4 CÓDIGOS REED-SOLOMON

Neste capítulo retornamos aos códigos de blocos lineares por meio dos códigos Reed-Solomon (RS). Isso se deve ao fato de que os Códigos RS são códigos largamente empregados em diversos sistemas de armazenamento e transmissão de informação, entre os quais podemos citar: gravação de músicas em CD, gravação de dados em fitas magnéticas, gravação de dados em discos rígidos, transmissão de sinais digitais de TV nos padrões ATSC, DVB-T e ISDB-T, etc.

Ao contrário dos outros códigos de bloco e também dos códigos convolucionais, os códigos convolucionais, os códigos RS possuem uma razoável capacidade de correção de erros em rajada. Por isso, muito freqüentemente ele é usado de forma concatenada com outros códigos, tais como os códigos convolucionais.

Para facilitar o entendimento dos códigos RS, este capítulo está dividido em seções que abordam os seguintes tópicos:

- Campos Finitos;
- Codificação RS e
- Decodificação RS.

4.1. INTRODUÇÃO

Os códigos Reed-Solomon (RS) são códigos cíclicos não binários com símbolos formados por seqüências de m bits, onde m é qualquer positivo inteiro tendo valor maior do que 2. Os códigos RS com símbolos de m bits existem para todo n e k para o qual

$$0 < k < n < 2^m + 2 \tag{4.1}$$

onde 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 mais comuns estão apresentadas na Tabela 4.1. Esses códigos, além de uma notável capacidade de correção de erros, são particularmente úteis para correção de rajada de erros. Os códigos RS são extensamente utilizados em diversos sistemas de comunicações concatenados, principalmente, com códigos convolucionais além de outros sistemas de armazenamento de informações.

Tabela 4.1 - Principais características dos códigos RS mais comuns.

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[1]:	$t = \left\lfloor \frac{n-k}{2} \right\rfloor$

A probabilidade de erro de símbolo, P_E, em função da probabilidade de erro de símbolo do canal, p, pode ser escrita como:

$$P_E \approx \frac{1}{2^m - 1} \sum_{j=t+1}^{2^m-1} j \binom{2^m - 1}{j} p^j (1-p)^{2^m - 1 - j} \tag{4.2}$$

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

A capacidade de correção de erro em rajada pode ser entendida a partir do seguinte exemplo:

Considere um código RS (n, k) = (255, 247) onde 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 perturbar a transmissão durante um período correspondente a 25 bits, conforme apresentado na Figura 4.1.

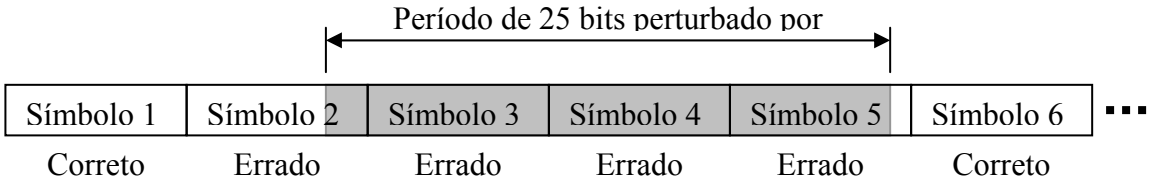


Figura 4.1 - Bloco de dados perturbado por ruído durante 25 períodos de bit.

[1] Como os códigos RS são não binário, t é a capacidade de correção de símbolos formados por m bits.

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

4.2. CAMPOS FINITOS

Para o entendimento dos princípios de codificação e de decodificação dos códigos não binários, tais como os códigos RS, é necessária a compreensão dos conceitos que envolvem os *campos finitos* conhecidos como *Campo de Galois* (GF).

Para qualquer número primo p existe um campo finito denominado GF(p) contendo p elementos. É possível estender GF(p) para um campo de p^m elementos, representado por GF(p^m), onde m é um número não nulo, positivo e inteiro. Note que GF(p^m) possui como subconjunto os elementos de GF(p). Os códigos RS são construídos a partir dos campos de extensão, GF(2^m).

Em um campo GF(2^m), cada elemento não zero é representado por uma potência de α. Um conjunto infinito de elementos, F, é formado começando pelos elementos $\{0, 1, \alpha\}$ e gerando elementos adicionais pela multiplicação progressiva da última entrada por α, ou seja,

$$F = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^j, \cdots\} = \{0, \alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^j, \cdots\} \tag{4.3}$$

Para a obtenção de um conjunto finito de elementos de GF(2^m) a partir de F, uma condição deve ser imposta sobre F para que ele possa conter 2^m elementos e seja fechado sob multiplicação. A condição que fecha os elementos de um campo sob multiplicação é caracterizada pelo polinômio irredutível

$$\alpha^{\left(2^m-1\right)} + 1 = 0 \tag{4.4}$$

ou equivalentemente,

$$\alpha^{\left(2^m-1\right)} = 1 = \alpha^0 \tag{4.5}$$

Usando esta restrição polinomial, qualquer elemento do campo que tenha grau igual ou maior que 2^m - 1 pode ser reduzido para um elemento com potência menor que 2^m - 1 como se segue:

$$\alpha^{\left(2^m+n\right)} = \alpha^{\left(2^m-1\right)}\alpha^{n+1} = \alpha^{n+1} \tag{4.6}$$

Assim, a Equação (4.5) pode ser usada para formar uma seqüência finita F^* a partir da seqüência finita F, da seguinte forma:

$$\begin{aligned} F^* &= \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}, \alpha^{2^m-1}, \alpha^{2^m}, \cdots\} \\ &= \{0, \alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{2^m-2}, \alpha^0, \alpha^1, \alpha^2, \cdots\} \end{aligned} \tag{4.7}$$

Portanto, pode-se observar a partir da Equação (4.7) que os elementos do campo finito GF(2^m) são dados por

$$GF(2^m) = \{0, \alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{2^m-2}\} \tag{4.8}$$

4.2.1. ADIÇÃO NO CAMPO DE EXTENSÃO GF(2^M)

Cada um dos 2^m elementos do campo finito GF(2^m) pode ser representado como um polinômio distinto de grau m - 1 ou menos. Cada elemento do campo GF(2^m) é representado por um polinômio $a_i(X)$, onde pelo menos um dos m coeficientes de $a_i(X)$ é não nulo. Para i = 0, 1, 2, ... , 2^m - 2,

$$\alpha^i = a_i(X) = a_{i,0} + a_{i,1}X + a_{i,2}X^2 + \cdots + a_{i,m-1}X^{m-1} \tag{4.9}$$

A adição de dois elementos do campo finito é definida como a soma módulo-2 de cada coeficiente do polinômio de mesma potência, i. e.,

$$\alpha^i + \alpha^j = (a_{i,0} + a_{j,0}) + (a_{i,1} + a_{j,1})X + \cdots + (a_{i,m-1} + a_{j,m-1})X^{m-1} \tag{4.10}$$

4.2.2. DEFINIÇÃO DE UM CAMPO FINITO POR UM *POLINÔMIO PRIMITIVO*

Campos finitos de GF(2^m) são construídos a partir de *polinômios primitivos* que por sua vez, são necessários para a definição dos códigos RS. Entretanto, é conveniente definir inicialmente o que são *polinômios irredutíveis*.

Um polinômio irredutível, f(X), de grau m é dito ser primitivo, se o menor inteiro positivo n para o qual f(X) divide $X^n + 1$ é $n = 2^m - 1$.

Qualquer polinômio irredutível sobre* GF(2) *de grau m divide $X^{2^m-1} + 1$**.**

A partir da definição e da propriedade apresentadas acima, a seguinte condição é necessária e suficiente para garantir que um polinômio é primitivo:

Um polinômio, f(X),de grau m, é dito ser irredutível sobre* GF(2) *se f(X) não é divisível por qualquer outro polinômio, sobre* GF(2)*, de grau menor que m, mas maior que zero.

Exemplo 4.1

Baseado na definição de polinômio primitivo apresentada anteriormente verifique se os polinômios irredutíveis a seguir são primitivos.

a) $1 + X + X^2 + X^3 + X^4$
b) $1 + X + X^4$

Solução:

a) Pode-se verificar se o polinômio é primitivo se o menor grau de $X^n + 1$ para o qual o polinômio é divisor, é $n = 2^m - 1$. Conseqüentemente, ele não pode dividir nenhum $X^n + 1$ de grau $1 \leq n < 15$.

$$n = 2^m - 1 = 2^4 - 1 = 16 - 1 = 15$$

Logo, o menor grau para o $X^n + 1$, para o qual $1 + X + X^2 + X^3 + X^4$ é divisor é 15.

$X^{15} + 1$	$X^4 + X^3 + X^2 + X + 1$
$(X^{15} + X^{14} + X^{13} + X^{12} + X^{11})$	$X^{11} + X^{10} + X^6 + X^5 + X + 1$
$X^{14} + X^{13} + X^{12} + X^{11} + 1$	
$(X^{14} + X^{13} + X^{12} + X^{11} + X^{10})$	
$X^{10} + 1$	
$(X^{10} + X^9 + X^8 + X^7 + X^6)$	
$X^9 + X^8 + X^7 + X^6 + 1$	
$(X^9 + X^8 + X^7 + X^6 + X^5)$	
$X^5 + 1$	
$(X^5 + X^4 + X^3 + X^2 + X)$	
$X^4 + X^3 + X^2 + X + 1$	
$(X^4 + X^3 + X^2 + X + 1)$	
0	

O que confirma que $1 + X + X^2 + X^3 + X^4$ é irredutível. Mas, verifica-se também que:

$X^5 + 1$	$X^4 + X^3 + X^2 + X + 1$
$(X^5 + X^4 + X^3 + X^2 + X)$	$X + 1$
$X^4 + X^3 + X^2 + X + 1$	
$(X^4 + X^3 + X^2 + X + 1)$	
0	

Logo, $X^4 + X^3 + X^2 + X + 1$ é irredutível, mas não é primitivo.

b) Para $1 + X + X^4$, verifica-se que:

$X^{15} + 1$	$X^4 + X + 1$
$(X^{15} + X^{12} + X^{11})$	$X^{11} + X^8 + X^7 + X^5 + X^3 + X^2 + X + 1$
$X^{12} + X^{11} + 1$	
$(X^{12} + X^9 + X^8)$	
$X^{11} + X^9 + X^8 + 1$	
$(X^{11} + X^8 + X^7)$	
$X^9 + X^7 + 1$	
$(X^9 + X^6 + X^5)$	
$X^7 + X^6 + X^5 + 1$	
$(X^7 + X^4 + X^3)$	
$X^6 + X^5 + X^4 + X^3 + 1$	
$(X^6 + X^3 + X^2)$	
$X^5 + X^4 + X^2 + 1$	
$(X^5 + X^2 + X)$	
$X^4 + X + 1$	
$(X^4 + X + 1)$	
0	

Pode se verificar também que $1 + X + X^4$ não divide nenhum outro $X^n + 1$ para $1 \leq n < 15$. Logo $1 + X + X^4$ é irredutível e primitivo.

* * *

Como pode ser observado, é relativamente fácil verificar se um polinômio é irredutível e primitivo. Entretanto a obtenção de um polinômio primitivo de um grau pré-determinado não é uma tarefa fácil. Normalmente esses polinômios são obtidos através de busca computacional. A Tabela 4.2 apresenta alguns polinômios primitivos de ordem 3 até 24.

Tabela 4.2 - Alguns polinômios primitivos.

m	Polinômio	m	Polinômio
3	$1+X+X^3$	14	$1+X+X^6+X^{10}+X^{14}$
4	$1+X+X^4$	15	$1+X+X^{15}$
5	$1+X^2+X^5$	16	$1+X+X^3+X^{12}+X^{16}$
6	$1+X+X^6$	17	$1+X^3+X^{17}$
7	$1+X^3+X^7$	18	$1+X^7+X^{18}$
8	$1+X^2+X^3+X^4+X^8$	19	$1+X+X^2+X^5+X^{19}$
9	$1+X^4+X^9$	20	$1+X^3+X^{20}$
10	$1+X^3+X^{10}$	21	$1+X^2+X^{21}$
11	$1+X^2+X^{11}$	22	$1+X+X^{22}$
12	$1+X+X^4+X^6+X^{12}$	23	$1+X^5+X^{23}$
13	$1+X+X^3+X^4+X^{13}$	24	$1+X+X^2+X^7+X^{24}$

4.2.3. O CAMPO DE EXTENSÃO GF(2^3)

Considere o caso de $m = 3$, ou seja, GF(2^3) e o polinômio primitivo $f(X) = 1 + X + X^3$. Um polinômio de grau m possui precisamente m raízes. Resolvendo para as raízes de $f(X)$, então os valores de X para $f(X) = 0$ devem ser encontrados. Seja α, um elemento do campo de extensão definido como uma raiz de $f(X)$. Assim,

$$f(\alpha) = 1 + \alpha + \alpha^3 = 0$$

$$\alpha^3 = 1 + \alpha \tag{4.11}$$

Desta forma, α^3 pode ser obtida como a soma ponderada dos termos de ordem mais baixa. De fato, todas as potências de α podem ser também representadas, conforme mostra a Tabela 4.3. A Tabela 4.3 mostra ainda o mapeamento dos sete elementos $\{\alpha^i\}$ e o elemento zero, em termos dos elementos base $\{X^0, X^1, X^2\}$, descritos pela Equação 4.10.

Tabela 4.3 - Mapeamento dos elementos do campo em termo de seus elementos base para $f(X) = 1 + X + X^3$, e representação das potências de α.

ELEMENTOS				REPRESENTAÇÃO DAS POTÊNCIAS DE α
GF(2^3)	BASE			
	X^0	X^1	X^2	
0	0	0	0	0
α^0	1	0	0	α^0
α^1	0	1	0	α^1
α^2	0	0	1	α^2
α^3	1	1	0	$\alpha^3 = 1 + \alpha$
α^4	0	1	1	$\alpha^4 = \alpha.\alpha^3 = \alpha\ (1 + \alpha) = \alpha + \alpha^2$
α^5	1	1	1	$\alpha^5 = \alpha.\alpha^4 = \alpha\ (\alpha + \alpha^2) = \alpha^2 + \alpha^3 = 1 + \alpha + \alpha^2$
α^6	1	0	1	$\alpha^6 = \alpha.\alpha^5 = \alpha\ (1 + \alpha + \alpha^2) = \alpha + \alpha^2 + \alpha^3 = 1 + \alpha^2$

* * *

A partir das equações definidas na Tabela 4.2, pode-se definir as duas operações aritméticas possíveis sobre GF(2^3): a adição e a multiplicação. Ambas estão apresentadas nas Tabelas 4.4 e 4.5, respectivamente, e foram obtidas do conjunto de equações da Tabela 4.3.

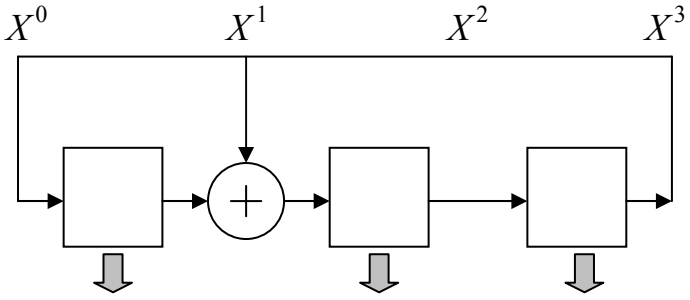
Tabela 4.4 - Tabela de adição para GF(2^3) com $f(X) = 1 + X + X^3$.

$\oplus$	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 4.5 - Tabela de multiplicação para GF(2^3) com $f(X) = 1 + X + X^3$.

⊗	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

O mapeamento dos elementos do campo em termos de seus elementos bases apresentados na Tabela 4.3 podem ser demonstrados através de registradores de deslocamento, conforme mostrado na Figura 4.2. O circuito gera (com m = 3) os (2^m -1) elementos não nulos do campo. Note que as conexões de realimentação do circuito correspondem aos coeficientes do polinômio $1 + X + X^3$, exatamente da mesma forma que o circuito gerador de paridade para os códigos cíclicos binários.



Início	**1**	**0**	**0**	α^0
1º deslocamento	**0**	**1**	**0**	α^1
2º deslocamento	**0**	**0**	**1**	α^2
3º deslocamento	**1**	**1**	**0**	α^3
4º deslocamento	**0**	**1**	**1**	α^4
5º deslocamento	**1**	**1**	**1**	α^5
6º deslocamento	**1**	**0**	**1**	α^6

Figura 4.2 - Elementos base não nulos de $1 + X + X^3$ gerados por registradores de deslocamento.

Iniciando por um elemento não nulo no primeiro estágio do registrador de deslocamento e promovendo seguidos deslocamentos cíclicos, verifica-se que todos os elementos base não nulos do polinômio $1 + X + X^3$ podem ser obtidos lendo-se o conteúdo dos registradores a cada deslocamento.

No sétimo deslocamento, obtém-se novamente α^0, pois da Equação (4.5), obtém-se $\alpha^{(2^m-1)} = \alpha^7 = \alpha^0$.

4.3. CODIFICAÇÃO RS

Conforme apresentado na Tabela 4.1, em termos dos parâmetros *n*, *k*, *t*, para a forma mais comum dos códigos RS, tem-se que

$$(n,k) = (2^m - 1,\ 2^m - 1 - 2t) \qquad m > 2 \tag{4.12}$$

onde $n - k = 2t$ 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:

$$g(X) = g_0 + g_1 X + g_2 X^2 + \cdots + g_{2t-1} X^{2t-1} + X^{2t} \tag{4.13}$$

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, ... ,α^{2t}. Assim, o polinômio gerador g(X) pode ser obtido fazendo

$$g(X) = (X - \alpha)(X - \alpha^2)...(X - \alpha^{2t}). \tag{4.14}$$

Considere como exemplo 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 forma:

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

Escrevendo o polinômio da ordem mais baixa para a mais alta, e trocando os sinais negativos por positivos (no campo binário +1 = -1), g(X) fica:

$$g(X) = \alpha^3 + \alpha^1 X + \alpha^0 X^2 + \alpha^3 X^3 + X^4 \tag{4.15}$$

4.3.1. CODIFICAÇÃO NA FORMA SISTEMÁTICA

Uma vez que os códigos RS são códigos cíclicos, eles podem ser codificados na forma sistemática de forma análoga ao procedimento para os códigos binários, ou seja, conforme apresentado no Capítulo 2,

$$X^{n-k}\,\mathrm{m}(X) = \mathrm{q}(X)\mathrm{g}(X) + \mathrm{p}(X). \tag{4.16}$$

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). Note que, na forma sistemática, o polinômio resto, p(X), é o polinômio paridade da palavra código. A Equação (4.16) pode ser escrita ainda como:

$$\mathrm{p}(X) = X^{n-k}\,\mathrm{m}(X) \text{ módulo } \mathrm{g}(X) \tag{4.17}$$

A palavra código polinomial resulta em

$$\mathrm{c}(X) = \mathrm{p}(X) + X^{n-k}\mathrm{m}(X) \tag{4.18}$$

Exemplo 4.2:

Considere a seqüência mensagem binária 010110111. Faça a codificação sistemática da mensagem com um código RS (7, 3), cujo polinômio gerador é aquele obtido pela Equação 4.14. Para geração dos símbolos em GF(2^3), considere o polinômio primitivo de grau 3 apresentado na Tabela 4.2.

Solução:

A seqüência 010110111 pode ser segmentada em elementos base do campo gerado por $1 + X + X^3$, na forma 010 110 111, para a obtenção dos elementos do campo α^1, α^3 e α^5, conforme mostrado na Tabela 4.3.

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

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

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 as Tabelas 4.4 e 4.5, respectivamente, conforme apresentado a seguir.

$$\begin{array}{l|l}
\alpha^5X^6 + \alpha^3X^5 + \alpha^1X^4 & \alpha^0X^4 + \alpha^3X^3 + \alpha^0X^2 + \alpha^1X + \alpha^3 \\
\hline
(\alpha^5X^6 + \alpha^1X^5 + \alpha^5X^4 + \alpha^6X^3 + \alpha^1X^2) & \alpha^5X^2 + \alpha^0X + \alpha^4 \\
\quad 0 \quad + \alpha^0X^5 + \alpha^6X^4 + \alpha^6X^3 + \alpha^1X^2 & \\
\qquad (\alpha^0X^5 + \alpha^3X^4 + \alpha^0X^3 + \alpha^1X^2 + \alpha^3X) & \\
\qquad\quad 0 \quad + \alpha^4X^4 + \alpha^2X^3 + \quad 0 \quad + \alpha^3X & \\
\qquad\qquad (\alpha^4X^4 + \alpha^0X^3 + \alpha^4X^2 + \alpha^5X + \alpha^0) & \\
\qquad\qquad\qquad \alpha^6X^3 + \alpha^4X^2 + \alpha^2X + \alpha^0 \;\rightarrow \text{ resto} &
\end{array}$$

Logo,

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

Assim, da Equação 4.18 obtém-se:

$$c(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6 \qquad (4.19a)$$

4.3.2. 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*) apresentado na Equação 4.15, requer uma cadeia de registradores de deslocamento conforme mostrado na Figura 4.3.

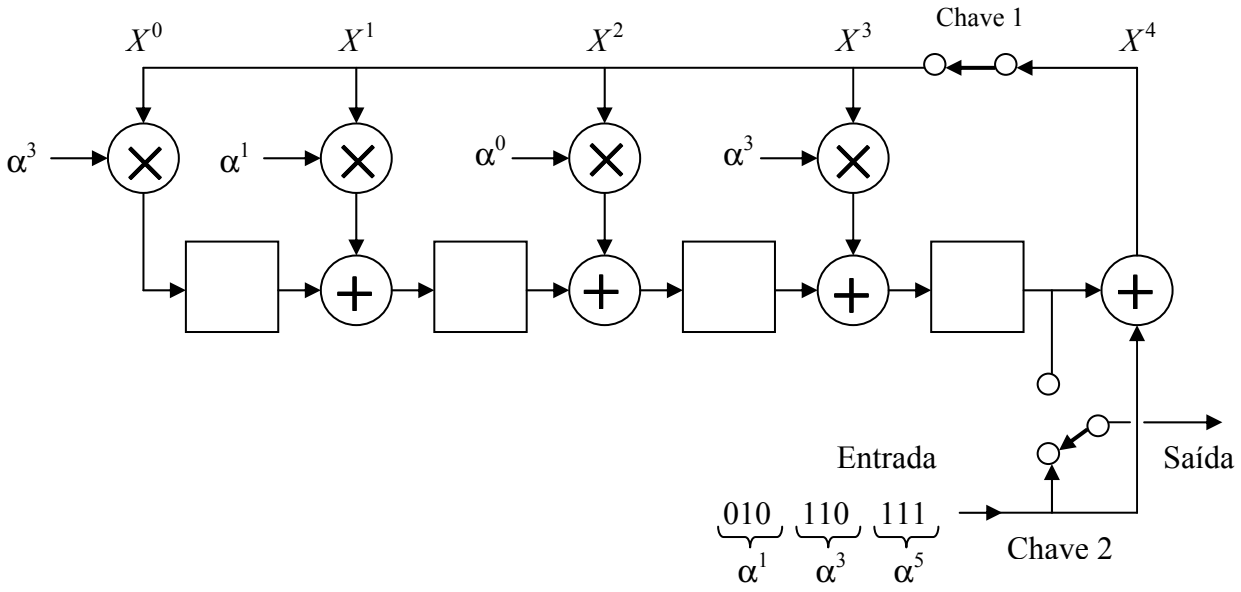


Figura 4.3 - Codificador com registradores de deslocamento para o código RS (7, 3).

Assim como no caso binário, no codificador da Figura 4.3, o número de estágios do registrador de deslocamento é igual a (*n-k*). Entretanto, 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.

Note que 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 é similar ao caso binário e se dá da seguinte forma:

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 $p(X) + X^{n-k}m(X)$, onde $p(X)$ representam os símbolos de paridade, e $m(X)$ os símbolos de mensagem na forma polinomial.

Exemplo 4.3:

Considere a seqüência mensagem $m(X) = \alpha^1 + \alpha^3 X + \alpha^5 X^2$. Faça a codificação sistemática da mensagem com um código RS (7, 3), usando o codificador da Figura 4.3, mostrando a cada ciclo de *clock* a saída e o conteúdo do registrador de deslocamento.

Solução:

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

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

$$c(X) = \sum_{n=0}^{6} u_n X^n = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6 \qquad (4.19b)$$

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

Note que no processo de codificação as operações de adição e multiplicação devem respeitar as Tabelas 4.4 e 4.5, respectivamente.

* * *

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

$$c(X) = \mathrm{m}(X)\mathrm{g}(X) \tag{4.20}$$

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

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

O polinômio código apresentado na Equação 4.19 resulta em zero quando calculado para qualquer raiz de g(X), conforme mostrado a seguir, para cada uma das raízes.

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

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

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

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

4.4. DECODIFICAÇÃO RS

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

$$\mathrm{e}(X) = \sum_{i=0}^{n-1} e_i X^i \ . \tag{4.21}$$

Para um código RS (7, 3), a Equação 4.21 torna-se:

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

Agora, assuma que durante uma transmissão o polinômio código representado pela Equação 4.19 tenha sido corrompido por ruído e 2 símbolos foram recebidos com erro, de acordo com o padrão de duplo erro apresentado a seguir.

$$\mathrm{e}(X) = 0 + 0X + 0X^2 + \alpha^2 X^3 + 0X^4 + \alpha^5 X^5 + 0X^6 \tag{4.22}$$

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

Isto é, α^2 (001) introduz 1 bit errado no símbolo da posição X^3 e α^5 (111) introduz 3 bits errados no símbolo da posição X^5. Conseqüentemente, o polinômio código pode ser obtido a partir de:

$$\mathrm{r}(X) = \mathrm{c}(X) + \mathrm{e}(X) \tag{4.23}$$

que resulta em

$$\begin{array}{lccccccc} \mathrm{c}(X) = & \alpha^0 + & \alpha^2 X + & \alpha^4 X^2 + & \alpha^6 X^3 + & \alpha^1 X^4 + & \alpha^3 X^5 + & \alpha^5 X^6 \\ + & & & & & & & \\ \mathrm{e}(X) = & 0 + & 0\,X + & 0\,X^2 + & \alpha^2 X^3 + & 0\,X^4 + & \alpha^5 X^5 + & 0\,X^6 \\ = & & & & & & & \\ \mathrm{r}(X) = & \alpha^0 + & \alpha^2 X + & \alpha^4 X^2 + & \alpha^0 X^3 + & \alpha^1 X^4 + & \alpha^2 X^5 + & \alpha^5 X^6 \end{array} \tag{4.24}$$

Neste exemplo existem quatro incógnitas: duas posições de erro e dois valores errados. Note que 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 do campo GF(2^3). Uma vez que existem quatro incógnitas neste exemplo, são necessárias quatro equações para sua solução

4.4.1. CÁLCULO DA SÍNDROME

Para o código RS (7, 3) aqui considerado, cada vetor síndrome possui quatro símbolos. Conforme já apresentado, 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 forma a síndrome, S_i, pode ser determinada calculando-se r(X) para as raízes de g(X), ou seja,

$$\begin{aligned} S_i &= \mathrm{r}(X); \quad X = \alpha^i \\ S_i &= \mathrm{r}(\alpha^i); \quad i = 1, \cdots, n-k \end{aligned} \tag{4.25}$$

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

Para o polinômio recebido r(X) apresentado na Equação 4.24 os quatro símbolos da síndrome são:

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

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

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

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

Exemplo 4.4:

Mostre que as síndromes do padrão de erro representado pela Equação 4.22 são iguais às síndromes calculadas para o polinômio recebido representado pela Equação 4.24.

Solução:

$$\begin{aligned} S_i &= \mathrm{r}(X); \quad X = \alpha^i \\ S_i &= \mathrm{r}(\alpha^i); \quad i = 1, \cdots, n-k \end{aligned}$$

$$\begin{aligned} S_i &= [\mathrm{c}(X) + \mathrm{e}(X)]; \quad X = \alpha^i \\ S_i &= [\mathrm{c}(\alpha^i) + \mathrm{e}(\alpha^i)] = 0 + \mathrm{e}(\alpha^i) \\ S_i &= \mathrm{e}(\alpha^i) \end{aligned}$$

Da Equação 4.22:

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

Assim:

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

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

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

$$\begin{aligned} S_2 &= e(\alpha^4) = \alpha^2\alpha^{12} + \alpha^5\alpha^{20} \\ &= \alpha^0 + \alpha^4 \\ &= \alpha^5 \end{aligned}$$

Estes resultados confirmam que as síndromes de e(X) e r(X), quando calculadas para as raízes de g(X), são exatamente as mesmas.

* * *

4.4.2. Localização de Erro

De acordo com a Equação 4.21, para todo $e_i \neq 0$, então existe na posição i um erro cujo valor é e_i. Isso pode ser observado por meio da Equação 4.22, repetida a seguir por conveniência, que mostra claramente os valores dos erros e suas posições.

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

Note que existem dois erros: um na posição X^3 e outro na posição X^4, cujos valores são respectivamente α^2 e α^5. Assim, para corrigir uma palavra recebida, cada valor de erro e_i e sua localização X^i, deve ser determinada.

Conforme definido e demonstrado anteriormente, as síndromes podem ser determinadas tanto a partir do polinômio recebido quanto por meio do polinômio de erro. Desta forma, pode-se generalizar o sistema de equações que determinam os valores da síndrome fazendo:

$$\begin{aligned} S_1 &= r(\alpha) = e_0\,\alpha^0 + e_1\,\alpha^1 + \cdots + e_{n-1}\,\alpha^{n-1} \\ S_2 &= r(\alpha^2) = e_0(\alpha^2)^0 + e_1(\alpha^2)^1 + \cdots + e_{n-1}(\alpha^2)^{n-1} \\ &\vdots \\ S_{2t} &= r(\alpha^{2t}) = e_0(\alpha^{2t})^0 + e_1(\alpha^{2t})^1 + \cdots + e_{n-1}(\alpha^{2t})^{n-1} \end{aligned} \tag{4.26}$$

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

$$\sigma(X) = 1 + \sigma_1 X + \sigma_2 X^2 + \cdots + \sigma_t X^t \tag{4.27}$$

Os recíprocos das raízes de σ(*X*) revelam as posições de erros do padrão de erro e(*X*). Então usando a técnica de modelagem auto-regressiva, pode-se formar uma matriz a partir das síndromes, onde as primeiras *t* síndromes são utilizadas para determinar as próximas síndromes. Isto é,

$$\begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_{t-1} & S_t \\ S_2 & S_3 & S_4 & \cdots & S_t & S_{t+1} \\ & & & \vdots & & \\ S_{t-1} & S_t & S_{t+1} & \cdots & S_{2t-3} & S_{2t-2} \\ S_t & S_{t+1} & S_{t+2} & \cdots & S_{2t-2} & S_{2t-1} \end{bmatrix} \begin{bmatrix} \sigma_t \\ \sigma_{t-1} \\ \vdots \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -S_{t+1} \\ -S_{t+2} \\ \vdots \\ -S_{2t-1} \\ -S_{2t} \end{bmatrix}. \tag{4.28}$$

Aplica-se o modelo auto-regressivo da Equação 4.28 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

$$\begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix} \tag{4.29}$$

$$\begin{bmatrix} \alpha^2 & 0 \\ 0 & \alpha^3 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^3 \\ \alpha^5 \end{bmatrix} \Rightarrow \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^2 & 0 \\ 0 & \alpha^3 \end{bmatrix}^{-1} \begin{bmatrix} \alpha^3 \\ \alpha^5 \end{bmatrix} \tag{4.30}$$

Conforme apresentado no Anexo 4.1, no final deste capítulo, o inverso de uma matriz diagonal é a matriz formada pelo inverso de seus elementos. Portanto,

$$\begin{bmatrix} \alpha^2 & 0 \\ 0 & \alpha^3 \end{bmatrix}^{-1} = \begin{bmatrix} \alpha^{-2} & 0 \\ 0 & \alpha^{-3} \end{bmatrix} = \begin{bmatrix} \alpha^5 & 0 \\ 0 & \alpha^4 \end{bmatrix} \tag{4.31}$$

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

$$\begin{bmatrix} \alpha^2 & 0 \\ 0 & \alpha^3 \end{bmatrix} \begin{bmatrix} \alpha^5 & 0 \\ 0 & \alpha^4 \end{bmatrix} = \begin{bmatrix} \alpha^2\alpha^5 + 0 \cdot 0 & \alpha^2 0 + 0\alpha^4 \\ 0\alpha^5 + \alpha^3 0 & 0 \cdot 0 + \alpha^3\alpha^4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{4.32}$$

Substituindo então o resultado de (4.31) em (4.30) e efetuando a multiplicação, obtém-se

$$\begin{bmatrix}\sigma_2\\ \sigma_1\end{bmatrix}=\begin{bmatrix}\alpha^5 & 0\\ 0 & \alpha^4\end{bmatrix}\begin{bmatrix}\alpha^3\\ \alpha^5\end{bmatrix}=\begin{bmatrix}\alpha^5\alpha^3+0\,\alpha^5\\ 0\,\alpha^3+\alpha^4\alpha^5\end{bmatrix}=\begin{bmatrix}\alpha\\ \alpha^2\end{bmatrix}. \tag{4.33}$$

Substituindo agora os resultados de (4.33) em (4.27), obtém-se:

$$\sigma(X)=\alpha^0+\sigma_1 X+\sigma_2 X^2=\alpha^0+\alpha^2 X+\alpha X^2. \tag{4.34}$$

Como as raízes de $\sigma(X)$ são os recíprocos das posições de erros, o próximo passo é a determinação das raízes de (4.34). Isso pode ser feito por meio de testes exaustivos do polinômio $\sigma(X)$, com cada um dos elementos do campo, conforme mostrado a seguir. Qualquer elemento X que resulta em $\sigma(X) = 0$ é uma raiz, e permite localizar um erro.

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

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,

$$\begin{aligned}
\frac{1}{\alpha^2}=\alpha^5 &\Rightarrow \text{Posição } X^5\\
\frac{1}{\alpha^4}=\alpha^3 &\Rightarrow \text{Posição } X^3
\end{aligned}.$$

Conseqüentemente, o polinômio padrão de erro já pode ser escrito com as posições de erros reveladas, isto é:

$$\hat{e}(X)=e_3X^3+e_5X^5. \tag{4.35}$$

onde $\hat{\mathbf{e}}(X)$ denota o polinômio de erro *estimado*. Note que duas das quatro incógnitas foram determinadas, ou seja, as duas posições de erros. Resta agora determinar as outras duas incógnitas que são os valores dos erros.

4.4.3. 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. De (4.26) para as síndromes S_1 e S_2 obtém-se:

$$\begin{aligned} S_1 &= \mathrm{r}(\alpha) = e_3\alpha^3 + e_5\alpha^5 = \alpha^2 \\ S_2 &= \mathrm{r}(\alpha^2) = e_3\alpha^6 + e_5\alpha^{10} = 0 \end{aligned} \quad . \tag{4.36}$$

Escrevendo as equações acima na forma matricial, obtém-se:

$$\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix} \begin{bmatrix} e_3 \\ e_5 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ 0 \end{bmatrix} \tag{4.37}$$

que pode ser reescrita como

$$\begin{bmatrix} e_3 \\ e_5 \end{bmatrix} = \begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix}^{-1} \begin{bmatrix} \alpha^2 \\ 0 \end{bmatrix} \tag{4.38}$$

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

Agora a matriz a ser invertida não é uma matriz diagonal e requer uma solução um pouco mais trabalhosa, conforme apresentado no Anexo 4.1, ou seja, para uma matriz [A] o seu inverso pode ser determinado como:

$$\mathrm{Inv}[A] = \frac{[\mathrm{cofator}[A]]^T}{\det[A]}$$

$$\mathrm{Inv}\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix} = \frac{\left[\mathrm{cofator}\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix}\right]^T}{\det\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^{10} \end{bmatrix}} = \frac{\begin{bmatrix} \alpha^{10} & \alpha^6 \\ \alpha^5 & \alpha^3 \end{bmatrix}^T}{\alpha^3\alpha^{10} - \alpha^6\alpha^5} = \frac{\begin{bmatrix} \alpha^{10} & \alpha^5 \\ \alpha^6 & \alpha^3 \end{bmatrix}}{\alpha^6 + \alpha^4}$$

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

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

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

Resolvendo (4.38) para os valores de erros, obtém-se:

$$\begin{bmatrix} e_3 \\ e_5 \end{bmatrix} = \begin{bmatrix} \alpha^0 & \alpha^2 \\ \alpha^3 & \alpha^0 \end{bmatrix} \begin{bmatrix} \alpha^2 \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha^0\alpha^2 + \alpha^2 0 \\ \alpha^3\alpha^2 + \alpha^0 0 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ \alpha^5 \end{bmatrix} \tag{4.39}$$

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

$$\hat{e}(X) = \alpha^2 X^3 + \alpha^5 X^5 . \tag{4.40}$$

4.4.4. Correção do Polinômio Recebido com o Polinômio de Erro Estimado

O polinomio transmitido estimado é obtido fazendo:

$$\hat{c}(X) = r(X) + \hat{e}(X) = \hat{c}(X) + e(X) + \hat{e}(X) \tag{4.41}$$

$$\begin{aligned} r(X) = \quad & \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^0 X^3 + \alpha^1 X^4 + \alpha^2 X^5 + \alpha^5 X^6 \\ + \\ \hat{e}(X) = \quad & 0 + 0X + 0X^2 + \alpha^2 X^3 + 0X^4 + \alpha^5 X^5 + 0X^6 \\ = \\ \hat{\mathbf{c}}(X) = \quad & \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6 \end{aligned} \tag{4.42}$$

Uma vez que os símbolos mensagem constituem os $k = 3$ símbolos mais a direita do polinômio, então a mensagem decodificada é

$$\underbrace{010}_{\alpha^1}\ \underbrace{110}_{\alpha^3}\ \underbrace{111}_{\alpha^5} \tag{4.43}$$

* * *

4.5. EXERCÍCIOS

1. Deseja-se obter um código Reed-Solomon (n, k) primitivo a partir de um GF(2^6) com capacidade de correção igual a 10 símbolos. Pergunta-se:

   a) Quais são os valores de n e de k para este código?
   b) Qual é o grau do polinômio gerador para este código?

2. Considere um Código RS (127, 97). Responda:

   a) Qual é a capacidade de correção de símbolos deste código?
   b) Qual é o maior comprimento da rajada de bits que pode ser corrigida pelo código?
   c) Qual é o grau do polinômio gerador deste código?

3. Considere um Código Reed-Solomon (31, 15). Responda:

   a) Quantos são os bits por símbolo do código?
   b) Qual é o comprimento do bloco em bits?
   c) Quantos símbolos errados podem ser corrigidos?
   d) Qual é a maior comprimento de rajada de erros que pode ser corrigida?

4. Considere o campo de Galois $GF(2^4)$ gerado por $p(X) = 1 + X^3 + X^4$ apresentado na tabela a seguir. Encontre os polinômios geradores para os códigos:

   a) RS (15, 13).
   a) RS (15, 11).
   b) RS (15, 9).
   c) RS (15, 7).

Representação por potência	Representação polinomial	Representação por potência	Representação polinomial
0	0	α^7	$1 + \alpha + \alpha^2$
α^0	1	α^8	$\alpha + \alpha^2 + \alpha^3$
α^1	α	α^9	$1 + \alpha^2$
α^2	α^2	α^{10}	$\alpha + \alpha^3$
α^3	α^3	α^{11}	$1 + \alpha^2 + \alpha^3$
α^4	$1 + \alpha^3$	α^{12}	$1 + \alpha$
α^5	$1 + \alpha + \alpha^3$	α^{13}	$\alpha + \alpha^2$
α^6	$1 + \alpha + \alpha^2 + \alpha^3$	α^{14}	$\alpha^2 + \alpha^3$

5. Considere o Campo de Galois gerado a partir do polinômio primitivo $p(X) = 1 + X^2 + X^3$ apresentado a seguir. Pede-se:

   a) Obtenha o polinômio gerador para o código RS (7, 5)
   b) Codifique a mensagem m = 111000010000101, onde o bit mais significativo é o bit mais a direita.

Representação por potência	Representação polinomial	Representação por potência	Representação polinomial
0	0	α^3	$1 + \alpha^2$
α^0	1	α^4	$1 + \alpha + \alpha^2$
α^1	α	α^5	$1 + \alpha$
α^2	α^2	α^6	$\alpha + \alpha^2$

6. Considere o código Reed-Solomon (7, 3) gerado a partir de campo apresentado a seguir. Pede-se:

   a) Codificar a mensagem $m(X) = 1 + \alpha X + \alpha^2 X^2$.
   b) Calcule as síndromes para o vetor recebido $r(X) = \alpha^0 + \alpha^2 X + \alpha^3 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^0 X^5 + \alpha^5 X^6$.
   c) Decodifique o polinômio recebido apresentado na questão "b".

Representação por potência	Representação polinomial	Representação por potência	Representação polinomial
0	0	α^3	$1 + \alpha$
α^0	1	α^4	$\alpha + \alpha^2$
α^1	α	α^5	$1 + \alpha + \alpha^2$
α^2	α^2	α^6	$1 + \alpha^2$

* * *

4.6. REFERÊNCIA BIBLIOGRÁFICA

[1] SKLAR, B., *Digital Communications: Fundamentals and Applications – 2nd ed.*, PTR Prentice Hall, Upper Saddle River, NJ, 2001. 1079 p.

ANEXO 4.1 - OPERAÇÕES ELEMENTARES COM MATRIZES

▪ MULTIPLICAÇÃO DE MATRIZES

Considere uma matriz **A** com dimensões $m \times n$ e uma matriz **B** com dimensões $r \times p$. O produto **C** = **AB** (nesta ordem) é definido se e somente se $r = n$, ou seja, o número de colunas da matriz **A** deve ser igual ao número de linhas da matriz **B.**

O produto é então uma matriz $m \times p$ definida como uma matriz **C** obtida conforme mostrado a seguir.

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \qquad \mathrm{B} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{bmatrix}$$

$$\mathrm{C} = \mathbf{A} \cdot \mathbf{B} = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} & a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} \\ a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} & a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} \\ a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31} & a_{31}b_{12} + a_{32}b_{22} + a_{33}b_{32} \end{bmatrix} \qquad \text{(A4.1)}$$

Exemplo 1:

$$\mathbf{A} = \begin{bmatrix} 4 & 3 \\ 7 & 2 \\ 9 & 0 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 2 & 5 \\ 1 & 6 \end{bmatrix} \quad \mathbf{C} = \mathbf{A} \cdot \mathbf{B} = \begin{bmatrix} 4 \cdot 2 + 3 \cdot 1 & 4 \cdot 5 + 3 \cdot 6 \\ 7 \cdot 2 + 2 \cdot 1 & 7 \cdot 5 + 2 \cdot 6 \\ 9 \cdot 2 + 0 \cdot 1 & 9 \cdot 5 + 0 \cdot 6 \end{bmatrix} \Rightarrow \quad \mathbf{C} = \begin{bmatrix} 11 & 38 \\ 17 & 47 \\ 18 & 45 \end{bmatrix}$$

Cuidado! Geralmente a multiplicação de matrizes não é comutativa, ou seja, AB ≠ BA.

▪ DETERMINANTES DE SEGUNDA ORDEM

Um determinante de segunda ordem é representado e definido por

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \qquad D = \det \mathbf{A} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}. \qquad \text{(A4.2)}$$

Exemplo 2:

$$\mathbf{A} = \begin{bmatrix} 4 & 3 \\ 2 & 5 \end{bmatrix} \qquad D = \det \mathbf{A} = \begin{vmatrix} 4 & 3 \\ 2 & 5 \end{vmatrix} = 4 \cdot 5 - 3 \cdot 2 = 14 .$$

- **DETERMINANTES DE TERCEIRA ORDEM**

Considere a matriz a apresentada a seguir.

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Um determinante de terceira ordem pode ser definido por:

$$D = \det \mathbf{A} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{21} \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31} \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \qquad \text{(A4.3)}$$

Note que os sinais dos termos a_{11}, a_{21} e a_{31} são, respectivamente, + - +. Além disso, os determinantes de segunda ordem que multiplicam os termos a_{11}, a_{21} e a_{31} são obtidos a partir das matrizes menores para os respectivos termos. A matriz menor para um termo a_{jl} é aquela que resulta do apagamento da linha j e da coluna l, conforme mostrado a seguir.

$$\begin{bmatrix} a_{11} & & \\ & a_{22} & a_{23} \\ & a_{32} & a_{33} \end{bmatrix} \Rightarrow a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix}$$

$$\begin{bmatrix} & a_{12} & a_{13} \\ a_{21} & & \\ & a_{32} & a_{33} \end{bmatrix} \Rightarrow a_{21} \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix}$$

$$\begin{bmatrix} & a_{12} & a_{13} \\ & a_{22} & a_{23} \\ a_{31} & & \end{bmatrix} \Rightarrow a_{31} \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}$$

Exemplo 3:

$$\mathbf{A} = \begin{bmatrix} 1 & 3 & 0 \\ 2 & 6 & 4 \\ -1 & 0 & 2 \end{bmatrix}$$

$$\det \mathbf{A} = 1 \begin{vmatrix} 6 & 4 \\ 0 & 2 \end{vmatrix} - 2 \begin{vmatrix} 3 & 0 \\ 0 & 2 \end{vmatrix} + (-1) \begin{vmatrix} 3 & 0 \\ 6 & 4 \end{vmatrix} = 1(12-0) - 2(6-0) + (-1)(12-0)$$

$$\det \mathbf{A} = 12 - 12 - 12 = -12$$

- **INVERSÃO DE UMA MATRIZ DIAGONAL**

A matriz inversa de uma matriz diagonal é a matriz cujos elementos são os inversos dos elementos da matriz que se deseja inverter. Ou seja:

$$\mathbf{A}=\begin{bmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{bmatrix} \quad \Rightarrow \quad \mathbf{A}^{-1}=\begin{bmatrix} 1/a_{11} & 0 & 0 \\ 0 & 1/a_{22} & 0 \\ 0 & 0 & 1/a_{33} \end{bmatrix} \tag{A4.4}$$

Exemplo 4:

$$\mathbf{A}=\begin{bmatrix} 4 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 5 \end{bmatrix} \Rightarrow \mathbf{A}^{-1}=\begin{bmatrix} 0{,}25 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0{,}20 \end{bmatrix}$$

Verificação: Se uma matriz A foi invertida corretamente, então $A.A^{-1}$ é igual a uma matriz identidade.

$$\begin{bmatrix} 4 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 5 \end{bmatrix}\begin{bmatrix} 0{,}25 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0{,}20 \end{bmatrix}=\begin{bmatrix} 4\cdot 0{,}25 & 0 & 0 \\ 0 & (-1)\cdot(-1) & 0 \\ 0 & 0 & 5\cdot 0{,}2 \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

- **INVERSÃO DE UMA MATRIZ NÃO SINGULAR 2×2**

Considere a matriz

$$\mathbf{A}=\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Sua inversa é

$$\mathbf{A}^{-1}=\frac{1}{\det \mathbf{A}}\begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} \tag{A4.5}$$

Exemplo 5:

$$\mathbf{A}=\begin{bmatrix} 3 & -2 \\ 2 & 1 \end{bmatrix} \Rightarrow \mathbf{A}^{-1}=\frac{1}{3\cdot 1-(-2)\cdot 2}\begin{bmatrix} 1 & 2 \\ -2 & 3 \end{bmatrix} \Rightarrow \mathbf{A}^{-1}=\frac{1}{7}\begin{bmatrix} 1 & 2 \\ -2 & 3 \end{bmatrix} \Rightarrow \mathbf{A}^{-1}=\begin{bmatrix} 1/7 & 2/7 \\ -2/7 & 3/7 \end{bmatrix}$$

Verificação: Se uma matriz A foi invertida corretamente, então $A.A^{-1}$ é igual a uma matriz identidade.

$$\begin{bmatrix} 3 & -2 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 1/7 & 2/7 \\ -2/7 & 3/7 \end{bmatrix}=\begin{bmatrix} 3\cdot 1/7+(-2)(-2/7) & 3\cdot 2/7+(-2)\cdot 3/7 \\ 2\cdot 1/7+1\cdot(-2/7) & 2\cdot 2/7+1\cdot 3/7 \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- **INVERSÃO DE UMA MATRIZ DE TERCEIRA ORDEM OU MAIOR**

Pode-se inverter uma matriz **A** de ordem qualquer por meio de seu determinante e de sua matriz de cofatores, de acordo com a seguinte expressão:

$$\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \left[\text{cofator } \mathbf{A}\right]^T . \tag{A4.6}$$

Os cofatores da matriz **A** são os determinantes das matrizes menores para cada elemento da matriz **A**. Para ilustrar a construção da matriz de cofatores, considere a matriz **A** de terceira ordem e a representação de sua matriz de cofatores apresentadas a seguir e.

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \quad \Rightarrow \quad \text{cofator } \mathbf{A} = \begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix} \tag{A4.7}$$

Os elementos A_{11}, A_{12}, ... , A_{33} são os determinantes de cada uma das matrizes menores para cada elemento a_{11}, a_{12}, ... , a_{33}, conforme mostrado a seguir.

$$\begin{aligned} A_{11} &= \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} & A_{12} &= -\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} & A_{13} &= \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} \\ A_{21} &= -\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} & A_{22} &= \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} & A_{23} &= -\begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{vmatrix} \\ A_{31} &= \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} & A_{32} &= -\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} & A_{33} &= \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \end{aligned} \tag{A4.8}$$

Exemplo 6:

$$\mathbf{A} = \begin{bmatrix} -1 & 1 & 2 \\ 3 & -1 & 1 \\ -1 & 3 & 4 \end{bmatrix} \quad \Rightarrow \quad \mathbf{A}^{-1} = \frac{1}{\det[\mathbf{A}]} \left[\text{cofator}[\mathbf{A}]\right]^T$$

$$\det[\mathbf{A}] = (-1)\begin{vmatrix} -1 & 1 \\ 3 & 4 \end{vmatrix} - 3\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} + (-1)\begin{vmatrix} 1 & 2 \\ -1 & 1 \end{vmatrix}$$

$$\det[\mathbf{A}] = (-1)(-4-3) - [3(4-6)] + (-1)(1+2) = 7 + 6 - 3$$

$$\det[\mathbf{A}] = 10$$

$$A_{11} = \begin{vmatrix} -1 & 1 \\ 3 & 4 \end{vmatrix} = -7 \qquad A_{12} = -\begin{vmatrix} 3 & 1 \\ -1 & 4 \end{vmatrix} = -13 \qquad A_{13} = \begin{vmatrix} 3 & -1 \\ -1 & 3 \end{vmatrix} = 8$$

$$A_{21} = -\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 2 \qquad A_{22} = \begin{vmatrix} -1 & 2 \\ -1 & 4 \end{vmatrix} = -2 \qquad A_{23} = \begin{vmatrix} -1 & 1 \\ -1 & 3 \end{vmatrix} = 2$$

$$A_{31} = \begin{vmatrix} 1 & 2 \\ -1 & 1 \end{vmatrix} = 3 \qquad A_{32} = \begin{vmatrix} -1 & 2 \\ 3 & 1 \end{vmatrix} = 7 \qquad A_{33} = \begin{vmatrix} -1 & 1 \\ 3 & -1 \end{vmatrix} = -2$$

$$\text{cofator}[\mathbf{A}] = \begin{bmatrix} -7 & -13 & 8 \\ 2 & -2 & 2 \\ 3 & 7 & -2 \end{bmatrix}$$

$$[\text{cofator}[\mathbf{A}]]^T = \begin{bmatrix} -7 & 2 & 3 \\ -13 & -2 & 7 \\ 8 & 2 & -2 \end{bmatrix}$$

$$\mathbf{A}^{-1} = \frac{1}{10}\begin{bmatrix} -7 & 2 & 3 \\ -13 & -2 & 7 \\ 8 & 2 & -2 \end{bmatrix}$$

$$\mathbf{A}^{-1} = \begin{bmatrix} -0{,}7 & 0{,}2 & 0{,}3 \\ -1{,}3 & -0{,}2 & 0{,}7 \\ 0{,}8 & 0{,}2 & -0{,}2 \end{bmatrix}$$

* * *

REFERÊNCIA BIBLIOGRÁFICA DO ANEXO 4.1

KREYSZIG, E., *Advanced Engineering Mathematics - 7th ed.*, John Wiley & Sons, Singapore, 1993.