UNIVERSIDADE FEDERAL DE ALFENAS

Bianca Lapa Ribeiro

Caracterização Algébrica de Códigos Reed-Solomon

Alfenas/MG

2023

Bianca Lapa Ribeiro

Caracterização Algébrica de Códigos Reed-Solomon

Trabalho de Conclusão de Curso apresentado como parte dos requisitos para obtenção do título de Licenciada em Matemática pelo Instituto de Ciências Exatas da Universidade Federal de Alfenas. Área de concentração: Matemática Aplicada. Orientador: Anderson José de Oliveira.

Alfenas/MG

2023

Bianca Lapa Ribeiro

Caracterização Algébrica de Códigos Reed-Solomon

A Banca examinadora abaixo-assinada, aprova a Monografia apresentada como parte dos requisitos para obtenção do título de Licenciada em Matemática pelo Instituto de Ciências Exatas da Universidade Federal de Alfenas. Área de concentração: Matemática Aplicada.

Aprovado em: 01 / 02 /2023

Banca Examinadora:

Prof. Dr. Anderson José de Oliveira
Instituto de Ciências Exatas
Orientador

Prof. Dr. Evandro Monteiro
Instituto de Ciências Exatas
Avaliador 1

Profa. Dra. Cátia Regina de Oliveira Quilles Queiroz
Instituto de Ciências Exatas
Avaliador 2

Profa. Dra. Angela Leite Moreno
Instituto de Ciências Exatas
Suplente

Os sonhos são como uma bússola, indicando os caminhos que seguiremos e as metas que queremos alcançar. São eles que nos impulsionam, nos fortalecem e nos permitem crescer.

Augusto Cury

Agradecimentos

Primeiramente, agradeço a Deus, pois Ele foi essencial em todas as minhas conquistas e superações, permitindo que tudo isso acontecesse.

À Universidade Federal de Alfenas (UNIFAL-MG), pela oportunidade de fazer o curso.

Aos professores que me acompanharam ao longo do curso e que, com empenho, se dedicam à arte de ensinar.

Aos membros da banca examinadora, pelo interesse e disponibilidade.

Em especial, ao Prof. Dr. Anderson José de Oliveira, por ter me orientado e acompanhado no desenvolvimento deste trabalho, sem medir esforços e com uma dedicação inabalável. Minha eterna gratidão pelo compartilhamento de seu conhecimento e tempo, bem como sua amizade.

À minha família, pelo amor, esforço, incentivo e apoio incondicional que me ajudaram na conclusão do meu curso e começo de uma nova carreira.

Às amizades construídas durante o curso que fizeram parte da minha formação e que proporcionaram momentos incríveis, apoiando e aconselhando nos momentos difíceis, de desânimo e cansaço.

A todos que direta ou indiretamente fizeram parte de minha formação.

Resumo

Os códigos corretores de erros (CCE's) são importantes no processo de detecção e correção de erros que podem ocorrer em situações envolvendo a transmissão e o armazenamento de informações. Os códigos BCH (Bose, Chaudhuri e Hocquenghen) representam uma importante classe dos CCE's e possuem simplicidade nos processos de codificação e decodificação. Uma importante subclasse desses códigos BCH são os chamados códigos Reed-Solomon (RS), que são códigos q-ários que possuem forte estrutura algébrica em seu processo de construção e são utilizados em diversos sistemas de armazenamento e transmissão de dados, como por exemplo em CD's e discos rígidos, além de possuírem uma notável capacidade de correção de erros. O objetivo deste trabalho é apresentar as características principais do processo de codificação e decodificação dos códigos RS, além de analisar a importância das estruturas algébricas em seu processo de construção. A metodologia adotada baseia-se em uma natureza qualitativa e quantitativa, uma vez que será realizada uma revisão de literatura sobre o assunto e efetuados diversos cálculos. Por meio dos estudos realizados, é possível compreender a importância e influência da álgebra no processo de construção dos códigos Reed-Solomon.

Palavras-chave: Álgebra. Códigos Corretores de Erros. Códigos BCH.

Abstract

Error correcting codes (ECC's) are important in the process of detecting and correcting errors that may occur in situations involving the transmission and storage of information. The BCH codes (Bose, Chaudhuri and Hocquenghen) represent an important class of ECC's and have simplicity in the encoding and decoding processes. An important subclass of these BCH codes are the so-called Reed-Solomon (RS) codes, which are q-ary codes that have a strong algebraic structure in their construction process and are used in various data storage and transmission systems, such as example on CD's and hard disks, in addition to have a notable error correction capacity. The aim of this work is to present the main characteristics of the encoding and decoding process of RS codes, in addition to analyzing the importance of algebraic structures in their construction process. The methodology is based on a qualitative and quantitative nature, since a literature review on the subject will be carried out and several calculations will be carried out. Through the realized studies, it is possible to understand the importance and influence of algebra in the construction process of the Reed-Solomon codes.

Keywords: Algebra. Error Correcting Codes. BCH codes.

Lista de ilustrações

Sumário

1 *Introdução*

Os códigos corretores de erros (CCE's) possuem a capacidade de detectar e corrigir erros que podem surgir durante os processos de transmissão e armazenamento de informações em um sistema de comunicação. Existem vários tipos de códigos corretores de erros e dentre esses tipos, os códigos BCH (Bose, Chaudhuri and Hocquenghen), uma importante classe de códigos cíclicos, possuem algumas facilidades nos processos de codificação e decodificação. Uma subclasse dos códigos BCH são os códigos Reed-Solomon (RS), os quais são códigos q-ários que possuem forte estrutura algébrica em seu processo de construção e utilizados em diversas situações, possuindo uma notável capacidade de correção de erros, [1].

Em [2] são apresentadas duas construções dos códigos Reed-Solomon, a original, como a imagem de uma função polinomial, e a descoberta por Gorenstein e Ziegler por um polinômio gerador, além de apresentar o algoritmo Shiozaki-Gao para a decodificação de palavras-código dos códigos Reed-Solomon, codificadas de maneira não sistemática.

Uma importante aplicação é apresentada em [3], na qual é utilizada a codificação Reed-Solomon/Digital Fountain (RS/DF), projetada a fim de garantir a recuperação total dos dados de telemetria de um foguete de sondagem em um vôo balístico suborbital, onde existe ruído no canal percorrido pelo foguete. Nesse sentido, a codificação RS/DF realiza a concatenação entre as codificações Reed-Solomon e Digital Fountain para corrigir e recuperar os dados corrompidos/apagados pelo canal.

De acordo com [4], [5] e [6], pode-se perceber os parâmetros e a eficiência de correção de erros em rajada de códigos Reed-Solomon utilizados em aplicações práticas de telecomunicações, visto que esses códigos são amplamente aplicados em comunicações digitais e sistemas de armazenamento em massa para corrigir erros de rajada associados a defeitos de mídia.

Pode-se perceber também a aplicação de códigos corretores de erros na transmissão e armazenamento de informações genéticas, verificando a existência de uma estrutura matemática relacionada com a estrutura do DNA, em que as sequências podem ser identificadas e reproduzidas como palavras-código de códigos corretores de erros sobre extensões de Galois. Em particular, em [7] é apresentada a reprodução de uma sequência de DNA relacionada à proteína mitocondrial ATP6, por meio dos códigos BCH, a fim de identificar onde ocorre a troca de nucleotídeo (mutação) e como essa alteração pode modificar a arquitetura biológica dessa sequência acarretando, por exemplo, algumas doenças.

O objetivo deste trabalho é apresentar os processos de codificação e de decodificação

de códigos Reed-Solomon (RS), além de analisar a importância das estruturas algébricas em seu processo de construção.

Este trabalho está estruturado da seguinte forma: no Capítulo 2 serão apresentados os principais conceitos teóricos utilizados no decorrer deste trabalho. Tais conceitos envolvem as estruturas algébricas de grupos, anéis, corpos e extensões de corpos, elementos de um sistema de comunicação, códigos corretores de erros (CCE's), códigos BCH (Bose, Chaudhuri e Hocquenghen) e os códigos Reed-Solomon (RS).

No Capítulo 3 será apresentado um detalhamento algébrico do processo de codificação, em particular, na forma sistemática e com registradores de deslocamento de $(n-k)$ estágios, além do processo de decodificação de códigos Reed-Solomon, com os principais elementos teóricos e a apresentação de exemplos envolvendo o código RS$(7,3)$.

No Capítulo 4 será apresentada a análise de um exemplo envolvendo os códigos Reed-Solomon, que tem a finalidade, por meio de sua resolução detalhada, de apresentar os conceitos teóricos apresentados no Capítulo 3, além das principais contribuições das estruturas algébricas no processo de construção dos códigos Reed-Solomon.

Por fim, no Capítulo 5 serão apresentadas as Considerações Finais deste estudo.

2 *Referencial teórico*

Neste capítulo serão apresentados os principais conceitos teóricos utilizados no decorrer deste trabalho. As referências utilizadas foram [1], [2], [3], [4], [5], [6], [7], [8] e [9].

2.1 Estruturas Algébricas

Nesta seção serão apresentados os conceitos fundamentais das estruturas algébricas de grupos, anéis, corpos e extensões de corpos. As referências utilizadas para o detalhamento teórico foram [2], [3] e [4].

2.1.1 Grupos

Definição 2.1 *Uma operação binária $*$ sobre um conjunto S é uma regra que associa a cada par ordenado (a, b) de elementos algum elemento de S, com $a * b$ denotado o elemento associado a (a, b) através de $*$.*

Definição 2.2 *Um conjunto G não vazio, ou seja, munido de uma operação binária sobre G, será um grupo se satisfazer as seguintes condições:*

- *associatividade: $a * (b * c) = (a * b) * c$, quaisquer que sejam a,b e $c \in G$;*
- *existência do elemento neutro: existe um elemento $e \in G$ tal que $a * e = e * a = a$, qualquer que seja $a \in G$;*
- *existência de simétricos: para cada $a \in G$ existe um elemento $a' \in G$ tal que $a * a' = a' * a = e$.*

Além dessas propriedades, se a operação satisfazer a propriedade de comutatividade: $a * b = b * a$, quaisquer que sejam $a, b \in G$, o grupo receberá o nome de grupo comutativo ou abeliano.

Definição 2.3 *Seja G um grupo. O número de elementos de G é chamado de ordem de G, denotada por $|G|$. Um grupo de ordem finita é chamado grupo finito. Caso contrário, é denominado de grupo infinito.*

Exemplo 2.1 *Grupo aditivo de classes de restos (comutativo) é, para qualquer inteiro $m > 1$, o conjunto das classes de resto módulo m, ou seja, $\mathbb{Z}_m$=$\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$ é o conjunto quociente de $\mathbb{Z}$ pela relação de congruência, módulo m. Satisfaz as propriedades de associatividade, comutatividade e elemento neutro, sendo $\overline{0}$ o elemento neutro da adição. Já a classe $\overline{m-a}$ é o oposto de $\overline{a} \in \mathbb{Z}_m$ na adição módulo m. Logo ($\mathbb{Z}_m$,+) é um grupo comutativo, para todo inteiro $m > 1$, chamado grupo aditivo das classes de restos módulo m, onde sua ordem é m.*

Exemplo 2.2 *Um grupo multiplicativo de classes de restos goza das propriedades associativa e comutativa. Além disso, a classe $\overline{1}$ é o seu elemento neutro. No entanto, devido $\overline{0}$ de $\mathbb{Z}_m$ não possuir inverso e o restante do conjunto nem sempre ser um grupo multiplicativo, há uma restrição da multiplicação módulo m aos elementos $\mathbb{Z}_m^* = \mathbb{Z}_m$ - $\overline{0}$, é um grupo multiplicativo se, e somente se, m é um número primo.*

2.1.2 Anéis

Definição 2.4 *Seja A um conjunto não vazio em que estejam definidas duas operações binárias, as quais chamaremos de soma e produto em A e denotaremos por $+$ e $*$, respectivamente. Assim:*

$$\begin{array}{rccc} + : & A \times A & \to & A \\ & (a,b) & \mapsto & a+b \end{array} \qquad e \qquad \begin{array}{rccc} * : & A \times A & \to & A \\ & (a,b) & \mapsto & a*b \end{array}$$

Chamaremos $< A, +, * >$ de anel se as seguintes seis propriedades são verificadas quaisquer que sejam $a, b, c \in A$.

- *associatividade da soma:* $(a+b)+c = a+(b+c)$;
- *existência do elemento neutro para a soma:* $\exists\, 0 \in A$ *tal que* $a+0 = 0+a = a$;
- *existência do inverso aditivo:* $\forall\, x \in A$ *existe um número* $y \in A$, *denotado por* $y = -x$, *tal que* $x+y = y+x = 0$;
- *comutatividade da soma:* $a+b = b+a$;
- *associatividade do produto:* $(a*b)*c = a*(b*c)$;
- *distributividade à direita e à esquerda:* $a*(b+c) = a*b+a*c$; $(a+b)*c = a*c+b*c$.

  Se um anel $< A, +, * >$ satisfaz a propriedade:

- $< A, +, * >$ *é um anel com unidade 1 se* $\exists\, 1 \in A$, $0 \neq 1$, *tal que* $x*1 = 1*x = x$, $\forall\, x \in A$;

  Se um anel $< A, +, * >$ satisfaz a propriedade:

- $< A, +, * >$ *é um anel comutativo se* $\forall\, x, y \in A,\ x * y = y * x$;

  Se um anel $< A, +, * >$ *satisfaz a propriedade:*

- $< A, +, * >$ *é um anel sem divisores de zero* $\forall\, x, y \in A,\ x * y = 0 \Rightarrow x = 0$ *ou* $y = 0$.

2.1.3 Corpos

Definição 2.5 *Seja F um conjunto não vazio com duas operações binárias definidas sobre ele, adição $(+)$ e multiplicação $(\cdot)$. Um corpo é todo anel comutativo $(A, +, \cdot)$ com elemento unidade, tal que todo elemento não nulo de F possui inverso multiplicativo. Em outras palavras, um corpo é a terna ordenada $(F, +, \cdot)$ que satisfaz as seguintes condições:*

- *$(F, +)$ é um grupo abeliano. O elemento identidade é o 0 (zero);*
- *$(F^*, \cdot)$ é um grupo abeliano. O elemento identidade é o 1 (um);*
- *A multiplicação é distributiva em relação à adição, à direita e à esquerda, isto é, para quaisquer $a, b, c \in F$, $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$.*

Um corpo F que apresenta um número finito de elementos, sendo esse número sua ordem, é chamado de corpo finito.

Definição 2.6 *Um corpo de Galois é um corpo com número finito de elementos e é representado por $GF(p)$, onde p é número primo.*

Para qualquer inteiro positivo m é possível estender um corpo primo $GF(p)$ com p elementos para um corpo estendido $GF(p^m)$ com p^m elementos. A ordem de qualquer corpo finito estendido é potência de um primo. Podemos construir códigos a partir de $GF(2)$ ou $GF(2^m)$ e, consequentemente, a aritmética usada é binária.

Definição 2.7 *Um polinômio $p(x)$ de grau m sobre $GF(2)$ é dito irredutível se ele não é divisível por nenhum outro polinômio sobre $GF(2)$ de grau menor que m mas maior que zero.*

Proposição 2.1 Para qualquer $m \geq 1$ existe um polinômio irredutível de grau m.

Definição 2.8 *Um polinômio irredutível $p(x)$ de grau m é dito primitivo se o menor inteiro positivo n para o qual $p(x)$ divide $X^n + 1$ for $n = 2^m - 1$.*

A construção de um corpo de Galois, a partir de um polinômio primitivo, resulta em uma representação em forma de potência, uma em forma de polinômio e uma em forma vetorial.

Construção de Corpos de Galois $GF(2^m)$

Em [7] é apresentado um método para construção de um corpo de Galois sobre $GF(2)$ com 2^m elementos, sendo $m \geq 1$. Dessa forma, sejam 0 e 1 os elementos de $GF(2)$, o símbolo α e a operação de multiplicação "$\cdot$" definida da seguinte forma:

$$\begin{gathered} 0 \cdot \alpha^j = \alpha^j \cdot 0 = 0; \\ 1 \cdot \alpha^j = \alpha^j \cdot 1 = \alpha^j; \\ \vdots \\ \alpha^i \cdot \alpha^j = \alpha^j \cdot \alpha^i = \alpha^{i+j}. \end{gathered}$$

Assim, temos um conjunto de elementos sobre o qual a operação "$\cdot$" é definida:

$$F = \{0, 1, \alpha, \alpha^2, \alpha^3, ..., \alpha^j, ...\}.$$

Vamos estabelecer uma condição sobre o elemento α para considerar que o conjunto F tenha 2^m elementos, sendo fechado para a operação de multiplicação definida anteriormente. Seja $p(X)$ um polinômio primitivo de grau m sobre $GF(2)$ e seja α uma raiz de $p(X)$, ou seja, $p(\alpha) = 0$.

Como $p(X)$ divide $X^{2^m-1} + 1$ temos que

$$X^{2^m-1} + 1 = q(x) \cdot p(X),$$

em que $q(X)$ é um polinômio qualquer sobre $GF(2)$.

Substituindo X por α:

$$\alpha^{2^m-1} + 1 = q(\alpha) \cdot p(\alpha) \Rightarrow \alpha^{2^m-1} + 1 = q(\alpha) \cdot 0 \Rightarrow \alpha^{2^m-1} + 1 = 0.$$

Adicionando 1 em ambos lados da igualdade, obtemos:

$$\alpha^{2^m-1} = 1.$$

Portanto, existe um elemento $\alpha^{2^m-1} \neq 0$ a partir do qual os elementos do conjunto F tornam-se finitos. Assim, $F = \{0, 1, \alpha, \alpha^2, \alpha^3, ..., \alpha^{2^m-2}\}$ é um corpo de Galois com 2^m elementos.

Exemplo 2.3 *Seja $m = 3$ e consideremos o polinômio primitivo sobre $GF(2)$, $p(x) = 1 + x + x^3$. O conjunto F será dado da seguinte forma:*

$$F = \{0, 1, \alpha, \alpha^2, \alpha^3, ..., \alpha^{2^3-2}\} \Rightarrow F = \{0, 1, \alpha, \alpha^2, \alpha^3, ..., \alpha^6\}.$$

Admitindo que α seja uma raiz desse polinômio, ou seja, $p(\alpha) = 0$, temos:

$$0 = 1 + \alpha + \alpha^3 \Rightarrow \alpha^3 = 1 + \alpha.$$

A partir dessa relação podemos construir $GF(2^3)$:

$$\alpha^4 = \alpha^3 \cdot \alpha = (1 + \alpha) \cdot \alpha = \alpha + \alpha^2$$
$$\alpha^5 = \alpha^4 \cdot \alpha = (\alpha + \alpha^2) \cdot \alpha = \alpha^2 + \alpha^3 = 1 + \alpha + \alpha^2$$
$$\alpha^6 = \alpha^5 \cdot \alpha = (1 + \alpha + \alpha^2) \cdot \alpha = \alpha + \alpha^2 + \alpha^3 = \alpha + \alpha^2 + \alpha + 1 = 1 + \alpha^2.$$

As representações vetorial, polinomial e por potência são apresentadas na Tabela 1 a seguir.

Tabela 1 – $GF(2^3)$ gerado por $p(x) = 1 + x + x^3$.

Representações		
Potência	**Polinomial**	**Vetorial**
0	0	(000)
$\alpha^0 = 1$	1	(100)
α	α	(010)
α^2	α^2	(001)
α^3	$1 + \alpha$	(110)
α^4	$\alpha + \alpha^2$	(011)
α^5	$1 + \alpha + \alpha^2$	(111)
α^6	$1 + \alpha^2$	(101)

2.2 Elementos de um Sistema de Comunicação

Nesta seção serão apresentados os elementos fundamentais associados a um sistema de comunicação. As referências utilizadas foram [1] e [7].

Definição 2.9 *Um sistema de comunicação é um conjunto de mecanismos que tem como objetivo transmitir informações de uma fonte a um destinatário via um canal de comunicação. Um sistema de comunicação pode ser dividido em dois sistemas: analógicos e digitais.*

Os principais elementos de um sistema de comunicação são:

1. Transmissor: responsável por gerar a informação, no qual localizam-se :
   - Fonte: local em que o sinal é gerado.
   - Codificador de fonte: realiza a conversão do sinal da saída da fonte em uma sequência de dígitos binários, que são os códigos.
2. Canal: região em que é transmitida a informação e que são introduzidos os ruídos.
   - Codificador de canal: transforma a sequência da saída do codificador de fonte em uma palavra-código (dígitos binários), através da redundância para eliminar os efeitos ruidosos adquiridos no canal.
   - Modulador: converte a saída do codificador de canal para uma forma adequada para ser transmitida.
   - Demodulador: com o sinal recebido do canal, se estima sua versão digital e é enviada para o codificador de canal.
   - Decodificador de canal: realiza uma tentativa de corrigir alguns erros que possam aparecer nos dígitos fornecidos pelo demodulador, estimando os dígitos na saída do codificador da fonte.
3. Receptor: representa o usuário que vai receber a informação.
   - Decodificador de fonte: é o local que transforma a sequência estimada na saída do decodificador de canal em uma estimativa na saída da fonte.
   - Destinatário: é quem recebe a informação transmitida.

A Figura 1 apresenta os principais elementos de um sistema de comunicação.

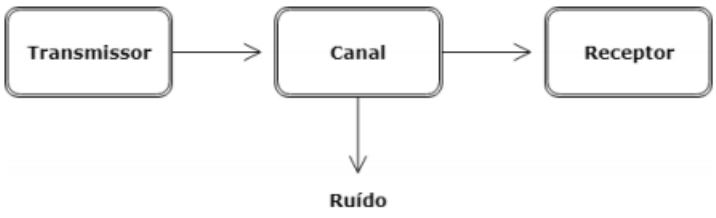

Figura 1 – Diagrama de blocos de um sistema de comunicação.
Fonte: [7].

Nas seções 2.3, 2.4 e 2.5 a seguir serão apresentados os conceitos fundamentais sobre os códigos corretores de erros, os códigos BCH e os códigos Reed-Solomon. As principais referências utilizadas foram [2], [1], [7], [5] e [6].

2.3 Códigos Corretores de Erros

Atualmente, os códigos corretores de erros podem ser divididos em dois grupos: códigos de blocos e códigos convolucionais, sendo que cada um dos grupos possui diversos códigos, para as mais diversas aplicações.

Os códigos convolucionais possuem caráter probabilístico, pois a princípio, alguns matemáticos procuraram estimar a probabilidade de erros das "melhores" famílias de códigos de blocos e tinham o objetivo de compreender a codificação e a decodificação de um ponto de vista probabilístico, considerando a noção de decodificação sequencial. Nesse contexto, a decodificação sequencial exigiu a criação de uma nova classe de códigos sem blocos, com comprimento indefinido, representáveis por uma árvore em que a decodificação é feita percorrendo toda a extensão dessa árvore.

Os códigos de bloco são caracterizados pelo fato do processo de codificação ser feito sobre blocos de bits ou bloco de símbolos, isto é, uma sequência de bits ou símbolos é segmentada em blocos de k bits ou símbolos, a partir dos quais são geradas palavras-código com n bits ou símbolos. A taxa de codificação de um código de bloco é caracterizada como a relação entre o número de bits de informação e o número de bits da palavra-código, ou seja, $R = \dfrac{k}{n}$.

Definição 2.10 *Um código de bloco C de comprimento n sobre um alfabeto A é qualquer subconjunto do conjunto A^n das sequências $c = \{c_i | 1 \leq i \leq n\}$. Um código de bloco é caracterizado por três parâmetros: comprimento, dimensão e distância mínima e denotado por (n, k, d_{min}).*

Definição 2.11 *A distância de Hamming, denotada por $dist(x, y)$, é definida como o número de elementos em que dois vetores $x = \{x_1, \cdots, x_n\}$ e $y = \{y_1, \cdots, y_n\}$ se diferem.*

Definição 2.12 *O peso de Hamming de um vetor $x = \{x_1, \cdots, x_n\}$ é o número de coordenadas não-nulas de x_i e denotado por $w_t(x)$.*

Definição 2.13 *A distância mínima d_{min} de um código de blocos C, é a menor distância de Hamming entre dois vetores distintos quaisquer desse código e denotada por:*

$$d_{min} = \{dist(x, y) : x, y \in C, x \neq y\}.$$

Definição 2.14 *A capacidade de correção de erro é o número máximo de erros que podem ser corrigidos por palavra-código, e é dada por:*

$$t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor,$$

em que t é o maior inteiro não superior a $\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$.

A capacidade de correção de erro, t, está relacionada com a distância mínima do código da seguinte maneira: $d_{min} \leq 2t+1$, ou seja, quanto maior a capacidade de correção de erros de um código maior a sua distância mínima.

Definição 2.15 *Um código de bloco de comprimento n e 2^k palavras código, é um código linear se e só se as suas 2^k palavras-código formam um subespaço de dimensão k em relação ao espaço formado pelas 2^n n-uplas possíveis em $GF(2)$.*

2.4 Códigos BCH

Os códigos cíclicos formam uma importante subclasse dos códigos de bloco lineares. Um código de bloco C é denominado cíclico se qualquer deslocamento de uma palavra código resulta em uma outra palavra código.

Seja um código linear C e $v = (v_0, v_1, v_2, ..., v_{n-1})$ um vetor de C. Se as componentes do vetor v forem deslocadas uma posição para a direita e a última componente v_{n-1} for deslocada para primeira posição à esquerda, obtemos o seguinte vetor: $v(1) = (v_{n-1}, v_0, v_1, v_2, ..., v_{n-2})$. Esse processo de deslocamento das componentes de um vetor é chamado de deslocamento cíclico de v.

Definição 2.16 *Um código linear $C(n,k)$ é um código cíclico se qualquer deslocamento cíclico de uma palavra-código de C resulta em uma outra palavra-código do código C.*

Podemos representar a palavra código $v = (v_0, v_1, v_2, ..., v_{n-1})$ pelo polinômio-código $v(x) = v_0 + v_1x + v_2x^2 + ... + v_{n-1}x^{n-1}$.

Os códigos BCH (Bose, Chaudhuri e Hocquenghen) são uma importante classe cíclica de códigos corretores de erros, em que são utilizados corpos finitos em sua construção, admitindo representação em termos de polinômios sobre $GF(p)$. Os códigos BCH binários são uma generalização dos códigos de Hamming[1] e podem corrigir múltiplos erros.

Teorema 2.1 *Para qualquer inteiro $m \geq 3$ e $t < 2^m - 1$ existe um código BCH binário com capacidade de correção de t erros, com os seguintes parâmetros:*

- *comprimento do bloco: $n = 2^m - 1$;*
- *número de dígitos de verificação de paridade: $n - k \leq mt$;*

[1] Códigos de Hamming: são códigos de blocos lineares, desenvolvidos por Richard Hamming, baseados na adição de bits de paridade. Assim, é possível detectar erros por meio da adição de bits de paridade a um determinado número de bits de dados.

- *distância mínima:* $d_{min} \geq 2^t + 1$.

O código BCH definido anteriormente é gerado por um polinômio que é especificado em termos de suas raízes no corpo finito $GF(2^m)$.

Definição 2.17 *Seja* $g(x) = 1 + g_1x + g_2x^2 + ... + g_{n-k-1}x^{n-k-1} + g_{n-k}x^{n-k}$ *um polinômio não nulo de grau mínimo* $n - k$ *de um código cíclico binário* $C(n, k)$. *O polinômio* $g(x)$ *é chamado de polinômio gerador de* $C(n, k)$.

Teorema 2.2

Seja $f(X)$ um polinômio com coeficientes em $GF(2)$. Se um elemento β de $GF(2^m)$ é uma raiz de $f(X)$, então o polinômio $f(X)$ também tem como raízes β^{2^l} para qualquer $l \geq 0$. Este elemento é chamado de conjugado de β.

O polinômio gerador de um código BCH é o polinômio de menor grau sobre o corpo de Galois $GF(2^m)$ que tem $\alpha, \alpha^2, \alpha^3, ..., \alpha^{2t}$ e seus conjugados como todas suas raízes. Se α é um elemento primitivo de $GF(2^m)$, então o código BCH resultante é um código BCH primitivo.

Teorema 2.3 *O polinômio mínimo* $\phi(X)$ *de um elemento* β *em* $GF(2^m)$ *é dado por:*

$$\phi(X) = \prod_{i=1}^{t-1}(X + \beta^{2^i}) \ .$$

Seja $\phi(X)$ o polinômio mínimo de α^i. Então o polinômio gerador $g(X)$ é dado pelo mínimo múltiplo comum dos polinômios mínimos $\{\phi_1(X), \phi_2(X), ..., \phi_{2t}(X)\}$:

$$g(X) = MMC\{\phi_1(X), \phi_2(X), ..., \phi_{2t}(X)\} \ .$$

Teorema 2.4 *O polinômio gerador* $g(X)$ *de um código BCH binário com comprimento* $2^m - 1$ *e capacidade de correção de* t *erros é dado por:*

$$g(X) = MMC\{\phi_1(X), \phi_3(X), ..., \phi_{2t-1}(X)\} \ .$$

Um código BCH de comprimento $2^m - 1$, com capacidade de correção $t = 1$ (um único erro) é gerado por $g(X) = \phi_1(X)$, no qual $\phi_1(X)$ é um polinômio primitivo de grau m, e é um código de Hamming.

2.5 Códigos Reed-Solomon

Os códigos Reed-Solomon (RS) são particularmente úteis para correção de rajada de erros, além de possuírem capacidade de correção de erros. Esses códigos são muito utilizados em diversos sistemas de armazenamento de informações.

Definição 2.18 *Os códigos Reed-Solomon são códigos cíclicos não binários com símbolos constituídos por sequências de m bits, em que m é qualquer positivo inteiro tendo valor maior do que 2. Assim, os códigos RS com símbolos de m bits existem para todo n e k, com $0 < k < n < 2^m + 2$, em que k é o número de símbolos de dados que estão sendo codificados e n é o número de símbolos códigos em um bloco codificado.*

As principais características dos códigos RS são apresentadas na Tabela 2 a seguir.

Tabela 2 – Principais características dos códigos RS.

Comprimento do código	$n = 2^m - 1$
Número de bits de informação	$k = 2^m - 1 - 2t$
Número de bits de paridade	$n - k = 2t$
Distância mínima	$d_{min} = n - k + 1$
Capacidade de correção	$t = \left\lfloor \frac{n-k}{2} \right\rfloor$

Definição 2.19 *A probabilidade de erro de símbolo, P_E, é encontrada em função da probabilidade de erro de símbolo do canal, p, isto é,*

$$P_E \approx \frac{1}{2^m - 1} \sum_{j=t+1}^{2^m-1} \binom{2^m - 1}{j} p^j (1-p)^{2m-1-j},$$

em que t é a capacidade de correção de erro de símbolo do código, sendo que cada símbolo possui m bits.

Exemplo 2.4 *Consideremos um código Reed-Solomon, de comprimento n e dimensão k, dado por RS $(n, k) = (255, 247)$, em que $m = 8$ bits (= 1 byte). A capacidade de correção de erros deste código é:*

$$t = \left\lfloor \frac{n-k}{2} \right\rfloor = \left\lfloor \frac{255 - 247}{2} \right\rfloor = 4,$$

ou seja, todos os padrões de 4 símbolos errados ou menos, em um bloco de 255 símbolos. Imagine que um surto de ruído seja capaz de perturbar a transmissão durante um período correspondente a 25 bits, como mostrado na Figura 2.

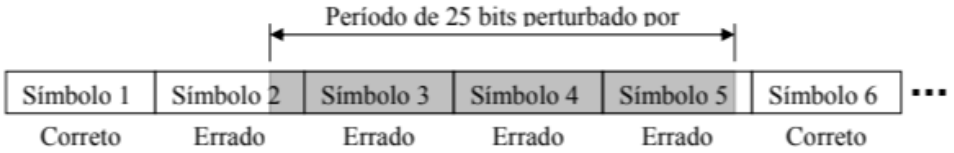

Figura 2 – Bloco de dados perturbado por ruído durante 25 períodos de bit.
Fonte: [2].

Como cada símbolo possui 8 *bits, logo um período de* 25 *bits afeta* 4 *símbolos e, além disso, como o código corrige qualquer padrão de até* 4 *símbolos errados, todos os símbolos afetados serão corrigidos. Essa característica não binária possibilita aos códigos RS uma grande vantagem em termos de correção de erros em rajada em relação aos outros códigos de blocos binários.*

Na codificação dos códigos RS, o polinômio gerador assume a seguinte forma:

$$g(X) = g_0 + g_1X + g_2X^2 + g_{2t-1}X^{2t-1} + X^{2t}.$$

O grau do polinômio gerador é igual ao número de símbolos de paridade. Uma vez que o grau do polinômio gerador é igual a $2t$, deve haver precisamente $2t$ potências sucessivas de α que são raízes do polinômio. As raízes de $g(X)$ são designadas como: $\alpha, \alpha^2, \ldots, \alpha^{2t}$. Sendo assim, o polinômio gerador $g(X)$ pode ser obtido do seguinte modo:

$$g(X) = (X - \alpha)(X - \alpha^2)\ldots(X - \alpha^{2t}).$$

Exemplo 2.5 *Consideremos o código RS* $(7, 3)$ *com capacidade de correção de duplo erro de símbolo. O polinômio gerador em termos de suas* $2t = n - k = 4$ *raízes é descrito da seguinte maneira:*

$$\begin{aligned} g(X) &= (\mathrm{X} - \alpha)(X - \alpha^2)(X - \alpha^3)(X - \alpha^4) \\ &= (\mathrm{X}^2 - (\alpha + \alpha^2)X + \alpha^3)(X^2 - (\alpha^3 + \alpha^4)X + \alpha^7) \\ &= (\mathrm{X}^2 - \alpha^4X + \alpha^3)(X^2 - \alpha^6X + \alpha^0) \\ &= (\mathrm{X}^4 - (\alpha^4 + \alpha^6)X^3 + (\alpha^3 + \alpha^10 + \alpha^0)X^2 + (\alpha^4 + \alpha^9)X + \alpha^3. \end{aligned}$$

Assim, escrevendo o polinômio da ordem mais baixa para a mais alta, e trocando os sinais negativos por positivos (no campo binário $+1 = -1$*), tem-se:*

$$g(X) = \alpha^3 + \alpha^1X + \alpha^0X^2 + \alpha^3X^3 + X^4.$$

3 *Detalhamento algébrico da codificação e da decodificação de códigos Reed-Solomon*

Neste capítulo será apresentado um detalhamento algébrico dos processos de codificação e de decodificação de códigos Reed-Solomon, com os principais elementos teóricos e a apresentação de exemplos envolvendo o código RS$(7, 3)$. A principal referência utilizada foi [4].

3.1 Codificação de Códigos Reed-Solomon

Em termos dos parâmetros (n, k, t), para a forma mais comum dos códigos RS, tem-se que:

$$(n, k) = (2^m - 1, 2^m - 1 - 2t), \qquad m > 2,$$

em que $n - k = 2t$ é o número de símbolos de paridade e t é a capacidade de correção de erro de símbolo do código. O polinômio gerador para um código RS assume a seguinte forma:

$$g(X) = g_0 + g_1X + g_2X^2 + \cdots + g_{2t-1}X^{2t-1} + X^{2t}.$$

O grau do polinômio gerador é igual ao número de símbolos de paridade.

Uma vez que o grau do polinômio gerador é igual a $2t$, deve haver precisamente $2t$ potências sucessivas de α que são raízes do polinômio.

As raízes de $g(X)$ são designadas como: α, α^2, $\cdots$, α^{2t}.

Dessa forma, o polinômio gerador $g(X)$ pode ser obtido da seguinte forma:

$$g(X) = (X - \alpha)(X - \alpha^2)\cdots(X - \alpha^{2t}).$$

Exemplo 3.1 *Consideremos o código RS*$(7, 3)$ *com capacidade de correção de duplo erro de símbolo.*

O polinômio gerador em termos de suas raízes $(2t = n - k = 4)$*,é descrito como:*

$$\begin{aligned} g(X) &= (X - \alpha)(X - \alpha^2)(X - \alpha^3)(X - \alpha^4) \\ &= (X - (\alpha + \alpha^2)X + \alpha^3)(X^2 - (\alpha^3 + \alpha^4)X + \alpha^7) \\ &= (X^2 - \alpha^4X + \alpha^3)(X^2 - \alpha^6X + \alpha^0) \\ &= (X^4 - (\alpha^4 + \alpha^6)X^3 + (\alpha^3 + \alpha^10 + \alpha^0)X^2 + (\alpha^4 + \alpha^9)X + \alpha^3 \\ &= X^4 - \alpha^3X^3 + \alpha^0X^2 - \alpha^1X + \alpha^3. \end{aligned}$$

Escrevendo o polinômio da ordem mais baixa para a mais alta, e trocando os sinais negativos por positivos, $g(X)$ pode ser escrito como:

$$g(X) = \alpha^3 + \alpha^1 X + \alpha^0 X^2 + \alpha^3 X^3 + X^4.$$

3.1.1 Codificação na forma sistemática

Os códigos Reed-Solomon podem ser codificados na forma sistemática de forma análoga ao procedimento para os códigos binários, uma vez que os códigos RS são códigos cíclicos. Assim,

$$X^{n-k} m(X) = q(X) g(X) + p(X),$$

em que $q(X)$ e $p(X)$ são os polinômios quociente e resto, da divisão da mensagem deslocada de $n-k$ posições, $X^{n-k}m(X)$, pelo polinômio gerador, $g(X)$.

Note que, na forma sistemática, o polinômio resto, $p(X)$, é o polinômio paridade da palavra código, então a equação pode ser escrita como:

$$p(X) = X^{n-k} m(X) \mod g(X).$$

A palavra código polinomial resulta em:

$$c(X) = p(X) + X^{n-k} m(X).$$

Exemplo 3.2 *Consideremos a sequência da mensagem binária* 010110111*. A codificação sistemática da mensagem com um código RS*$(7, 3)$*, cujo polinômio gerador é aquele obtido por* $g(X) = (X - \alpha)(X - \alpha^2) \cdots (X - \alpha^{2t})$ *para geração dos símbolos em* $GF(2^3)$ *pode ser realizada considerando o polinômio primitivo* $p(X) = 1 + X + X^3$*.*

A sequência 010110111 *pode ser segmentada em elementos base do corpo gerado por* $1 + X + X^3$*, na forma* 010 110 111*, para a obtenção dos elementos do corpo* α^1*,* α^3 *e* α^5*, conforme apresentado na Tabela 3, apresentada a seguir.*

Logo, o polinômio mensagem é $\alpha^1 + \alpha^3 X + \alpha^5 X^2$*, que multiplicado por* X^{n-k}*, torna-se:*

$$X^4(\alpha^1 + \alpha^3 X + \alpha^5 X^2) = \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6.$$

O polinômio paridade é o resto da divisão do polinômio deslocado, $X^{n-k}m(X)$*, por* $g(X)$*.*

Note que a divisão polinomial deve ser feita em $GF(2^3)$*, ou seja, as regras de adição e de multiplicação devem obedecer aos cálculos das Tabelas* 4 *e* 5*.*

Tabela 3 – Mapeamento dos elementos do corpo em termo de seus elementos base para $f(X) = 1+X+X^3$ e representação das potências de α.

Representações		
Potência	**Polinomial**	**Vetorial**
0	0	(000)
$\alpha^0 = 1$	1	(100)
α	α	(010)
α^2	α^2	(001)
α^3	$1 + \alpha$	(110)
α^4	$\alpha + \alpha^2$	(011)
α^5	$1 + \alpha + \alpha^2$	(111)
α^6	$1 + \alpha^2$	(101)

Tabela 4 – Adição para $GF(2^3)$ com $f(X) = 1 + X + X^3$.

$\oplus$	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	0	α^3	α^6	α^1	α^5	α^4	α^2
α^1	α^3	0	α^4	α^0	α^2	α^6	α^5
α^2	α^6	α^4	0	α^5	α^1	α^3	α^0
α^3	α^1	α^0	α^5	0	α^6	α^2	α^4
α^4	α^5	α^2	α^1	α^6	0	α^0	α^3
α^5	α^4	α^6	α^3	α^2	α^0	0	α^1
α^6	α^2	α^5	α^0	α^4	α^3	α^1	0

Tabela 5 – Multiplicação para $GF(2^3)$ com $f(X) = 1 + X + X^3$

$\otimes$	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^1	α^1	α^2	α^3	α^4	α^5	α^6	α^0
α^2	α^2	α^3	α^4	α^5	α^6	α^0	α^1
α^3	α^3	α^4	α^5	α^6	α^0	α^1	α^2
α^4	α^4	α^5	α^6	α^0	α^1	α^2	α^3
α^5	α^5	α^6	α^0	α^1	α^2	α^3	α^4
α^6	α^6	α^0	α^1	α^2	α^3	α^4	α^5

Realizando a divisão polinomial do polinômio $X^{n-k}m(X) = \alpha^5X^6 + \alpha^3X^5 + \alpha^1X^4$ *pelo polinômio* $g(X) = \alpha^0X^4 + \alpha^3X^3 + \alpha^0X^2 + \alpha^1X + \alpha^3$*, obtemos o quociente* $q(X) = \alpha^5X^2 + \alpha^0X + \alpha^4$ *e resto* $p(X) = \alpha^6X^3 + \alpha^4X^2 + \alpha^2X + \alpha^0$.

Logo,

$$p(X) = \alpha^0 + \alpha^2X + \alpha^4X^2 + \alpha^6X^3.$$

Assim, como a palavra código polinomial é dada por $c(X) = p(X) + X^{n-k}m(X)$, *com* $p(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3$ *e* $X^{n-k}m(X) = \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6$, *obtém-se:*

$$c(X) = (\alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3) + (\alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6),$$

isto é,

$$c(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6.$$

3.1.1.1 Codificação na forma sistemática com registradores de deslocamento de $(n-k)$ estágios

A implementação de um codificador RS$(7,3)$ descrito pelo polinômio $g(X)$, requer uma cadeia de registradores de deslocamento, conforme mostrado na Figura 3 a seguir.

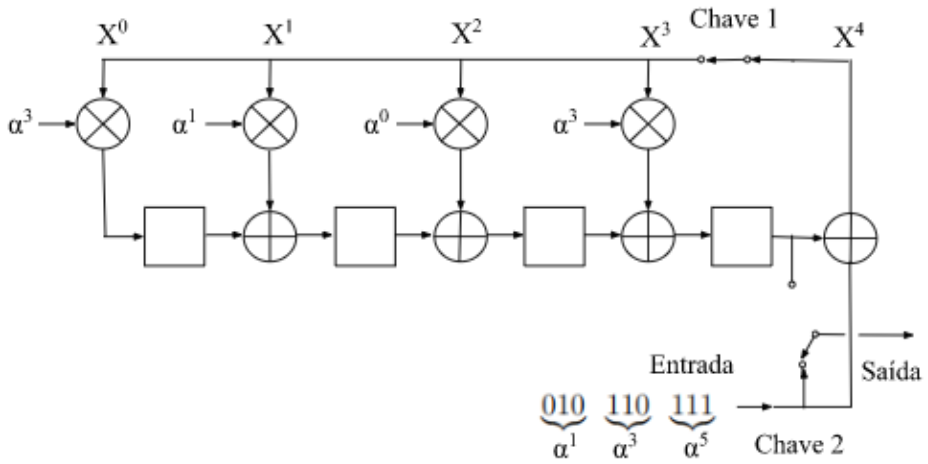

Figura 3 – Codificador com registradores de deslocamento para o código RS$(7,3)$.
FONTE: adaptado de [1].

Assim como no caso binário, no codificador o número de estágios do registrador de deslocamento é igual a $(n-k)$.

Contudo, enquanto no caso binário cada estágio armazena 1 bit, no codificador RS, cada estágio armazena 1 símbolo.

No caso específico do codificador para o código RS$(7,3)$, cada estágio armazena então 3 bits.

No caso binário, cada termo do polinômio gerador era representado por ausência ou presença da conexão de realimentação para cada estágio, correspondentes aos coeficientes "$0s$" e "$1s$", respectivamente.

Nos codificadores RS, todos os termos do polinômio são representados por conexões de realimentação que são multiplicadas pelos respectivos símbolos coeficientes.

O processo de codificação descrito a seguir é similar ao caso binário.

1. Inicialmente a Chave 1 está fechada, permitindo o carregamento da mensagem no registrador de deslocamento de $(n-k)$ estágios.

2. Ao mesmo tempo a Chave 2 está fechada para baixo durante os primeiros k ciclos de *clock* afim de permitir a transferência simultânea dos símbolos de mensagem diretamente para a saída do codificador.

3. Após a transferência dos k símbolos de mensagem para a saída do codificador, a Chave 1 é aberta e a Chave 2 é fechada para cima.

4. Os $(n-k)$ ciclos de *clock* restantes deslocam os símbolos de paridade para fora do registrador de deslocamento.

5. O número total de ciclos de *clock* é igual a n e na saída do codificador obtém-se a palavra código polinomial $p(X) + X^{n-k}m(X)$, em que $p(X)$ representam os símbolos de paridade, e $m(X)$ os símbolos de mensagem na forma polinomial.

Exemplo 3.3 *Consideremos a sequência mensagem* $m(X) = \alpha^1 + \alpha^3 X + \alpha^5 X^2$. *A codificação sistemática da mensagem com um código* $RS(7,3)$ *pode ser realizada usando o codificador da Figura 3 e mostrando a cada ciclo de clock a saída e o conteúdo do registrador de deslocamento.*

O conteúdo dos registradores, apresentado na Tabela 6, é formado pela realimentação a cada ciclo clock no codificador, a partir dos coeficientes do polinômio gerador e obedecendo as regras das duas operações aritméticas possíveis sobre $GF(2^3)$*: a adição e a multiplicação, apresentadas anteriormente.*

Tabela 6 – Codificação Reed-Solomon.

Fila de entrada	Ciclos *clock*	Conteúdo dos registradores	Realimentação	Fila de saída
$\alpha^1 \quad \alpha^3 \quad \alpha^5$	0	$0 \quad 0 \quad 0 \quad 0$	α^5	α^5
$\alpha^1 \quad \alpha^3$	1	$\alpha^1 \quad \alpha^6 \quad \alpha^5 \quad \alpha^1$	α^0	$\alpha^3\alpha^5$
α^1	2	$\alpha^3 \quad 0 \quad \alpha^2 \quad \alpha^2$	α^4	$\alpha^1\alpha^3\alpha^5$
–	3	$\alpha^0 \quad \alpha^2 \quad \alpha^4 \quad \alpha^6$	0	$\alpha^6\alpha^1\alpha^3\alpha^5$
–	4	$0 \quad \alpha^0 \quad \alpha^2 \quad \alpha^4$	0	$\alpha^4\alpha^6\alpha^1\alpha^3\alpha^5$
–	5	$0 \quad 0 \quad \alpha^0 \quad \alpha^2$	0	$\alpha^2\alpha^4\alpha^6\alpha^1\alpha^3\alpha^5$
–	6	$0 \quad 0 \quad 0 \quad \alpha^0$	0	$\alpha^0\alpha^2\alpha^4\alpha^6\alpha^1\alpha^3\alpha^5$
–	7	$0 \quad 0 \quad 0 \quad 0$	0	$-\alpha^0\alpha^2\alpha^4\alpha^6\alpha^1\alpha^3\alpha^5$

1. *No ciclo clock* 0*, o conteúdo do registrador é todo nulo, ou seja,* $0 \quad 0 \quad 0 \quad 0$*, conforme apresentado na Figura 4.*

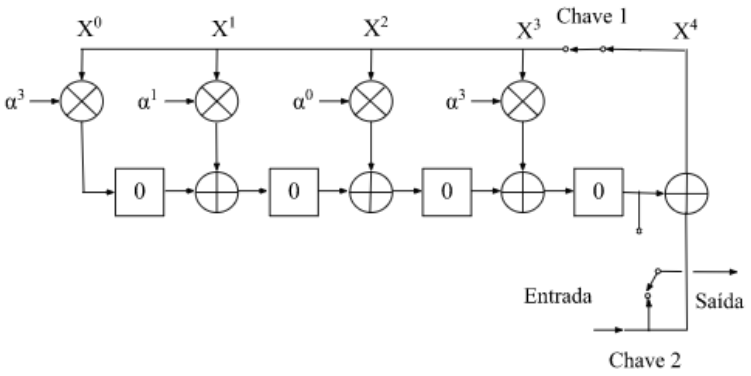

Figura 4 – Ciclo *clock* 0.
FONTE: do autor.

2. *No ciclo clock* 1*, entrou* α^5*. Logo, tem-se as seguintes operações:*

$\alpha^5 \cdot \alpha^3 = \alpha^1$
$\alpha^5 \cdot \alpha^1 = \alpha^6$; $\quad \alpha^6 + 0 = \alpha^6$
$\alpha^5 \cdot \alpha^0 = \alpha^5$; $\quad \alpha^5 + 0 = \alpha^5$
$\alpha^5 \cdot \alpha^3 = \alpha^1$; $\quad \alpha^1 + 0 = \alpha^1$

Assim, o conteúdo do registrador é: $\alpha^1 \quad \alpha^6 \quad \alpha^5 \quad \alpha^1$*, conforme apresentado na Figura 5.*

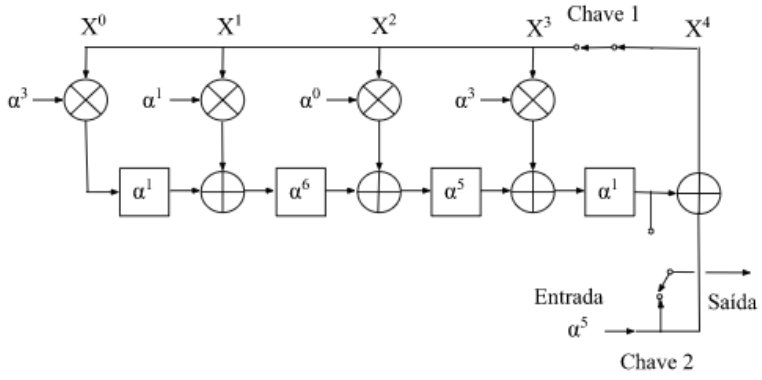

Figura 5 – Ciclo *clock* 1.
FONTE: do autor.

3. *No ciclo clock* 2*, entrou* α^0*. Logo, tem-se as seguintes operações:*

$\alpha^0 \cdot \alpha^3 = \alpha^3$
$\alpha^0 \cdot \alpha^1 = \alpha^1$; $\quad \alpha^1 + \alpha^1 = 0$
$\alpha^0 \cdot \alpha^0 = \alpha^0$; $\quad \alpha^0 + \alpha^6 = \alpha^2$
$\alpha^0 \cdot \alpha^3 = \alpha^3$; $\quad \alpha^3 + \alpha^5 = \alpha^2$

Assim, o conteúdo do registrador é: $\alpha^3 \quad 0 \quad \alpha^2 \quad \alpha^2$*, conforme apresentado na Figura 6.*

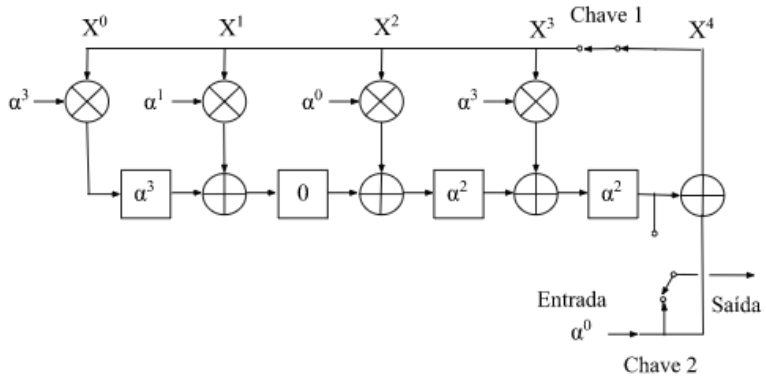

Figura 6 – Ciclo *clock* 2.
FONTE: do autor.

4. *No ciclo clock* 3, *entrou* α^4. *Logo, tem-se as seguintes operações:*

   $\alpha^4 \cdot \alpha^3 = \alpha^0$
   $\alpha^4 \cdot \alpha^1 = \alpha^5$; $\quad \alpha^5 + \alpha^3 = \alpha^2$
   $\alpha^4 \cdot \alpha^0 = \alpha^4$; $\quad \alpha^4 + 0 = \alpha^4$
   $\alpha^4 \cdot \alpha^3 = \alpha^0$; $\quad \alpha^0 + \alpha^2 = \alpha^6$

   Assim, o conteúdo do registrador é: $\alpha^0 \quad \alpha^2 \quad \alpha^4 \quad \alpha^6$, *conforme apresentado na Figura 7.*

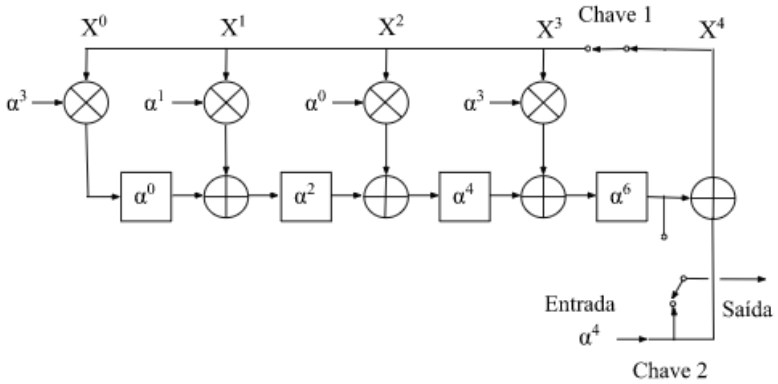

Figura 7 – Ciclo *clock* 3.
FONTE: do autor.

5. *No ciclo clock* 4, *entrou* 0. *Logo, tem-se as seguintes operações:*

   $0 \cdot \alpha^3 = 0$
   $0 \cdot \alpha^1 = 0$; $\quad 0 + \alpha^0 = \alpha^0$
   $0 \cdot \alpha^0 = 0$; $\quad 0 + \alpha^2 = \alpha^2$
   $0 \cdot \alpha^3 = 0$; $\quad 0 + \alpha^4 = \alpha^4$

   Assim, o conteúdo do registrador é: $0 \quad \alpha^0 \quad \alpha^2 \quad \alpha^4$, *conforme apresentado na Figura 8.*

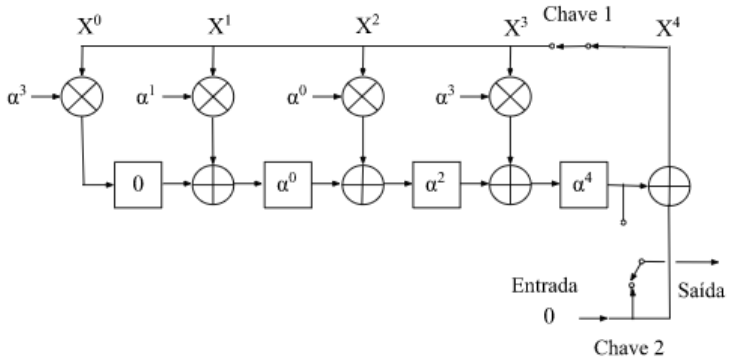

Figura 8 – Ciclo *clock* 4.
FONTE: do autor.

6. *No ciclo clock* 5*, entrou* 0*. Logo, tem-se as seguintes operações:*

   $0 \cdot \alpha^3 = 0$
   $0 \cdot \alpha^1 = 0$; $\quad 0 + 0 = 0$
   $0 \cdot \alpha^0 = 0$; $\quad 0 + \alpha^0 = \alpha^0$
   $0 \cdot \alpha^3 = 0$; $\quad 0 + \alpha^2 = \alpha^2$

   Assim, o conteúdo do registrador é: $0 \quad 0 \quad \alpha^0 \quad \alpha^2$*, conforme apresentado na Figura 9.*

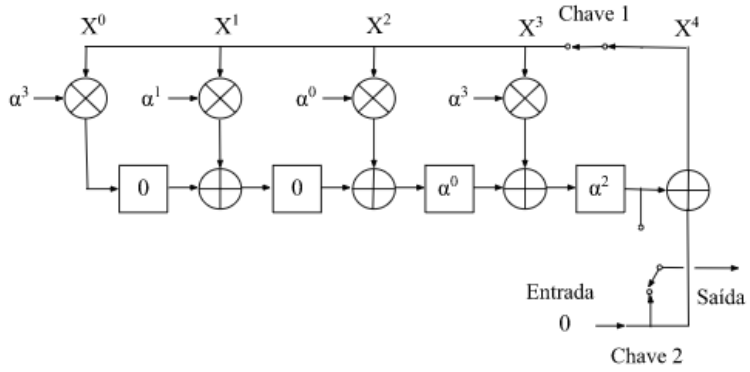

Figura 9 – Ciclo *clock* 5.
FONTE: do autor.

7. *No ciclo clock* 6*, entrou* 0*. Logo, tem-se as seguintes operações:*

   $0 \cdot \alpha^3 = 0$
   $0 \cdot \alpha^1 = 0$; $\quad 0 + 0 = 0$
   $0 \cdot \alpha^0 = 0$; $\quad 0 + 0 = 0$
   $0 \cdot \alpha^3 = 0$; $\quad 0 + \alpha^0 = \alpha^0$

   Assim, o conteúdo do registrador é: $0 \quad 0 \quad 0 \quad \alpha^0$*, conforme apresentado na Figura 10.*

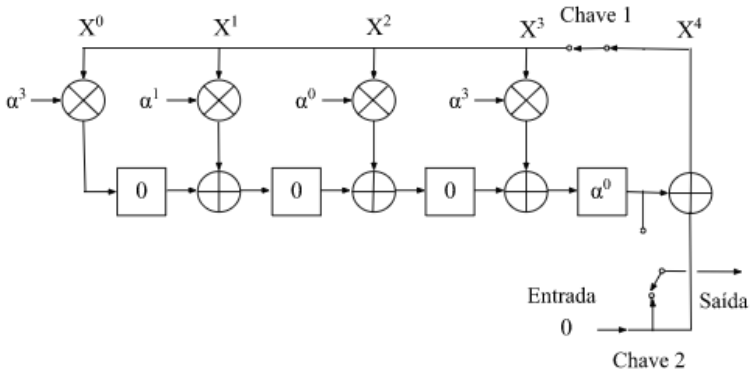

Figura 10 – Ciclo *clock* 6.
FONTE: do autor.

8. *No ciclo clock* 7*, entrou* 0*. Logo, tem-se as seguintes operações:*

   $0 \cdot \alpha^3 = 0$
   $0 \cdot \alpha^1 = 0;$ $\quad 0 + 0 = 0$
   $0 \cdot \alpha^0 = 0;$ $\quad 0 + 0 = 0$
   $0 \cdot \alpha^3 = 0;$ $\quad 0 + 0 = 0$

   Assim, o conteúdo do registrador é: 0 0 0 0, *conforme apresentado na Figura 11.*

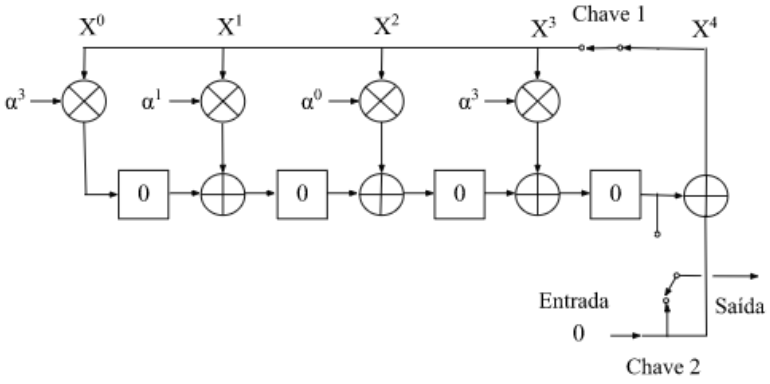

Figura 11 – Ciclo *clock* 7.
FONTE: do autor.

Na forma polinomial a fila de saída pode ser escrita como:

$$c(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6$$

ou

$$(100) + (001)X + (011)X^2 + (101)X^3 + (010)X^4 + (110)X^5 + (111)X^6.$$

As raízes do polinômio gerador $g(X)$ devem ser também raízes da palavra código gerada por $g(X)$, porque uma palavra válida é:

$$c(X) = m(X)g(X).$$

Desse modo, uma palavra código arbitrária quando calculada para qualquer raiz de $g(X)$, deve resultar em zero, ou seja,

$$c(\alpha) = c(\alpha^2) = c(\alpha^3) = c(\alpha^4) = 0.$$

O polinômio código resulta em zero quando calculado para qualquer raiz de $g(X)$, conforme mostrado a seguir, para cada uma das raízes.

$$\begin{aligned} c(\alpha) &= \alpha^0 + \alpha^2\alpha + \alpha^4\alpha^2 + \alpha^6\alpha^3 + \alpha^1\alpha^4 + \alpha^3\alpha^5 + \alpha^5\alpha^6 \\ &= \alpha^0 + \alpha^3 + \alpha^6 + \alpha^9 + \alpha^5 + \alpha^8 + \alpha^{11} \\ &= \alpha^0 + \alpha^3 + \alpha^6 + \alpha^2 + \alpha^5 + \alpha^1 + \alpha^4 \\ &= \alpha^1 + \alpha^0 + \alpha^6 + \alpha^4 \\ &= \alpha^3 + \alpha^3 \\ &= 0. \end{aligned}$$

$$\begin{aligned} c(\alpha^2) &= \alpha^0 + \alpha^2\alpha^2 + \alpha^4\alpha^4 + \alpha^6\alpha^6 + \alpha^1\alpha^8 + \alpha^3\alpha^{10} + \alpha^5\alpha^{12} \\ &= \alpha^0 + \alpha^4 + \alpha^8 + \alpha^{12} + \alpha^9 + \alpha^{13} + \alpha^{17} \\ &= \alpha^0 + \alpha^4 + \alpha^1 + \alpha^5 + \alpha^2 + \alpha^6 + \alpha^3 \\ &= \alpha^5 + \alpha^6 + \alpha^0 + \alpha^3 \\ &= \alpha^1 + \alpha^1 \\ &= 0. \end{aligned}$$

$$\begin{aligned} c(\alpha^3) &= \alpha^0 + \alpha^2\alpha^3 + \alpha^4\alpha^6 + \alpha^6\alpha^9 + \alpha^1\alpha^{12} + \alpha^3\alpha^{15} + \alpha^5\alpha^{18} \\ &= \alpha^0 + \alpha^5 + \alpha^{10} + \alpha^{15} + \alpha^{13} + \alpha^{18} + \alpha^{23} \\ &= \alpha^0 + \alpha^5 + \alpha^3 + \alpha^1 + \alpha^6 + \alpha^4 + \alpha^2 \\ &= \alpha^4 + \alpha^0 + \alpha^3 + \alpha^2 \\ &= \alpha^5 + \alpha^5 \\ &= 0. \end{aligned}$$

$$\begin{aligned} c(\alpha^4) &= \alpha^0 + \alpha^2\alpha^4 + \alpha^4\alpha^8 + \alpha^6\alpha^{12} + \alpha^1\alpha^{16} + \alpha^3\alpha^{20} + \alpha^5\alpha^{24} \\ &= \alpha^0 + \alpha^6 + \alpha^{12} + \alpha^{18} + \alpha^{17} + \alpha^{23} + \alpha^{29} \\ &= \alpha^0 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha^1 \\ &= \alpha^2 + \alpha^0 + \alpha^5 + \alpha^1 \\ &= \alpha^6 + \alpha^6 \\ &= 0. \end{aligned}$$

3.2 Decodificação de Códigos Reed-Solomon

Para um código RS, o padrão de erro pode ser descrito na forma polinomial como:

$$e(X) = \sum_{i=0}^{n-1} e_i X^i.$$

Para um código RS$(7, 3)$, a equação apresentada anteriormente torna-se:

$$e(X) = \sum_{i=0}^{6} e_i X^i = e_0 + e_1 X + e_2 X^2 + e_3 X^3 + e_4 X^4 + e_5 X^5 + e_6 X^6.$$

Agora, assuma que durante uma transmissão o polinômio código representado por $c(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6$ tenha sido corrompido por ruído e 2 símbolos foram recebidos com erro, de acordo com o padrão de duplo erro apresentado a seguir.

$$e(X) = 0 + 0X + 0X^2 + \alpha^2 X^3 + 0X^4 + \alpha^5 X^5 + 0X^6.$$

ou

$$(000) + (000)X + (000)X^2 + (001)X^3 + (000)X^4 + (111)X^5 + (000)X^6,$$

ou seja, $\alpha^2(001)$ introduz 1 bit errado no símbolo da posição X^3 e $\alpha^5(111)$ introduz 3 bits errados no símbolo da posição X^5.

Consequentemente, o polinômio código pode ser obtido a partir de:

$$r(X) = c(X) + e(X),$$

resulta em

$$\begin{aligned} &c(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6 \\ &+ \\ &e(X) = 0 + 0X + 0X^2 + \alpha^2 X^3 + 0X^4 + \alpha^5 X^5 + 0X^6 \end{aligned}$$

=

$r(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^0 X^3 + \alpha^1 X^4 + \alpha^2 X^5 + \alpha^5 X^6$.

Neste exemplo existem quatro incógnitas: duas posições de erro e dois valores errados.

A diferença fundamental entre a codificação binária e a não binária é que na primeira basta identificar as posições de erro e inverter os bits, enquanto que na segunda, além de identificar as posição dos símbolos errados, é necessário substituir o símbolo errado pelo símbolo correto, que é um elemento da extensão $GF(2^3)$.

Se existem quatro incógnitas neste exemplo, então são necessárias quatro equações para sua solução.

3.2.1 Cálculo da síndrome de erros

Para o código RS$(7, 3)$ aqui considerado, cada vetor síndrome possui quatro símbolos.

As raízes de $g(X)$ também são raízes de $c(X)$, ou seja, quando $c(X)$ é calculado para as raízes de $g(X)$, os valores resultantes são iguais a zero.

Qualquer erro introduzido em um polinômio código resultará em um polinômio que não terá as mesmas raízes de $g(X)$.

Desta maneira, a síndrome, S_i, pode ser determinada calculando-se $r(X)$ para as raízes de $g(X)$, ou seja,

$$S_i = r(X); \;\; X = \alpha^i,$$

$$S_i = r(\alpha^i); \;\; i = 1, ..., n-k.$$

Se $r(X)$ não contiver erros, então cada uma das síndromes S_i será igual a zero.

Para o polinômio recebido $r(X)$ apresentado, ou seja,

$$r(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^0 X^3 + \alpha^1 X^4 + \alpha^2 X^5 + \alpha^5 X^6,$$

os quatro símbolos da síndrome são:

$$\begin{aligned} S_1 &= \alpha^0 + \alpha^2\alpha + \alpha^4\alpha^2 + \alpha^1\alpha^4 + \alpha^0\alpha^3 + \alpha^2\alpha^5 + \alpha^5\alpha^6 \\ &= \alpha^0 + \alpha^3 + \alpha^6 + \alpha^3 + \alpha^5 + \alpha^0 + \alpha^4 \\ &= \alpha^2. \end{aligned}$$

$$\begin{aligned} S_2 &= \alpha^0 + \alpha^2\alpha^2 + \alpha^4\alpha^4 + \alpha^0\alpha^6 + \alpha^1\alpha^8 + \alpha^2\alpha^{10} + \alpha^5\alpha^{12} \\ &= \alpha^0 + \alpha^4 + \alpha^1 + \alpha^6 + \alpha^2 + \alpha^5 + \alpha^3 \\ &= 0. \end{aligned}$$

$$\begin{aligned} S_3 &= \alpha^0 + \alpha^2\alpha^3 + \alpha^4\alpha^6 + \alpha^0\alpha^9 + \alpha^1\alpha^{12} + \alpha^2\alpha^{15} + \alpha^5\alpha^{18} \\ &= \alpha^0 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha^6 + \alpha^3 + \alpha^2 \\ &= \alpha^3. \end{aligned}$$

$$\begin{aligned} S_4 &= \alpha^0 + \alpha^2\alpha^4 + \alpha^4\alpha^8 + \alpha^0\alpha^{12} + \alpha^1\alpha^{16} + \alpha^2\alpha^{20} + \alpha^5\alpha^{24} \\ &= \alpha^0 + \alpha^6 + \alpha^5 + \alpha^5 + \alpha^3 + \alpha^1 + \alpha^1 \\ &= \alpha^5. \end{aligned}$$

Exemplo 3.4 *As síndromes do padrão de erro representado por* $e(X) = 0 + 0X + 0X^2 + \alpha^2X^3 + 0X^4 + \alpha^5X^5 + 0X^6$ *são iguais às síndromes calculadas para o polinômio recebido representado por* $r(X) = \alpha^0 + \alpha^2X + \alpha^4X^2 + \alpha^0X^3 + \alpha^1X^4 + \alpha^2X^5 + \alpha^5X^6$.

Com efeito,

$$S_i = r(X); \quad X = \alpha^i$$

$$S_i = r(\alpha^i); \quad i = 1, ..., n-k$$

$$S_i = [c(X) + e(X)]; \quad X = \alpha^i$$

$$S_i = [c(\alpha^i) + e(\alpha^i)] = 0 + e(\alpha^i)$$

$$S_i = e(\alpha^i).$$

De $e(X) = 0 + 0X + 0X^2 + \alpha^2X^3 + 0X^4 + \alpha^5X^5 + 0X^6$, *tem-se:*

$$e(X) = \alpha^2X^3 + \alpha^5X^5.$$

Desta forma,

$$\begin{aligned} S_1 = \mathrm{e}(\alpha^1) &= \alpha^2\alpha^3 + \alpha^5\alpha^5 \\ &= \alpha^5 + \alpha^3 \\ &= \alpha^2. \end{aligned}$$

$$\begin{aligned} S_2 = \mathrm{e}(\alpha^2) &= \alpha^2\alpha^6 + \alpha^5\alpha^{10} \\ &= \alpha^1 + \alpha^1 \\ &= 0. \end{aligned}$$

$$\begin{aligned} S_3 = \mathrm{e}(\alpha^3) &= \alpha^2\alpha^9 + \alpha^5\alpha^{15} \\ &= \alpha^4 + \alpha^6 \\ &= \alpha^3. \end{aligned}$$

$$\begin{aligned} S_4 = \mathrm{e}(\alpha^4) &= \alpha^2\alpha^{12} + \alpha^5\alpha^{20} \\ &= \alpha^0 + \alpha^4 \\ &= \alpha^5. \end{aligned}$$

Portanto, as síndromes de $e(X)$ e $r(X)$, quando calculadas para as raízes de $g(X)$, são exatamente as mesmas.

3.2.2 Localização de erro

De acordo com o padrão de erro, $e(X) = \sum_{i=0}^{n-1} e_i X^i$, para todo $e_i \neq 0$, então existe na posição i um erro cujo valor é e_i. A seguir, são apresentados novamente os valores dos erros e suas posições.

$$e(X) = 0 + 0X + 0X^2 + \alpha^2X^3 + 0X^4 + \alpha^5X^5 + 0X^6,$$

isto é,

$$e(X) = \alpha^2X^3 + \alpha^5X^5.$$

Note que existem dois erros: um na posição X^3 e outro na posição X^5, cujos valores são respectivamente α^2 e α^5. Dessa forma, para corrigir uma palavra recebida, cada valor de erro e_i e sua localização X_i, deve ser determinada.

Como as síndromes podem ser determinadas tanto a partir do polinômio recebido quanto por meio do polinômio de erro, então pode-se generalizar o sistema de equações que determinam os valores das síndromes da seguinte forma:

$$S_1 = r(\alpha) = e_0\alpha^0 + e_1\alpha^1 + \cdots + e_{n-1}\alpha^{n-1}$$

$$S_2 = r(\alpha^2) = e_0(\alpha^2)^0 + e_1(\alpha^2)^1 + \cdots + e_{n-1}(\alpha^2)^{n-1}$$

$$\vdots$$

$$S_{2t} = r(\alpha^{2t}) = e_0(\alpha^{2t})^0 + e_1(\alpha^{2t})^1 + \cdots + e_{n-1}(\alpha^{2t})^{n-1}.$$

Neste sistema de equações existem $2t$ incógnitas (t valores de erros e t posições de erros), e $2t$ equações simultâneas que não podem ser resolvidas pela forma usual por serem não lineares.

Qualquer técnica que resolva este sistema de equações é um algoritmo de decodificação Reed-Solomon.

Quando um vetor síndrome diferente de zero é calculado, significa que um erro foi recebido.

Inicialmente, é necessário determinar a posição do erro ou erros. Isso pode ser feito por meio de um polinômio localizador de erros pode ser definido como:

$$\sigma(X) = 1 + \sigma_1 X + \sigma_2 X^2 + \cdots + \sigma_t X^t.$$

Os recíprocos das raízes de $\sigma(X)$ revelam as posições de erros do padrão de erro $e(X)$.

Então, usando a técnica de modelagem auto-regressiva[1], pode-se formar uma matriz a partir das síndromes, onde as primeiras t síndromes são utilizadas para determinar as próximas síndromes.

$$\begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_{t-1} & S_t \\ S_2 & S_3 & S_4 & \cdots & S_t & S_{t+1} \\ \vdots & & & & & \\ S_{t-1} & S_t & S_{t+1} & \cdots & S_{2t-3} & S_{2t-2} \\ S_t & S_{t+1} & S_{t+2} & \cdots & S_{2t-2} & S_{2t-1} \end{bmatrix} \begin{bmatrix} \sigma_t \\ \sigma_{t-1} \\ \vdots \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -S_{t+1} \\ -S_{t+2} \\ \vdots \\ -S_{2t-1} \\ -S_{2t} \end{bmatrix}.$$

Aplica-se o modelo auto-regressivo pelo uso da matriz de maior dimensão que tem determinante não nulo.

Para o código RS $(7, 3)$ que está sendo considerado aqui, esta matriz é uma matriz 2×2, e o modelo é escrito como:

$$\begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix}$$

daí,

$$\begin{bmatrix} \alpha^2 & 0 \\ 0 & \alpha^3 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^3 \\ \alpha^5 \end{bmatrix} \Rightarrow \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^2 & 0 \\ 0 & \alpha^3 \end{bmatrix}^{-1} \begin{bmatrix} \alpha^3 \\ \alpha^5 \end{bmatrix}.$$

O inverso de uma matriz diagonal é a matriz formada pelo inverso de seus elementos. Assim,

[1] Um modelo auto-regressivo de ordem p tem a forma $Z_t = \phi_1 Z_{t-1} + \phi_2 Z_{t-2} + ... + \phi_p Z_{t-p} + a_t$, ou seja, $\phi(B)Z_t = a_t$ com o polinômio $\phi(B) = 1 + \phi_1 B - \phi_2 B^2 - ... - \phi_p B^p$.

$$\begin{bmatrix} \alpha^2 & 0 \\ 0 & \alpha^3 \end{bmatrix}^{-1} = \begin{bmatrix} \alpha^{-2} & 0 \\ 0 & \alpha^{-3} \end{bmatrix} = \begin{bmatrix} \alpha^5 & 0 \\ 0 & \alpha^4 \end{bmatrix}.$$

Verificação:

Se a inversão foi feita corretamente, então a multiplicação da matriz original pela matriz invertida deve resultar em uma matriz identidade. Com efeito,

$$\begin{bmatrix} \alpha^2 & 0 \\ 0 & \alpha^3 \end{bmatrix} \begin{bmatrix} \alpha^5 & 0 \\ 0 & \alpha^4 \end{bmatrix} = \begin{bmatrix} \alpha^2\alpha^5 + 0 \cdot 0 & \alpha^2 0 + 0\alpha^4 \\ 0\alpha^5 + \alpha^3 0 & 0 \cdot 0 + \alpha^3\alpha^4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Fazendo a substituição e efetuando a multiplicação, obtém-se:

$$\begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^5 & 0 \\ 0 & \alpha^4 \end{bmatrix} \begin{bmatrix} \alpha^5\alpha^3 & 0\alpha^5 \\ 0\alpha^3 & \alpha^4\alpha^5 \end{bmatrix} = \begin{bmatrix} \alpha \\ \alpha^2 \end{bmatrix}.$$

Agora, substituindo os resultados na forma do polinômio localizador, obtém-se:

$$\sigma(X) = 1 + \sigma_1 X + \sigma_2 X^2 = \alpha^0 + \alpha^2 X + \alpha X^2.$$

Como as raízes de $\sigma(X)$ são os recíprocos das posições de erros, o próximo passo é a determinação das raízes.

Testes exaustivos do polinômio $\sigma(X)$, com cada um dos elementos da extensão.

Qualquer elemento X que resulta em $\sigma(X) = 0$ é uma raiz, e permite localizar um erro.

$$\begin{array}{rcccccl}
\sigma(\alpha^0) & = & \alpha^0 + \alpha^2\alpha^0 + \alpha\alpha^0 & = & \alpha^0 + \alpha^2 + \alpha & = & \alpha^5 \\
\sigma(\alpha^1) & = & \alpha^0 + \alpha^2\alpha^1 + \alpha\alpha^2 & = & \alpha^0 + \alpha^3 + \alpha^3 & = & \alpha^0 \\
\sigma(\alpha^2) & = & \alpha^0 + \alpha^2\alpha^2 + \alpha\alpha^4 & = & \alpha^0 + \alpha^5 + \alpha^5 & = & 0 \\
\sigma(\alpha^3) & = & \alpha^0 + \alpha^2\alpha^3 + \alpha\alpha^6 & = & \alpha^0 + \alpha^5 + \alpha^0 & = & \alpha^5 \\
\sigma(\alpha^4) & = & \alpha^0 + \alpha^2\alpha^4 + \alpha\alpha^8 & = & \alpha^0 + \alpha^6 + \alpha^2 & = & 0 \\
\sigma(\alpha^5) & = & \alpha^0 + \alpha^2\alpha^5 + \alpha\alpha^{10} & = & \alpha^0 + \alpha^0 + \alpha^4 & = & \alpha^4 \\
\sigma(\alpha^6) & = & \alpha^0 + \alpha^2\alpha^6 + \alpha\alpha^{12} & = & \alpha^0 + \alpha + \alpha^6 & = & \alpha^4
\end{array}$$

De acordo com esses resultados, verifica-se que $\sigma(X)$ possui como raízes os elementos de campo α^2 e α^4.

As posições de erros X^i são reveladas pelo recíproco das raízes encontradas, ou seja:

$$\tfrac{1}{\alpha^2} = \alpha^5 \Rightarrow \text{posição } X^5,$$

$$\tfrac{1}{\alpha^4} = \alpha^3 \Rightarrow \text{posição } X^3.$$

Consequentemente, o polinômio padrão de erro já pode ser escrito com as posições de erros reveladas, ou seja,

$$\hat{e}(X) = e_3X^3 + e_5X^5,$$

em que $\hat{e}(X)$ denota o polinômio de erro estimado.

Note que duas das quatro incógnitas foram determinadas, isto é, as duas posições de erros. Resta determinar as outras duas incógnitas que são os valores dos erros.

3.2.3 Valores dos erros

Para a determinação dos valores dos erros e_3 e e_5, quaisquer duas das quatro equações de síndrome podem ser usadas.

Da generalização do sistema de equações para determinar os valores das síndromes S_1 e S_2 obtém-se:

$$S_1 = r(\alpha) = e_3\alpha^3 + e_5\alpha^5 = \alpha^2,$$
$$S_2 = r(\alpha^2) = e_3\alpha^6 + e_5\alpha^{10} = \alpha^2.$$

Escrevendo na forma matricial, obtém-se:

$$\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix} \begin{bmatrix} e^3 \\ e^5 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ 0 \end{bmatrix},$$

que pode ser reescrita como:

$$\begin{bmatrix} e^3 \\ e^5 \end{bmatrix} = \begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix}^{-1} \begin{bmatrix} \alpha^2 \\ 0 \end{bmatrix},$$

a fim de facilitar a determinação dos valores de e_3 e de e_5.

A matriz a ser invertida não é uma matriz diagonal.

Para uma matriz $[A]$ sua inversa pode ser determinada como:

$$Inv[A] = \frac{\left[cofator[A]\right]^T}{det[A]}.$$

$$Inv \begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix} = \frac{\left[cofator \begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix}\right]^T}{det \begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix}} = \frac{\begin{bmatrix} \alpha^{10} & \alpha^6 \\ \alpha^5 & \alpha^3 \end{bmatrix}^T}{\alpha^3\alpha^{10} - \alpha^6\alpha^5}.$$

$$Inv \begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix} = \frac{\begin{bmatrix} \alpha^{10} & \alpha^5 \\ \alpha^6 & \alpha^3 \end{bmatrix}}{\alpha^6 + \alpha^4} = \frac{\begin{bmatrix} \alpha^{10} & \alpha^5 \\ \alpha^6 & \alpha^3 \end{bmatrix}}{\alpha^3}.$$

$$Inv \begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix} = \alpha^{-3} \begin{bmatrix} \alpha^{10} & \alpha^5 \\ \alpha^6 & \alpha^3 \end{bmatrix} = \alpha^4 \begin{bmatrix} \alpha^{10} & \alpha^5 \\ \alpha^6 & \alpha^3 \end{bmatrix} = \begin{bmatrix} \alpha^0 & \alpha^2 \\ \alpha^3 & \alpha^0 \end{bmatrix}.$$

Verificação:
Se a inversão foi feita corretamente, então a multiplicação da matriz original pela matriz invertida deve resultar em uma matriz identidade. De fato,

$$\begin{bmatrix} \alpha^{10} & \alpha^5 \\ \alpha^6 & \alpha^3 \end{bmatrix} \begin{bmatrix} \alpha^0 & \alpha^2 \\ \alpha^3 & \alpha^0 \end{bmatrix} = \begin{bmatrix} \alpha^3\alpha^0 + \alpha^5\alpha^3 & \alpha^3\alpha^2 + \alpha^5\alpha^0 \\ \alpha^6\alpha^0 + \alpha^{10}\alpha^3 & \alpha^6\alpha^2 + \alpha^{10}\alpha^0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Para os valores de erros, obtém-se:

$$\begin{bmatrix} e_3 \\ e_5 \end{bmatrix} = \begin{bmatrix} \alpha^0 & \alpha^2 \\ \alpha^3 & \alpha^0 \end{bmatrix} \begin{bmatrix} \alpha^2 \\ \alpha^0 \end{bmatrix} = \begin{bmatrix} \alpha^0\alpha^2 + \alpha^2 0 \\ \alpha^3\alpha^2 + \alpha^0 0 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ \alpha^5 \end{bmatrix}.$$

O polinômio padrão de erro pode ser escrito com as posições de erros e os valores dos erros definidos, isto é,

$$\hat{e}(X) = \alpha^2 X^3 + \alpha^5 X^5.$$

3.2.4 Correção do polinômio recebido com o polinômio de erro estimado

O polinômio transmitido estimado é obtido fazendo:

$$\hat{c}(X) = r(X) + \hat{e}(X).$$

Como $r(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^0 X^3 + \alpha^1 X^4 + \alpha^2 X^5 + \alpha^5 X^6$
e $\hat{e}(X) = 0 + 0X + 0X^2 + \alpha^2 X^3 + 0X^4 + \alpha^5 X^5 + 0X^6$
=
segue que $\hat{c}(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6$.

Os símbolos mensagem constituem os $k = 3$ símbolos mais a direita do polinômio, então a mensagem decodificada é:

$$\underbrace{010}_{\alpha^1} \ \underbrace{110}_{\alpha^3} \ \underbrace{111}_{\alpha^5}.$$

4 *Detalhamento de algumas situações envolvendo códigos Reed-Solomon*

Neste capítulo será apresentado o detalhamento de algumas situações envolvendo códigos Reed-Solomon, por meio da codificação de uma mensagem a ser enviada a um destinatário e o cálculo das síndromes de um vetor recebido por um receptor. O objetivo é, por meio da resolução detalhada do exemplo, apresentar os conceitos teóricos envolvendo os códigos Reed-Solomon, apresentados no Capítulo 3, além de apresentar as principais contribuições das estruturas algébricas nessa importante área de pesquisa, os códigos corretores de erros, em particular os códigos Reed-Solomon.

4.1 Detalhamento de um Exemplo Envolvendo Códigos Reed-Solomon

Considere o código Reed-Solomon RS$(7, 3)$, gerado a partir do corpo apresentado na Tabela 7.

Tabela 7 – $GF(2^3)$ gerado por $p(x) = 1 + x + x^3$.

Representações		
Potência	**Polinomial**	**Vetorial**
0	0	(000)
$\alpha^0 = 1$	1	(100)
α	α	(010)
α^2	α^2	(001)
α^3	$1 + \alpha$	(110)
α^4	$\alpha + \alpha^2$	(011)
α^5	$1 + \alpha + \alpha^2$	(111)
α^6	$1 + \alpha^2$	(101)

(a) Codificação da mensagem $m(X) = 1 + \alpha X + \alpha^2 X^2$.

(b) As síndromes para o vetor recebido

$$r(X) = \alpha^0 + \alpha^2 X + \alpha^3 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^0 X^5 + \alpha^5 X^6.$$

Os itens (a) e (b) serão resolvidos a seguir, como forma de aplicar os conceitos teóricos apresentados no Capítulo 3, além de explicitar como a álgebra está presente nesse processo de construção, por meio do detalhamento dos cálculos.

(a) O polinômio gerador para um código RS é da seguinte forma:

$$g(X) = g_0 + g_1 X + g_2 X^2 + ... + g_{2t-1} X^{2t-1} + X^{2t}.$$

Desse modo, o polinômio gerador $g(X)$ pode ser obtido fazendo:

$$g(X) = (X - \alpha)(X - \alpha^2) \cdots (X - \alpha^{2t}),$$

em que α, α^2, ..., α^{2t} são as raízes do polinômio.

Para o código RS $(7, 3)$ com capacidade de correção de duplo erro de símbolo, o polinômio gerador em termos de suas quatro raízes, uma vez que, $2t = n - k = 7 - 3 = 4$, é descrito da seguinte forma:

$$\begin{aligned} g(X) &= (X - \alpha)(X - \alpha^2)(X - \alpha^3)(X - \alpha^4) \\ &= (X^2 - (\alpha + \alpha^2)X + \alpha^3)(X^2 - (\alpha^3 + \alpha^4)X + \alpha^7) \\ &= (X^2 - \alpha^4 X + \alpha^3)(X^2 - \alpha^6 X + \alpha^0) \\ &= X^4 - (\alpha^4 + \alpha^6)X^3 + (\alpha^3 + \alpha^{10} + \alpha^0)X^2 - (\alpha^4 + \alpha^9)X + \alpha^3 \\ &= X^4 - \alpha^3 X^3 + \alpha^0 X^2 - \alpha^1 X + \alpha. \end{aligned}$$

Escrevendo o polinômio da ordem mais baixa para a mais alta, e trocando os sinais negativos por positivos, $g(X)$ pode ser escrito como:

$$g(X) = \alpha + \alpha^1 X + \alpha^0 X^2 + \alpha^3 X^3 + X^4.$$

Codificação na forma sistemática

$$X^{n-k} m(X) = q(X)g(X) + p(X),$$

onde $q(X)$ e $p(X)$ são os polinômios quociente e resto, da divisão da mensagem deslocada de $n - k$ posições, $X^{n-k}m(X)$, pelo polinômio gerador, $g(X)$.

Na forma sistemática, o polinômio resto, $p(X)$, é o polinômio paridade da palavra código.

Para o código RS$(7, 3)$ e considerando a mensagem $m(X) = 1 + \alpha X + \alpha^2 X^2$, a mensagem deslocada de $n-k$ posições, $X^{n-k}m(X)$, pode ser obtida fazendo a multiplicação de $m(X) = 1 + \alpha X + \alpha^2 X^2$ por X^4, uma vez que, $X^{n-k} = X^{7-3} = X^4$. Assim,

$$X^4(1 + \alpha X + \alpha^2 X^2) = X^4 + \alpha X^5 + \alpha^2 X^6.$$

Como o polinômio paridade, $p(X)$, é o resto da divisão do polinômio deslocado, $X^{n-k}m(X)$, por $g(X)$, segue que

$$p(X) = X^{n-k} m(X) \mod g(X).$$

A divisão polinomial deve ser feita em $GF(2^3)$, ou seja, deve obedecer as regras das duas operações aritméticas possíveis sobre $GF(2^3)$: a adição e a multiplicação, apresentadas nas Tabelas 4 e 5.

Realizando a divisão polinomial do polinômio $X^{n-k}m(X) = \alpha^2X^6 + \alpha X^5 + \alpha^0X^4$ pelo polinômio $g(X) = \alpha^0X^4 + \alpha^3X^3 + \alpha^0X^2 + \alpha^1X + \alpha^3$ obtemos o quociente $q(X) = \alpha^2X^2 + \alpha^6X + \alpha^0$ e resto $p(X) = \alpha^6X^3\alpha^5X^2 + \alpha^4X + \alpha^3$.

A palavra-código na forma polinomial resulta em:

$$c(X) = p(X) + X^{n-k}m(X),$$

ou seja,

$$c(X) = (\alpha^3 + \alpha^4X + \alpha^5X^2 + \alpha^6X^3) + (\alpha^0X^4 + \alpha X^5 + \alpha^2X^6),$$

$$c(X) = \alpha^3 + \alpha^4X + \alpha^5X^2 + \alpha^6X^3 + \alpha^0X^4 + \alpha X^5 + \alpha^2X^6.$$

Codificação na forma sistemática com registradores de deslocamento de $(n-k)$ estágios

O esquema apresentado a seguir na Tabela 8, retrata o processo de codificação RS na forma sistemática, tomando como referência o caso apresentado no Capítulo 3, adaptado para o caso que está sendo estudado neste capítulo.

Tabela 8 – Codificação Reed-Solomon.

Fila de entrada	Ciclos *clock*	Conteúdo dos registradores	Realimentação	Fila de saída
α^0 α^1 α^2	0	0 0 0 0	α^2	α^2
α^0 α^1	1	α^5 α^3 α^2 α^5	α^6	$\alpha^1\alpha^2$
α^0	2	α^2 α^4 α^4 0	α^0	$\alpha^0\alpha^1\alpha^2$
–	3	α^3 α^4 α^5 α^6	0	$\alpha^6\alpha^0\alpha^1\alpha^2$
–	4	0 α^3 α^4 α^5	0	$\alpha^5\alpha^6\alpha^0\alpha^1\alpha^2$
–	5	0 0 α^3 α^4	0	$\alpha^4\alpha^5\alpha^6\alpha^0\alpha^1\alpha^2$
–	6	0 0 0 α^3	0	$\alpha^3\alpha^4\alpha^5\alpha^6\alpha^0\alpha^1\alpha^2$
–	7	0 0 0 0	0	$-\alpha^3\alpha^4\alpha^5\alpha^6\alpha^0\alpha^1\alpha^2$

1. No ciclo *clock* 0, o conteúdo dos registrador é todo nulo, ou seja, 0 0 0 0, conforme apresentado na Figura 12.

2. No ciclo *clock* 1, entrou α^2. Logo, tem-se as seguintes operações:

   $\alpha^2 \cdot \alpha^3 = \alpha^5$

   $\alpha^2 \cdot \alpha^1 = \alpha^3$; $\qquad \alpha^3 + 0 = \alpha^3$

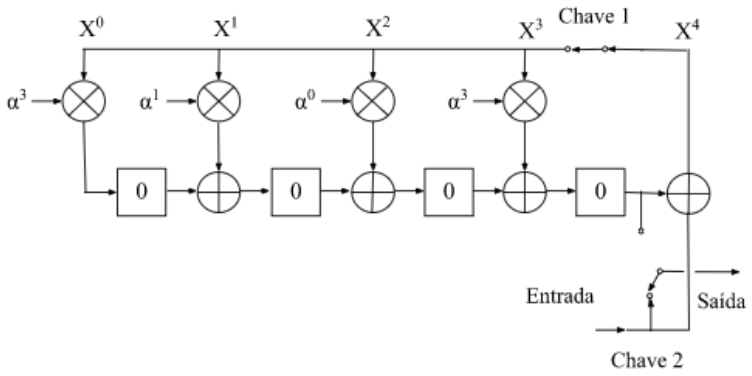

Figura 12 – Ciclo *clock* 0.
FONTE: do autor.

$\alpha^2 \cdot \alpha^0 = \alpha^2$; $\alpha^2 + 0 = \alpha^2$
$\alpha^2 \cdot \alpha^3 = \alpha^5$; $\alpha^5 + 0 = \alpha^5$
Assim, o conteúdo do registrador é: $\alpha^5 \quad \alpha^3 \quad \alpha^2 \quad \alpha^5$, conforme apresentado na Figura 13.

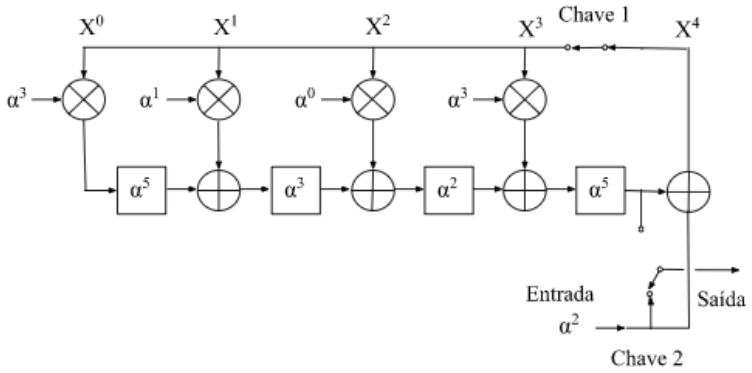

Figura 13 – Ciclo *clock* 1.
FONTE: do autor.

3. No ciclo *clock* 2, entrou α^6. Logo, tem-se as seguintes operações:

   $\alpha^6 \cdot \alpha^3 = \alpha^2$
   $\alpha^6 \cdot \alpha^1 = \alpha^0$; $\alpha^0 + \alpha^5 = \alpha^4$
   $\alpha^6 \cdot \alpha^0 = \alpha^6$; $\alpha^6 + \alpha^3 = \alpha^4$
   $\alpha^6 \cdot \alpha^3 = \alpha^2$; $\alpha^2 + \alpha^2 = 0$
   Assim, o conteúdo do registrador é: $\alpha^2 \quad \alpha^4 \quad \alpha^4 \quad 0$, conforme apresentado na Figura 14.

4. No ciclo *clock* 3, entrou α^0. Logo, tem-se as seguintes operações:

   $\alpha^0 \cdot \alpha^3 = \alpha^3$
   $\alpha^0 \cdot \alpha^1 = \alpha^1$; $\alpha^1 + \alpha^2 = \alpha^4$

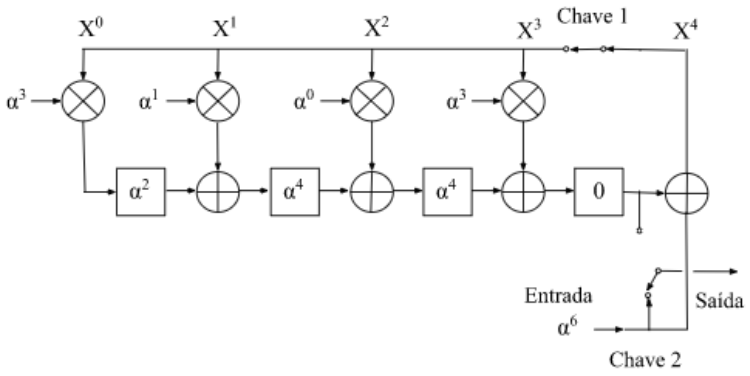

Figura 14 – Ciclo *clock* 2.
FONTE: do autor.

$\alpha^0 \cdot \alpha^0 = \alpha^0$; $\alpha^0 + \alpha^4 = \alpha^5$
$\alpha^0 \cdot \alpha^3 = \alpha^3$; $\alpha^3 + \alpha^4 = \alpha^6$

Assim, o conteúdo do registrador é: $\alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6$, conforme apresentado na Figura 15.

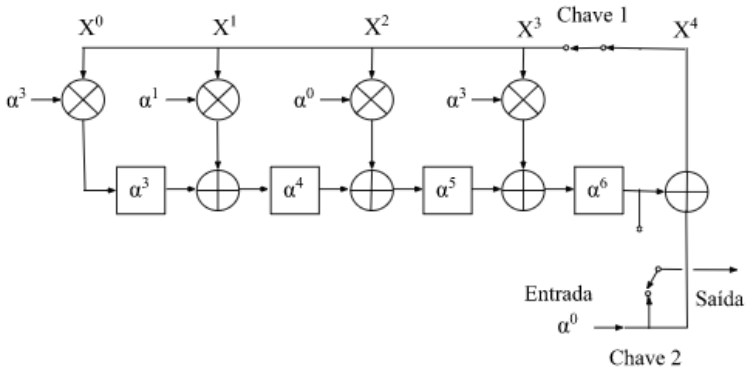

Figura 15 – Ciclo *clock* 3.
FONTE: do autor.

5. No ciclo *clock* 4, entrou 0. Logo, tem-se as seguintes operações:

   $0 \cdot \alpha^3 = 0$
   $0 \cdot \alpha^1 = 0$; $0 + \alpha^3 = \alpha^3$
   $0 \cdot \alpha^0 = 0$; $0 + \alpha^4 = \alpha^4$
   $0 \cdot \alpha^3 = 0$; $0 + \alpha^5 = \alpha^5$

   Assim, o conteúdo do registrador é: $0 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5$, conforme apresentado na Figura 16.

6. No ciclo *clock* 5, entrou 0. Logo, tem-se as seguintes operações:

   $0 \cdot \alpha^3 = 0$
   $0 \cdot \alpha^1 = 0$; $0 + 0 = 0$

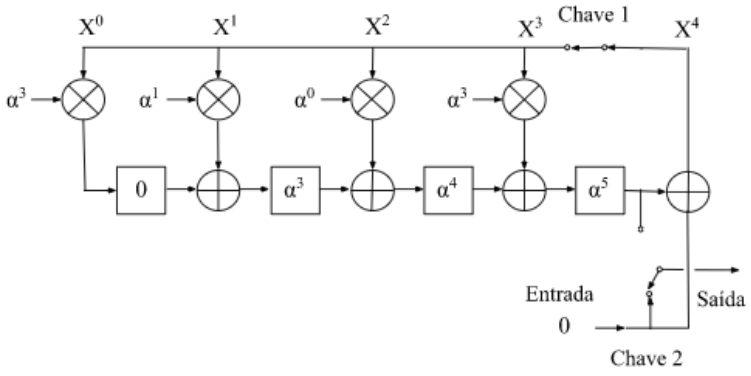

Figura 16 – Ciclo *clock* 4.
FONTE: do autor.

$0 \cdot \alpha^0 = 0; \qquad 0 + \alpha^3 = \alpha^3$
$0 \cdot \alpha^3 = 0; \qquad 0 + \alpha^4 = \alpha^4$

Assim, o conteúdo do registrador é: 0 0 α^3 α^4, conforme apresentado na Figura 17.

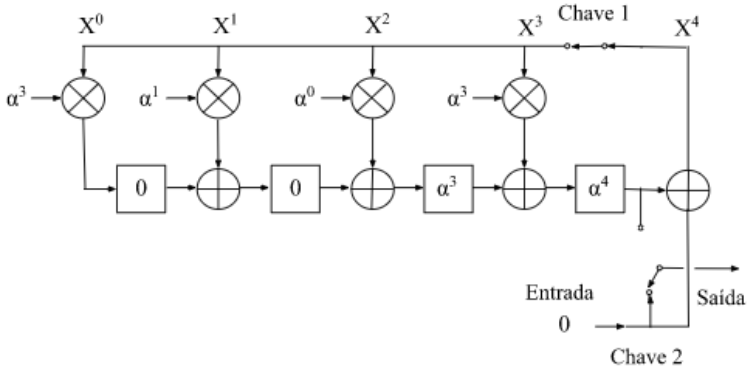

Figura 17 – Ciclo *clock* 5.
FONTE: do autor.

7. No ciclo *clock* 6, entrou 0. Logo, tem-se as seguintes operações:

   $0 \cdot \alpha^3 = 0$
   $0 \cdot \alpha^1 = 0; \qquad 0 + 0 = 0$
   $0 \cdot \alpha^0 = 0; \qquad 0 + 0 = 0$
   $0 \cdot \alpha^3 = 0; \qquad 0 + \alpha^3 = \alpha^3$

   Assim, o conteúdo do registrador é: 0 0 0 α^3, conforme apresentado na Figura 18.

8. No ciclo *clock* 7, entrou 0. Logo, tem-se as seguintes operações:

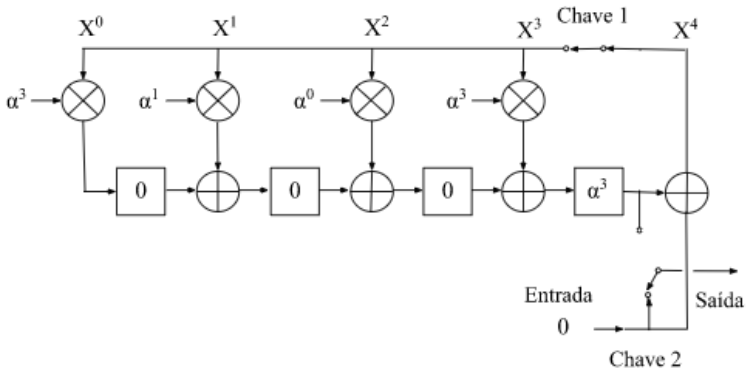

Figura 18 – Ciclo *clock* 6.
FONTE: do autor.

$0 \cdot \alpha^3 = 0$
$0 \cdot \alpha^1 = 0; \qquad 0 + 0 = 0$
$0 \cdot \alpha^0 = 0; \qquad 0 + 0 = 0$
$0 \cdot \alpha^3 = 0; \qquad 0 + 0 = 0$

Assim, o conteúdo do registrador é: 0 0 0 0, conforme apresentado na Figura 19.

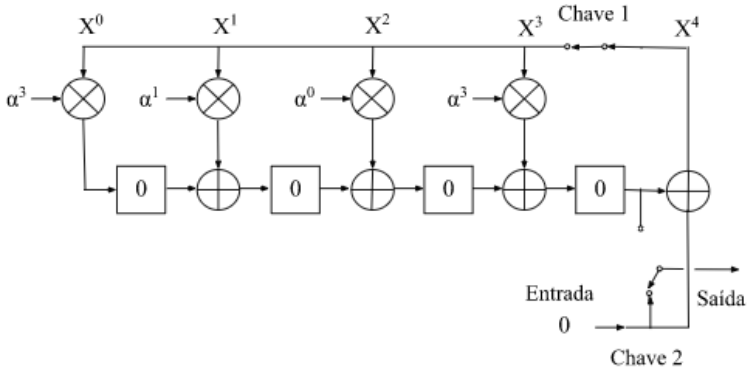

Figura 19 – Ciclo *clock* 7.
FONTE: do autor.

Na forma polinomial a fila de saída pode ser escrita como:

$$c(X) = \alpha^3 + \alpha^4 X + \alpha^5 X^2 + \alpha^6 X^3 + \alpha^0 X^4 + \alpha^1 X^5 + \alpha^2 X^6.$$

As raízes do polinômio gerador $g(X)$ devem ser também raízes da palavra código gerada por $g(X)$, porque uma palavra válida atende a seguinte condição:

$$c(X) = m(X)g(X).$$

Assim, uma palavra código arbitrária quando calculada para qualquer raiz de $g(X)$, deve resultar em zero, ou seja,

$$c(\alpha) = c(\alpha^2) = c(\alpha^3) = c(\alpha^4) = 0.$$

$$\begin{aligned}
c(\alpha) &= \alpha^3 + \alpha^4\alpha + \alpha^5(\alpha^1)^2 + \alpha^6(\alpha^1)^3 + \alpha^0(\alpha^1)^4 + \alpha^1(\alpha^1)^5 + \alpha^2(\alpha^1)^6 \\
&= \alpha^3 + \alpha^4\alpha + \alpha^5\alpha^2 + \alpha^6\alpha^3 + \alpha^0\alpha^4 + \alpha^1\alpha^5 + \alpha^2\alpha^6 \\
&= \alpha^3 + \alpha^5 + \alpha^7 + \alpha^9 + \alpha^4 + \alpha^6 + \alpha^8 \\
&= \alpha^3 + \alpha^5 + \alpha^0 + \alpha^2 + \alpha^4 + \alpha^6 + \alpha^1 \\
&= \alpha^2 + \alpha^6 + \alpha^3 + \alpha^1 \\
&= \alpha^0 + \alpha^0 \\
&= 0.
\end{aligned}$$

$$\begin{aligned}
c(\alpha^2) &= \alpha^3 + \alpha^4\alpha^2 + \alpha^5(\alpha^2)^2 + \alpha^6(\alpha^2)^3 + \alpha^0(\alpha^2)^4 + \alpha^1(\alpha^2)^5 + \alpha^2(\alpha^2)^6 \\
&= \alpha^3 + \alpha^4\alpha^2 + \alpha^5\alpha^4 + \alpha^6\alpha^6 + \alpha^0\alpha^8 + \alpha^1\alpha^8 + \alpha^2\alpha^{12} \\
&= \alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12} + \alpha^8 + \alpha^{11} + \alpha^{14} \\
&= \alpha^3 + \alpha^6 + \alpha^2 + \alpha^5 + \alpha^1 + \alpha^4 + \alpha^0 \\
&= \alpha^4 + \alpha^3 + \alpha^2 + \alpha^0 \\
&= \alpha^6 + \alpha^6 \\
&= 0.
\end{aligned}$$

$$\begin{aligned}
c(\alpha^3) &= \alpha^3 + \alpha^4\alpha^3 + \alpha^5(\alpha^3)^2 + \alpha^6(\alpha^3)^3 + \alpha^0(\alpha^3)^4 + \alpha^1(\alpha^3)^5 + \alpha^1(\alpha^3)^6 \\
&= \alpha^3 + \alpha^4\alpha^3 + \alpha^5\alpha^6 + \alpha^6\alpha^9 + \alpha^0\alpha^{12} + \alpha^1\alpha^{15} + \alpha^2\alpha^{18} \\
&= \alpha^3 + \alpha^7 + \alpha^{11} + \alpha^{15} + \alpha^{12} + \alpha^{16} + \alpha^{20} \\
&= \alpha^3 + \alpha^0 + \alpha^4 + \alpha^1 + \alpha^5 + \alpha^2 + \alpha^6 \\
&= \alpha^1 + \alpha^2 + \alpha^3 + \alpha^6 \\
&= \alpha^4 + \alpha^4 \\
&= 0.
\end{aligned}$$

$$\begin{aligned}
c(\alpha^4) &= \alpha^3 + \alpha^4\alpha^4 + \alpha^5(\alpha^4)^2 + \alpha^6(\alpha^4)^3 + \alpha^0(\alpha^4)^4 + \alpha^1(\alpha^4)^5 + \alpha^2(\alpha^4)^6 \\
&= \alpha^3 + \alpha^4\alpha^4 + \alpha^5\alpha^8 + \alpha^6\alpha^{12} + \alpha^0\alpha^{16} + \alpha^1\alpha^{20} + \alpha^2\alpha^{24} \\
&= \alpha^3 + \alpha^8 + \alpha^{13} + \alpha^{18} + \alpha^{16} + \alpha^{21} + \alpha^{26} \\
&= \alpha^3 + \alpha^1 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha^0 + \alpha^5 \\
&= \alpha^0 + \alpha^3 + \alpha^6 + \alpha^5 \\
&= \alpha^1 + \alpha^1 \\
&= 0.
\end{aligned}$$

(b) Para o código RS $(7, 3)$, cada vetor síndrome possui quatro símbolos.

A síndrome, S_i, pode ser determinada calculando-se $r(X)$ para as raízes de $g(X)$, ou seja,

$$S_i = r(X); \;\; X = \alpha^i,$$

$$S_i = r(\alpha^i); \;\; i = 1, ..., n-k.$$

Se $r(X)$ não contiver erros, então cada uma das síndromes S_i será igual a zero.

Para o polinômio recebido $r(X) = \alpha^0 + \alpha^2 X + \alpha^3 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^0 X^5 + \alpha^5 X^6$, os quatro símbolos da síndrome são:

$$\begin{aligned}
S_1 = r(\alpha^1) &= \alpha^0 + \alpha^2\alpha^1 + \alpha^3(\alpha^1)^2 + \alpha^6(\alpha^1)^3 + \alpha^1(\alpha^1)^4 + \alpha^0(\alpha^1)^5 + \alpha^5(\alpha^1)^6 \\
&= \alpha^0 + \alpha^2\alpha^1 + \alpha^3\alpha^2 + \alpha^6\alpha^3 + \alpha^1\alpha^4 + \alpha^0\alpha^5 + \alpha^5\alpha^6 \\
&= \alpha^0 + \alpha^3 + \alpha^5 + \alpha^2 + \alpha^5 + \alpha^5 + \alpha^4 \\
&= \alpha^1 + \alpha^3 + 0 + \alpha^4 \\
&= \alpha^0 + \alpha^4 \\
&= \alpha^5.
\end{aligned}$$

$$\begin{aligned}
S_2 = r(\alpha^2) &= \alpha^0 + \alpha^2\alpha^2 + \alpha^3(\alpha^2)^2 + \alpha^6(\alpha^2)^3 + \alpha^1(\alpha^2)^4 + \alpha^0(\alpha^2)^5 + \alpha^5(\alpha^2)^6 \\
&= \alpha^0 + \alpha^2\alpha^2 + \alpha^3\alpha^4 + \alpha^6\alpha^6 + \alpha^1\alpha^8 + \alpha^0\alpha^{10} + \alpha^5\alpha^{12} \\
&= \alpha^0 + \alpha^2\alpha^2 + \alpha^3\alpha^4 + \alpha^6\alpha^6 + \alpha^1\alpha^1 + \alpha^0\alpha^3 + \alpha^5\alpha^5 \\
&= \alpha^0 + \alpha^4 + \alpha^0 + \alpha^5 + \alpha^2 + \alpha^3 + \alpha^3 \\
&= \alpha^5 + \alpha^4 + \alpha^5 + \alpha^3 \\
&= \alpha^0 + \alpha^2 \\
&= \alpha^6.
\end{aligned}$$

$$\begin{aligned}
S_3 = r(\alpha^3) &= \alpha^0 + \alpha^2\alpha^3 + \alpha^3(\alpha^3)^2 + \alpha^6(\alpha^3)^3 + \alpha^1(\alpha^3)^4 + \alpha^0(\alpha^3)^5 + \alpha^5(\alpha^3)^6 \\
&= \alpha^0 + \alpha^2\alpha^3 + \alpha^3\alpha^6 + \alpha^6\alpha^9 + \alpha^1\alpha^{12} + \alpha^0\alpha^{15} + \alpha^5\alpha^{18} \\
&= \alpha^0 + \alpha^2\alpha^3 + \alpha^3\alpha^6 + \alpha^6\alpha^2 + \alpha^1\alpha^5 + \alpha^0\alpha^1 + \alpha^5\alpha^4 \\
&= \alpha^0 + \alpha^5 + \alpha^2 + \alpha^1 + \alpha^6 + \alpha^1 + \alpha^2 \\
&= \alpha^4 + \alpha^4 + \alpha^5 + \alpha^1 \\
&= 0 + \alpha^3 \\
&= \alpha^3.
\end{aligned}$$

$$
\begin{aligned}
S_4 = r(\alpha^4) &= \alpha^0 + \alpha^2\alpha^4 + \alpha^3(\alpha^4)^2 + \alpha^6(\alpha^4)^3 + \alpha^1(\alpha^4)^4 + \alpha^0(\alpha^4)^5 + \alpha^5(\alpha^4)^6 \\
&= \alpha^0 + \alpha^2\alpha^4 + \alpha^3\alpha^8 + \alpha^6\alpha^{12} + \alpha^1\alpha^{16} + \alpha^0\alpha^{20} + \alpha^5\alpha^{24} \\
&= \alpha^0 + \alpha^2\alpha^4 + \alpha^3\alpha^1 + \alpha^6\alpha^5 + \alpha^1\alpha^2 + \alpha^0\alpha^6 + \alpha^5\alpha^3 \\
&= \alpha^0 + \alpha^6 + \alpha^4 + \alpha^4 + \alpha^3 + \alpha^6 + \alpha^1 \\
&= \alpha^2 + 0 + \alpha^4 + \alpha^2 \\
&= \alpha^2 + \alpha^2 \\
&= 0.
\end{aligned}
$$

4.2 Algumas Contribuições da Álgebra no Estudo dos Códigos Reed-Solomon

Percebe-se a importância da álgebra no processo de construção de códigos corretores de erros. Em particular, neste capítulo foram apresentadas duas situações, envolvendo a codificação de uma mensagem a ser enviada para um destinatário, além dos cálculos das síndromes associadas a um vetor recebido por um destinatário.

Nesta construção foi utilizada a extensão do corpo $GF(2^3)$, as tabelas relacionadas às operações de soma e produto dessa extensão, além de representações polinomiais, vetoriais e por potência. No entanto, para se entender todo esse processo fpi necessário um estudo das estruturas básicas de grupos e anéis e a aritmética modular associada a essas estruturas. Além disso, em outras situações podem ser utilizadas outras extensões de corpos, a depender da especificidade do problema.

Ao analisar os códigos corretores de erros, faz-se uso de diversos elementos de álgebra linear, desde a representação matricial, passando pelo cálculo de determinantes, sistemas lineares, espaços vetoriais, subespaços vetoriais, combinações lineares, dependência linear, entre outros, conforme pode ser observado no detalhamento da codificação e decodificação de códigos Reed-Solomon, apresentado no Capítulo 3.

Portanto, com o estudo e construção deste trabalho foi possível identificar diversas aplicações da álgebra no estudo dos códigos corretores de erros, em particular, os códigos Reed-Solomon.

5 *Considerações finais*

Durante o processo de transmissão da informação em um sistema de comunicação, podem ocorrer interferências que comprometem o recebimento correto da informação enviada de uma fonte a um destinatário. Como forma de detectar e em muitos casos efetuar a correção dos erros ocorridos na transmissão da informação, os códigos corretores de erros (CCE's) tem uma grande relevância. Uma importante classe de códigos corretores de erros são os códigos BCH, com uma estrutura algébrica forte presente em sua construção, além de apresentar uma simplicidade nos processos de codificação e decodificação. Os códigos Reed-Solomon (RS), uma subclasse dos códigos BCH, são códigos q-ários com notável capacidade de correção de erros e muito utilizados em diversos sistemas de armazenamento e transmissão de dados, transmissão de sinais digitais de TV e discos rígidos.

Com a realização deste trabalho, foi possível analisar relações existentes entre a Álgebra e Engenharia, ou seja, como as estruturas algébricas podem ser aplicadas no processo de construção dos códigos corretores de erros, em particular, os códigos Reed-Solomon. Além disso, foi possível efetuar os cálculos de alguns exemplos envolvendo os processos de codificação e decodificação dos códigos Reed-Solomon. Como proposta futura e incentivo a futuros trabalhos na área, sugere-se a realização de uma análise, por meio de situações-problema envolvendo as principais aplicações dos códigos Reed-Solomon.

Ademais, vale ressaltar que, com a realização deste trabalho, foi possível perceber que a teoria dos códigos corretores de erros, em particular, os códigos Reed-Solomon, é um tema de vital importância, visto que apresenta possibilidades de aplicação em diversos sistemas de armazenamento e transmissão de informação, e que, normalmente, não faz parte da grade curricular de um curso de Matemática - Licenciatura. Além disso, permitiu o aprimoramento na elaboração da escrita científica e a possibilidade de participação em eventos da área. Este trabalho foi motivado a partir de uma iniciação científica realizada com outras colegas, sob orientação do mesmo orientador, intitulada *"Estruturas algébricas utilizadas na construção de códigos BCH e aplicações em estudos mutacionais"*, a qual possibilitou a participação em diversos eventos da área, como o caso do Congresso Nacional de Matemática Aplicada e Computacional (CNMAC), por exemplo, com a apresentação e publicação de um resumo nos Anais do evento, com o trabalho intitulado *"Extensão de Galois $GF(2^5)$ aplicada na obtenção de um polinômio gerador em um código BCH"*, com a finalidade de apresentar a construção do polinômio gerador de um código BCH com capacidade de correção de cinco erros ($t = 5$) a partir da extensão $GF(2^5)$, gerada pelo polinômio primitivo $p(X) = 1 + X^2 + X^5$.

Referências

[1] LIN, S.; COSTELLO, D. J. Jr. **Error Control Coding.** 2 ed. Prentice Hall, 2004.

[2] CAMPELO, D. G. 95f. **Decodificação de Códigos Não Sistemáticos de Reed-Solomon.** Dissertação (Mestrado em Matemática Aplicada). Universidade Federal do Rio Grande do Sul. Porto Alegre, 2012.

[3] PIAI, T. G. 66f. **Código Corretor de Erro para Telemetria de Foguetes de Sondagem**. Trabalho de Conclusão de Curso (Bacharelado em Engenharia Elétrica). Universidade Estadual de Londrina. Londrina, 2018.

[4] SILVA, A. H. L.; RODOLFO, T. A. 67f. **Implementação de uma Arquitetura Reed-Solomon para uso em Redes OTN 10.7 Gbps**. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Computação). Porto Alegre, 2007.

[5] SINGH, Dr. **Error Detection and Correction Using Reed Solomon Codes**. 3 ed. Uday, 2013.

[6] ZANITTI, D. B. C; BENEDITO, C. W. O. **Códigos Reed-Solomon para Correção de Erros em Rajada**. Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 7, n. 1, 2020.

[7] OLIVEIRA, A. N. 87f. **Códigos BCH Aplicados no Processo de Análise de Fenômenos Mutacionais.** Dissertação (Mestrado em Estatística Aplicada e Biometria). Universidade Federal de Alfenas. Alfenas, 2020.

[8] DOMINGUES, H. H. **Álgebra Moderna**. 4 ed. ref. São Paulo: Atual, 2003.

[9] FRALEIGH, J.B. **A First Course in Abstract Algebra**. Addison Wesley, 2003.