Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 3, N. 1, 2015.
Trabalho apresentado no XXXV CNMAC, Natal-RN, 2014.

COMPARAÇÃO DE TÉCNICAS PARA O CÁLCULO DE IDEMPOTENTES GERADORES DE CÓDIGOS CÍCLICOS

Gustavo Terra Bastos, **Marinês Guerreiro**,
Departamento de Matemática - DMA, UFV,
36.570-000, Viçosa, MG
E-mail: gtbastos@yahoo.com.br, marines@ufv.br/

Resumo: *Neste trabalho apresentamos técnicas recentes para o cálculo de idempotentes primitivos em álgebras de grupo ou em álgebras polinomiais. Esses idempotentes podem ser vistos como geradores de códigos cíclicos minimais. Exibiremos duas abordagens para tais cálculos: a primeira, que chamaremos abordagem polinomial, é realizada no anel das classes residuais módulo x^n-1 de um anel de polinômios, onde n denota o comprimento do código. Já a segunda é realizada no contexto de álgebras de grupo de grupos abelianos sobre corpos finitos de ordem prima. Em particular, consideramos grupos cíclicos de ordem n e apresentamos um isomorfismo entre o anel de classes residuais e a álgebra de grupo de modo que possamos trabalhar livremente nestas duas abordagens.*

Palavras-chave: *Códigos cíclicos minimais, Idempotentes primitivos, λ-aplicação*

1 Códigos Cíclicos

Seja $n \geq 1$ um número natural e $\mathbb{F}_l$ um corpo finito com l elementos. Um **código linear de comprimento** n é um subespaço $\mathfrak{C} \subset \mathbb{F}_l^n$ (inclusão própria).

Os códigos cíclicos são um caso particular de códigos lineares. Nesta seção apresentamos os códigos cíclicos como ideais de um anel de polinômios e ideais em uma álgebra de grupo para um grupo cíclico sobre um corpo finito. Estas duas abordagens serão usadas durante todo o trabalho.

Definimos a permutação cíclica de coordenadas em $\mathbb{F}_l^n$, por

$$\begin{array}{rccc} T_\pi & : & \mathbb{F}_l^n & \to & \mathbb{F}_l^n \\ & & c=(c_0,\ldots,c_{n-1}) & \mapsto & T_\pi(c)=(c_{n-1},c_0,\ldots,c_{n-2})\,. \end{array} \tag{1}$$

Definição 1.1. *Um código linear $\mathfrak{C}$ é chamado **código cíclico** se, para toda palavra $u=(u_0,u_1,...,u_{n-1})$ em $\mathfrak{C}$, o vetor $T_\pi(u)=(u_{n-1},u_0,...,u_{n-2})$ também está em $\mathfrak{C}$, ou seja, $T_\pi(\mathfrak{C}) \subset \mathfrak{C}$.*

Considere $\mathcal{R}_n$ o anel das classes residuais em $\mathbb{F}_l[X]$ módulo X^n-1, ou seja,

$$\mathcal{R}_n = \frac{\mathbb{F}_l[X]}{\langle X^n-1\rangle}.$$

Todo elemento de $\mathcal{R}_n$ pode ser representado de forma única por um polinômio

$$a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$$

de grau no máximo $n-1$.

DOI: 10.5540/03.2015.003.01.0159

Os códigos cíclicos podem ser *realizados* de diferentes formas. É fácil verificar que

$$\begin{array}{rccc} \varphi: & \mathbb{F}_l^n & \longrightarrow & \mathcal{R}_n \\ & (b_0,...,b_{n-1}) & \mapsto & \displaystyle\sum_{i=0}^{n-1} b_i X^i \end{array} \tag{2}$$

é um isomorfismo e que os códigos cíclicos em $\mathbb{F}_l^n$ correspondem aos ideais no anel quociente $\mathcal{R}_n$.

Podemos também considerar os códigos cíclicos como ideais na álgebra de grupo de um grupo cíclico. De fato, dado $G = \langle a / a^n = 1 \rangle$ um grupo cíclico finito de ordem n, definimos a aplicação

$$\begin{array}{rccc} \psi: & \mathbb{F}_l^n & \longrightarrow & \mathbb{F}_l G \\ & (b_0,...,b_{n-1}) & \mapsto & \displaystyle\sum_{i=0}^{n-1} b_i a^i. \end{array} \tag{3}$$

É fácil verificar que ψ é um isomorfismo de $\mathbb{F}_l$-espaços vetoriais.

Teorema 1.2. *Um subespaço vetorial $\mathfrak{C}$ de $\mathbb{F}_l^n$ é um código cíclico se, e somente se, $\psi(\mathfrak{C})$ é um ideal de $\mathbb{F}_l G$.*

Por (2) e (3), temos o isomorfismo $\psi\varphi^{-1}$ entre $\mathcal{R}_n$ e $\mathbb{F}_l G$ tal que

$$\begin{array}{ccccccc} & & \varphi^{-1} & & & \psi & \\ \mathcal{R}_n & & \longrightarrow & & \mathbb{F}_l^n & \longrightarrow & \mathbb{F}_l G \\ \displaystyle\sum_{i=0}^{n-1} b_i X^i & & \mapsto & (b_0, b_1, ..., b_{n-1}) & & \mapsto & \displaystyle\sum_{i=0}^{n-1} b_i a^i \ . \end{array} \tag{4}$$

Verifica-se facilmente que este é um isomorfismo de álgebras.

De posse dessas informações, apresentamos as técnicas para o cálculo de idempotentes primitivos em ambos os contextos, a saber, o polinomial e o de álgebra de grupo. Dado o isomorfismo (4), podemos trabalhar livremente em ambas as abordagens, considerando que na segunda (álgebra de grupo) o grupo seja cíclico.

Ficará claro durante a exibição das técnicas quais são as vantagens e desvantagens de cada uma.

2 Primeira abordagem - polinomial

2.1 λ-Aplicação e Idempotentes Primitivos em Anéis Semissimples

Vamos expor neste capítulo um método para obter códigos cíclicos minimais a partir de uma abordagem polinomial. Chamamos este método de **λ-técnica** e ela é definida a partir de uma **λ-aplicação** e um **λ-produto** de polinômios, que são definidos a seguir. A principal referência para esta seção é [6].

2.2 A λ-aplicação e as classes ciclotômicas

Nesta seção consideramos a seguinte **hipótese geral**:

$$\begin{array}{l} r \geqslant 2 \text{ e } \alpha_i \geqslant 1 \text{ são números inteiros,} \\ m = \displaystyle\prod_{i=1}^{r} p_i^{\alpha_i}, \text{ com } p_i \text{ primos ímpares distintos, para } 1 \leq i \leq r, \\ mdc\left(\dfrac{\varphi(p_i^{\alpha_i})}{2}, \dfrac{\varphi(p_j^{\alpha_j})}{2}\right) = 1, \text{ para } 1 \leq i \neq j \leq r, \\ l \neq 2 \text{ é uma raiz primitiva } mod\ p_i^{\alpha_i}, \text{ para cada } 1 \leq i \leq r \text{ e } mdc(l, m) = 1, \end{array} \tag{5}$$

DOI: 10.5540/03.2015.003.01.0159

Considere o conjunto $A = \{0, 1, ..., (m-1)\}$. Para $a, b \in A$, definimos

$$a \sim b \text{ se, e somente se, } a \equiv bl^i (mod\, m), \text{ para algum inteiro } i \geq 0. \tag{6}$$

Esta é uma relação de equivalência no conjunto A cujas classes de equivalência são chamadas **classes l-ciclotômicas de A**.

Se t é o menor inteiro positivo tal que $s \equiv sl^t (mod\, m)$, então a classe l-ciclotômica de s é definida por $C_s = \{s, sl, ..., sl^{t-1}\}$.

Notações 2.1. *Sob a hipótese geral* (5)*, estabelecemos as seguintes notações e definições:*

(i) *Para* $1 \leq i \leq r$, $\overline{m}_i = \dfrac{m}{p_i^{\alpha_i}}$.

(ii) $A_i = \{0, 1, 2, ..., p_i^{\alpha_i} - 1\}$ *e* $A = \{0, 1, ..., (m-1)\}$.

(iii) R_i *e* N_i *são os conjuntos de resíduos quadráticos e não quadráticos módulo* $p_i^{\alpha_i}$.

(iv) $R_{p_i^{\beta_i}} = \left\{ rp_i^{\beta_i} / r \in R_i \right\}$, $N_{p_i^{\beta_i}} = \left\{ sp_i^{\beta_i} / s \in N_i \right\}$, $X_i = R_i (ou\ N_i)$ *e* $Y_i = N_i (ou\ R_i)$.

(v) $\mathcal{R}_m = \dfrac{\mathbb{F}_l[x]}{\langle x^m - 1 \rangle}$ *e* $\mathcal{R}_{p_i^{\alpha_i}} = \dfrac{\mathbb{F}_{l^2}[x]}{\left\langle x^{p_i^{\alpha_i}} - 1 \right\rangle}$.

(vi) δ *é uma raiz* m*-ésima primitiva da unidade em alguma extensão do corpo* $\mathbb{F}_{l^2}$.

(vii) *Para qualquer* m*, sempre denotamos a classe ciclotômica* C_0 *módulo* m *por* $\{0\}$.

Definição 2.2 ([6], Definition 2.2)**.** *Dado o produto cartesiano* $A_1 \times A_2 \times ... \times A_r$*, definimos a* λ***-aplicação*** *por*

$$\begin{array}{rccc} \lambda: & A_1 \times A_2 \times ... \times A_r & \longrightarrow & A \\ & (a_1, ..., a_r) & \mapsto & \displaystyle\sum_{k=1}^{r} a_k \overline{m}_k (mod\, m), \end{array}$$

O seguinte resultado é o conhecido Teorema Chinês do Resto.

Lema 2.3. *A* λ*-aplicação é uma bijeção. (A* λ*-aplicação é um isomorfismo de grupos abelianos.)*

Observação 2.4 ([6], Theorem 2.4)**.** *Sob a hipótese geral* (5)*,* $\dfrac{\varphi\left(\prod_{i=1}^{r} p_i^{\beta_i}\right)}{2^{r-1}}$ *é a ordem de* l *módulo* $\displaystyle\prod_{i=1}^{r} p_i^{\beta_i}$*, para* $1 \leq \beta_i \leq \alpha_i$*. Ressaltamos que esse resultado é um caso particular da* função de Carmichael.

Observação 2.5. *De [6], a* λ*-aplicação faz corresponder a cada classe* l*-ciclotômica de* A *a união de dois produtos cartesianos de classes* l^2*-ciclotômicas módulo* $p_i^{\alpha_i}$*, para cada* $1 \leq i \leq r$*, a saber,* $X_{p_1^{\beta_1}} \times ... \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times ... \times Y_{p_r^{\beta_r}}$ *e vice-versa, onde* $X_{p_i^{\beta_i}} = R_{p_i^{\beta_i}} \left(ou\ N_{p_i^{\beta_i}} \right)$ *e* $Y_{p_i^{\beta_i}} = N_{p_i^{\beta_i}} \left(ou\ R_{p_i^{\beta_i}} \right)$

Lema 2.6. *Sob a hipótese geral* (5)*, para cada* $1 \leq i \leq r$ *e* $1 \leq \beta_i \leq \alpha_i - 1$*, os conjuntos* $R_i, N_i, R_{p_i^{\beta_i}}$ *e* $N_{p_i^{\beta_i}}$ *são as classes* l^2*-ciclotômicas módulo* $p_i^{\alpha_i}$.

Teorema 2.7. *Sob a hipótese geral* (5)*, o número de classes* l*-ciclotômicas módulo* m *é*

$$\frac{(2\alpha_1 + 1) \dots (2\alpha_r + 1) + 1}{2}.$$

DOI: 10.5540/03.2015.003.01.0159

Demonstração. De acordo com o Lema 2.6, os conjuntos (grupos aditivos abelianos) A_i podem ser particionados com relação as suas classes l^2-ciclotômicas $X_{p_i^{\beta_i}}$, onde $0 \leq \beta_i \leq \alpha_i - 1$ e $1 \leq i \leq r$, além das classes do tipo C_0 módulo $p_i^{\alpha_i}$. Ainda, conforme foi afirmado na Observação 2.5, qualquer classe l-ciclotômica pode ser vista como λ-imagem de uma combinação arbitrária de classes l^2-ciclotômicas. Por hora desconsideremos a classe C_0 módulo m, gerada de forma única pelos zeros dos A_i, para todo $1 \leq i \leq r$. Logo existem $(2\alpha_1+1)(2\alpha_2+1)\ldots(2\alpha_r+1)-1$ combinações possíveis. Neste cálculo devemos descartar um dos dois tipos de combinações abaixo:

$$\lambda\left(X_{p_1^{\beta_1}} \times \ldots \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times \ldots \times Y_{p_r^{\beta_r}}\right) \text{ ou } \lambda\left(Y_{p_1^{\beta_1}} \times \ldots \times Y_{p_r^{\beta_r}} \cup X_{p_1^{\beta_1}} \times \ldots \times X_{p_r^{\beta_r}}\right), \quad (7)$$

pois estas λ-imagens geram a mesma classe l-ciclotômica.

Assim existem $\dfrac{(2\alpha_1+1)(2\alpha_2+1)\ldots(2\alpha_r+1)-1}{2}$ classes l ciclotômicas. Adicionando mais uma classe, a saber, a classe C_0 módulo m e a partir de algumas manipulações, verificamos a igualdade

$$\frac{(2\alpha_1+1)\ldots(2\alpha_r+1)+1}{2} = 2^{r-1}\prod_{i=1}^{r}\alpha_i + 2^{r-2}\sum_{k=1}^{r}\prod_{\substack{i=1\\ i\neq k}}^{r}\alpha_i + \ldots + 2\sum_{1\leq i<j\leq r}\alpha_i\alpha_j + \sum_{i=1}^{r}\alpha_i + 1. \quad (8)$$

□

Aqui desenvolvemos um método para explicitar os idempotentes primitivos de $\mathcal{R}_m$ descrevendo-os como λ-**produto** de idempotentes primitivos de $\mathcal{R}_{p_i^{\alpha_i}}$, para cada $1 \leq i \leq r$.

Definição 2.8. *Para $1 \leq i \leq r$, seja $f_i(x) = \sum_{j_i=0}^{p_i^{\alpha_i}-1} a_{j_i}x^{j_i} \in \mathbb{F}_{l^2}[x]$. Definimos*

$$\lambda(f_1(x) \otimes \ldots \otimes f_r(x)) = \sum_{\lambda(j_1,\ldots,j_r)\in\lambda(A_1\times\ldots\times A_r)} a_{j_1}\cdot\ldots\cdot a_{j_r}x^{\lambda(j_1,\ldots,j_r)}. \quad (9)$$

*Chamamos este produto de λ-**produto** dos polinômios $f_i(x) = \sum_{j_i=0}^{p_i^{\alpha_i}-1} a_{j_i}x^{j_i}$.*

Observação 2.9.

(i) Para $1 \leq i \leq r$ e $0 \leq \beta_i \leq \alpha_i - 1$, denotemos por $\theta_{bp_1^{\beta_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}}$ o idempotente primitivo correspondente a classe l-ciclotômica $C_{bp_1^{\beta_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}}$ no anel semissimples $\mathcal{R}_m$, onde $l^t \not\equiv b \in A$, com $t \in \mathbb{N}$ e $mdc\left(b, \prod_{i=1}^{r} p_i\right) = 1$.

(ii) Denotemos por $\theta^*_{p_i^{\beta_i}}$ e $\theta^{**}_{p_i^{\beta_i}}$ os idempotentes primitivos básicos correspondentes as classes l^2-ciclotômicas $X_{p_i^{\beta_i}}$ e $Y_{p_i^{\beta_i}}$, respectivamente no anel $\mathcal{R}_{p_i^{\alpha_i}}$. Além disso, dado $s \in A$, defina $\sigma_s(x) = \sigma_{C_s}(x) = \sum_{t\in C_s} x^t$.

(iii) Sejam $X_1 \times \ldots \times X_r$, $X_{p_1^{\beta_1}} \times \ldots \times X_{p_r^{\beta_r}}$ e $\theta^*_{p_1^{\beta_1}} \otimes \ldots \otimes \theta^*_{p_r^{\beta_r}}$ as primeiras partes das expressões $\lambda(X_1 \times \ldots \times X_r \cup Y_1 \times \ldots \times Y_r)$, $\lambda\left(X_{p_1^{\beta_1}} \times \ldots \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times \ldots \times Y_{p_r^{\beta_r}}\right)$ e $\lambda\left(\theta^*_{p_1^{\beta_1}} \otimes \ldots \otimes \theta^*_{p_r^{\beta_r}}\right) + \lambda\left(\theta^{**}_{p_1^{\beta_1}} \otimes \ldots \otimes \theta^{**}_{p_r^{\beta_r}}\right)$, respectivamente. Ainda, X_i, $X_{p_i^{\beta_i}}$ e $\theta^*_{p_i^{\beta_i}}$ são as i-ésimas entradas de $X_1 \times \ldots \times X_r$, $X_{p_1^{\beta_1}} \times \ldots \times X_{p_r^{\beta_r}}$ e $\theta^*_{p_1^{\beta_1}} \otimes \ldots \otimes \theta^*_{p_r^{\beta_r}}$, respectivamente.

DOI: 10.5540/03.2015.003.01.0159

Teorema 2.10. *Se, para cada* $0 \leq \beta_i \leq \alpha_i$, *as i-ésimas entradas da primeira parte de*

$$C_1 = \lambda(X_1 \times ... \times X_r \cup Y_1 \times ... \times Y_r) \text{ e}$$

$$C_{bp_1^{\beta_1}p_2^{\beta_2}\cdot...\cdot p_r^{\beta_r}} = \lambda\left(X_{p_1^{\beta_1}} \times ... \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times ... \times Y_{p_r^{\beta_r}}\right),$$

são R_i *e* $R_{p_i^{\beta_i}}\left(ou\ N_{p_i^{\beta_i}}\right)$, *então* $\theta_{bp_1^{\beta_1}p_2^{\beta_2}\cdot...\cdot p_r^{\beta_r}} = \lambda\left(\theta^*_{p_1^{\beta_1}} \otimes ... \otimes \theta^*_{p_r^{\beta_r}}\right) + \lambda\left(\theta^{**}_{p_1^{\beta_1}} \otimes ... \otimes \theta^{**}_{p_r^{\beta_r}}\right)$, *onde, para* $1 \leq i \leq r$, $\theta^*_{p_i^{\beta_i}}$ *e* $\theta^{**}_{p_i^{\beta_i}}$ *são os idempotentes primitivos correspondentes as classes* l^2*-ciclotômicas* $R_{p_i^{\beta_i}}\left(ou\ N_{p_i^{\beta_i}}\right)$ *e* $N_{p_i^{\beta_i}}\left(ou\ R_{p_i^{\beta_i}}\right)$, *respectivamente.*

3 Segunda abordagem - álgebra de grupo

3.1 Códigos Abelianos Minimais

Sejam $\mathbb{F}_2$ o corpo finito com 2 elementos e G um grupo finito de ordem ímpar. Um ideal minimal de $\mathbb{F}_2G$ será dito um **código abeliano binário minimal**. Nesta seção apresentamos as expressões dos idempotentes primitivos geradores dos códigos binários cíclicos de comprimento p^mq^n, pq e $p_1p_2p_3$, onde p, q, p_1, p_2 e p_3 são todos primos ímpares distintos dois a dois. Iniciamos com dois resultados técnicos. Em [5], foram determinados todos os códigos minimais sob as seguintes hipóteses:

$$\begin{aligned} &G \text{ é um grupo abeliano finito de expoente } p^m \text{ ou } (2p^m), \\ &\mathbb{F} \text{ um corpo finito com q elementos onde } q \text{ tem ordem multiplicativa } \varphi(p^m) \ mod\, p^m. \end{aligned} \tag{10}$$

Em [2], os autores fizeram o estudo dos idempotentes primitivos para grupos da forma $G_p \times G_q$, onde G_p e G_q denotam grupos abelianos, o primeiro um p-grupo e o segundo um q-grupo, que satisfazem as seguintes condições, que, em particular, satisfazem (10):

$$\begin{aligned} &mdc(p-1,\, q-1) = 2, \\ &\overline{2} \text{ gera o grupo das unidades de } \mathbb{Z}_{p^2} \text{ e } \mathbb{Z}_{q^2} \\ &mdc(p-1, q) = mdc(p, q-1) = 1. \end{aligned} \tag{11}$$

Observação 3.1. *Em* (11)*, a primeira hipótese nos garante que pelo menos um dos números primos* p *e* q *é da forma* $4k+3$, *onde* $k \in \mathbb{N}$.

Seja G um grupo de ordem ímpar. Para um subgrupo $H \leq G$, definimos $\widehat{H} = \dfrac{1}{|H|}\sum_{h\in H} h$, da mesma forma que [5] e, para um elemento $x \in G$, $\widehat{x} = \widehat{\langle x \rangle}$.

3.2 Códigos em $\mathbb{F}_2\left(\mathcal{C}_p \times \mathcal{C}_q\right)$

Sejam $p \neq q$ primos ímpares. Considere o grupo $G = \langle g \mid g^{pq} = 1\rangle$, $a = g^q$, $b = g^p$ e $G = \mathcal{C}_p \times \mathcal{C}_q$, onde $\mathcal{C}_p = \langle a\rangle$ e $\mathcal{C}_q = \langle b\rangle$. Nesta seção, descrevemos todos os idempotentes primitivos de $\mathbb{F}_2\left(\mathcal{C}_p \times \mathcal{C}_q\right)$.

Teorema 3.2 ([2], Theorem IV.1)**.** *Seja* $G = \langle a\rangle \times \langle b\rangle$ *como acima e assuma que* p *e* q *satisfazem* (11)*. Então os idempotentes primitivos de* $\mathbb{F}_2G$ *são*

$$e_0 = \widehat{G},\quad e_1 = \widehat{a}(1-\widehat{b}),\quad e_2 = (1-\widehat{a})\widehat{b},\quad e_3 = uv + u^2v^2 \text{ e } e_4 = uv^2 + u^2v,$$

onde,

$$u(a) = \begin{cases} a^{2^0} + a^{2^2} + \cdots + a^{2^{p-3}}, & se\ p \equiv 1\,(mod\ 4)\ ou \\ 1 + a^{2^0} + a^{2^2} + \cdots + a^{2^{p-3}}, & se\ p \equiv 3\,(mod\ 4) \end{cases} \tag{12}$$

e

$$u'(a) = \begin{cases} a^2 + a^{2^3} + \cdots + a^{2^{p-2}}, & se\ p \equiv 1\,(mod\ 4)\ ou \\ 1 + a^2 + a^{2^3} + \cdots + a^{2^{p-2}}, & se\ p \equiv 3\,(mod\ 4) \end{cases} \tag{13}$$

DOI: 10.5540/03.2015.003.01.0159

3.3 Códigos em $\mathbb{F}_2\left(\mathcal{C}_{p^m} \times \mathcal{C}_{q^n}\right)$, para $m \geq 2, n \geq 2$

Teorema 3.3 ([2], Theorem V.1)**.** *Sejam p e q números primos que satisfazem (11) e $G = \langle a\rangle \times \langle b\rangle$, com $\langle a\rangle = \mathcal{C}_{p^m}$ e $\langle b\rangle = \mathcal{C}_{q^n}$. Então os códigos minimais de $\mathbb{F}_2G$ são gerados pelos seguintes idempotentes primitivos*

$$e_0 = \widehat{a}\widehat{b}, \quad e_{0j} = \widehat{a}\left(\widehat{b^{q^j}} + \widehat{b^{q^{j-1}}}\right), \quad e_{i0} = \left(\widehat{a^{p^i}} + \widehat{a^{p^{i-1}}}\right)\widehat{b}, \quad e_{ij}^{*} = uv + u^2v^2 \text{ e } e_{ij}^{**} = uv^2 + u^2v,$$

onde

$$\begin{aligned} u &= \widehat{a^{p^i}}\left(a^{2^0p^{i-1}} + a^{2^2p^{i-1}} + \cdots + a^{2^{p-3}p^{i-1}}\right), \text{ se } p \equiv 1\,(mod\ 4) \text{ ou} \\ u &= \widehat{a^{p^i}}\left(1 + a^{2^0p^{i-1}} + a^{2^2p^{i-1}} + \cdots + a^{2^{p-3}p^{i-1}}\right), \text{ se } p \equiv 3\,(mod\ 4) \end{aligned}$$

e

$$\begin{aligned} v &= \widehat{b^{q^j}}\left(b^{2^0q^{j-1}} + b^{2^2q^{j-1}} + \cdots + b^{2^{q-3}q^{j-1}}\right), \text{ se } q \equiv 1\,(mod\ 4) \text{ ou} \\ v &= \widehat{b^{q^j}}\left(1 + b^{2^0q^{j-1}} + b^{2^2q^{j-1}} + \cdots + b^{2^{q-3}q^{j-1}}\right), \text{ se } q \equiv 3\,(mod\ 4) \end{aligned}$$

3.4 Códigos em $\mathbb{F}_2\left(\mathcal{C}_{p_1} \times \mathcal{C}_{p_2} \times \mathcal{C}_{p_3}\right)$

Os métodos das seções anteriores podem ser estendidos para o caso geral, mas os cálculos tornam-se muito mais complexos. Como uma ilustração, mostramos abaixo como obter os idempotentes primitivos quando $|G|$ envolve três primos distintos.

Teorema 3.4 ([2], Theorem IV.10)**.** *Sejam p_1, p_2 e p_3 três primos ímpares distintos tais que $mdc\left(p_i - 1, p_j - 1\right) = 2$, para $1 \leq i \neq j \leq 3$, e $\bar{2}$ um gerador do grupo $U\left(\mathbb{Z}_{p_i}\right)$. Então os idempotentes primitivos da álgebra de grupo $\mathbb{F}_2G$, para $G = \mathcal{C}_{p_1} \times \mathcal{C}_{p_2} \times \mathcal{C}_{p_3}$, com $\mathcal{C}_{p_1} = \langle a\rangle$, $\mathcal{C}_{p_2} = \langle b\rangle$ e $\mathcal{C}_{p_2} = \langle c\rangle$, são*

$e_0 = \hat{a}\hat{b}\hat{c}$ $\quad$ $e_1 = \hat{a}\hat{b}(1-\hat{c})$
$e_2 = \hat{a}(1-\hat{b})\hat{c}$ $\quad$ $e_3 = (1-\hat{a})\hat{b}\hat{c}$
$e_4 = (uv + u^2v^2)\hat{c}$ $\quad$ $e_5 = (u^2v + uv^2)\hat{c}$
$e_6 = (uw + u^2w^2)\hat{b}$ $\quad$ $e_7 = (u^2w + uw^2)\hat{b}$
$e_8 = (vw + v^2w^2)\hat{a}$ $\quad$ $e_9 = (v^2w + vw^2)\hat{a}$
$e_{10} = (1-\hat{a})(1-\hat{b})(1-\hat{c}) + u^2v^2w + uvw^2$ $\quad$ $e_{11} = (1-\hat{a})(1-\hat{b})(1-\hat{c}) + u^2v^2w^2 + uvw$
$e_{12} = (1-\hat{a})(1-\hat{b})(1-\hat{c}) + u^2vw^2 + uv^2w^2$ $\quad$ $e_{13} = (1-\hat{a})(1-\hat{b})(1-\hat{c}) + uv^2w + u^2vw^2$

onde $u = u(a), v = v(b)$ e $w = w(c)$ são definidos como em 3.2, respectivamente.

4 Análise das técnicas apresentadas

Ambas as técnicas apresentadas neste trabalho nos permitem calcular os idempotentes primitivos dos códigos cíclicos minimais de modo algorítmico. A partir do cálculo de exemplos específicos, observamos que as fórmulas apresentadas em [6] podem conter alguns erros em seus coeficientes. A limitação de espaço nos fez optar por não apresentar o exemplo neste resumo.

As técnicas polinomiais envolvem a utilização de extensões do corpo base e, algumas vezes, descuidam do fato de que o produto de idempotentes primitivos nem sempre é primitivo.

Por outro lado, a técnica de álgebra de grupo se mostrou muito eficiente no cálculo dos idempotentes primitivos, utilizando simplesmente a estrutura dos subgrupos do grupo subjacente, o que evita, por exemplo, o uso de raízes primitivas, usadas na técnica polinomial. Outra vantagem é que fica muito claro de onde se origina cada idempotente primitivo a partir da estrutura do grupo. Isto facilita, por exemplo, determinar certas equivalências de códigos minimais,

conforme [4], e também nos permite determinar claramente quantos fatores primitivos aparecem quando o produto de dois idempotentes primitivos não é primitivo.

Pelos estudos que realizamos até o momento dos desenvolvimentos dessas técnicas, acreditamos que uma boa combinação de ambas possa minimizar possíveis erros nas expressões dos idempotentes.

Referências

[1] S.K. Arora and M. Pruthi *Minimal cyclic codes of length* $2p^n$. Finite Fields Appl. **5** no. 2 (1999) 177-187.

[2] G. Chalom, R. A. Ferraz, M. Guerreiro and C. Polcino Milies *Minimal Binary Abelian Codes of length* $p^m q^n$. preprint in arXiv:1205.5699.

[3] R. Ferraz *Simple components and central units in group algebras*. J. Algebra, **279** (2004) 191-203.

[4] R. Ferraz, M. Guerreiro, C. Polcino Milies, *G-equivalence in group algebras and minimal abelian codes*, IEEE Transactions on Information Theory, **60** N. 1 (2014) 252-260.

[5] R. Ferraz, C. Polcino Milies, *Idempotents in group algebras and minimal abelian codes*, Finite Fields and their Appl., **13**, (2007) 382-393.

[6] P. Kumar e S.K. Arora λ*-Mapping and Primitive Idempotents in semi simple ring* R_m. Communications in Algebra, to appear

[7] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An Introduction to the Theory of Numbers*, 5th Edition, John Wiley, New York, 1991.

[8] C. Polcino Milies, S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, 2002.

[9] M. Pruthi and S.K. Arora *Minimal cyclic codes of prime power length*. Finite Fields Appl. **3** no. 2 (1997) 99-113.

DOI: 10.5540/03.2015.003.01.0159