T E S E D E M E S T R A D O

ALGUMAS APLICAÇÕES E PROPRIEDADES DE CÓDIGOS ALGÉBRICOS

ÊVIO DA ROCHA ARAÚJO

COORDENAÇÃO DO MESTRADO EM ENGENHARIA ELÉTRICA
DEPARTAMENTO DE ELETRÔNICA E SISTEMAS
UNIVERSIDADE FEDERAL DE PERNAMBUCO
CIDADE UNIVERSITÁRIA

RECIFE - BRASIL

- 1990 -

UNIVERSIDADE FEDERAL DE PERNAMBUCO

DEPARTAMENTO DE ELETRÔNICA E SISTEMAS

ALGUMAS APLICAÇÂOES E PROPRIEDADES DE CÓDIGOS ALGÉBRICOS

POR

ÊVIO DA ROCHA ARAÚJO

Tese apresentada à Coordenação de Pós-Graduação em Engenharia Elétrica do Centro de Tecnologia da Universidade Federal de Pernambuco, como parte dos requesitos para obtenção do titulo de Mestre em Engenharia Elétrica.

Orientador Valdemar Cardoso da Rocha Jr.

Aos meus Pais,
Waldemar e Dal11

à minha esposa
Gir1eide e
à Pol1yanna.

Je n*ai pas 1es temp.
Evariste Galois

Ao meu amigo,
Fred Nogales
Saudades . . .

AGRADECI MENTOS

Gostaria de expressar meus agradecimentos a todos aqueles que direta ou indiretamente contribuíram para a elaboração deste trabalho.

A todos os professores do curso de Mestrado em Engenharia Elétrica.

Aos professores Ricardo Campei 1 o de Souza e Mareia Mahon Campei 1 o de Souza pelos ensinamentos, incentivo e amizade, principalmente nas horas mais difíceis.

Aos meus amigos de curso, Fred. Fernanda, Mario, Hirtes e Thomas, pelos bons momentos que passamos juntos.

Aos companheiros do Laboratório de Eletrônica do Metrti-do Recife pelo incentivo e amizade.

Aos Engenheiros Ricardo Esberard e Alejandre Reyes do Sistema de Sinalização do Metrô do Recife.

Ao professor Marcos Martins pelo apoio e confiança principalmente enquanto Chefe da Gerencia do Laboratório de Eletrônica do Metrô do Recife.

A Wander e Andréa pela rapidez e qualidade do serviço de datilografia executado.

Â CAPES pelo apoio financeiro concedido durante a elaboração deste trabalho.

Ao meu irmão, Ézio que me indicou os primeiros caminhos na área das ciências exatas.

Ao professor Valdemar Cardoso da Rocha Júnior por sua orientação, incentivo, paciência e amizade.

RESUMO

Nesta tese são apresentadas e analisadas de *forma* sistemática algumas aplicações e propriedades de códigos algébricos. Tais propriedades permitem obter procedimentos para a construção de códigos, simplificação de alguns métodos para decodificação de cOdi^ gos BCH e melhora no desempenho dos sistemas de comunicação digital^ através das técnicas de decisão suave aplicadas à decodificação por armadilha de erros. Alguns tópicos^ principalmente aqueles relaciona dos com a geração e decodif**1**cação de códigos muitiniveis pseudocicli, cos são de grande interesse atual e certamente continuam a *m&re?c&r* a atenção daqueles que se dedicam a codificação algébrica.

1 MDI CE

PAG

PÃG

PAG

CAPITULO 1

1. INTRODUÇÃO

O problema fundamental em um sistema de comunicação é o de reproduzir, de maneira confiável, a mensagem transmitida de um ponto a outro. Para solucionar este problema Claude Shannon criou em 1948 um novo ramo da matemática aplicada denominado de Teoria da Informação. [13.

Um sistema de comunicação e basicamente composto dos seguintes elementos [13

Fonte : A fonte gera as mensagens que serão transmiti, das ao destinatário.

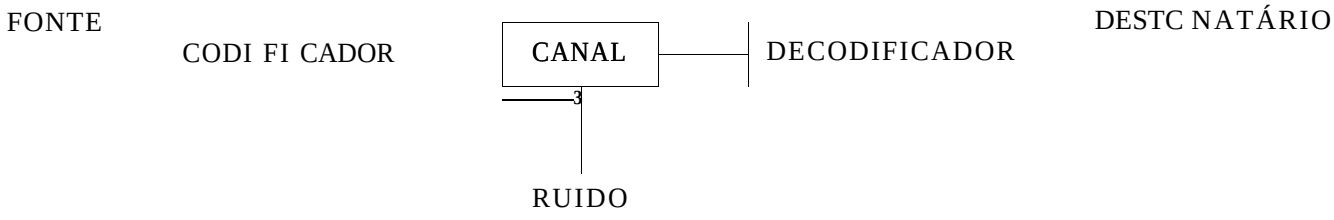
Codificador : O codificador transforma a mensagem recebida da fonte em sinais aceitáveis pelo canal.

Canal : Ê o meio pelo qual a mensagem codificada e transmitida.

Decodificador : Quando os sinais passam pelo canal sofrem distorções devido a presença de ruídos. O decodificador toma uma decisão de qual mensagem foi transmitida pela fonte a partir da mensagem recebida.

Destinatário : O decodificador entrega a mensagem estimada para o destinatário.

A figura seguinte mostra em diagrama de blocos o sistema de comunicação acima descrito.



Uma técnica empregada para resolver o problema descri, to acima, faz uso de códigos corretores de erros. Será mostrado que o acréscimo de símbolos adicionais Credundantes) aos símbolos produ zidos pela fonte Cdígitos de informação} aumenta a probabilidade do decodificador estimar corretamente qual mensagem foi transmitida pela fonte. Claude Shannon, em 1948 através do teorema de codifica ção para um canal com ruido, estabeleceu que todo canal tem uma capacidade máxima de transmissão C e que para qualquer taxa de transmissão R < C, existem códigos de taxa R, os quais, com decodifi_ cação de máxima verossimilhança, têm uma probabilidade de decodifica ção errônea arbitrariamente pequena. Este teorema indica a existên cia de códigos que tornam a probabilidade de decodificação *errônea.* arbitrariamente pequena, mas não indica como construir tais códigos [13 e [23.

A presença de ruido sobre o canal provoca erros durante a transmissão das mensagens. Estes erros podem ser de dois ti pos

Erros aleatórios : Quando os erros são esporádicos e independentes, ou seja, um erro num determinado digito de informação não afeta dígitos adjacentes.

Erros em surtos : Quando *occrrem* em surtos de vários erros de cada vez, diz-se neste caso que o canal tem memória.

Os códigos corretores de erros podem ser classificados em dois grandes grupos :

1} Códigos Lineares : Possuem seus dígitos redundantes calculados como uma combinação linear módulo q dos dígitos de í nfor mação.

2) Códigos Não-Lineares : Empregam lógica não linear tais como portas E, OU, NÃO OU, etc, para o cálculo dos dígitos de redundância.

Dependendo de como a redundância é adicionada aos dígitos de informação, dois tipos diferentes de códigos lineares são obti dos :

1> Códigos de Bloco : São aqueles em que os dígitos de redundância acrescentados a um bloco de dígitos de informação verifica a ocorrência ou não de erros, apenas naquele bloco.

2> Códigos de Ãrvore : São aquelas em que os dígitos de redundância em um bloco de dígitos verifica a ocorrência ou não de erros em mais de um bloco. A subclasse mais importante destes códigos é a dos códigos convolucionais, os quais são mais simples e de fácil implementação com relação a outros tipos de códigos de árvore.

Os objetivos da teoria da codificação são basicamente: [63

1} Encontrar códigos longos e eficientes
2> Encontrar métodos de codificação e decodificação ef1cientes
3?> Estabelecer limites de desempenho.

O objetivo principal deste trabalho ê de apresentar de forma sistemática algumas propriedades e aplicações de códigos algébricos que permitem construir códigos algébricos e simplificar sua decodificação. Nos capítulos 2 e 3 ê feita uma revisão dos códigos de blocos lineares e dos códigos cíclicos. No capitulo 4 a construção de uma classe de códigos multiniveis pseudociclicos bem como sua decodificação algébrica são apresentadas. No capitulo 5 são mostradas as propriedades algébricas dos códigos BCH que simplificam o processo de deteção e *carr&ç^o* dos erros. No capitulo 6 o método de decodificação por armadilha para erros Cerror-trapping), é estudado na versão para decisão abrupta e decisão suave, finalmente no capitulo 7. são feitos comentários gerais, discutindo vantagens e restrições decorrentes do trabalho apresentado, bem como sugestões para futuras investigações.

CAPITULO 2

CÓDIGOS DE BLOCO LINEARES

Neste capitulo iremos apresentar uma introdução aos códigos de bloco lineares. São definidos os conceitos de distância de Hamming, distância mínima, síndrome, arranjo padrão e classes laterais e apresentados os algoritmos de decodificação por máxima verossimilhança, busca sistemática e decodificação probabilística. No final do capitulo são mostrados os códigos de repetição, os códigos de um único digito de paridade e o código de Hamming.

2.1. CONCEITOS BÁSICOS

2.1.1. PESO DE HAMMING

Def1nição 2.1. O peso de Hamming WCv} de uma énupla $v = Cv_o, v_i, \ldots v_{n-i}\}$, ê o número de posições v_i não nulas,

2.1.2. DISTANCIA DE HAMMING

Definição 2.2. A distância de Hamming HCv.u} entre duas énuplas $v = C v, v, \ldots, v\}$ e $u = C u. u \ldots u\}$, ê o número de posições onde as duas diferem.

Devemos observar que a distância de Hamming constitui uma métrica. Alem disto, como consequência direta das definições de peso e distância de Hamming temos que

$$HCv.u) = WC v\text{-}u2> \qquad C2.1)$$

2.1.3. CÓDIGO LINEAR

Definição 2.3 Um código linear C Cn.k.d) sobre GFCqD é um subespaço. de dimensão k. do espaço vetorial V_{ri} de todas as énuplas q-árias.

2.1.4. DISTÂNCIA MINIMA DO CODIGO

Dgfinição 2.4. A distância minima d de um código C é a menor distância de Hamming encontrada entre suas paiavras-código, ou seja, HCv.u) > d. para todo v * u *e* C.

Podemos observar que

$$d = \min_{v * O \pounds C} W(C v l> \quad \text{C2.2}\}$$

2.1.5. PALAVRAS-CÔDIGO

Os q^{y} vetores de C, são chamados de paiavras-código. O processo de codificação consiste em adicionar n-k dígitos redundantes a cada uma das q mensagens possíveis de k dígitos, para *formar uma* palavra-côdigo de comprimento n. Os dígitos redundantes são obtidos pela combinação linear dòs k dígitos de informação. O cõdigo obtido ê dito ter comprimento de bloco n e taxa R = k/n.

2. 2. MATRIZ GERADORA DE UM CÓDIGO LINEAR

Sendo um código linear CCn.k.d) um subespaço, de dimensão k, do espaço vetorial V_{ri} de todas as ênuplas, e possível encontrar k paiavras-código linearmente independentes. g_{ϱ}, $g^{\wedge}$. . . . em C. de *forma* que toda paiavra-código v em C e uma combinação linear destas k paiavras-código, ou seja.

$$v = m_o q_o + m_{\acute{i}} g_i \quad \text{* } \text{™} \quad g, \qquad \text{C2.3)}$$

onde m e GFCq) para 0 < i < k. Podemos formar uma matriz com estas k paiavras-código linearmente independentes, ou seja, as k linhas da matriz k x n.

G =

$$k - 1$$

onde $g_i = (g_{i0}, g_{i1}, \ldots, g_{i,n-k-1})$ para g_{ij} e GF(q), $0 \le i \le k$ e $0 \le j \le n$.

Se $m = (m_0, m_1, \ldots, m_{k-1})$ é a mensagem a ser codificada, a palavra-código correspondente pode ser obtida pela multiplicação de m pela matriz G.

$$v = m.G$$

Como as linhas de G geram o código linear C, a matriz G é chamada de matriz geradora do código C.

2.2.1. MATRIZ GERADORA NA FORMA SISTEMÁTICA

Quando um código de bloco linear está na forma sistemática, as palavras-código são divididas em duas partes, uma parte correspondendo à mensagem e a outra à verificação de paridade ou redundância. A parte da mensagem consiste de k dígitos de informação inalterados e a parte de verificação de paridade consiste de n-k dígitos, que são uma combinação linear dos dígitos de informação [33. Na figura abaixo mostramos o formato de uma palavra-código na forma sistemática.

VERIFICAÇÃO DE PARIDADE	MENSAGEM
n-k dígitos	k-dígitos

FIG. 2.1. - PALAVRA CÓDIGO NA FORMA SISTEMÁTICA

Um código linear C(n,k,d) na forma sitemática é completamente especificado por uma matriz G, k x n, da seguinte forma:

$$G = [\, P \mid I_k \,] \qquad (2.5)$$

onde P é uma matriz (n-k) x k e I_k é a matriz identidade de ordem k [33.

2. 3. MATRIZ DE VERIFICAÇÃO DE PARIDADE

Uma outra importante matriz associada com os códigos de blocos lineares é a matriz H de verificação de paridade. Dada uma matriz G de um código linear, com k linhas e n colunas existe uma matriz H com n-k linhas e n colunas, tal que qualquer vetor do espaço das linhas de G é ortogonal às linhas de H e qualquer vetor que ê ortogonal às linhas de H está no espaço das linhas de G. Por tanto,

v. H^T = O v í CCn.k.d).

Se a matriz geradora de um código de bloco linear CCn.k.d} esta na forma G = [P j I_k] então a matriz de verificação de paridade poderá ser escrita na forma

$$H = [\ I_{n\_k}\ ;\ P^T\ ] \quad \text{C2. 6}\}$$

onde P^T e a matriz transposta da matriz P e $I_{r>-k}$ é a matriz identida de de ordem Cn-k). Um código linear CCn.k.d) è completamente espec^ ficado pela sua matriz H.

2. 4 CÓDIGO DUAL

As q combinações lineares das linhas da matriz H formam um código linear C Cn, n-k, d'}. Este código é o espaço nulo do código *linear* CCn,k,d} gerado pela matriz G, ou seja, para todo v *e* C e qualquer w c C_d, v. w = O. Ce chamado de código dual de C_d. Desta forma a matriz de verificação de paridade do código linear C é a matriz geradora do seu código dual C_d. [43.

2.5. SÍNDROME

Defínlção 2. 5. Seja H a matriz de verificação de paridade de um código linear CCn.k.d). A síndrome da enupla r = $Cr_o . r_1 \quad r_{n-1}$ > é o vetor

Assim podemos observar que S é um vetor com n-k componentes, ou seja, S = Cs , s. . . . s , D; alem disto estas componentes são todas nulas se e somente se r = Cr , r. . . . r 2> é uma paiavra-código do código definido por H. Desta forma, quando s * O os erros sâío detetados.

Sejam v = Cv , v, ... v) a paiavra-código transmitida, r = C r , r. .... r) a ênupla recebida e e = C e , e , . . . , e) o vetor erro provocado pelo efeito do ruido sobre a palavra transmitida.

A relação entre estes três vetores e dada por:

r = v + e. . . . . .

Assim temos

S = r H^T = Cv + e2>H^T = e H^T. C2. 9)

e a síndrome contem *i nf crmâç&&s* sobre o vetor erro.

Seja H = f h , h , ... hl onde h são as colunas de H; então, da equação C2.QO. temos que

S = £ r h = E^e h . onde e ^ O. C2. 10)

2 6. CAPACIDADE DE DETEÇÃO E CORREÇÃO DE ERROS DE UM CÓDIGO DE BLOCO LINEAR

2.6.1. CAPACIDADE DE DETEÇKO DE ERROS ALEATÓRIOS

Se a distância mínima de um código de bloco linear C é d. então quaisquer duas paiavras-código distintas diferem em pelo menos d posições. Portanto, para este código, nenhum padrão de erros com d - 1 ou menos erros mudará uma paiavra-código em outra. Quando uma paiavra-código é transmitida, ocorrendo no máximo d - 1 erros, a palavra recebida não será uma paiavra-código e sua síndrome correspondente será diferente de zero, sendo portanto os erros detectados. í33

2. 6. 2. DISTRIBUIÇÃO DE PESOS DE UM CÓDIGO CCn.k.d)

Seja um código linear CCn.k.d). Seja A^ o numero de paiavras-código de peso i em C. Os números $A_o, A_i, \ldots A_n$ são chamados de distribuição de pesos do código C. .

Se o código linear C é usado apenas para deteção de erros num canal simétrico binário CBSO. a probabilidade de que o decodificador falhe na deteção de erros pode ser obtida da distribui, ção de pesos de código C. Seja P^CE) a probabilidade de falha na deteção de erros; então

$$P_u(E) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i} \quad (2.11)$$

onde p é a probabilidade de transição do canal simétrico binário CBSO. [33

2. 6. 3. CAPACIDADE DE CORREÇÃO DE ERROS ALEATÓRIOS

TEOREMA 2. 1 Um código linear CCn.k.d) corrige qualquer padrão de _j ou menos erros, onde |_tj denota o maior inteiro menor ou igual a t e t = Cd - l)/2. £53

PROVA : Assumiremos que c e r são respectivamente, os vetores transmitido e recebido. Da desigualdade triangular temos que

$$H(c,v) - H(c,r) \leq H(r,v) \quad (2.12)$$

Se v denota uma paiavra-código diferente de c, então HCc.v) > d; também por hipótese HCc.r) < |Cd-l)/2j então a equação C2.12) torna-se

$$d - (d-1)/2 \leq H(r,v)$$
$$(d-1)/2 + 1 \leq H(r,v)$$

e portanto HCc, r) 5 HCr, v) para toda paiavra-código v X c.

2. 6. 4. COTA SUPERIOR PARA A PROBABILIDADE DE CORREÇÃO DE ERROS ALEATÔRIOS

Se um código de bloco corretor de t erros ê usado estritamente para *cor r&çlSío* de erros sobre um canal simétrico binário CBSO, com probabilidade de transição p, então a probabilida de do decodificador cometer uma decodíficação errada é limitada pela seguinte cota superior £33

$$P(E) < \sum_{i=t+1}^{n} \binom{n}{i} p^{i} (1-p)^{n-i} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.13)$$

2. 7. ARRANJO PADRÃO

2.7.1. CLASSE LATERAL

Definição 2.6 Seja CCn.k.d} um código linear sobre um corpo com q elementos. Para qualquer vetor e, o conjunto

$$e + C = \{e + v : v \in C\} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.14)$$

é chamado de classe lateral de C. [43. Além disso, o vetor de peso mínimo em uma classe lateral é chamado de Lider da Classe Lateral. [43.

2.7.2. CONSTRUÇÃO DO ARRANJO PADRÃO

Uma maneira apropriada de descrever a ação do decodifi_ cador é por meio de uma tabela, chamada arranjo padrão do código. O arranjo padrão produz uma partição do espaço vetorial de q^n ênuplas em q^{n-k} classes laterais, cada uma contendo q^k énuplas. A primeira linha é formada pelas paiavras-código com a paiavra-código nula na primeira posição a esquerda, ou seja.

$$v_1 = 0, v_2, v_3, \ldots, v_{q^k}$$

e as linhas seauintes são as outras classes laterais $e_i + C$. arrumadas de mesma *forma,* e com o 1ider da classe lateral, não perten cente as classes anteriormente construídas, na primeira posição a esquerda, ou seja.

2. 8. DECODIFICAÇÃO DE CÓDIGOS LINEARES

Qualquer procedimento de decodificação usado no recep tor e uma regra de partição das q^n possíveis palavras recebidas em v q subconjuntos disjuntos $D^{\wedge}$, $D^{\wedge}$ . . . $D^{\wedge}k$ de *forma* que a palavra código v está contida no subconjunto $D^{\wedge}$ para $1 < i < q^k$. Então cada conjunto $D^{\wedge}$ está associado auma paiavra-código v . Se o vetor r está contido em D então ele é decodificado como v [33. O arranjo padrão **l** **i** é um método de partição útil como uma maneira de compreender a estru tura de códigos lineares porém não é fácil sua implementação como algoritmo de decodificação í63. Apresentamos a seguir alguns métodos de decodificação.

2.8.1. DECODI FI CAÇÃO POR MÁXIMA VEROSSI MI LHANÇA

Este método consiste em comparar a palavra recebida r com todas as possíveis paiavras-cédígo, e aquela que possuir a menor distância de Hamming com relação a r é considerada como sendo a paiavra-cOdigo transmitida. O problema neste procedimento é que o tempo necessário para decodificar uma énupla recebida torna-se muito longo, mesmo para valores moderados de k. tornando este processo de decodifi cação em geral inadequado. [63.

2. 8. 2. DECODI FI CAÇÃO POR TABELA DE SÍNDROME

Este procedimento consiste em associar a cada síndrome não nula um padrão de erros corrigivel. Como existe uma corresponder) cia biunívoca entre as classes laterais e as síndromes, podemos esco 1her os líderes das Classes Laterais como padrões de erros mais prováveis, e aplicar o seguinte procedimento para decodi fi cação [63.

2.9. PRINCIPAIS CÓDIGOS DE BLOCO LINEARES

2.9.1. CÓDIGOS DE REPETIÇÃO

Um código de repetição é caracterizado pelos seguintes parâmetros :

$$k = 1$$
$$c = n - k > 1$$
$$n = k + c = 1 + c$$

A distância mínima é d = n ea sua eficiência é R =l/n,
Neste código os n-1 dígitos de redundância sào uma repetição do único digito de informação. [63.

2. 9. 2. CÓDIGO DE UM ÚNICO DÍGITO DE PARIDADE

Este código possui um único digito de redundância por palavra e ê obtido pela soma módulo p **C** p *é* a característica do corp } dos n - 1 dígitos de informação [63.

Os parâmetros deste código são :

$$k > 1$$
$$c = 1$$
$$n = k + c = k + l$$

A sua distância mínima ê d = 2 e sua eficiência R = k/n = k Ak + 1).

2. 9. 3. CÓDIGOS DE HAMMING

Os códigos de Hamming foram os primeiros códigos não triviais desenvolvidos para corrigir erros [63. Para qualquer inteiro m > 3. existe um código de Hamming com os seguintes parâmetros :

A matriz de verificação de paridade H do código de Hamming consiste de todas as 2™ - 1 m-tuplas distintas e não nulas como colunas. Na *forma,* sistemática a matriz H tem a seguinte *forma*

$$H = [\, I \mid Q \,]$$

onde I è uma matriz identidade de ordem m e a submatríz Q consiste de $2^m - m - 1$ colunas que são as m-tuplas de peso maior ou igual a dois T33.

EXEMPLO : Para m = 3 temos n = 2 - l = 7 e então

$$H = \begin{matrix} 1\,0\;\;0\;\;1\,0\;\;1\,1 \\ 0\;\;1\,0\;\;1\,1\,1\,0 \\ 0\;\;0\;\;1\,0\;\;1\,1\,1 \end{matrix}$$

CÓDIGOS PERFEITOS

Defínição 1.8 Um código CCn.k.d> com símbolos em GFCq> corretor de t erros é perfeito se e somente se

$$\pounds\, tq-1)\;\; C \;=\; q \qquad\qquad C2.155$$

Os códigos de Hamming são especiais no sentido de que *é uma* classe de códigos facilmente decodificada e também porque são perf ei tos.

$$vt:\dot{j} \;—\; v_O \;^{+}{}_{l} v\, x \quad v_2 x^2 \;\bullet\; . \;.\; . \quad v_{D-1}\, x^{rt-l}$$

que é um elemento de R , o anel de polinómios módulo $x^{r'} - 1$ [53. Multiplicando vCx) por x obtemos

$$x.\, v\, C\, x\,) = v_o x + v_{\acute{i}} x^{2} + .. + v_{n-1} x^{n}$$
$$= v_{n-l} + v_o x + v_{\overset{2}{1}} \;\; . \;.\; . + V_{n-2} X^{r»-i}$$

desde que a multiplicação ê módulo $x^{r'} - 1$. Portanto, multiplicar por x em R_n é equivalente a um deslocamento cíclico. Do resultado acima podemos apresentar uma definição alternativa para códigos cíclicos, ou seja, um código cíclico de comprimento n é um ideal de R . Quando a representação por polinómios é usada nos referimos ás pai avras-códi go como pol i nómi os-códi go. [53

3. 2. O POLINÓMIO GERADOR gCx)

TEOREMA 3. 1 Um conjunto de polinómios e um ideal se e somente se ele consiste de todos os múltiplos de algum polinómio. [103.

O teorema acima nos diz que todo ideal de R_{Tl} é um ideal principal; desta forma todo código cíclico tem um polinómio gerador, que denotaremos por gCx). As propriedades do polinómio gerador gCxD podem ser determinadas a partir da teoria dos anéis de polinómios com coeficientes em um corpo de Galois GFCq). módulo $x^{n} - 1$. Í33.

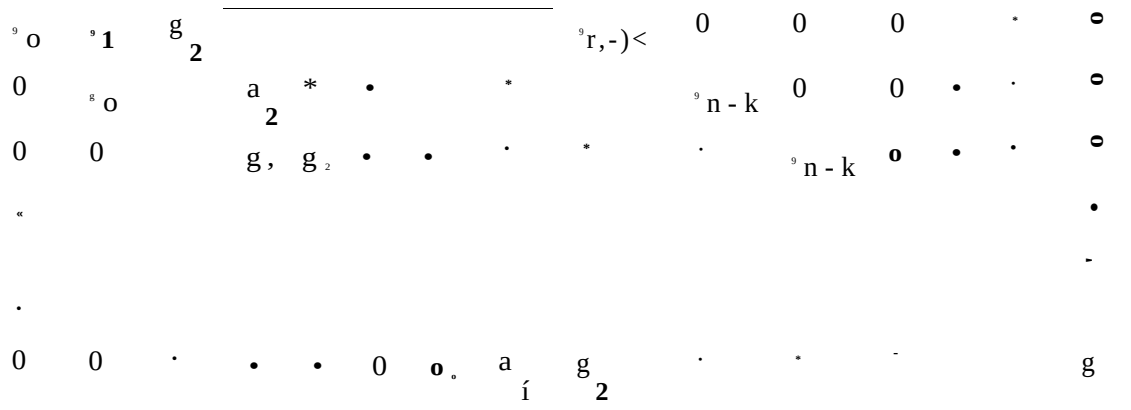
Apresentaremos a seguir as principais propriedades de $gCx) = \overset{r}{\underset{i=\acute{i}}{E}} 9 \; *^{x} \bullet$

C1) gCx), o polinómio mónico de menor grau em C, é único.

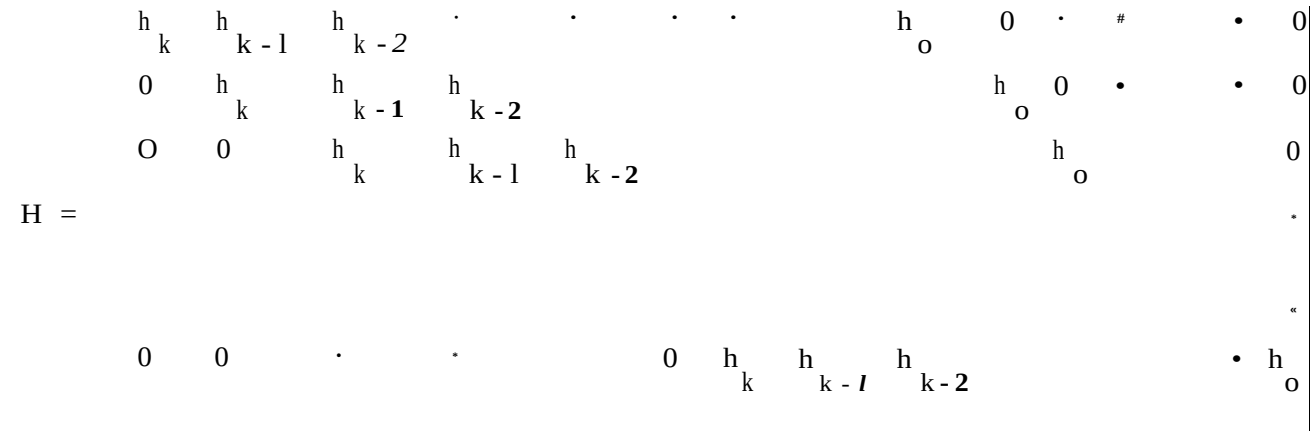
C2> $g_{\circ} = 1$

C3) gCx) ICx^{n} - 1)

Se as k ênuplas correspondendo aos k polinómios códigos são usadas como linhas de uma matriz k x n, obtemos a seguinte matriz geradora de C:



Podemos obter a partir de hCx> a matriz de verificação de paridade do código cíclico C.



Como $\sum_{i=0}^{k} h_t v_{r.-v-j} = 0$ para $1 < j < n - k$ então toda palavra código v de C é ortogonal as linhas de H. Portanto, H é a matriz de verificação de paridade do código C, e o espaço-linha de H e o código dual de C.

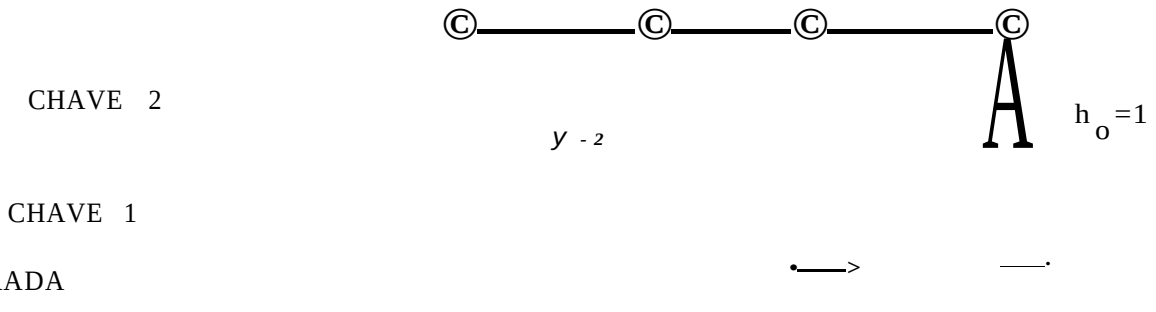
TEOREMA 3.2 Seja um código cíclico CCn.k.d) com polinómio gerador gCx). O código dual de C é também cíclico e é gerado pelo polinómio x* hCx ¹>, onde hCx2> = Cxⁿ -l^/gCx) [33.

O circuito da figura 3.1. utiliza n-k registradores de deslocamento e prê-multiplica o polinómio mCxD por x^{n-k} As conexões g_1, g_2, ..., g_{n-k-i} são pesos associados aos coeficientes correspondentes em gCxX Inicialmente, o registrador contém apenas zeros. A chave 1 é fechada e a chave 2 fica na posição 1; os dígitos de informação são então enviados simultaneamente á salda e ao circuito de divisão. Após a transmissão de k dígitos de informação, os n-k dígitos de verificação de paridade estão no resgistrador e então a chave 1 é aberta e a chave 2 é movida para a posição 2. Desta forma nos próximos n-k intervalos de tempo, os dígitos de veri. ficação de paridade são transmitidos.

3. 5. 2. CODIFICAÇÃO COM *K* ESTÁGIOS DE REGISTRADORES DE DESLOCAMENTOS

Podemos codificar as mensagens utilizando k estágios de registradores de deslocamento, porém as conexões de realímentação são obtidas a partir do polinómio de verificação de paridade hCx> í3).

O circuito é mostrado na figura abaixo:



$$h(x) = 1 + h_1 x + \ldots + h_{k-1} x^{k-1}$$

FIG. 3. 2 - CODIFICADOR COM *K* ESTÁGIOS DE REGISTRADORES DE DESLOCAMENTO.

corresponder a um padrão de erros com e ^ O, o polinómio recebido rCx) Carmazenado em um registrador) e o registrador da síndrome são deslocados ciclicamente e simultaneamente uma vez. Desta *forma* será obtido o vetor $r^{(1)}$ Cx> e o novo conteúdo do registrador da síndrome será s Cx>. Agora o circuito decodificador verifica se $s^{(1)}$ Cx5 corresponde a um padrão de erros com um erro localizado na posição de ordem mais alta, ou seja, x^n

Se a síndrome sCx) de rCx) corresponder a um padrão de erros com um erro na posição x^n , então o dlaito r de rCx> deverá ser corrigido. O efeito do erro e sobre a síndrome sCx> ê

então removido, isto deverá ser feito subtraindo eCx) = x' de sCxX

Quando corrigimos a palavra recebida rCx) obtemos

$$p C x) « r * r + . . . + r + x + (.r «* e >x$$
$$1 \quad o \quad I \quad r>-2 \quad r.-i \quad r>-1$$

Agora deslocando ciclicamente r^Cx) e o registrador da síndrome simultaneamente uma vez, obtemos

$$r \quad Cx> = Cr \quad e» e > + r x + . . . + r x$$
$$1 \quad n-1 \quad n-l \quad o \quad n-2$$

A sindrome $s_{í}^{(1)}$'Cx> de $r_{í}^{(1)}$ Cx) ê o resto da divisão de x ísCx5 + x 3 pelo polinómio gerador gCx>. Como o resto da divisão de x • s(x) e x^n por gCx2> são respectivamente $s^{(1)}$Cx2> e 1, então temos que

$$s_{í} \quad Cx2> = s \quad Cx) •+ 1$$

Portanto, se 1 ê adicionado os dígitos mais â esquerda do conteúdo do registrador da síndrome obtemos $s_{í}$ CxX

O circuito decodificador repete o procedimento acima, digito por digito, durante n passos.

Se eCx) foi um padrão de erros corrigivel o conteúdo do registrador da sindrome deverá ser zero no final do processo de decodificação e a palavra recebida será corretamente decodificada. Se o conteúdo do registrador da síndrome for diferente de zero, no final do processo de decodificação, os erros serão apenas detectados. 133.

PASSO 3: O primeiro símbolo recebido é lido do registrador da palavra recebida. Ao mesmo tempo o registrador da sidrorne é delocado uma vez. Se o primeiro símbolo recebido está errado, ele é corrigido pela salda do detetor. A salda do detetor também serve para modificar o conteúdo do registra dor da síndrome.

PASSO 4: A nova síndrome obtida no passo 3 é usada para detetar se o segundo símbolo recebido ($\hat{C}_{T-2}$) esta correto. O decodifica - dor repete os passos 2 e 3.

PASSO 5: O decodificador decodifica símbolo por símbolo da palavra recebida, até que toda a palavra rCx) tenha sido lida do registrador da palavra recebida.

3. 6. 2. DECODIFICAÇÃO POR ARMADILHA PARA ERROS

A decodificação por armadilha para erros Cerror trapping) consiste numa variação do algoritmo de Meggitt, fazendo a restrição nos padrões de erros que serão corrigidos, ou seja, que o padrão de erros se espalhe por um número de dígitos. ciclicamente consecutivos em deslocar ciclicamente, bit por bit, a síndrome da pa lavra recebida, observando sempre o seu peso CWs). Quando o peso da síndrome torna-se menor ou igual a t Cnúmero de erros corrigíveis), o padrão de erros coincide com a síndrome. Para corrigir basta somar o conteúdo do registrador da síndrome com o conteúdo do registrador da palavra recebida. Se após n deslocamentos não ocorrer que Ws seja menor ou igual a t, então os erros são detetados. Este procedimento é restrito essencialmente a códigos de baixa eficiência, pois para sua aplicação a condição n/k > t deve ser satisfeita. A decodifica ção por armadilha para erros foi inventada independentemente por Kasami [113. Mlthell. [123 e [133 e Rudolph [93.

Uma explicação mais detalhada sobre esta técnica será dada em um capitulo subsequente.

3. 6. 3. DECODIFICAÇÃO POR LÓGICA DE MAIORIA

Este algoritmo baseia-se na for/nação de 2J equações de verificação de paridade ortogonais na posição x[r]* [1] da paiavra-códi go. Isto permite a correção de J erros por palavra. Quando 2J = d - 1 o código é dito completamente ortogonalízável. Este procedimento é aplicável a outros tipos de códigos de bloco e também a códigos convolucionais. [33 e [53.

3.7. CÓDIGOS BCH CBOSE. CHAUDHURI-HOCQUENGHEM}

Estes códigos foram criados independentemente por Hocquengbem C195SO e por Bose e Cbaudhuri t'1960}. Os códigos BCH são cíclicos e representam a classe mais importante de códigos de bloco com algoritmos algébricos de decodíficação. Para quaisquer inteiros positivos m, t Ct < 2™ - 1) existe um código BCH com os seguintes parâmetros

$$n = 2^m - 1$$

$$n - k = c < mt$$

$$d > ó = 2t + 1$$

onde *ô* é denominado distância projetada.

3. 7. 1. DEFINIÇÃO DE CÓDIGOS BCH

Um código BCH com distância projetada *6* sobre GFCq> é um código cíclico cujo polinómio gerador gCx5 é o polinómio mónico de menor grau sobre GFCqD tendo

c*[l] , *b* < *í* <b + ó- 2 como raízes; 1. e. ,

gCx2> = mmm ÍM Cx2>, M Cx}. ... ,M Cx)3. . . . . .C3. 5>

onde M[(1>] CxD é o polinómio mínimo de *a*[i].

3. 8. CÓDIGOS REED-SOLOMON

Um código Reed-Solomon CRS) sobre GFCq) é um código BCH com comprimento do bloco q-1 cujo polinómio geraor é

$$gCx) = \prod_{i=b}^{b*Ó-2} Cx - a^{i}) \quad \text{C3. 6)}$$

O grau de gCx) é *6* - 1, portanto

$$6 = n - k + 1 \quad \text{C3. 7)}$$

e como, pela cota BCH, d > *6* , a distância mínima de um código RS satisfaz

$$d > n - k + 1$$

Então, considerando a cota superior de Singleton, d 2? n — k •+ 1, temos que

$$d « n - k + 1 \quad \text{C3. e:>}$$

Portanto, podemos dizer que os códigos RS são uma família de códigos MDS CCódigos de distância máxima separáveis) [33.

CAPITULO 4

CÓDIGOS MULTINÍVEIS PSEUDOCÍCLICOS

4.1. INTRODUÇÃO

Vimos anteriormente que o polinómio gerador gCx) de um código cíclico é fator de x^n - 1. Desta forma, existem relativamente poucos códigos cíclicos para a maioria dos valores de n e k. Assim, é interessante procurar códigos lineares que mesmo não sendo verdadeiramente cíclicos, compartilhem a estrutura matemática e a fácil implementação dos códigos cíclicos. Os códigos pseudociclicos [103 se enquadram nesta categoria. Neste capitulo descreveremos os procedimentos para geração e decodificação algébrica de uma classe de códigos muitiníveis pseudociclicos, cujos polinómios geradores são fatores de x^n - b, onde n = Cp^{ms} -ÍO/T é o comprimento do bloco, b é um elemento não nulo de GFCp*) cuja ordem divide r, p sendo um primo impar e s um inteiro [143.

A distância mínima destes códigos é estabelecida num caminho similar ao da prova da cota BCH [43, entretanto operando com polinómios módulo $x^{r'}$ - b. Os códigos obtidos são constaciclicos [153. Demonstraremos como os códigos pseudociclicos podem ser decodificados por um procedimento algébrico através do *empr&go* de uma transformação afim, que torna o código pseudociclico um código cíclico, num campo de extensão GFCq^m), sendo q = p^9 e m um inteiro [163. Usaremos a decodificação algébrica no domínio da frequência, por meio da transformada de Fourier de campo finito CTFCFD [53, [173 e usando o algoritmo de Euclides para determinação do polinómio localizador de erros Í173.

4.2. GERAÇÃO DE CÓDIGOS MULTINÍVEIS PSEUDOCICLICOS

Nesta seção apresentaremos alguns lemas e um teorema que proporcionam a estrutura necessária para a construção dos códigos Í143.

4.2.1. CÓDIGOS CONSTACICLICOS E NEGACÍCLICOS

DEFINIÇÃO 4.1 : Um código constaciclico consiste de palavras código que são múltiplas de um polinómio gerador gCx) módulo x^r' - b, onde b ê um elemento não nulo de GFCp^s> = GFCq>. Como consequência desta definição estes códigos são preservados por deslocamentos constaciclicos, ou seja; se CC , C , . . . , C) ê uma paiavra-código então CbC ,C ,C , . . . , C } também ê uma paiavra-código.

Quando b = -1 então obtemos os códigos negacíclicos [103.

4.2.2. EXISTÊNCIA DE FATORES PRIMITIVOS EM X^r'-b

LEMA 4.1 O polinómio x^n - b contêm um fator primitivo se e somente se a ordem de b ê r, para r < q - 1. Em caso contrário, nenhum dos seus fatores são primitivos.

PROVA Vamos supor que ct *é* uma raiz de um polinómio primitivo que ê fator de x^n - b. Então segue que c*^n = b, onde n = **C**q™ - , p^s = q . Agora, se a ordem de b ê l, onde 1 **<,** r i q- 1, então ct^nl = b^l = 1, o que ê uma contradição pois nl < q"' - 1 e por hipótese a ordem de *a* é q™ - 1. O caso em que r > q - 1 ê mostrado assumindo que *a*, um elemento primitivo de GFC q^m>, ê uma raiz de x^n - b. Portanto o»^n<q^1 = b^q^1 = 1 o que novamente é uma contradição, pois nCq-1} = C q^m-l D Cq-15 < q^n - 1
r

Nos exemplos a seguir iremos considerar um alfabeto com cinco níveis, ou seja, q = p^s = 5 e m=2. Portanto o campo original será GFC5^ e o campo de extensão GFC25>.

Na tabela I são mostrados os elementos de GFC25), gerados pelas potências de um elemento primitivo *a* que ê raiz de ntx) = x^2 + x + 2.

EXEMPLO 4.1 : Para r = 4 . n = 24X4 = 6

As raízes de :

x - 1 são *ct* , *ct* , a . *a* , *ct* e a

x - 2 sao a, a , a , *ct* , a e a

x - 3 são *a* , *a* . *a* , *ct* *ct* e a

x - 4 sao ei , *ct* , *ct* , *ct* , c* e a

Como os elementos primitivos de GFC25) são :

a, ct . *c** , *a* , *a* * *a* . *ct* e ct

E as ordens de 1,2,3 e 4 (modulo 5) são, respectivamen te, 1, 4, 4 e 2, então apenas x - 2 e x*⁵ - 3 possuem fatores primitivos.

EXEMPLO 4.2 Para r = 6, C portanto r > q - 1 = 4) temos n = 24/6 = 4.

Assim x⁴ - 1, x⁴ - 2, x⁴ - 3 e x⁴ - 4 não possuem nenhum fator primitivo. Podemos observar que as raízes de :

x - 1 são *a* , *ct* *ct* e oi

x⁴ - 2 não possui raízes em GFC25)

x⁴ - 3 não possuí raízes em GFC25)

x - 4 são *a* , *ct* , *ct* e œ

LEMA 4.2 : O polinómio xⁿ - b. onde n = C*q*™ - D / r e b ê um elemento não nulo de GFCq), possui todas suas raízes em GFC qᵐ> se e somente se a ordem f de b divide r, ou seja; r = f. u para algum inteiro u.

PROVA : Vamos supor que *0* e GFCq™) seja uma raiz de xⁿ - b, ou seja = b C1). Elevando ambos os membros de C1) à r-iêsima potencia temos (*P** = bʳ C2). Porém. /?ⁿʳ = "¹ = 1 e para a equação C2) permanecer válida devemos ter bʳ = 1 que será verdade apenas se a ordem f de b divide r.

EXEMPLO 4.3 Para r = 1 temos n = Cq - 1)/1 =24.

Os polinómios da forma $x^{24} - b$ em GFC5) são $x^{24} - l$, $x^{24} - 2$, $x^{24} - 3$ e $x^{24} - 4$. Como foi visto, a ordem de 1 *é* 1, logo apenas o polinómio $x^{24} - 1$ possui todas suas raízes em GFC252), ou seja, as raízes de $x^{24} - 1$ são todos os elementos não nulos de GFC25}.

EXEMPLO 4.4 Para r = 2 temos n = 24/2 =12

Como as ordens de 1 e 4 são 1 e 2, respectivamente, e ambas dividem r =2, assim $x^{12} - l$ e $x^{12} - 4$ possuem todas suas raízes em GFC25>. As raízes de $x^{12} - 1$ são todas as potências pares de a e as raízes de $x^{12} - 4$ são todas as potências ímpares de *a*.

EXEMPLO 4.5 Para r = 3 temos n = 24/B = 8

Como a ordem de 1 divide r =3, então x - 1 possui todas suas raízes em GFC25} são elas $a°=l$, a^{3}, *a°*, c***. a^{12}, a^{1}"'. a^{18} e a^{21}

EXEMPLO 4.6 Para r = 4 , n = 24/4 = 6

Neste caso como as ordens de 1, 2, 3 e 4 dividem r = 4 os polinómios *x°* - 1, x^{6} - 2, x^{*5} - 3 e x^{*5} - 4 possuem todas suas raízes em GFC25}. As raízes de

x^{4} - 1 são $a = l, a^{4}, a^{8}, a^{12}, a^{16}, a^{20}$

x^{2} - 2 são $a, a^{Z>}, a^{P}, a^{13}, a^{17}, a^{21}$ e a

x^{3} - 3 são $a^{3}, a^{7}, a^{11}, a^{15}, a^{IP}, a^{23}$ e a

x^{4} - 4 são $a^{2}, a^{16}, a^{IO}, a^{14}, a^{18}, a^{22}$ e a

EXEMPLO 4.7 Para r = 6 temos n = 24/6 = 4

Neste caso as ordens de 1 e 4 dividem r = 6, assim os polinómios x^{4} - 1 e x^{4} - 4 possuem todas suas raízes em GFC2S). As raízes de :

x^{4} - 1 são a^{O} =1, a^{tf}, a^{12} & a^{18}

x^{4} - 4 são a^{3}, a^{P}, a^{15} e a^{21}

4.2.3. DETERMINAÇÃO DAS RAÍZES DE $X^r - b$

LEMA 4.3 As raízes de $x^n - b = O$ são ct^{e+ir}. $O < i < n - 1$ contanto que $c^{*en} = b$. onde $O < e < r - 1$.

PROVA Substituindo diretamente x por a^{e+ir} em $x^r - b$ temos $a^{Cetir)ri} . a^{en} - b = a^{irr>} a^{en} - b = a^{irr>} - b = O$, pois $a^{irr>} = ct^{i(q^m - l.»} = 1$.

EXEMPLO 4.8 Para r = 2 temos n = 12. Vamos determinar as raízes de $x^4 - 1$, para o que devemos incialmente encontrar o valor de e, $O < e$ í~ $r - 1$, tal que $c^{*er>} = b$; ou seja; $O < e < 1$, tal que a • 1; assim e = O. As raízes de $x - 1$ são da forma a, $O < i < n - 1$, ou seja, $a^{°+12}$, $0 < i < 11$. que são as potências pares de a.

EXEMPLO 4.9 Para r = 4 temos n = 6

Para determinarmos as raízes de $x^6 - 3$ devemos encontrar um inteiro e, $O < e 5: 3$, tal que a =3 Assim e = 3 e as raízes de $x - 3$ são $a^{O \tilde{} \tilde{} 9+4\backslash}$, $O < i S 5$, ou seja $a^3, a^7, a^{11}, a^{15}, a^{IP}, a^{23}$ ci ea

4.2.4. DETERMINAÇÃO DAS RAÍZES DE X^r -» b

LEMA 4.4 As raízes de x^n b • 0 são $a^{e''r/2+ir}$. $O < i < n - 1$. contanto que $ct^{er>} = b$, $O < e < r - 1$.

PROVA : Substituindo x por $a^{*fr/2+w}$ em $x^r + b$

temos a •+ b = a •a *a + b. C3X Entretanto, a = b, $a^{irn} = 1$ e como a ê primitivo, temos que $a^{rn/2} = a^{(q^m - l>/2} = -1$. Sulbst11uindo estes valores em C3> temos -a + b = -b-»-b = 0.

EXEMPLO 4.10 Para r = 2 temos n = 12. Vamos determinar as raízes de $x^{12} - 4 = x^{12} + 1$ e para tal precisamos encontrar um e, O 2í e 5 1 tal que $c»^{e\ 12} = 1$, então e = O. Assim as raízes de $x^{12} + 1$ são $c«^{eu/2+ri} = o<^{i+2i}$, $O 5 i < 11$, são elas : $c\%, a^3, a^5, a^7, a^P, a^{11}, a^{13}, a^{15}, a^{17}, a^{IP}, a^{21}$ e a^{23}

EXEMPLO 4.11 Para r = 6 temos n = 4. As raízes de - 1 = x^4 •* 4 serão determinadas, para o que devemos inicialmente encontrar um inteiro e, O < e < 5, tal que a*'^{4} = 4, então e = 3. Assim as raízes de x •» 4 são a = a . 0 5 1 í 3, ou seja, c* . c» , a e a que são respectivamente 2. 4, 3 e 1.

Os lemas anteriores indicam como e quando é possível encontrar as raízes do polinómio x ± b. O *tear ema* a seguir nos dará uma cota inferior para a distância mínima dos códigos que serão construi dos.

4.2.5. UMA COTA INFERIOR PARA d

TEOREMA 4.1 Seja *a* um elemento primitivo do campo de Galois GFCq™) no qual x^n - b tem todas suas raízes. n = Cq^m - l)/r e b ê um elemento não nulo de GFCq) cuja ordem divide r. Supondo que ci$^{e*i\,r}$, 0 < 1 < d-2, são raízes de x$^{r'}$-b = 0 o código cujo polinómio gerador ê o mínimo múltiplo comum Cmmc> dos polinómios mínimos correspondendo as raízes et acima, tem distância mínima pelo menos d

PROVA O código que está sendo considerado está no espaço nulo da seguinte matriz, construída com um subconjunto das raízes de x^{7}"' - b = 0.

$$M = \begin{matrix} & a^{-t'n-2)} & \\ Ctt2r)Cn-l) & Cetr)Cr.-2) & e+2r \\ & ct^{Ce+2r)Cn-2)} & \\ 'CetCd-2)lOCn-i> & 'CetCd-2)r)Cn-2) & Cd-2) \end{matrix}$$

Agora vamos considerar o determinante A formado com quaisquer d-1 colunas de M.

$$\dot{u} = \begin{matrix} a & Ci & a^{d-1} \\ C e u) & & C e t r)^{d-1} \\ & a & et \end{matrix}$$

$$\begin{matrix} t e t r t d-2))a_1 & te+rCd-2))a_2 & C \cdots rCd-2))^{d-1} \\ ex \quad a & & 01 \end{matrix}$$

Fatorando os a da í-esíma coluna para todo 1

$$A = ct^{eia} \begin{matrix} 1 & a & 2 & \cdots & a_{d-1} \\ 01 & & Ot & & a^{d-1} \\ 2ra & & 2ra & & 2ra_{d-1} \end{matrix}$$

$$\begin{matrix} td-2)ro_1 & Cd-22)ro_2 & td-2)^{d-1} \\ CA & a & a \end{matrix}$$

Portanto, $h = c^* \begin{pmatrix} a_1 & a_2 & \cdots & a_{d-1} \end{pmatrix} A$

onde $A_í$ é o determinante de Vandermonde; então

$$a - \begin{matrix} or & ar \\ c\ a - & CA^* \end{matrix}$$
$$a.^n \triangleright a$$

Porém, $O < a < n$ Implica que $O < ar < nr = q^m - 1$ e como, por

hipótese, ct tem ordem $q^m - l$. então $ct^{ar} * CA^{ar}$. $j * i$ Então, $* O$ e portanto $A * 0$, garantindo que quaisquer d-1 ou menos colunas de M são linearmente independentes. Conseqüentemente a distância mínima do código é pelo menos d.

4.2.6. CONSTRUÇÃO DE UMA CLASSE DE CÓDIGOS MULTITNiVEIS PSEUDOCÍCLICOS

Nos exemplos seguintes mostraremos como a teoria desenvolvida acima pode ser aplicada na construção de códigos corretores de erros. Vamos continuar utilizando um alfabeto com 5 níveis, q = p^{s} = 5 e m = 2. Portanto o campo original é GFC5} e seu campo de extensão será GFC253.

Na Tabela I são mostrados os elementos de GFC252), onde o polinómio primitivo usado foi rjCx) = x + x + 2. Na Tabela II são mostrados os fatores irredutíveis de x^{24} - 1, com os expoentes de suas respectivas raízes. Esta Tabela facilita a obtenção do polinómio gerador gC>*0*, uma vez que suas raízes tenham sido escolhidas.

EXEMPLO 4.12 Para r = 2 temos n = 12. Como vimos, os elementos de GFC5> cuja ordem divide 2 são 1 e 4 portanto os binômios a serem fatorados são x^{12} -1 e x^{12} -4 = x^{12} +1. Assim os códigos obtidos de x^{12} - 1 são cíclicos e os obtidos de x^{12} •+ 1 são negacíclicos.

Vamos supor que queremos obter um código cujo polinómio gerador gCxT^{1} e fator de x^{12} - 1, e que tenha distância mínima d = 4. Assim, pelo teorema anterior, o polinómio gerador deverá possuir três raízes consecutivas. Sejam $a^{«-i}$, a^{2k} e $a^{2(V•1>}$ estas raízes, para O < k < 11. Fazendo k = 0, temos cu° = 1, *c*^{2}* e *cu**. Devemos encontrar os polinómios mínimos de *a*°, *a*^{2} e *ct**, ou seja,

M°Cx3 = x - 1

M$^{(2)}$Cx) = x^{2} + 3x + 4

M$^{<4>}$Cx} = x^{2} - x -»• 1

onde

M$^{(i>}$Cx) é o polinómio mínimo de a^{V}

Assim

gC>0 = m.m.c ÍM°Cx}. M$^{(2>}$Cx). M$^{<4>}$Cx}3

gCx} = Cx - l)Cx^{2} * 3x + 42>C x^{2} - x • 1>

= x^{5} -»• x^{4} - 3x^{2} + 5x - 4

O código obtido ê um código cíclico Cb = 1) com parâmetros n = 12, k = 7 e d = 5 .

EXEMPLO 4.13 Para r = 4 temos n = 24/4 = 6 e os polinómios geradores podem ser escolhidos como fatores de x - 1, x - 2 . x - 3 e x - 4. No caso de x - 4 = x + 1, suas raízes são a^{2}, a^{5}, a^{10}, a^{14}, a^{17}, a^{22} ea . Para um código com distância mínima d = 2 o polinómio gCx) basta ter uma raiz. Assim, podemos escolher x - 3 ou x - 2, cujas raízes são $c^{<18}$ e ci^{C}. r especti vãmente.

Os códigos obtidos neste caso possuem parâmetros C6.5.2) e portanto são MDS Cdistância máxima separáveis), ou seja d • *n* - *k* * 1.

Outros códigos com distância mínima maior que 2 podem ser obti dos

Cn.Jc.d)	gtx)	Raízes de gCx)
C6.3.4)	x^{3} + x^{2} + 3x 4 2	Ca^{2}. a*\ a^{10})
C6.1.6)	x^{5} 4 3x^{4} 4 4x^{3} 4 2x^{2} 4 $_{x}$ «4 3	Ca^{2}.ct^{6}, ct^{10}.et*^{4}, a^{22})

Códigos constaciclicos são obtidos pela fatoração de x^{e} - 2 :

Cn,)c,d)	gCx)	Raizes de gCx>
C6.4.3)	x^{2} 4 x 4 2	Ca, a^{3})
C6.2.S)	x^{4} 4 x^{3} 4 4x^{2} 4 2x 4 4	Ca,a^{5},c.^{P},c«^{21})

EXEMPLO 4.14 Para r = 6 temos n = 24/6 = 4 . Como n =2, temos n = Cq^{2} - 1)/Cq 4 1) = q - 1, assim, para valores de r = q 4 i, o comprimento do bloco será q - 1. Os valores para b são 1 e 4. Assim, os polinómios geradores são fatores de x^{4} - 1 e x^{4} - 4 = x^{4} 4 i. Para x^{4} - 1, suas raizes são *a*° - 2, a^{12} = 4, $a^{\cdot 8}$ = 3 e a^{24} = l e x^{4} - 1 = Cx - DCx - 2)Cx - 3)Cx - 4). Códigos Reed-Solomon sobre GFC5) são obtidos pela fatoração de x^{4} - 1.

Para - 4 = x⁴ -+ 1 temos ot$^{3+<5t}$ O < i < 3 como raízes, ou seja c*³, c*ᵖ, a¹~ᵛ e et²¹. Da Tabela II podemos observar que x⁴ - 4 = Cx - aᵖ) Cx - a²¹} Cx - a³) Cx - a¹⁵) = Cx² +2) Cx² -»• 3) possui dois polinómios irredutíveis em GFC52> de grau 2; códigos corretores de um Cínico erro podem ser formados, porem apenas se os símbolos do código pertencerem ao campo de extensão GFC25X

4. 3. DECODIFICAÇÃO ALGÉBRICA DE CÓDIGOS MULTINÍVEIS PSEUDOCÍCLICOS

Nesta seção demonstraremos como códigos pseudocíclicos podem ser decodificados por um procedimento algébrico. A ideia básica é o emprego de uma transformação afim, que faz do código pseudociclico um código cíclico equivalente num campo de extensão GFCq™2> [163. Usaremos a decodificação algébrica no domínio da frequência, por meio da transformada de Fourier de campo finito CTFCF) [53 e [173 e o algoritmo de Euclides para determinação do polinómio localizador de erros [173.

Para poder empregar corretamente a TFCF para vetores de comprimento n, faz-se necessária a utilização de um nücleo que tenha ordem n. Vimos na seção anterior que as raízes de x - b só contém fatores primitivos quando a ordem de b ê r. Desta forma, com com exceção do caso em que b = 1. o cálculo da síndrome não *ccrr&s* ponde a uma transformada com inversa. Dessa forma. foi necessário utilizar uma transformação afim [103 para resolver esta dificuldade. O lema a seguir estabelece as condições que devem ser satisfeitas pela transformação afim utilizada [163.

LEMA 4. 5 Sendo c*$^{ie*ir>}$. a < i < a + d- 2. O < a < n - 1 as raízes consecutivas do polinómio gerador gCx), a permutação afim x = $_{a}{}^{(e*ur>}$ y. 0 < u < d - 2 , transforma o código pseudociclico em um código cíclico equivalente sendo *cx* primitivo em

PROVA A substituição de x = $_{a}{}^{(**ur>}$ $_{y\ em\ x^{n}}$ - b dá como resultado

a y - b = a y - b . . . . . <.4.1->

como $a^{n\,r} = 1$ e $a^{n\,e} = b$, temos de C4. 1}

$by^{r\,'} - b \ll b\ Cy^{n} - 1)$ . . . . . .C4.2>

Assim $y^{r\,'} - 1$ dâ origem a códigos estritamente cíclicos porem em GFCq™} e não em GFC q>. As raízes de $y^{n} - 1$ têm ordens que dividem n [103, sendo facilmente obtidas a partir das raízes de $x^{n} - b$ e da transformação afim empregada, tendo como expoentes Ci-LDr, onde u é um parâmetro O < u < d - 2. e i ê variável, a 5 í < a -* d - 2. Obviamente, o código cíclico obtido por meio da transformação afim é equivalente ao código pseudoclclico original, ambos tem portanto os mesmos parâmetros e também a mesma distância *mínima.*

Q. E. D.

4.3.1. ALGORITMO DE DECODIFICAÇÃO

Apresentaremos a seguir o algoritmo de decodificação algébrica e daremos um exemplo no final.

Seja fCx-> o polinómio que representa a soma do polinómio mensagem vC x3 e do polinómio erro eCx2>. Devemos aplicar inicialmente a transformação afim em fCxD. para transformar o código pseudocíclico em cíclico. Assim temos: fCy) = vCyD + eCy}. Os passos para decodificação de fCxT> são.

1. CALCULO DO POLINÓMIO SÍNDROME SCZ3

$$SC2D = \sum_{i=0}^{d-2} S_i\ Z^{i} \quad \text{. . . . . C4.3>}$$

onde $S_i = fCc»^{i\,r}:>$. O < i < d - 2

como fCy) = vCy> * eCyD, então resulta

S = vCa) + eta) = eta),

visto que

$$V(a^{1'}) = O$$

lembrando que

$$S = E \cdot O < J < d - 2$$

onde

$E = (E_0, E_1, E_2, \ldots E_j \ldots E_{n-1})$ representa a TFCF de eCyZ>. Nesta etapa determinamos os primeiros d-1 valores de E.

2. CALCULO DO POLINÓMIO LOCALIZADOR DE ERROS LCZ>

Aplicar o algoritmo de Euclides ao par de polinómios Z^{2t} e SCZX Lembrar que SCZ> é do grau $d - 2 = 2t + l - 2 = 2t - l$. Parar quando o grau do polinómio resto for menor que t [173. As localizações dos erros, na palavra recebida, são indicadas pelos expoentes dos valores recíprocos das raizes de LCZX

3. DETERMINAÇÃO DO VETOR E ASSOCIADO AO POLINÓMIO ECZ>

O vetor E, TFCF do vetor erro e, associado ao polinómio eCx), é obtido por extensão recursiva a partir de LCZ> e SCZ} [173.

4. CÁLCULO DA TFCF INVERSA DE ECZ}

A fim de determinar eCy> calcularemos a TFCF inversa de ECZD

$$e = (e_0, e_1, e_2, \ldots e_{n-1})$$

onde

$$e_i = nC \bmod p) \sum_{j} E_j a^{\sim ri\ 1}$$

porém rCmod p) = Cp-lVr

e então resulta

$$e = r \sum_{n-1} E\ cT^{TX3}\ r/Cp-1). \qquad (C4.4)$$

5. APLICAÇÃO DA TRANSFORMAÇÃO AFIM INVERSA PARA OBTER e(x)

Com o intuito de obter eCx) aplicamos a transformada afim inversa.

6. CORREÇÃO DOS ERROS

Subtraindo eCx> de *fCzO* efetuamos a correção dos erros. i.e,

$$vCx> \ll fCx> - eCx>. \qquad (C4.5)$$

EXEMPLO 4.15 Vamos considerar o código pseudociclico C6.2.50 com 5 níveis, ou seja p = 5 e s = 1, obtido a partir da fatoração de x - 2. Como foi visto anteriormente as raízes de x° - 2 estão contidas em GFC25) e possuem os seguintes expoentes : 1 + 4i , O < i < 5. Como a distância minima é d = 5 o polinómio gCx) deverá possuir 4 raízes consecutivas. Vamos escolher et^{21}, a, a^5 e et como raízes. Usando a Tabela III, podemos determinar os polinómios mínimos de Ca. $a^52>$ e $Ca^P, a^{21})$

ou seja

$$Cx - cOCx - a^5) = x^2 + 4x + 2$$

$$Cx - a^P)Cx - a^{21}) = x^2 * 2$$

Assim o polinómio gerador gCx> e dado por

gCx) = C x² + 4x 2)C x² + 2) = x"* + 4x³ • 4x² + 3x + 4.

Seja fCx) = 3x -• x o polinómio recebido; a transforma
21
çSo afim a ser utilizada é x = a y. Assim as raízes de gCx) tem os seguintes expoentes O, 4, 8 e 12. Substituindo x por c«²¹y em fCx) obtemos :

$$
\begin{aligned}
fCy) &= 3\,Ca^{21}\,y)^5 \quad a^{21}y \\
&= 3\,a\,y + ct\,y \\
&= 3\,C3a + D\,y^5 \bullet + a^{21}y \\
&= C4a + 3)\,y^5 + a^{21}y \\
&= a\,y + a\,y \\
&\quad 3 \quad 5 \quad 21
\end{aligned}
$$

fly) = a y •+ a y

SSo os seguintes as passos para decodificar fCx)

1. CALCULO DO POLINÓMIO SÍNDROME SC2D .

$S_o = fCa°) = fCl) = a^3 \quad a^{21} = 4a + 3 \quad 2a + 4 = a + 2 = a^{15}$

$S_{í} = fCa^4) = a^3(a^4)^5 + a^{21}a^* = a^{23} + a = 2a\text{-»-}3 + a = 3a + 3 = a^{1<5}$

$S_2 = fCa^8) = a^3(a^8)^5 + a^{2'}a^8 = a^{1P} * a^5 = 3a + 4a + 3 = 2a+l = a^8$

$S_3 = fCa^{12}) = a^3Ca^{12})^5 + a^{21}a^{12} = a^{19} + a^{p} = a+2+3a+l = 4a+3 = a^3$

Assim

$$SCZ) = a^3 Z^3 - a^8 Z^2 4 a^{145} Z + a^{15}$$

2. CALCULO DO POLINÓMIO LOCALIZADOR DE ERROS LCZ)

Antes de iniciarmos o cálculo, vale lembrar que :

$L_0 CZ) = O \;.\; L_1 CZ) = 1$

$q_1 CZ) = \dfrac{r\_CZ)}{r_{i-í}\,CZ)}$ onde $q_i CZ)$ é o quociente da divisão de $r_{1-2} CZ)$ por $r_{i-1} CZ)$

e $L_i CZ) = L_{v-2} CZ) - q_l CZ) L_{i-1} CZ)$

Assim temos :

i	L CZ)	r CZ>	q CZ)
0	0	z^4	—
1	1	a Z +c< Z +a Z+ct	—
2	-Ca Z+a 5	*a ZT +c* Z+a*	*a Z+ct*
3	l+La Z+a 2>Cc* Z-^a	a Z + c<	*a Z+ct*

$$LCZ2 = L_3 CZ> = 1 4 Ca^{21}Z + a^{\cdot 4})Ca^{15}Z * a^4\}$$

$$LCZ> = 4Z^2 4 Z 4 4$$

Observe que os coeficientes de LCZ> são :

$L_o = 4$, $L_1 = 1$ e $L_2 = 4$.

3. CALCULO DO VETOR E

Temos que $\pounds_{t=o}^{11} E_1 L = O$ ou seja

$$E_{1-2} L_2 4 E_{j-1} L_1 + E_J L_o = 0$$

Como os E^, O < i í d - 2, Jâ são conhecidos no cálculo da síndrome, ou seja, $S_o = E_o$ para O < j < 3, resta apenas calcular E_4 e E_5. CNeste caso $m_o = 0$^ sendo

$$L_o = 4, L_1 = 1 \text{ e } L_2 = 4$$

temos

$$E_{J-2} 4 + E_{j-1} + E_j 4 = 0$$

então

$$E_{J-2} = E_{j-1} 4 4E_j$$

assim

$$E_4 = E_3 4 4E_2 = a^3 4 4a^8 = a^*$$

$$E_5 = E_4 4 4E_3 = a^4 4 4a^3 = c^{*2\circ}$$

e portanto :

$$E = (a^{15}, a^{8}, a^{3}, a^{4}, a^{20})$$

que é a transformada CTFCF) de eCyX

4. CÁLCULO DA TFCF INVERSA DE E

A transformada inversa de E é dada por

$$i \quad nC\mathrm{mod}\ p2> \quad j$$

onde a é um elemento de ordem n de GFC25>. Usaremos a = a* como núcleo da transformação.

Assim

$$e = E + E + E + E + E + E =$$

$$= ct + a + a + a + a + ct = 0$$

$$e = E + E\ ct^{4} + E\ a^{9} * E\ o^{12} + E\ a^{1} * - E\ o'^{20}$$

De forma semelhante calculam-se todos os e_i*s.

Então

$$e = CO.\ a^{21}.\ O.\ O.\ O.\ a^{3}\}$$

ou seja

$$eCy) = a^{35}\ y \cdot a^{21}\ y$$

5. APLICAÇÃO DA TRANSFORMAÇÃO AFIM INVERSA PARA OBTER eCx)

$$y = x/a^{21} = a^{3}\ x$$

então

$$eCx) = a^{3,3.5}\ Ca\ x) + a^{21,.3.}\ (a\ x)$$

$$= a^{18}\ x + a^{5}\ x^{24}$$

$$= 3x^{5} + x$$

6. CORREÇÃO DOS ERROS

vCx) = fCx3 - eCx) = O

Tabela I - Eleméritos de GFC25) usando o polinómio primitivo nCx) = x^2 + x + 2.

O				
1				
a		2a	a^{13} = a^{A} 4a	a^{ip} = 3a
a^2	4a + 3	a 3a ^ 1	a = a 4 2	$a^{2°}$ = 2a 4 4
Ct =	4a + 2	a 3a 4 4	a^{15} a + 3	a^{21} = 2a 4 i
3				
a —	3a + 2	a^{10} = a 4	a^{10} = 2a 4 3	a^{22} = 4a 4 1
4	4a + 4	3a ^ 3	oi 37 a 4 1	a^{23} = <^a 4 c
a =	2	12 4	a = 3	a^{24} = 1
o =				
a =				

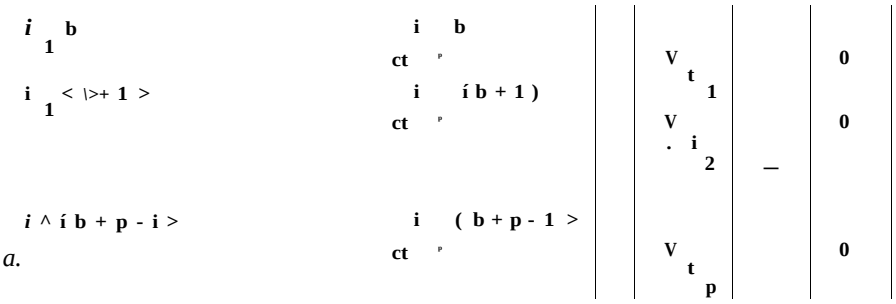
Tabela II - Fatores irredutíveis de $x^4 - 1$ e os expoentes das raízes correspondentes

POLINÓMIO	EXPOENTES DAS RAÍZES
$x^2 * x + 2$	C1 .5)
$x^2 + 4x + 2$	Cl 3.17}
$x^2 + 2$	C9,21>
$x^2 + 2x \bullet 3$	
$x^2 * 3x + 3$	09.23}
$x^2 \wedge 3$	C3.155
$x - 3$	C18}
$x^2 + 3x * 4$	C2.10}
$x - 2$	Ct»
$x^2 + 2x + 4$	Cl4,225
$x - 1$	CO}
$x^2 \wedge x 4 1$	C8.16)
$x + 1$	C125
$x^2 - x + 1$	C4.20}

Tabela I I I - Elementos de GFC25) usando o polinómio primitivo nCx) = x² 4 4x 4 2.

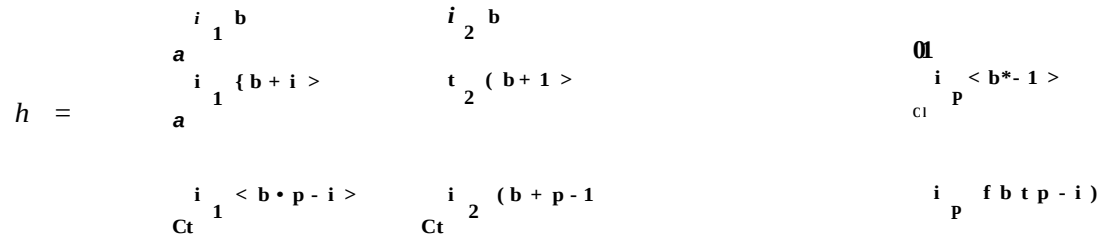
0			
1			
	2a	a **13** 4a	a **1P** = 3a
ct² = a + 3	a 2a 1	**14** 4a -v 2	a²° = 3a **4** 4
*ct*³ = 4a •+ 3	o **P** 3a + 1	**i 5** a + 2	a **21** = ~2a • 4
o* = 2a * 2	a **1O** 4a + 4	**1***O* 3a 4 3	a²² = a - 1
a⁵ = 4a 4 1	3a 4 2	*a* **17** a 4 4	a²³ = 2a + 3
a⁰ = 2	**12** 4	a **1B** 3	²* 4 a = 1

Assumindo que o peso de v é p < ó - 1 Ficamos com

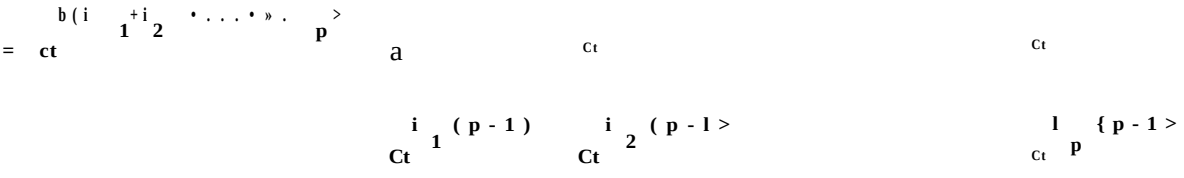


onde i , i . . . . . i indicam as posíç&es não nulas de vCxZ).
1 2 p

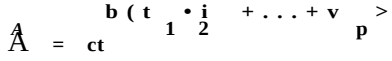
Agora vamos considerar o determinante A, formado pelas colunas d H^T usadas acima.



fatorando os **ct** da k-ésima coluna para todo k. 1 < k *: p obtemos



Por tanto



onde A é um determinante de Vandermonde que é diferente de zero
V
[103.
Portanto vCx3 = O e d > ó.

5. 2. DECODIFICAÇÃO SIMPLIFICADA DE CÓDIGOS BCH

Apresentaremos lemas e teoremas que estabelecem as propriedades dos códigos BCH que permitem simplificar as operações no processo de decodifícação, quando desejarmos detetar ou corrigir erros. O decodificador utiliza um conjunto de dígitos da síndrome com um comprimento que depende do número máximo de erros a serem detetados ou corrigidos El83.

5.2.1. MATRIZ DE VERIFICAÇÃO DE PARIDADE DOS CÓDIGOS BCH

Uma ênupla binária v = C v_0. v_1 . . . .v_{n-1} > é uma paia**vt**a-código de um código BCH de comprimento n = 2 - 1 se e somente se o polinómio vt"x) = $v_0 + v_i x + . . . + v_{r.-i} x^n$ tem ct. $a^2, . . . ,$ ct como raízes, ou seja:

$$vCct\ D = v_0\ v_1\ ct^1 \bullet v_2\ ct^{21} + ... + v_{Ti-1}\ a^{<r,-1>1} = O. . . . . C5.1>$$

para 1 < i < St.

Podemos escrever a equação C5.15 na forma matricial mostrada abaixo:

$$fv_0\ v_1 . . . .v_{D-1J} \quad ct^{2i} \quad = O \qquad C5.2\}$$

$$(n-1>i$$

para 1 < i < 2t. A igualdade dada por C5. 2!> nos diz que o produto interno de fv , v . . . . . v "| por fl, a , a^{21}, ... c*$^{(n\ 1}$*^{1}1 é nulo. Podemos então formar a seguinte matriz.

a (A a^r>-1

. 2 . 2.2 2 = n - 1
Ca 5 Ca 5 Ca 5 Ca 5

[H] = C5. 35

. , 2t. . 21.2 21.3 , 2t.n-l
1 Ca) Ca) Ca 5 ... Ca 5

Portanto de C5. 3) seaue que se V = fV , V . . . V 3 é uma palavra- código em um código BCH *carretar* de t erros, então:
o I r»-1

[v3 . fH3 = O C5. 45

O código ê o espaço-nulo da matriz H e H ê a matriz de verificação de paridade do código [33.

5. 2. 2. MATRIZ REDUZIDA DOS CÓDIGOS BCH

LEMA 5.1 : A matriz r ~i c »1 »1 (l-HTJ • X > J -7 . O < i < t -1 . O < 1 < n-1 , tem posto t , onde X ê um parâmetro, 1 < X < 6 - t e a ê um elemento de ordem n de um campo de Galois.
o o o

PROVA : A prova segue os mesmos passos usados para provar o teorema da cota BCH. Temos que :

a im o+X >	a im o+X > 2	a (m o tX > (n - l >
a (Til + X + 1 >	a (m o • X • 1) 2	a <m o + X-t- 1 > < n - i >
a o	a	a

[M] = C5. 55

l a (m o +-X+1 o - 1 > a im o -t-X+t o - 2 > a (m o +X+t o -J > l n - 1 >

Considere um determinante D formado pela seleção de quaisquer t coluna de [M3, onde b = m + X.
o o

PROVA Seja £e3 a representação de um vetor erro contendo no máximo t_o erros, i.e., um vetor de peso menor ou igual a t_o, e fv3 o vetor código transmitido,

A ênupla recebida £r3 é dada por

[r3 = [v3 + fe3 C5.6)

Usando a matriz £M3 do Lema 5.1 como a matriz de de verificação de paridade, então segue que

$[M3.[r3^T = [M3.[v3^T + [M3.[e3^T = [M3.fe3^T$. desde que $£M3.£v3^T = O$

Considerando que foi assumido que Íe3 tem peso menor ou igual a t^, o produto $ÍM3.[e3^T$ pode ser escrito como

Xl Xl

a

í t-X > i (X * í > l (í • X > 1

Cl o a CS. 7>

< i_o - í + X > l_1 (t_O - í * X > 1_2 íi $_o$ - 1 + X > v_i

a a

onde $e^{\wedge}_i$, 1 < i < são as componentes não nulas do vetor erro fe3. Na forma polinomial £e3 pode ser representado por eCx) como segue

$e(x) = e_1 x^{l_1} + e_2 x^{i_2}$ ... C5.8)

Fazendo-se x = *a* em eCx), onde O < i ± t_o - l e X é um parâmetro, 1 < X < 6 - t_o, o lado direito de C5.8) coincide com C5.7). Também, pelo Lema C5.1D, a matriz produto dada por C5.7) pode ser um vetor coluna não nulo se e somente se e_i O, para pelo menos um valor de i, no intervalo, 1 5 i < t_Q. Segue então o seguinte teorema.

$$eCx) = \pounds \quad e \quad .x^{s}$$

$$s = p + i \qquad s$$

O polinómio recebido rCx) é então dado por

$$rCx) = vCx5 + eCxZ \qquad (C5.11)$$

ou

$$rCx) = cCx) - pCx) + eCx) \qquad (C5.12)$$

5.3.1. POLINÓMIO LOCALIZADOR DAS PERFURAÇÓES LCx)

O polinómio localizador das perfurações ê dado pela seguinte expressão

$$LCx) = \prod_{S=1}^{P} Ca^{5} x - 1) = \mathbf{E}^{P} L_{l} x \qquad (C5.13)$$

5.3.2. POLINÓMIO SÍNDROME SCx)

O polinómio síndrome sCx) ê dado pela seguinte expressão Í173.

$$SCx) = \pounds_{J=o}^{Ó-2} S_{J} x^{J} \qquad (C5.14)$$

onde

$$S_{j} = rCa^{\circ}) = eCa^{\circ}) - pCa^{\circ}) \qquad (C5.15)$$

desde que

$$cCa^{j \cdot m}{}^{\circ}) = O, \quad O < J < 6 - 2$$

5. 3. 3. POLINÓMIO SÍNDROME MODIFICADO TC x>

Em seguida vamos considerar e definir o polinómio síndrome modificado TCx2> [173.

$$T(x) = \sum_{i=0}^{6-2} T_i x^i$$

$$T(x) = S(x) \Lambda(x) \bmod x^{6-1} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5.16)$$

onde

$$\Lambda(x) = \prod_{s=1}^{p} (1 - a^{l_s} x) = \sum_{i=0}^{p} \Lambda_i x^i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5.17)$$

e o polinómio localizador das perfurações.

5.3.4. OS COEFICIENTES DE MAIS ALTA ORDEM DE TCx>

LEMA 5.2 Os 6 - 1 - p coeficientes de mais alta ordem do polinómio síndrome modificado TCx} são dados pela seguinte expressão

$$T_i = \sum_{s=1}^{p} e_{l_s} a^{(m_0+1)l_s} \Lambda(a^{-l_s}), \quad p \le i \le 2t-2$$

PROVA : Temos que

$$T(x) = S(x)\Lambda(x) \bmod x^{2t}$$

$$T(x) = \left(\sum_{j=0}^{2t-2} S_j x^j\right)\left(\sum_{i=0}^{p} \Lambda_i x^i\right) \bmod x^{2t}$$

$$T(x) = (S_0 + S_1 x + \ldots + S_{2t-2} x^{2t-2})(1 + \Lambda_1 x + \ldots + \Lambda_p x^p) \bmod x^{2t-1}$$

Observando que

$$T_o = L_o$$

$$T_1 = S_1 L_0 + S_o L_i$$

$$T = S L + S L + \ldots + S. L.$$
$$i \quad i\,o \quad i-l\,l \quad i-J\,J$$

Como $S = rCa^{m+i}$ ° 5. temos que

$$T_i = r\,(a^{m+i}\,°\,)L_o \;\text{»•}\; r\,(a^{w>\,\bullet\bullet i-i}\,)L_* + {}^{+}\,r\,(\,«^{m_O\,+\bullet\,v-j}$$

O < j < P

os *6* - 1 - p coeficientes de ordem mais alta de TCx5 são :

$$T = \mathbf{E}^{p}\,\mathbf{r}\,(a^{TIi\,+\bullet l-J}\,°\,> L \ldots p < i < 6-2 \quad \ldots . C5.185$$

expressão C5.185 pode ser simplificada utilizando a equação C5. 145.

$$T - \mathbf{E}^{P}_{1=o}\,[eCo^{m\,\bullet i-j}\,°\,\mathbf{5}\,"\,p(o.^{+i-1}\,>L$$

Lembrando que

$$eCx5 = \mathbf{E}^{p+l\,o}_{S=p+1}\,e_L\,.x^{i}_{s} \qquad pCx5 = \mathbf{E}^{P}_{s=i}\,{}^{c}_{l}\,\bullet^{x}_{s}$$

Temos

$$T. = \mathbf{E}^{p}_{j=o}\,\mathbf{E}^{p+l\,o}_{a=p}\,{}^{e}!\,\bullet^{a}_{s}\;\mathbf{O}\;\mathbf{E}^{P}_{*=1}\,\mathbf{C}\,m_{o}\,\wedge -j5\,i_{s}$$

$$T_i = \sum_{j=0}^{P4-1} \left[\sum_{s=p+1}^{} \left(\sum_{J=0}^{} \right) \right]$$

$$T_i = \sum_{s=p+1}^{} \left[\sum_{J=0}^{*} \left(\sum_{s=1}^{} \right) \right]$$

mas $\prod_{JJ} L(ct^{-i_a}) = L(ct^{-1_m})$ e então

$$T_i = \sum_{s=p+1}^{} e_{.a^{\circ}} L(ct^{s}) - \sum_{s=1}^{} e_{,a^{\circ}} L(ct^{s}) \qquad C5.19)$$

como $L(ct^{-1^{s}}) = O$ para 1 5: s < p, então

$$T = \sum_{s=p+1}^{} et^{1_{O}} L(ct^{-1} \qquad p < i < 6 - 2 \qquad C5.20)$$

5.3.5. DETEÇÃO SIMPLIFICADA DE ERROS EM CÓDIGOS B.C.H PERFURADOS

O teorema seguinte estabelece as condições para simplificar o processo de decodificação dos códigos BCH perfurados usados para deteção de erros.

TEOREMA 5.3 : Quando um código BCH Cn.k.ó) perfurado em p dígitos é usado para a deteção de até t^ erros, t < ô — p, o vetor recebido é uma paiavra-código válida se e somente se o polinómio síndrome modificado TCx) tem um conjunto de t coeficientes iguais a zero, escolhidos entre seus ó-l-p coeficientes de mais alta ordem.

PROVA : Um conjunto particular de t coeficientes consecutivos de TCx) contidos em seus 6 - 1 - p coeficientes de mais alta ordem podem ser escritos com ajuda da equação C5.20) da seguinte maneira

5. 3. 6. CORREÇÃO SIMPLIFICADA DE ERROS EM CÓDIGOS B. C. H PERFURADOS

TEOREMA 5. 4 : A correção de erros. num código BCH Cn,k,6) perfurado por p dígitos, pode ser realizada com um conjunto de 2t^ < ó-l-p coeficientes consecutivos do polinómio da síndrome modificada TCx), escolhidos entre seus ó - 1 - p coeficientes de ordem superior.

PROVA A prova segue exatamente os mesmos passos usados para provar o teorema 3 com 2t = t [183.

CAPÍTULO 6

DECODIFICAÇÃO POR ARMADILHA PARA ERROS EM CÓDIGOS CÍCLICOS

O método de Meggitt para decodificação pode ser aplicado para qualquer código ciclíco, porém algumas modificações são necessárias para sua implementação £33. Apresentaremos uma variação prática do decodificador de Meggitt, chamada de decodicador por armadilha para erros Cerror-trapping). A decodificação por armadilha para erros foi inventada independentemente por Kasanu , [113. Mitcbell. [123 e [133 e Rudolph, [93. Este método é mais eficaz para a decodificação de códigos corretores de um único erro, alguns códigos corretores de dois erros e códigos corretores de erros em surtos. Quando este método é aplicado para códigos longos, com altas taxas e com larga capacidade de correção, ele torna-se muito ineficiente e a capacidade de *correção* de tais còdigos e sacrificada. [33.

6.1. DECODIFICAÇÃO POR ARMADILHA PARA ERROS CDECISÃO ABRUPTA)

6.1.1. CAPTURA DOS ERROS

Se colocarmos algumas restrições sobre os padrões de erros que desejamos corrigir, o decodfícador de Meggitt poderá ser implementado praticamente [33. Vamos restringir os erros que desejamos corrigir àqueles que estão confinados em Cn-k) posições consecutivas, incluindo o caso em que as Cn-k) posições ocupam o início e o fim da palavra. Com esta restrição, mostraremos que a correção e deteção de erros se resume praticamente em comparar o peso da síndrome com o valor de t, onde t é a capacidade de correção do código.

Vamos considerar um código cíclico Cn,k,d) com polinómio gerador gCx) e supor que a palavra vCx) foi transmitida e corrompida por um padrão de erros eCxX Então a palavra recebida será

rCx3 = vCx3 + eCx) C6.13

Inicialmente vamos supor que os erros estejam *ccnfína* dos nas Cn-k) posíç&es de mais alta ordem, ou seja, x^{k}, x^{k+1} . . . . . x^{n-1} de rCx>. Desta forma temos

$$eCxD = e_{k}x^{*} + e_{k+1}x^{**1} + \ldots + e_{n-1}x^{n-1} \quad \ldots\ldots C6.2D$$

Se rCx) è ciclicamente deslocado Cn-k2 vezes os erros estarão confinados nas Cn—JO posiçóes de mais baixa ordem, ou seja, nas posições dos dígitos de paridade x°, x^{1}, x^{2} . . . x^{n-k-1} de $r^{(n-k)}Cx5$.

DÍGITOS DE PARIDADE	DÍGITOS DE INFORMAÇÃO
n-k	k

FIG. 6.1 - FORMATO DAS PALAVRAS-CóDIGO

O padrão de erros correspondente será

$$e\ lx) = e_{k} + e_{k+1}x + \ldots e_{r>-1}x \quad \ldots\ldots C6.32$$

Desde que a síndrome s tx> de r **XJ** e igual ao resto da divis&o de $e^{(r)}$ Cxí por gCx) e como o grau de $e^{(r)}$ *Cx2 è menor que Cn-k2, obtemos a seguinte igualdade

$$s\ (.x> = e\ Cx) = e_{k} + e_{k+1}x \cdot e_{n-1}x \quad \ldots\ldots (b.4:$$

. , multiplicando $s^{(n-k>}$ por x^{k}, temos

$$x^{k}s^{(n-k)}Cx> = eCx2 = e_{k}x^{k} + e_{k+J}x^{k+1} + \ldots + e_{n-1}x^{r»-i} \quad \ldots\ldots CS.52$$

Isto que dizer que. se os erros estão confinados em Cn-k2 posições de mais alta ordem do polinómio recebido rCx), o padrão de erros eCx) é idêntico a x^{*} $s^{(n-k)}$ *Cx2 Quando este evento *ocorra* simplesmente computamos $s^{(n-k>}Cx>$ e somamos x $s^{(n-k)}$ *Cx) a rCx2>. O vetor resultante e a palavra código transmitida.

Se os erros não estão confinados nas Cn-JO posições de mais alta ordem, mas confinados em Cn-JO posições consecutivas x', x ..... x de rCx2>, então rtx) ê deslocado ciclicamente n-i vezes para a direita, os erros poderão ser confinados nas Cn-k) posições de mais baixa ordem de r'[n l>] Cx5 e o padrão de erros será idêntico a x .s Cx2>, onde s Cx> ê a síndrome de r C**XJ.**

Portanto. se os erros estão confinados nas Cn-k) posições que não são as Cn-kO posições de mais alta ordem de rCx), apôs todo o vetor rCx} ter sido deslocado no registrador da síndrome, o conteúdo do registrador da síndrome deverá ser deslocado um certo número de vezes até ficar idêntico aos dígitos do vetor erro. Este procedimento *é* chamado captura dos erros Cerror-trapping}.

Mostraremos a seguir como detetar que os erros foram capturados no registrador da síndrome.

TEOREMA 6.1 Se o número de erros em rCx5 ê menor ou igual a t e se eles estão confinados em Cn-k5 posições consecutivas, os erros estarão capturados no registrador da síndrome apenas quando o peso da síndrome no registrador torna-se menor ou igual a t. £33.

PROVA Um padrão de erros eCx> com t ou menos erros os quais estão confinados em Cn-kO posições consecutivas, deve ser da *forma* eCx5 = X[3] BCx2>, onde BCx2> tem t ou menos termos não nulos e tem grau igual ou menor que n -k - 1. Para o caso em que as n - k posições ocupam o fim e o inicio da palavra. a forma *acima* pode ser obtida com um certo número de deslocamentos.

Dividindo eCsO pelo polinõmio gerador gCx>, temes

$$X^{j} B(x) = a(x) g(x) + s(x) \quad (6.65)$$

onde sCx5 é a síndrome de X[j]BCx5. Desde que sCx5 + X[j]BCx5 é um múltiplo de gCx5, ele é um polinômlo-cõdigo. A síndrome sCx5 não pode ter peso menor ou igual a t sem que sCx5 = X[i]BCxX

Suponha que o peso de sCx5 é menor ou igual a t e que sCx5 * X[i]BCx5. Então sCx5 + X[j]BCx5 ê um vetor código não nulo com peso *menor* que 2t •* 1. Isto é impossível desde que o código corretor de t erros deve ter um peso mínimo maior ou igual a 2t 1.

Portanto, concluímos que os erros estão capturados no registrador da síndrome apenas quando o peso da síndrome torna-se *menor* ou igual a t [33.

Podemos agora apresentar o algoritmo de decodificação por armadilha para erros.

6.1.2. ALGORITMO DE DECODIFICAÇÃO POR ARMADILHA PARA ERROS

1- *PASSO:* Calculo da síndrome sCx)

2- PASSO: Comparação do peso da síndrome W_s com t CW$_s$ < t?)

3- PASSO: Se W_s < t então os erros foram capturados e a síndrome e igual aos erros nas Cn-KO posições correspondentes; soma-se a síndrome com rCx) e os erros são corrigidos.

4- PASSO: Se W > t desloca-se o conteúdo do reaistrador da síndrome com as realimentaçóes ligadas para obter a nova síndrome s tx).

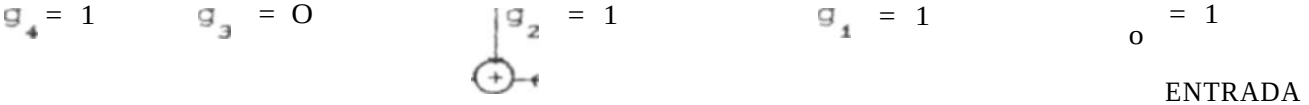
5- PASSO: Apôs cada deslocamento compara-se o peso da síndrome s **Cxj** con t.

6- PASSO. Se para algum i. 1 5 i £ n - 1 W £ t entàc os erros foram capturados; soma-se rCx) com X*s^{1} Cx) e os erros são corrigidos.

7- PASSO: Se apôs o enésimo deslocamento, sempre ocorre que W_s > t, então os erros não podem ser capturados e são apenas detetados.

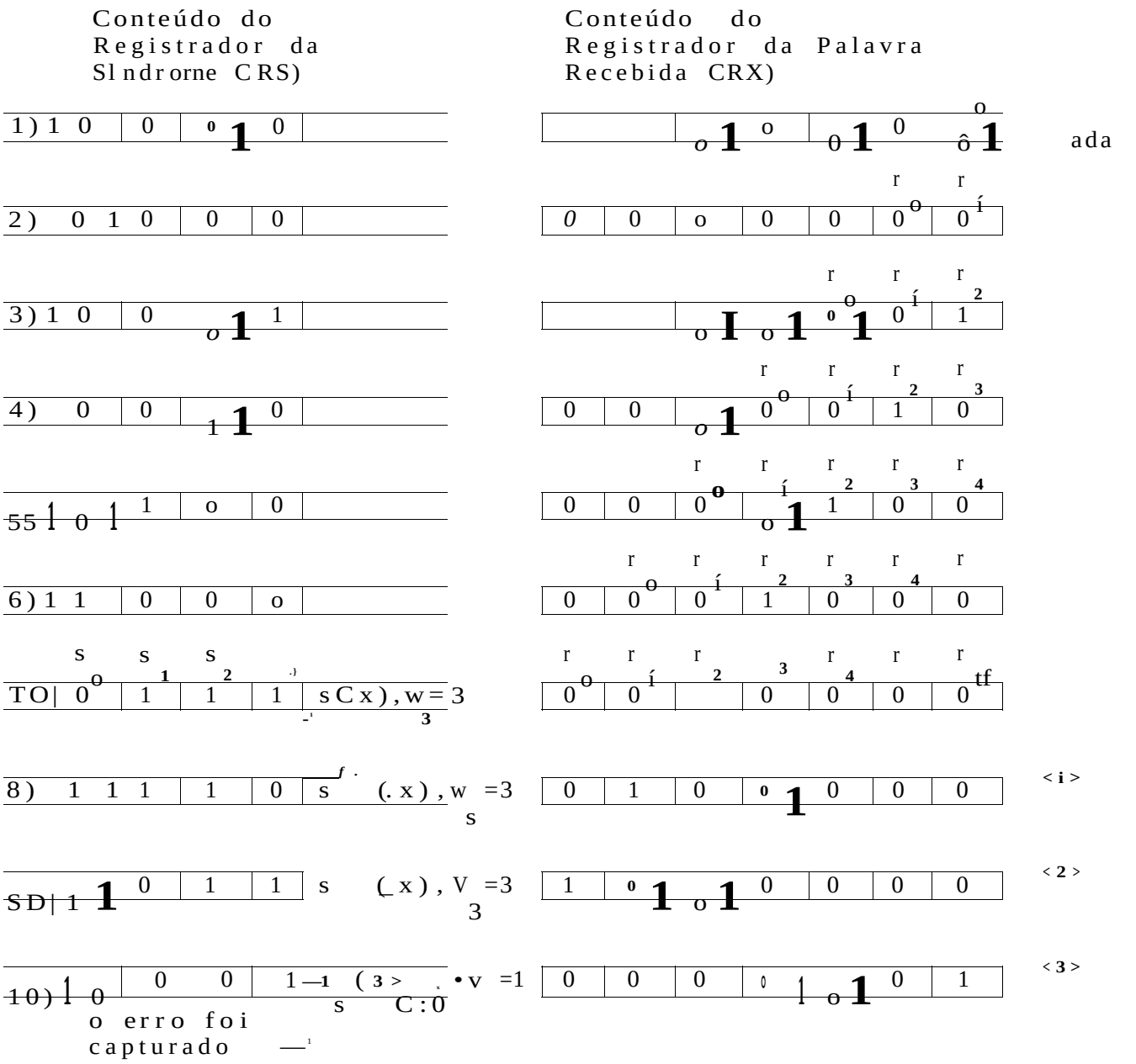
EXEMPLO 6.1 : Neste exemplo o decodificador será constituído basicamente de um registrador da palavra recebida CRX), um circuito com realimentação linear e seu registrador da síndrome CRSI> e um circuito feito com lógica combinacional para deteção do peso da síndrome Cse W < O. Será apenas mostrado o conteúdo dos registradores da palavra recebida e da síndrome. Será considerado o código binário C7.3.4) com polinómio gerador $gCx> = x^4 * x^2 \cdot x + 1$ portanto, t = 1. A palavra recebida foi r =C0, O, 1, O, O, O, O).

Na figura seguinte é mostrado o circuito para cálculo da síndrome



FIO. 6.2 - CIRCUITO COM REALIMENTAÇÃO LINEAR PARA CÁLCULO DA SI NDROME

Na página seguinte s3o mostrados os conteúdos dos registradores RS e RX durante todo o processo de decodifícação da palavra recebida.



Fia. 6. 3 - Conteúdo dos Reaistradcres RS e RX

No instante 10 o peso da síndrome é igual a um e o erro é capturado.

6. 2. DECODIFICAÇÃO POR ARMADILHA PARA ERROS SUAVES EM CÓDIGOS CICLICOS

Descreveremos um decodificador por armadilha para erros que usa eficientemente os níveis de saída do demodulador quantízados suavemente como parte integrante do processo de decodifi_ cação [193. Este decodificador opera com símbolos muitiníveis, que são elementos de um corpo de Galoís, usados para representar os níveis de saída do demodulador do sistema de comunicação.

6.2.1. QUANTIZAÇÃO DA SAÍDA DO CANAL

Em sistemas de comunicação, por razões práticas, frequentemente a tensão analógica na saida do demodulador é quantízada. É comum a escolha do número de níveis de quantízação como uma potência de 2, ou seja, q = 2™ para simplificar futuros processamentos digitais Tl73.

Assumiremos que os niveis de quantização estão igualmente espaçados e serão atribuídos aos mesmos valores inteiros de O a 2 - 1. Esta escolha provoca uma queda de desempenho porém e_._ **3**____v e atenuada quando oito ou **e** níveis de quantização são usados Í173.

Os elementos do corpo de Galois GFCq[m]} serão usados para representar os níveis de saída do demodulador Desta *forma* è necessário avaliar as implicações que tal atribuição tem sobre o conceito de distância suave.

6. 2. 2. DISTANCIA SUAVE

DEFINIÇÃO 6.1 A distância suave Cd 2 entre dois níveis é o valor absoluto da diferença entre eles.

A diferença entre dois elementos de *GFC2.[m]1>* coincide com sua distância suave quando um deles é uma m-tupla toda nula ou todas suas componentes são 1, ou seja, seus níveis são de máxima confiabilidade. Em geral a diferença entre um par de elementos do campo pode não coincidir com sua respectiva distância suave.

Entretanto, no processo de decodificação, as componentes da palavra recebida, que é quantizada suavemente, são comparadas com níveis de máxima confiabilidade das paiavras-códígo válidas. Portanto não é necessário que os niveis atribuídos à saída do demodulador sejam separados por distâncias de Hamming, que coincidam com suas correspondentes distâncias suaves.

A representação dos níveis de decisão-suave por elementos do corpo de Galois, permite integrar as informações de decisão - suave no processo de decodificação por armadilha para erros, como será mostrado a seguir.

6.2.3. CÓDIGOS CÍCLICOS SUAVES

Considere um código cíclico binário Cn.k.d), com polinómio gerador gCx) e comprimento $n = 2^m - 3$

DEFINIÇÃO 6.2 Um código cíclico suave de caracteristi_ca 2 é formado considerando como paiavras-códígo todas as ênuplas com símbolos em GFC2^m) que satisfazem as equações de verificação de paridade do código cíclico binário Cn,k,d). Resultando desta *forma* um ccnãiyt) c&uTyoS 2^{Tn}-ário Cn.k.d).

Num sistema de decisão - suave, com ausência de ruído, os níveis da palavra-código recebida devem ser de confiabilidade máxima, ou seja, m-tupias com todas as componentes iguais a zero ou um. Portanto a distância mínima entre paiavras-códígo válidas é agora

$$d_s = Cq - 1)\, d \qquad C6.7)$$

EXEMPLO 6.2 : Considere o código de repetição C3.1.3) cujo polinómio gerador *é* gCx) = $x^2 + x + 1$, então as paiavras-códi_go são CO.O.O) e Cl.1.1).

Vamos formar um código cíclico suave com caracter1sti_ca 2. com símbolos em GFC40. Os elementos de GFC4) podem ser representados por O, 1, a e a^2. Sendo a matriz de verificação de paridade

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Então o código cíclico suave será composto pelas paiavras-código CO. O. 05. Cl. 1. 1}. Ca. a. a5 e Ca², a². a²5.

Como as paiavras-código válidas são aquelas de máxima confiabilidade, ou sejam. CO, O, 05 e Ca², a², a²5 então a distância mínima entre as paiavras-código válidas é agora d = Cq-15d = 9.

O conceito de código cíclico suave é muito interessante porque ele fornece a estrutura necessária para o uso de propriedades de códigos lineares no contexto de decisão suave. Por exemplo, a decomposição do espaço das ênuplas quantizadas suavemente em classes laterais pode ser feita com um arranjo padrão suave, síndromes podem ser calculadas, etc. Entretanto nosso principal interesse ê com a decodifícação de códigos cíclicos usando armadilha para erros com decisão suave. Desta forma faremos o desenvolvimento teórico necessário através de lemas e teoremas.

LEMA 6. 1 Uma síndrome nula corresponde a uma palavra-códígo do código cíclico suave.

PROVA Pela definição todas as palavras - código do código cíclico suave satisfazem as equações de verificação de parida uc ^o.uigu o^nário e portanto são múltiplas do polinómio gerador gCx5.

LEMA 6. 2 Os m - 1 elementos a^i, 0 < í < m - 2. de GFC2^m5, são linearmente independentes e por combinação linear apenas geram elementos de peso suave < C2^m - 15/2. [193

6. 2. 4. ARRANJO PARA CÓDIGOS CÍCLICOS SUAVES CACS5

O ACS é um arranjo retangular com linhas e colunas. A sua primeira linha é formada com palavras código de confiabilidade máxima, começando com a ênupla toda nula. Assim, : palavra com todas as componentes iguais a zero e o líder Cda classe lateral5 da primeira linha Cclasse lateral5. O lider da segunda linha *é* uma paiavra-código suave, não usada anteriormente, de menor peso suave e o restante da linha é formado somando-se o seu 11der à paiavra-códi. go de confiabilidade máxima situada no topo da coluna correspondente, ou seja. imediatamente acima.

A terceira e sucessivas linhas são formadas de *maneira* semelhante, começando sempre com uma paiavra-código suave de menor peso suave que não tenha sido usada anteriormente.

TEOREMA 6.1 Os líderes do ACS tem peso suave $w_s < t_s + 1$ e portanto representam erros suaves corrigíveis.

PROVA Vamos supor que um líder L tem peso suave $w_s > t_s + 1$. Como a primeira linha do ACS possui apenas palavras código de peso suave $d_s > St_s + 1$, então existe pelo menos uma palavra-código suave de peso suave $< t_s$ na linha onde L é lider. Porém isto contradiz a regra de construção do ACS.

TEOREMA 6.2 Qualquer paiavra-código suave pode ser escrita como a soma, sobre GFC2^m), de uma palavra código suave de confiabilidade máxima e uma palavra código suave de peso $< t_s$.

PROVA Isto é uma imediata consequência da construção do ACS combinado com o resultado do teorema C6.1).

TEOREMA 6.3 O ACS tem $2^{(m-1)k}$ lideres que são compôstos de elementos com peso suave $< (2^m-1)/2$.

PROVA Pela definição, um código cíclico suave tem k posições de informação que são ocupadas pelos elementos de GFC2^m). Então, temos um total de 2^{mk} paiavras-códígo suaves. O ACS possue 2^k colunas e portanto $2^{mk}/2^k = 2^{(m-1)k}$ linhas, ou seja, $2^{(m-1)k}$ lideres. A segunda parte deste teorema é uma consequência da aplicação do Lema C6. 2) para códigos lineares.

TEOREMA 6. 4 Uma versão binária de decisão abrupta de uma paiavra-códigо suave recebida leva a uma paiavra-código correta apenas quando o padrão de erros suaves é corrigivel.

PROVA Conceituaimente, a decodifícação de uma paiavra-código suave v pode ser feita da seguinte maneira.

Primeiro localizamos a linha do ACS onde a palavra recebida v está localizada, então subtraimos o 1ider r, da linha, de v. O resultado é uma paiavra-código suave de máxima confiabilidade c *Como* d > 2t $_s^s$ 1 e pelo teorema C6. 22 e lema CB. 22, o líder r, tem peso suave < t « é único e pode ser assumido como sendo padrão de erros $_s$ suaves. Portanto, a paiavra-códigо binária mais próxima é uma versão por decisão abrupta de c.

6. 2. 5. ALGORITMO DE DECODIFICAÇÃO POR ARMADILHA PARA ERROS SUAVES

1— PASSO: Cálculo da síndrome suave sCx2

2— PASSO: Comparação do peso suave da síndrome W com t CW < t *?2 $_s$ $_s$ $_s$ $_s$ onde t **<** J_ d - 1/2 J e [x j é a parte inteira de x.

3— PASSO: Se W < t então uma versão da decisão abrupta da ênupla $_s$ $_s$ recebida é entregue ao destinatário, caso cada componente da síndrome tenha peso suave menor que q/2.

4— PASSO: Se W > t desloca-se o reqístrador da síndrome com as £ S realímentações ligadas para obter a nova síndrome s Cx2.

5— PASSO: Após o í-èsimo deslocamento compara-se o peso da síndrome obtida s$^{(l)}$Cx2 com t . $_s$

B— PASSO: Se para alqum i, l < i < n - l . W < t então um erro $_s$ $_s$ suave foi capturado e subtraí-se x^{l}s$^{(l)}$Cx2 de rCx2

7— PASSO: Se lima palavra de máxima confiabilidade foi obtida, i.e. . uma paiavra-código onde cada componente é toda nula ou toda um. então os erros foram corrigidos.

8— PASSO: Caso contrário, continue o processo de deslocamento comparando W com t

9— PASSO: Se após o enésimo deslocamento, nunca ocorreu que W < t , $_s$ $_s$ e se ocorreu a correção não levou a uma palavra código de máxima confiabilidade, então os erros não podem ser captu rado e são apenas detetados.

EXEMPLO 6.2 : Considere o código binário C7.3.45 com polinómio gerador gCx5 = $x^4 + x^2$ •+ x * 1. A saída do demodulador é quantizada em 8 níveis de amplitude, sendo cada nível representado por um elemento de GFC85, como mostrado abaixo.

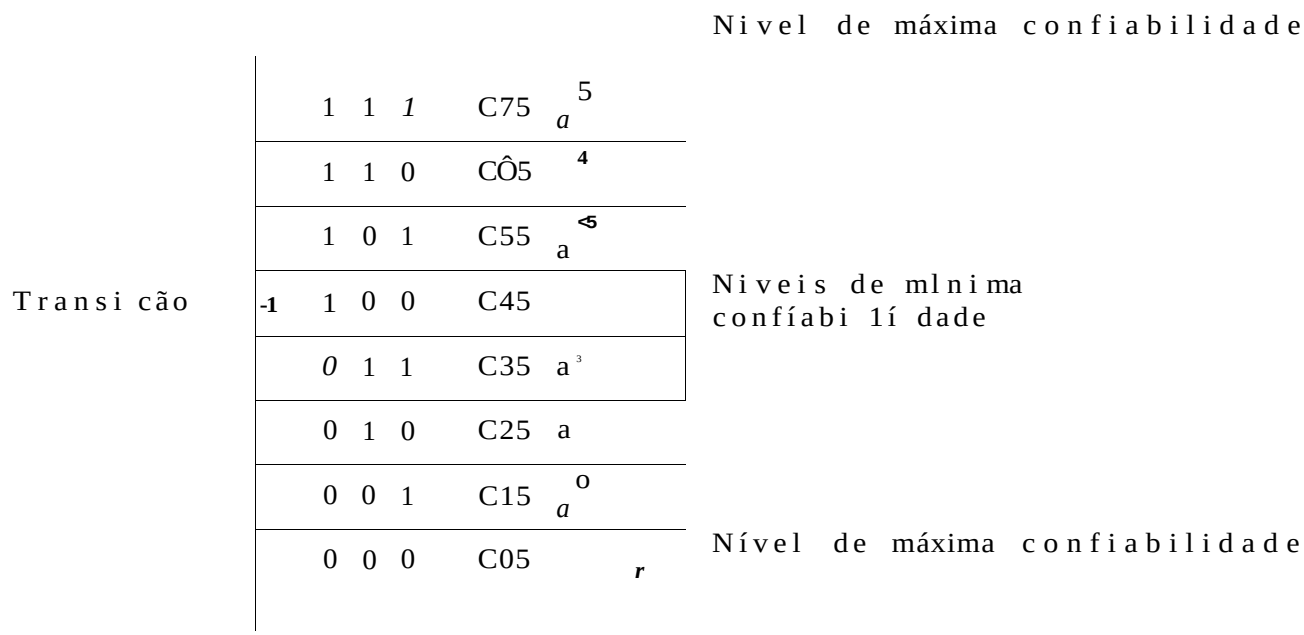


FIG. 6.4 - Níveis de Decisão Suave em GFC85

A distância suave do código é dada por d_{ε} = C8-154=28, portanto t =13. Vamos supor que a ênupla r = Ca ,0,0,a ,0,0,05 é recebi da.

A figura a seguir mostra o circuito usado neste exemplo para cálculo da síndrome suave.

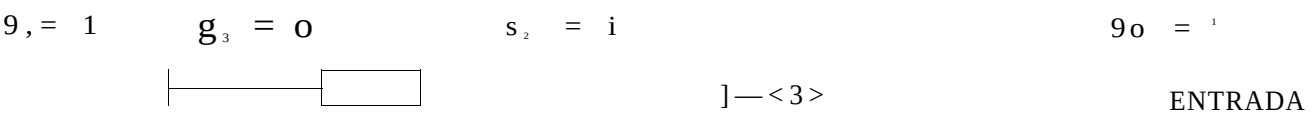


FIG. 6.5 - Circuito com Realimentação Linear para Cálculo da Síndrome Suave

O decodificador será constituído basicamente de um registrador da palavra recebida CRX) e um circuito para cálculo da síndrome com seu registrador da síndrome CRS).

Mostraremos em seguida no processo de decodificação da palavra recebida apenas o conteúdo do registrador da palavra recebi, da CRX) e do registrador da síndrome CRSO.

Inicialmente a palavra recebida é deslocada em RX e RS para o cálculo da síndrome com todas as realimentações ligadas Cpassos 1 a 7 na figura abaixo); no passo 7, a palavra recebida está totalmente contida em RX e sua síndrome em RS, porém $W_{\varepsilon} = 15 > 13$, desta *forma* é feito um novo deslocamento em RX e em RS com as realimentações ligadas. No passo 8, apesar de $W_s = 13$, podemos observar que o conteúdo de RS não é igual ao erro, portanto se somarmos o conteúdo de RS com as 4 posições de mais alta ordem de r^{*1} Cx) não obteremos uma palavra de confiabilidade máxima, portanto é necessário continuarmos a deslocar RX e RS.

No passo 11, = 13 e os erros foram capturados. e agora podemos corrigir a palavra recebida. Esta *correção* é feita somando-se o conteúdo do registrador da síndrome com a palavra recebida deslocada convenientemente como mostrado. Além disto deveio ,ar que. erros deste tipo não são corrigidos na versão de decodificação por armadilha para erros com decisão abrupta.

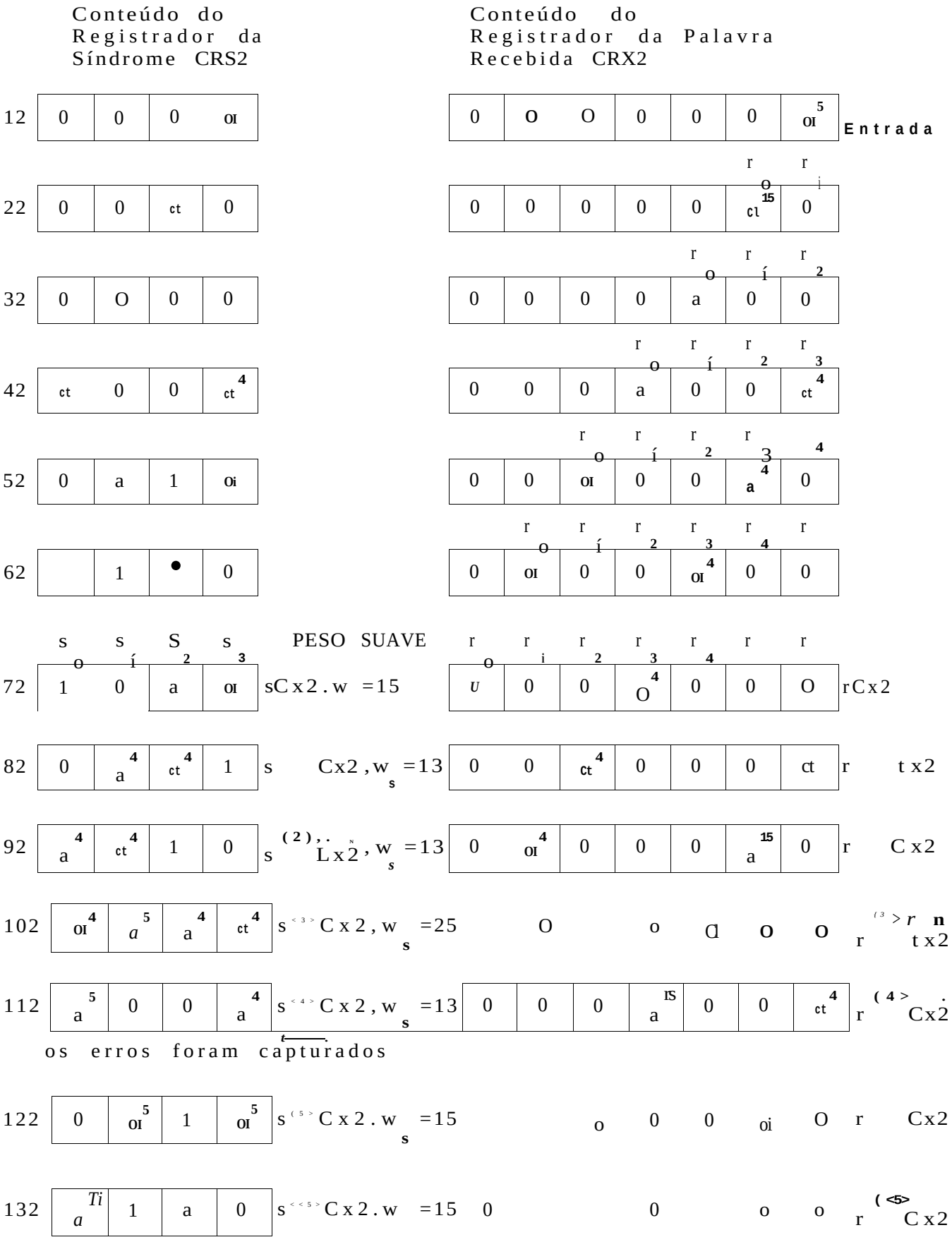


FIG. 6.6 - Conteúdo dos Registradores RS e RX

CAPITULO 7

CONCLUSÕES

Este trabalho apresentou de forma sistemática algumas propriedades dos códigos algébricos. Tais propriedades permitiram obter procedimentos para a construção de códigos, simplificação de alguns procedimentos de decodificação e melhoria no desempenho dos sistemas de comunicação digital através das técnicas de decisão suave na decodificação por armadilha de erros.

Nos três primeiros capítulos foi apresentada uma breve revisão dos códigos de bloco lineares, dos códigos cíclicos, com a intenção de dar o suporte necessário para a compreensão das propriedades e aplicações dos códigos algébricos.

No capitulo 4, baseado nas propriedades algébricas dos polinómios sobre um corpo de Galois GFCq), foi mostrado um procedimento sistemático para a construção de uma classe de códigos pseudocíclicos. Este capítulo é rico em exemplos que facilitam a *compreensão* dos principais teoremas e lemas utilizados. Na segunda parte deste capitulo foi mostrado como estes códigos podem ser decodificados por um procedimento algébrico. Para este fim, foi utilizada uma transformação afim que faz do código pseudocíclico um código cíclico equivalente num campo de extensão GFC q^m2>. Um aspecto interessante deste capítulo foi a geração de códigos MDS Cdistância máxima separáveis) pseudocíclicos. Estes códigos têm a vantagem de possuir algumas propriedades dos códigos cíclicos adequadas para codificação e decodificação.

No capítulo 5 foram apresentadas as principais propriedades algébricas dos códigos BCH. Os resultados obtidos mostram que o trabalho de decodificação é função do número de erros a serem detetados ou corrigidos. Isto implica por exemplo na redução da complexidade do processo de encontrar o polinómio localizador de erros, quando a correção de erros é realizada, reduz-se o número de passos e explora-se polinómios de graus menores.

No capitulo 6 o método de decodificação por armadilha para erros foi apresentado nas versões por decisão abrupta e por decisão suave. A segunda versão utilizou eficientemente os níveis de saída do demodulador, quantizados suavemente, como parte integrante do processo de decodifícação. Foi visto, por exemplo, que alguns erros não corrigidos pela versão por decisão abrupta são corrigidos pela versão de decisão suave.

Como sugestão para pesquisas futuras seria interessante estudar as propriedades apresentadas, principalmente a decodificação por armadilha para erros, no domínio da frequência, com o uso da transformada de Fouríer de campo finito.

Vale a pena mencionar que os tópicos tratados no capítulo 4 são de grande interesse atual [20-243 e certamente continuam a *merecer* a atenção daqueles que se dedicam à codificação algêbrica.

APÊNDICE

SÍNTESE DE REGISTRADORES DE DESLOCAMENTO

1. INTRODUÇÃO

Neste apêndice apresentamos um algoritmo e respectivo programa em linguagem BASIC para síntese do menor registrador de deslocamento com realimentação linear CLFSR2) que pode gerar uma dada sequência finita de dígitos £253. O algoritmo apresentado coincide com o algoritmo interativo introduzido por Berlekamp para decodificação de códigos BCH £153.

2. PROPRIEDADES DOS COMPRIMENTOS DOS LFSR's

Um registrador de deslocamento, com realímentação linear CLFSR2> geral de comprimento L ê mostrado na figura 1 e consiste de uma ligação em série de L células de retardo, ou armaze rjamerj/o-^, trom possibilidade c^ *formar uma* combinação linear dos seus conteúdos, que serve como entrada para seu primeiro estágio.

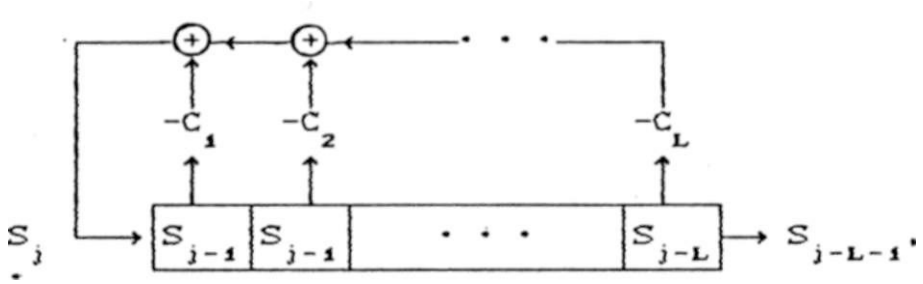


FIGURA 1

A saída do LFSR é assumida como sendo o conteúdo do último estágio. O conteúdo inicial $S_o, S_i, \ldots S_{L-1}$ dos L estágios coincide com as L primeiras saídas e os dígitos restantes da saída são unicamente determinados pela seguinte fórmula recursiva.

Os dígitos de salda e os coeficientes de realimentaçâo C , C , . . . C são considerados como pertencendo ao mesmo corpo F, o qual pode ser um corpo finito GFCq) ou um corpo infinito, tal como o corpo dos números reais. No nosso caso. trabalharemos em GFC2). Não é necessário que * O Cou seja. o último estágio do LFSR não precisa ser conectado).

Um LFSR é dito gerar uma sequência finita S^, S^. . . . S quando esta sequência coincide com as primeiras n saídas do LFSR para alguma condição inicial. Se L > N. o LFSR sempre gera a sequência. Se L < N. segue de Cl) que o LFSR gera a sequência se e apenas se:

$$S_j = \sum_{i=i}^{li} r_i S_{j-i} = 0 \qquad j = L.\ L+1 \ldots N-1 \ldots \text{C2)}$$

TEOREMA 01 [253 Se algum LFSR de comprimento L gera a sequência $S_0, S_1 \ldots S_{n-1}$, mas não gera a sequência $S_0, S_1 \ldots, S_{N-1}, S_N$, então qualquer LFSR que gera a última sequência tem comprimento L*. satisfazendo

$$L' > N + 1 - L \ldots \text{C3)}$$

LEMA 01 [253 Se algum LFSR de comprimento L^CS) gera $S_0 . S_1 \ldots S_{N-1}$ mas não gera $S_0 . S_1 \ldots S_{N-1}, S_N$ então

$$L_{N+1} Cs) > \text{máx } f\sim L_N Cs).\ N + 1 - L_N Cs)l$$

3. ALGORITMO PARA SÍNTESE DE LFSR's

Nesta etapa, demonstraremos um teorema que estabelecerá a validade do algoritmo de síntese.

TEOREMA Q2 . Se algum LFSR de comprimento L CS) que gera a sequência $S_0, S_1 \ldots S_{N-1}$, também gera $S_0 . S_1 \ldots S_{N-1}, S_N$, então: L Cs) = L Cs). Inversamente, se algum LFSR de comprimento L Cs) que gera $S_0, S_1 \ldots S_{n-1}$, não gera $S_0, S_1 \ldots S_{N-1}, S_N$ então

$$L_{N+1} Cs) = \text{máx } fL_N Cs).\ N + 1 - L_N Cs)]$$

PROVA : Definiremos o Polinómio de Conexão do LFSR da figura 1, como sendo o polinómio:

$$C(D) = 1 + C_1 D + C_2 D^2 + \ldots + C_L D^L \qquad (C4)$$

que possuí grau < L. Por convenção tomaremos C(D) = 1, para o LFSR de comprimento L = O.

Quando $S_0, S_1 \ldots S_{N-1}$ são todos zeros, mas $S_N \neq 0$, então L(S) = N + 1, desde que qualquer LFSR menor deve ser carregado inicialmente com zeros e então deve gerar apenas zeros. Além disso qualquer LFSR com L = N + 1 gera a sequência $S_0, S_1, \ldots, S_{N-1}, S_N$ neste caso.

Para um dado S, seja

$$C^{(N)}(D) = 1 + C_1^{(N)} D + \ldots + C_{L(S)}^{(N)} D^{N(S)} \qquad (C5)$$

O polinómio de conexão para o LFSR de mínimo comprimento L(S) que S_{N-1}. Por hipótese indutiva, vamos assumir que L(S) e $C^{(N)}(D)$ foram encontrados para N = 1, 2 ... n, com a igualdade obtida no Lema OI para N = 1, 2, ..., n-1. Tentaremos encontrar $L_{n+1}(S)$ e algum $C^{(n+1)}(D)$ e mostrar a igualdade obtida no Lema OI para N = n.

Pela hipótese indutiva, temos de C2) que

$$f(0, j) = L_n(S), \quad n-1$$

$$S_j + \sum_{i=1}^{L(S)} C_i^{(n)} S_{j-i} \qquad (C6)$$

$$d, \quad j = n$$

Se $d_n = 0$, então este LFSR também gera os primeiros n + 1 dígitos de S. Então $L_{n+1}(S) = L_n(S)$ e podemos escolher $C^{(n+1)}(D) = C^{(n)}(D)$.

Se d $\neq$ O, um novo LFSR deve ser encontrado para gerar os primeiros n + 1 dígitos de S. Neste caso seja m o comprimento de uma sequência antes da mudança de comprimento do registrador de comprimento mínimo, ou seja:

$$L(s^n) < L(s^m)$$
$$L(s^{n+1}) = L(s^m)$$

Desde que uma mudança de comprimento foi requerida, LFSR com polinómio de conexão $C^{(m)}(D)$ e comprimento $L(s^m)$ não pode gerar a sequência $S_0, S_1, \ldots S_{m-1}$. Portanto de C2) temos:

$$\Delta_j = L(s^n) - L(s^m) + 1 \quad j = 1, \ldots, m-1$$

$$L(s^j) = \sum_{i=1}^{m} C_i^{(m)} S_{j-i} \qquad \ldots\ldots C8)$$

$$\Delta_m = L(s^n) - L(s^m) \quad j = m$$

Pela hipótese indutiva, o Lema OI permanece válido com a igualdade para N = m. E itão

$$L(s^{m+1}) = L(s^n) = \max\left[L(s^m),\ m + 1 - L(s^m)\right]$$

Neste caso devido a equação C7) temos

$$L(s^n) = m + 1 - L(s^m) \qquad \ldots\ldots\ldots\ldots C9)$$

podemos dizer agora que o polinómio de conexão

$$C(D) = C^{(n)}(D) - d_n \cdot d_m^{-1} D^{n-m} C^{(m)}(D) \qquad \ldots\ldots\ldots C10)$$

é válido para escolha de $C^{(n+1)}(D)$. Podemos observar que o grau de C(D) será no máximo

$$\max[L(s^n),\ n - m + L(s^m)] = \max[L(s^n),\ n + i - L(s^n)]$$

Assim CCD) é um possível polinómio de conexão para o LFSR de comprimento L onde

= max f L Cs), n + 1 - L Cs) 1 CID

Além disso de CIO) temos que :

$$EC.s, \quad \text{« s . •»} \quad \sum_{1=1}^{I-(s>} {}^{c(n>} S_{j-t} \cdot - d\, d^{-1} \sum_{j-n+m}^{i.\,m(s>} E\, s$$

fO. J =L, L + 1, ... n - 1

d - d d d = 0 . j = n
Ti n m m

onde a última igualdade resulta de C6) e de C8)

Portanto, segue de C2) que o LFSR de comprimento L com polinómio de conexão CCD) gera os n + 1 dígitos S, S.....S , S .
o 1 n—1 ri
Desde que L satisfaz o Lema 01 com a igualdade, concluímos que L = L Cs) e portanto a igualdade do Lema OI é sempre obtida.
n

QED.

4. ALGORITMO PARA SÍNTESE DE LFSR

PASSO 1: CCD) = 1 BC D) =1 x = 1
L = 0 b = 1 N = 0

PASSO 2: Se N = n, pare. Caso contrário
faça d = S + £ C S
N t r»-v

PASSO 3: Se d = O. então faça x = x + 1 e vá para C6)

PASSO 4: Se d * O e 2L > N. então faça
CCD) = CCD) - d b D * BCD)
x • x * 1 e vá para C6)

PASSO S: Se d * O e 2L < N, então

TCD) = CCD) [TCD) armazena temporíariamente CCD)3

CCD) = CCD) - d.b⁻¹D* BCD)

L = N •+ 1 - L

b = d

x = 1

PASSO 6: N = N + 1 volte para C2)

5. PROGRAMA EM BASIC

```
0       REM SÍNTESE DE REGISTRADORES DE DESLOCAMENTO
1       DIM CDC100).BDC1OO).TDC100),SC1OO)
2       FOR 1=0 TO ÍOO
3       CDCI)=0
4       BDCI)=0
5       TDCI)=0
6       SCI)=0
7       NEXT I
e       INPUT "SAÍDA NA IMPRESSORA ? C1,0)"; PERG
IO      INPUT "N";NP
ii      IF PERG>0 THEN LPRINT " N = ⁴•;NP
15      FOR 1=0 TO NP-1
20      PRINT "SC";I;")=";
25      INPUT SCI)
26      IF PERG>0 THEN LPRINT "SC";I;")=";SCD
30      NEXT I
99      REM
100     CDC0)=1
ÍOI     PRINT "ETAPA 1"
102     IF PERG>0 THEN LPRINT "ETAPA 1"
105     BDCO)=1
110     X=l
115     L=0
120     B=l
125     N=0
199     REM
200     IF N=NP THEN STOP
```

```
201     PRINT "ETAPA 2"
202     IF PERG>0 THEN LPRINT "ETAPA 2"
205     D=SC YD
207     PRINT "SCND =*';SCN): PRINT "N=";N: PRINT "L=";L
208     IF PERG>0 THEN LPRINT "SCN2 =";SCN) ;" N=";N;" L=";L
210     FOR 1=1 TO L
215      B1=CDCI2*SCN-I2
220     B2=D
221     PRINT "B1=";B1; "B2=";B2
225     GOSUB lOOO
230     D=BO
232     PRINT "BO=0";BO
235     NEXT I
299     REM
300     IF NOT D=0 THEN GOTO 400
301     PRINT "ETAPA 3"
305     X=X+1
310     GOTO 600
399     REM
400     L2=2*L
40b"    IF L2<=N THEN GOTO £jO
406     PRINT "ETAPA 4"
407     IF PERG>0 THEN LPRINT "ETAPA 4"
410     DB=D/B
415     IF NOT DB=0 THEN GOSUB 2000
420     X=X+1: GOTO 600
499     REM
500     Nl=NP
501     PRINT "ETAPA 5"
502     IF PERG>0 THEN LPRINT "ETAPA 5"
505     FOR 1=0 TO Nl-1
510     TLX12 =CDC12 . NEXT I
520     DB=D/B
521     PRINT "D/B=";DB
525     IF NOT DB=0 THEN GOSUB 2000
530     L=N+1-L
535     FOR 1=0 TO Nl-1
540     BLXI2=TDCI2
```

542 NEXT I

543 FOR **1=0** TO Nl-1: PRINT **"BDC** "; I **;") = "; BDC** I): NEXT I

545 **B=D**

550 , P. (1962). The properties of decomposed granite. Geotechnique, vol. 12, 226-243.

599 REM

600 Lutenegger, *h.*J. and Saber, R.J. (1988). Determination of collapse potential of soils. Geot. Testing Journal,

601 PRINTASEE'/; V© 1*5 =TJC1K73*178.

602 **KSffarf,** J.P. (1980). Classification geothechnigue des sols

603 PRINT" a propos de la classification LPC. Bulletin de

605 p^^j^is.soji des LPC, No. 105, 49-52.

610 **HRrHalrB^pB** (1973). Mechanical properties of rockfill,

615 PRI lent Dam Engineering, 110-199, John Wiley & few York.

620 IF PERGX **=0.** GOTO. 665

622 LSeVf. J^B^, Irfan, T.Y., Cipullo, A. (1989). The charac-terfzatXon of granitic saprolitic soils. XII ICSMFE,

623 LPRI Ntfbl'CCfe,"; **333^543** CDC J)

624

625 ***PMQvioive,*** J. (1985). Stress paths for a compacted soil LPRIN$ur*ing collapse due toLw*tt|**.ng.** PhD Thesis, University

626

665 ^*Rt«Io;E3'APAnd' Nishida, K. (1968). Physical and chemical

666 » ^ « ^ « ? W (V o - a **2 o** " e soil grains - soils

ir PERGX **=0** THEN INPUT PARA

670 Matsuo, S. and Nishida, K. (1970). The properties of decomposed granite soils and their influence on

680 GOTO jafiJCmeability. Soils and Foundation, vol. 10, No. 1,

999 REM 93-105-

1OO0 B&t$as<-**B2** E.L. (1969). Engineering properties of sasumua

1010 IF **B0Sl**a^E?f'Bc**0**=7**0**th ICSMFE, Vol« 143-152, Mexico City.

1015 **ffle** ***WtklH, THSH*** ,B<F£fcnco Filho, J.M. and Alvise, C.R. (1988).

1030 RETUJ^outing of caniculae in residual sois and behavior of le foundations of Balbina dam. Proc. 2nd Int. Conf

2000 NN=X on Geomechanics in Tropical Soils, Vol. 1, 385-390,

2005 N2=NPs-**W**aPore-

2010 C©R MeFi&oTfO B2&L, Roase, M.M., and Porto, E.C. (1989).

2015 Bl =-rfei«^^T3ended PlPe Piles: testing and piling in calcar-eous sand. Proc. 21th Offshore Technology Conference.

2O20 B2=CDCI+NN)

2025 &E&DB'|&dtV and Ward, W.C- (1983). Eolian enviroment. In ***(ea.)*** Carbonate Depositional Enviroments. American

2O30 CDCI-**&6*HBIation of Petroleum geologists, Memoir 33, 132-

2035 NEXT I70*

2040 RETURN

EXEMPLO

N = 5

S = S . S, S . S . S = 10100
O 1 2 3 4

N = 3

S C O D = 1

S C I 2> = 0

S C 2) = 1

S C 3) = 0

S C 4) = 0

ETAPA 1

ETAPA 2

SCN> = 1 N=0 L=0

ETAPA 5

CC= 0) = 1

CC= 1) =-1

L = 1

D= 1 B= 1 x= 1

ETAPA 6

ETMTM 'ó ¹

SCN) = 0 N= 1 L=

ETAPA 4

CC= 0) = *1*

CC= 1) = O

CC= 2) = 0

L = 1

D=-l B= 1 X= 2

ETAPA 6

ETAPA 2

SCN> = 1 N= 2 L=

ETAPA

CC= 0) = 1

CC= 1) = 0

ETAPA 6
ETAPA 2
SCrO = 0 N= 3 L= 2
CC= O 2 = 1
CC= 1 2 = 0
CC= 2 >=--1
C O 3 2 = 0
CC= 4) = 0
L = 2
D= 0 B = 1 X= 2
ETAPA e
ETAPA 2
SCN> = 0 N= 4 L= 2
ETAPA 5
cc = O 2 = 1
CC= 1 2 = 0
CC= 2 2 = 0
CC= 3 > = 0
CC= 4 2 = 0
CC= 5 2 = 0
L = 3
D = - l B= -1 X = 1
ETAPA 6

"LFSR"

BIBLIOGRAFIA E REFERÊNCIAS

£13 - SHANNON, **C.**, "A Mathematical Theory of Communication", Bell systems tech. j. Vol. 27, Cpt.I). pp. 374-427, Cpt.II). pp. 623-656, 1948.

Ü23 - GALLAGER, R. G., "Information Theory and Reliable Communi. cation", John Wiley e Sons., Inc., 1968.

r33 - LIN, S. and COSTELLO, **D.**, Jr., "Error Control Coding Fundamentals and Applications", Prentice-Hall, 1983.

[43 - MACWILLIAMS, F. J. and SLOANE, N. J. A., "The Theory of Error - Correcting Codes". North-Hoi1and, 1986.

[53 - CAMPELLO **DE** SOUZA, R. **M.**, "Transform Techniques for Channel Coding". Ph. **D** Thesis. University of Manchester, U.K., 1983.

[63 - ROCHA Jr., V. **C.**, "Códigos Corretores de Erros", Minicurso -esentado no V Congresso Nacional da SBMAC, João Pessoa, PB, agosto. 1982.

£73 - CAMPELLO DE SOUZA. R. **M.**. "Decodifícação Probabilística de Códigos Lineares", Tese de Mestrado, Universidade Federal de Pernambuco, 1979.

[83 - OLIVEIRA. H. **M.**. "Técnicas de Decisão Suave", Tese de Mestrado, Universidade Federal de Pernambuco, 1983.

[93 - RUDOLPH, L. "Easily Implementend Error-Correction-Decoding", G. E. Report N~ **62MCDe.** General Eletric Corporation. Oklahoma City. Okla., December **1962.**

[103 - PETERSON. W. W and WELDON. E. J. Jr., "Error-Correct!ng Codes". 2nd Ed. MIT Press. 1972.

£113 - KASAMI, T., "A Decoding Method for Multipie-Error-Correcting Cyclic Codes by Using Threshold", Conv. Rec. Inf. Process. Soc. Jap., Tokyo, November 1961.

[123 - MITCHELL, M. E. et al., "Coding and Decoding Operation Research", G. E. Advanced Electronics Final Report on Contract AF 19 06042-6183,, Air Force Cambridge Research Labs., Cambridge, Mass., 1961.

£133 - MITCHELL, M. E.. "Error-Trap Decoding of Cyclic Codes", G. E. Report N— 62MCD3, General Eletric Military Communications Dep., Oklahoma City, Okla., December 1

[143 - ROCHA Jr., V. C.; CAMPELLO DE SOUZA. R.M. and FARRELL, P. G.. "Multilevel Pseudocyclic Codes", J. Inf. Optim. Sci. Vol. 11, Nº 1, 1990, pp. 101-106.

£153 - BERLEKAMP, E. R.. "Algebraic Coding Theory", McGraw - Hill, New York, 1968.

[IJJ - /w-A-riA Jr., V. C., "Algebraic Decoding of CIass of Multi1evel Pseudocyclic Codes", Electronics Letters, 2nd March, Vol.25. N- 5, 1989. pp. 341 -342.

£173 - CLARK, G. C.. Jr and CAIN, J.B., "Error-Correction Coding for Digital Communications", PIenurn Press. 1981.

£183 - ROCHA Jr.. V. C.; HONARY, B. K. and BATE, S.. "Algebraic Properties of B.C.H. Codes' Useful for Decoding", International Journal of Satellite Communications, Vol. 7, N- 3, 989. pp. 225-229.

£193 - ROCHA Jr., V. C.. "Soft Error-Trapping Decoding of Cyclic Codes", Electronics Letters. February, Vol.25, N~ 4, 1989, pp. 293-294.

£203 - DÜR. A., "The Automorphism Groups of Reed-Solomon Codes", Journal of Combinatorial Theory. Series A. Vol. 44, 1987. pp. 69-82.

£213 - DOR, A.. "On Linear MDS Codes of Length q+1 over GFCqD for Even q". Journal of Combinatorial Theory, Series A, Vol. 49. 1988. pp. 172-174.

£223 - DAHL. C. AND PEDERSEN, J.P.. "Cyclic and Pseudo-Cyclic MDS Codes of length q+1", J. Comb. Theory, Serie A, to appear.

£233 - DAHL, C. AND PEDERSEN. J.P., "Classification of Pseudo-Cyclic MDS Codes". IEEE Trans. IT. to appear.

£243 - KRISHMA, A. AND SARWAATE. D.. "Pseudocyclic Maximum-Distance-Separable Codes". IEEE Trans. IT. to appear, July 1990.

£253 - MASSEY, J. L.. "Shift - Register Synthesis and BCH Decoding". IEEE Trans., Vol. IT - 15 N~ 1. JANUARY 1969, pp. 122-127.

£263 JR.. V. C., "Maximum Distance Separable 'jltilevel Codes", IEEE Transactions Information Theory. Vol. IT-30. N- 3. 1984. pp. 547-548.

£273 - BIRKHOFF. G. and MACLANE. S.. "A Survey of Modern Algebra". Macmillan. 1977.

£283 - ROCHA Jr.. V. C.. "A Class of Multilevel Error-Correct!ng Codes". Int. J. Electronics. Vol.51. N~ 6. 825-829. 1981.

£293 - THOMAS, S., "A Linear Complexity Approach to Cyclic Codes". Tese de Doutorado. Swiss Federal Institute of Technology, Zuerich. 1988.