# Construção de Códigos $\mathbb{Z}_{2^k}$-pseudolineares através de Aplicações Casadas Isométricas e Extensões de Galois sobre Anéis Locais

Patricia de Rezende Barbosa, e Reginaldo Palazzo Jr.

*Abstract*— **Neste trabalho apresentamos um procedimento para a determinação das aplicações isométricas entre os espaços de Lee e de Hamming. Este procedimento faz uso dos conceitos de particionamento de conjuntos e de representação modular. Baseado nessas aplicações isométricas, apresentamos uma proposta de construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares através dos códigos cíclicos provenientes da extensão de Galois de dimensão $r$ sobre anéis locais.**

## I. Introdução

A $\mathbb{Z}_4$-linearidade proposta em [2] contribuiu significativamente ao processo de inserção dos códigos não lineares no contexto de transmissão da informação bem como no estudo das características lineares inerentes a tais códigos.

No contexto de inserção dos códigos não lineares no processo de transmissão da informação em [13] mostrou-se a não existência de códigos $\mathbb{Z}_{2^k}$-lineares pois o grupo de simetrias de $\mathbb{Z}_2^k$ não possui um subgrupo cuja ação seja fortemente transitiva sobre $\mathbb{Z}_2^k$. A ação ser fortemente transitiva implica que a aplicação $m_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^k$ tenha que ser uma bijeção e que os espaços métricos sejam isométricos.

Nesta direção em [10] foi mostrada a possibilidade de que se a aplicação $m_k$ for injetora então é possível obter-se o casamento e mais, a isometria entre os espaços métricos $(\mathbb{Z}_{2^k}, d_L)$ e $(\mathbb{Z}_2^{2^{k-1}}, d_H)$. Esta classe de códigos foi chamada códigos $\mathbb{Z}_{2^k}$-*pseudolineares*.

Neste trabalho apresentamos um procedimento sistemático para a determinação das aplicações (injetivas) isométricas entre os espaços de Lee e de Hamming. Para alcançarmos este objetivo faremos uso do conceito de particionamento de conjuntos, equivalentemente, o de recobrimento de regiões $2^k \times 2^k$ através de subregiões que serão identificadas como sendo as regiões de Voronoi associadas aos elementos do alfabeto do código. Com isso, mostraremos que tais regiões são congruentes e que portanto, são geometricamente uniformes. Dessa forma, o processo de decodificação fica bastante simplificado. Uma vez realizado o particionamento será necessário estabelecer a aplicação $m_k$ tal que os espaços métricos de Lee e de Hamming sejam isométricos. Para tal, iremos fazer uso do conceito de representação modular. Finalmente, de posse das aplicações isométricas apresentamos a proposta de construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares através dos códigos BCH provenientes da extensão de Galois de dimensão $r$ sobre $\mathbb{Z}_{2^k}$.

A autora está no Programa de Mestrado, FEEC-UNICAMP, email:pbarbosa@dt.fee.unicamp.br

O autor está no Departamento de Telemática, FEEC-UNICAMP. Este trabalho foi financiado pela Fundação de Amparo à Pesquisa do Estado de São Paulo, FAPESP, 95/4720-8, e pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico, CNPq, 301416/85-0, Brasil. email:palazzo@dt.fee.unicamp.br.

## II. Preliminares

Nesta seção iremos apresentar os conceitos necessários para o entendimento e a fundamentação da proposta de construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares.

### A. Recobrimento de regiões $\mathbb{Z}_{2^k} \times \mathbb{Z}_{2^k}$

Dada uma célula básica de ordem $4^k$, gerada por aritmética modular, consistindo de células em um reticulado regular em $\mathbb{Z}^2$, a pergunta que se faz é a seguinte: quais são os possíveis formatos $S_j$ destas células que recobrem a célula básica dada sob a restrição de que para uma célula demarcada em $S_j$ a distância entre essas células na justaposição dos $S_j$'s é a maior possível?

A motivação por trás deste problema está relacionada com a determinação das aplicações isométricas $m_k : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^{2^{k-1}}$ que deverão ser utilizadas na construção dos códigos $\mathbb{Z}_{2^k}$-pseudolineares [10]. Além desta aplicação, existem outras tais como armazenagem de dados em meios ópticos ou magnéticos, modulações digitais tipo $M$-QAM, alocação de frequência em telefonia móvel, etc., consideradas em [6], [8], [11], e [12].

Uma solução sistemática deste problema de recobrimento é importante. Uma maneira de se alcançar este objetivo é usar de um procedimento que, a princípio, se resume a duas etapas. A primeira etapa está relacionada com o problema da partição do número inteiro $2^k$. Esta partição deverá fornecer todos os possíveis formatos com $2^k$ células. A segunda etapa está relacionada com o grupo de simetrias associado a cada possível formato resultante da partição de $2^k$. Em princípio, todos os formatos com o maior número de simetrias são os candidatos. Entre estes, somente os que satisfazem o critério de distância são selecionados. Esses são os formatos que irão recobrir a célula básica sob as restrições colocadas.

O conjunto de formatos que apresenta a maior distância possível entre as células demarcadas, é aquele constituído pelos formatos que recobrem a região. Este conjunto é exatamente o conjunto das possíveis regiões de Voronoi $S_j$, $1 \leq j \leq k$, que recobre a região considerada. Para ver isto, considere uma célula básica de ordem $4^k$. Note que esta célula básica é formada por $2^k$ classes laterais com $2^k$ elementos em cada classe. Considere agora somente uma das classes. Suponha que possamos especificar através da partição $2^k$-ária a localização de cada um dos $2^k$ elementos. Assim, a forma que irá recobrir esta região vem naturalmente, [7].

A técnica de particionamento de conjuntos [6] será utilizada neste caso para determinar a localização dos dígitos do alfabeto do código e também as possíveis regiões de Voronoi em um arranjo de $2^k \times 2^k$, células com a maior distância de Lee possível.

### *B. Uniformidade geométrica*

Seja $S$ um conjunto finito de sinais pertencente a um espaço métrico $(M, d)$. O grupo de simetrias de $S$, denotado por $\Gamma(S)$, consiste do conjunto de isometrias de $S$ tal que $\gamma(S) = S$, onde $\gamma$ é uma isometria em $\Gamma(S)$.

Seja $S$ o conjunto a ser associado ao alfabeto do código e seja $G$ um grupo, então

*Definição 1:* Um grupo $(G, *)$ atua em um conjunto de sinais $S$, se existe um homomorfismo $\sigma : G \to \Gamma(S)$. Nestas condições, a órbita de $s \in S$ sob a ação de $G$ é o conjunto $Orb_G(s) = \{\sigma(g)(s); g \in G\}$. Se para cada $s_1, s_2 \in S$, existe um $g \in G$, tal que $\sigma(g)(s_1) = s_2$, então $G$ atua transitivamente em $S$.

Da Definição 1 decorre que o conjunto de sinais $S$ é geometricamente uniforme.

*Definição 2:* [3] Um conjunto de sinais S está casado a um grupo G se existir uma aplicação $m : G \longrightarrow S$ tal que para todos $g, g' \in G$ ,

$$d(m(g), m(g')) = d(m(g^{-1} \cdot g'), m(e))$$

chamamos $m$ de aplicação casada. Se $m$ é injetora dizemos que $m^{-1}$ é um rotulamento casado.

Se $m : G \to S$ é uma aplicação casada então $H = m^{-1}(m(e))$ é um subgrupo de $G$ e $g \equiv g' \ mod \ H$ se, e somente se, $m(g) = m(g')$. Assim, qualquer aplicação casada $m$ corresponde a uma bijeção $gH \longmapsto m(g)$ das classes laterais à esquerda de $H$ em $G$ nos elementos de $S$. É imediato, via o teorema do homorfismo [15], que se $H \lhd G$, $H$ um subgrupo normal de $G$, então a aplicação quociente $m : \dfrac{G}{H} \to S$ é um rotulamento casado. Dizemos que um rotulamento $m : G \to S$ é um rotulamento efetivo se $H$ não contém nenhum subgrupo normal de $G$ não trivial. Neste caso, dizemos que $S$ é efetivamente casado a $G$.

*Teorema 3:* [3] Existe um rotulamento casado entre um conjunto de sinais $S$ e um grupo $G$ se, e somente se, $G$ é isomorfo a um subgrupo transitivo de $\Gamma(S)$.

*Definição 4:* [9] Dado um conjunto de sinais $S$, dizemos que um subgrupo $U(S)$ de $\Gamma(S)$ é um grupo gerador de $S$ se $S = \{u(s_0) : u \in U(S)\}$ para $s_0$ fixo em $S$ e $U(S)$ é minimal para a geração de S no sentido que a função $m : U(S) \to S$, $m(u) = u(s_0)$ é uma bijeção.

*Definição 5:* [9] Dizemos que um código $\mathcal{C} \subseteq \mathcal{S}^{\mathcal{I}}$ é $G$-linear se existem uma isometria $\mu : G \to S$, um código de grupo $\mathcal{D} \leq \mathcal{G}^{\mathcal{I}}$ e uma permutação $\sigma \in S_I$ tal que $\sigma(\mathcal{C}) = \mu(\mathcal{D})$, onde denotamos também por $\mu$ a extensão $\mu : G^I \to S^I$.

*Teorema 6:* [9] Seja $S$ um conjunto de sinais, então as seguintes afirmações são equivalentes:

*(i)* $S$ é geometricamente uniforme;
*(ii)* Existe um rotulamento casado entre $S$ e o grupo $U(S)$;
*(iii)* $S$ é $U(S)$-linear com $m : U(S) \to S$.

### *C. Representação modular*

A importância do conceito de representação modular está relacionada com o seguinte problema. Dada a matriz geradora de um código linear, então o vetor espectro de pesos de Hamming das palavras-código é facilmente determinado. Todavia, dado um vetor espectro de pesos de Hamming o que se deseja é determinar a existência de uma matriz geradora associada a este espectro de pesos. Nesta direção é que iremos apresentar o procedimento para resolver este problema.

Para isso, considere $G_0$ como sendo a matriz geradora de um código binário linear $(n, k)$. Então $G_0$ pode ser interpretada como tendo $k$ linhas e $n$ diferentes *tipos* de colunas, onde por *tipo* queremos dizer a representação binária de um inteiro, isto é, um elemento de $\mathbb{F}_2^k$. Como em geral um rearranjo das colunas implica em um código equivalente, e se rearranjos não são importantes, então um código pode ser descrito por um conjunto de colunas de cada tipo.

Seja $M$ uma matriz que tenha como colunas todas as possíveis combinações de $k$ elementos de $\mathbb{F}_2$ exceto a combinação nula. Assim, $M$ é uma matriz $k \times 2^k - 1$ onde a $j$-ésima coluna de $M$, para $1 \leq j \leq 2^k - 1$, é a coluna tipo $j$. Com isso, a representação modular de $M$ é dada pelo vetor de comprimento $2^k - 1$, consistindo de um elemento de cada tipo, isto é, $N = (1, 1, \cdot, \cdot, \cdot, 1)$. Então a matriz geradora $G$ de um código binário linear pode ser descrita por um vetor de $m$ componentes, onde cada componente é um inteiro positivo, $n_i$, representando o número de colunas do tipo $i$, isto é,

$$N = (n_1, n_2, \ldots, n_m), \qquad \text{tal que} \qquad \sum_{i=1}^{m} n_i = n.$$

Chamamos $N$ de *representação modular*.

Considere $K$ como sendo a matriz dada por $K = M^T G_0$. Então, $K$ tem como linhas todas as possíveis combinações lineares das linhas de $G_0$, consequentemente, tem todas as palavras-código como linhas.

Considere agora a matriz $C$ como sendo $C = M^T M$, então $C$ é uma matriz simétrica. Com isso, temos o seguinte resultado:

*Teorema 7* (MacDonald, [16]) O vetor espectro de pesos de Hamming, $W$, das $2^k - 1$ palavras-código não nulas de um código de grupo binário pode ser determinado como as componentes do vetor resultante da multiplicação, como matrizes de números reais, do vetor de representação modular $N$ pela matriz $C$, isto é, $W = NC$.

Note que se a matriz $C$ for vista como uma matriz de números reais, então a mesma é não-singular. A inversa de $C$ é facilmente determinada como sendo

$$C^{-1} = \frac{2C - J}{2^{k-1}},$$

onde $J$ é a matriz com todos os elementos 1.

Do Teorema 7, temos que um dado conjunto de pesos é factível se puder ser arranjado em um vetor $W$ tal que $N = WC^{-1}$ tenha componentes que sejam inteiros não negativos.

## III. Extensão de Anéis de Galois

A motivação para se utilizar o conceito de extensão de anéis de Galois, [15], em teoria da codificação está diretamente relacionada com a construção de códigos cíclicos sobre anéis locais $\mathbb{Z}_q$, onde $q$ é uma potência de um primo, $q = p^k$.

Como estamos interessados no processo de geração de códigos binários não lineares via a aplicação $m_k$ iremos considerar nesta seção um procedimento de construção de códigos BCH sobre anéis $\mathbb{Z}_q$.

A diferença básica da construção de códigos BCH sobre anéis para a construção tradicional de códigos BCH sobre corpos reside no fato de que as raízes do polinômio gerador dos códigos BCH sobre anéis encontram-se na extensão do anel $\mathbb{Z}_q$, ao invés de serem encontradas na extensão do corpo $\mathbb{F}_q$.

Iremos considerar o caso em que $p$ e $n$ são relativamente primos, isto é, o máximo divisor comum é um, denotado por $mdc(n,p) = 1$. É de conhecimento geral que um código cíclico de comprimento $n$ sobre $\mathbb{Z}_q$ é o ideal principal no anel de polinômios sobre $\mathbb{Z}_q$ módulo $(x^n - 1)$ e que este ideal é gerado por qualquer polinômio $g(x)$ que divide $(x^n - 1)$.

Sejam $\mathbb{Z}_q[x]$ o anel de polinômios sobre $\mathbb{Z}_q$ e $p(x)$ um polinômio primitivo de grau $r$ irredutível sobre $\mathbb{F}_p$ e, consequentemente, irredutível sobre $\mathbb{Z}_q$. Denotaremos o anel de Galois por $GR(p^k, r)$ como sendo o quociente de $\mathbb{Z}_q[x]$ pelo ideal gerado por $p(x)$, denotado por $\langle p(x) \rangle$, isto é,

$$R \cong GR(p^k, r) \cong \frac{\mathbb{Z}_q[x]}{\langle p(x) \rangle}.$$

Note que $GR(p^k, r)$ consiste de todas as classes laterais de polinômios sobre $\mathbb{Z}_q$ módulo $p(x)$, equivalentemente, consiste do conjunto de todos os polinômios de grau $r - 1$ com as operações de soma e multiplicação $mod\, p(x)$. Além disso, $R$ é um anel comutativo com identidade denominado *extensão de Galois de dimensão $r$ de $\mathbb{Z}_q$*. Esta extensão é única a menos de isomorfismo [15].

Como estamos interessados na classe dos códigos cíclicos, então o objetivo será de fornecer um procedimento para a construção de tais códigos. O primeiro passo está relacionado com a fatoração de $(x^n - 1)$. É de conhecimento que o grupo das unidades de $R$, denotado por $R^*$, é um grupo abeliano multiplicativo. Por ser abeliano, o mesmo pode ser decomposto como o produto direto de grupos cíclicos. Da mesma forma que no corpo, estamos interessados em grupos cíclicos cujos elementos são raízes de $(x^n - 1)$, para algum $n$ tal que $mdc(n,p) = 1$.

Os resultados a seguir fornecem os elementos necessários para a construção do grupo cíclico de interesse $G_n$, isto é, o subgrupo cíclico de $R^*$ (como sendo a extensão do anel $\mathbb{Z}_{p^k}$) contendo todas as raízes de $(x^n - 1)$.

*Teorema 8:* [15] Existe um único subgrupo cíclico de $R^*$ cuja ordem é relativamente prima a $p$. Este subgrupo tem ordem $p^r - 1$.

*Teorema 9:* [14] Suponha que $f \in R$ gere um subgrupo de ordem $n$ em $R^*$, onde $mdc(n,p) = 1$. Então o polinômio $(x^n - 1)$ pode ser fatorado como $x^n - 1 = (x - f)(x - f^2) \cdots (x - f^n)$ se, e somente se, $R_p(f)$ tem ordem $n$ em $\mathbb{F}^*_{p^r}$ (grupo multiplicativo de $\mathbb{F}_{p^r}$), onde $R_p(f)$ denota o resto da divisão de $f$ por $p$.

*Corolário 10:* [14] Um polinômio $h(x)$ que divide $(x^n - 1)$ e possui coeficientes em $\mathbb{Z}_q$ pode ser fatorado em $G_n$ como

$$h(x) = (x - \beta^{e_1})(x - \beta^{e_2}) \cdots (x - \beta^{e_l}),$$

se, e somente se, $R_p(h(x))$ pode ser fatorado sobre $\mathbb{F}_{p^k}$ como

$$R_p(h(x)) = (x - R_p(\beta)^{e_1})(x - R_p(\beta)^{e_2}) \cdots (x - R_p(\beta)^{e_l}).$$

onde $\beta$ é o elemento gerador de $G_n$.

*Teorema 11:* [14] Suponha que $\overline{f} = R_p(f)$ gere um subgrupo cíclico de ordem $n$ em $\mathbb{F}^*_{p^r}$. Então $f$ gera um subgrupo cíclico de ordem $nd$ em $R^*$, onde $d$ é um inteiro maior ou igual a 1, e $f^d$ gera o subgrupo cíclico $G_n$ de $R^*$.

Note que o grupo cíclico $G_n$ é obtido do Teorema 11, enquanto que o polinômio minimal de $\beta^i \in R^*$ é obtido do Corolário 10. Dessa forma, o código cíclico terá polinômio gerador dado por $g(x) = mmc\{m_1(x), m_2(x), \cdots, m_j(x)\}$, onde $m_i(x)$ denota o polinômio minimal associado ao elemento $\beta^i$, e $mmc$ denota o mínimo multiplo comum.

### *A. Exemplo de $GR(4,3)$*

Nesta seção iremos considerar um exemplo da técnica de extensão de Galois sobre anéis locais (referimos o leitor para [5]). Iremos considerar o anel $GR(4,3)$ dado por

$$\begin{aligned} GR(4,3)[x] &= \frac{\mathbb{Z}_4[x]}{\langle x^3 + x + 1 \rangle} \\ &= \left\{ a + bx + cx^2;\ a, b, c \in \mathbb{Z}_4 \right\}. \end{aligned}$$

Considere agora o corpo $\mathbb{F}_8[x]$ proveniente da extensão através de um polinômio de grau 3, isto é,

$$\mathbb{F}_8[x] = \frac{\mathbb{F}_2[x]}{\langle x^3 + x + 1 \rangle} = \{a' + b'x + c'x^2;\ a', b', c' \in \mathbb{F}_2\}$$

$$= \{0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2\}$$

Seja $\alpha$ um elemento primitivo em $\mathbb{F}_8$, equivalentemente, $\alpha$ é uma raiz de $x^3 + x + 1 = 0$, ou seja, $\alpha^3 = \alpha + 1$. Com isso, os elementos de $\mathbb{F}_8$ são mostrados na Tabela I.

Seja $f = (0\ 1\ 0) \in GR^*(4,3)$, onde $GR^*(4,3)$ denota o grupo das unidades de $GR(4,3)$. Então, $\overline{f} = R_2(f) = (0\ 1\ 0) = f$ gera um subgrupo cíclico de ordem $n = (2^r - 1) = 7$ em $\mathbb{F}_8$, onde $R_2(f)$ é a redução módulo 2 do elemento $f$. Assim, $f$ deve gerar um grupo de ordem $nd = 7d$ em

| | |
|---|---|
| $0 \rightarrow$ | $(\ 0\ \ 0\ \ 0\ )$ |
| $1 \rightarrow$ | $(\ 1\ \ 0\ \ 0\ )$ |
| $\alpha \rightarrow$ | $(\ 0\ \ 1\ \ 0\ )$ |
| $\alpha^2 \rightarrow$ | $(\ 0\ \ 0\ \ 1\ )$ |
| $\alpha^3 \rightarrow$ | $(\ 1\ \ 1\ \ 0\ )$ |
| $\alpha^4 \rightarrow$ | $(\ 0\ \ 1\ \ 1\ )$ |
| $\alpha^5 \rightarrow$ | $(\ 1\ \ 1\ \ 1\ )$ |
| $\alpha^6 \rightarrow$ | $(\ 1\ \ 0\ \ 1\ )$ |

TABLE I

ELEMENTOS DE $\mathbb{F}_8$

$GR^*(4,3)$, onde $d \geq 1 \in \mathbb{Z}$ e $f^d$ gera o subgrupo cíclico $G_n$ de $GR^*(4,3)$.

As operações em $GR^*(4,3)$ são feitas módulo $x^3 + x + 1$. Logo, $x^3 = -x - 1 = 3x + 3$ (coeficientes em $\mathbb{Z}_4$). Então, considerando $f = (0\ 1\ 0) = x$, a representação dos elementos de $GR^*(4,3)$ é como mostrada na Tabela II.

| | | | |
|---|---|---|---|
| $0 \rightarrow$ | $(\ 0\ \ 0\ \ 0\ )$ | $f^7 \rightarrow$ | $(\ 3\ \ 0\ \ 2\ )$ |
| $1 \rightarrow$ | $(\ 1\ \ 0\ \ 0\ )$ | $f^8 \rightarrow$ | $(\ 2\ \ 1\ \ 0\ )$ |
| $f \rightarrow$ | $(\ 0\ \ 1\ \ 0\ )$ | $f^9 \rightarrow$ | $(\ 0\ \ 2\ \ 1\ )$ |
| $f^2 \rightarrow$ | $(\ 0\ \ 0\ \ 1\ )$ | $f^{10} \rightarrow$ | $(\ 3\ \ 3\ \ 2\ )$ |
| $f^3 \rightarrow$ | $(\ 3\ \ 3\ \ 0\ )$ | $f^{11} \rightarrow$ | $(\ 2\ \ 1\ \ 3\ )$ |
| $f^4 \rightarrow$ | $(\ 0\ \ 3\ \ 3\ )$ | $f^{12} \rightarrow$ | $(\ 1\ \ 3\ \ 1\ )$ |
| $f^5 \rightarrow$ | $(\ 1\ \ 1\ \ 3\ )$ | $f^{13} \rightarrow$ | $(\ 3\ \ 0\ \ 3\ )$ |
| $f^6 \rightarrow$ | $(\ 1\ \ 2\ \ 1\ )$ | $f^{14} \rightarrow$ | $(\ 1\ \ 0\ \ 0\ )$ |

TABLE II

ELEMENTOS DE $GR^*(4,3)$

Portanto, $nd = 14$ implicando que $d = 2$. Logo, $f$ gera um grupo de ordem 14 em $GR^*(4,3)$ e, portanto, $f^2 = x^2 = (0\ 0\ 1)$ gera um grupo de ordem 7 em $GR^*(4,3)$. Assim, $\beta = x^2$ é um elemento primitivo em $G_7$.

Podemos agora construir um código BCH de comprimento $n = 7$ sobre $\mathbb{Z}_4$. Considerando que a distância de projeto (distância de Hamming) do código seja $d_{\min} \geq 3$, o polinômio gerador $g(x)$ do código tem como raízes $\beta$ e $\beta^2$. Este polinômio é dado por $g(x) = mmc(m_1(x),\ m_2(x))$, onde $m_i(x)$ é o polinômio minimal de $\beta^i$, $i = 1, 2$.

O polinômio minimal de $\beta$ e $\beta^2$ é dado por

$$\begin{aligned} m_1(x) = m_2(x) \quad &= (x-\beta)(x-\beta^2)(x-\beta^4) \\ &= 3 + x + 2x^2 + x^3. \end{aligned}$$

A correspondente matriz geradora $G$ é dada por

$$G = \begin{bmatrix} 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 3 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 3 & 1 & 2 & 1 \end{bmatrix}$$

## IV. CÓDIGOS $\mathbb{Z}_{2^k}$-PSEUDOLINEARES, $k \geq 3$

No caso $\mathbb{Z}_4$, [2], observamos que a aplicação $m_2$ possui a característica de associar um código quaternário linear a um código binário, isto é, $m_k : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$ sendo que este apresenta a propriedade de que o perfil de distâncias é o mesmo para qualquer palavra-código considerada. Isto é exatamente a propriedade de casamento, [3], entre o grupo $\mathbb{Z}_4$ e o conjunto de sinais $\mathbb{Z}_2^2 = \mathbb{Z}_2 \times \mathbb{Z}_2$.

*Definição 12:* A distância de Lee entre $a$ e $b \in \mathbb{Z}_q$ é definida por $d_{Lee}(a,b) = w_{Lee}(a \ominus b),\ \ a, b \in \mathbb{Z}_q$ com

$$w_{Lee}(a) = \begin{cases} a, & \text{se} \quad a \leq \left\lfloor \frac{q}{2} \right\rfloor \\ q - a, & \text{se} \quad a > \left\lfloor \frac{q}{2} \right\rfloor \end{cases}$$

onde $\lfloor x \rfloor$ denota o maior inteiro menor ou igual a $x$, $\ominus$ denota subtração módulo $q$, e $w_{Lee}$ denota o peso de Lee. Assim, $(\mathbb{Z}_q, d_{Lee})$ é um espaço métrico.

Como em $\mathbb{Z}_4$ é natural associar a distância de Lee e em $\mathbb{Z}_2^2$ a distância de Hamming, então os espaços métricos $(\mathbb{Z}_4, d_{Lee})$ e $(\mathbb{Z}_2^2, d_H)$ são isométricos.

De modo a estender a aplicação $m_k$ para alfabetos $2^k$-ários precisamos conhecer a estrutura do domínio e da imagem da aplicação $m_k$.

Nesta seção, consideramos um procedimento para a determinação da aplicação casada isométrica $m_k$ entre o espaço de Lee, $(\mathbb{Z}_{2^k}, d_{Lee})$ e o espaço de Hamming $(\mathbb{Z}_2^{2^{k-1}}, d_H)$, isto é,

$$m_k : \mathbb{Z}_{2^k} \rightarrow \mathbb{Z}_2^{2^{k-1}}, \qquad k \geq 3$$

para a construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares. O procedimento que usaremos na determinação das aplicações casadas e isométricas $m_k$ faz uso da técnica de particionamento de conjuntos proposta em [6], e da representação modular.

Note que para $k = 2$, a aplicação casada $m_2 : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$ é isométrica e também uma bijeção, isto é, $m_2$ é um rotulamento casado e mais do que isso, é um rotulamento efetivo. Com isso, das Definições 4 e 5 e Teorema 6, vemos que existem códigos $\mathbb{Z}_4$-lineares. Todavia, para $k \geq 3$ as aplicações $m_k$ são casadas porém não efetivas. Quando isso ocorre, dizemos que os códigos são $\mathbb{Z}_{2^k}$-pseudolineares.

### A. Aplicações casadas isométricas

Com o objetivo de estabelecer as aplicações casadas isométricas entre os símbolos de $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_{16}$ e $\mathbb{Z}_{32}$ com os símbolos de $\mathbb{Z}_2^2$, $\mathbb{Z}_2^4$, $\mathbb{Z}_2^8$ e $\mathbb{Z}_2^{16}$ é que iremos considerar como exemplo o caso da aplicação entre $\mathbb{Z}_8$ e $\mathbb{Z}_2^4$.

Na Fig. 1 é mostrado a representação de pares ordenados de $\mathbb{Z}_8 \times \mathbb{Z}_8$ bem como as palavras-código do código de grupo cíclico $C = \{00, 13, 26, 31, 44, 57, 62, 75\}$.

A determinação do código de grupo cíclico é uma consequência de se encontrar uma transformação conveniente com as características de que as linhas desta transformação sejam vetores linearmente independentes e tal que o determinante da transformação seja igual a $2^k$, onde $k$ é um inteiro positivo. Equivalentemente, realizar o particionamento da célula básica $2^k \times 2^k$. É desejável que pelo menos uma das linhas da transformação seja uma das soluções inteiras provenientes da equação de Diofanto $x^2 + y^2 = 2^k$. Todavia, nem sempre é possível satisfazer tal condição, uma vez que a geração de um conjunto cíclico via a transformação pode estar fora do espaço das soluções de Diofanto.

Como neste caso $x^2 + y^2 = 8$, então dentre o conjunto de soluções selecionamos as soluções $(3, 1)$ e $(1, 3)$ que conduzem a um código de grupo cíclico como mostrado na Fig. 1.

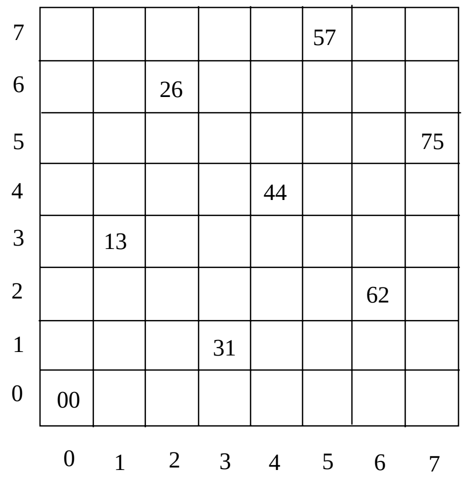


Fig. 1. Arranjo $\mathbb{Z}_8 \times \mathbb{Z}_8$ com seus respectivos pares ordenados

A determinação da aplicação isométrica faz uso do conceito de representação modular. Note na Fig. 1 que os pesos de Lee são obtidos a partir do menor número de quadrados que são necessários para se atingir uma palavra-código partindo da palavra-código 00. Com isso, o vetor espectro de peso é dado por $W = (4, 4, 4, 8, 4, 4, 4)$. Consequentemente, o vetor representação modular é obtido de $N = WC^{-1}$. Dessa forma, $N = (0, 0, 0, 2, 2, 2, 2)$. É fácil de se ver que os dígitos que formam as palavras-código têm peso de Lee par, consequentemente $N = (0, 0, 0, 1, 1, 1, 1)$ pode ser usado como o vetor representação modular. Portanto, a aplicação casada isométrica entre os símbolos de $\mathbb{Z}_8$ e os símbolos de $\mathbb{Z}_2^4$ é dada por

| $m_3$ : $\mathbb{Z}_8$ | $\rightarrow$ | $\mathbb{Z}_2^4$ |
|---|---|---|
| 0 | | 0000 |
| 1 | | 0101 |
| 2 | | 0011 |
| 3 | | 0110 |
| 4 | | 1111 |
| 5 | | 1010 |
| 6 | | 1100 |
| 7 | | 1001 |

Gostaríamos de chamar a atenção ao fato de que as regiões de Voronoi são retângulos $2 \times 4$ e que as mesmas são congruentes.

Ao fazermos uso deste procedimento para os demais casos, chegamos às Tabelas III e IV onde são apresentados para cada alfabeto os vetores peso, $W$, os vetores tipo, $N$, e as aplicações isométricas na forma matricial. A notação $\left(4^3, 8, 4^3\right)$ utilizada em ambas as tabelas significa $(4, 4, 4, 8, 4, 4, 4)$.

Conhecendo as aplicações isométricas entre $(\mathbb{Z}_{2^k}, d_{Lee})$ e $(\mathbb{Z}_2^{2^{k-1}}, d_H)$ e fazendo uso do conceito de extensão de Galois de dimensão $r$ sobre $\mathbb{Z}_{2^k}$, apresentamos a seguir alguns códigos $\mathbb{Z}_{2^k}$-pseudolineares gerados através dos códigos BCH sobre $\mathbb{Z}_{2^k}$.

Os códigos $\mathbb{Z}_{2^k}$-pseudolineares provenientes de $GR(2^k, 2)$ são códigos lineares, com excessão dos correspondentes códigos duais. Os códigos apresentados na Tabela V são códigos não lineares cujas distâncias de Hamming são iguais às dos códigos lineares binários, [17], portanto apresentando a mesma capacidade de correção de erros. No caso do $GR(4, 4)$ este é o melhor código obtido. Todavia, o correspondente código binário linear apresenta $d_H = 11$. Como as aplicações isométricas apresentam a propriedade de que os rótulos possuem peso de Lee que são múltiplos de 4 e que os mesmos constituem um conjunto geometricamente uniforme, a complexidade do processo de decodificação é bastante simplificada quando comparada com a complexidade do processo de decodificação do código linear binário.

## V. Conclusões

Neste trabalho foi apresentado um procedimento para a determinação das aplicações isométricas entre os espaços de Lee e de Hamming. Este procedimento fez uso dos conceitos de particionamento de conjuntos e de representação modular. Baseado nestas aplicações isométricas, foi apresentado um procedimento para a construção de códigos $\mathbb{Z}_{2^k}$-pseudolineares através dos códigos cíclicos provenientes da extensão de Galois de dimensão $r$ sobre os anéis de inteiros módulo $q = 2^k$.

## References


[1] J. R. Gerônimo, *Extensões da $\mathbb{Z}_4$-linearidade via Grupos de Simetrias*, Tese de Doutorado, FEEC-UNICAMP, 1997.

[2] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 301-319, March 1994.

[3] H. A. Loeliger, "Signal sets matched to groups," *IEEE Trans. Inform. Theory*, vol. IT-37, pp. 1675-1682, Nov. 1991.

[4] G.D. Forney, "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol.IT-37, pp. 1241-1260, Set. 1991.

[5] José Carmelo Interlando, *Uma Contribuição aos Códigos Lineares sobre Anéis Locais*, Tese Doutorado, FEEC-UNICAMP, 1994.

[6] C. de Almeida, *Modulação Codificada Generalizada via Equação de Diofanto*, Tese Doutorado, FEEC-UNICAMP, 1990.

[7] R. Palazzo, Jr., e C. de Almeida, "Tiling with polyominoes under the modular arithmetic and distance criteria," *1994 IEEE International Symposium on Information Theory*, Noruega.

[8] C. de Almeida e R. Palazzo, Jr., "Efficient two dimensional interleaving technique by use of the set partitioning concept," *IEE Electronics Letters*, vol. 32, No.6, pp. 538-540, Março 1996.

[9] H. Lazari, e R. Palazzo, Jr., "Geometrically uniform partitions of signal sets in the hyperbolic plane," *Seventh Intl. Workshop on Algebraic and Combinatorial Coding Theory*, 2000, Bansko, Bulgaria.

[10] R. Palazzo, Jr., J.R. Gerônimo, e J.A.F. Afonso, "Proposta de construção de códigos $\mathbb{Z}_8$ e $\mathbb{Z}_9$ pseudolineares," *15 Simpósio Brasileiro de Telecomunicações*, 1997, Recife, pp.493-497.

[11] C. de Almeida, e R. Palazzo, Jr., "On the frequency allocation for mobile radio telephone systems," *IEEE Intl. Symposium on Personal, Indoor and Mobile Radio Communications*, Toronto, Canada, pp. 96-99, 1995.

| Alfabeto | Vetor Peso (W) | Vetor Tipo (N) |
|---|---|---|
| $\mathbb{Z}_4$ | $(3,2,3)$ | $(2,1,1)$ |
| $\mathbb{Z}_8$ | $(4,4,4,8,4,4,4)$ | $(0,0,0,2,2,2,2)$ |
| $\mathbb{Z}_{16}$ | $(8,4,8^3,12,8,16,8,12,8^3,4,8)$ | $(0^7,2,2,2,2,4,4,0,0)$ |
| $\mathbb{Z}_{32}$ | $(8^4,16^7,24^4,32,24^4,16^7,8^4)$ | $(0^{15},2,2,2,2,8,0^3,10,2,2,2,0^4)$ |

TABLE III

Tabela contendo o alfabeto, o vetor peso e o vetor tipo

| Alfabeto | Vetor Tipo (N) | Aplicação Isométrica |
|---|---|---|
| $\mathbb{Z}_4$ | $(0,1^2)$ | $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ |
| $\mathbb{Z}_8$ | $(0^3,1^4)$ | $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ |
| $\mathbb{Z}_{16}$ | $(0^7,1^4,2^2,0^2)$ | $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$ |
| $\mathbb{Z}_{32}$ | $(0^{15},1^4,4,0^3,5,1^3,0^4)$ | $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$ |

TABLE IV

Tabela das aplicações isométricas

| Extensão de Galois | $g(x)$ | $(n,k,d_L)$ | $(n',k',d_H)$ | Código |
|---|---|---|---|---|
| GR(4,3) | $3+x+2x^2+x^3$ | $(7,4,4)$ | $(14,8,4)$ | não linear |
| GR(4,4) | $1+x+3x^2+3x^4+3x^5$ $+2x^7+x^8+2x^9+x^{10}$ | $(15,5,10)$ | $(30,10,10)$ | não linear |
| GR(8,2) | $1+x+x^2$ | $(3,1,6)$ | $(12,3,6)$ | linear |
| GR(8,3) | $7+5x+6x^2+x^3$ | $(7,4,8)$ | $(28,12,8)$ | não linear |

TABLE V

Tabela de códigos $\mathbb{Z}_{2^k}$-pseudolineares


[12] C. de Almeida, e R. Palazzo, Jr., "Binary quadratic forms: a solution to the set partitioning problem over GF(q)," *IEEE Intl. Symposium on Information Theory*, San Diego, 1990.

[13] J.R. Gerônimo, R. Palazzo, Jr., S.I.R. Costa, J.C. Interlando, e P. Brumatti, "Sobre a não existência de códigos $\mathbb{Z}_{2^k}$-lineares binários, onde $k \geq 3$," *15 Simpósio Brasileiro de Telecomunicações*, setembro 8-12, 1997, Recife.

[14] P. Shankar, "On BCH codes over arbitrary integer rings," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 480-483, July 1979.

[15] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.

[16] W.W. Peterson, e E.J. Weldon Jr., *Error Correcting Codes*, MIT Press, 1962.

[17] A. E. Brower, and T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory,* vol.IT-39, pp. 662-677, 1993.