Linearidade de Códigos Quaternários

Thael Ferreira Zaruz
Universidade Federal de Uberlândia
thaelzaruz@gmail.com

Alonso Sepúlveda Castellanos
Universidade Federal de Uberlândia
alonso.castellanos@ufu.br

RESUMO

Neste trabalho, introduzimos algebricamente os códigos quaternários como códigos corretores de erros sobre $\mathbb{Z}_4$, o anel dos inteiros módulo 4. Descrevemos especificamente todos os códigos lineares quaternários de $\mathbb{Z}_4^n$, para $n = 1$ e $n = 2$. Usando o conceito definido de produto interno, definimos a noção de códigos ortogonais, o que nos leva aos códigos duais, auto-ortogonais e autoduais. Também mostramos a forma da matriz geradora de qualquer código linear quaternário de comprimento n e de seu dual. Em seguida, falamos da aplicação de Gray, suas propriedades e das imagens binárias de códigos quaternários. Respondemos também as perguntas: Quando um código binário é linear quaternário? E quando a imagem binária de um código linear quaternário é linear?

ABSTRACT

In this paper, we introduce algebraically the quaternary codes as error correcting codes over $\mathbb{Z}_4$, the ring of integers $\mod 4$. We specifically describe all the quaternary linear codes of $\mathbb{Z}_4^n$ for $n = 1$ and $n = 2$. Using the defined concept of inner product, we define the orthogonal codes, what bring us to dual codes, self-orthogonal codes and self-dual code. We also show the generator matrix form of any quaternary linear codes of length n and its dual-code. After that, we talk about the Gray map, its properties and the binary images of quaternary codes. We also answered the questions: When a binary code is quaternary linear? And when the binary image of a quaternary linear code is linear?

Palavras-chave: Códigos quaternários, linearidade, aplicação de Gray.

1 Introdução

O objetivo da teoria de códigos corretores de erros é criar formas para a detecção e correção de erros que possam ocorrer na transmissão de informação. Um exemplo do uso dessa teoria é a adição de redundâncias no envio de dados ou a repetição desse envio. Resultados de estudos nessa área são utilizados na gravação de DVD's, na criptografia de dados, no envio de informações de naves espaciais para as estações na Terra, entre outros.

Um código corretor de erros é um conjunto de n-uplas, chamadas palavras em um alfabeto finito. Os códigos mais utilizados são os binários, ou seja, sobre o anel dos inteiros módulo 2 e especialmente os deste tipo que são lineares.

Nos últimos anos, códigos quaternários têm atraído bastante atenção por poderem ser representados como a imagem binária de códigos não lineares, sendo que estes contêm

mais palavras que qualquer um que seja linear, como exposto em [1]. Essa representação é feita usando a aplicação de Gray, conforme [2].

2 CÓDIGOS QUATERNÁRIOS

Seja $\mathbb{Z}_4$ o anel dos inteiros módulo 4, n um inteiro positivo e $\mathbb{Z}_4^n$ o conjunto das n-uplas sobre $\mathbb{Z}_4$, isto é:

$$\mathbb{Z}_4^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{Z}_4 \quad \text{para} \quad i = 1, \ldots, n\}.$$

Qualquer conjunto não vazio $\mathcal{C}$ de $\mathbb{Z}_4^n$ é chamado de **código quaternário** ou um código sobre $\mathbb{Z}_4$, e n é o comprimento do código. As n-uplas em $\mathcal{C}$ são chamadas de **palavras** do código $\mathcal{C}$.

Sejam $\mathcal{C}$ e $\mathcal{C}'$ códigos quaternários de comprimento n. Se $\mathcal{C}' \subseteq \mathcal{C}$, $\mathcal{C}'$ é chamado de subcódigo de $\mathcal{C}$. Para todo $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_n) \in \mathbb{Z}_4^n$ definimos a soma por:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

Com a soma definida acima, temos que $\mathbb{Z}_4^n$ é um grupo abeliano de ordem 4^n. Todo subgrupo de $\mathbb{Z}_4^n$ será chamado de **código linear quaternário** ou código $\mathbb{Z}_4$ linear. Para todo $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n) \in \mathbb{Z}_4^n$ definimos o produto interno de x e y por:

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n.$$

Se $x \cdot y = 0$ dizemos que x e y são ortogonais.

Seja $\mathcal{C}$ um código linear quaternário de comprimento n. Definimos o conjunto:

$$\mathcal{C}^{\perp} = \{x \in \mathbb{Z}_4^n : x \cdot y = 0 \text{ para todo } y \in \mathcal{C}\}.$$

Vejamos que $\mathcal{C}^{\perp}$ é um subgrupo de $\mathbb{Z}_4^n$. É claro que $0 = (0, \ldots, 0) \in \mathbb{Z}_4^n$ também pertence a $\mathcal{C}^{\perp}$, e além disso, dados $x, x' \in \mathcal{C}^{\perp}$ com $x = (x_1, \ldots, x_n)$ e $x' = (x'_1, \ldots, x'_n)$ temos que para $y = (y_1, \ldots, y_n) \in \mathcal{C}$, satisfaz que

$$\begin{aligned}
(x - x') \cdot y &= (x_1 - x'_1, \ldots, x_n - x'_n) \cdot (y_1, \ldots, y_n) \\
&= (x_1 - x'_1) \cdot y_1 + \cdots + (x_n - x'_n) \cdot y_n \\
&= x_1 y_1 - x'_1 y_1 + \cdots + x_n y_n - x'_n y_n \\
&= 0.
\end{aligned}$$

Logo $x - x' \in \mathcal{C}^{\perp}$. Assim, $\mathcal{C}^{\perp}$ também é um código linear quaternário, chamado de **código dual** de $\mathcal{C}$. Se o código $\mathcal{C}$ satisfaz que $\mathcal{C} \subset \mathcal{C}^{\perp}$, $\mathcal{C}$ é chamado de **código auto-ortogonal**. Se $\mathcal{C} = \mathcal{C}'$, o código $\mathcal{C}$ é chamado de **código autodual**.

Dizemos que dois códigos quaternários $\mathcal{C}_1$ e $\mathcal{C}_2$ ambos de comprimento n são **equivalentes** se um deles pode ser obtido a partir do outro permutando suas coordenadas e (se necessário) mudando seus sinais. Códigos quaternários que diferem apenas pela permutação de coordenadas são chamados de equivalentes por permutação. O grupo de **automorfismos**, denotado por $Aut(\mathcal{C})$, de um código quaternário $\mathcal{C}$, é o grupo gerado por todas as permutações e mudanças de sinais das coordenadas que preservam o conjunto de palavras do código $\mathcal{C}$. Por exemplo, tomando o código linear quaternário de comprimento 3, $\mathcal{H}_1 = \langle(1,\ 3,\ 3)\rangle \subseteq \mathbb{Z}_4^3$, dado por $\mathcal{H}_1 = \Big\{(0,\ 0,\ 0),\ (1,\ 3,\ 3),\ (2,\ 2,\ 2),\ (3,\ 1,\ 1)\Big\}$. Vemos que se mudarmos de sinal o gerador $(1,\ 3,\ 3)$ obtemos o código $\mathcal{H}_2 = \langle(-1\ , -3\ , -3)\rangle = \langle(3,\ 1,\ 1)\rangle = \mathcal{H}_1$. Logo, a mudança de sinal em todas as coordenadas do gerador de $\mathcal{H}_1$ é um automorfismo de $\mathcal{H}_1$. Outro automorfismo de $\mathcal{H}_1$ seria uma permutação que troca a segunda e a terceira coordenada. Agora, trocando as 2 primeiras coordenadas do gerador de $\mathcal{H}_1$, obtemos o código $\mathcal{H}_3 = \langle(3,\ 1,\ 3)\rangle = \Big\{(0,\ 0,\ 0),\ (3,\ 1,\ 3),\ (2,\ 2,\ 2),\ (1,\ 3,\ 1)\Big\}$. Como $\mathcal{H}_3 \neq \mathcal{H}_1$ essa permutação não pertence a $Aut(H_1)$, porém $\mathcal{H}_1$ e $\mathcal{H}_3$ são códigos equivalentes.

Pelo Teorema Fundamental dos grupos abelianos finitos (ver [3, Teorema 2.10.3]), sabemos que um grupo aditivo abeliano de ordem p^m, com p primo e $m > 0$, pode ser escrito unicamente como a soma direta de m_1 subgrupos cíclicos de ordem $p^{e_1}, \ldots,\ m_r$ subgrupos cíclicos de ordem p^{e_r} onde $m_1, e_1, \ldots, m_r, e_r$ são inteiros positivos tais que $e_1 > \cdots > e_r$. Então, dizemos que o grupo é do tipo $(p^{e_1})^{m_1} \ldots (p^{e_r})^{m_r}$. Sabemos que $m = m_1e_1 + \cdots + m_re_r$ também que um grupo abeliano formado pelo elemento identidade sozinho é do tipo p^0.

Por exemplo, o grupo aditivo $\mathbb{Z}_4^n$ é do tipo $(2^2)^n$, pois ele é a soma direta de n subgrupos cíclicos de ordem 2^2. De fato, podemos escrever $\mathbb{Z}_4^n$ como soma direta da seguinte forma:

$$\mathbb{Z}_4^n = \bigoplus_{\mathrm{i}=1}^{n} \left\{ \left(0, \ldots, 0, \underset{i}{x}, 0, \ldots, 0\right) : x \in \mathbb{Z}_4 \right\},$$

onde cada subconjunto da forma $\{(0, \ldots, 0, x, 0, \ldots, 0) : x \in \mathbb{Z}_4\}$ é um subgrupo cíclico de ordem 2^2.

Um código linear quaternário é um subgrupo de algum $\mathbb{Z}_4^n$, sendo n o comprimento do código e sua ordem será uma potência de 2. Assim podemos dizer qual é o tipo de um código linear quaternário. Claramente códigos quaternários lineares equivalentes tem o mesmo tipo. Então os possíveis tipos para um código linear quaternário são da forma $(2^2)^m$, $(2^2)^{m_1} \cdot 2^{m_2}$, 2^m ou 2^0. A seguir, falaremos do tipo $(2^2)^m$ como 4^m e do tipo $(2^2)^{m_1} \cdot 2^{m_2}$ como $4^{m_1}2^{m_2}$.

Para $n = 1$, temos que $\mathbb{Z}_4^1$ tem apenas três subgrupos, que são dos tipos 4^1, 2^1 ou 4^0 respectivamente. Assim existem três códigos lineares quaternários de comprimento 1, e eles são $\{0, 1, 2, 3\}$, $\{0, 2\}$ e $\{0\}$.

Para $n = 2$, temos que os subgrupos de $\mathbb{Z}_4^2$ são do tipo $4^2, 4^12^1, 2^2, 4^1, 2^1$, ou 2^0.

Existe apenas um código linear quaternário de comprimento 2 e tipo 4^2, que é $\mathbb{Z}_4^2$. Ele é gerado pelas linhas da matriz 2×2 sobre $\mathbb{Z}_4$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Essa matriz é chamada de matriz geradora do código $\mathbb{Z}_4^2$. As palavras do código geradas por essa matriz são $\Big\{(0,\ 0),\ (0,\ 1),\ (0,\ 2),\ (0,\ 3),\ (1,\ 0),\ (1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (2,\ 0),\ (2,\ 1),\ (2,\ 2),\ (2,\ 3),\ (3,\ 0),\ (3,\ 1),\ (3,\ 2), (3,\ 3)\Big\}$. Existem 4 subgrupos de $\mathbb{Z}_4^2$ que são do tipo 4^12^1. Cada um deles é gerado pelas linhas de uma das matrizes 2×2 abaixo:

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}.$$

Claramente $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ e $\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$, geram o mesmo subgrupo, então a segunda matriz não é listada. Os códigos lineares quaternários gerados pela primeira e segunda matriz são equivalentes por permutação. Da mesma forma, os gerados pela terceira e quarta matrizes também são. Portanto, existem apenas dois códigos lineares quaternários não equivalentes de comprimento 2 e do tipo 4^12^1.

Existe apenas um código quaternário linear de comprimento 2 e do tipo 2^1. Sua matriz geradora é da forma

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Esse é um código autodual. De fato as palavras geradas por essa matriz são

$$\Big\{(2\ 0),\ (2\ 2),\ (0\ 2), (0\ 0)\Big\}.$$

O produto interno entre duas dessas palavras e entre elas mesmas é igual a 0, portanto, o código é igual ao seu dual.

Códigos lineares quaternários de comprimento 2 e do tipo 4^1 são gerados por qualquer uma das matrizes 1×2 abaixo:

$$(1\ 0),\ (0\ 1),\ (1\ 1),\ (1\ 2),\ (2\ 1),\ (1\ 3),\ (3\ 1).$$

Podemos ver que as duas primeiras matrizes geram códigos equivalentes por permutação, como a quarta e a quinta matrizes e a sexta e a sétima. Além disso, os gerados pela terceira e sexta matrizes são equivalentes, já que se trocarmos o sinal de um dos elementos da matriz chegamos na outra matriz. Portanto, existem 3 códigos quaternários lineares que não são equivalentes de comprimento 2 e tipo 4^1.

Os códigos de comprimento 2 tipo 2^1 são gerados por qualquer uma das seguintes matrizes 1×2:

$$(2\ 0),\ (0\ 2),\ (2\ 2).$$

Claramente a primeira e a segunda matriz geram códigos equivalentes. Portanto, existem dois códigos lineares quaternários de comprimento 2 e tipo 2^1. Ambos são auto-ortogonais.

Finalmente, existe apenas um código linear quaternário de comprimento 2 e tipo 2^0 que é $\{(0\ 0)\}$.

Portanto, juntando todos os tipos existem $1 + 2 + 1 + 3 + 2 + 1 = 10$ códigos lineares quaternários de comprimento 2 que não são equivalentes.

3 MATRIZES GERADORAS

Nesta seção vamos assumir que os elementos 0 e 1 de $\mathbb{Z}_2$ também são considerados respectivamente os elementos 0 e 1 de $\mathbb{Z}_4$. Uma palavra $x = (x_1, \ldots, x_n) \in \mathbb{Z}_2^n$ também é considerada uma palavra $x = (x_1, \ldots, x_n) \in \mathbb{Z}_4^n$, da mesma forma que uma matriz sobre $\mathbb{Z}_2$, também é considerada uma matriz sobre $\mathbb{Z}_4$. Assim, se M é uma matriz sobre $\mathbb{Z}_2$ então M e $2M$ podem ser consideradas matrizes sobre $\mathbb{Z}_4$ bem definidas, onde as entradas de M serão 0 e 1 e as entradas de $2M$ serão 0 e 2.

Seja $\mathcal{C}$ um código linear sobre $\mathbb{Z}_4$ de comprimento n. Uma matriz G de ordem $k \times n$ sobre $\mathbb{Z}_4$ é chamada de *matriz geradora* de $\mathcal{C}$ se as linhas de G geram $\mathcal{C}$ e nenhum subconjunto das linhas de G geram $\mathcal{C}$.

Proposição 3.1: *Qualquer código linear $\mathcal{C}$ sobre $\mathbb{Z}_4$ contendo alguma palavra não nula é equivalente por permutação a um código linear sobre $\mathbb{Z}_4$ com matriz geradora da forma*

$$\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{pmatrix}, \tag{1}$$

onde I_{k_1} e I_{k_2} denotam as matrizes identidade de ordem k_1 e k_2 respectivamente. A e C são matrizes sobre $\mathbb{Z}_2$ e B é uma matriz sobre $\mathbb{Z}_4$. Então $\mathcal{C}$ é um grupo abeliano do tipo $4^{k_1}2^{k_2}$ e contém $2^{2k_1+k_2}$ palavras.

Demonstração. Nós aplicamos indução em um código de comprimento n e dividimos em dois casos:

1. Existe uma palavra c do código $\mathcal{C}$ de ordem 4.

   Depois de permutar as coordenadas da palavra c e, se necessário, multiplicar essa palavra por -1, podemos assumir que a palavra do código de ordem 4 é da forma $(1, c_2, \ldots, c_n)$. Seja $\mathcal{C}' = \{(0, x_2, \ldots, x_n) \in \mathcal{C}\}$. Claramente $\mathcal{C}'$ também é um código linear sobre $\mathbb{Z}_4$ e pode ser considerado como um código de comprimento $n-1$ por termos deletado a primeira coordenada. Pela hipótese de indução, $\mathcal{C}'$ tem uma matriz geradora da forma

$$\begin{pmatrix} 0 & I_{k_1-1} & A_1 & B_1 \\ 0 & 0 & 2I_{k_2} & 2C \end{pmatrix},$$

onde A_1 e C são matrizes sobre $\mathbb{Z}_2$ e B_1 é uma matriz sobre $\mathbb{Z}_4$. Então $\mathcal{C}$ tem matriz geradora da forma

$$\begin{pmatrix} 1 & c_2 \cdots c_{k_1} & c_{k_1+1} \cdots c_{k_1+k_2} & c_{k_1+k_2+1} \cdots c_n \\ 0 & I_{k_1-1} & A_1 & B_1 \\ 0 & 0 & 2I_{k_2} & 2C \end{pmatrix}.$$

Depois de adicionar uma combinação linear das ultimas $k_1 - 1 + k_2$ linhas na primeira linha da matriz acima, podemos assumir que a nova matriz é da forma da matriz (1).

2. Não existe nenhuma palavra de ordem 4 em $\mathcal{C}$.

   Temos então que toda palavra de $\mathcal{C}$ é de ordem 2. Desde que $\mathcal{C} \neq \{(0, \ldots, 0)\}$, existe uma palavra de ordem 2 em $\mathcal{C}$. Como no item 1, podemos assumir que essa palavra é da forma

   $$(2, 2c_2, \cdots, 2c_n).$$

   Defina $\mathcal{C}'$ como no item 1. Então $\mathcal{C}'$ também é um código linear sobre $\mathbb{Z}_4$ sem palavras de ordem 4. $\mathcal{C}'$ pode ser considerado um código de comprimento $n-1$. Pela hipótese de indução, $\mathcal{C}'$ tem matriz geradora da forma

   $$(0 \;\; 2I_{k_2-1} \;\; 2C_1)$$

   onde C_1 é uma matriz sobre $\mathbb{Z}_2$. Então $\mathcal{C}$ tem matriz geradora da forma

   $$\begin{pmatrix} 2 & 2c_2 \cdots 2c_{k_2} & 2c_{k_2+1} \cdots 2c_n \\ 0 & 2I_{k_2-1} & 2C_1 \end{pmatrix}$$

   Depois de adicionar uma combinação linear das ultimas $k_2 - 1$ linhas na primeira linha da matriz acima, podemos assumir que a nova matriz é da forma

   $$(2I_{k_2} \;\; 2C),$$

   que é uma matriz da forma (1) com $k_1 = 0$. Como a matriz geradora de $\mathcal{C}$ é da forma (1), é óbvio que $\mathcal{C}$ é um grupo abeliano de tipo $4^{k_1}2^{2k_2}$ que contém $2^{2k_1+k_2}$ palavras

□

Sejam $u_1, \cdots, u_{k_1} \in \mathbb{Z}_4$ e $u_{k_1+1}, \cdots, u_{k_1+k_2} \in \mathbb{Z}_2$. Podemos chamar $u_1, \cdots, u_{k_1}, u_{k_1+1}, \cdots, u_{k_1+k_2}$ de símbolos de informação. Então a codificação é realizada pela multiplicação de matrizes

$$(u_1, \cdots, u_{k_1}, u_{k_1+1}, \cdots, u_{k_1+k_2})G.$$

Proposição 3.2: *O código dual de um código linear sobre $\mathbb{Z}_4$ que tem matriz geradora da forma (1) tem matriz geradora da forma*

$$\begin{pmatrix} -B^t - C^t A^t & C^t & I_{n-k_1-k_2} \\ 2A^t & 2I_{k_2} & 0 \end{pmatrix}, \tag{2}$$

onde n é o comprimento de $\mathcal{C}$. $\mathcal{C}^\perp$ é um grupo abeliano do tipo $4^{n-k_1-k_2}2^{k_2}$ e contém $2^{2n-2k_1-k_2}$ palavras.

Demonstração. Denote por $\mathcal{C}'$ o código linear sobre $\mathbb{Z}_4$ com matriz geradora da forma (2). Observe que

$$\mathcal{C} \cdot \mathcal{C}'^t = \begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{pmatrix} \cdot \begin{pmatrix} -B-AC & 2A \\ C & 2I_{k_2} \\ I_{n-k_1-k_2} & 0 \end{pmatrix} = (0),$$

logo temos que $\mathcal{C}' \subset \mathcal{C}^{\perp}$.

Seja $c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}^{\perp}$. Depois de adicionar uma combinação linear das primeiras $n - k_1 - k_2$ linhas de (2) e c, podemos obter uma palavra de $\mathcal{C}^{\perp}$, que é da forma

$$c' = (c_1, \ldots, c_{k_1}, c_{k_1+1}, \ldots, c_{k_1+k_2}, 0, \ldots, 0).$$

Desde que c' seja ortogonal às últimas k_2 linhas de (1), cada $c_{k_1+1}, \ldots, c_{k_1+k_2}$ é 0 ou 2. Depois de adicionar uma combinação linear das ultimas k_2 linhas de (2) a c', podemos obter uma palavra do código $\mathcal{C}^{\perp}$ da forma

$$c'' = (c_1, \ldots, c_{k_1}, 0, \ldots, 0).$$

Como c' é ortogonal as primeiras k_1 linhas de (1), então $c_1 = \cdots = c_{k_1} = 0$. Portanto, $c \in \mathcal{C}'$. □

A matriz (2) é chamada de matriz teste de paridade de um código linear $\mathcal{C}$ sobre $\mathbb{Z}_4$ gerado pelas linhas da matriz (1). Uma palavra $c = (c_1 \ldots, c_n)$ pertence a $\mathcal{C}$ se e somente se c é ortogonal a todas as linhas de (2).

Corolário 3.1: *Qualquer código autodual sobre $\mathbb{Z}_4$ de comprimento n, contém 2^n palavras.*

Demonstração. Seja $\mathcal{C}$ um código autodual sobre $\mathbb{Z}_4$ de comprimento n com matriz geradora (1). Pela Proposição 3.1, $|\mathcal{C}| = 2^{2k_1+k_2}$ e pela Proposição 3.2, $|\mathcal{C}^{\perp}| = 2^{2n-2k_1-k_2}$. Desde que $\mathcal{C}^{\perp} = \mathcal{C}$, temos $2^{2n-2k_1-k_2} = 2^{2k_1+k_2}$. Portanto, $n = 2k_1 + k_2$ e $|\mathcal{C}| = 2^n$. □

4 EXEMPLOS

Exemplo 4.1 Seja $\mathcal{K}_4$ o código linear sobre $\mathbb{Z}_4$ com matriz geradora

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}. \tag{3}$$

Pela Proposição 3.1, $\mathcal{K}_4$ é do tipo $4^1 2^2$. Portanto, $|\mathcal{K}_4| = 16$. Segue da Proposição 3.2 que $\mathcal{K}_4^{\perp}$ também é do tipo $4^1 2^2$. Portanto, $|\mathcal{K}_4| = 16$. Vemos que quaisquer duas linhas da matriz (3), distintas ou não, são ortogonais. Portanto, $\mathcal{K}_4 \subseteq \mathcal{K}_4^{\perp}$. Assim $\mathcal{K}_4 = \mathcal{K}_4^{\perp}$ e $\mathcal{K}_4$ é um código autodual.

Exemplo 4.2 Seja $\mathcal{C}_1$ o código linear sobre $\mathbb{Z}_4$ com matriz geradora

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \end{pmatrix}. \tag{4}$$

É fácil ver que $\mathcal{C}_1$ é auto-ortogonal. Pela Proposição 3.1, $\mathcal{C}_1$ é do tipo $4^1 2^1$ e pela Proposição 3.2, $\mathcal{C}_1^{\perp}$ é do tipo $4^2 2^1$. $\mathcal{C}_1^{\perp}$ tem matriz geradora

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & 0 & 1 \\ 2 & 2 & 0 & 0 \end{pmatrix}. \tag{5}$$

Exemplo 4.3 Seja $\mathcal{O}_8$ o código linear sobre $\mathbb{Z}_4$ com matriz geradora

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{pmatrix}. \tag{6}$$

Pela Proposição 3.1 $\mathcal{O}_8$ é do tipo 4^4 e pela Proposição 3.2 $\mathcal{O}_8^{\perp}$ também é do tipo 4^4. É fácil verificar que qualquer duas linhas da matriz geradora, distintas ou não, são ortogonais. Portanto, $\mathcal{O}_8 = \mathcal{O}_8^{\perp}$, isto é, $\mathcal{O}_8$ é autodual. $\mathcal{O}_8$ é chamado de octacódigo.

Exemplo 4.4 Seja $\mathcal{K}_8$ o código linear sobre $\mathbb{Z}_4$ com matriz geradora

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix}. \tag{7}$$

Pela Proposição 3.1 $\mathcal{K}_8$ é do tipo $4^1 2^6$ e pela Proposição 3.2 $\mathcal{K}_8^{\perp}$ também é do tipo $4^1 2^6$. É fácil verificar que qualquer duas linhas da matriz geradora, distintas ou não, são ortogonais. Portanto, $\mathcal{K}_8 = \mathcal{K}_8^{\perp}$, isto é, $\mathcal{K}_8$ é autodual.

5 APLICAÇÃO DE GRAY

Nesta seção vamos introduzir uma aplicação que constrói códigos binários interessantes a partir de códigos quaternários. A aplicação de Gray é usualmente denotada por ϕ e definida por:

$$\begin{aligned} \phi : \mathbb{Z}_4 &\to \mathbb{Z}_2^2 \\ 0 &\mapsto (00) \\ 1 &\mapsto (01) \\ 2 &\mapsto (11) \\ 3 &\mapsto (10) \end{aligned}$$

Claramente, ϕ é uma bijeção de $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$. A seguir, vamos relacionar a aplicação de Gray com o peso e a distância de Hamming e o peso e a distância de Lee. Para isso, vamos introduzir estes conceitos.

Denotemos o peso de Hamming de um vetor binário $v = (v_1, \ldots, v_n)$ por $w(v) = |\{i : v_i \neq 0$ para $i = 1, \ldots n\}|$, que é o número de entradas distintas de 0 e a distância de Hamming entre dois vetores binários $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ do mesmo comprimento por $d(u, v) = |\{i : u_i \neq v_i$ para $i = 1, \ldots, n\}|$, que é o número de entradas distintas entre os dois vetores. Já o peso de Lee de $0, 1, 2, 3 \in \mathbb{Z}_4$, é definido por

$$w_L(0) = 0, \ w_L(1) = w_L(3) = 1, \ w_L(2) = 2.$$

O peso de Lee, denotado por $w_L(x)$, de um $x = (x_1, \ldots, x_n) \in \mathbb{Z}_4^n$ é definido como a soma dos pesos de Lee de suas coordenadas, isto é

$$w_L(x) = \sum_{i=1}^{n} w_L(x_i).$$

Essa função peso define uma distância em $\mathbb{Z}_4$ por

$$d_L(x,y) = w_L(x-y),$$

que é chamada distância de Lee.

Pelas definições anteriores, podemos ver que

$$w_L(x) = w(\phi(x)) \quad \forall x \in \mathbb{Z}_4, \tag{8}$$

e podemos também verificar que

$$d_L(x,y) = d(\phi(x),\phi(y)) \quad \forall x,y \in \mathbb{Z}_4. \tag{9}$$

Nas equações (8) e (9) acima, observamos a relação entre o peso de Lee com o peso de Hamming e a distância de Lee com a distância de Hamming através da aplicação de Gray.

Assim vemos que a aplicação de Gray ϕ não é um homomorfismo[1] de grupos aditivos de $\mathbb{Z}_4$ para $\mathbb{Z}_2^2$.

Na tabela abaixo introduzimos as aplicações α, β, γ de $\mathbb{Z}_4$ para $\mathbb{Z}_2$ que serão úteis quando realizarmos operações com a aplicação de Gray.

$\mathbb{Z}_4$	α	β	γ
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

TABELA 1

Claramente, α é um homomorfismo de $\mathbb{Z}_4$ para $\mathbb{Z}_2$, mas β e γ não são. Cada elemento $x \in \mathbb{Z}_4$ pode ser escrito como $\alpha(x) + 2\beta(x)$, realizando a soma em $\mathbb{Z}_4$. Também temos que a soma realizada em $\mathbb{Z}_2$ $\alpha(x) + \beta(x) + \gamma(x) = 0 \quad \forall x \in \mathbb{Z}_4$.

A aplicação de Gray ϕ pode ser expressa em termos de β e γ como se segue:

$$\phi(x) = (\beta(x), \gamma(x)) \quad \forall x \in \mathbb{Z}_4.$$

As aplicações α, β, γ podem ser estendidas para $\mathbb{Z}_4^n$. Dado $x = (x_1, \ldots, x_n) \in \mathbb{Z}_4^n$, definimos

$$\alpha(x) = (\alpha(x_1), \ldots, \alpha(x_n)),$$
$$\beta(x) = (\beta(x_1), \ldots, \beta(x_n)),$$
$$\gamma(x) = (\gamma(x_1), \ldots, \gamma(x_n)).$$

Então ϕ é estendido para $\mathbb{Z}_4^n$ como se segue:

$$\phi(x) = (\beta(x), \gamma(x)) \quad \forall x \in \mathbb{Z}_4^n. \tag{10}$$

Claramente, a extensão ϕ é uma bijeção de $\mathbb{Z}_4^n$ para $\mathbb{Z}_2^{2n}$. Para qualquer $x \in \mathbb{Z}_4^n$, $\phi(x)$ é chamado de imagem binária de x sobre ϕ.

Teorema 5.1: *ϕ é uma aplicação que preserva os pesos, de*

($\mathbb{Z}_4^n$, peso de Lee) para ($\mathbb{Z}_2^{2n}$, peso de Hamming),

isto é:

$$w_L(x) = w(\phi(x)) \quad \forall x \in \mathbb{Z}_4^n, \tag{11}$$

e ϕ também é uma aplicação que preserva as distancias, de

[1] Um homomorfismo entre grupos aditivos G e $\tilde{G}$ é uma aplicação $\theta : G \longrightarrow \tilde{G}$ tal que para $x, y \in G$ temos que $\theta(x+y) = \theta(x) + \theta(y)$.

($\mathbb{Z}_4^n$, distancia de Lee) para ($\mathbb{Z}_2^{2n}$, distancia de Hamming),

isto é:

$$d_L(x,y) = d(\phi(x),\phi(y)) \quad \forall x,y \in \mathbb{Z}_4^n. \tag{12}$$

Demonstração. Para qualquer $x = (x_1,\ldots,x_n) \in \mathbb{Z}_4^n$, $w_L(x) = \sum_{i=1}^{n} w_L(x_i)$ e

$$\begin{aligned} w(\phi(x)) &= w((\beta(x),\gamma(x))) = w(\beta(x)) + w(\gamma(x)) \\ &= \sum_{i=1}^{n} w(\beta(x_i)) + \sum_{i=1}^{n} w(\gamma(x_i)) \\ &= \sum_{i=1}^{n} w((\beta(x_i),\gamma(x_i)) \\ &= \sum_{i=1}^{n} w(\phi(x_i)). \end{aligned}$$

Por (8), $w_L(x_i) = w(\phi(x_i))$, para $i = 1,2,\ldots,n$. Portanto, temos (11). Analogamente, de (9) obtemos (12). □

Proposição 5.1: *Para qualquer $x = (x_1,\ldots,x_n) \in \mathbb{Z}_4^n$, temos que*

$$w_L(x) \equiv \sum_{i=1}^{n} x_i \pmod 2 \tag{13}$$

Seja $\phi(x) = (y_1,y_2,\ldots,y_{2n}) \in \mathbb{Z}_2^{2n}$, então

$$\sum_{i=1}^{n} x_i \equiv \sum_{i=1}^{2n} y_i \pmod 2 \tag{14}$$

Em particular, se $\sum_{i=1}^{n} x_i = 0$ ou 2 em $\mathbb{Z}_4$, então x é uma palavra de peso de Lee par em $\mathbb{Z}_4^n$ e $\phi(x)$ é uma palavra de peso (de Hamming) par em $\mathbb{Z}_2^{2n}$.

Demonstração. Tomando $\sum_{i=1}^{n} x_i$ como uma soma em $\mathbb{Z}_4$, então temos que

$$\sum_{i=1}^{n} x_i = w_1(x) + 2w_2(x) + 3w_3(x), \text{ onde } w_a(x) = |\{i : x_i = a\}| \text{ para } a \in \mathbb{Z}_4.$$

Mas $w_L(x) = w_1(x) + 2w_2(x) + w_3(x)$, sendo o lado direito da equação como uma soma em $\mathbb{Z}$. Portanto, temos (13). Além disso, tomando $\sum_{i=1}^{2n} y_i$ como uma soma em $\mathbb{Z}$, pelo Teorema 5.1 temos

$$\sum_{i=1}^{2n} y_i = w(\phi(x)) = w_L(x). \tag{15}$$

De (13) e (15) obtemos (14).

□

6 IMAGENS BINÁRIAS DE CÓDIGOS QUATERNÁRIOS

Seja $\mathcal{C}$ um código sobre $\mathbb{Z}_4$ de comprimento n. Defina

$$\widetilde{C} = \phi(\mathcal{C}) = \{\phi(\mathbf{c}) | \mathbf{c} \in \mathcal{C}\},$$

que é chamado de imagem binária de $\mathcal{C}$ sobre a aplicação de Gray ou, simplesmente, a imagem binária de $\mathcal{C}$. Se $\mathcal{C}$ tem comprimento n, então $\widetilde{C} \subseteq \mathbb{Z}_2^{2n}$, isto é, $\widetilde{C}$ é um código binário de comprimento $2n$. Lembremos que

$$\min\{w(\phi(\mathbf{c})) \mid \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq (0 \ldots 0)\},$$

e

$$\min\{d(\phi(\mathbf{c}), \phi(\mathbf{c}')) \mid \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \mathbf{c} \neq \mathbf{c}'\},$$

são o peso (de Hamming) mínimo e a distância (de Hamming) mínima de $\widetilde{C}$, respectivamente. Similarmente definimos

$$\min\{w_L(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq (0 \ldots 0)\},$$

e

$$\min\{d_L(\mathbf{c}, \mathbf{c}') \mid \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \mathbf{c} \neq \mathbf{c}'\},$$

como o peso mínimo de Lee e a distância mínima de Lee de $\mathcal{C}$, respectivamente. O Teorema 5.1 implica, em particular:

Proposição 6.1: *Seja $\mathcal{C}$ um código sobre $\mathbb{Z}_4$ de comprimento n e $\widetilde{C} = \phi(\mathcal{C})$. Então o peso mínimo de Lee e a distância mínima de Lee de $\mathcal{C}$ são iguais ao peso e distância mínima (de Hamming) de $\widetilde{C} = \phi(\mathcal{C})$, respectivamente.*

Da Proposição 5.1 obtemos

Proposição 6.2: *Seja $\mathcal{C}$ um código sobre $\mathbb{Z}_4$ de comprimento n e assuma que para toda palavra $\mathbf{c} = (c_1, \ldots, c_n)$ de $\mathcal{C}$, $\sum_{i=1}^{n} c_i \equiv 0 \pmod 2$, então toda palavra de $\mathcal{C}$ tem peso de Lee par e toda palavra de sua imagem binária $\phi(\mathcal{C})$ são de peso (de Hamming) par.*

Exemplo 6.1 Consideremos a imagem binária do código quaternário $\mathcal{C} = \{(0,0),\ (2,2)\}$ de comprimento 2 e tipo 2^1. Temos

$$\phi(0,0) = (\beta(0,0), \gamma(0,0)) = (0,0,0,0),$$
$$\phi(2,2) = (\beta(2,2), \gamma(2,2)) = (1,1,1,1).$$

Portanto,

$$\phi(\mathcal{C}_3) = \{(0,0,0,0),\ (1,1,1,1)\},$$

o que é um código binário linear.

Exemplo 6.2 A imagem binária $\phi(\mathcal{K}_4)$ do código linear quaternário $\mathcal{K}_4$ com matriz geradora

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix},$$

consiste das seguintes 16 palavras:

$$\begin{array}{cc}
0\,0\,0\,0\,0\,0\,0\,0 & 0\,0\,1\,1\,0\,0\,1\,1\\
0\,0\,0\,0\,1\,1\,1\,1 & 0\,0\,1\,1\,1\,1\,0\,0\\
1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,0\,0\,1\,1\,0\,0\\
1\,1\,1\,1\,0\,0\,0\,0 & 1\,1\,0\,0\,0\,0\,1\,1\\
0\,1\,0\,1\,0\,1\,0\,1 & 0\,1\,1\,0\,0\,1\,1\,0\\
0\,1\,0\,1\,1\,0\,1\,0 & 0\,1\,1\,0\,1\,0\,0\,1\\
1\,0\,1\,0\,1\,0\,1\,0 & 1\,0\,0\,1\,1\,0\,0\,1\\
1\,0\,1\,0\,0\,1\,0\,1 & 1\,0\,0\,1\,0\,1\,1\,0
\end{array}$$

Podemos ver que $\phi(\mathcal{K}_4)$ é um código binário com distância mínima 4. Assim $\phi(\mathcal{K}_4)$ é o código binário de Hamming estendido (ver [4], p. 27) de comprimento 8. Ele tem a seguinte matriz geradora

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1\\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1\\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}. \tag{16}$$

Exemplo 6.3 A imagem binária $\phi(\mathcal{C}_1)$ do código linear $\mathcal{C}_1$ do Exemplo 4.2 com matriz geradora

$$\begin{pmatrix}
1 & 1 & 1 & 1\\
0 & 2 & 0 & 2
\end{pmatrix}$$

consiste das seguintes 8 palavras

$$\begin{array}{cc}
0\,0\,0\,0\,0\,0\,0\,0 & 0\,1\,0\,1\,0\,1\,0\,1\\
0\,0\,0\,0\,1\,1\,1\,1 & 0\,1\,0\,1\,1\,0\,1\,0\\
1\,1\,1\,1\,1\,1\,1\,1 & 1\,0\,1\,0\,1\,0\,1\,0\\
1\,1\,1\,1\,0\,0\,0\,0 & 1\,0\,1\,0\,0\,1\,0\,1
\end{array}$$

$\phi(\mathcal{C}_1)$ também é um código binário linear com matriz geradora

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1\\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}. \tag{17}$$

Denote por $\alpha(M), \beta(M), \gamma(M), \phi(M)$ as imagens de todas as linhas de uma matriz M sobre as aplicações $\alpha, \beta, \gamma, \phi$ respectivamente. Então $\phi(M) = (\beta(M), \gamma(M))$.

Proposição 6.3: *Seja $\widetilde{C} = \phi(\mathcal{C})$ a imagem binária de um código quaternário linear $\mathcal{C}$ com matriz geradora (1). Se $\widetilde{C}$ é linear, $\widetilde{C}$ tem matriz geradora da forma*

$$\begin{pmatrix}
I_{k_1} & A & \alpha(B) & I_{k_1} & A & \alpha(B)\\
0 & I_{k_2} & C & 0 & I_{k_2} & C\\
0 & 0 & \beta(B) & I_{k_1} & A & \gamma(B)
\end{pmatrix} \tag{18}$$

Demonstração. Assuma que $\widetilde{C}$ é linear, então $\widetilde{C}$ é gerado pela imagem binária das linhas da matriz

$$\begin{pmatrix}
I_{k_1} & A & B\\
2I_{k_1} & 2A & 2B\\
3I_{k_1} & 3A & 3B\\
0 & 2I_{k_2} & 2C
\end{pmatrix},$$

onde A e C são matrizes sobre $\mathbb{Z}_2$ e B é uma matriz sobre $\mathbb{Z}_4$. Temos que

$$\begin{aligned}
\phi(I_{k_1}\ A\ B) &= (\beta(I_{k_1}\ A\ B)\ \gamma(I_{k_1}\ A\ B))\\
&= (0\ 0\ \beta(B)\ I_{k_1}\ A\ \gamma(B)).
\end{aligned}$$

$$\begin{aligned}\phi(2I_{k_1}\ 2A\ 2B) &= (\beta(2I_{k_1}\ 2A\ 2B)\ \gamma(2I_{k_1}\ 2A\ 2B))\\ &= (I_{k_1}\ A\ \alpha(B)\ I_{k_1}\ A\ \alpha(B)).\end{aligned}$$

$$\begin{aligned}\phi(3I_{k_1}\ 3A\ 3B) &= (\beta(3I_{k_1}\ 3A\ 3B)\ \gamma(3I_{k_1}\ 3A\ 3B))\\ &= (I_{k_1}\ A\ \gamma(B)\ 0\ 0\ \beta(B)).\end{aligned}$$

$$\begin{aligned}\phi(0\ 2I_{k_2}\ 2C) &= (\beta(0\ 2I_{k_2}\ 2C)\ \gamma(0\ 2I_{k_2}\ 2C))\\ &= (0\ I_{k_2}\ C\ 0\ I_{k_2}\ C).\end{aligned}$$

A partir de $\alpha(B)+\beta(B)+\gamma(B)=0$, obtemos que

$$(I_{k_1}\ A\ \gamma(B)\ 0\ 0\ \beta(B)) = (0\ 0\ \beta(B)\ I_{k_1}\ A\ \gamma(B)) + (I_{k_1}\ A\ \alpha(B)\ I_{k_1}\ A\ \alpha(B)).$$

Assim $\widetilde{C}$ é gerado pelas linhas de (18). Claramente as linhas de (18) são linearmente independentes. Portando (18) é a matriz geradora de $\widetilde{C}$.

□

Note que a matriz geradora de $\phi(\mathcal{K}_4)$ dada no Exemplo 6.2 é precisamente a dada pela Proposição 6.3.

7 CONDIÇÕES DE LINEARIDADE

Um código binário $\widetilde{C}$ é chamado de linear quaternário se após uma permutação de suas coordenadas, ele é a imagem binária de um código linear quaternário. Agora queremos estudar os seguintes problemas:

(i) Quando um dado código binário é linear quaternário?

(ii) Quando a imagem binária de um código linear quaternário é linear?

Uma condição necessária para um código binário ser linear quaternário é

Proposição 7.1: *Se um código binário é linear quaternário, então seu comprimento é par.*

Defina a permutação σ no vetor de dimensão $2n$ $(x_1,\ldots,x_{2n})$ como segue:

$$\sigma:\ (x_1,\ldots,x_n,x_{n+1},\ldots,x_{2n})\ \rightarrow\ (x_{n+1},\ldots,x_{2n},x_1,\ldots,x_n) \tag{19}$$

Chamamos σ de aplicação de "troca". Vemos que,

$$\sigma = (1\ n+1)(2\ n+2)\cdots(n\ 2n).$$

Então para qualquer $x\in\mathbb{Z}_4^n$,

$$\sigma(\phi(x)) = \sigma(\beta(x)\gamma(x)) = (\gamma(x),\beta(x)) = \phi(-x). \tag{20}$$

Portanto temos:

Proposição 7.2: *Se um código binário $\widetilde{C}$ é linear quaternário, depois de uma permutação de suas coordenadas, $\sigma(\widetilde{C})=\widetilde{C}$.*

Denote por $*$ a multiplicação componente a componente de dois vetores, isto é:

$$(x_1,\ldots,x_n)*(y_1,\ldots,y_n) = (x_1y_1,\ldots,x_ny_n).$$

Lema 7.1: *Para todo $x,y\in\mathbb{Z}_4^n$, temos*

$$(\phi(x)+\sigma(\phi(x)))*(\phi(y))+\sigma(\phi(y))) = \phi(2\alpha(x)*\alpha(y)),$$

sendo que a multiplicação de $\alpha(x)*\alpha(y)$ por 2 é feita sobre $\mathbb{Z}_4$.

Demonstração. Por (19),

$$\begin{aligned}(\phi(x)+\sigma(\phi(x)))*(\phi(y))+\sigma(\phi(y))) &= ((\beta(x),\gamma(x))+(\gamma(x),\beta(x)))*((\beta(y),\gamma(y))+(\gamma(y),\beta(y)))\\ &= ((\beta(x)+\gamma(x),\gamma(x)+\beta(x))*((\beta(y)+\gamma(y),\gamma(y)+\beta(y))\\ &= (\alpha(x),\alpha(x))*(\alpha(y),\alpha(y))\\ &= (\alpha(x)*\alpha(y),\alpha(x)*\alpha(y))\\ &= \phi(2\alpha(x)*\alpha(y)).\end{aligned}$$

□

Lema 7.2: *Para todo $x,y\in\mathbb{Z}_4^n$, temos*

$$\phi(x+y)=\phi(x)+\phi(y)+(\phi(x)+\sigma(\phi(x)))*(\phi(y)+\sigma(\phi(y))). \tag{21}$$

Demonstração. Pelo Lema 7.1, (21) é equivalente a

$$\phi(x)+\phi(y)+\phi(x+y)=\phi(2\alpha(x)*\alpha(y)). \tag{22}$$

Portanto, é suficiente verificar (22). Assim, sabemos que

$$\phi(x)+\phi(y)+\phi(x+y)=(\beta(x)+\beta(y)+\beta(x+y),\gamma(x)+\gamma(y)+\gamma(x+y)),$$

e

$$\phi(2\alpha(x)*\alpha(y))=(\alpha(x)*\alpha(y),\alpha(x)*\alpha(y)).$$

Deste modo precisamos mostrar que

$$\begin{aligned}\beta(x)+\beta(y)+\beta(x+y) &= \gamma(x)+\gamma(y)+\gamma(x+y)\\ &= \alpha(x)*\alpha(y) \text{ para todo } x,y\in\mathbb{Z}_4^n.\end{aligned}$$

Usando a Tabela 1, verificamos a identidade acima para $n=1$ e portanto, o resultado é válido para quaisquer $x,y\in\mathbb{Z}_4^n$.

□

Corolário 7.1: *Para todo $x,y\in\mathbb{Z}_4^n$, temos*

$$\phi(x+y)=\phi(x)+\phi(y)+\phi(2\alpha(x)*\alpha(y)). \tag{23}$$

Agora podemos responder os problemas propostos no começo desta seção.

Proposição 7.3: *Um código binário $\widetilde{C}$, não necessariamente linear, de comprimento par é linear quaternário se e somente se depois de uma permutação de suas coordenadas, satisfaz:*

$$u,v\in\widetilde{C}\Rightarrow u+v+(u+\sigma(u))*(v+\sigma(v))\in\widetilde{C} \tag{24}$$

Demonstração. Assuma que $\widetilde{C}=\phi(\mathcal{C})$, onde $\mathcal{C}$ é um código linear quaternário. Seja $u,v\in\widetilde{C}$, então existem $x,y\in\mathcal{C}$ tais que $u=\phi(x),\ v=\phi(y)$. Desde que $\mathcal{C}$ seja linear, $x+y\in\mathcal{C}$. Pelo Lema 7.2,

$$\begin{aligned}u+v+(u+\sigma(u))*(v+\sigma(v)) &= \phi(x)+\phi(y)+(\phi(x)+\sigma(\phi(x)))*(\phi(y)+\sigma(\phi(y)))\\ &= \phi(x+y)\in\phi(\mathcal{C})=\widetilde{C}.\end{aligned}$$

Reciprocamente, assumamos que vale a condição (24). Seja $2n$ a dimensão de $\widetilde{C}$. Defina $\mathcal{C}=\{c\in\mathbb{Z}_4^n\mid\phi(c)\in\widetilde{C}\}$. Vamos provar que $\mathcal{C}$ é um código linear quaternário. Seja $x,y\in\mathcal{C}$. Então $\phi(x),\phi(y)\in\widetilde{C}$. Por (24), $\phi(x)+\phi(y)+(\phi(x)+\sigma(\phi(x)))*(\phi(y)+\sigma(\phi(y)))\in\widetilde{C}$. Por (21), $\phi(x+y)\in\widetilde{C}$. Portanto $x+y\in\mathcal{C}$. □

Corolário 7.2: *Um código linear binário $\widetilde{C}$ de comprimento par é linear quaternário se e somente se depois de uma permutação se suas coordenadas,*

$$u, v \in \widetilde{C} \Rightarrow (u + \sigma(u)) * (v + \sigma(v)) \in \widetilde{C}.$$

Proposição 7.4: *A imagem binária $\widetilde{C} = \phi(\mathcal{C})$ de um código linear quaternário $\mathcal{C}$ é linear se e somente se*

$$x, y \in \mathcal{C} \Rightarrow 2\alpha(x) * \alpha(y) \in \mathcal{C}. \tag{25}$$

Demonstração. Suponhamos que $\widetilde{C}$ é linear. Desde que $\mathcal{C}$ seja linear, para quaisquer $x, y \in \mathcal{C}$, $x + y \in \mathcal{C}$. Então $\phi(x), \phi(y), \phi(x + y) \in \widetilde{C}$. Como $\widetilde{C}$ é linear, $\phi(x) + \phi(y) + \phi(x + y) \in \widetilde{C}$. Pelo Corolário 7.1, temos que $\phi(2\alpha(x) * \alpha(y)) \in \widetilde{C}$. Como ϕ é uma bijeção, $2\alpha(x) * \alpha(y) \in \mathcal{C}$.

Reciprocamente, assumamos que a condição (25) é válida. Sejam $u, v \in \widetilde{C}$. Existem $x, y \in \mathcal{C}$ tais que $u = \phi(x), v = \phi(y)$. Por (25), $2\alpha(x) * \alpha(y) \in \mathcal{C}$. Como $\mathcal{C}$ é linear, $x + y + 2\alpha(x) * \alpha(y) \in \mathcal{C}$ e $\phi(x + y + 2\alpha(x) * \alpha(y)) \in \widetilde{C}$. Pelo Corolário 7.1,

$$\begin{aligned}&\phi(x + y) + \phi(2\alpha(x) * \alpha(y)) + \phi(2\alpha(x + y) * \alpha(2\alpha(x) * \alpha(y)))\\ &= \phi(x + y + 2\alpha(x) * \alpha(y)) \in \widetilde{C}.\end{aligned}$$

Claramente, $\alpha(2\alpha(x) * \alpha(y)) = 0$. Portanto,

$$\phi(x + y) + \phi(2\alpha(x) * \alpha(y)) \in \widetilde{C}.$$

Novamente pelo Corolário 7.1,

$$\phi(2\alpha(x) * \alpha(y)) = \phi(x + y) + \phi(x) + \phi(y).$$

Assim

$$\begin{aligned} u + v &= \phi(x) + \phi(y)\\ &= \phi(x) + \phi(y) + \phi(x + y) + \phi(x + y)\\ &= \phi(2\alpha(x) * \alpha(y)) + \phi(x + y) \in \widetilde{C}.\end{aligned}$$

Isso prova que $\widetilde{C}$ é linear.

□

Corolário 7.3: *Seja $\mathcal{C}$ um código linear quaternário, sejam $x_1, \ldots, x_m$ um conjunto gerador de $\mathcal{C}$, e $\widetilde{C} = \phi(\mathcal{C})$. Então $\widetilde{C}$ é linear se e somente se $2\alpha(x_i) * \alpha(x_j) \in \mathcal{C}$ para todo i, j tal que $1 \leq i \leq j \leq m$.*

Demonstração. Como $(x + y) * z = x * z + y * z$ para todo $x, y, z \in \mathbb{Z}_4^n$ e pelo fato de α ser um homomorfismo de grupos, temos que o resultado é válido. □

Exemplo 7.1 Considere o Octacódigo $\mathcal{O}_8$ introduzido no Exemplo 4.3. A matriz geradora dele é (6). Denote a primeira e segunda linha de (6) por x_1 e x_2 respectivamente, isto é

$$x_1 = (1\ 0\ 0\ 0\ 3\ 1\ 2\ 1),$$

$$x_2 = (0\ 1\ 0\ 0\ 1\ 2\ 3\ 1).$$

Claramente $2\alpha(x_1) * \alpha(x_2) = (0\ 0\ 0\ 0\ 2\ 0\ 0\ 2) \notin \mathcal{O}_8$.

Pela Proposição 7.4, $\phi(\mathcal{O}_8)$ não é linear. Como $\mathcal{O}_8$ é um código autodual, $\phi(\mathcal{O}_8)$ é formalmente autodual, $\phi(\mathcal{O}_8)$ é chamado de código de *Nordstrom-Robinson*. Este é um código binário não linear de comprimento 16 e tem 256 palavras. É fácil ver que a soma dos elementos de cada linha da matriz geradora (6) é igual a 0 em $\mathbb{Z}_4$, de onde obtemos que a soma das componentes de toda palavra de $\mathcal{O}_8$ é igual a 0 em $\mathbb{Z}_4$. Pela Proposição 6.2 todas

as palavras de $\phi(\mathcal{O}_8)$ são de peso par. Checando os pesos de todas as palavras de $\phi(\mathcal{O}_8)$, sabemos que $\phi(\mathcal{O}_8)$ tem peso mínimo 6.

Exemplo 7.2 Considere o código quaternário $\mathcal{K}_8$ introduzido no Exemplo 4.4 com matriz geradora (7). Podemos facilmente ver que para quaisquer duas linhas x e y, $2\alpha(x)*\alpha(y) \in \mathcal{K}_8$. Pelo Corolário 7.3, $\phi(\mathcal{K}_8)$ é um código binário linear. Como $\mathcal{K}_8$ é um código quaternário autodual, $\phi(\mathcal{K}_8)$ é formalmente autodual.

REFERÊNCIAS

[1] D. Özkaya, "A survey on quaternary codes and their binary images," Master's thesis, Middle East Technical University, 2009.

[2] Z.-X. Wan, *Quaternary Codes*. World Scientific Publishing Co. Pte. Ltd., 1997.

[3] I. N. Herstein, *Abstract Algebra*. Prentice Hall, 1996.

[4] F. M. Williams and N. Sloane, *The Theory of error-Correcting Codes*. North-Holland Publishing Company, New York, 1981.