UM ESTUDO SOBRE AS PROPRIEDADES ESTRUTURAIS DAS ÁLGEBRAS DE CÓDIGO

Benito, Samuel Henrique Gomes Velez[1]
Martin, Maria Eugenia[2]

Resumo: Este trabalho investiga a estrutura das álgebras de código, uma classe de álgebras comutativas e não associativas definidas a partir de um código linear binário. Com base em sua definição formal, analisamos as condições de não degenerescência necessárias para garantir sua simplicidade, mostrando que essas álgebras não possuem ideais próprios não triviais, exceto em casos restritos. Estudamos também o comportamento do operador adjunto associado aos elementos da base, obtendo a decomposição de Peirce e as respectivas leis de fusão. Por fim, investigamos as involuções de Miyamoto, os grupos por elas determinados e a condição de Seress, estabelecendo as propriedades necessárias para caracterizar essas álgebras como álgebras axiais de tipo Jordan.

Palavras-chave: Álgebras de código; Código linear binário; Álgebras axiais de tipo Jordan; Grupo de Miyamoto

FUNDAMENTAÇÃO TEÓRICA

Em 1948, no artigo “A Mathematical Theory of Communication”, publicado na revista The Bell System Technical Journal, Claude Shannon mostrou que, dado um canal de comunicação com ruído, existe um número, chamado capacidade do canal, tal que a comunicação confiável pode ser alcançada a qualquer taxa abaixo dessa capacidade, desde que sejam utilizadas técnicas adequadas de codificação e decodificação. Essa contribuição foi o estopim para o surgimento de uma nova área na Álgebra – a Teoria dos Códigos –, que versa sobre a transmissão de mensagens em um canal com interferência, bem como a reconstituição de dados corrompidos.

Ao longo dos anos, a Teoria de Códigos apresentou intenso desenvolvimento, revelando sua aplicabilidade nas mais diversas áreas, em especial na ciência da computação e nas engenharias. Em particular, os resultados envolvendo a preservação de informações através da predição ou mesmo correção de erros mostram-se essenciais para o desenvolvimento de sistemas de comunicação eficientes e que cumpram adequadamente seus

[1]Universidade Federal do Paraná (UFPR); Bacharelado em Matemática; samuelbenito@ufpr.br.
[2]Universidade Federal do Paraná (UFPR); Professora Orientadora; eugenia@ufpr.br.

propósitos.

A codificação de canal também é chamada de codificação algébrica, já que ferramentas algébricas são amplamente utilizadas no estudo da codificação de canal, a saber:

Definição 1. *Seja $A = \{a_1, a_2, ..., a_q\}$ um conjunto com q elementos, denominado **alfabeto** do código e cujos elementos são **símbolos** do código. Definimos uma **palavra** q-ária de tamanho n sobre A como uma lista $w_1w_2...w_n$, com $w_i \in A$, para todo $1 \leq i \leq n$. Além disso, denominamos **código** q-ário de comprimento n sobre A um conjunto C não-vazio de palavras q-árias de mesmo comprimento n.*

Note que, através dessa ideia, as palavras de um código podem ser interpretadas como n-uplas $w_1w_2...w_n = (w_1, w_2, ..., w_n)$ em A^n. Por essa razão, revela-se fundamental o estudo de conjuntos adequados para atuarem como alfabetos de código. Vamos dotar o conjunto A de uma estrutura algébrica. A ideia é definir duas operações em A de modo que ele se torne um corpo. Claro que, nesse caso, A será um corpo com apenas um número finito de elementos, isto é, $A = \mathbb{F}_q$ em que q é uma potência de um número primo.

A partir dessa fundamentação, é possível iniciar o estudo da teoria dos **códigos lineares**, os quais são definidos como sendo subespaços vetoriais de $\mathbb{F}_q^n$. Esses subespaços apresentam atributos peculiares que justificam uma análise mais profunda, como, por exemplo, uma quantidade finita de bases distintas, além de se mostrarem os principais exemplos de estruturas que podem atuar na transmissão de mensagens e símbolos com predição e correção de erros. A principal vantagem na utilização de códigos lineares é que os procedimentos de codificação e decodificação são mais rápidos e simples do que aqueles para códigos não lineares arbitrários. Para um aprofundamento na teoria de códigos, consulte [3].

Neste trabalho, aplicamos conhecimentos prévios de teoria de códigos ao estudo das chamadas álgebras de código, uma classe de álgebras comutativas e não associativas definidas a partir de códigos lineares binários (i.e., sobre $\mathbb{F}_2$), introduzidas em 2019 por A. Castillo-Ramirez, J. McInroy e F. Rehren, (veja [1]).

Definição 2. *Seja $C \subseteq \mathbb{F}_2^n$ um código linear binário de comprimento n, $\mathbb{F}$ um corpo e Λ um*

conjunto de parâmetros de estrutura

$$\Lambda := \{a_{i,\alpha}, b_{\alpha,\beta}, c_{i,\alpha} \in \mathbb{F} \mid i \in \textit{supp}(\alpha); \alpha, \beta \in C^*, \beta \neq \alpha, \alpha^c\}$$

em que $C^* := C - \{\mathbf{0}, \mathbf{1}\}$*, com* $\mathbf{0} := (0, \ldots, 0)$ *e* $\mathbf{1} := (1, \ldots, 1)$*,* $\textit{supp}(\alpha) := \{1 \leq i \leq n \mid \alpha_i = 1\}$ *e* $\alpha^c = \mathbf{1} + \alpha$*. A* ***álgebra de código*** $A_C(\Lambda)$ *é uma álgebra comutativa não associativa sobre o corpo* $\mathbb{F}$ *com base*

$$\{t_i \mid 1 \leq i \leq n\} \cup \{e^\alpha \mid \alpha \in C^*\}$$

e multiplicação dada por:

$$t_i \cdot t_j = \delta_{i,j} t_i$$

$$t_i \cdot e^\alpha = \begin{cases} a_{i,\alpha} e^\alpha, & \textit{se } \alpha_i = 1, \\ 0, & \textit{se } \alpha_i = 0 \end{cases}$$

$$e^\alpha \cdot e^\beta = \begin{cases} b_{\alpha,\beta} e^{\alpha+\beta}, & \textit{se } \alpha \neq \beta, \beta^c \\ \sum_{i \in \textit{supp}(\alpha)} c_{i,\alpha} t_i, & \textit{se } \alpha = \beta \\ 0, & \textit{se } \alpha = \beta^c \end{cases}$$

Observação. Chamaremos os elementos t_i de **elementos torais** e os e^α de **elementos de código**.

Para aprofundarmos o estudo estrutural das álgebras de código, é fundamental estabelecermos a conexão dessas estruturas com as chamadas *álgebras axiais*.

Seja $\mathbb{F}$ um corpo com característica diferente de dois, $\mathcal{F} \subseteq \mathbb{F}$ um subconjunto, e $\star : \mathcal{F} \times \mathcal{F} \to 2^{\mathcal{F}}$ uma operação binária simétrica. Chamamos o par $(\mathcal{F}, \star)$ de uma **lei de fusão** sobre $\mathbb{F}$.

Seja A uma álgebra comutativa e não associativa sobre $\mathbb{F}$. Para um elemento $a \in A$, o **operador adjunto** ad_a é definido por $\text{ad}_a(v) := av$, para todo $v \in A$. Seja $\text{Spec}(a)$ o conjunto de autovalores de ad_a, e para $\lambda \in \text{Spec}(a)$, seja $A_\lambda(a)$ o autoespaço de ad_a associado a λ.

Definição 3. *Seja* $(\mathcal{F}, \star)$ *uma lei de fusão sobre* $\mathbb{F}$*. Um elemento* $a \in A$ *é um* ***eixo***-$\mathcal{F}$ *se*

as seguintes condições são satisfeitas:

1. a *é idempotente (isto é,* $a^2 = a$*);*
2. a *é semissimples (isto é, o operador adjunto* ad_a *é diagonalizável);*
3. *Spec*$(a) \subseteq \mathcal{F}$ *e* $A_\lambda A_\mu \subseteq \bigoplus_{\gamma \in \lambda \star \mu} A_\gamma$*, para todo* $\lambda, \mu \in$ *Spec*(a)*.*

Dizemos que um eixo-$\mathcal{F}$ a *é* ***primitivo*** *se* $A_1 = \langle a \rangle$*.*

Definição 4. *Uma* ***álgebra axial*** *é um par* (A, X)*, em que* A *é uma álgebra comutativa não associativa e* X *é um conjunto de eixos-*$\mathcal{F}$ *que geram* A*. Dizemos que a álgebra axial é* ***primitiva*** *se todos os eixos em* X *são primitivos.*

Definição 5. *Dizemos que uma álgebra axial* (A, X) *é de* ***tipo Jordan*** *se o operador adjunto* ad_a*,* $a \in X$*, possuir autovalores* $\{0, 1, \eta\}$ *e obedecer à seguinte lei de fusão:*

$$A_i A_i \subseteq A_i \quad A_1 A_0 = \{0\} \quad A_i A_\eta \subseteq A_\eta \quad A_\eta A_\eta \subseteq A_1 \oplus A_0 \quad i = 0, 1.$$

Quando a lei de fusão for clara pelo contexto, omitiremos o $\mathcal{F}$ e utilizaremos simplesmente os termos eixo e álgebra axial, denotando a álgebra apenas por A.

A partir dessa fundamentação, o objetivo deste trabalho é investigar a fundo as propriedades das álgebras de código. Nas próximas seções, analisaremos as condições para que essas álgebras sejam simples e detalharemos a decomposição de Peirce associada aos seus idempotentes. Além disso, exploraremos a ação dos grupos de Miyamoto induzidos por essas estruturas e, por fim, estabeleceremos as condições de Seress, que determinam sob quais exigências estruturais uma álgebra de código pode ser classificada como uma álgebra axial de tipo Jordan.

RESULTADOS PRINCIPAIS

Aqui, daremos ênfase à estrutura das álgebras de código. Entretanto, antes de apresentarmos qualquer resultado, precisamos estabelecer um lema auxiliar da Teoria dos Códigos. Para sua formulação, introduziremos inicialmente duas definições que serão fundamentais.

Definição 6. *Para cada $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{F}_2^n$, denotamos o **peso de Hamming** por $|\alpha| := |supp(\alpha)|$. O **suporte** do próprio código C é definido como supp$(C) := \bigcup_{\alpha \in C}$ supp(α) e o conjunto dos pesos de Hamming de todas palavras-código em C é denotado por wt$(C) := \{|\alpha| : \alpha \in C\}$.*

Definição 7. *Considere o produto escalar usual $(\cdot, \cdot) : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ dado por $(u, v) := \sum_{i=1}^n u_i v_i$ para $u, v \in \mathbb{F}_2^n$. Para qualquer $v \in \mathbb{F}_2^n$ e $k \in \{0, 1\}$, definimos*

$$C_k(v) := \{\alpha \in C : (\alpha, v) = k\}.$$

Quando v for claro pelo contexto, escrevemos C_i ao invés de $C_i(v)$. Note que, por definição, temos $\alpha \in C_{(\alpha,v)}$.

Lema 1. *Seja $C \subseteq \mathbb{F}_2^n$ um código linear binário de comprimento n. Seja $v \in \mathbb{F}_2^n$ e $C_k = C_k(v)$, para $k \in \{0, 1\}$. Então:*

1. *A aplicação $\alpha \mapsto (\alpha, v)$ é um homomorfismo de C em $\mathbb{F}_2$, vistos como grupos aditivos. Consequentemente, C é a união disjunta de C_0 e C_1.*
2. *C_0 é um código linear binário, logo, em particular, é não vazio.*
3. *Se C_1 é não vazio, então $|C_0| = |C_1| = \frac{|C|}{2}$.*

Além disso, se $\mathbf{1} \in C$, então:

4. *Se v tem peso ímpar, então os complementos das palavras-código em C_0 estão em C_1 e vice-versa.*
5. *Se v tem peso par, então cada C_k é fechado sob complementação.*

Demonstração.

1. Considere a aplicação $\varphi : C \to \mathbb{F}_2$ dada por $\varphi(\alpha) = (\alpha, v)$. Sejam $\alpha, \beta \in C$:

$$\begin{aligned}\varphi(\alpha + \beta) = (\alpha + \beta, v) &= \sum_{i=1}^n (\alpha + \beta)_i v_i = \sum_{i=1}^n (\alpha_i + \beta_i) v_i \\ &= \sum_{i=1}^n \alpha_i v_i + \sum_{i=1}^n \beta_i v_i = (\alpha, v) + (\beta, v) = \varphi(\alpha) + \varphi(\beta).\end{aligned}$$

Logo, φ é um homomorfismo de grupos aditivos. Além disso, $C_0 = \varphi^{-1}(\{0\})$ e $C_1 = \varphi^{-1}(\{1\})$. Como $C_0 \subseteq C$ e $C_1 \subseteq C$ então $C_0 \cup C_1 \subseteq C$. Por outro lado, seja $\alpha \in C$ então $\varphi(\alpha) = 0$ ou $\varphi(\alpha) = 1$ logo $\alpha \in C_0$ ou $\alpha \in C_1$ isto é $\alpha \in C_0 \cup C_1$. Logo, $C = C_0 \cup C_1$ e claramente $C_0 \cap C_1 = \emptyset$.

2. Note que φ é também uma transformação linear de $\mathbb{F}_2$-espaços vetoriais e que $C_0 = \ker(\varphi)$ logo C_0 é subespaço vetorial de C e, portanto, é um código linear binário.

3. Se $C_1 \neq \emptyset$, existe $\alpha \in C$ tal que $(\alpha, v) = 1$. Defina a plicação $f : C_0 \to C_1$, dada por $f(\beta) = \beta + \alpha$. Precisamos provar que f está bem definida. De fato, se $\beta \in C_0$, então $(\beta, v) = 0$. Logo, $(\beta + \alpha, v) = (\beta, v) + (\alpha, v) = 0 + 1 = 1$ ou seja $\beta + \alpha \in C_1$.

   Vejamos que f é uma bijeção: claramente, se $f(\beta) = \beta + \alpha = f(\gamma) = \gamma + \alpha$ então necessariamete $\beta = \gamma$ e logo f é injetiva. Agora, suponha que $\delta \in C_1$, então $\delta = (\delta + \alpha) + \alpha = f(\delta + \alpha)$ e como $(\delta + \alpha, v) = (\delta, v) + (\alpha, v) = 1 + 1 = 0$ então $\delta + \alpha \in C_0$. Portanto, f é sobrejetiva.

   Logo, $|C_0| = |C_1|$ e, como $C = C_0 \sqcup C_1$, segue que $|C| = |C_0| + |C_1| = 2|C_0|$ logo $|C_0| = |C_1| = \frac{|C|}{2}$.

4. Se $\mathbf{1} \in C$ define-se $\alpha^c = \mathbf{1} + \alpha$. Se v tem peso ímpar e $\alpha \in C_0$ então

$$(\alpha^c, v) = (\mathbf{1} + \alpha, v) = (\mathbf{1}, v) + (\alpha, v) = (\mathbf{1}, v) = \sum_{i=1}^{n} v_i = |v| \pmod 2 = 1,$$

   logo $\alpha^c \in C_1$. Analogamente prova-se que se $\alpha \in C_1$ então $\alpha^c \in C_0$.

5. Se v tem peso par, então $(\mathbf{1}, v) = 0$ o que implica que $(\alpha^c, v) = (\mathbf{1}, v) + (\alpha, v) = (\alpha, v)$. Assim, se $\alpha \in C_k$ então $\alpha^c \in C_k$, ou seja C_0 e C_1 são fechados por complementação. □

Definição 8. *Uma álgebra de código $A_C(\Lambda)$ é dita **não degenerada** se $\operatorname{supp}(C) = \{1, \ldots, n\}$, $|C^*| > 0$ e nenhum dos parâmetros de estrutura em Λ é zero.*

Algumas álgebras, com escolhas específicas dos parâmetros de estrutura, serão mais interessantes do que outras. Em particular, estaremos interessados em álgebras

com um grupo de automorfismos grande, o que imporá restrições sobre os parâmetros estruturais. Uma fonte natural de automorfismos pode ser encontrada no próprio código. Dois códigos C e D são ditos **similares** se existe $g \in S_n$ tal que $g(C) = D$, em que S_n age naturalmente em C permutando as coordenadas das palavras-código. Definimos o **grupo de automorfismos** de C por $\mathrm{Aut}(C) := \{g \in S_n : g(C) = C\}$.

Definição 9. *Seja $G \leq$ Aut(C). Os parâmetros de estrutura Λ são chamados de G-**regulares** se para todo $g \in G$:*

1. $a_{i,\alpha} = a_{g(i),g(\alpha)}$ *para todo* $i \in$ *supp*(α), $\alpha \in C^*$
2. $b_{\alpha,\beta} = b_{g(\alpha),g(\beta)}$ *para todo* $\alpha, \beta \in C^*$, $\beta \neq \alpha, \alpha^c$
3. $c_{i,\alpha} = c_{g(i),g(\alpha)}$ *para todo* $i \in$ *supp*(α), $\alpha \in C^*$

*Eles são ditos **regulares** se forem Aut(C)-regulares.*

Seja $G \leq$ Aut(C) e considere a aplicação $\varphi : G \to$ Aut$(A_C(\Lambda))$, em que para cada $g \in G$, $\varphi(g)$ é a extensão linear para $A_C(\Lambda)$ de:

$$\varphi(g)(t_i) := t_{g^{-1}(i)}$$
$$\varphi(g)(e^\alpha) := e^{g^{-1}(\alpha)}$$

Lema 2. *Seja $G \leq$ Aut(C). A aplicação $\varphi : G \to$ Aut$(A_C(\Lambda))$ (definida como antes) é um homomorfismo de grupos bem definido (isto é, uma representação de álgebra de G em $A_C(\Lambda)$) se, e somente se, os parâmetros de estrutura forem G-regulares. Além disso, quando esta representação está definida, ela é fiel.*

Demonstração. Como G possui uma ação bem definida sobre as palavras-código de C, e portanto em C^*, e também em $\mathbb{F}^n$, é claro que φ é um homomorfismo de grupos. Resta verificar se, para todo $g \in G$, $\varphi(g)$ respeita o produto na álgebra. Verificando isso, fazendo uma conta direta, encontramos que as condições acima são necessárias e suficientes. Quando a ação é definida, é claro que ela é fiel, pois Aut(C) age fielmente em $\mathbb{F}^n$. □

Observação. A partir daqui, vamos assumir que a álgebra $A_C(\Lambda)$ é não degenerada.

O primeiro resultado que apresentaremos relacionado à estrutura das álgebras de código mostra que, em geral, essas álgebras são simples. Lembramos que uma álgebra A é dita **simples** se não possuir ideais próprios não triviais.

Teorema 1. *Uma álgebra de código $A_C(\Lambda)$ é simples a menos que $C = \{\mathbf{0}, \mathbf{1}, \alpha, \alpha^c\}$.*

Demonstração. Seja I um ideal não trivial de A. Seja $x \in I$ tal que $x \neq 0$. Escrevemos $x = \sum_{i=1}^{n} \lambda_i t_i + \sum_{\alpha \in C^*} \lambda_\alpha e^\alpha$. Há dois casos a considerar.

Suponha que $\lambda_\alpha \neq 0$ para algum $\alpha \in C^*$. Podemos escolher α de modo que não exista $\beta \in C^*$ com supp$(\beta) \supsetneq$ supp(α) e $\lambda_\beta \neq 0$. Então,

$$(t_{j_1}(\dots(t_{j_k}x))\dots) = a_{j_1,\alpha}\dots a_{j_k,\alpha}\lambda_\alpha e^\alpha \in I$$

em que supp$(\alpha) = \{j_1, \dots, j_k\}$. Logo, $e^\alpha \in I$. Observe que, para qualquer $\beta \in C - \{\mathbf{0}, \mathbf{1}, \alpha, \alpha^c\}$, temos $e^\beta \in I$ porque $e^{\alpha+\beta}e^\alpha = b_{\alpha+\beta,\beta}e^\beta \in I$. Além disso, como $\alpha^c = \beta + (\beta + \alpha^c)$, onde $\beta, \beta + \alpha^c \in C - \{\mathbf{0}, \mathbf{1}, \alpha, \alpha^c\}$, também temos $e^{\alpha^c} = \frac{1}{b_{\beta+\alpha^c,\beta}} e^{\beta+\alpha^c}e^\beta \in I$. Portanto, $e^\beta \in I$ para todo $\beta \in C^*$. Observe que $(e^\beta)^2 = \sum_{i \in \text{supp}(\beta)} c_{i,\beta} t_i$ para qualquer $\beta \in C^*$. Logo, para todo $j = \{1, \dots, n\}$ podemos encontrar $\beta \in C^*$ tal que $j \in$ supp(β), logo $t_j = \frac{1}{c_{j,\beta}} t_j (e^\beta)^2 \in I$. Portanto, $I = A$.

Agora suponha que $\lambda_\alpha = 0$ para todo $\alpha \in C^*$, então $\lambda_i \neq 0$ para algum $i = \{1, \dots, n\}$. É fácil ver que $t_i = \frac{1}{\lambda_i} t_i x \in I$. Agora, $e^\beta = \frac{1}{a_{i,\beta}} t_i e^\beta \in I$ para qualquer $\beta \in C^*$ com $i \in$ supp(β). Portanto, $x' = e^\beta$ recai no caso acima e concluímos que $I = A$. □

Vejamos agora que a condição imposta sobre o código C no teorema anterior é de fato necessária.

Lema 3. *Se $C = \{\mathbf{0}, \mathbf{1}, \alpha, \alpha^c\}$, então uma álgebra de código $A_C(\Lambda)$ possui dois ideais próprios não triviais, sendo eles:*

$$\langle \sum_{i \in \textit{supp}(\alpha)} t_i, e^\alpha \rangle, \quad \langle \sum_{i \in \textit{supp}(\alpha^c)} t_i, e^{\alpha^c} \rangle.$$

Demonstração. Uma verificação direta mostra que ambos satisfazem a definição de ideal.

O próximo resultado sobre a estrutura das álgebras de código diz respeito ao com-

portamento do operador de adjunto associado aos elementos idempotentes da base, permitindo obter a decomposição de Peirce e as respectivas leis de fusão para esses elementos.

Teorema 2. *(Decomposição de Peirce). Seja $A_C(\Lambda)$ uma álgebra de código. Para todo $1 \leq i \leq n$, o operador ad_{t_i} é semissimples com autovalores $1, 0$ e o conjunto $\{a_{i,\alpha} : i \in supp(\alpha), \alpha \in C^*\}$. Suponha que $a_{i,\alpha} \neq 1$ para todo $\alpha \in C^*$ com $\alpha_i = 1$, então a álgebra $A_C(\Lambda)$ admite a decomposição em autoespaços*

$$A_C(\Lambda) = A_1 \oplus A_0 \oplus \bigoplus A_{a_{i,\alpha}}$$

em que $A_1 = \langle t_i \rangle$, $A_0 = \langle t_j, e^\alpha : j \in \{1, \ldots, n\}, j \neq i, \alpha_i = 0 \rangle$ e $A_{a_{i,\alpha}} = \langle e^\beta : \beta_i = 1, a_{i,\beta} = a_{i,\alpha} \rangle$. Além disso, A_0 tem dimensão $\frac{|C|}{2} + n - 2$. Finalmente, se denotamos os autovalores de t_i por $\{1, 0, a_1, \ldots, a_k\}$, então a lei de fusão com respeito a t_i é dada por:

$$A_1A_1 \subseteq A_1 \qquad A_1A_0 = \{0\} \qquad A_1A_{a_j} \subseteq A_{a_j}$$

$$A_0A_0 \subseteq A_0 \qquad A_0A_{a_j} \subseteq \bigoplus_{l=1}^{k} A_{a_l} \qquad A_{a_j}A_{a_j} \subseteq A_1 \oplus A_0$$

$$A_{a_j}A_{a_i} \subseteq A_0$$

para $i, j = 1, \ldots, k$ e $i \neq j$.

Demonstração. Os subespaços são claros a partir da definição de álgebras de código. Para a dimensão de A_0, observe que possuímos $n - 1$ elementos torais gerando A_0. Agora, pela não-degenerescência, existe $\xi \in C$ tal que $\xi_i = 1$. Seja agora $v \in \mathbb{F}_2^n$ o vetor que possui 1 na i-ésima coordenada e 0 no resto, disso segue que $C_1(v) \neq \emptyset$ e pelo Lema 1(3) temos $|C_0(v)| = \frac{|C|}{2}$. Há tantos elementos de código gerando A_0 como elementos em $C_0(v)$ menos o vetor nulo. Assim, $\dim(A_0) = n - 1 + \frac{|C|}{2} - 1 = \frac{|C|}{2} + n - 2$.

Pela definição dos autoespaços de $A_C(\Lambda)$ em relação ao operador ad_{t_i}, qualquer elemento da álgebra pode ser escrito como combinação linear dos geradores das suas respectivas bases. O subespaço A_1 é gerado puramente pelo elemento toral t_i. O subespaço A_0 é gerado pelos torais t_j (com $j \neq i$) e pelos elementos de código e^α tais que $\alpha_i = 0$. Já os subespaços não triviais A_{a_k} são gerados pelos elementos de código e^β tais que $\beta_i = 1$

e $a_{i,\beta} = a_k$. Para demonstrar as contenções da lei de fusão, analisamos o produto entre elementos arbitrários x e y pertencentes a esses subespaços. Inicialmente, consideramos as interações com o toral principal. Tomando $x = at_i \in A_1$, se multiplicarmos por um elemento genérico $y = ct_i \in A_1$, obtemos $ac(t_it_i) = act_i$, provando que $A_1A_1 \subseteq A_1$. Se tomarmos $y \in A_0$, com y sendo um elemento de código, note que como a iésima coordenada não está no suporte de y, usando o fato de que 0 é autovalor do operador adjunto, chegamos que $t_iy = 0$. Por outro lado, se $y \in A_0$ for um toral, obtemos também 0 como resultado, portanto $A_1A_0 = \{0\}$ Caso $y \in A_{a_k}$, a definição de autovetor nos dá $t_iy = a_ky$, o que assegura a que $A_1A_{a_k} \subseteq A_{a_k}$. Em seguida, avaliamos o produto de elementos no autoespaço associado a 0. Sejam $x, y \in A_0$. Ao tomar $x = e^\alpha$ e $y = e^\beta$, as restrições da base implicam que $\alpha_i = 0$ e $\beta_i = 0$. A operação da álgebra estabelece que este produto gera termos associados a $e^{\alpha+\beta}$. Somando as coordenadas em $\mathbb{Z}_2$, a i-ésima coordenada do novo vetor será a soma $0 + 0 = 0$. Como a coordenada resultante é 0, os vetores gerados permanecem no subespaço A_0. Analogamente, o produto entre torais t_jt_k em A_0 resulta no próprio toral ou em zero, o que conclui que $A_0A_0 \subseteq A_0$. Expandindo a análise para a propagação com outros autovalores, tomamos $x = e^\alpha \in A_0$ e $y = e^\beta \in A_{a_j}$. Aqui, temos $\alpha_i = 0$ e $\beta_i = 1$. Ao avaliar o produto, a soma na coordenada de posição i fornece $0 + 1 = 1$. Sendo assim, o novo vetor associado a $\alpha + \beta$ obrigatoriamente possui 1 na posição i, impossibilitando sua pertinência a A_0. Ele deve habitar a soma direta dos autoespaços não triviais, o que justifica a lei $A_0A_{a_j} \subseteq \bigoplus A_{a_k}$. Por fim, analisamos a inversão que ocorre ao multiplicar dois elementos dos autoespaços não triviais. Tomando $x = e^\alpha \in A_{a_j}$ e $y = e^\beta \in A_{a_k}$ com $k \neq j$, primeiramente, note que $x \neq y$ pois se fossem iguais, ambos gerariam o mesmo autovalor ao multiplicar por t_i. Além disso, ambos os vetores possuem 1 na posição i, ou seja, $\alpha_i = 1$ e $\beta_i = 1$. Ao calcular o produto, a nova palavra de código associada a $e^{\alpha+\beta}$ terá sua i-ésima coordenada dada pela soma modular $1 + 1 = 0 \pmod 2$, o que força os vetores gerados de volta para o subespaço A_0. Nos casos específicos em que $k = j$ temos duas alternativas, $\alpha \neq \beta$ ou $\alpha = \beta$, no primeiro caso. como ambas as palavras possuem 1 na iésima coordenada, obtemos que o produto deve cair em A_0. Por outro lado, se $\alpha = \beta$, a definição do produto na álgebra dita que o produto recai sobre uma combinação linear dos elementos torais t_k, os quais pertencem a $A_1 \oplus A_0$. Consequentemente, o produto inteiro fica restrito a $A_1 \oplus A_0$, completando a demonstração da lei de fusão para todos os subespaços. □

Suponha agora que $a_{i,\alpha} \neq 1$ para todo $\alpha \in C^*$ com $\alpha_i = 1$. Então, vemos a partir do teorema anterior que a lei de fusão para t_i é $\mathbb{Z}_2$-graduada. Portanto, isso induz uma $\mathbb{Z}_2$-graduação em $A_C(\Lambda)$:

$$A_C(\Lambda) = A_+ \oplus A_-,$$

em que $A_+ := A_0 \oplus A_1$ e $A_- := \bigoplus A_{a_{i,\alpha}}$. Se char$(\mathbb{F}) \neq 2$, existe um automorfismo de álgebra natural, de ordem no máximo dois, denotado por $\tau_i \in$ Aut$(A_C(\Lambda))$, que age trivialmente em A_+ e inverte o sinal dos vetores em A_-. Chamamos τ_i de **involução de Miyamoto** associada a t_i. Note que quando A é não degenerada, A_- é não vazio e τ_i tem de fato ordem dois. O grupo $M = \langle \tau_i : i = 1, \ldots, n \rangle$ gerado pelas involuções de Miyamoto, é chamado de **grupo de Miyamoto**.

Proposição 1. *Suponha que char*$(\mathbb{F}) \neq 2$ *e seja* $A_C(\Lambda)$ *uma álgebra de código com parâmetros de estrutura regulares onde* $a_{i,\alpha} \neq 1$ *para todo* $i \in$ *supp*(α), $\alpha \in C^*$. *Defina* $G \leq$ *Aut*$(A_C(\Lambda))$ *como sendo o grupo gerado por Aut*(C) *e o grupo de Miyamoto* M. *Então*

$$G = M : \textit{Aut}(C)$$

é um produto semidireto de $M = \langle \tau_i : i = 1, \ldots, n \rangle$ *por Aut*(C).

Demonstração. Pelo Lema 2, Aut(C) possui uma ação fiel e bem definida sobre $A_C(\Lambda)$. Em particular, sua ação sobre t_i é dada pela permutação dos índices. Como M fixa todos os índices, temos $M \cap$ Aut$(C) = 1$. Seja $\alpha \in C$ e $i = 1, \ldots, n$. Como $\alpha_i = (\alpha g)_{g(i)}$ para todo $g \in$ Aut(C), vemos que $\tau_i g = g\tau_{g(i)}$. Em particular, temos que MAut$(C) =$ Aut$(C)M$ é um grupo e, portanto, $G = M$Aut(C). Além disso, M é um subgrupo normal de G e, assim, temos um produto semidireto. □

Por último, introduziremos a condição de Seress, que será fundamental para estabelecer em quais condições uma álgebra de código é uma álgebra axial de tipo Jordan.

Teorema 3. *Dizemos que a lei de fusão para um idempotente* e *satisfaz a* ***condição de Seress*** *se* $1, 0 \in \mathcal{F}$ *e* $A_0 A_\lambda \subseteq A_\lambda$, *para todos os autovalores* $\lambda \neq 1$.

Proposição 2. *Suponha que $a_{i,\alpha} \neq 1$ para todo $i \in$ supp(α), $\alpha \in C^*$. Então, a lei de fusão para t_i satisfaz a condição de Seress se, e somente se, t_i possui no máximo um autovalor que não é 0 ou 1.*

Demonstração. Pelo Teorema 2 não é difícil ver que a lei de fusão satisfaz a condição de Seress se ad_{t_i} possui no máximo um autovalor que não é 0 ou 1. Reciprocamente, suponha que a lei de fusão para ad_{t_i} satisfaz a condição de Seress e existe pelo menos um autovalor $\lambda \neq 0, 1$. Pelo Teorema 2, todos os e^α tais que $\alpha_i = 0$ estão no autoespaço associado a 0. Seja $e^\beta \in A_\lambda$. Por hipótese, a lei de fusão satisfaz a condição de Seress e, portanto, $b_{\alpha,\beta}e^{\alpha+\beta} = e^\beta e^\alpha \in A_\lambda$ para todo $\alpha \in C_0(i)$ tal que $\alpha \neq \beta^c$. Pelo Lema 1, este espaço tem dimensão de pelo menos $\frac{|C|}{2} - 1$ se $\mathbf{1} \in C$ e $\frac{|C|}{2}$ se $\mathbf{1} \notin C$. Pelo Teorema 2, $\dim A_1 \oplus A_0 = n + \frac{|C|}{2} - 1$. Como $\dim A$ é $n + |C| - 2$ se $\mathbf{1} \in C$ e $n + |C| - 1$ se $\mathbf{1} \notin C$, por um argumento de contagem, vemos que λ deve ser o único autovalor não trivial. □

Observamos que, se existe exatamente um autovalor a de t_i que é diferente de 1 ou 0, então a lei de fusão é a mesma que a das álgebras axiais de tipo Jordan conforme definição 5.

CONSIDERAÇÕES FINAIS

Neste trabalho, exploramos a rica estrutura das álgebras de código, compreendendo como propriedades originárias da teoria de códigos lineares binários se traduzem em características fundamentais na álgebra não associativa. A análise da decomposição de Peirce e a determinação dos ideais dessas álgebras revelaram sob quais circunstâncias elas se mantêm simples e evidenciaram o comportamento de seus autoespaços.

Além disso, o estudo dos grupos de Miyamoto e a aplicação das condições de Seress demonstraram ser passos essenciais, fornecendo as ferramentas algébricas necessárias para classificar tais estruturas como álgebras axiais de tipo Jordan.

Como desdobramento natural desta pesquisa, estudaremos outras propriedades estruturais dessas álgebras, bem como sob quais condições ela possui uma forma bilinear associativa, denominada Forma de Frobenius. Estudaremos exemplos ilustrativos, incluindo o caso do código de Hamming H_8, para o qual a álgebra associada A_{H_8} é axial.

Adicionalmente, exploraremos a relação entre álgebras código e álgebras de Jordan (veja [4]), procurando estabelecer condições necessárias e suficientes sobre o código

linear para que a álgebra associada seja de Jordan. Por fim, pretendemos estender esses resultados para o contexto de códigos não necessariamente binários.

REFERÊNCIAS

[1] CASTILLO-RAMIREZ, A.; MCINROY, J.; REHREN, F. **Code algebras, axial algebras and VOAs**. Journal of Algebra, v. 518, p. 146-176, 2019.

[2] HALL, J.I.; REHREN F.; SHPECTOROV S. **Primitive axial algebras of Jordan Type**. Journal of Algebra, v. 437, p. 79-115, 2015.

[3] LING, S.; XING, C. **Coding Theory: A First Course.** Estados Unidos: Cambridge University Press, 2004.

[4] MARTIN, M. E. **Deformações e Isotopias de álgebras de Jordan**. 2013. Tese (Doutorado) - Institute of Mathematics and Statistics, São Paulo University, São Paulo, 2013.