DECODIFICAÇÃO ALGÉBRICA DE UMA CLASSE DE CÓDIGOS MULTINIVEIS PSEUDOCÍCLICOS

Valdemar Cardoso da Rocha Júnior

Departamento de Eletrônica e Sistemas - UFPE
Cidade Universitária 50.741, Recife-PE

R E S U M O

A decodificação algébrica de uma classe de códigos multiníveis pseudocíclicos é apresentada. A transformada de Fourier de campo finito é a ferramenta empregada, em conjunto com uma permutação afim. A permutação afim empregada não preserva o código original porém mapeia-o em um código equivalente, cíclico em um campo de extensão.

INTRODUÇÃO

Em 1984 Rocha [1] introduziu uma classe de códigos multiníveis pseudocíclicos e de distância máxima separável (MDS). O interesse em códigos MDS advém do fato de possuirem o maior valor possível de distância mínima, para valores fixados de comprimento e número de dígitos de informação. Para códigos lineares, estes parâmetros são relacionados pela cota de Singleton [2] $d \leq n - k + 1$, onde d é a distância mínima, n o comprimento e k o número de dígitos de informação do código. Códigos MDS satisfazem a cota de Singleton com igualdade. Códigos MDS pseudocíclicos tem a vantagem adicional de possuirem algumas das propriedades de códigos cíclicos, úteis para a codificação e a decodificação [3]. Posteriormente este trabalho foi extendido [5] e generalizado para códigos multiníveis pseudocíclicos , não necessariamente do tipo MDS. A decodificação algébrica desta família de códigos é o objeto do presente texto.

CÓDIGOS MULTINÍVEIS PSEUDOCÍCLICOS

Nesta seção é apresentado um resumo da teoria dos códigos multiníveis pseudocíclicos. Maiores detalhes podem ser obtidos nas referências [1], [3], [4] e [5].

Os códigos considerados tem os seguintes parâmetros:

Comprimento do bloco : $n = (q^m - 1)/r$, onde $q = p^s$,

p um número primo e
r, s e m são inteiros.

Número de dígitos de informação : k

Distância mínima : $d \leq n - k + 1$

O polinômio gerador g(x) destes códigos é um fator de $x^n - b$, onde a ordem de b divide r, $b \neq 0$, $b \in GF(q)$. O polinômio $x^n - b$ é caracterizado por suas raízes, pertencentes a um campo de Galois $GF(q^m)$, cujos expoentes são assim representados:

$e + ir$, onde $0 \leq i \leq n - 1$, $\alpha^{en} = b$, $0 \leq e \leq r - 1$

O ponto a ser enfatizado é que, a fim de garantir uma distância mínima d para o código, g(x) deve ser o mínimo múltiplo comum dos polinômios mínimos de d-1 raízes cujos expoentes formam uma progressão aritmética.

O termo "raízes consecutivas" será usado com o significado de que entre duas delas, $e + ir$ e $e + (i + 1)r$, por exemplo, não haverá nenhuma outra raiz de $x^n - b$.

DECODIFICAÇÃO ALGÉBRICA

O desenvolvimento apresentado a seguir explora com vantagem a estrutura matemática dos códigos pseudocíclicos.

Para poder empregar corretamente a transformada de Fourier de campo finito (TFCF) [6], faz-se necessária a utilização de um núcleo que tenha ordem n. Como as raízes de g(x), em princípio, não contêm nenhum elemento de ordem n, com exceção do caso em que $b = 1$, o cálculo da síndrome não corresponderia a uma transformada com inversa. Daí foi necessário utilizar uma permutação afim [3] para resolver esta dificuldade.

O lema a seguir estabelece as condições que devem ser satisfeitas pela transformação afim.

LEMA 1.

Sendo $\alpha^{(e+ir)}$, $a \leq i \leq a + d - 2$, $0 \leq a \leq n - 1$, as raízes consecutivas do polinômio gerador g(x), a permutação afim $x = \alpha^{(e+ur)} y$, $0 \leq u \leq d - 2$, transforma o código pseudocíclico em um código cíclico equivalente, sendo α primitivo em $GF(q^m)$.

PROVA.

A substituição de $x = \alpha^{(e+ur)} y$ em $x^n - b$ dá como resultado:

$$\alpha^{n(e+ur)} y^n - b = \alpha^{ne} y^n - b \quad \ldots\ldots\ldots (1)$$

visto que $\alpha^{nr} = 1$ e como $\alpha^{ne} = b$ [5], então (1) pode ser escrito como :

$$by^n - b = b(y^n - 1) \quad \ldots\ldots\ldots\ldots\ldots (2)$$

Obviamente $y^n - 1$ dá origem a códigos estritamente cíclicos, porém sobre GF(q^m) e não sobre GF(q). As raízes de $y^n - 1$ tem ordens que dividem n [3], sendo facilmente obtidas a partir das raízes de $x^n - b$ e da transformação afim empregada, tendo como expoentes (i - u)r, onde u é um parâmetro $0 \leq u \leq d - 2$, e i é variável, $a \leq i \leq a + d - 2$.

Obviamente, o código cíclico obtido por meio da transformação afim é equivalente ao código pseudocíclico original, ambos tem portanto os mesmos parâmetros e também a mesma distância mínima d. C.Q.D.

Um valor conveniente para u é aquele que mapeia os expoentes das raízes de g(x) em 0, r, 2r, ...,(d - 2)r. Observar que tal escolha é sempre possível, por serem consecutivas d-1 raízes de g(x) e devido à estrutura pseudo cíclica.

Após a aplicação da permutação afim, a decodificação algébrica se processa de forma exatamente idêntica à que é usada para códigos BCH [7]. A seguir é apresentada uma descrição dos passos que constituem o algorítmo.

Algorítmo de Decodificação

Seja f(x) o polinômio que representa a soma do polinômio mensagem v(x) e do polinômio erro e(x). Aplica-se a transformação afim em f(x), gerando assim

$$f(y) = v(y) + e(y)$$

1. Cálculo do polinômio síndrome S(z)

$$S(z) = \sum_{i=0}^{d-2} S_i z^i$$

onde $S_i = f(\alpha^{ir})$, $0 \leq i \leq d - 2$

como f(y) = v(y) + e(y), então resulta :

$S_i = v(\alpha^{ir}) + e(\alpha^{ir}) = e(\alpha^{ir})$, visto que $v(\alpha^{ir}) = 0$

Lembrar que $S_j = E_j$, $0 \leq j \leq d - 2$

onde $E = (E_0, E_1, E_2, \ldots, E_j, \ldots, E_{n-1})$ representa a TFCF do vetor erro.

2. Cálculo do polinômio localizador de erros L(z)

Aplicar o algorítmo de Euclides ao par de polinômios z^{2t} e S(z). Lembrar que S(z) é do grau

$$d - 2 = 2t + 1 - 2 = 2t - 1$$

Parar quando o grau do polinômio resto for menor que t [7]. As localizações dos erros, na palavra recebida, são indicadas pelos expoentes dos valores recíprocos das raízes de L(z).

3. Determinar o vetor E associado ao polinômio E(z), que representa a TFCF do vetor erro e, associado ao polinômio e(x), por extensão recursiva a partir de L(z) e S(z) [7].

4. Calcular a TFCF inversa de E(z) a fim de determinar e(y).

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

$$e_i = \frac{1}{n(\text{mod } p)} \sum_{j=0}^{n-1} E_j \alpha^{-rij}, \text{ porém } n(\text{mod } p) = (p-1)/r,$$

então resulta $e_i = \sum_{j=0}^{n-1} E_j \alpha^{-rij} r/(p-1)$

5. Aplicar a transformação afim inversa para obter e(x).

6. Efetuar a correção dos erros subtraindo e(x) de f(x)

$$v(x) = f(x) - e(x)$$

EXEMPLO

Considere o código pseudocíclico (6,2,5), com 5 níveis, i.e., p = 5, s = 1, obtido a partir da fatoração de $x^6 - 2$. As raízes de $x^6 - 2$ estão contidas em GF(25) e tem expoentes $1 + 4i$, $0 \leq i \leq 5$. Estas raízes podem ser agrupadas em pares conjugados, que correspondem a polinômios do segundo grau, do seguinte modo:

RAÍZES		POLINÔMIO MÍNIMO
(α, α^5)	.....	$x^2 + 4x + 2$
(α^9, α^{21})	.....	$x^2 + 2$
$(\alpha^{13}, \alpha^{17})$	.....	$x^2 + x + 2$

Neste exemplo será empregado o polinômio gerador g(x), mostrado abaixo, com quatro raízes consecutivas α^{21}, α, α^5, α^9, portanto com d = 5.

$$(x^2 + 4x + 2)(x^2 + 2) = x^4 + 4x^3 + 4x^2 + 3x + 4 = g(x)$$

A obtenção de cada polinômio mínimo, a partir de suas respectivas raízes, foi feita com o auxílio de uma tabela com os elementos de GF(25), a qual é apresentada no APÊNDICE.

Seja $f(x) = 3x^5 + x$ o polinômio recebido.

A transformação afim, a ser utilizada, é dada por $x = \alpha^{21} y$. As raízes de g(y) tem portanto os expoentes 0, 4, 8 e 12. Daí resulta :

$$f(y) = 3(\alpha^{21}y)^5 + \alpha^{21}y = \alpha^3 y^5 + \alpha^{21} y$$

1. Cálculo do polinômio síndrome S(z)

$S_0 = f(1) = 4\alpha^3 = \alpha^{15}$

$S_1 = f(\alpha^4) = \alpha^{16}$

$S_2 = f(\alpha^8) = \alpha^8$

$S_3 = f(\alpha^{12}) = \alpha^3$

$S(z) = \alpha^3 z^3 + \alpha^8 z^2 + \alpha^{16} z + \alpha^{15}$

2. Cálculo do polinômio localizador de erros L(z)
(consultar a referência [7])

L(z)	$r_i(z)$	$q_i(z)$
0	z^4	-
1	$\alpha^3 z^3 + \alpha^8 z^2 + \alpha^{16} z + \alpha^{15}$	-
$-(\alpha^{21} z + \alpha^{14})$	$\alpha^{12} z^2 + \alpha^{12} z + \alpha^{17}$	$\alpha^{21} z + \alpha^{14}$
$1 + (\alpha^{21} z + \alpha^{14})(\alpha^{15} z + \alpha^4)$	$\alpha^{20} z + \alpha^{16}$	$\alpha^{15} z + \alpha^4$

$$L(z) = 1 + (\alpha^{21} z + \alpha^{14})(\alpha^{15} z + \alpha^4) = 4z^2 + z + 4$$

3. Cálculo do vetor E.

$\sum_{i=0}^{2} E_{j-i}L_i = 0$, i.e., $E_{j-2}L_2+E_{j-1}L_1+E_jL_0 = 0$

Como os E_i, $0 \leq i \leq d-2$, já são conhecidos do cálculo da síndrome, resta apenas calcular E_4 e E_5.

$4E_4 + E_3 + 4E_2 = 0$, ou seja $E_4 = E_3 + 4E_2 = \alpha^4$

$4E_5 + E_4 + 4E_3 = 0$, ou seja $E_5 = E_4 + 4E_3 = \alpha^{20}$

Portanto, $E = (\alpha^{15}, \alpha^{16}, \alpha^8, \alpha^3, \alpha^4, \alpha^{20})$ é a TFCE do vetor erro associado a e(y).

4. A transformada inversa de E [6] é dada por

$$e_i = \frac{1}{n(\text{mod } p)} \sum_{j=0}^{n-1} E_j a^{-ij}$$

onde a é um elemento de ordem n. Será usado $a = \alpha^4$ como núcleo da transformação, lembrando que $6 \equiv 1$ módulo 5.

$$e_i = \sum_{j=0}^{5} E_j \alpha^{-4ij}$$

Resulta

$e = (0, \alpha^{21}, 0, 0, 0, \alpha^3)$, i.e.,

$e(y) = \alpha^3 y^5 + \alpha^{21} y = \alpha^3(\alpha^3 x)^5 + \alpha^{21}(\alpha^3 x)$

Aplicando a transformação inversa $y = x/\alpha^{21} = \alpha^3 x$, obtém-se :

$e(x) = 3x^5 + x$

Finalmente,

$v(x) = r(x) - e(x) = 0$

COMENTÁRIOS

Este trabalho demonstrou que códigos pseudocíclicos multiníveis podem ser decodificados por um procedimento algébrico. O passo fundamental, que permitiu o uso da decodificação algébrica, foi o emprego de uma transformação afim aplicada ao código pseudocíclico. Como resultado da aplicação da transformação afim, foi obtido um código cíclico sobre $GF(q^m)$. Uma vez obtido um código estritamente cíclico, o método clássico de decodificação algébrica é de aplicação imediata. Este procedimento oferece uma alternativa interessante para decodificar os códigos negacíclicos [8] introduzidos por Berlekamp.

Embora outros procedimentos de decodificação existam como, por exemplo, busca exaustiva, conjuntos de informação, armadilha para erros, etc. [3], [7], [9], as técnicas algébricas para decodificar códigos de bloco despontam como talvez as mais eficientes, quando códigos com $t \geq 2$ são usados.

AGRADECIMENTOS

Este trabalho recebeu apoio parcial do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

APÊNDICE

Transformação Afim

Uma transformação afim, com parâmetros a e b, $a \neq 0$, a e b sendo elementos de $GF(q^m)$, é uma permutação que muda um símbolo da posição x para a posição $z = ax+b$. A permutação afim usada neste trabalho é do tipo $z = ax$, isto é, com $b = 0$.

Tabela de elementos de GF(25), módulo $p(x)=x^4+4x+2$

0	$\alpha^5=4\alpha+1$	$\alpha^{11}=3\alpha+2$	$\alpha^{17}=\alpha+4$	$\alpha^{23}=2\alpha+3$
1	$\alpha^6=2$	$\alpha^{12}=4$	$\alpha^{18}=3$	
α	$\alpha^7=2\alpha$	$\alpha^{13}=4\alpha$	$\alpha^{19}=3\alpha$	
$\alpha^2=\alpha+3$	$\alpha^8=2\alpha+1$	$\alpha^{14}=4\alpha+2$	$\alpha^{20}=3\alpha+4$	
$\alpha^3=4\alpha+3$	$\alpha^9=3\alpha+1$	$\alpha^{15}=\alpha+2$	$\alpha^{21}=2\alpha+4$	
$\alpha^4=2\alpha+2$	$\alpha^{10}=4\alpha+4$	$\alpha^{16}=3\alpha+3$	$\alpha^{22}=\alpha+1$	

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Rocha,V.C.Jr., "Maximum Distance Separable Multilevel Codes", IEEE Trans. on Info.Th., VolIT-30 , Nº 3, pp. 547-548, May 1984.

[2] MacWilliams, F.J. & Sloane, N.J.A., The Theory of Error-Correcting Codes, North-Holland, 1977.

[3] Peterson, W.W. & Weldon, E.J., Error Correcting Codes, MIT Press, segunda edição, 1972.

[4] Rocha, V.C.Jr., "Multilevel Double-Error-Correcting Codes", Elect. Lett., Vol 17, pp. 45-46, Jan. 1981.

[5] Rocha, V.C.Jr. et alii, "Multilevel Pseudocyclic Codes", Journal of Information and Optimization Sciences (no prelo).

[6] Blahut, R.E., "Transform Techniques for Error Control Codes", IBM J. Res. Develop., Vol. 23, Nº 3, pp. 299-315, May 1979.

[7] Clark, G.C. & Cain, J.B., "Error-Correction Coding for Digital Communications", Plenum Press, New York, 1981.

[8] Berlekamp, E.R., "Algebraic Coding Theory", McGraw Hill, 1968.

[9] Wei, V.K., "An Error-Trapping Decoder for Nonbinary Cyclic Codes", IEEE Trans. on Info. Th., Vol. IT-30, Nº 3, pp. 538-541, May 1984.