Códigos de Reed-Muller

Reed-Muller Codes

Mariana Garabini Cornelissen
Universidade Federal de São João del Rei (UFSJ)
Departamento de Estatística, Física e Matemática (DEFIM), São João del-Rei, MG, Brasil
https://orcid.org/0000-0002-3613-5025, mariana@ufsj.edu.br

Isabella Fonseca Araújo
Universidade Federal de São João del Rei (UFSJ), São João del-Rei, MG, Brasil
https://orcid.org/0000-0001-7046-6285, isabellaraujo@outlook.com

Rafael Ribeiro de Assis Melo
Universidade Federal de São João del Rei (UFSJ), São João del-Rei, MG, Brasil
https://orcid.org/0000-0002-2432-0629, rafaelribeiromelo@hotmail.com

Informações do Artigo

Como citar este artigo

CORNELISSEN, Mariana Garabini; ARAÚJO, Isabella Fonseca; MELO, Rafael Ribeiro de Assis. Códigos de Reed-Muller. **REMAT: Revista Eletrônica da Matemática**, Bento Gonçalves, RS, v. 6, n. 1, p. 01-13, jan. 2020. DOI: https://doi.org/10.35819/remat2020v6i1id3429

Histórico do Artigo
Submissão: 04 de abril de 2019.
Aceite: 21 de novembro de 2019.

Resumo
Os códigos de Reed-Muller foram descobertos por David Eugene Muller e decodificados por Irving Stoy Reed em 1954. Tais códigos pertencem à família dos códigos lineares e são bastante utilizados hoje em dia, principalmente pelo seu simples e eficiente algoritmo de decodificação. Existem várias maneiras de se definir os códigos de Reed-Muller. Neste trabalho apresentamos, de maneira clara e simples, uma definição recursiva para todos os códigos de Reed-Muller de ordem $r \in \mathbb{N}$, denotados por $R(r, m)$, onde $0 \leq r \leq m$ e $m \in \mathbb{N}$. Utilizando essa definição, demonstramos quais são os principais parâmetros: comprimento, número de elementos e distância mínima dos códigos de Reed-Muller de primeira ordem, $R(1, m)$ para todo $m \in \mathbb{N}$. Além disso, apresentamos também uma aplicação dos códigos de primeira ordem em um programa espacial da National Aeronautics and Space Administration (NASA).

Palavras-chave
Códigos
Reed-Muller
Mariner 9

Keywords
Codes
Reed-Muller
Mariner 9

Abstract
The Reed-Muller codes were discovered by David Eugene Muller and decoded by Irving Stoy Reed in 1954. Such codes belong to the linear code family and are widely used nowadays, mainly for their simple and efficient decoding algorithm. There are several ways to define Reed-Muller codes. In this work, we present, in a clear and simple way, a recursive definition for all Reed-Muller codes of order $r \in \mathbb{N}$, denoted by $R(r, m)$, where $0 \leq r \leq m$, $m \in \mathbb{N}$. Using this definition, we show the main parameters: length, number of elements and minimum distance of first-order Reed-Muller codes, $R(1, m)$ for all $m \in \mathbb{N}$. In addition, we present an application of the first-order codes in a National Aeronautics and Space Administration (NASA) space program.

1 Introdução

Os códigos corretores de erros são um campo de pesquisa muito ativo na atualidade, presentes em diversas áreas do conhecimento, como na computação, engenharia e matemática. Eles são usados para transmitir mensagens codificadas que ao serem transmitidas eletronicamente por meio de um canal, podem sofrer alguns erros como interferências eletromagnéticas e de digitação. Esses erros, chamados de ruídos, fazem com que a mensagem recebida seja diferente da original. Assim, o objetivo da teoria dos códigos corretores de erros, que teve início em meados da década de 1940, é desenvolver métodos que permitam detectar e corrigir erros que possam ocorrer no envio de uma mensagem. Um desses métodos consiste em acrescentar informações nas mensagens pré-codificadas para que na sua transmissão, caso ocorra algum erro, este erro seja detectado e possivelmente corrigido.

Neste artigo estudamos uma classe de códigos corretores de erros chamada de Códigos de Reed-Muller, que pertence à família dos códigos lineares e que são códigos muito utilizados hoje em dia. Esta classe de códigos foi descoberta por David Eugene Muller e decodificada por Irving Stoy Reed. David E. Muller (1924 – 2008) foi um matemático e cientista da computação que iniciou seu trabalho na área de ciência da computação em 1952 na Universidade de Illinois. Reed (1923 – 2012), foi um matemático e engenheiro, e é mais conhecido por também ter co-inventado o código de Reed-Solomon, além do código de Reed-Muller, e também por suas contribuições na engenharia elétrica, como radar, processamento de sinal e imagem. Existem várias maneiras de se definir os códigos de Reed-Muller. Neste trabalho apresentamos uma descrição clara e simples de todos os códigos de Reed-Muller de ordem qualquer. Utilizando tal descrição, demonstramos quais são os principais parâmetros: comprimento, número de elementos e distância mínima de todos os códigos de Reed-Muller de primeira ordem. Além disso, também abordamos uma das aplicações do código de Reed-Muller de primeira ordem, o **Mariner 9**, que foi uma sonda espacial enviada pela National Aeronautics and Space Administration (NASA) em 30 de Maio de 1971 e que sobrevoou o planeta Marte a fim de tirar fotos.

Portanto, o objetivo desse texto é apresentar uma definição recursiva para todos os códigos de Reed-Muller de ordem $r \in \mathbb{N}$, denotados por $R(r, m)$, onde $0 \leq r \leq m$ e $m \in \mathbb{N}$ e, a partir dessa definição, demonstrar quais são os principais parâmetros dos $R(1, m)$ para todo $m \in \mathbb{N}$. E, por fim,

apenas para exemplificar uma aplicação de tais códigos, citamos um programa espacial da NASA que utilizou o código $R(1,5)$ para enviar fotos do planeta Marte para a Terra. Para saber mais sobre esse exemplo, o leitor pode consultar [2].

2 Conceitos Preliminares

Nesta seção, apresentamos algumas definições e resultados da teoria introdutória dos códigos corretores de erros para que o leitor tenha uma base teórica para compreender melhor as demais seções desse trabalho.

Definição 2.1. (Códigos Corretores de Erros) *Um código corretor de erros é um subconjunto próprio qualquer de* $\mathcal{F}^n = \underbrace{\mathcal{F} \times \mathcal{F} \times \ldots \times \mathcal{F}}_{n\ vezes}$*, com* $n \in \mathbb{N}$ *e* $\mathcal{F}$ *é um conjunto finito qualquer, chamado de alfabeto do código.*

Já os códigos lineares podem ser definidos como:

Definição 2.2. (Códigos Lineares) *Seja* $\mathcal{F}$ *um corpo finito. Um código* $\mathcal{C} \subset \mathcal{F}^n$ *é chamado de código linear se for um subespaço vetorial de* $\mathcal{F}^n$*.*

Neste artigo, trabalhamos apenas com códigos binários, isto é, códigos definidos sobre o alfabeto $\mathcal{F}$ igual ao corpo $\mathbb{F}_2 = \{0, 1\}$.

Observação 2.3. *Todo código linear é por definição um espaço vetorial de dimensão finita. Sejam* k *a dimensão do código* $\mathcal{C}$*,* $\{v_1, v_2, \ldots, v_k\}$ *uma de suas bases e* $a_1, a_2, \ldots, a_k$ *escalares em* $\mathbb{F}_2$*. Todo vetor* $v \in \mathcal{C}$ *se escreve como combinação linear dos vetores* $\{v_1, v_2, \ldots, v_k\}$ *de forma única, isto é:*

$$v = a_1v_1 + a_2v_2 + a_3v_3 + \cdots + a_kv_k$$

Logo, um código linear $\mathcal{C} \subset \mathbb{F}_2^n$ *de dimensão* k *possui* 2^k *elementos.*

A distância entre duas palavras, ou seja, entre dois elementos de um código é definida por:

Definição 2.4. (Distância de Hamming) *Dados dois elementos* $u = (u_1, u_2, \ldots, u_n)$ *e* $v = (v_1, v_2, \ldots, v_n) \in \mathcal{F}^n$ *com* $\mathcal{F}$ *um conjunto finito qualquer, chama-se distância de Hamming entre* u *e* v *ao número de posições em que estes dois elementos diferem, isto é:*

$$d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|$$

Daqui para frente, denotaremos por $|S|$ a cardinalidade de um conjunto S.

Dado um código $\mathcal{C} \subset \mathcal{F}^n$ chama-se de "distância mínima" do código $\mathcal{C}$ o número:

$$d = min\{d(u,v) : u, v \in \mathcal{C}, u \neq v\}$$

Um código $\mathcal{C} \subset \mathcal{F}^n$ possui três parâmetros fundamentais:

- o comprimento do código: n
- o número de elementos ou palavras do código: M
- a distância mínima do código: d

Em códigos lineares podemos sempre calcular a distância de um elemento até a origem, ou seja, o número de dígitos não nulos desse elemento, que é chamado de peso.

Definição 2.5. (Peso de um Código Linear) *O peso de um código linear $\mathcal{C}$, que denominaremos por $w(\mathcal{C})$, é o peso mínimo de todas as palavras não nulas de $\mathcal{C}$, isto é,*

$$w(\mathcal{C}) = min\{w(u) : u \in \mathcal{C} \backslash \{0\}\}$$

onde $w(u) = |\{i : u_i \neq 0\}|$, é o peso de u. Observe que $w(u) = d(u, 0)$.

Observação 2.6. *Note que, se $\mathcal{C} \subset \mathcal{F}^n$ é um código linear com distância mínima d então $\forall x, y \in \mathcal{F}^n$ temos que $d(x, y) = w(x - y)$. Agora, se $x, y \in \mathcal{C}$ e $x \neq y$ então $z = x - y \in \mathcal{C} - \{0\}$ e $d(x, y) = w(z)$. Logo, a distância mínima de um código linear coincide com o peso desse código.*

Segue abaixo o principal resultado da teoria básica dos códigos corretores de erros.

Teorema 2.7. *Seja $\mathcal{C}$ um código com distância mínima d. Então:*

(i) $\mathcal{C}$ detecta até (d − 1) erros;

(ii) $\mathcal{C}$ corrige até a parte inteira de $\frac{d-1}{2}$ erros, que será denotado por $\lambda = [\frac{d-1}{2}]$.

O leitor pode encontrar a demonstração desse resultado em [1].

Observe que, de acordo com o Teorema 2.7, quanto maior a distância mínima de um código, maior será sua capacidade de detecção e correção de erros.

3 Códigos de Reed-Muller

Os códigos de Reed-Muller formam uma classe importante e bem conhecida de códigos corretores de erros lineares e binários. Esses códigos foram descobertos por David Eugene Muller em 1954 e o primeiro algoritmo de decodificação para esses códigos foi concebido por Irving Stoy Reed também em 1954. A grande vantagem desses códigos é que eles possuem um fácil algoritmo de codificação e um eficiente algoritmo de decodificação. Por isso, são códigos bastante utilizados em diversas aplicações, tais como redes de sensores sem fio, na área de criptografia e também pela agência espacial americana NASA no envio de mensagens do espaço para a Terra.

Existem várias maneiras de se definir os códigos de Reed-Muller. Abaixo apresentamos uma definição recursiva para tais códigos. Denotaremos por $R(r,m)$ os códigos de Reed-Muller de ordem r onde $0 \leq r \leq m$ e $m \in \mathbb{N}$.

- Os códigos de Reed-Muller de ordem 0, $R(0,m)$, com $m \geqslant 0$ são definidos como:

$$R(0,0) = \{0,1\}$$

$$R(0,1) = \{00,11\}$$

$$R(0,2) = \{0000,1111\}$$

$$\vdots$$

$$R(0,m) = \{\underbrace{00\ldots0}_{2^m}, \underbrace{11\ldots1}_{2^m}\}$$

  Ou seja, os códigos $R(0,m)$ são formados por dois vetores, um só de 0's e um só de 1's, ambos de comprimento 2^m.

- Os códigos de Reed-Muller de primeira ordem, $R(1,m)$, para $m \geqslant 1$, são códigos binários definidos recursivamente por:

$$R(1,1) = \mathbb{F}_2 \times \mathbb{F}_2 = \{00,01,10,11\} = \mathbb{F}_2^2$$

$$R(1,m) = \{uu, u(u+\overline{1}) \ / \ u \in R(1,m-1), \overline{1} = \underbrace{11\ldots1}_{2^{m-1}}\}$$

  Como exemplo, vamos construir o $R(1,2)$. Observe que, de acordo com a definição acima, os elementos de $R(1,2)$ são obtidos por meio da justaposição (colocar um ao lado do outro) dos

elementos de $R(1,1)$ e também da justaposição do elemento de $R(1,1)$ com ele mesmo adicionado do vetor 1 de igual tamanho. A seguir explicitamos tal construção com os elementos 00 e 01 do $R(1,1)$:

$$\underbrace{00}_{u} \to \underbrace{00}_{u}\underbrace{00}_{u}, \ \underbrace{00}_{u}\underbrace{11}_{(u+\overline{1})}$$

$$\underbrace{01}_{u} \to \underbrace{01}_{u}\underbrace{01}_{u}, \ \underbrace{01}_{u}\underbrace{10}_{(u+\overline{1})}$$

Logo,

$$R(1,2) = \{0000, 0011, 0101, 1010, 1001, 1111, 1100, 0110\}$$

Da mesma maneira, utilizando os elementos de $R(1,2)$ e a construção acima, obtemos o $R(1,3)$:

$$R(1,3) = \begin{Bmatrix} 00000000 & 01010101 & 10101010 & 11111111 \\ 00110011 & 01100110 & 10011001 & 11001100 \\ 00001111 & 01011010 & 10100101 & 11110000 \\ 00111100 & 01101001 & 10010110 & 11000011 \end{Bmatrix}$$

e assim sucessivamente.

- Os códigos de Reed-Muller de ordem r, $R(r,m)$, com $0 \leq r \leq m$, são definidos como:

$$R(r,m) = \begin{cases} \mathbb{F}_2^{2^r} & \text{, se } \ m = r \\ u(u+v), \quad u \in R(r,m-1) \ \text{ e } \ v \in R(r-1,m-1) & \text{ , se } \ r < m \end{cases}$$

Como exemplos, vamos exibir $R(2,2)$ e $R(2,3)$:

$$R(2,2) = \mathbb{F}_2^4 = \begin{Bmatrix} 0000 & 0001 & 0010 & 0011 \\ 0100 & 0101 & 0110 & 0111 \\ 1000 & 1001 & 1010 & 1011 \\ 1100 & 1101 & 1110 & 1111 \end{Bmatrix}$$

Vamos construir agora o $R(2,3)$. Observe que os elementos de $R(2,3)$ são obtidos pela justaposição de elementos da forma u e $u+v$ onde $u \in R(2,2)$ e $v \in R(1,2)$. Portanto, para **u=0000** $\in R(2,2)$ temos as seguintes possibilidades para $\mathbf{u}(u+v)$:

$$\mathbf{0000}0000, \mathbf{0000}0011, \mathbf{0000}0101, \mathbf{0000}1010, \mathbf{0000}1001, \mathbf{0000}1111, \mathbf{0000}1100, \mathbf{0000}0110$$

Já para **u=0110** $\in R(2,2)$ temos as seguintes possibilidades para os elementos de $R(2,3)$ que são da forma $\mathbf{u}(u+v)$:

$$\mathbf{0110}0000, \mathbf{0110}0011, \mathbf{0110}0101, \mathbf{0110}1010, \mathbf{0110}1001, \mathbf{0110}1111, \mathbf{0110}1100, \mathbf{0110}0110$$

Fazendo isso com todos os elementos $u \in R(2,2)$, obtemos o código $R(2,3)$ como abaixo:

$$R(2,3) = \left\{ \begin{array}{cccccccc} 00000000 & 00000011 & 00000101 & 00001010 & 00001001 & 00001111 & 00001100 & 00000110 \\ 00010000 & 00010011 & 00010101 & 00011010 & 00011001 & 00011111 & 00011100 & 00010110 \\ 00100000 & 00100011 & 00100101 & 00101010 & 00101001 & 00101111 & 00101100 & 00100110 \\ 00110000 & 00110011 & 00110101 & 00111010 & 00111001 & 00111111 & 00111100 & 00110110 \\ 01000000 & 01000011 & 01000101 & 01001010 & 01001001 & 01001111 & 01001100 & 01000110 \\ 01010000 & 01010011 & 01010101 & 01011010 & 01011001 & 01011111 & 01011100 & 01010110 \\ 01100000 & 01100011 & 01100101 & 01101010 & 01101001 & 01101111 & 01101100 & 01100110 \\ 01110000 & 01110011 & 01110101 & 01111010 & 01111001 & 01111111 & 01111100 & 01110110 \\ 10000000 & 10000011 & 10000101 & 10001010 & 10001001 & 10001111 & 10001100 & 10000110 \\ 10010000 & 10010011 & 10010101 & 10011010 & 10011001 & 10011111 & 10011100 & 10010110 \\ 10100000 & 10100011 & 10100101 & 10101010 & 10101001 & 10101111 & 10101100 & 10100110 \\ 10110000 & 10110011 & 10110101 & 10111010 & 10111001 & 10111111 & 10111100 & 10110110 \\ 11000000 & 11000011 & 11000101 & 11001010 & 11001001 & 11001111 & 11001100 & 11000110 \\ 11010000 & 11010011 & 11010101 & 11011010 & 11011001 & 11011111 & 11011100 & 11010110 \\ 11100000 & 11100011 & 11100101 & 11101010 & 11101001 & 11101111 & 11101100 & 11100110 \\ 11110000 & 11110011 & 11110101 & 11111010 & 11111001 & 11111111 & 11111100 & 11110110 \end{array} \right\}$$

Já os elementos de $R(5,7)$ são elementos da forma $\mathbf{u}(u+v)$ onde $u \in R(5,6)$ e $v \in R(4,6)$. Portanto, com essa definição recursiva, conseguimos construir todos os códigos de Reed-Muller.

Inicialmente os códigos de Reed-Muller foram definidos somente como códigos binários. Hoje já existem generalizações desses códigos definidos sobre um corpo finito com q elementos, $q \geq 2$.

Na próxima seção, daremos ênfase aos códigos de Reed-Muller de primeira ordem, $R(1,m)$, e demonstraremos quais são os parâmetros fundamentais desses códigos.

4 Códigos de Reed-Muller de Primeira Ordem

A partir de agora, estamos interessados somente nos códigos de Reed-Muller binários de primeira ordem e suas aplicações. Lembremos que os códigos de Reed-Muller de primeira ordem, denotados por $R(1,m)$, com $m \in \mathbb{N}$ e $m \geq 1$ são definidos por:

$$R(1,1) = \{00, 01, 10, 11\} = \mathbb{F}_2^2$$

Para $m > 1$ temos a seguinte definição:

$$R(1,m) = \{uu, u(u+\overline{1}) \ / \ u \in R(1,m-1), \overline{1} = \underbrace{11\ldots1}_{2^{m-1}}\}$$

Nosso objetivo agora é calcular os parâmetros $[n, M, d]$ dos códigos de Reed-Muller de primeira ordem.

- Comprimento n

  De acordo com a definição dos Códigos de Reed-Muller de primeira ordem temos:

$$R(1,0) \subset \mathbb{F}_2^1 = \mathbb{F}_2^{2^0}$$

$$R(1,1) \subset \mathbb{F}_2^2 = \mathbb{F}_2^{2^1}$$

$$R(1,2) \subset \mathbb{F}_2^4 = \mathbb{F}_2^{2^2}$$

$$\vdots$$

$$R(1,m) = \mathbb{F}_2^{2^m}$$

  Dessa forma, segue que o comprimento de $R(1,m)$ é dado por:

$$n = 2^m.$$

- Número de elementos M

  Teorema 4.1. $|R(1,m)| = 2^{m+1}$ *que é o número de palavras de* $R(1,m)$.

  Prova. *Vamos mostrar o resultado por indução em* m.

  Para $m = 1$*, vimos que* $R(1,1) = \{00, 01, 10, 11\} = \mathbb{F}_2^2$ *donde* $|R(1,1)| = 4 = 2^{1+1}$*. Suponha então que* $|R(1,m)| = 2^{m+1}$ *(hipótese de indução). Queremos mostrar que*

$$|R(1,m+1)| = 2^{m+2}$$

Agora, $R(1,m+1) = \{uu, u(u+\overline{1}) \ / \ u \in R(1,m), \overline{1} = \underbrace{11\ldots1}_{2^m}\}$*, donde* $|R(1,m+1)| = 2.|R(1,m)| = 2.2^{m+1} = 2^{m+2}$*.* ■

Pela Observação 2.3 e usando que $|R(1,m)| = 2^{m+1}$ segue que a dimensão dos códigos de Reed-Muller de primeira ordem é $k = m+1$.

- Distância mínima d

  Vamos mostrar agora que a distância mínima do código Reed-Muller de 1ª ordem é $d = 2^{m-1}$.

  Para isso, temos que mostrar que o peso de qualquer palavra de $R(1,m)$, exceto as palavras $\bar{0} = \underbrace{000\ldots0}_{2^m}$ e $\bar{1} = \underbrace{111\ldots1}_{2^m}$ é igual a 2^{m-1}. (Observe que $w(\bar{0}) = 0$ e $w(\bar{1}) = 2^m$). Com isso, segue pela Observação 2.6 que $d = w(R(1,m)) = 2^{m-1}$.

Teorema 4.2. *Seja* $c \in R(1,m)$*,* $c \neq \bar{0} = \underbrace{000\ldots0}_{2^m}$ *e* $c \neq \bar{1} = \underbrace{111\ldots1}_{2^m}$*. Então,* $w(c) = 2^{m-1}$*.*

Prova. *Vamos mostrar novamente por indução em* m*.*

Para $m = 1$*, temos que* $R(1,1) = \{00, 01, 10, 11\}$*, donde qualquer palavra,* $c \neq \bar{0} = 00$ *e* $c \neq \bar{1} = 11$*, tem peso* $2^{1-1} = 1$*. Observe que,* 01 *e* 10*, ambas tem peso* 1*. Logo, o resultado é verdadeiro para* $m = 1$*.*

Hipótese de Indução: Em $R(1,m-1)$ *qualquer palavra,* $c \neq \bar{0} = \underbrace{000\ldots0}_{2^{m-1}}$ *e* $c \neq \bar{1} = \underbrace{111\ldots1}_{2^{m-1}}$*, tem peso* $2^{(m-1)-1} = 2^{m-2}$*.*

Observe que, em $R(1,m)$ *dizer que qualquer palavra,* $c \neq \bar{0} = \underbrace{000\ldots0}_{2^m}$ *e* $c \neq \bar{1} = \underbrace{111\ldots1}_{2^m}$*, tem peso* 2^{m-1} *equivale a dizer que ela é composta por metade* $0's$ *e metade* $1's$ *já que seu comprimento é* 2^m *e* $2^{m-1} = \frac{2^m}{2}$*.*

Seja c *uma palavra de* $R(1,m)$*,* $c \neq \bar{0} = \underbrace{000\ldots0}_{2^m}$ *e* $c \neq \bar{1} = \underbrace{111\ldots1}_{2^m}$*.*

Temos duas possibilidades:

(1) $c = u\ u, u \in R(1,m-1)$*.*

Como $c \neq \underbrace{000\ldots0}_{2^m}$ *e* $c \neq \underbrace{111\ldots1}_{2^m}$*, então,* $u \neq \underbrace{000\ldots0}_{2^{m-1}}$ *e* $u \neq \underbrace{111\ldots1}_{2^{m-1}}$*. Por hipótese de indução,* $w(u) = 2^{m-2}$*, ou seja,* u *tem* 2^{m-2} *posições iguais a* 1*. Logo,* $c = u\ u$ *terá*

$2.2^{m-2} = 2^{m-1}$ *posições iguais a* 1*. Portanto,* $w(c) = 2^{m-1}$*.*

(2) $c = u\ (u + \bar{1}), u \in R(1, m-1)$*.*

(2.1) Se $u = \underbrace{000\ldots0}_{2^{m-1}}$*, então,* $u + \bar{1} = \underbrace{111\ldots1}_{2^{m-1}}$*. Logo,*

$$c = \underbrace{000\ldots0}_{2^{m-1}}\underbrace{111\ldots1}_{2^{m-1}} \Longrightarrow w(c) = 2^{m-1}$$

.

(2.2) Se $u = \underbrace{111\ldots1}_{2^{m-1}}$*, então,* $u + \bar{1} = \underbrace{000\ldots0}_{2^{m-1}}$*. Logo,*

$$c = \underbrace{111\ldots1}_{2^{m-1}}\underbrace{000\ldots0}_{2^{m-1}} \Longrightarrow w(c) = 2^{m-1}$$

.

(2.3) Caso $u \neq \underbrace{000\ldots0}_{2^{m-1}}$ *e* $u \neq \underbrace{111\ldots1}_{2^{m-1}}$ *temos que,* $c = u\ (u + \bar{1})$*, onde* $u \in R(1, m-1)$*.*

Pela hipótese de indução, $w(u) = 2^{m-2} = \frac{2^{m-1}}{2}$*, ou seja, metade das coordenadas de* u *são iguais a zero e metade das coordenadas de* u *são iguais a* 1*. Observe que,* 0 *em* u*, vira* 1 *em* $u + \bar{1}$ *e,* 1 *em* u*, vira* 0 *em* $u + \bar{1}$*. Logo, a palavra* $u\ (u + \bar{1})$ *terá* 2.2^{m-2} *posições iguais a* 1*. Portanto,*

$$w(c) = 2^{m-1}$$

■

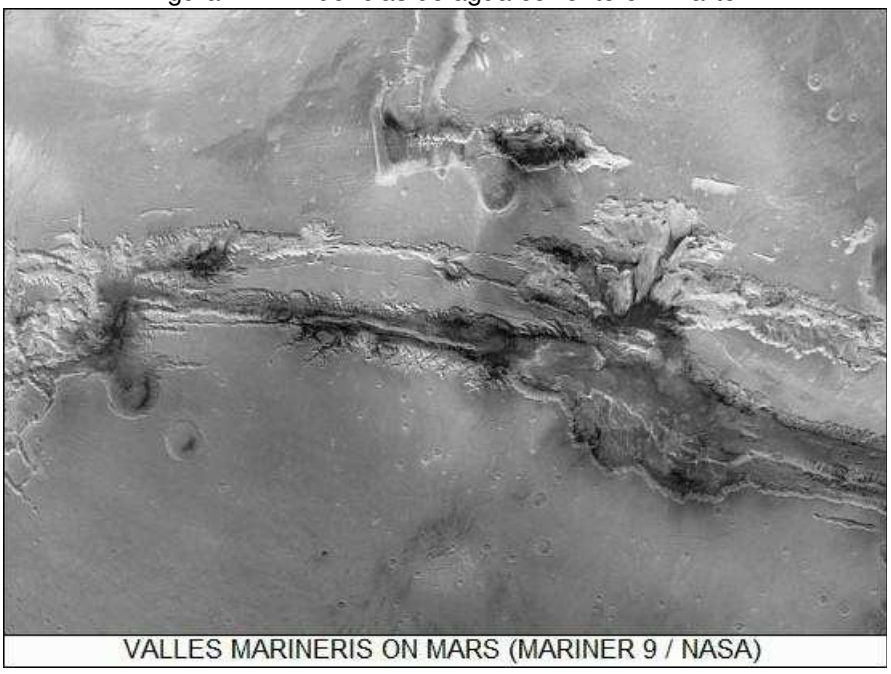
5 Aplicações

Os códigos de Reed-Muller possuem diversas aplicações, tais como redes de sensores sem fio (códigos de Reed-Muller de segunda ordem), criptografia, circuitos elétricos, concepção de algoritmos de dispersão, dentre outras. Abaixo, apresentamos um exemplo de aplicação dos códigos de Reed-Muller de primeira ordem em um programa espacial da NASA (National Aeronautics and Space Administration).

5.1 Mariner 9

Em julho de 1965, o mundo finalmente obteve algumas respostas para as muitas questões colocadas sobre aquele misterioso ponto vermelho no horizonte. Nessa data, a NASA obteve sua primeira missão vitoriosa à Marte, denominada Mariner 4, ganhando terreno histórico onde outras tentativas fracassaram ao capturar as primeiras imagens do planeta vermelho. A espaçonave histórica conseguiu registrar 21 imagens de Marte enquanto voava a uma distância de cerca de 6.000 milhas. No entanto, depois da euforia inicial com essa proeza de magia tecnológica, as fotos em si foram um pouco decepcionantes já que Marte se parecia muito com a lua e as fotos não apresentaram lagos, vulcões, vales e montanhas, como os pesquisadores esperavam. Outras missões foram lançadas após o sucesso da Mariner 4, algumas mais bem sucedidas do que outras, mas diversas descobertas foram feitas a partir da transmissão de 7329 imagens (em preto e branco) da superfície de Marte em 349 dias de órbita da missão Mariner 9. Lançada em 30 de maio de 1971, essa nave espacial registrou fotos de vulcões gigantescos, um grande cânion de 3.000 milhas de comprimento e o mais intrigante de tudo: prova de antigos leitos de rios em Marte (Figura 1).

Figura 1 – Evidências de água corrente em Marte.



Fonte: `https://www.khanacademy.org/partner-content/nasa/searchingforlife/mars-modern-exploration/a/mariner-9`. Acesso em: 29 dez. 2019.

No envio dessas imagens para a Terra, foi utilizado para detectar e corrigir os possíveis erros na transmissão desses dados enviados, o Código de Reed-Muller de primeira ordem $R(1, m)$, com

$m = 5$, ou seja, o $R(1,5)$. Conforme provado na seção anterior, os parâmetros (n, M, d) do $R(1,5)$ são:

$$n = 32 \ (2^m = 2^5)$$
$$M = 64 \ (2^{m+1} = 2^6)$$
$$d = 16 \ (2^{m-1} = 2^4)$$

Cada foto foi composta a partir de 64 tons de cinza ($M = 64$), desde o cinza mais claro (branco) até o cinza mais escuro (preto). A cada uma dessas tonalidades de cinza foi associada uma sequência binária (feita só de 0's e 1's) de comprimento igual a 6. Como é uma sequência binária de tamanho 6, temos $2^6 = 64$ possibilidades, que são exatamente os 64 tons de cinza, sendo o tom branco denotado por 000000 e o preto por 111111. Mas, como o comprimento dessas sequências (comprimento 6) é muito pequeno foi utilizado o $R(1,5)$ para transformar cada sequência dessas de 6 dígitos em uma sequência de 32 dígitos ($n = 32$), aumentando 26 dígitos em cada sequência. Dessa forma, melhora-se a detecção e correção de possíveis erros na transmissão dessas fotos para a Terra.

Assim, o código da Mariner 9 tem comprimento igual a 32, ou seja, é composto por 64 palavras de 32 dígitos cada. E, como esse código possui distância mínima igual a 16, ($d = 16$), de acordo com o Teorema 2.7, o código da Mariner 9 detecta até 15 erros ($= d-1$) e corrige até 7 erros ($=[\frac{d-1}{2}]$).

Apesar de não ser o objetivo desse texto apresentar os algoritmos de codificação e decodificação dos códigos de Reed-Muller, apresentamos abaixo, em um exemplo, como é feita a codificação com o $R(1,5)$ de uma determinada tonalidade de cinza. A codificação nos outros códigos $R(r,m)$ é feita de maneira análoga. O leitor interessado em saber mais sobre o algoritmo de codificação e decodificação do $R(1,5)$ pode consultar [2].

A codificação utilizada pelo $R(1,5)$ nada mais é do que a multiplicação da sequência original de 6 dígitos por uma matriz, denotada por $G(1,5)$. Essa matriz $G(1,5)$ possui tamanho 6 x 32 e suas linhas formam uma base para o espaço vetorial $R(1,5)$, considerando a primeira linha sempre igual ao vetor formado somente por 1's:

$$\begin{bmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{bmatrix}_{6\times 32}$$

Para exemplificar, recodificaremos a tonalidade de cinza dada por 100011. Portanto, devemos efetuar a seguinte operação

$$[100011] \, .G(1,5) = [11111111000000000000000011111111]$$

obtendo-se $11111111000000000000000011111111$ (32 dígitos), que representa a mesma tonalidade de 100011 (6 dígitos), porém com mais informações acrescentadas para possibilitar detecção e correção de um maior número de erros.

Referências

HEFEZ, A.; VILLELA, M. L. **Códigos Corretores de Erros**. 1. ed. Rio de Janeiro: IMPA, 2002.

DIAS, J. S.; CORNELISSEN, M. G. O Código da Nave Espacial Mariner 9. **Revista de Ciências Exatas e Naturais**, v. 19, n. 2, p. 168-186, 2017.