Caracterização Geométrica dos Códigos Propelineares e a Não Existência de Códigos Propelineares m-ários, $m \geq 3$

Martinho da Costa Araujo, Reginaldo Palazzo Jr., Marcelo Muniz Silva Alves, e Sueli I. R. Costa

Abstract— **O objetivo deste trabalho é apresentar códigos propelineares binários invariantes por translação como sendo subgrupos do produto direto de $\mathbb{Z}_2^{k_1}$ por $\mathbb{Z}_4^{k_2}$ e por $\mathbb{Q}_8$, denotado por $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times \mathbb{Q}_8$. Devido a essa caracterização dos códigos propelineares binários invariantes por translação, mostramos que os mesmos pertencem à classe dos códigos G-lineares binários. Mostramos também, que não existem códigos propelineares m-ários invariantes por translação sobre o anel dos inteiros módulo m, $m \geq 3$.**

I. Introdução

Em [1], Rifà, Bassart e Pujol introduziram o conceito de códigos propelineares binários. Posteriormente em [2], apresentaram uma subclasse desses códigos, qual seja a dos códigos propelineares binários invariantes por translação. Esses códigos podem ser descritos algebricamente como subgrupos do produto semidireto de $\mathbb{Z}_2^n$ por $\mathbf{S_n}$, o qual denotaremos por $\mathbb{Z}_2^n \rtimes \mathbf{S_n}$, onde $\mathbf{S_n}$ simboliza o grupo simétrico de grau n. Sob o ponto de vista geométrico, podemos pensar nesses códigos como subgrupos do grupo de simetrias de $\mathbb{Z}_2^n$, denotado por $\Gamma(\mathbb{Z}_2^n)$.

Neste trabalho, apresentaremos uma classificação dos códigos propelineares binários invariantes por translação como sendo códigos G-lineares [4], ou seja, códigos obtidos de uma ação *fortemente transitiva* de um subgrupo de $\Gamma(\mathbb{Z}_2^n)$ sobre $\mathbb{Z}_2^n$, equivalentemente, códigos geometricamente uniformes [6]. Mostraremos também que não existem códigos propelineares invariantes por translação sobre $\mathbb{Z}_m$ para $m \geq 3$, ou seja, não existem subgrupos de $\mathbb{Z}_m^n \rtimes \mathbf{S_n}$, $m \geq 3$ e $n \geq 2$ inteiros cuja ação sobre $\mathbb{Z}_m^n$ seja preservada pela distância de Hamming, d_H.

II. Preliminares

Nesta seção apresentaremos algumas definições e resultados básicos das estruturas matemáticas que iremos utilizar ao longo deste trabalho.

Consideremos o espaço de Hamming $(\mathbb{Z}_m^n, d_H)$. Uma *isometria* em $\mathbb{Z}_m^n$ é uma função $\phi : \mathbb{Z}_m^n \longrightarrow \mathbb{Z}_m^n$ que preserva a distância de Hamming, ou seja, $d_H(\phi(x), \phi(y)) = d_H(x, y)$ para todo $x, y \in \mathbb{Z}_m^n$. Uma isometria que deixa um subconjunto X de $\mathbb{Z}_m^n$ invariante é chamada de uma simetria de X. O conjunto das isometrias de X, indicado por $\Gamma(X)$, é um subgrupo do grupo das permutações de X, denotado por $\mathbf{S_X}$, com a operação de composição de funções.

Um grupo G *atua* sobre um conjunto não vazio X, se existir um homomorfismo $\sigma : G \longrightarrow \mathbf{S_X}$. Dado $x_0 \in X$, o subconjunto de X

$$Orb_G(x_0) = \{gx_0 \mid g \in G\},$$

é chamado de *órbita* de x_0 sob a ação de G. Quando $Orb_G(x_0) = X$, dizemos que a ação de G sobre X é *transitiva*, ou que G atua transitivamente sobre X. Se além disso, para todo $a, b \in X$ existir um único $g \in G$ tal que $g(a) = b$, dizemos que a ação de G sobre X é *fortemente transitiva*.

Seja G um grupo que atua sobre um conjunto não vazio X e $x \in X$. O subgrupo

$$Stab_G(x) = \{g \in G \mid g(x) = x\},$$

é chamado *estabilizador* de $x \in X$.

III. Códigos Propelineares e G-lineares

A seguir, apresentaremos algumas definições e propriedades dos códigos propelineares e G-lineares

Definição 1: Seja $(\mathbb{Z}_2^n, d_H)$ o espaço de Hamming n-dimensional e $\mathbf{S_n}$ o grupo simétrico de grau n. Diremos que um subconjunto $C \subseteq \mathbb{Z}_2^n$, com $\mathbf{0} \in C$ é um **código propelinear** de comprimento n, se existir uma função $\pi : C \to \mathbf{S_n}$, definida por $\pi(v) = \pi_v$, tal que seu grafo $\Omega(\pi) = \{(v, \pi_v)\ ; \text{para todo } v \in C\}$ seja um subgrupo de $\mathbb{Z}_2^n \rtimes \mathbf{S_n}$.

Definição 2: [4] Seja G um grupo, d_G uma métrica sobre G e C um código binário de comprimento n em $(\mathbb{Z}_2^n, d_H)$. Diremos que C é G-linear, se a menos de uma permutação de coordenadas $C = \phi(\hat{C})$ para algum subgrupo $\hat{C}$ de G e $\phi : G^n \to \mathbb{Z}_2^{kn}$, para $k \geq 2$, é uma isometria.

Desta forma, observamos que quando um código C é propelinear, então temos uma identificação natural de C com o subgrupo $(\Omega(\pi), *)$ de $\mathbb{Z}_2^n \rtimes \mathbf{S_n}$. Esta identificação produz uma ação fortemente transitiva de $(\Omega(\pi), *)$ sobre C, definida pela função $f : (\Omega(\pi), *) \times C \to C$, tal que

$$f((v, \pi_v), x) = (v, \pi_v) * x = v + \pi_v(x) = v * x,$$

para todo $(v, \pi_v) \in (\Omega(\pi), *)$ e $x \in C$.

O autor está no Departamento de Matemática, Universidade Federal do Mato Grosso, Rondonópolis, Brasil. e-mail: martinho@dt.fee.unicamp.br.

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

O autor está no programa de doutorado IMECC-UNICAMP, e-mail: msilva@ime.unicamp.br.

A autora está no Departamento de Matemática, IMECC-UNICAMP. e-mail: sueli@ime.unicamp.br.

Portanto, para todo $x \in C$ temos que $Orb_{\Omega(\pi)}(x) = C$. Quando um código C é G-linear segue por definição, que o alfabeto $\mathbb{Z}_2^k$ está efetivamente casado ao grupo G [5], ou seja, G é isomorfo a um subgrupo do grupo de simetrias $\Gamma(\mathbb{Z}_2^n)$ de $\mathbb{Z}_2^n$, cuja ação sobre $\mathbb{Z}_2^k$ é fortemente transitiva.

Exemplo 3: Considere $\pi : \mathbb{Z}_2^n \to \mathbf{S_n}$, tal que $(\Omega(\pi), *)$ seja um subgrupo de $\mathbb{Z}_2^n \rtimes \mathbf{S_n}$, isto é, um código propelinear dado por:

1. Para $n = 2$

v	00	11	01	10
π_v	id	id	(12)	(12)

Note que $(\Omega(\pi), *)$ é um subgrupo de $\mathbb{Z}_2^2 \rtimes \mathbf{S_2} \cong \mathbb{D}_4$, onde $\mathbb{D}_n$ denota o grupo diedral com $2n$ elementos, gerado por $(v, \pi_v) = ((01), (12))$, ou seja, $(\Omega(\pi), *) = \langle 01, (12)\rangle \cong \mathbb{Z}_4$. Como a ação de $\mathbb{Z}_4$ sobre $\mathbb{Z}_2^2$ é fortemente transitiva, obtemos os códigos $\mathbb{Z}_4$-lineares [3].

2. Para $n = 3$

v	000	011	100	111	001	010	101	110
π_v	id	id	id	id	(23)	(23)	(23)	(23)

Observe que o subgrupo $(\Omega(\pi), *) = \langle (100, id),\ (110,\ (23))\rangle$, é isomorfo ao produto direto $\mathbb{Z}_2 \times \mathbb{Z}_4$. Além disso, a ação de $(\Omega(\pi), *)$ sobre $\mathbb{Z}_2^3$ é fortemente transitiva. Portanto, este código propelinear é também um código $\mathbb{Z}_2 \times \mathbb{Z}_4$-linear.

3. Para $n = 3$

v	000	011	101	110	001	010	100	111
π_v	id	id	id	id	(23)	(23)	(23)	(23)

Note que $(\Omega(\pi), *) = \langle (110, id),\ (100, (23))\rangle \cong \mathbb{D}_4$. Este código propelinear é também um código $\mathbb{D}_4$-linear.

Definição 4: Seja C um código propelinear binário. Dizemos que C é um código propelinear invariante por translação se a ação $(\Omega(\pi), *)$ sobre $\mathbb{Z}_2^n$ é preservada pela distância de Hamming.

Em outras palavras, um código propelinear binário C é invariante por translação quando $d_H(u, v) = d_H(u * x, v * x)$, para todo $u, v \in C$ e todo $x \in \mathbb{Z}_2^n$, [2].

Lema 5: [2] Um código propelinear binário C é invariante por translação se, e somente se, $w_H(v) = d_H(x, v * x)$, para todo $v \in C$ e todo $x \in \mathbb{Z}_2^n$.

Proposição 6: Se C é um código propelinear binário invariante por translação, então o estabilizador de C é $Stab_C(x) = \{0, id\}$.

Demonstração: Pela identificação natural de C com $(\Omega(\pi), *)$ temos que

$$Stab_{\Omega(\pi)}(x) = \{(v, \pi_v) \in (\Omega(\pi), *) : (v, \pi_v)(x) = v * x = x\}$$

Como C é invariante por translação, então

$$v * x = x \Rightarrow 0 = d_H(x, v * x) = w_H(v)$$

$$\Rightarrow v = 0, \forall x \in \mathbb{Z}_2^n, \text{ ou seja, } (v, \pi_v) = (0, id).$$

■

Corolário 7: [2] Se C é um código propelinear binário invariante por translação, então $|C| = 2^k$, para $k \leq n$.

Teorema 8: Seja C um código propelinear binário invariante por translação de comprimento n, com cardinalidade $|C| = 2^n$, para $n \geq 2$, então C é um código G-linear.

Demonstração: Como C é propelinear binário invariante por translação, implica que podemos identificar C com um subgrupo $G = (\Omega(\pi), *)$ de $\mathbb{Z}_2^n \rtimes \mathbf{S_n}$, portanto temos uma ação fortemente transitiva de G sobre C. Pela Proposição 6 e

$$|G| = |Stab_G(x)|\ [G : Stab_G(x)],$$

temos que

$$|G| = |Stab_G(x)|\ |Orb_G(x)| = |Orb_G(x)|, \forall x \in \mathbb{Z}_2^n.$$

Com isso, podemos afirmar que $|G| = |C| = 2^n$. Portanto, C é um código G-linear. ■

Exemplo 9: Considere $\pi : \mathbb{Z}_2^n \to \mathbf{S_n}$, tal que $(\Omega(\pi), *)$ seja um subgrupo de $\mathbb{Z}_2^n \rtimes \mathbf{S_n}$, isto é, um código propelinear dado por

1. Para $n = 5$

v	00000	00001	00010	00011	00100	00101
π_v	id	id	id	id	id	id
v					00110	00111
π_v					id	id
v	11000	11001	11010	11011	11100	11101
π_v	id	id	id	id	id	id
v					11110	11111
π_v					id	id
v	01000	01001	01010	01011	01100	01101
π_v	(12)	(12)	(12)	(12)	(12)	(12)
v					01110	01111
π_v					(12)	(12)
v	10000	10001	10010	10011	10100	10101
π_v	(12)	(12)	(12)	(12)	(12)	(12)
v					10110	10111
π_v					(12)	(12)

Note que este código propelinear binário é invariante por translação, onde $(\Omega(\pi), *) \cong \mathbb{Z}_2^3 \times \mathbb{Z}_4$, portanto, $\mathbb{Z}_2^3 \times \mathbb{Z}_4$-linear.

IV. Códigos Propelineares m-ários

Consideremos o espaço de Hamming $(\mathbb{Z}_m^n,\ d_H)$ e $\mathbf{S_n}$. Sabemos que $(\mathbb{Z}_m^n, \oplus, \otimes)$, onde $\oplus$, $\otimes$ é a soma e o produto módulo m, é um $\mathbb{Z}_m$-módulo livre. Além disso, também podemos considerar o produto semidireto do $\mathbb{Z}_m$-módulo livre $\mathbb{Z}_m^n$ por $\mathbf{S_n}$, denotado por $\mathbb{Z}_m^n \rtimes \mathbf{S_n}$. Com isso, podemos investigar os subgrupos desse produto semidireto. Mais precisamente, os códigos propelineares m-ários para $m \geq 3$.

Como o produto semidireto é definido pela ação de um grupo sobre um conjunto, as vezes é possível induzir nesse conjunto propriedades algébricas provenientes do grupo e relacioná-las com a métrica, com isso tornando essse conjunto um espaço métrico. O que desejamos, é que esta

métrica seja invariante sob esta ação. Dentro desse contexto, mostraremos que não é possível obter códigos propelineares m-ários invariantes por translação para $m \geq 3$.

Definição 10: Seja $(\mathbb{Z}_m^n,\ d_H)$ o espaço de Hamming n-dimensional e $\mathbf{S_n}$ o grupo simétrico de grau n. Diremos que um subconjunto $C \subseteq \mathbb{Z}_m^n$, com $\mathbf{0} \in C$ é um **código propelinear m-ário** de comprimento n, se existir uma função $\pi : C \to \mathbf{S_n}$, definida por $\pi(v) = \pi_v$, tal que seu grafo $\Omega(\pi) = \{(v, \pi_v)\ ;\text{para todo } v \in C\}$ seja um subgrupo de $\mathbb{Z}_m^n \rtimes \mathbf{S_n}$.

Dessa definição, segue que o código propelinear m-ário $C \subseteq \mathbb{Z}_m^n$ é identificado com o subgrupo $(\Omega(\pi), \star)$ de $(\mathbb{Z}_m^n \rtimes \mathbf{S_n}, \star)$, de modo que $u \star v = u \oplus \pi_u(v)$, $\forall u, v \in C$. Por isso, nos referimos a C e $\Omega(\pi)$, indistintamente.

Definição 11: Seja C um código propelinear m-ário. Diremos que C é um código **propelinear invariante por translação,** se para todo $u, v \in C$ e $x \in \mathbb{Z}_m^n$ temos que

$$d_H(u, v) = d_H(u \star x, v \star x).$$

Proposição 12: Seja C um código propelinear m-ário. Diremos que C é invariante por translação se, e somente se,

$$wt_H(v) = d_H(x, v \star x)\ , \forall x \in \mathbb{Z}_m^n \text{ e } \forall v \in C.$$

Demonstração: Por conveniência, denotamos o elemento inverso de $v \in C$ por $s = v^{-1}$. Suponha que C seja um código propelinear m-ário invariante por translação, então $wt_H(v) = d_H(\mathbf{0}, v) = d_H(\mathbf{0} \star x, v \star x) = d_H(x, v \star x)$, para todo $x \in \mathbb{Z}_2^n$. Reciprocamente, para quaisquer $u, v \in C$ temos que

$$\begin{aligned}
d_H(u,v) &= d_H(w \star u, w \star v), \forall w \in C;\\
d_H(u,v) &= d_H\left(u^{-1} \star u, u^{-1} \star v\right) = d_H\left(\mathbf{0}, u^{-1} \star v\right)\\
d_H(u,v) &= wt_H\left(u^{-1} \star v\right)\\
d_H(u,v) &= d_H\left(x, \left(u^{-1} \star v\right) \star x\right), \forall x \in \mathbb{Z}_2^n\\
d_H(u,v) &= d_H\left(x, u^{-1} \star (v \star x)\right)\\
d_H(u,v) &= d_H\left(u \star x, u \star u^{-1} \star (v \star x)\right);\\
d_H(u,v) &= d_H(u \star x, v \star x).
\end{aligned}$$

■

Consideremos o espaço de Hamming $(\mathbb{Z}_m^n, d_H)$ e $C \subset \mathbb{Z}_m^n$ um código sobre $\mathbb{Z}_m^n$. Dado $\mathbf{v} = (\lambda_1, \lambda_2, \ldots, \lambda_n) \in C$ podemos escrever

$$\mathbf{v} = (\lambda_1, \lambda_2, \ldots, \lambda_n) = \sum_{i=1}^{n} \lambda_i \mathbf{e}_i \in \mathbb{Z}_m^n$$

onde $\mathcal{B} = \{\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}\}$ é a **base canônica** do $\mathbb{Z}_m$-módulo livre $\mathbb{Z}_m^n$. Definimos o **suporte** de $\mathbf{v} = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ como sendo

$$Supp(\mathbf{v}) = \{i : 1 \leq i \leq n\,, \lambda_i \neq 0\}.$$

Nesse caso, $wt_H(\mathbf{v}) = |Supp(\mathbf{v})|$.

Lema 13: Seja C um código propelinear invariante por translação. Se $\mathbf{v} \in C$ e $\pi_{\mathbf{v}} \neq id$, então $\pi_{\mathbf{v}}(\mathbf{v}) \neq \mathbf{v}$.

Demonstração: Suponha que $\pi_{\mathbf{v}}(\mathbf{v}) = \mathbf{v}$, isto implica que existem vetores coordenados $\mathbf{e_i} \neq \mathbf{e_j}$ tal que $\pi_{\mathbf{v}}(\mathbf{e_i}) \neq \mathbf{e_j}$, ou seja, $i, j \notin Supp(\mathbf{v})$. Logo,

$$\begin{aligned}
wt_H(\mathbf{v}) &= d_H(\mathbf{e_i}, \mathbf{v} \star \mathbf{e_i})\\
&= d_H(\mathbf{e_i}, \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{e_i}))\\
&= wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{e_i}) - \mathbf{e_i})\\
&= wt_H(\mathbf{v} \oplus \mathbf{e_j} \oplus \mathbf{e_i})\\
&= wt_H(\mathbf{v}) + 2,
\end{aligned}$$

o que contradiz o fato de C ser invariante por translação. ■

Lema 14: [2] Seja C um código propelinear invariante por translação. Se $\mathbf{v} \in C$, então $\pi_{\mathbf{v}} = id$ ou $\pi_{\mathbf{v}}(\mathbf{v}) \neq \mathbf{v}$. Quando $\pi_{\mathbf{v}}(\mathbf{v}) \neq \mathbf{v}$, para cada $i, j \in I_n = \{1, 2, \ldots, n\}$ tal que $\pi_{\mathbf{v}}(\mathbf{e_i}) = \mathbf{e_j} \neq \mathbf{e_i}$ temos:

$$i \in Supp(\mathbf{v}) \text{ se, e somente se, } j \notin Supp(\mathbf{v}).$$

Demonstração: Como C é invariante por translação temos que

$$wt_H(\mathbf{v}) = d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x})\ , \forall \mathbf{v} \in C, \mathbf{x} \in \mathbb{Z}_2^n.$$

Suponha que $\pi_{\mathbf{v}} \neq id$, então existem vetores coordenados $\mathbf{e_i} \neq \mathbf{e_j}$ tais que

$$\begin{aligned}
wt_H(\mathbf{v}) &= d_H(\mathbf{e_i}, \mathbf{v} \star \mathbf{e_i}) \qquad (1)\\
&= wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{e_i}) \oplus \mathbf{e_i})\\
&= wt_H(\mathbf{v} \oplus \mathbf{e_j} \oplus \mathbf{e_i}).
\end{aligned}$$

Se $i \in Supp(\mathbf{v})$, então $\lambda_i = 1$, isto é, $\lambda_i \oplus 1 = 0$. Por 1, temos que $\lambda_i \oplus \lambda_j = 1$, ou seja, $\lambda_j = 0$, logo $j \notin Supp(\mathbf{v})$. A recíproca basta trocar $\mathbf{e_i}$ por $\mathbf{e_j}$. ■

Teorema 15: Sejam m, n inteiros positivos maiores que 1. Não existem códigos propelineares m-ários invariantes por translação para $m > 2$, exceto para $C \subset \mathbb{Z}_m^n$ linear e tal que $\pi_v = id$ para todo $v \in C$.

Demonstração: Se $C \subset \mathbb{Z}_m^n$ é linear e tal que $\pi_{\mathbf{v}} = id$ para todo $\mathbf{v} \in C$, então C é trivialmente invariante por translação. Agora, basta mostrar que existe $\mathbf{x} \in \mathbb{Z}_m^n$ tal que

$$wt_H(\mathbf{v}) \neq d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x}) = wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x}) - \mathbf{x})$$

para algum $\mathbf{v} \in C$. Considermos os seguintes casos:
1. Pelos Lemas 13 e 14, segue que para $\pi_{\mathbf{v}} \neq id$ temos $\pi_{\mathbf{v}}(\mathbf{v}) \neq \mathbf{v}$ e que existe um vetor de peso 1, digamos $\mathbf{e_i}$ tal que $\pi_{\mathbf{v}}(\mathbf{e_i}) = \mathbf{e_j} \neq \mathbf{e_i}$, ou seja, $i \in Supp(\mathbf{v})$ e $j \notin Supp(\mathbf{v})$. Portanto, $wt_H(\mathbf{v}) = d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x}) = wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x}) - \mathbf{x}) \leq wt_H(\mathbf{v}) + 2$.
2. Para $m \geq 3$, basta considerar $\pi_{\mathbf{v}}(\mathbf{v}) \neq \mathbf{v}$, pelo item 1, temos que

$$i \in Supp(\mathbf{v}) \text{ e } j \notin Supp(\mathbf{v}).$$

Escolhendo $\mathbf{x} = \lambda \mathbf{e_i}$ com $\lambda \neq 0$ e $\lambda \neq \lambda_i$, temos que

$$\begin{aligned}
wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x}) - \mathbf{x}) &= wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\lambda \mathbf{e_i}) - \lambda \mathbf{e_i})\\
&= wt_H(\mathbf{a}),
\end{aligned}$$

onde $\mathbf{a} = \lambda_\mathbf{1}, \lambda_\mathbf{2}, \ldots, \lambda_\mathbf{i} - \lambda, \ldots, \lambda + \lambda_\mathbf{j}, \ldots, \lambda_\mathbf{n}$.
Pela nossa escolha, $0 \neq \lambda_i \oplus (-\lambda) \in Supp(\mathbf{v})$ e apesar de $\lambda_j = 0$, pois $j \notin Supp(\mathbf{v})$ temos $0 \neq \lambda \oplus \lambda_j \notin Supp(\mathbf{v})$. Portanto,

$$wt_H(\mathbf{v} \oplus \pi_\mathbf{v}(\mathbf{x}) - \mathbf{x}) = wt_H(\mathbf{v}) + \mathbf{1},$$

o que contradiz o fato de C ser invariante por translação. ■

V. Conclusões

Neste trabalho apresentamos os códigos propelineares como subgrupos do produto semidireto de $\mathbb{Z}_m^n$ por $\mathbf{S_n}$. Classificamos alguns códigos propelineares invariantes por translação, sob o ponto de vista geométrico, como códigos G-lineares. Mostramos, que não existem códigos propelineares m-ários invariantes por translação, para $m \geq 3$, ou seja, não existem subgrupos do produto semidireto $\mathbb{Z}_m^n \rtimes \mathbf{S_n}$ cuja ação sobre $\mathbb{Z}_m^n$ preserva a distância de Hamming. Gostaríamos de mencionar que as tabelas dos exemplos apresentados foram obtidas com a ajuda do pacote computacional GAP, [7].

VI. Agradecimentos

Os autores gostariam de agradecer aos Profs. Drs. Jorge Pedraza Arpasi e João Roberto Gerônimo pelas discussões técnicas ao longo deste trabalho.

References

[1] J.Rifá, J.M.Bassart e J.Pujol, "On completely regular propelinear codes" , *In Proc.6th International Conference, AAECC-6, No. 357 in LNCS, Lectures Notes in Computer Science*, pp.341-355, Springer-Verlag, 1989.

[2] J.Rifá, and J.Pujol, "Translation-inavariant propelinear codes," *IEEE Trans. Inform. Theory*, vol.IT-43, pp. 590-598, March 1997.

[3] A.R.Hammons, Jr., A.R.Calderbanck, P.V.Kumar, N.J.A.Sloane, and P.Solé, "The $\mathbb{Z}_4$-lineridade of Kerdock, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol.IT-40, pp.301-309, March 1994.

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

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

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

[7] A.Niemeyer, M. Schöenert, et al..., " GAP- Groups, Algorithms and Programming ", Version 3, April 1997.