Redes e Sistemas de Telecomunicações

RT001

Teoria da Informação e Codificação de Canal (Parte 2)

Prof. Dr. Estevan Lopes

Inatel | CAMINHOS QUE CONECTAM COM O FUTURO

CAPÍTULO 3

3.1. INTRODUÇÃO

O estudo será feito nas seguintes etapas:

1) Introdução ao RS
2) Campo Finito (Campo de Galois)
3) Codificação
4) Decodificação

- Os códigos RS são usados em diversos sistemas de armazenamento e transmissão de informação, entre os quais:
  - Transmissão de sinais digitais de TV nos padrões ATSC, DVB-T e ISDB-T
  - Transmissão de comunicação móvel celular
- Os códigos RS são códigos cíclicos não binários com símbolos formados por sequências de *m* bits.
- Os códigos RS possuem uma razoável capacidade de correção de erros em rajada.

3.1. INTRODUÇÃO

Principais características dos códigos RS.

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

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

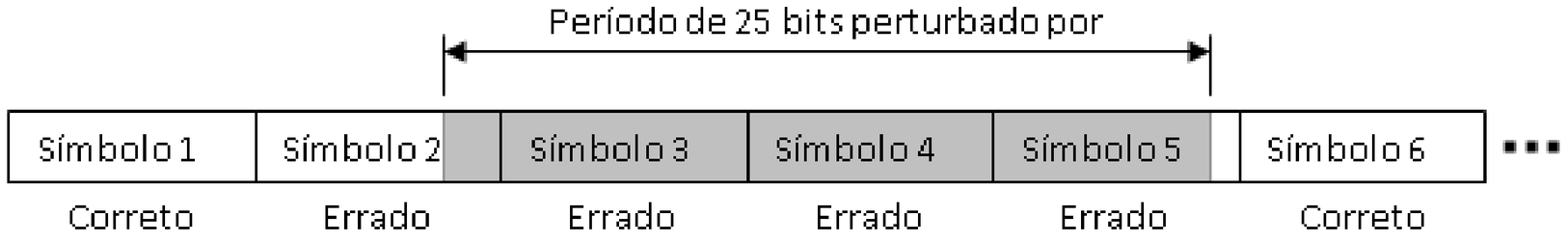
$$t = \left\lfloor \frac{n-k}{2} \right\rfloor = \left\lfloor \frac{255-247}{2} \right\rfloor = 4$$

Inatel
CAMINHOS QUE CONECTAM COM O FUTURO

3.1. INTRODUÇÃO

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,



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.

3.1. INTRODUÇÃO

- Para 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,

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

3.2. CAMPOS FINITOS

- 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

$$\alpha^{\left(2^m-1\right)}+1=0 \qquad \text{ou} \qquad \alpha^{\left(2^m-1\right)}=1=\alpha^0$$

- 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

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

- Assim, a Equação $\alpha^{\left(2^m-1\right)}=1=\alpha^0$ pode ser usada para formar uma sequência finita *F** a partir da sequência infinita *F*, da seguinte forma

$$F^*=\{0,1,\alpha,\alpha^2,\cdots,\alpha^{2^m-2},\alpha^{2^m-1},\alpha^{2^m},\cdots\}=\{0,\alpha^0,\alpha^1,\ \alpha^2,\cdots,\ \alpha^{2^m-2},\alpha^0,\alpha^1,\ \alpha^2,\cdots\}$$

- Observa-se a partir da Equação anterior os elementos do campo finito GF(2^m) são dados por

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

3.2. CAMPOS FINITOS

3.2.1. 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.

EXEMPLO 3.1

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

$1 + X + X^4$ não divide nenhum outro $X^n + 1$ para $1 \le n < 15$. .

$m = 4$

$n = 2^m - 1$

$n = 2^4 - 1 = 15$

$X^{15} + 1 \Rightarrow \text{Resto} = 0$

$X^{14} + 1 \Rightarrow \text{Resto} \neq 0$

$\vdots$

$X^4 + 1 \Rightarrow \text{Resto} \neq 0$

Logo, $1 + X + X^4$ é primitivo

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

3.2. CAMPOS FINITOS

3.2.1. DEFINIÇÃO DE UM CAMPO FINITO POR UM POLINÔMIO PRIMITIVO

- 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 apresenta alguns polinômios primitivos de ordem 3 até 24.

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**	$1 + X + X^2 + X^7 + X^{24}$

3.2. CAMPOS FINITOS

3.2.1. DEFINIÇÃO DE UM CAMPO FINITO POR UM POLINÔMIO PRIMITIVO

Tabela - $GF(2^4)$ gerado por $p(X) = 1 + X + X^4$

$$\alpha = (0100)$$
$$+$$
$$\alpha = (0100)$$
$$\text{---------}$$
$$(0000)$$

REPRESENTAÇÕES					
POR POTÊNCIA	POLINOMIAL	VETORIAL	POR POTÊNCIA	POLINOMIAL	VETORIAL
0	0	(0000)	α^7	$1 + \alpha + \alpha^3$	(1101)
$\alpha^0 = 1$	1	(1000)	α^8	$1 + \alpha^2$	(1010)
α^1	α	(0100)	α^9	$\alpha + \alpha^3$	(0101)
α^2	α^2	(0010)	α^{10}	$1 + \alpha + \alpha^2$	(1110)
α^3	α^3	(0001)	α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0111)
α^4	$1 + \alpha$	(1100)	α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1111)
α^5	$\alpha + \alpha^2$	(0110)	α^{13}	$1 + \alpha^2 + \alpha^3$	(1011)
α^6	$\alpha^2 + \alpha^3$	(0011)	α^{14}	$1 + \alpha^3$	(1001)

A adição entre dois elementos de campo é mais facilmente realizável com os elementos em sua representação polinomial.

$$\alpha^5 + \alpha^7 = \alpha + \alpha^2 + 1 + \alpha + \alpha^3 = 1 + \alpha^2 + \alpha^3 = \alpha^{13}$$

O produto entre dois elementos α^7 e α^{12}.

$$\alpha^7 \cdot \alpha^{12} = \alpha^{19}$$

Note que $\alpha^{19} > \alpha^{14}$ e assim, o expoente deve ser reduzido fazendo, $19 \div (2^m - 1) = 19 \div 15 = 1$ e o resto é 4.

$$\alpha^7 \cdot \alpha^{12} = \alpha^{19} = \alpha^4$$

3.2. CAMPOS FINITOS

3.2.1. DEFINIÇÃO DE UM CAMPO FINITO POR UM POLINÔMIO PRIMITIVO

REPRESENTAÇÕES					
POR POTÊNCIA	POLINOMIAL	VETORIAL	POR POTÊNCIA	POLINOMIAL	VETORIAL
0	0	(0000)	α^7	$1 + \alpha + \alpha^3$	(1101)
$\alpha^0 = 1$	1	(1000)	α^8	$1 + \alpha^2$	(1010)
α^1	α	(0100)	α^9	$\alpha + \alpha^3$	(0101)
α^2	α^2	(0010)	α^{10}	$1 + \alpha + \alpha^2$	(1110)
α^3	α^3	(0001)	α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0111)
α^4	$1 + \alpha$	(1100)	α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1111)
α^5	$\alpha + \alpha^2$	(0110)	α^{13}	$1 + \alpha^2 + \alpha^3$	(1011)
α^6	$\alpha^2 + \alpha^3$	(0011)	α^{14}	$1 + \alpha^3$	(1001)

A divisão entre dois elementos deve ser feita por meio do produto do dividendo pelo inverso do divisor, lembrando que:

$$\frac{\alpha^i}{\alpha^j} = \alpha^i \cdot \alpha^{-j} = \alpha^i \cdot (\alpha^0 \cdot \alpha^{-j}) = \alpha^i \cdot (\alpha^{2^m-1} \cdot \alpha^{-j})$$

Seja o $GF(2^4)$ gerado por $p(X) = 1 + X + X^4$. A divisão de α^7 por α^{12} é:

$$\frac{\alpha^7}{\alpha^{12}} = \alpha^7 \cdot \alpha^{-12} = \alpha^7 \cdot (\alpha^{2^m-1} \cdot \alpha^{-12}) = \alpha^7 \cdot (\alpha^{15} \cdot \alpha^{-12}) = \alpha^{10}$$

$$\frac{\alpha^7}{\alpha^{12}} = \alpha^{10}$$

Inatel
CAMINHOS QUE CONECTAM COM O FUTURO

3.2. CAMPOS FINITOS

3.2.2. 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,

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

$$\alpha^3 = 1 + \alpha$$

3.2. CAMPOS FINITOS

3.2.2. O CAMPO DE EXTENSÃO GF(2^3)

- 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				
α^0				
α^1				
α^2				
α^3	1	1	0	$\alpha^3 = 1 + \alpha$
α^4				
α^5				
α^6				

3.2. CAMPOS FINITOS

3.2.2. O CAMPO DE EXTENSÃO GF(2^3)

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

3.3. CODIFICAÇÃO RS

- Os termos dos parâmetros *n*, *k*, *t*, para a forma mais comum dos códigos RS, tem-se que

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

onde $n - k = 2t$ é o número de símbolos de paridade, t é a capacidade de correção de erro de símbolo do código.

- O polinômio gerador para um código RS assume a seguinte forma:

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

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

- Logo. existe $2t$ 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

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

3.3. CODIFICAÇÃO RS

- 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:

$$g(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^3)(X - \alpha^4)$$

$$= (X^2 - (\alpha + \alpha^2)X + \alpha^3)(X^2 - (\alpha^3 + \alpha^4)X + \alpha^7)$$

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

$$= (X^4 - (\alpha^4 + \alpha^6)X^3 + (\alpha^3 + \alpha^{10} + \alpha^0)X^2 + (\alpha^4 + \alpha^9)X + \alpha^3$$

$$= X^4 - \alpha^3 X^3 + \alpha^0 X^2 - \alpha^1 X + \alpha^3$$

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

- 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:

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

3.3. CODIFICAÇÃO RS

3.3.1. CODIFICAÇÃO NA FORMA SISTEMÁTICA

- 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,

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

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.

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

- A palavra código polinomial resulta em

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

3.3. CODIFICAÇÃO RS

3.3.1. CODIFICAÇÃO NA FORMA SISTEMÁTICA

Exemplo 3.2

Considere a mensagem da sequência binária 010110111. Faça a codificação sistemática da mensagem com um código RS (7, 3). Para geração dos símbolos em GF(2^3), considere o polinômio primitivo de grau 3 apresentado na Tabela de polinômios.

A sequência 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 mostra a Tabela

	ELEMENTOS			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	$\alpha^4 = \alpha + \alpha^2$
α^5	1	1	1	$\alpha^5 = 1 + \alpha + \alpha^2$
α^6	1	0	1	$\alpha^6 = 1 + \alpha^2$

010 → α^1

110 → α^3

111 → α^5

Inatel
CAMINHOS QUE CONECTAM COM O FUTURO

3.3. CODIFICAÇÃO RS

3.3.1. CODIFICAÇÃO NA FORMA SISTEMÁTICA

Exemplo 3.2

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

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 1 e 2, respectivamente.

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

3.3. CODIFICAÇÃO RS

3.3.1. CODIFICAÇÃO NA FORMA SISTEMÁTICA

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

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

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

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

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

Assim, usando a Equação: $c(X) = p(X) + X^{n-k} m(X)$ tem-se:

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

3.4. DECODIFICAÇÃO RS

- 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 anterior 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 pela Equação

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

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

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

3.4. DECODIFICAÇÃO RS

- 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. Consequentemente, o polinômio código recebido pode ser obtido a partir de

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

que resulta em

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

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

- 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.

3.4. DECODIFICAÇÃO RS

3.4.1. CÁLCULO DA SÍNDROME

- Para o código RS (7, 3), aqui considerado, cada vetor síndrome possui quatro símbolos, ou seja $2t$.
- 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

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

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

3.4. DECODIFICAÇÃO RS

3.4.1. CÁLCULO DA SÍNDROME

- Para o polinômio recebido r(X) apresentado na Equação

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

os quatro símbolos da síndrome são:

$$S_1 = r(\alpha) = \alpha^0 + \alpha^2\alpha + \alpha^4\alpha^2 + \alpha^0\alpha^3 + \alpha^1\alpha^4 + \alpha^2\alpha^5 + \alpha^5\alpha^6$$
$$= \alpha^0 + \alpha^3 + \alpha^6 + \alpha^3 + \alpha^5 + \alpha^0 + \alpha^4 = \alpha^2$$

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

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

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

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

3.4. DECODIFICAÇÃO RS

3.4.2. LOCALIZAÇÃO DE ERRO

- De acordo com a Equação

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

, 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

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

que mostra claramente os valores dos erros e suas posições.

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

- Existem dois erros: um na posição X^3 e outro na posição X^5, 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.

3.4. DECODIFICAÇÃO RS

3.4.2. LOCALIZAÇÃO DE ERRO

- 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 que 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, pode-se formar uma matriz a partir das síndromes, onde as primeiras t síndromes são utilizadas para determinar as próximas síndromes.

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

3.4. DECODIFICAÇÃO RS

3.4.2. LOCALIZAÇÃO DE ERRO

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

$$S_1 = \alpha^2 \qquad S_2 = 0 \qquad S_3 = \alpha^3 \qquad S_4 = \alpha^5$$

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

$$\begin{cases} S_1\sigma_2 + S_2\sigma_1 = S_3 \\ S_2\sigma_2 + S_3\sigma_1 = S_4 \end{cases} \Rightarrow \begin{cases} \alpha^2\sigma_2 + 0\,\sigma_1 = \alpha^3 \rightarrow \alpha^2\sigma_2 = \alpha^3 \rightarrow \sigma_2 = \alpha^3/\alpha^2 \rightarrow \sigma_2 = \alpha \\ 0\,\sigma_2 + \alpha^3\sigma_1 = \alpha^5 \rightarrow \alpha^3\sigma_1 = \alpha^5 \rightarrow \sigma_1 = \alpha^5/\alpha^3 \rightarrow \sigma_1 = \alpha^2 \end{cases}$$

$$\sigma(X) = 1 + \sigma_1 X + \sigma_2 X^2 \qquad \Rightarrow \qquad \sigma(X) = 1 + \alpha^2 X + \alpha X^2$$

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

3.4. DECODIFICAÇÃO RS

3.4.2. LOCALIZAÇÃO DE ERRO

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

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

- 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.

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

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

3.4. DECODIFICAÇÃO RS

3.4.2. LOCALIZAÇÃO DE ERRO

- 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,

$$\frac{1}{\alpha^2} = \alpha^5 \Rightarrow \text{Posição } X^5$$

$$\frac{1}{\alpha^4} = \alpha^3 \Rightarrow \text{Posição } X^3$$

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

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

$$\hat{e}(X) = e_3 X^3 + e_5 X^5$$

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.

3.4. DECODIFICAÇÃO RS

3.4.3. 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. Assim, de

$$S_1 = \mathrm{r}(\alpha) = e_0\,\alpha^0 + e_1\,\alpha^1 + \cdots + e_{n-1}\,\alpha^{n-1}$$
$$S_2 = \mathrm{r}(\alpha^2) = e_0(\alpha^2)^0 + e_1(\alpha^2)^1 + \cdots + e_{n-1}(\alpha^2)^{n-1}$$
$$\vdots$$
$$S_{2t} = \mathrm{r}(\alpha^{2t}) = e_0(\alpha^{2t})^0 + e_1(\alpha^{2t})^1 + \cdots + e_{n-1}(\alpha^{2t})^{n-1}$$

$$S_1 = \mathrm{r}(\alpha) = e_3\alpha^3 + e_5\alpha^5 = \alpha^2$$
$$S_2 = \mathrm{r}(\alpha^2) = e_3\alpha^6 + e_5\alpha^{10} = 0$$

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

para as síndromes S_1 e S_2 obtém-se,

$$\begin{cases} \alpha^3 e_3 + \alpha^5 e_5 = \alpha^2 \\ \alpha^6 e_3 + \alpha^{10} e_5 = 0 \end{cases} \qquad \begin{cases} \alpha^3 e_3 + \alpha^5 e_5 = \alpha^2\,(\alpha^5) \\ \alpha^6 e_3 + \alpha^{10} e_5 = 0 \end{cases} \qquad \begin{cases} \alpha^8 e_3 + \alpha^{10} e_5 = \alpha^7 \\ \alpha^6 e_3 + \alpha^{10} e_5 = 0 \end{cases}$$

$$\begin{cases} \alpha^1 e_3 + \alpha^{10} e_5 = \alpha^7 \\ \alpha^6 e_3 + \alpha^{10} e_5 = 0 \end{cases} \qquad \alpha^5 e_3 = \alpha^7 \qquad e_3 = \frac{\alpha^7}{\alpha^5} \Rightarrow e_3 = \alpha^2$$

$$\alpha^6 e_3 + \alpha^{10} e_5 = 0 \Rightarrow \alpha^6\alpha^2 + \alpha^{10} e_5 = 0 \Rightarrow e_5 = \frac{\alpha^8}{\alpha^{10}} \Rightarrow e_5 = \alpha^{-2}.\alpha^7 \Rightarrow e_5 = \alpha^5 \qquad \hat{e}(X) = \alpha^2 X^3 + \alpha^5 X^5$$

3.4. DECODIFICAÇÃO RS

3.4.4. CORREÇÃO DO POLINÔMIO RECEBIDO COM O POLINÔMIO DE ERRO ESTIMADO

- O polinômio transmitido estimado é obtido fazendo:

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

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

$$+$$

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

$$=$$

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

0
α^0
α^1
α^2
$\alpha^3 = 1 + \alpha$
$\alpha^4 = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha + \alpha^2$
$\alpha^6 = 1 + \alpha^2$

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

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

* * *