TE111 – Comunicação Digital

Introdução à Codificação de Canal

Evelio M. G. Fernández

13 de novembro de 2018

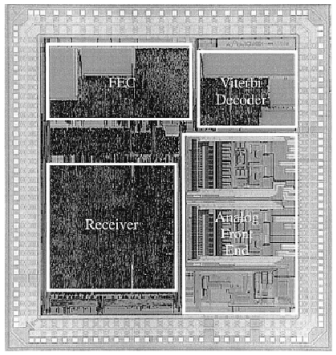
Notes

Quais os Benefícios da Codificação de Canal?

1. O uso de codificação de canal pode: aumentar a faixa de operação de um sistema de comunicação, reduzir a taxa de erros, diminuir os requerimentos de potência transmitida ou uma combinação destes benefícios.
2. Um bom projeto de sistema de comunicação precisa encontrar o melhor compromisso entre largura de banda, potência e taxa de erro de bits para uma determinada aplicação.

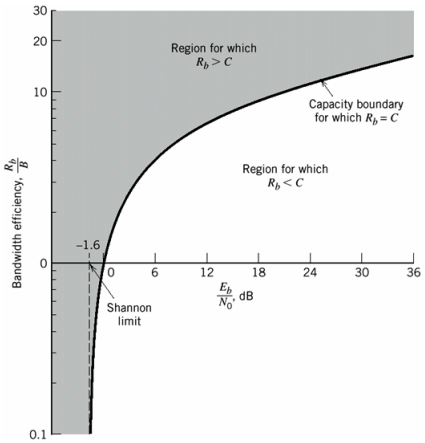
Notes

Chip de um Receptor de Satélite



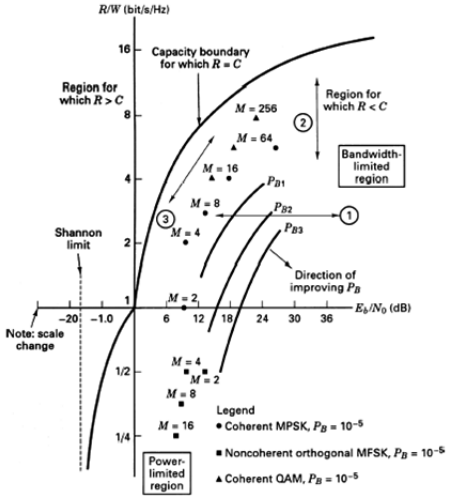
Notes

Eficiência Espectral



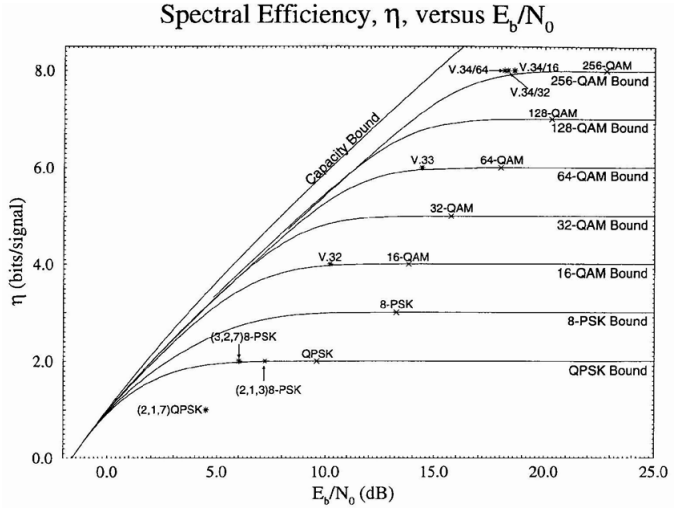
Notes

Eficiência Espectral



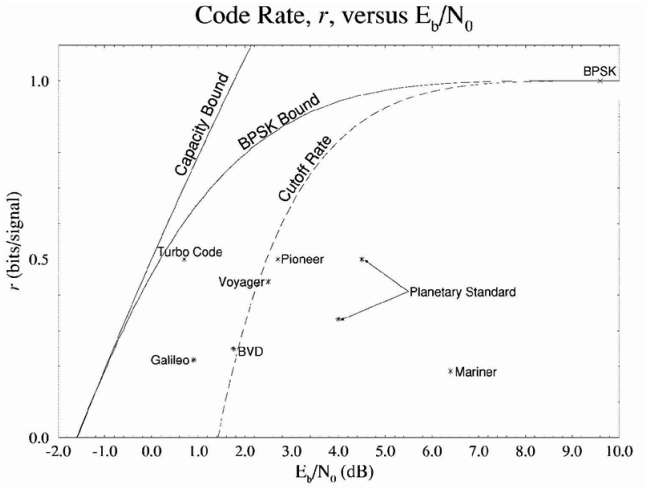
Notes

Eficiência Espectral com Codificação de Canal



Notes

Eficiência Espectral com Codificação de Canal – BPSK



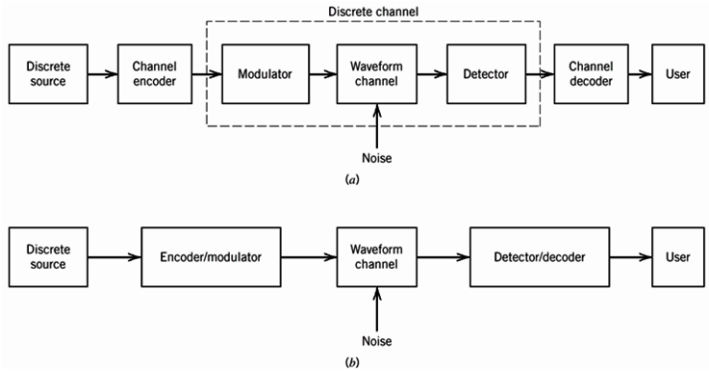
Notes

Exemplos de Esquemas de Codificação de Canal

- Disco Compacto: Utiliza códigos de Reed-Solomon (RS) concatenados em um esquema conhecido como CIRC (*cross-interleaved RS code*);
- Comunicação por Satélite: O padrão DVB-S utiliza um código convolucional puncionado de taxa $1/2$ e $K = 7$ concatenado com um código RS (204, 188);
- Sistemas COFDM (DVB-T, 802.11a): Utilizam códigos convolucionais concatenados com códigos RS em esquemas similares aos utilizados em comunicação por satélite;
- Gigabit Ethernet: Utiliza modulação codificada (TCM: Trellis-Coded Modulation) para atingir ganho de codificação de 6 dB.

Notes

Sistema de Comunicação com Codificação de Canal



Notes

Sistema de Comunicação com Codificação de Canal

Principal problema de engenharia a ser resolvido: Projetar e implementar o codificador/decodificador de canal de tal forma que:

- A informação possa ser transmitida (ou armazenada) em um ambiente ruidoso tão rápido (ou tão densamente) quanto possível;
- A informação possa ser reproduzida de forma confiável na saída do decodificador;
- O custo de implementação do codificador e do decodificador esteja dentro de limites aceitáveis.

Notes

Alguns Códigos BCH (*Bose-Chaudhuri-Hocquenghem*)

BCH Codes (Partial Catalog)

n	k	t
7	4	1
15	11	1
	7	2
	5	3
31	26	1
	21	2
	16	3
	11	5
63	57	1
	51	2
	45	3
	39	4
	36	5
	30	6
127	120	1
	113	2
	106	3
	99	4
	92	5
	85	6
	78	7
	71	9
	64	10
	57	11
	50	13
	43	14
	36	15
	29	21
	22	23
	15	27
	8	31

n	k	t	Coding Gain, G (dB) MPSK, $P_B = 10^{-9}$
31	26	1	2.0
63	57	1	2.2
	51	2	3.1
127	120	1	2.2
	113	2	3.3
	106	3	3.9

Notes

Códigos de Bloco

Códigos de Bloco Binários

Um código de bloco binário de tamanho M e comprimento de bloco n é um conjunto de M palavras binárias de comprimento n bits, chamadas de palavras-código. Geralmente, $M = 2^k$, k inteiro $\Rightarrow$ código (n, k).

Notes

Distância de Hamming Mínima

Seja $C = \{c_l | l = 0,1,\ldots,M-1\}$ um código de bloco binário composto por M palavras-código de comprimento n.

O **peso de Hamming**, $w(c)$, de uma palavra-código é igual ao número de posições diferentes de zero na palavra-código;

A **distância de Hamming**, $d(c_i, c_j)$, entre duas palvaras-código c_i e c_j é o número de posições em que c_i e c_j diferem;

A **distância de Hamming mínima**, $d_{\min}$, do código C é a distância de Hamming entre as duas palavras-código com menor distância de Hamming entre elas. Ou seja,

$$d_{\min} = \min_{\substack{c_i, c_j \in C \\ i \neq j}} d(c_i, c_j);$$

Capacidade de correção de erros: $t = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$.

Notes

Códigos de Bloco Lineares

Um código de bloco binário é linear se a soma módulo-2 bit a bit de quaisquer subconjunto de palavras-código resulta numa outra palavra código;

Um código de bloco binário linear é um subespaço vetorial de GF$(2)^n$, o espaço vetorial das n-uplas binárias;

Alguns códigos elementares:

- Códigos de paridade simples: $C(k, k+1)$ ou $C(n, n-1)$;
- Códigos de repetição: $C(n, 1)$;
- Códigos de Hamming: $C(2^m - 1, 2^m - 1 - m), \quad m \geq 3.$

Notes

Descrição de Códigos de Bloco Lineares por Matrizes

Matriz Geradora: $\mathbf{G}_{[k\times n]}$

Equação de codificação: $\mathbf{c} = \mathbf{mG}$, onde $\mathbf{m}_{[1\times k]} \rightarrow$ vetor mensagem

Exemplo: Considere $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$.

Qual a palavra-código correspondente à mensagem $\mathbf{m} = [0\,1\,1]$?

Notes

Descrição de Códigos de Bloco Lineares por Matrizes

- $C \rightarrow$ subespaço de GF$(2)^n$, de dimensão k;
- $C^{\perp} \rightarrow$ complemento ortogonal $=$ conjunto de todos os vetores ortogonais aos vetores de C;
- $C^{\perp} \rightarrow$ também é um subespaço de GF$(2)^n$, de dimensão $n-k$;
- $C^{\perp} =$ Código dual de C composto por 2^{n-k} palavras de GF$(2)^n$;
- Seja $\mathbf{H}_{[(n-k)\times n]} \rightarrow$ matriz contendo uma base para $C^{\perp}$,

$\Longrightarrow \mathbf{cH}^T = \mathbf{0} \rightarrow$ equação de verificação de paridade,

$\Longrightarrow \mathbf{H}_{[(n-k)\times n]} \rightarrow$ Matriz de verificação de paridade de C.

Notes

Codificação Sistemática

Matriz geradora na forma sistemática: $\mathbf{G} = \left[\mathbf{I}_k \,|\, \mathbf{P}_{[k\times(n-k)]}\right]$.

- Qualquer matriz geradora pode ser transformada na forma sistemática através de uma sequência de operações elementares sob as linhas seguida de permutações de colunas $\Longrightarrow$ códigos equivalentes;
- Todo código de bloco linear é equivalente a um código que pode ser codificado por um codificador sistemático.

Matriz de verificação de paridade na forma sistemática:

$$\mathbf{H} = \left[-\mathbf{P}^T_{[(n-k)\times k]} \,|\, \mathbf{I}_{n-k}\right].$$

Exemplo: Seja $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$.

Obtenha as matrizes geradora e de verificação de paridade na forma sistemática.

Notes

Arranjo Padrão para Códigos Binários

$\mathbf{c}_1 = \mathbf{0}$	$\mathbf{c}_2$	$\mathbf{c}_3$	$\ldots$	$\mathbf{c}_i$	$\ldots$	$\mathbf{c}_{2^k}$
$\mathbf{e}_2$	$\mathbf{c}_2 + \mathbf{e}_2$	$\mathbf{c}_3 + \mathbf{e}_2$	$\ldots$	$\mathbf{c}_i + \mathbf{e}_2$	$\ldots$	$\mathbf{c}_{2^k} + \mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{c}_2 + \mathbf{e}_3$	$\mathbf{c}_3 + \mathbf{e}_3$	$\ldots$	$\mathbf{c}_i + \mathbf{e}_3$	$\ldots$	$\mathbf{c}_{2^k} + \mathbf{e}_3$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\mathbf{e}_j$	$\mathbf{c}_2 + \mathbf{e}_j$	$\mathbf{c}_3 + \mathbf{e}_j$	$\ldots$	$\mathbf{c}_i + \mathbf{e}_j$	$\ldots$	$\mathbf{c}_{2^k} + \mathbf{e}_j$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\mathbf{e}_{2^{n-k}}$	$\mathbf{c}_2 + \mathbf{e}_{2^{n-k}}$	$\mathbf{c}_3 + \mathbf{e}_{2^{n-k}}$		$\mathbf{c}_i + \mathbf{e}_{2^{n-k}}$		$\mathbf{c}_{2^k} + \mathbf{e}_{2^{n-k}}$

Para um dado canal, a probabilidade de erro na decodificação é minimizada quando os padrões de erro mais prováveis de acontecer são selecionados como líderes de cosets.

Notes

Decodificação por Síndrome

Seja: $\mathbf{r} \rightarrow$ palavra recibida.
$\Longrightarrow \mathbf{r} = \mathbf{c} + \mathbf{e}$.

Cálculo da síndrome:

$$\mathbf{s} = \mathbf{r}\mathbf{H}^T = \mathbf{c}\mathbf{H}^T + \mathbf{e}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T$$

Todos os vetores em um mesmo coset têm a mesma síndrome.

Procedimento de decodificação para códigos de bloco:

1. Dado $\mathbf{r}$, calcular $\mathbf{s} = \mathbf{r}\mathbf{H}^T$;
2. Identificar o líder de coset correspondente, $\mathbf{e}$;
3. Calcular $\widehat{\mathbf{c}} = \mathbf{r} + \mathbf{e}$.

Notes

Singleton Bound e *Hamming Bound*

- **Singleton Bound:** A distância mínima de qualquer código de bloco (n, k) satisfaz,
$$d_{\min} \leq n - k + 1;$$
- Códigos com $d_{\min} = n - k + 1$ são chamados de códigos de distância máxima (MDS: *Maximum-Distance Separable*);
- **Hamming Bound:** $2^{n-k} \geq \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}$;
- **Códigos perfeitos:** Satisfazem o Hamming Bound com a igualdade:
  - Códigos de repetição $C(n, 1)$, n ímpar;
  - Códigos de Hamming binários;
  - Códigos de Hamming não binários;
  - Código de Golay binário $C(23, 12)$, $t = 3$;
  - Código de Golay ternário $C(11, 6)$, $t = 2$.

Notes

Exemplo – Código (6,3)

Considere um código de bloco binário linear com

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

000000	110100	011010	101110	101001	011101	110011	000111
000001	110101	011011	101111	101000	011100	110010	000110
000010	110110	011000	101100	101011	011111	110001	000101
000100	110000	011110	101010	101101	011001	110111	000011
001000	111100	010010	100110	100001	010101	111011	001111
010000	100100	001010	111110	111001	001101	100011	010111
100000	010100	111010	001110	001001	111101	010011	100111
010001	100101	001011	111111	111000	001100	100010	010110

Construa uma tabela de síndromes para este código. É um código perfeito o quase perfeito?

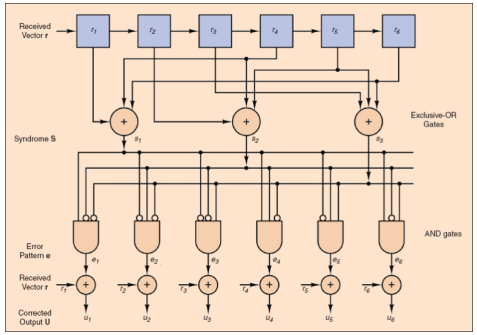
Notes

Exemplo: Decodificador do Código (6, 3)

$$\mathbf{s} = \mathbf{r}\mathbf{H}^T$$

$$\mathbf{s} = [r_1\, r_2\, r_3\, r_4\, r_5\, r_6] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$s_1 = r_1 + r_4 + r_6$$
$$s_2 = r_2 + r_4 + r_5$$
$$s_3 = r_3 + r_5 + r_6$$



Notes

Códigos Cíclicos

Um código de bloco linear é um **código cíclico** se cada deslocamento cíclico das palavras-código é também uma palavra-código.

Vantagens:

- Descrição algébrica elegante;
  - $c(x) = m(x)g(x),\ g(x) \rightarrow$ polinômio gerador;
  - $c(x)h(x) = 0 \mod (x^{n-1}) \rightarrow h(x)$: polinômio de verificação de paridade;
  - $c(\beta_1) = 0, \ldots, c(\beta_t) = 0$, onde $\beta_i \in \text{GF}(p^m)$;
- Codificação e cálculo de síndromes utilizando registradores de deslocamento;
- Correção de surtos de erros;
- Correção de erros aleatórios através da solução de equações de polinômios.

Notes

Códigos Cíclicos: Representação Polinomial

Palavra-código: $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}, \quad c_i \in \text{GF}(p)$

Deslocamento cíclico: $xc(x) \rightarrow$ deslocamento cíclico no tempo ou rotação à direita sujeita à condição

$$x^n = 1 \text{ ou } x^n - 1 = 0 \quad (x^n + 1 = 0 \text{ para códigos binários})$$

Polinômio gerador: $g(x) = 1 + g_1 x + g_2 x^2 + \cdots + g_{n-k} x^{n-k}$

$$\Rightarrow c(x) = a(x)g(x) \mod (x^{n-1})$$

onde:

- Grau $[c(x)] \leq n - 1$;
- Grau $[g(x)] = n - k$;
- Grau $[a(x)] \leq k - 1$;
- $a(x)$: polinômio associado à mensagem a ser codificada na palavra código $c(x)$.

Seja $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$

$$\Rightarrow a(x)g(x) = \underbrace{a_0 g(x)}_{\in C} + \underbrace{a_1 x g(x)}_{\in C} + \underbrace{a_2 x^2 g(x)}_{\in C} + \cdots + \underbrace{a_{k-1} x^{k-1} g(x)}_{\in C}$$

$\Longrightarrow$ $a(x)g(x) =$ combinação linear de palavras-código que resulta em uma outra palavra-código de C.

Notes

Código Cíclico Sistemático

$$\mathbf{c} = \left[\underbrace{p_0, p_1, \ldots, p_{n-k-1}}_{n-k \text{ bits de cheque de paridade}} , \underbrace{m_0, m_1, \ldots, m_{k-1}}_{k \text{ bits de mensagem}} \right]$$

Seja $m(x)$: polinômio-mensagem,

$$m(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}.$$

Então, $c(x)$: polinômio-código resultante da codificação sistemática,

$$c(x) = \underbrace{p_0 + p_1 x + \cdots + p_{n-k-1} x^{n-k-1}}_{p(x)} + \underbrace{m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}}_{x^{n-k} m(x)}.$$

Sabendo que $c(x) = a(x)g(x)$,

$$\Longrightarrow \frac{x^{n-k} m(x)}{g(x)} = a(x) - \frac{p(x)}{g(x)},$$

$\Longrightarrow$ $p(x) \rightarrow$ resto da divisão de $x^{n-k} m(x)$ por $g(x)$.

Notes

Procedimento para Codificação Sistemática

1. $m(x)x^{n-k} = ?$
2. Resto da divisão $\dfrac{x^{n-k} m(x)}{g(x)} = p(x)?$
3. $p(x) + x^{n-k} m(x) = c(x).$

Exemplo: Sejam $m(x) = 1 + x^3$, $g(x) = 1 + x + x^3$, $C(7,4)$. Qual a palavra-código correspondente à $m(x)$?

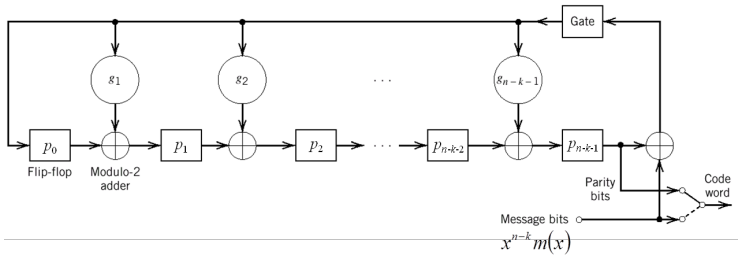
Fatoração de $x^7 + 1$ em polinômios irredutíveis em GF(2):

$$(x^7 + 1) = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

- 2 polinômios de grau 4 (geradores de códigos (7, 3));
- 2 polinômios de grau 3 (geradores de códigos (7, 4));
- 1 polinômio de grau 1 (geradores de códigos (7, 6)).

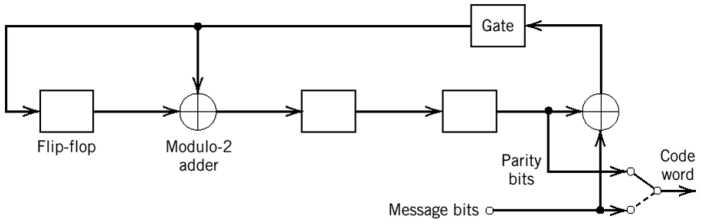
Notes

Codificador de um Código Cíclico (n, k)



Notes

Codificador do Código Cíclico (7, 4)



Notes

Cálculo da Síndrome

Seja $r(x) = r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}$ → polinômio recebido.

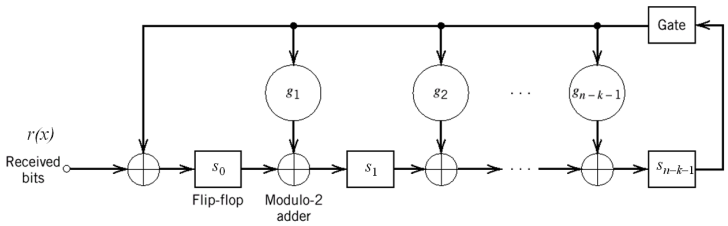
Sabendo que $r(x) = c(x) + e(x)$, então polinômio síndrome correspondente, $s(x)$, de grau $\leq n - k - 1$, pode ser calculado como:

$$\begin{aligned} s(x) &= r(x) \text{ modulo-}[g(x)] \\ &= c(x) \text{ modulo-}[g(x)] + e(x) \text{ modulo-}[g(x)] \\ &= e(x) \text{ modulo-}[g(x)] \end{aligned}$$

$\Longrightarrow$ $s(x)$ é também a síndrome do polinômio que representa o padrão de erro.

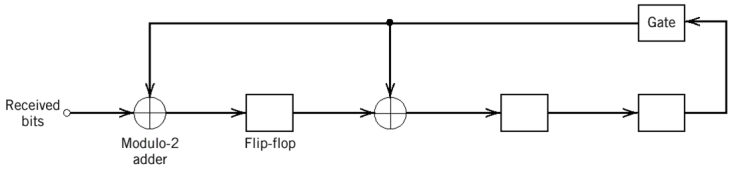
Notes

Circuito de Cálculo das Síndromes



Notes

Cálculo de Síndromes – Código (7, 4)



Notes

Propriedades do Polinômio Síndrome

1. A síndrome de um polinômio recebido também é a síndrome do polinômio erro correspondente;
2. Se $s(x)$ é a síndrome de $r(x)$, então a síndrome de $xr(x)$ será $xs(x)$, isto é,

$$xr(x) = xq(x)g(x) + xs(x)$$

   Em geral, $x^i s(x) \rightarrow$ síndrome de $x^i r(x)$;
3. $s(x)$ é idêntico a $e(x)$ supondo que os erros estejam confinados aos $n - k$ bits de verificação de paridade.

Notes

Códigos CRC

Códigos de verificação de redundância cíclica (CRC: *Cyclic Redundancy Check*). Podem detectar:

- Todos os surtos de erro de tamanho $n-k$ ou inferior, incluindo surtos do tipo *end-around*;
- Uma fração dos surtos iguais ou maiores que $n-k+1$. A fração é igual a $1-2^{n-k-1}$;
- Para $l \geq n-k+1$, a fração de surtos não detectáveis de comprimento l é igual a $2^{-(n-k)}$;
- Todas as combinações de $d_{\min}-1$ ou menos erros;
- Todos os padrões de erro com um número ímpar de erros se o polinômio gerador do código tiver um número par de coeficientes diferentes de zero.

Exemplos:

- CRC – 12 $\rightarrow g(x) = 1 + x + x^2 + x^3 + x^{11} + x^{12}$;
- CRC – 16 $\rightarrow g(x) = 1 + x^2 + x^{15} + x^{16}$;
- CRC – ITU $\rightarrow g(x) = 1 + x^5 + x^{12} + x^{16}$.

Notes

Exercício 1

Procura-se um código cíclico não sistemático para proteger blocos de informação de 8 bits. Para isso, um polinômio gerador de grau 7 é utilizado.

a) Quais serão os valores de n e k do código?
b) Mostre que o polinômio $g(x) = x^7 + x^6 + x^4 + 1$ pode ser usado.
c) Encontre a palavra-código associada ao byte $\mathrm{A1}_{\mathrm{HEX}}$.
d) Calcule a síndrome associada à palavra recebida $\mathbf{r} = [0000111101100001]$.
e) Mostre que o código não pode detectar 4 erros.

Notes

Exercício 2

Alguns testes foram realizados num canal onde se pretende melhorar o desempenho com a utilização de um código de Hamming. Foram enviados um total de 10^9 bits e na saída do canal foram constatados um total de $7{,}85 \times 10^5$ bits errados.

a) Faça uma estimativa da taxa de erro de bits do canal supondo um modelo BSC.

b) Determine o tamanho máximo do bloco codificado que pode ser usado com segurança se até um erro for permitido por cada bloco. Após esse cálculo considere $n = 511$.

c) Qual a probabilidade de um bloco não conter erros?

d) Qual a probabilidade de um bloco conter exatamente um erro?

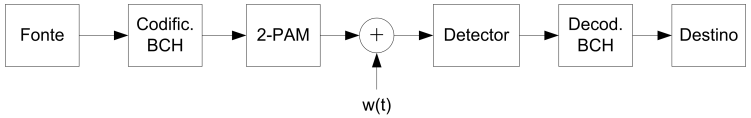
e) Qual a probabilidade de dois ou mais erros em um bloco?

f) Quantos bits de redundância são necessários considerando que desejamos $d_{\min} = 3$?

Notes

Exercício 3

Considere o seguinte esquema de transmissão digital em que o código BCH utilizado tem parâmetros $n = 31$, $k = 16$ e capacidade de correção de erros, $t = 3$.



a) Determine a relação E_b/N_0 necessária para se atingir uma taxa de erro de bits de pelo menos 10^{-4} considerando o sistema sem a utilização de codificação de canal.

b) Determine a taxa erro de bits do sistema utilizando codificação de canal e operando com a relação sinal-ruído calculada na parte (a).

Notes

Códigos Cíclicos Binários *vistos* a partir de GF(2^m)

Seja $g(x)$ o polinômio gerador de um código cíclico binário de comprimento $n = 2^m - 1$ com zeros $\beta_1, \beta_2, \ldots, \beta_r$ em GF(2^m). O polinômio $c(x)$ sobre GF(2) é um polinômio código se e somente se

$$c(\beta_1) = c(\beta_2) = \cdots = c(\beta_r) = 0$$

onde $c(\beta_i)$ é avaliado em GF(2^m).

BCH bound: Se um código cíclico linear é construído de forma que:

- Cada palavra-código tem n bits;
- β é um elemento de ordem n em GF(2^m);
- O polinômio gerador do código, $g(x)$, inclui, entre suas raízes, $(\delta - 1)$ potências consecutivas de β;

então, é garantido que o código tem distância mínima igual a δ ou maior.

Notes

Corpos Finitos

- Um corpo finito com q elementos é chamado de GF(q) (Galois Field);
- GF(p) = inteiros com aritmética módulo um número primo, p;
- GF(p^m) = polinômios sobre GF(p) com aritmética módulo um polinômio primo de grau m (extension field);
- Todo corpo finito é o espaço vetorial de m-uplas sobre o corpo GF(p) de inteiros com aritmética módulo um número primo p. Portanto, GF(q) = GF(p^m);
- GF(2^m) = espaço vetorial de m-uplas binárias conjuntamente com operações de soma módulo-2 e multiplicação módulo um polinômio binário primitivo de grau m.

Notes

Construção de Corpos Finitos

- **Exemplo:** Considerando GF(p) = inteiros com aritmética módulo um número primo, p, construir GF(7).
- Para cada elemento $a \in$ GF(p), $a \neq 0$, haverá um menor inteiro, n, tal que $a^n = 1$, $\implies$ n : ordem de a;
- Seja a um elemento diferente de zero em GF(q). Seja n a ordem de a. Então, n divide $q-1$ $\implies$ $a^{(q-1)} = 1$;
- Se a ordem de a for $q-1$, então a é um elemento primitivo de GF(q);
- **Exemplo:** Qual é o elemento primitivo de GF(7)?
- Seja α um elemento primitivo de GF(q), então

$$\text{GF}(q) = \{0,1,\alpha,\alpha^2,\ldots,\alpha^{q-2}\}.$$

Notes

Soma e Produto Módulo-8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	0	3	6	1
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Notes

Soma Módulo-2 (bit-a-bit) das 3-uplas

	000	**001**	**010**	**011**	**100**	**101**	**110**	**111**
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

Notes

Operação de "Multiplicação" das 3-uplas

	001	**010**	**011**	**100**	**101**	**110**	**111**
001	001	010	011	100	101	110	111
010	010	100	110	011	001	111	101
011	011	110	101	111	100	001	010
100	100	011	111	110	010	101	001
101	101	001	100	010	111	011	110
110	110	111	001	101	011	010	100
111	111	101	010	001	110	100	011

Notes

Construção de GF(2^m)

- Seja α um elemento primitivo de GF(2^m), então

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

- Um polinômio irredutível, $p(x)$, de grau m sobre GF(2) é um **polinômio primitivo** se tiver como raiz um elemento primitivo de GF(2^m) $\implies p(\alpha) = 0$;
- $\implies$ GF(2^m) = espaço vetorial de m-uplas binárias conjuntamente com operações de soma módulo-2 e multiplicação módulo um polinômio binário primitivo de grau m.

Notes

Construção de GF(2^3) a partir de $p(x) = x^3 + x + 1$

Potência de α	Polinômio	3-upla
0	0	000
1	1	001
α	α	010
α^2	α^2	100
α^3	$\alpha + 1$	011
α^4	$\alpha^2 + 1$	101
α^5	$\alpha^2 + \alpha$	110
α^6	$\alpha^2 + \alpha + 1$	111

Notes

GF(2^4) construído a partir de $p(x) = x^4 + x + 1$

Potência de α	Polinômio	4-upla
0	0	0000
1	1	1000
α	α	0100
α^2	α^2	0010
α^3	α^3	0001
α^4	$1 + \alpha$	1100
α^5	$\alpha + \alpha^2$	0110
α^6	$\alpha^2 + \alpha^3$	0011
α^7	$1 + \alpha + \alpha^3$	1101
α^8	$\alpha^2 + \alpha$	1010
α^9	$\alpha + \alpha^3$	0101
α^{10}	$1 + \alpha + \alpha^2$	1110
α^{11}	$\alpha + \alpha^2 + \alpha^3$	0111
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	1111
α^{13}	$1 + \alpha^2 + \alpha^3$	1011
α^{14}	$1 + \alpha^3$	1001

Notes

Propriedades de GF(2^m)

- Seja $f(x)$ um polinômio com coeficientes em GF(2). Seja β um elemento de GF(2^m). Se β é uma raiz de $f(x)$, então para qualquer $l \geq 0$, o elemento β^{2^l} também é uma raiz de $f(x)$. Elementos da forma β^{2^l} são chamados de conjugados de β;
- O **polinômio minimal**, $\phi(x)$, de β (e de seus conjugados) é o polinômio de menor grau com coeficientes em GF(2) tal que $\phi(\beta) = 0$;
- Sejam $\phi(x)$ o polinômio minimal de um elemento β em GF(2^m) e e o menor inteiro tal que $\beta^{2^e} = \beta$. Então,

$$\phi(x) = \prod_{i=0}^{e-1} (x + \beta^{2^i}).$$

- **Exercício:** Determine o polinômio minimal correspondente a $\beta = \alpha^3$ em GF(2^4).

Notes

Polinômios Minimais dos Elementos em GF(2^4)

Raizes Conjugadas	Polinômios Minimais
0	x
1	$x+1$
α,α^2,α^4,α^8	x^4+x+1
α^3,α^6,α^9,α^{12}	$x^4+x^3+x^2+x+1$
α^5,α^{10}	x^2+x+1
α^7,α^{11},α^{13},α^{14}	x^4+x^3+1

Notes

BCH Bound

Se um código cíclico linear é construído de forma que:

- Cada palavra-código tem n bits;
- β é um elemento de ordem n em GF(2^m);
- O polinômio gerador do código, $g(x)$, inclui, entre suas raízes, $(\delta-1)$ potências consecutivas de β;

então,

- é garantido que o código tem distância mínima igual a δ ou maior;
- $\delta \rightarrow$ distância de projeto.

Notes

Construção de Códigos BCH

- Para cada raiz β^r incluída em $g(x)$, existe um polinômio minimal $\phi_r(x)$ que tem β^r como raiz [i.e., $\phi_r(\beta^r) = 0$] e com coeficientes em GF(2).
- O polinômio gerador, com coeficientes binários, que contém todas as raízes necessárias pode ser obtido como sendo o mínimo comum múltiplo (LCM) de todos os polinômios minimais correspondentes às raízes utilizadas:

$$g(x) = \text{LCM}\{\phi_1(x),\phi_2(x),\ldots,\phi_{\delta-1}(x)\}.$$

Notes

Tipos de Códigos BCH

- Se $\beta = \alpha$ é um elemento primitivo de GF(2^m), o código BCH resultante é chamado de **código BCH primitivo** e as suas palavras-código têm comprimento $n = 2^m - 1$ bits:
  - $n = 2^m - 1$;
  - $k \geq n - mt$;
  - $d_{\min} \geq 2t + 1$;
  - O polinômio gerador do código, $g(x)$, é o polinômio de menor grau sobre GF(2) contendo $\alpha,\alpha^2,\alpha^3,\ldots,\alpha^{2t}$ como raízes;
- Se β não é um elemento primitivo de GF(2^m), o código BCH resultante é chamado de **código BCH não primitivo** e as suas palavras-código têm comprimento igual à ordem de β.

Exemplo: Encontrar o polinômio gerador de um código BCH primitivo com $n = 15$ e $t = 2$.

Notes

GF(2^6) construído a partir de $p(x) = x^6 + x + 1$

TABLE 6.2 GALOIS FIELD GF(2^6) WITH $p(\alpha) = 1 + \alpha + \alpha^6 = 0$

0	0						(0	0	0	0	0	0)
1	1						(1	0	0	0	0	0)
α		α					(0	1	0	0	0	0)
α^2			α^2				(0	0	1	0	0	0)
α^3				α^3			(0	0	0	1	0	0)
α^4					α^4		(0	0	0	0	1	0)
α^5						α^5	(0	0	0	0	0	1)
α^6	$1 + \alpha$						(1	1	0	0	0	0)
α^7		$\alpha + \alpha^2$					(0	1	1	0	0	0)
α^8			$\alpha^2 + \alpha^3$				(0	0	1	1	0	0)
α^9				$\alpha^3 + \alpha^4$			(0	0	0	1	1	0)
α^{10}					$\alpha^4 + \alpha^5$		(0	0	0	0	1	1)
α^{11}	$1 + \alpha$					$+ \alpha^5$	(1	1	0	0	0	1)
α^{12}	1	$+ \alpha^2$					(1	0	1	0	0	0)
α^{13}		α	$+ \alpha^3$				(0	1	0	1	0	0)
α^{14}			α^2	$+ \alpha^4$			(0	0	1	0	1	0)
α^{15}				α^3	$+ \alpha^5$		(0	0	0	1	0	1)
α^{16}	$1 + \alpha$				$+ \alpha^4$		(1	1	0	0	1	0)
α^{17}		$\alpha + \alpha^2$				$+ \alpha^5$	(0	1	1	0	0	1)
α^{18}	$1 + \alpha + \alpha^2$		$+ \alpha^3$				(1	1	1	0	0	0)
α^{19}		$\alpha + \alpha^2 + \alpha^3$		$+ \alpha^4$			(0	1	1	1	0	0)
α^{20}			$\alpha^2 + \alpha^3$		$+ \alpha^4 + \alpha^5$		(0	0	1	1	1	1)
α^{21}	$1 + \alpha$			$+ \alpha^3$	$+ \alpha^4 + \alpha^5$		(1	1	0	1	1	1)
α^{22}	1	$+ \alpha^2$			$+ \alpha^4 + \alpha^5$		(1	0	1	0	1	1)
α^{23}	1			$+ \alpha^3$		$+ \alpha^5$	(1	0	0	1	0	1)
α^{24}	1				$+ \alpha^4$		(1	0	0	0	1	0)
α^{25}		α				$+ \alpha^5$	(0	1	0	0	0	1)
α^{26}	$1 + \alpha + \alpha^2$						(1	1	1	0	0	0)
α^{27}		$\alpha + \alpha^2 + \alpha^3$					(0	1	1	1	0	0)
α^{28}			$\alpha^2 + \alpha^3 + \alpha^4$				(0	0	1	1	1	0)
α^{29}				$\alpha^3 + \alpha^4 + \alpha^5$			(0	0	0	1	1	1)
α^{30}	$1 + \alpha$				$+ \alpha^4 + \alpha^5$		(1	1	0	0	1	1)

TABLE 6.2 Continued.

α^{31}	1		$+ \alpha^2$			$+ \alpha^5$	(1	0	1	0	0	1)
α^{32}	1			$+ \alpha^3$			(1	0	0	1	0	0)
α^{33}		α			$+ \alpha^4$		(0	1	0	0	1	0)
α^{34}			α^2			$+ \alpha^5$	(0	0	1	0	0	1)
α^{35}	$1 + \alpha$			$+ \alpha^3$			(1	1	0	1	0	0)
α^{36}		$\alpha + \alpha^2$			$+ \alpha^4$		(0	1	1	0	1	0)
α^{37}			$\alpha^2 + \alpha^3$			$+ \alpha^5$	(0	0	1	1	0	1)
α^{38}	$1 + \alpha$			$+ \alpha^3 + \alpha^4$			(1	1	0	1	1	0)
α^{39}		$\alpha + \alpha^2$			$+ \alpha^4 + \alpha^5$		(0	1	1	0	1	1)
α^{40}	$1 + \alpha + \alpha^2 + \alpha^3$					$+ \alpha^5$	(1	1	1	1	0	1)
α^{41}	1		$+ \alpha^2 + \alpha^3 + \alpha^4$				(1	0	1	1	1	0)
α^{42}		α		$+ \alpha^3 + \alpha^4 + \alpha^5$			(0	1	0	1	1	1)
α^{43}	$1 + \alpha + \alpha^2$				$+ \alpha^4 + \alpha^5$		(1	1	1	0	1	1)
α^{44}	1		$+ \alpha^2 + \alpha^3$			$+ \alpha^5$	(1	0	1	1	0	1)
α^{45}	1			$+ \alpha^3 + \alpha^4$			(1	0	0	1	1	0)
α^{46}		α			$+ \alpha^4 + \alpha^5$		(0	1	0	0	1	1)
α^{47}	$1 + \alpha + \alpha^2$					$+ \alpha^5$	(1	1	1	0	0	1)
α^{48}	1		$+ \alpha^2 + \alpha^3$				(1	0	1	1	0	0)
α^{49}		α		$+ \alpha^3 + \alpha^4$			(0	1	0	1	1	0)
α^{50}			α^2		$+ \alpha^4 + \alpha^5$		(0	0	1	0	1	1)
α^{51}	$1 + \alpha$			$+ \alpha^3$		$+ \alpha^5$	(1	1	0	1	0	1)
α^{52}	1		$+ \alpha^2$		$+ \alpha^4$		(1	0	1	0	1	0)
α^{53}		α		$+ \alpha^3$		$+ \alpha^5$	(0	1	0	1	0	1)
α^{54}	$1 + \alpha + \alpha^2$				$+ \alpha^4$		(1	1	1	0	1	0)
α^{55}		$\alpha + \alpha^2 + \alpha^3$				$+ \alpha^5$	(0	1	1	1	0	1)
α^{56}	$1 + \alpha + \alpha^2 + \alpha^3$				$+ \alpha^4$		(1	1	1	1	1	0)
α^{57}		$\alpha + \alpha^2 + \alpha^3$			$+ \alpha^4 + \alpha^5$		(0	1	1	1	1	1)
α^{58}	$1 + \alpha + \alpha^2 + \alpha^3$				$+ \alpha^4 + \alpha^5$		(1	1	1	1	1	1)
α^{59}	1		$+ \alpha^2 + \alpha^3$		$+ \alpha^4 + \alpha^5$		(1	0	1	1	1	1)
α^{60}	1			$+ \alpha^3 + \alpha^4 + \alpha^5$			(1	0	0	1	1	1)
α^{61}	1				$+ \alpha^4 + \alpha^5$		(1	0	0	0	1	1)
α^{62}	1					$+ \alpha^5$	(1	0	0	0	0	1)

$\alpha^{63} = 1$

Notes

Códigos BCH com raízes em GF(2^6)

TABLE 6.3 MINIMAL POLYNOMIALS OF THE ELEMENTS IN GF(2^6)

Elements	Minimal polynomials
$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}$	$1 + X + X^6$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{33}$	$1 + X + X^2 + X^4 + X^6$
$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$	$1 + X + X^2 + X^5 + X^6$
$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}$	$1 + X^3 + X^6$
$\alpha^9, \alpha^{18}, \alpha^{36}$	$1 + X^2 + X^3$
$\alpha^{11}, \alpha^{22}, \alpha^{44}, \alpha^{25}, \alpha^{50}, \alpha^{37}$	$1 + X^2 + X^3 + X^5 + X^6$
$\alpha^{13}, \alpha^{26}, \alpha^{52}, \alpha^{41}, \alpha^{19}, \alpha^{38}$	$1 + X + X^3 + X^4 + X^6$
$\alpha^{15}, \alpha^{30}, \alpha^{60}, \alpha^{57}, \alpha^{51}, \alpha^{39}$	$1 + X^2 + X^4 + X^5 + X^6$
α^{21}, α^{42}	$1 + X + X^2$
$\alpha^{23}, \alpha^{46}, \alpha^{29}, \alpha^{58}, \alpha^{53}, \alpha^{43}$	$1 + X + X^4 + X^5 + X^6$
$\alpha^{27}, \alpha^{54}, \alpha^{45}$	$1 + X + X^3$
$\alpha^{31}, \alpha^{62}, \alpha^{61}, \alpha^{59}, \alpha^{55}, \alpha^{47}$	$1 + X^5 + X^6$

TABLE 6.4 GENERATOR POLYNOMIALS OF ALL THE BCH CODES OF LENGTH 63

n	k	t	$g(X)$
63	57	1	$g_1(X) = 1 + X + X^6$
	51	2	$g_2(X) = (1 + X + X^6)(1 + X + X^2 + X^4 + X^6)$
	45	3	$g_3(X) = (1 + X + X^2 + X^5 + X^6)g_2(X)$
	39	4	$g_4(X) = (1 + X^3 + X^6)g_3(X)$
	36	5	$g_5(X) = (1 + X^2 + X^3)g_4(X)$
	30	6	$g_6(X) = (1 + X^2 + X^3 + X^5 + X^6)g_5(X)$
	24	7	$g_7(X) = (1 + X + X^3 + X^4 + X^6)g_6(X)$
	18	10	$g_{10}(X) = (1 + X^2 + X^4 + X^5 + X^6)g_7(X)$
	16	11	$g_{11}(X) = (1 + X + X^2)g_{10}(X)$
	10	13	$g_{13}(X) = (1 + X + X^4 + X^5 + X^6)g_{11}(X)$
	7	15	$g_{15}(X) = (1 + X + X^2)g_{13}(X)$

Exercício: Encontrar o polinômio gerador de um código BCH não primitivo com $n = 21$, $t = 2$ e raízes em GF(2^6).

Notes

Decodificação de Códigos BCH Primitivos

Seja: $r(x) = c(x) + e(x)$. Lembrar que:

$$\begin{aligned} s(x) &= r(x) \text{ modulo-}[g(x)] \\ &= c(x) \text{ modulo-}[g(x)] + e(x) \text{ modulo-}[g(x)] \\ &= e(x) \text{ modulo-}[g(x)] \end{aligned}$$

$$\implies e(x) = q(x)g(x) + s(x).$$

Sendo conhecidas as raízes dos polinômios que representam as palavras-código, então:

$$r(\alpha^i) = c(\alpha^i) + e(\alpha^i) = e(\alpha^i), \quad i = 1,2,\ldots,2t,$$

$$\implies e(\alpha^i) = q(\alpha^i)g(\alpha^i) + s(\alpha^i) = 0 + s(\alpha^i),$$

$$\implies s_i = s(x)|_{x=\alpha^i} = s(\alpha^i) = r(\alpha^i): \quad i = 1,2,\ldots,2t.$$

Notes

Decodificação de Códigos BCH Primitivos

Supor que o padrão de erro $e(x)$ contém ν erros nas posições $x^{j_1}, x^{j_2}, \ldots, x^{j_\nu}$, ou seja,

$$e(x) = x^{j_1} + x^{j_2} + \cdots + x^{j_\nu}, \text{ onde } 0 \leq j_1 < j_2 < \cdots < n.$$

Então podemos construir o seguinte sistema de equações:

$$\begin{aligned} s_1 &= \alpha^{j_1} + \alpha^{j_2} + \cdots + \alpha^{j_\nu} \\ s_2 &= (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \cdots + (\alpha^{j_\nu})^2 \\ &\vdots \\ s_{2t} &= (\alpha^{j_1})^{2t} + (\alpha^{j_2})^{2t} + \cdots + (\alpha^{j_\nu})^{2t} \end{aligned}$$

onde $j_1, j_2, \ldots, j_\nu$ são incógnitas que representam as posições dos erros.

Qualquer método para resolver este sistema de equações é um algoritmo de decodificação para códigos BCH binários primitivos.

Notes

Códigos BCH não Binários

Códigos BCH Primitivos sobre GF(p)

Seja α um elemento primitivo em GF(p^m). O polinômio gerador, $g(x)$, de um código BCH p-ário primitivo corretor de t erros é o polinômio de menor grau sobre GF(p) contendo $\alpha, \alpha^2, \alpha^3, \ldots \alpha^{2t}$ como raízes em GF(p^m). Seja $\phi_i(x)$ o polinômio minimal de α_i, $1 \leq i \leq 2t$. Então,

$$g(x) = \text{LCM}\{\phi_1(x), \phi_2(x), \ldots, \phi_{2t}(x)\}.$$

Notes

Códigos de Reed-Solomon

Códigos de Reed-Solomon (RS)

Um código de Reed-Solomon é um código BCH primitivo (não binário) de comprimento $n = p^m - 1$ sobre GF(p^m). O polinômio gerador desse código tem a forma

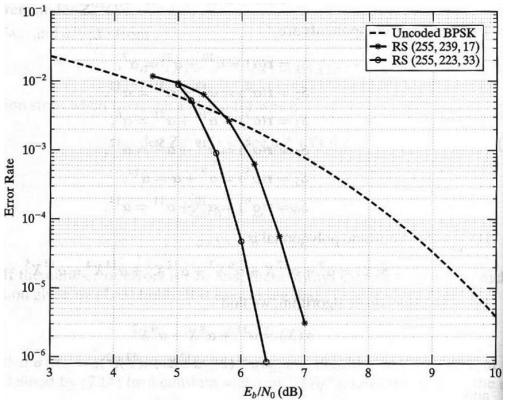
$$\begin{aligned} g(x) &= (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{2t}) \\ &= g_0 + g_1 x + g_2 x^2 + \cdots + g_{2t-1}x^{2t-1} + g_{2t}x^{2t}, \end{aligned}$$

onde α é um elemento primitivo de GF(p^m), t é a capacidade de correção de erros do código e $g_i \in$ GF(q).

- $n = p^m - 1$ símbolos de GF(p^m);
- $k = p^m - 1 - 2t$ símbolos de GF(p^m);
- $d_{\min} = n - k + 1 \implies$ códigos RS são MDS!

Notes

Desempenho de Códigos de Reed-Solomon



Notes

Exercício

Deseja-se gerar um código de Reed-Solomon sobre GF(2^3) com capacidade de correção $t = 1$.

a) Determine os parâmetros n e k, a quantidade de palavras do código e o comprimento máximo (em bits) do erro que pode ser corrigido;

b) Determine o polinômio gerador do código;

c) Codifique a mensagem $\mathbf{m} = (110\ 010\ 111\ 000\ 001)$. Suponha que na saída do canal três bits são afetados pelo ruído. Explique como a localização desses bits pode afetar no resultado da decodificação.

Notes

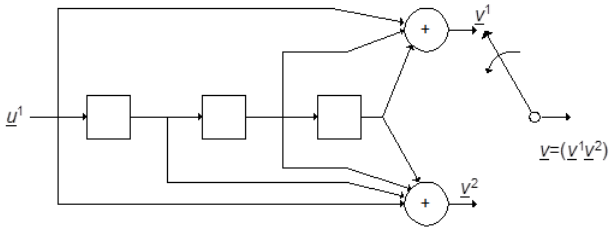
Estrutura e Codificação de Códigos Convolucionais

- **Códigos de Bloco** (n, k):
  n dígitos codificados $\Rightarrow$ função dos k dígitos (informação) da entrada no instante atual.

- **Código Convolucional** (n, k, m):
  n dígitos codificados $\Rightarrow$ função dos k dígitos de entrada e de K dígitos de informação guardados em uma memória (conjunto de SR's: *shift register*).

Notes

Codificador Convolucional $C_1(2, 1, 3)$



- $\mathbf{u}^1$: sequência de entrada, $k = 1$;
- $\mathbf{v} = (\mathbf{v}^1\mathbf{v}^2)$: sequência codificada, $n = 2$;
- m: ordem do codificador, $m = 3$;
- Memória: 1 SR de 3 estágios (3 FFD);
- Taxa: $R = 1/2$

Notes

Equação de Codificação em Forma Matricial – $C(2,1,m)$

$$\mathbf{G} = \begin{bmatrix} g_0^1 g_0^2 & g_1^1 g_1^2 & g_2^1 g_2^2 & \cdots & g_m^1 g_m^2 & \mathbf{00} & \mathbf{00} \\ \mathbf{00} & g_0^1 g_0^2 & g_1^1 g_1^2 & \cdots & g_{m-1}^1 g_{m-1}^2 & g_m^1 g_m^2 & \mathbf{00} \\ \mathbf{00} & \mathbf{00} & g_0^1 g_0^2 & \cdots & g_{m-2}^1 g_{m-2} & g_{m-1}^1 g_{m-1} & g_m^1 g_m^2 \\ \vdots & & \ddots & & & & \ddots \end{bmatrix}$$

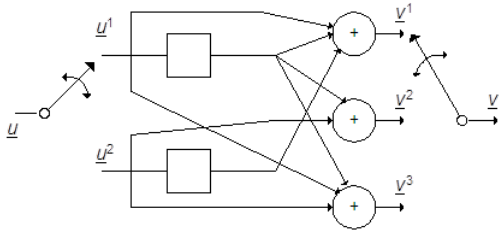
ou

$$\mathbf{G} = \begin{bmatrix} \mathbf{G_0} & \mathbf{G_1} & \mathbf{G_2} & \cdots & \mathbf{G_m} & & \\ & \mathbf{G_0} & \mathbf{G_1} & \mathbf{G_2} & \cdots & \mathbf{G_m} & \\ & & \mathbf{G_0} & \mathbf{G_1} & \mathbf{G_2} & \cdots & \mathbf{G_m} \\ & & \ddots & & & & \ddots \end{bmatrix}, \text{ onde } \mathbf{G_i} = \left[g_i^1 g_i^2 \right]$$

Equação de codificação: $\mathbf{v} = \mathbf{uG}$

Notes

Codificador Convolucional $C_2(3,2,1)$



- $\mathbf{u} = (\mathbf{u}^1\mathbf{u}^2)$: sequência de entrada, $k = 2$;
- $\mathbf{v} = (\mathbf{v}^1\mathbf{v}^2\mathbf{v}^3)$: sequência codificada, $n = 3$;
- Ordem do codificador, $m = \max_{i=1,2} \nu_i = 1$, ν_i = tamanho do i-ésimo SR, $i = 1,2,\ldots,k$;
- Memória: 1 SR de um estágio, $\nu_1 = \nu_2 = 1$ (1 FFD) em paralelo com a entrada;
- Taxa: $R = 2/3$.

Notes

Equação de Codificação em Forma Matricial – $C(3,2,m)$

$$\mathbf{G} = \begin{bmatrix} g^1_{1,0}g^2_{1,0}g^3_{1,0} & g^1_{1,1}g^2_{1,1}g^3_{1,1} & \cdots & g^1_{1,m}g^2_{1,m}g^3_{1,m} & \\ g^1_{2,0}g^2_{2,0}g^3_{2,0} & g^1_{2,1}g^2_{2,1}g^3_{2,1} & \cdots & g^1_{2,m}g^2_{2,m}g^3_{2,m} & \\ & g^1_{1,0}g^2_{1,0}g^3_{1,0} & \cdots & g^1_{1,m-1}g^2_{1,m-1}g^3_{1,m-1} & g^1_{1,m}g^2_{1,m}g^3_{1,m} \\ & g^1_{2,0}g^2_{2,0}g^3_{2,0} & \cdots & g^1_{2,m-1}g^2_{2,m-1}g^3_{2,m-1} & g^1_{2,m}g^2_{2,m}g^3_{2,m} \\ & \ddots & & \ddots & \ddots \end{bmatrix}$$

Equação de codificação: $\mathbf{v} = \mathbf{uG}$

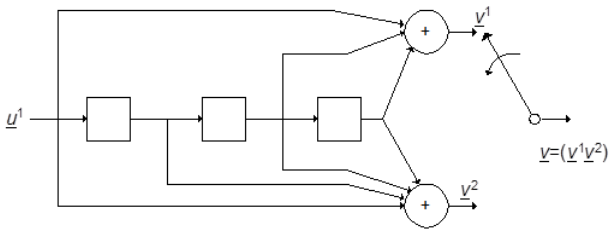
Notes

Comprimento de Restrição (*Constraint Length*)

- O constraint length, ν, de um codificador convolucional é definido como
$$\nu = \sum_{1 \le i \le k} \nu_i;$$
- Um codificador convolucional com taxa $R = k/n$ e *constraint length* ν é identificado como codificador (n, k, ν);
- Um código convolucional (n, k, ν) é o conjunto de todas as sequências de saída (palavras-código) produzidas por um codificador (n, k, ν).

Notes

Código $C_1(2,1,3)$ – Análise no Domínio da Transformada

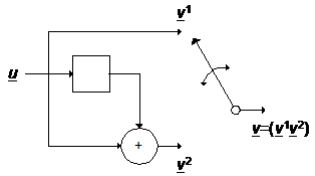


- $n = 2$, $k = 1$, $\nu = 3$, $n = 3$
- $g^1 = (1011) \Rightarrow g^1(D) = 1 + D^2 + D^3$
- $g^2 = (1111) \Rightarrow g^2(D) = 1 + D + D^2 + D^3$
- Mensagem: $\mathbf{u} = (10111) \Rightarrow u(D) = 1 + D^2 + D^3 + D^4$
- $v(D) =?$

Notes

Propriedades Estruturais de Códigos Convolucionais

Codificador convolucional $\equiv$ circuito sequencial (máquina de estados finita).
$\Rightarrow$ operação descrita por diagramas de estados (treliça, árvore, etc).
Exemplo: Código (2,1,1)



Notes

Distância Livre, d_{free}

$$d_{\text{free}} = \min_{\forall \mathbf{v}',\mathbf{v}'' \in C} \{d_{\text{H}}(\mathbf{v}',\mathbf{v}''), \mathbf{u}' \neq \mathbf{u}''\}$$

onde:

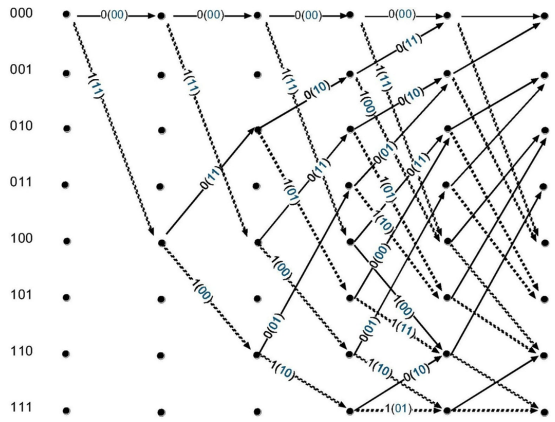
- $\mathbf{v}'$,$\mathbf{v}''$: sequências codificadas correspondentes a $\mathbf{u}'$ e $\mathbf{u}''$;
- d_{H}: distância de Hamming entre duas sequências quaisquer em C

$\rightarrow$ Para código linear: $\mathbf{v}' \equiv \mathbf{0} \Rightarrow d_{\text{H}}(\mathbf{0},\mathbf{v}) = w_{\text{H}}(\mathbf{v})$

onde, $w_{\text{H}}(\mathbf{v})$ é o peso de Hamming de $\mathbf{v}$.

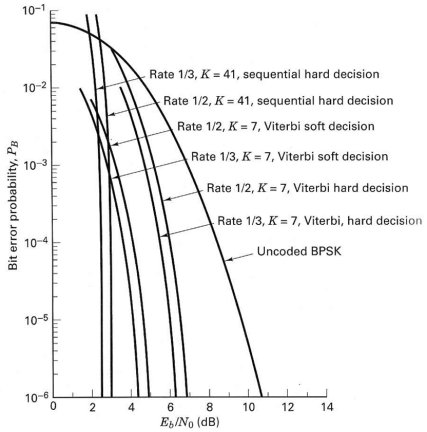
Notes

Treliça $C_1(2,1,3)$



Notes

Desempenho de Códigos Convolucionais



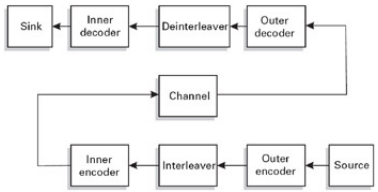
Notes

Melhores Códigos Convolucionais, $R = 1/2$ e $R = 1/3$

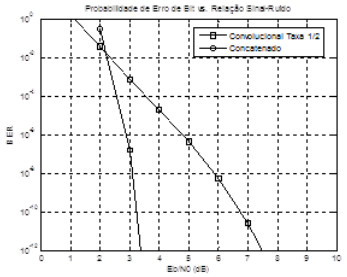
Rate	Constraint Length	Free Distance	Code Vector
$\frac{1}{2}$	3	5	111 101
$\frac{1}{2}$	4	6	1111 1011
$\frac{1}{2}$	5	7	10111 11001
$\frac{1}{2}$	6	8	101111 110101
$\frac{1}{2}$	7	10	1001111 1101101
$\frac{1}{2}$	8	10	10011111 11100101
$\frac{1}{2}$	9	12	110101111 100011101
$\frac{1}{3}$	3	8	111 111 101
$\frac{1}{3}$	4	10	1111 1011 1101
$\frac{1}{3}$	5	12	11111 11011 10101
$\frac{1}{3}$	6	13	101111 110101 111001
$\frac{1}{3}$	7	15	1001111 1010111 1101101
$\frac{1}{3}$	8	16	11101111 10011011 10101001

Notes

Códigos Concatenados



RS(204,188), $t = 8$ (encurtado de RS(255,239) sobre GF(2^8)) concatenado com CC(2,1,7), $d_{\text{free}} = 10$



Notes

Notes