n_i} também é única, conforme o seguinte corolário.

Corolário 4 *[1, Corollary 1] Seja $\mathbb{Z}_{p^k} = R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq R_{t-1} \subseteq R$ uma cadeia de anéis de Galois com correspondente cadeia $\mathbb{Z}_p = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_{t-1} \subseteq \mathbb{K}$ de corpos de Galois. Para cada i, onde $0 \leq i \leq t$, seja $a^i(X) \in \mathbb{Z}_{p^k}[X]$ tal que divide $X^n - 1$ e que pode ser fatorado sobre o subgrupo cíclico G_{n_i} como $a^i(x) = (X - (\zeta^i)^{e_1})(X - (\zeta^i)^{e_2}) \cdots (X - (\zeta^i)^{e_{l_i}})$ se, e somente se, $\bar{a}^i(X)$ pode ser fatorado como $\bar{a}^i(X) = (X - (\bar{\zeta}^i)^{e_1})(X - (\bar{\zeta}^i)^{e_2}) \cdots (X - (\bar{\zeta}^i)^{e_{l_i}})$ sobre os corpos $\mathbb{K}_i$.*

Teorema 5 *[1, Teorema 4] Seja $\mathbb{Z}_{p^k} = R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq R_{t-1} \subseteq R$ uma cadeia de anéis de Galois com correspondente cadeia $\mathbb{Z}_p = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_{t-1} \subseteq \mathbb{K}$ de corpos de Galois. Para cada i, onde $0 \leq i \leq t$, se barζ^i gera um subgrupo cíclico de ordem n_i em $\mathbb{K}_i^*$, então ζ^i gera um subgrupo ciclico de ordem $n_i d_i$ em R_i^*, onde cada d_i é um número inteiro maior ou igual a 1 e $(\zeta^i)^{d_i}$ gera o subgrupo cíclico G_{n_i} de R_i^*.*

Teorema 6 *[7, Lema XVI.7] Para cada i, onde $0 \leq i \leq t$, se $\mathbb{Z}_{p^k} = R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq R_{t-1} \subseteq R$ é uma cadeia de anéis de Galois com correspondente cadeia $\mathbb{Z}_p = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_{t-1} \subseteq \mathbb{K}$ de corpos de Galois, então existe apenas uma cadeia $G_{n_0} \subseteq G_{n_1} \subseteq G_{n_2} \subseteq \cdots \subseteq G_{n_t}$ de subgrupos cíclicos maximais de $R_0^* \subseteq R_2^* \subseteq R_3^* \subseteq \cdots \subseteq R_t^*$, onde a ordem de cada G_{n_i} é $p^{s_i} - 1$, para $0 \leq i \leq t$, que é relativamente prima com p.*

Exemplo 1 *Como $f(X) = X^8 + X^4 + X^3 + X^2 + 1 \in \mathbb{Z}_8[X]$ é um polinômio irredutível com grau $s = 2^3$, segue que $f(X)$ é irredutível sobre $\mathbb{Z}_{2^3}$ e $\mathbb{Z}_2$. Portanto $R = \frac{\mathbb{Z}_{2^3}[X]}{(f(X))} = GR(2^3, 8)$ e $\mathbb{K} = \frac{\mathbb{Z}_2[X]}{(f(X))} = GF(2, 8) = GF(2^8)$ com correspondentes anéis e corpos de Galois, respectivamente. Os elementos 1, 2, 2^2, 2^3 são os únicos divisores de 8 e sejam $s_1 = 1$, $s_2 = 2$, $s_3 = 2^2$, $s_4 = 2^3$. Assim, existem polinômios irredutíveis $f_2(X) = X^2 - X + 1$, $f_3(X) = X^4 + X + 1$, $f_4(X) = f(X)$ em $\mathbb{Z}_8[X]$ com graus s_2, s_3, s_4, respectivamente, de modo que podemos constituir os anéis de*

Galois $R_i = \frac{\mathbb{Z}_{2^3}[X]}{(f_i(X))} = GR(2^3, s_i)$, *onde* $1 \leq i \leq 4$. *Como* s_i *divide* s_{i+1} *para todo* $1 \leq i \leq 4$, *segue que* $R_1 \subseteq R_2 \subseteq R_3 \subseteq R$. *De modo análogo,* $\mathbb{K}_i = \frac{\mathbb{Z}_2[X]}{(f_i(X))} = GF(2, s_i) = GF(2^{s_i})$, *onde* $1 \leq i \leq 4$, *ou seja,* $\mathbb{K}_1 = GF(2,1) = \mathbb{Z}_2$, $\mathbb{K}_2 = GF(2,2)$, $\mathbb{K}_3 = GF(2,4)$ *e* $\mathbb{K} = GF(2,8)$ *com* $\mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \mathbb{K}_3 \subseteq \mathbb{K}$. *Seja* $\{X\}$ *a classe de resíduos de* X *em* R. *Seja* $\zeta = \{X\}$ *tal que* $\bar{\zeta} = \{X\}$ *em* $\mathbb{K}$. *Assim,* $\bar{\zeta}$ *é uma raiz primitiva em* $\mathbb{K}^*$ *e* ζ *tem ordem igual a* $4 \times 255 = 1020$ *em* R^*. *Logo,* ζ^4 *é um elemento primitivo de* G_{255}, *e se* $\alpha = \zeta^4$, *então* $G_{255} = \{1, \alpha, \alpha^2, \cdots, \alpha^{255}\}$. *Agora, para o subgrupo cíclico* G_{15} *de* R_3^*, *como* 15 *divide* 255, *tomamos o elemento* α^{17} *de* G_{255} *que gera o subgrupo cíclico* G_{15} *de* R^*. *Se calcularmos* ζ^{68} *em* R_3^*, *então a ordem de* ζ^{68} *é também* 15. *Consequentemente,* $\alpha^{17} = \zeta^{68}$ *gera um subgrupo ciclico de ordem* 15, *ou seja,* $G_{15} = \{1, \alpha^{17}, \alpha^{34}, \alpha^{51}, \alpha^{68}, \alpha^{85}, \alpha^{102}, \alpha^{119}, \alpha^{136}, \alpha^{153}, \alpha^{170}, \alpha^{187}, \alpha^{204}, \alpha^{221}, \alpha^{238}\}$, *onde* α^{17} *é um elemento primitivo em* K_3^*. *Agora, como a ordem de* α^{17} *é* 15 *e* 15 *é divisível por* 3, *segue que o próximo subgrupo cíclico é gerado por* $(\alpha^{17})^5 = \alpha^{85}$, *isto é,* $G_2 = \{1, \alpha^{85}, \alpha^{170}\}$ *é um subgrupo de* R_2^*. *O próximo subgrupo cíclico de* R *é* $G_1 = \{1\}$. *Deste modo, obtemos uma cadeia de subgrupos cíclicos* $G_1 \subseteq G_3 \subseteq G_{15} \subseteq G_{255}$ *sobre* $R_1^* \subseteq R_2^* \subseteq R_3^* \subseteq R^*$.

Seja G_{n_i} o subgrupo cíclico maximal de ordem n_i de R_i^* para cada i, onde $0 \leq i \leq t$. Consideramos que todos os elementos de G_{n_i} são as raízes de $X^{n_i} - 1$. Note que $mdc(n, p) = 1 = mdc(n_i, p)$, para cada i tal que $0 \leq i \leq t$. Agora, para cada i tal que $0 \leq i \leq t$, para a construção de um código BCH sobre o anel R_i, seja $g_i(X)$ o polinômio gerador. Para cada i tal que $0 \leq i \leq t$, seja ζ_i o elemento primitivo de G_{n_i} no anel R_i. Assim, $\bar{\zeta}_i$ é um elemento primitivo de K_i^*. Seja $\bar{\zeta}_i = R_p(\zeta_i)$ o resto não negativo quando ζ_i é dividido por p. Agora, escolha $\zeta_i^{e_j}$, onde $1 \leq j \leq n_i$, como as raízes do polinômio $g_i(X)$ do subgrupo cíclico G_{n_i}. Assim, $g_i(X)$ divide $X^{n_i} - 1$. Seja $M_i^{e_j}(X)$, onde $1 \leq j \leq n - k$, o polinómio mínimal de $\zeta_i^{e_j}$. Assim, a construção de $g_i(X)$ é dada por

$$g_i(X) = mmc\{M_i^{e_j}(X) : 1 \leq j \leq n - k\}.$$

Desse modo, $g_i(X)$ é um polinômio gerador de um código BCH C_i sobre R_i. Uma vez que cada $g_i(X)$ possui raízes no subgrupo cíclico, segue que $g_i(X)$ deve dividir $g_{i+1}(X)$. Consequentemente, existem as duas situações $s_i = b^i$ para $i = 2$ ou $s_i = b^i$ para $i > 2$. Assim, de modo análogo a [1] obtemos uma seqüência de códigos BCH $C_0, C_1, \cdots, C_{t-1}, C$ sobre $\mathbb{Z}_{p^k}$ com comprimentos $n_0, n_1, \cdots, n_{t-1}, n_t$ (respectivamente, uma seqüência de códigos BCH $C_0', C_1', \cdots, C_{t-1}', C'$ sobre $\mathbb{Z}_p$ com comprimentos $n_0, n_1, \cdots, n_{t-1}, n_t$). Assim, $\bar{g}_i(X) = r_p(g_i(X)) = mmc\{m_i^{e_j}(X) : 1 \leq j \leq n - k\}$ gera um código BCH C_i' com símbolos em $\mathbb{Z}_p$, onde $m_i^{e_j}(X)$, para $1 \leq j \leq nk$, são os polinômios mínimais de $r_p(\zeta_i^{e_j})$.

Teorema 7 *Seja* $\mathbb{Z}_{p^k} = R_0 \subseteq R_1 \subseteq R_2 \cdots \subseteq R_{t-1} \subseteq R$ *uma cadeia de anéis de Galois com correspondente cadeia* $\mathbb{Z}_p = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \cdots \subseteq \mathbb{K}_{t-1} \subseteq \mathbb{K}$ *de corpos de Galois. Para cada* i, *onde* $0 \leq i \leq t$, *seja* $g_i(X)$ *um polinômio gerador de um código cíclico de comprimento* n_i *com símbolos em* $\mathbb{Z}_{p^k}$. *Sejam* $\alpha_i^{e_{i_1}}, \alpha_i^{e_{i_2}}, \alpha_i^{e_{i_3}} \cdots \alpha_i^{e_{i_{n_i-k}}}$ *as raízes de* $g_i(X)$ *no subgrupo cíclico* G_{n_i}, *onde* α_i *tem ordem* n_i. *Assim, a distância mínima do código é maior do que o maior número de inteiros consecutivos módulo* n_i *no conjunto* $F_i = \{e_{i_1}, e_{i_2}, e_{i_3}, \cdots, e_{i_{n_i-k}}\}$.

Demonstração: Seja a cadeia de códigos gerados por $g_i(X)$ com símbolos em Z_{p^k}, denotados por C_i, e seja a cadeia de códigos gerados por $r_p(g_i(X))$ com símbolos em Z_p, dentotados por $\bar{C}_i$. Assim, podemos ver que todo $v_i(X)$ de $C_i, r_p(v_i(X))$ pertence $\bar{C}_i$. Seja d_i o número de inteiros consecutivos modulo n_i nos cojuntos

F_i. Assumimos que a distância mínima de C_i é menor que $d_i + 1$. Seja $r_i(X)$ em C_i tal que as n_i-uplas r_i tem peso de Hamming menor que $d_i + 1$. Assim, se $r_p(r_i(X)) = \overline{r_i}(X)$, então o peso de Hamming do vetor $\overline{r_i}$ é menor que $d_i + 1$. Mas, $r_p(g_i(X))$ possui como raízes d_i potências consecutivas de $r_p(\alpha_i)$, e portanto pelo limitante BCH dos códigos $\bar{C}_i$, segue que possui distância mínima no mínimo $d_i + 1$. Portanto, a distância mínima de C_i deve ser no mínimo $d_i + 1$.

2 Algoritmo

De modo análogo a [1] apresentamos um algoritmo para a construção de códigos BCH correspondentes à cadeia $R_0 \subseteq R_2 \subseteq R_3 \subseteq \cdots \subseteq R_t \subseteq R$ de anéis de Galois sobre $\mathbb{Z}_{p^k}$.

1. Escolha polinômios irredutíveis $f_i(X)$ sobre $\mathbb{Z}_{p^k}$ de grau b^i para cada i, onde $0 \leq i \leq t$, que são também irredutíveis sobre $GF(p)$ e forme a cadeia de anéis de Galois

$$\begin{aligned} \mathbb{Z}_{p^k} &= GR(p^k, 1) \subset GR(p^k, b) \subset \cdots \subset GR(p^k, b^{t-1}) \subset GR(p^k, s) \\ &= R_0 \subset R_1 \subset R_2 \cdots \subset R_{t-1} \subset R \end{aligned}$$

   e sua correspondente cadeia de corpos de Galois

$$\begin{aligned} \mathbb{Z}_p &= GR(p, 1) \subset GR(p, b) \subset \cdots \subset GR(p, b^{t-1}) \subset GR(p, s) \\ &= \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \cdots \subset \mathbb{K}_{t-1} \subset \mathbb{K}, \end{aligned}$$

   onde cada $GR(p, b^t) \simeq GF(p^{b^t})$.

2. Para cada i, onde $0 \leq i \leq t$, seja $\bar{\zeta}^i = r_p(\zeta^i)$ um elemento primitivo em $\mathbb{K}_i^*$. Se ζ^i possui ordem $d_i(p^{s_i} - 1)$ em R_i^* para alguns inteiros d_i, então $(\zeta^i)^{d_i}$ gera $G_{p^{s_i}-1}$. Suponha, para cada i onde $0 \leq i \leq t$, que α_i é um elemento de $G_{p^{s_i}-1}$.

3. Para cada i onde $0 \leq i \leq t$, se $\alpha_i^{e_{i_1}}, \alpha_i^{e_{i_2}}, \alpha_i^{e_{i_3}} \cdots \alpha_i^{e_{i_{n_i-k}}}$ são as raízes de $G_i(X)$, então encontre $M_i^{e_j}(X)$, para $j = 1, 2, 3, \cdots, n_i - k$, e os $g_i(X)$ são dados por $g_i(X) = mmc\{M_i^{e_j}(X) : 1 \leq j \leq n - k\}$, onde $\alpha_i^{e_{i_j}} = (\zeta^i)^{d_i e_{i_j}}$. O comprimento de cada código na cadeia é o mínimo múltiplo comum das ordens de $\alpha_i^{e_{i_1}}, \alpha_i^{e_{i_2}}, \alpha_i^{e_{i_3}} \cdots \alpha_i^{e_{i_{n_i-k}}}$, e à distância mínima do código é maior do que o maior número de inteiros consecutivos no conjunto $F_i = \{e_{i_1}, e_{i_2}, e_{i_3}, \cdots, e_{i_{nk}}\}$ para cada i, onde $0 \leq i \leq t$.

Exemplo 2 *Iniciamos pela construção de uma cadeia de códigos sobre o anel finito* $\mathbb{Z}_4$ *de comprimentos* 1, 3 *e* 15, *respectivamente. Seja* $f(X) = X^4 + X + 1 \in \mathbb{Z}_4[X]$ *um polinômio irredutível de grau* $s = 2^2$. *Assim,* $f(X)$ *é irredutível sobre* $\mathbb{Z}_{2^2}$ *e sobre* $\mathbb{Z}_2$. *Seja* $R = \frac{\mathbb{Z}_{2^2}[X]}{(f(X))} = GR(2^2, 4)$ *o anel de Galois e* $\mathbb{K} = \frac{\mathbb{Z}_2[X]}{(f(X))} = GF(2, 4) = GF(2^4)$ *o corpo de Galois correspondente. Os elementos* 1, 2 *e* 2^2 *são os únicos divisores de* 4 *e, portanto, sejam* $s_1 = 1$, $s_2 = 2$, $s_3 = 2^2$. *Logo, existem polinômios irredutíveis* $f_1(X)$, $f_2(X) = X^2 - X + 1$ *and* $f_3(X) = f(X)$ *em* $Z_4[X]$ *com graus* s_1, s_2 *e* s_3, *respectivamente, de tal forma que podemos formar os anéis de Galois* $R_i = \frac{\mathbb{Z}_{2^2}[X]}{(f_i(X))} = GR(2^2, s_i)$, *onde* $1 \leq i \leq 3$. *Como* s_i *divide* s_{i+1} *para todo* $1 \leq i \leq 3$, *segue que* $R_1 \subseteq R_2 \subseteq R$. *Novamente, pelo mesmo argumento, segue que* $\mathbb{K}_i = \frac{\mathbb{Z}_2[X]}{(f_i(X))} = GF(2, s_i) = GF(2^{s_i})$, *onde* $1 \leq i \leq 3$. *Logo,* $\mathbb{K}_1 = GF(2, 1) = Z_2$, $\mathbb{K}_2 = GF(2, 2)$ *e* $\mathbb{K} = GF(2, 4)$ *com* $\mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \mathbb{K}$. *Agora, seja* $\{X\}$ *a classe residual de* X *em* R. *Seja* u *em* R *tal que* $\overline{u} = \{X\}$ *está em* $\mathbb{K}$. *Assim,* $\overline{u} + 1$ *é um elemento primitivo em* $\mathbb{K}^*$ *e* $u + 11$ *possui ordem* 30 *em* R^*. *Assim,* $(u + 1)^2 = u^2 + 2u + 1$ *é*

um um elemento primitivo de G_{15} *e* $\alpha = (u+1)^2$. *Logo,* $G_{15} = \{1, \alpha, \alpha^2, \cdots, \alpha^{14}\}$ *e os elementos de* G_{15} *são dados por*

$$\begin{array}{ll}
\alpha = u^2 + 2u + 1 & \alpha^2 = 2u^2 + 3u \\
\alpha^3 = 3u^3 + u + 2 & \alpha^4 = u^2 \\
\alpha^5 = 2u^3 + u^2 + 3u + 3 & \alpha^6 = 3u^3 + 2u + 2 \\
\alpha^7 = u^3 + 3u^2 + u & \alpha^8 = 3u + 3 \\
\alpha^9 = 3u^3 + u^2 + u + 3 & \alpha^{10} = 2u^3 + 3u^2 + u \\
\alpha^{11} = u^3 + 3u^2 + 1 & \alpha^{12} = 3u^3 + 3u^2 \\
\alpha^{13} = u^3 + 3 & \alpha^{14} = u^3 + 2u^2 + 3u + 1.
\end{array}$$

Agora, para o subgrupo cíclico G_3 *de* R_2^*, *sabemos que* 3 *divide* 15 *e o resto é* 5. *Desse modo, seja o elemento* α^5 *de* G_{15} *o gerador do subgrupo cíclico* G_3 *de* R_2^*. *Como* $\alpha^5 = (u+1)^{10}$, *segue que o valor de* $(u+1)^{10}$ *em* R_2^* *é* $u+3$. *Assim,* $\alpha^5 = (u+1)^{10} = u+3$. *A ordem de* 3 *também é* 3. *Logo,* $G_3 = \{1, \alpha^5, \alpha^{10}\}$ *com* $\overline{u}+3$ *sendo primitivo em* $\mathbb{K}_2^*$. *Agora, a ordem de* α^5 *é* 3 *e* 3 *é divisível por* 1. *Assim, o próximo subgrupo cíclico é gerado por* $\alpha^{5\times 3} = 1$, *e portanto,* $G_1 = \{1\}$. *Logo, obtemos uma cadeia de subgrupos cíclicos maximais* $G_1 \subset G_3 \subset G_{15}$ *na cadeia* $R_1^* \subset R_2^* \subset R^*$. *Sejam* $\alpha = (u+1)^2$, $\zeta_2 = (u+1)^{10}$ *e* $\zeta_1 = (u+1)^{30} = 1$ *tal que* $\overline{\alpha} = \overline{u}+1$, $\bar{\zeta}_2 = (\overline{u}+1)^{10}$ *e* $\bar{\zeta}_1 = (\overline{u}+1)^{30} = 1$. *Assim,* α, ζ_2 *e* ζ_1 *são elementos primitivos de* G_{15}, G_3 *e* G_1 *tal que* $\overline{\alpha}$, $\bar{\zeta}_2$ *e* $\bar{\zeta}_1$ *são elementos primitivos em* $\mathbb{K}^*$, $\mathbb{K}_2^*$ *e* $\mathbb{K}_1^*$, *respectivamente. Para cada* C_1 *em* R_1 *segue que* $R_1^* = \{1, 3\}$, $\mathbb{K}_1^* = \{1\}$ *e* $G_1 = \{1\}$. *Portanto, um polinômio gerador é* $g_1(X) = X - 1$. *Assim,* $g_1(X) = X + 3$ *e* $\bar{g}_1(X) = X + 1$. *Similarmente, para* $g_2(X)$, *segue que* $\bar{\zeta}_2$ *é um elemento primitivo de* $\mathbb{K}_2^*$, $G_3 = \{1, \zeta_2, \zeta_2^2\}$ *e* $g_2(X) = (X - \zeta_2)(X - \zeta_2^2) = X^2 + X + 1$. *Isto implica que* $\bar{g}_2(X) = X^2 + X + 1$. *Agora, sabemos que* $G_{15} = \{1, \alpha, \alpha^2, \cdots, \alpha^{14}\}$ *e para um polinômio gerador* $g(X)$ *que tem* α *como raiz, segue que* $\alpha, \alpha^2, \alpha^{2^2}, \cdots$ *tem os mesmos polinômios minimais, e assim*

$$\begin{aligned}
M_1(X) &= (X - \alpha^3)(X - \alpha^6)(X - \alpha^9)(X - \alpha^{12}) \\
&= X^4 + X^3 + X^2 + X + 1.
\end{aligned}$$

Agora, $\alpha^3, (\alpha^3)^2, (\alpha^3)^{2^2}, (\alpha^3)^{2^3}, \cdots$ *tem os mesmos polinômios minimais, e assim*

$$\begin{aligned}
M_2(X) &= (X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8) \\
&= X^4 + X^2 + 3X + 1.
\end{aligned}$$

Similarmente, $\alpha^5, (\alpha^5)^2, (\alpha^5)^{2^2}, (\alpha^5)^{2^3}, \cdots$ *tem os mesmos polinomios minimais, e assim*

$$M_3(X) = (X - \alpha^5)(X - \alpha^{10}) = X^2 + X + 1.$$

Também, $\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$ *tem os mesmos polinomios minimais, e assim*

$$\begin{aligned}
M_4(X) &= (X - \alpha^7)(X - \alpha^{11})(X - \alpha^{13})(X - \alpha^{14}) \\
&= X^4 + 3X^2 + X + 1.
\end{aligned}$$

Portanto,

$$\begin{aligned}
g(X) &= lcm\{M_1(X), M_2(X), M_3(X), M_4(X)\} \\
&= M_1(X)M_2(X)M_3(X)M_4(X).
\end{aligned}$$

Deste modo, o código BCH C *sobre* R *generado por* $g(X)$ *possui comprimento* 15. *Portanto, correspondendo a cadeia* $R_1 \subset R_2 \subset R$, *existem códigos BCH* C_1, C_2 *e* C *com comprimentos* 1, 3 *e* 15, *respectivamente. Além disso,*

$$\begin{aligned}
&\bar{g}_1(X) = r_2(g_1(X)) = g_1(X) \\
&\bar{g}_2(X) = r_2(g_2(X)) = g_2(X) \\
&\bar{g}(X) = r_2(g(X)) = r_2(M_1(X))r_2(M_2(X))r_2(M_3(X))r_2(M_4(X)) \neq g(X)
\end{aligned}$$

geram os códigos BCH $\bar{C}_1$, $\bar{C}_2$ *e* $\bar{C}$ *com símbolos em* $GF(2)$, $GF(2^2)$ *e* $GF(2^4)$, *respectivamente. Também, as distâncias de Hamming mínima dos códigos* C_1, C_2 *e* C *são* 1, 3 *e* 15, *respectivamente.*

3 Conclusão

Com base no trabalho de Shankar [1] sobre a construção de códigos BCH com símbolos em um anel local $\mathbb{Z}_{p^k}$ e no corpo $\mathbb{Z}_p$, para cada membro de uma cadeia de anéis de Galois e de corpos de Galois, respectivamente, obtemos uma seqüência de códigos BCH $C_0, C_1, \cdots, C_{t-1}, C_t$ sobre $\mathbb{Z}_{p^k}$ com comprimentos $n_0, n_1, \cdots, n_{t-1}, n_t$ e uma seqüência de códigos BCH $C'_0, C'_1, \cdots, C'_{t-1}, C'_t$ sobre $\mathbb{Z}_p$ com comprimentos $n_0, n_1, \cdots, n_{t-1}, n_t$. Esta técnica fornece a opção de selecionar um código BCH mais adequado com capacidade de correção de erros e taxa de código, mas com comprimento previamente escolhido.

Referências

[1] Shankar, P., *On BCH codes over arbitrary integer rings*, IEEE Trans. Inform. Theory, IT-25(4), (1979), 480-483.

[2] Blake, I.F., *Codes over certain rings*, Inform. Contr., 20, (1972), 396-404.

[3] Blake, I.F., *Codes over integer residue rings*, Inform. Contr., 29, (1975), 295-300.

[4] Interlando, J.C. and Palazzo Jr., R., *A note on cyclic codes over* $\mathbb{Z}_m$, Latin Amer. Appl. Res., 25(S), (1995), 83-85.

[5] Spiegel, E., *Codes over* $\mathbb{Z}_m$, Inf. Control, 35, (1977), 48-51.

[6] Spiegel, E., *Codes over* $\mathbb{Z}_m$, *Reviseted*, Inf. Control, 37, (1978), 100-104.

[7] McDonlad, B.R., *Finite rings with identity*, Marcel Dekker, New York (1974).