Códigos de Reed-Solomon

Renata Moura renamoura2003@yahoo.com.br
Faculdade Sete Lagoas, Sete Lagoas, MG, Brazil

Mariana Garabini Cornelissen Hoyos mariana@ufsj.edu.br
Universidade Federal de São João del Rei, Ouro Branco, MG, Brazil

Resumo

Este trabalho apresenta a versão original dos Códigos de Reed-Solomon publicada em 1960 pelos matemáticos e engenheiros Irving Stoy Reed e Gustave Solomon. Esses códigos constituem uma classe de códigos cíclicos corretores de erros e são amplamente utilizados nas tecnologias de sistemas de comunicação digitais. Em especial, apresentamos nesse trabalho os *Quick Response Codes*, mais conhecidos como *QR Codes*, que utilizam os códigos de Reed-Solomon para a detecção e correção de erros.

Palavras-chave

Códigos, Reed-Solomon, *QR Codes*.

1 Introdução

A teoria dos códigos corretores de erros estuda formas de detectar e corrigir problemas que podem ocorrer durante uma transmissão de dados. Uma dessas maneiras consiste em acrescentar dados à informação original, antes de sua transmissão, permitindo assim, ao recuperar a informação original, detectar e até mesmo corrigir alguns possíveis erros. Essa teoria teve origem por volta da metade do século passado com os trabalhos de C.E. Shannon [10], R.W. Hamming [5] e M.J.E. Golay [3].

Hoje em dia já existem diversas classes e tipos de códigos. O objetivo desse trabalho é apresentar os códigos de Reed Solomon que constituem uma classe de códigos lineares. Os códigos lineares são os códigos mais utilizados na prática e são, por definição, subespaços vetoriais de K^n, onde K é um corpo finito.

Os códigos de Reed-Solomon foram criados em 1960 pelos matemáticos e engenheiros Irving Stoy Reed $(1923-2012)$ e Gustave Solomon $(1930-1996)$. Em [8], Reed e Solomon apresentaram uma 'nova' classe de códigos 'redundantes', juntamente com seu procedimento de decodificação. Os códigos RS (Reed-Solomon)

originais possuem uma estrutura não binária, que permite o tratamento de um tipo de erro específico, denominado *rajadas de erros*. Isso fez com que esses códigos fossem utilizados no desenvolvimento do sistema brasileiro de televisão digital e também nos sistemas de comunicação móvel (*modens*, celulares e *tablets*). Além disso, esses códigos possuem a melhor distância mínima possível, possibilitando ainda mais a difusão e aplicação desse tipo de código. Desde a sua criação, esses códigos tem sido extremamente utilizados nas tecnologias de sistemas de comunicação digitais.

Em 1961, outros dois matemáticos, Daniel Gorenstein e Neal Zierler, apresentaram uma classe de códigos (não binários) que incluía, como caso particular, os códigos RS, mostrando assim que os códigos RS formam uma subclasse dos códigos conhecidos hoje como códigos BCH (Bose-Chaudhuri-Hocquenghem)[6], que são códigos cíclicos. A maneira como os códigos de Reed-Solomon são utilizados hoje em dia, não segue mais a versão original dada pelos autores em [8], objeto de estudo desse artigo, e sim uma formulação equivalente que possui um algoritmo de decodificação mais eficiente. Essa outra abordagem dos códigos RS pode ser encontrada em [4] e a equivalência entre essas duas abordagens pode ser vista em [7].

Esse artigo está estruturado da seguinte maneira: na próxima seção, citamos algumas definições e resultados que são necessárias para o entendimento e desenvolvimento desse trabalho. Na terceira seção, apresentamos a versão original dos códigos de Reed Solomon dada em [8] e na seção seguinte apresentamos como aplicação dessa teoria, a história, a estrutura e o funcionamento dos *QR Codes*.

Assumiremos nesse texto, um conhecimento básico da teoria de códigos corretores de erros que pode ser consultado, por exemplo, em [6].

2 Preliminares

Nesta seção apresentamos algumas definições e resultados que serão utilizados ao longo desse trabalho. Optamos por não apresentar nesse texto as demonstrações desses resultados e indicar uma referência para o leitor interessado.

O primeiro resultado nos fala sobre a estrutura de um corpo finito, quando

retiramos desse corpo o elemento neutro da adição.

Teorema 2.1. *([6], Teorema 5, pág. 74) Se $\mathbb{F}$ é um corpo finito (com q elementos) então existe $a \in \mathbb{F}$ tal que $\mathbb{F}^* = \{1, a, a^2, ..., a^{q-2}\}$.*

Daqui em diante, denotaremos por $\mathbb{F}_q$ o corpo finito com q elementos.

Já o próximo resultado é uma consequência do algoritmo da divisão de polinômios em $\mathbb{F}[x]$.

Teorema 2.2. *([2], Corolário 3, pág. 285) Um polinômio de grau n sobre um corpo tem no máximo n raízes, contando multiplicidade.*

Os códigos de Reed-Solomon, objeto de estudo desse trabalho, são códigos cíclicos. Apresentamos abaixo a definição de códigos cíclicos.

Definição 2.1. *Um código $\mathcal{C} \in \mathbb{F}_q^n$ diz-se cíclico se:*

(i) $\mathcal{C}$ é linear (portanto $\mathcal{C}$ é subespaço vetorial de $\mathbb{F}_q^n$);

(ii) Se $x = (x_1, x_2, ..., x_{n-1}, x_n) \in \mathcal{C}$, então $(x_n, x_1, x_2, ..., x_{n-1}) \in \mathcal{C}$.

O vetor $(x_n, x_1, x_2, ..., x_{n-1}) \in \mathbb{F}_q^n$ diz-se um desvio cíclico de $x \in \mathbb{F}_q^n$ e iremos denotá-lo por $\sigma(x)$. Portanto, um código é cíclico se é linear e se contém os desvios cíclicos de todas as palavras do código. Assim, se $\mathcal{C}$ é um código cíclico, então $\sigma^i(c) \in \mathcal{C}$ para todo $c \in \mathcal{C}$ e para todo $i \in \mathbb{N}$.

Códigos (lineares) interessantes são aqueles nos quais a dimensão e a distância mínima são grandes relativamente ao comprimento do código. Um dos problemas fundamentais na Teoria de Códigos Corretores de Erros é estudar a dependência entre esses três parâmetros de um código (comprimento, dimensão e distância mínima). Abaixo apresentamos uma relação já verificada entre esses parâmetros, conhecida como *Cota de Singleton*.

Teorema 2.3. *([6], Corolário, pág. 180) Os parâmetros (n, k, d) sendo $n =$ comprimento, $k =$ dimensão e $d =$ distância mínima de um código linear satisfazem a desigualdade*

$$d \leq n - k + 1.$$

Um código será chamado MDS (*Maximum Distance Separable*) se valer a igualdade

$$d = n - k + 1.$$

Definição 2.2. *Uma matriz V quadrada de ordem $n \geq 2$ cujas as linhas estão em progressão geométrica e as entradas da primeira coluna são iguais ao número real 1 é chamada de matriz de Vandermonde.*

Uma matriz de Vandermonde de ordem n tem a forma geral:

$$V = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}$$

Observe que $V_{ij} = \alpha_i^{j-1}$, para todos os índices $i = 1, 2, \cdots, n$ e $j = 1, 2, \cdots, n-1$.

Proposição 2.1. *([9], Teorema, pág. 36) O determinante de uma matriz de Vandermonde de ordem n é dado por:*

$$|V| = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$$

Para finalizar essa seção, apresentamos o resultado abaixo que será utilizado na transformação dos códigos de Reed Solomon em códigos binários.

Teorema 2.4. *([2], Teorema 20.3, pág. 346) Sejam F um corpo e $p(x)$ um polinômio irredutível em $F[x]$. Se a é uma raiz de $p(x)$ em alguma extensão E de F, então*

$$F(a) \simeq \frac{F[x]}{\langle p(x) \rangle}$$

Além disso, se $p(x)$ tem grau n, então todo elemento de $F(a)$ pode ser escrito, de maneira única, como

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + ... + c_1a + c_0,$$

em que $c_0, c_1, ..., c_{n-1} \in F$.

Com essas definições e resultados, estamos prontos para entender a versão original dos códigos de Reed-Solomon, assunto da próxima seção.

3 Os Códigos de Reed-Solomon

Nesta seção apresentamos a definição e algumas propriedades dos códigos introduzidos por Reed e Solomon em 1960.

Seja K um corpo que é uma extensão de grau n sobre $\mathbb{Z}_2$. Sabemos pelo Teorema 2.1 que K^* é um grupo multiplicativo cíclico de cardinalidade $2^n - 1$. Seja β um gerador desse grupo e considere a seguinte aplicação para $m \in \mathbb{N}, m < 2^n$:

$$E : K^m \to K^{2^n}$$

$$(a_0, a_1, \ldots, a_{m-1}) \longmapsto (P(0), P(\beta), \ldots, P(\beta^{2^n-2}), P(1))$$

onde P é o polinômio $P(x) = a_0 + a_1x + ... + a_{m-1}x^{m-1} \in K[x]$ associado ao elemento $(a_0, a_1, \ldots, a_{m-1}) \in K^m$.

Observe que a aplicação E acima transforma uma m-upla em uma 2^n-upla, onde $2^n > m$. Vamos mostrar abaixo que a imagem dessa aplicação E é a codificação que queremos.

Proposição 3.1. *A aplicação E satisfaz as seguintes propriedades:*

(i) E é uma aplicação linear;

(ii) E é injetora.

Demonstração:

(i) Sejam $a = (a_0, a_1, ..., a_{m-1})$ e $b = (b_0, b_1, ..., b_{m-1}) \in K^m$ e considere os

polinômios em $K[x]$ dados por:

$$P_a(x) = a_0 + a_1x + ... + a_{m-1}x^{m-1}$$

$$P_b(x) = b_0 + b_1x + ... + b_{m-1}x^{m-1}$$

$$P(x) = P_a(x) + P_b(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_{m-1} + b_{m-1})x^{m-1}$$

Por definição da aplicação E, temos que:

$$E(a+b) = E(a_0+b_0, a_1+b_1, ..., a_{m-1}+b_{m-1}) = (P(0), P(\beta), ..., P(\beta^{2^n-2}), P(1))$$

Logo,

$$E(a + b) = (P_a(0) + P_b(0), P_a(\beta) + P_b(\beta), ..., P_a(1) + P_b(1))$$

$$E(a + b) = (P_a(0), P_a(\beta), ..., P_a(1)) + (P_b(0), P_b(\beta), ..., P_b(1))$$

donde

$$E(a + b) = E(a) + E(b)$$

Sejam $\lambda \in K$ e $P_\lambda(x) = \lambda a_0 + \lambda a_1 x + \cdots + \lambda a_{m-1}x^{m-1}$ o polinômio em $K[x]$ associado à $\lambda a = (\lambda a_0, \lambda a_1, ..., \lambda a_{m-1})$. Observe que

$$P_\lambda(x) = \lambda P_a(x)$$

onde $P(x)$ é o polinômio associado à $(a_0, a_1, \cdots, a_{m-1})$. Logo, $E(\lambda a) = \lambda E(a)\ \forall \lambda \in K, a \in K^m$, mostrando assim que E é uma aplicação linear.

(ii) Vamos mostrar agora que E é injetora. De fato,

$$KerE = \{a = (a_0, a_1, ..., a_{m-1}) \in K^m | E(a) = 0\}$$

Mas,

$$E(a) = (P(0), P(\beta), \ldots, P(\beta^{2^n-2}), P(1)) = 0 \Leftrightarrow P(0) = P(\beta) = \cdots = P(1) = 0$$

Como todos os 2^n elementos do conjunto $\{0, 1, \beta, \beta^2, \cdots, \beta^{2^n-2}\}$ são distintos e $m < 2^n$, segue pelo Teorema 2.2 que o polinômio P é o polinômio nulo, ou seja, $a = (0, 0, \cdots, 0)$. Logo, $Ker(E) = \{0\}$ e E é injetora, como queríamos mostrar.

□

Com o resultado acima, sabemos que a imagem da aplicação E é um subespaço vetorial de K^{2^n} denominado *Código de Reed-Solomon* e que será denotado por $\mathcal{C} = Im(E)$.

Veremos agora quais são os parâmetros principais (comprimento, dimensão, número de elementos e distância mínima) desse código.

Proposição 3.2. *O comprimento do código $\mathcal{C}$ é igual a 2^n.*

Demonstração: Como o código $\mathcal{C}$ é a imagem da aplicação linear E, temos que $\mathcal{C} \subset K^{2^n}$ donde podemos concluir que o comprimento das palavras nesse código é igual a 2^n, ou seja, cada palavra desse código possui 2^n símbolos. □

Como $\mathcal{C}$ é um código linear, podemos calcular sua dimensão, que nada mais é do que a dimensão de $\mathcal{C}$ como espaço vetorial.

Proposição 3.3. *A dimensão de $\mathcal{C}$ é igual a m.*

Demonstração: Sabemos que toda aplicação linear leva base em base e sabemos também que a base de K^m possui m elementos, ou seja, K^m é um espaço vetorial de dimensão m sobre K. Logo, o código $\mathcal{C} = Im(E)$ também possui uma base com m elementos, isto é, sua dimensão é igual a m. □

Com isso, conseguimos facilmente contar quantos elementos (quantas palavras) $\mathcal{C}$ possui.

Proposição 3.4. *A cardinalidade de $\mathcal{C}$ é igual a 2^{nm}.*

Demonstração: Denotaremos por $|\mathcal{C}|$ a cardinalidade desse código. Como vimos acima que $\mathcal{C}$ possui uma base com m elementos, suponha que $\{v_1, v_2, \ldots, v_m\}$ seja uma base para $\mathcal{C}$. Dessa forma, sabemos que todo elemento $c \in \mathcal{C}$ se escreve como:

$$c = a_1v_1 + a_2v_2 + \ldots + a_mv_m$$

com $a_1, a_2, \ldots, a_m \in K$.

Como a cardinalidade de K é igual a 2^n, temos 2^n possibilidades para a_1, 2^n possibilidades para a_2 e assim por diante. Ou seja, temos 2^n possibilidades para qualquer a_i, $i = 1, 2, \ldots, m$. Logo, o número de elementos de $\mathcal{C}$ será:

$$|\mathcal{C}| = (2^n)^m = 2^{nm}$$

□

E, para finalizar, calcularemos a distância mínima de $\mathcal{C}$.

Proposição 3.5. *A distância mínima de $\mathcal{C}$ é igual a $2^n - m + 1$.*

Demonstração: Como o código $\mathcal{C}$ é um código linear, sabemos que sua distância mínima é igual ao seu peso mínimo. Portanto, vamos calcular o peso mínimo de $\mathcal{C}$. Seja $c \in \mathcal{C}$ uma palavra não nula do código $\mathcal{C}$:

$$c = (P(0), P(\beta), \ldots, P(\beta^{2^n-2}), P(1))$$

e seja $w(c)$ o peso dessa palavra c, isto é, o número de posições não nulas de c. Como c tem comprimento igual a 2^n então $w(c) = 2^n -$ (número de posições nulas). Agora, como $P(x)$ é um polinômio de grau menor ou igual $m - 1$ então o número de posições nulas de c é, no máximo, $m - 1$. Logo,

$$w(c) \geq 2^n - (m - 1) = 2^n - m + 1$$

para toda palavra $c \in \mathcal{C}$. Assim, temos que a distância mínima d desse código

satisfaz

$$d \geq 2^n - m + 1$$

Por outro lado, sabemos pelo Teorema 2.3 que

$$d \leq 2^n - m + 1$$

Dessa forma, temos

$$d = 2^n - m + 1$$

o que implica que, os códigos de Reed-Solomon são códigos do tipo MDS (*Maximum Distance Separable*), ou seja, possuem a maior distância mínima possível. □

Observe que, ao receber a mensagem $(P(0), P(\beta), \ldots, P(\beta^{2^n-2}), P(1))$, para decodificar, teremos que resolver quaisquer m das 2^n equações do sistema linear abaixo, nas variáveis $a_0, a_1, \ldots, a_{m-1}$ (lembre-se que $m < 2^n$).

$$\begin{cases} P(0) = a_0 \\ P(\beta) = a_0 + a_1\beta + a_2\beta^2 + ... + a_{m-1}\beta^{m-1} \\ \vdots \\ P(\beta^{2^n-2}) = a_0 + a_1\beta^{2^n-2} + a_2\beta^{2^{n+1}-2^2} + ... + a_{m-1}\beta^{(2^n-2)(m-1)} \\ P(1) = a_0 + a_1 + a_2 + ... + a_{m-1} \end{cases}$$

Note que, se considerarmos quaisquer m equações do sistema acima, por exemplo, se considerarmos m elementos quaisquer, digamos, $\alpha_1, \alpha_2, \cdots, \alpha_m$, do conjunto $K = \{0, \beta, \beta^2, \cdots, \beta^{2^n-2}, 1\}$, temos o seguinte sistema linear:

$$\begin{cases} P(\alpha_1) = a_0 + a_1\alpha_1 + a_2\alpha_1^2 + \cdots + a_{m-1}\alpha_1^{m-1} \\ P(\alpha_2) = a_0 + a_1\alpha_2 + a_2\alpha_2^2 + \cdots + a_{m-1}\alpha_2^{m-1} \\ \vdots \\ P(\alpha_m) = a_0 + a_1\alpha_m + a_2\alpha_m^2 + \cdots + a_{m-1}\alpha_m^{m-1} \end{cases}$$

A matriz dos coeficientes desse sistema é a matriz abaixo

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{m-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \cdots & \alpha_m^{m-1} \end{vmatrix}$$

que é uma matriz de *Vandermonde*. De acordo com a Proposição 2.1, seu determinante é igual a:

$$\prod_{j<i}(\alpha_i - \alpha_j)$$

Como estamos sobre $\mathbb{Z}_2$, esse determinante se torna:

$$\prod_{j<i}(\alpha_i + \alpha_j)$$

E, como os $\alpha_i's$, $i = 1, 2, \cdots, m$ são todos distintos, segue que esse determinante é não nulo e o sistema linear tem solução única. Dessa forma, caso não haja erros durante a transmissão da mensagem, temos $\binom{2^n}{m}$ maneiras de se encontrar a mensagem original $(a_0, a_1, \cdots, a_m)$. Agora, qualquer erro que ocorra durante essa transmissão irá afetar a unanimidade dos valores obtidos para os a_i's.

Uma correspondência natural pode ser estabelecida entre os elementos do corpo K e uma certa sequência binária de comprimento n. Com isso, o código E pode ser considerado como uma aplicação de sequências binárias de tamanho mn em sequências binárias de tamanho $n2^n$ e se transforma em um código corretor de erros de sequências binárias. Vejamos abaixo uma maneira de fazer essa identificação.

De acordo com o Teorema 2.4, temos que

$$\mathbb{Z}_2(\alpha) \simeq \frac{\mathbb{Z}_2[x]}{\langle f(x) \rangle}$$

onde $f(x)$ é um polinômio irredutível de grau n.

Dessa forma, podemos identificar os elementos de $K = \mathbb{Z}_2(\alpha)$ com os coeficientes de um polinômio de grau menor ou igual a $n-1$:

$$k \in K = \mathbb{Z}_2(\alpha) \longleftrightarrow c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \text{ mod } f(x) \longleftrightarrow (c_0, c_1, \cdots, c_{n-1}) \in \mathbb{Z}_2^n$$

Para encerrar essa seção, apresentamos um exemplo de um código de Reed Solomon com $m = n = 3$.

Exemplo 3.1. *Considere $K = \mathbb{Z}_2(\alpha)$ uma extensão de grau $n = 3$ sobre $\mathbb{Z}_2$ de base $\{1, \alpha, \alpha^2\}$ com α raiz de $f(x) = x^3 + x + 1$. Temos que $|K| = 2^n = 2^3 = 8$ e podemos considerar $K^* = \langle\alpha\rangle = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. Observe que $\alpha^7 = 1$ e $\alpha^3 = \alpha + 1$.*

Seja E a aplicação dada por:

$$E : K^3 \to K^{2^3} = K^8$$

$$(b_0, b_1, b_2) \mapsto (P(0), P(\alpha), P(\alpha^2), ..., P(\alpha^6), P(1))$$

onde $P(x) = b_0 + b_1 x + b_2 x^2$.

A aplicação E acima é um código de Reed Solomon que possui $(2^3)^3 = 512$ palavras de comprimento $2^3 = 8$ e distância mínima igual a $d = 2^n - m + 1 = 2^3 - 3 + 1 = 6$. Portanto, esse código detecta até 5 erros e corrige até 2 erros.

Vamos calcular, por exemplo, a codificação da mensagem $(0, \alpha, \alpha^3) \in K^3$ pelo código E acima.

$$(0, \alpha, \alpha^3) \mapsto (P(0), P(\alpha), P(\alpha^2), ..., P(\alpha^6), P(1))$$

onde $P(x) = 0 + \alpha x + \alpha^3 x^2 = \alpha x + (\alpha + 1)x^2$

Observe que, como $\alpha^3 = \alpha + 1$, segue que:

$$\alpha^4 = \alpha^3.\alpha = (\alpha+1).\alpha = \alpha^2 + \alpha$$

$$\alpha^5 = \alpha^4.\alpha = (\alpha^2+\alpha).\alpha = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$$

$$\alpha^6 = \alpha^5.\alpha = (\alpha^2+\alpha+1).\alpha = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1$$

$$\alpha^7 = \alpha^6.\alpha = (\alpha^2+1).\alpha = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1$$

Assim, com as informações obtidas acima, temos:

$$P(0) = 0$$

$$P(1) = \alpha.1 + (\alpha+1).1 = 1$$

$$P(\alpha) = \alpha.\alpha + (\alpha+1)\alpha^2 = \alpha^2 + \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 + \alpha^2 = \alpha + 1$$

$$P(\alpha^2) = \alpha.\alpha^2 + (\alpha+1)(\alpha^2)^2 = \alpha^3 + \alpha^5 + \alpha^4 = \alpha + 1 + \alpha^2 + \alpha + 1 + \alpha^2 + \alpha = \alpha$$

$$P(\alpha^3) = \alpha.\alpha^3 + (\alpha+1)(\alpha^3)^2 = \alpha^4 + \alpha^7 + \alpha^6 = \alpha^2 + \alpha + 1 + \alpha^2 + 1 = \alpha$$

$$P(\alpha^4) = \alpha.\alpha^4 + (\alpha+1)(\alpha^4)^2 = \alpha^5 + \alpha^9 + \alpha^8 = \alpha^2 + \alpha + 1 + \alpha^2 + \alpha = 1$$

$$P(\alpha^5) = \alpha.\alpha^5 + (\alpha+1)(\alpha^5)^2 = \alpha^6 + \alpha^{11} + \alpha^{10} = \alpha^2 + 1 + \alpha^2 + 1 + \alpha + 1 = \alpha + 1$$

$$P(\alpha^6) = \alpha.\alpha^6 + (\alpha+1)(\alpha^6)^2 = \alpha^7 + \alpha^{13} + \alpha^{12} = 1 + \alpha^2 + 1 + \alpha^2 + 1 + \alpha + 1 = \alpha + 1$$

Logo,

$$E(0, \alpha, \alpha^3) = (0, \alpha+1, \alpha, \alpha, 1, 0, \alpha+1, 1)$$

$$\underbrace{(0, \alpha, \alpha^3)}_{3} \mapsto \underbrace{(0, \alpha+1, \alpha, \alpha, 1, 0, \alpha+1, 1)}_{8}$$

Transformando para sequências binárias:

$$K = \mathbb{Z}_2(\alpha) \simeq \frac{\mathbb{Z}_2(x)}{< x^3 + x + 1 >} = \{c_0 + c_1 x + c_2 x^2 + < x^3 + x + 1 > | c_i \in \mathbb{Z}_2\}$$

$$0 \longleftrightarrow 0 + 0x + 0x^2 \longleftrightarrow 000$$

$$\alpha \longleftrightarrow 0 + 1x + 0x^2 \longleftrightarrow 010$$

$$\alpha^3 \longleftrightarrow 1 + 1x + 0x^2 \longleftrightarrow 110$$

Assim,

$$(000, 010, 110) \mapsto (000, 110, 010, 010, 100, 000, 110, 100)$$

$$\underbrace{000010110}_{9} \mapsto \underbrace{000110010010100000110100}_{24}$$

vemos que uma sequência binária de 9 dígitos é codificada em uma sequência binária de 24 dígitos.

Na próxima seção, veremos uma utilização prática desses códigos.

4 *QR Codes*

Os *QR Codes* ou códigos QR surgiram em 1994 no Japão e foram criados pela empresa *Denso-Wave*, uma empresa do grupo Toyota, responsável por produzir produtos de identificação automática como leitores de códigos de barras e produtos relacionados. O nome *QR Code* corresponde às letras iniciais das palavras em inglês, *Quick Response Code*, e pode ser traduzido como Código de Resposta Rápida, nome dado pelo fato da empresa ter criado um código de leitura de alta velocidade.

Em 2002 com o avanço da tecnologia dos celulares que começaram a ser comercializados, facilitou-se a leitura dos *QR Codes* através dos celulares e o uso desse tipo de código se generalizou no Japão. Atualmente os *QR Codes* são amplamente utilizados em todo o mundo e em diversas ações, tais como: identificação de objetos, informações de empresas, direcionamento para pagamentos, cardápios de restaurantes, identificação em aeroportos, etc. Uma das aplicabilidades dos *QR Codes* é que eles dispensam a necessidade de digitar endereços da internet levando

o usuário direto à informação desejada, bastando para isso apontar a câmera do celular para o *QR Codes*.

Apesar da *Denso Wave* deter todos os direitos de patente sobre os *QR Codes*, a empresa dispensou qualquer tipo de cobrança na utilização dos mesmos para que eles fossem difundidos por todo o mundo. Toda normatização para a criação dos *QR Codes* está descrita em ISO/IEC 18004: 2015 [11].

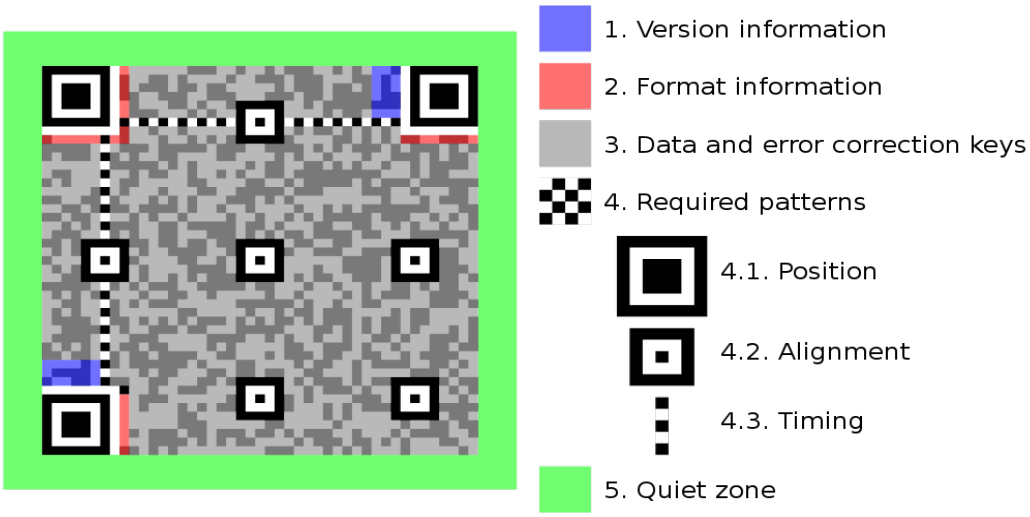
Os *QR Codes* são códigos de barras bidimensionais, pois conseguem armazenar informações tanto na horizontal como na vertical, possuindo assim uma capacidade de armazenamento de informações muito maior que os códigos de barras unidimensionais, que armazenam informações somente na horizontal. Uma grande vantagem é que os *QR Codes* podem ser lidos em qualquer direção e aceitam quatro tipos diferentes de caracteres: o numérico, o alfanumérico, binário/byte e o kanji/kana (caracteres da língua japonesa).

As informações em um *QR Code* são armazenadas em blocos, formando um mosaico como na figura abaixo:

Existem 40 versões de *QR Codes*, de diversos tamanhos, que diferem entre si na quantidade de informação armazenada. A versão de 177×177 módulos é a versão atual com maior capacidade de armazenamento: 7089 caracteres numéricos, 4296 alfanuméricos, 2953 binários/byte e 1817 kanji/kana.

Todos os *QR Codes* possuem uma estrutura comum, localizada em determinada região do mosaico e que possui uma funcionalidade específica. Na figura 3, mostramos quais são essas estruturas comuns e abaixo explicamos suas funcionalidades.

(a) Versão 21×21 (b) Versão 57×57 (c)Versão 177×177



1 - Informações sobre a versão: estes marcadores indicam qual é a versão do *QR Code*.

2 - Informações de formato: contém informações sobre o nível de correção de erros e a máscara de codificação usada.

3 - Dados e chaves de correção de erros: espaço onde são armazenados todos os dados da informação que será compartilhada, assim como os bits de redundância do Código de Reed-Solomon.

4 - Padrões requeridos:

4.1 - Padrão de posição: padrões de detecção de posição que permitem o scanner reconhecer e ler o *QR Codes* rapidamente.

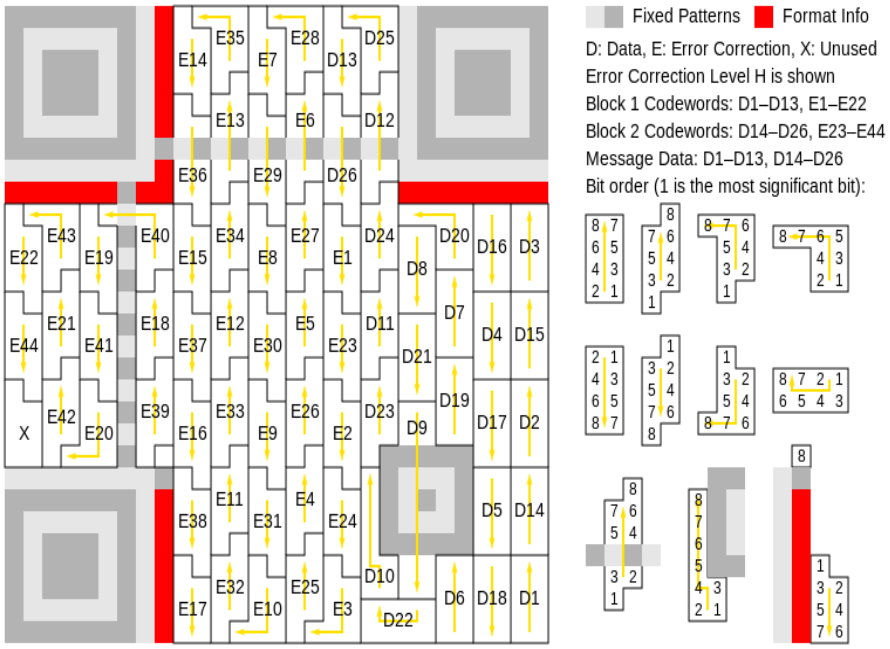
4.2 - Padrão de alinhamento: usados para corrigir a distorção dos *QR Codes* em superfícies curvas. O tamanho e a quantidade de marcadores de alinhamento

podem variar de acordo com o volume de informações armazenadas no código.

4.3 - Padrão de cronometragem: auxiliam na percepção do posicionamentodas linhas e colunas e também ajudam a determinar a dimensão do símbolo.

5 - Margens ou zona quieta: as margens brancas (na figura estão destacadas na cor verde) em volta do *QR Code* são necessárias para que o software de escaneamento possa identificar bem o limite do *QR Code* e de seus arredores.

Os *QR Codes* utilizam os códigos de Reed-Solomon para codificar as informações que são armazenadas com o intuito de detectar e recuperar possíveis erros de leitura. As informações são armazenadas em blocos organizados em forma de um *zig-zag*, como pode ser visto na Figura 4. Observe que os blocos iniciados com a letra D são blocos que contem dados relativos à mensagem armazenada e os blocos iniciados com a letra E são blocos que contem dados que são acrescidos à mensagem original, ou seja, a informação adicionada pela codificação, responsável pelo sistema de prevenção, detecção e correção de erros.



Existem quatro níveis de correção de erros (L - LOW (baixo), M - MEDIUM (médio), Q - QUARTIL (quartil) e H - HIGH (alto)) e quanto maior o nível, melhor

é a capacidade de correção do código. Entretanto, a capacidade de correção é inversamente proporcional à capacidade de armazenamento do código.

Na tabela 1 estão representados os níveis de correção de erros com as suas respectivas capacidades de correção. Por exemplo, no nível L, até 7% das informações podem ser restauradas.

Nível	Correção aproximada em porcentagem
L(médio)	7
M(médio)	15
Q (quartil)	25
H (alto)	30

Para saber qual o nível de correção adequado de acordo com a quantidade de caracteres que serão utilizados basta consultar [1].

5 Considerações Finais

Apesar desse artigo tratar de um tema, códigos corretores de erros, que não é abordado no Ensino Básico, entendemos que esse trabalho pode ser útil para professores de matemática que atuam tanto no Ensino Fundamental quanto no Ensino Médio por diversos motivos. Primeiro, porque permite ao professor aprofundar seu conhecimento, se apropriando de um conteúdo matemático novo. Além disso, esse artigo contribui para que o professor enriqueça suas aulas apresentando para os alunos uma aplicação da matemática em uma tecnologia muito utilizada por eles no dia a dia (os *QR Codes*). E, por fim, para o entendimento dos códigos de Reed Solomon, assunto desse trabalho, foram utilizados conceitos e resultados de álgebra que são trabalhados no 2^0 e 3^0 ano do Ensino Médio como Sistemas Lineares, Matrizes e Determinantes e Polinômios. Dessa forma, o professor ao ler esse artigo estará revisitando tais conteúdos, aperfeiçoando os conhecimentos necessários à sua atividade profissional, assegurando assim um ensino de melhor qualidade aos educandos.

Referências

[1] Error correction feature. https://www.qrcode.com/en/about/error-correction.html. Accessed: 2021-01-20.

[2] Joseph A Gallian. Contemporary abstract algebra 4-th edition, 1998.

[3] Marcel JE Golay. Notes on digital coding. *Proc. IEEE*, 37:657, 1949.

[4] Daniel Gorenstein and Neal Zierler. A class of error-correcting codes in pˆm symbols. *Journal of the Society for Industrial and Applied Mathematics*, 9(2):207–214, 1961.

[5] Richard W Hamming. Error detecting and error correcting codes. *The Bell system technical journal*, 29(2):147–160, 1950.

[6] Abramo Hefez and Maria Lúcia T Villela. *Códigos corretores de erros*. Instituto de Matemática Pura e Aplicada, 2008.

[7] Todd K Moon. *Error correction coding: Mathematical methods and algorithms*. John Wiley & Sons, 2020.

[8] Irving S Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.

[9] Marcos Savitraz et al. Determinante de algumas matrizes especiais. 2015.

[10] Claude E Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, 1948.

[11] D Wave. Information technology automatic identification and data capture techniques qr code bar code symbology specification. *International Organization for Standardization, ISO/IEC*, 18004, 2015.