ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
DEPARTAMENTO DE ENGENHARIA ELETRÔNICA
LABORATÓRIO DE COMUNICAÇÕES E SINAIS

PEE - 5869
TEORIA BÁSICA E APLICAÇÕES DAS SEQÜÊNCIAS DE CÓDIGOS

(Notas de aulas sobre: "Seqüências Binárias: Princípios Gerais e Características", baseadas na dissertação de mestrado: "Seqüências de Códigos para uso em Comunicação por Espalhamento Espectral", de Angel A. G. Martinez, submetido à EPUSP-PEE, Área de Sistemas Eletrônicos, defendida em 3/97 sob orientação do prof. P. J. E. Jeszensky)

DR. PAUL JEAN ETIENNE JESZENSKY
PROFESSOR ASSOCIADO
10/98

1-ALGUMAS DEFINIÇÕES E PROPRIEDADES BÁSICAS

As seqüências binárias, também chamadas de palavras código ou apenas de códigos, são vetores de comprimento fixo, sendo que o comprimento é igual ao número de elementos do vetor e será denotado por N. Os elementos do código pertencem a um conjunto de q elementos denominado de alfabeto. Quando o alfabeto consiste de dois elementos apenas, o código é denominado binário e cada um de seus elementos é chamado de bit. Os códigos construídos com os elementos de um alfabeto que possua mais que dois elementos são classificados como códigos não binários. Quando um código não binário é construído de um alfabeto, onde o número de elementos é uma potência de dois, $q=2^b$ com b um inteiro positivo, cada elemento do código tem uma representação binária equivalente, consistindo de b bits. Assim um código não binário de N elementos pode ser mapeado por um código binário de (bN) bits.

Numa palavra código binário de comprimento N podem ser obtidas 2^N palavras distintas e, generalizando, para um alfabeto de q elementos podem ser obtidas q^N palavras distintas.

Um parâmetro importante relacionado às seqüências é o peso Hamming que mede o número de elementos não nulos numa seqüência e será denotado por wH(.). Assim num alfabeto binário o peso Hamming coincide com o número de uns na seqüência, no entanto se o alfabeto for não binário o peso Hamming será calculado através da subtração do número de elementos nulos do número total de elementos

Uma forma de comparação entre duas seqüências é a denominada distância Hamming dH(.,.), que mede a diferença entre duas seqüências pelo número de elementos, ou posições, divergentes entre as mesmas. Este parâmetro está intimamente relacionado com a função de correlação cruzada periódica, que será um dos principais fatores de comparação entre códigos.

As operações aritméticas utilizadas em códigos binários, são realizadas conforme as convenções da Álgebra de Corpos Matemáticos (Álgebra Abstrata), em particular as de

maior interesse são as do Corpo de Galois (Galois Field), denotado por GF(.). As operações entre os elementos de um código binário são as abaixo descritas:

Adição			**Multiplicação**		
+	0	1	x	0	1
0	0	1	0	0	0
1	1	0	1	0	1

A tabela da adição também pode ser obtida por adição mod2. As seqüências tratadas a seguir serão sempre as binárias, consequentemente o conhecimento destas operações é fundamental.

As seqüências binárias serão representadas por um vetor $\vec{x} = \{x_0, x_1, \ldots, x_{N-1}\}$, com $x_i \in$ {0,1} ou {-1,+1} conforme o caso, para i variando de 0 até N-1 onde N é o comprimento da seqüência. Quando os elementos da seqüência forem +1 ou -1, a seqüência é dita polarizada e a polarização se dá através da seguinte equivalência: $1 \leftrightarrow -1$ e $0 \leftrightarrow +1$.

O produto escalar de duas seqüências x e y é definido por $\langle x, y \rangle = x_0.y_0 + \ldots.. + x_{N-1}.y_{N-1}$,. A norma de x, denotada por $\|x\|$, é a raiz quadrada positiva do produto escalar $\langle x, x \rangle$.

Será usado um operador T^k para indicar um deslocamento cíclico de uma seqüência. O expoente k de T, indicará o número de deslocamentos ocorridos sobre a seqüência original; se este é positivo o deslocamento é para a esquerda e se negativo para a direita. Assim, por exemplo, $T^2x = \{x_2, x_3, \ldots.., x_{N-1}, x_0, x_1\}$, representa o deslocamento cíclico da seqüência *x* duas casas para a esquerda e com isso as componentes que estavam no início passaram para o final.

O período de uma seqüência x, é definido como sendo o menor inteiro positivo M, tal que $T^M x = x$. Na maioria dos casos de interesse o valor de M é igual ao de N, apesar de M poder ser um divisor de N. Embora as seqüências $T^i x$, $T^j x$ sejam distintas, para i e j diferentes entre 0 e N-1, elas são denominadas de ciclicamente equivalentes, dada a sua origem comum. Este fato é importante, pois os sinais que chegam a um receptor num sistema

CDMA assíncrono, possuem uma defasagem aleatória sobre a qual não há controle, em princípio. Assim a recepção de dois sinais com seqüências ciclicamente equivalentes poderia eventualmente ser confundida no receptor (já em sistemas síncronos aquelas seqüências poderiam ser consideradas distintas). Estes deslocamentos são também denominados de fases da seqüência. Assim uma seqüência de período N possue N fases distintas.

Dada uma seqüência $x = \{x_0, x_1, ..., x_{N-1}\}$, denomina-se seqüência reversa (inversa ou ainda recíproca) de x à seqüência $w = \{x_{N-1}, x_{N-2}, ..., x_1, x_0\}$, isto é, onde o elemento $w_i = x_{N-1-i}$ para $0 \le i \le N-1$. Para um dado deslocamento da fase da seqüência w, pode-se calcular a fase correspondente da seqüência x através da seguinte fórmula:

$$(T^k w)_i = (T^{-k} x)_{N-1-i} = (T^{N-k} x)_{N-1-i} \qquad (01)$$

onde o índice externo ao parênteses, na expressão (01), refere-se ao i-ésimo elemento da seqüência $T^k w$.

Uma seqüência y é denominada de uma decimação q, q inteiro, de uma seqüência x, quando cada elemento de y é tomado de q em q elementos de x, de forma cíclica. Assim:

$$x = \{x_0, x_1, \ldots, x_{N-1}\} \qquad (02)$$

y será igual a:

$$y = \{x_0, x_q, x_{2q}, \ldots, x_{((N-1).q)}\} \qquad (03)$$

onde os índices de y são modN; portanto (N-1)q modN=N-q, isto é, $y_{N-1} = x_{N-q}$.

Denota-se esta decimação por y=x[q], indicando que a seqüência y é obtida por decimação q da seqüência x, com q inteiro.

Dadas duas seqüências x e y de comprimento igual a N, define-se como função de correlação cruzada periódica discreta à função $\theta_{x,y}(\ell)$ dada por:

$$\theta_{x,y}(\ell) = \langle x, T^{\ell} y \rangle, \quad \ell \in Z \tag{04}$$

De forma equivalente escreve-se a mesma equação para as duas seqüências

$$\theta_{x,y}(\ell) = \sum_{i=0}^{N-1} x_i . y_{i+\ell}, \qquad \ell \in Z \tag{05}$$

onde, por definição $y_{i+\ell} = y_{(i+\ell) \bmod N}$

Aplicando a desigualdade de Cauchy $|\langle x, y \rangle| \leq \|x\| . \|y\|$, tem-se:

$$|\theta_{x,y}(\ell)| \leq \|x\| . \|T^{\ell} y\| \leq \|x\| . \|y\| \tag{06}$$

A notação $\theta_{x,y}$ será indistintamente representada ainda por $\theta(x, y)$, apenas por uma questão de conveniência. Duas seqüências x e y são ditas não correlacionadas, ou ortogonais, se $\theta(x, y)(\ell) = 0$ para todo ℓ.

Apenas com estas definições pode-se provar ainda as seguintes relações:

$$\theta(x, T^k y)(\ell) = \theta(x, y)(\ell + k) \tag{07}$$

$$\theta(T^i x, T^k y)(\ell) = \theta(x, y)(\ell + k - i) \tag{08}$$

$$\theta(T^k x)(\ell) = \theta(x)(\ell) \tag{09}$$

A função $\theta_{x,x}(\ell)$ é conhecida como função de auto correlação e neste caso será denotada com apenas um único índice, $\theta_x(\ell)$. Com esta notação pode-se verificar que:

$$\theta_x(0) = \langle x, x \rangle \tag{10}$$

$$\theta_x(\ell) = \theta_x(\ell + N) \tag{11}$$

$$\theta_x(\ell) = \theta_x(-\ell) \tag{12}$$

$$\left|\theta_x(\ell)\right| \le \left\|x\right\|^2 = \langle x, x\rangle = \theta_x(0) \tag{13}$$

A somatória dos elementos de uma seqüência x qualquer é denotada por:

$$\sum x = \sum_{i=0}^{N-1} x_i \tag{14}$$

e com esta notação pode-se provar as seguintes identidades:

$$\sum_{\ell=0}^{N-1} \theta(x,y)(\ell) = \left(\sum x\right).\left(\sum y\right) \tag{15}$$

$$\sum_{\ell=0}^{N-1} \theta(x)(\ell) = \left|\left(\sum x\right)\right|^2 \tag{16}$$

2-LIMITES PARA AS FUNÇÕES DE CORRELAÇÃO[4,5]

Sejam as seqüências x, y, w, z e um inteiro n qualquer. As quatro funções de correlação cruzada $\theta_{w,x}, \theta_{y,z}, \theta_{w,y}, \theta_{x,z}$ obedecem a seguinte identidade:

$$\sum_{\ell=0}^{N-1} \theta_{w,y}(\ell).[\,\theta_{x,z}(\ell+n)\,] = \sum_{\ell=0}^{N-1} \theta_{w,x}(\ell).[\,\theta_{y,z}(\ell+n)\,] \tag{17}$$

Desta relação obtém-se as seguintes:

para z=y:

$$\sum_{\ell=0}^{N-1} \theta_{w,y}(\ell).[\,\theta_{x,y}(\ell+n)\,] = \sum_{\ell=0}^{N-1} \theta_{w,x}(\ell).[\,\theta_{y}(\ell+n)\,] \tag{18}$$

e desta última, fazendo-se w=x:

$$\sum_{\ell=0}^{N-1} \theta_{x,y}(\ell).[\,\theta_{x,y}(\ell+n)\,] = \sum_{\ell=0}^{N-1} \theta_{x}(\ell).[\,\theta_{y}(\ell+n)\,] \tag{19}$$

e agora se n=0:

$$\sum_{\ell=0}^{N-1}\left|\theta_{x,y}(\ell)\right|^2 = \sum_{\ell=0}^{N-1}\theta_x(\ell)\ \theta_y(\ell) \tag{20}$$

Das identidades anteriores pode-se derivar um limite inicial para a correlação cruzada periódica aplicando a desigualdade de Cauchy, expressão (06), tem-se:

$$\left|\theta_{x,y}(\ell)\right| \le \left[\theta_x(0).\theta_y(0)\right]^{1/2} \tag{21}$$

Aplicando-se agora a desigualdade de Cauchy à equação (20) tem-se:

$$\sum_{\ell=0}^{N-1}\left|\theta_{x,y}(\ell)\right|^2 \le \left(\sum_{\ell=0}^{N-1}\left|\theta_x(\ell)\right|^2\right)^{1/2}\left(\sum_{\ell=0}^{N-1}\left|\theta_y(\ell)\right|^2\right)^{1/2} \tag{22}$$

Desta forma pode-se chegar a um limite superior, bem como a um inferior, para as funções de correlação cruzada. Reescrevendo-se novamente (20) segue-se:

$$\sum_{\ell=0}^{N-1}\left|\theta_{x,y}(\ell)\right|^2 = \theta_x(0)\,\theta_y(0) + \sum_{\ell=1}^{N-1}\theta_x(\ell)\ \theta_y(\ell) \tag{23}$$

Assim temos a seguinte relação para o limite superior da função de correlação cruzada periódica:

$$\sum_{\ell=0}^{N-1}\left|\theta_{x,y}(\ell)\right|^2 \le \theta_x(0).\theta_y(0) + \left(\sum_{\ell=1}^{N-1}\left|\theta_x(\ell)\right|^2\right)^{1/2}.\left(\sum_{\ell=1}^{N-1}\left|\theta_y(\ell)\right|^2\right)^{1/2} \tag{24}$$

e para o limite inferior:

$$\sum_{\ell=0}^{N-1}\left|\theta_{x,y}(\ell)\right|^2 \ge \theta_x(0).\theta_y(0) - \left(\sum_{\ell=1}^{N-1}\left|\theta_x(\ell)\right|^2\right)^{1/2}.\left(\sum_{\ell=1}^{N-1}\left|\theta_y(\ell)\right|^2\right)^{1/2} \tag{25}$$

Um outro limite importante pode ser obtido pelo limite de Welch. Dado um conjunto X de K seqüências denota-se o pico para magnitude da correlação cruzada e da auto correlação fora de fase, respectivamente, por θ_c e θ_a, isto é:

$$\theta_c = \max\left\{\left|\theta_{x,y}(\ell)\right|; 0 \le \ell \le N-1,\ \ x,y \in X \text{ e } x \ne y\right\} \tag{26}$$

$$\theta_a = \max\left\{\left|\theta_x(\ell)\right|;\ 1 \le \ell \le N-1,\ x \in X\right\} \tag{27}$$

Com estas definições tem-se que para o conjunto X de K seqüências é válida a seguinte relação:

$$\left(\frac{\theta_c^2}{N}\right) + \frac{N-1}{N(K-1)}\left(\frac{\theta_a^2}{N}\right) \ge 1 \tag{28}$$

Definindo-se agora $\theta_{max} = \max\{\theta_a, \theta_c\}$, segue um outro limite importante, WELCH[6]:

$$\theta_{max} \ge N\left[\frac{K-1}{N.K-1}\right]^{1/2} \tag{29}$$

Estas expressões são úteis como termos de comparação entre famílias, como será visto no próximo item.

3-FAMÍLIAS DE SEQÜÊNCIAS

3.1 SEQÜÊNCIAS LINEARES

3.1.1 SEQÜÊNCIAS DE MÁXIMO COMPRIMENTO (SMC)

Estas seqüências também são conhecidas pelo nome de m-seqüências. São as mais conhecidas, pois direta ou indiretamente estão envolvidas no processo de obtenção de muitas outras famílias de código. As pesquisas destas filas de dígitos binários iniciaram-se por volta de 1950 e o estudo das mesmas recebeu grande colaboração de GOLOMB, entre outros. Estes códigos possuem ótimas propriedades de auto correlação que colaboram, em grande parte, para a etapa de sincronismo de alguns sistemas de comunicação.

Quanto às características da correlação cruzada, pode-se dizer que as mesmas possuem resultados atraentes, apesar de não serem os melhores. Por outro lado o algoritmo de obtenção de uma SMC é muito simples o que a torna adequada para sistemas de complexidade não muito elevada. No entanto, em sistemas onde há uma exigência maior

em relação ao sigilo estas não são adequadas por serem lineares e muito conhecidas (fáceis de serem decodificadas). Aliado a este fato o número de SMC's de mesmo período e distintas, que não sejam ciclicamente equivalentes, é pequeno. Assim o número de usuários, comportados por um sistema CDMA em que cada usuário utilize uma SMC ciclicamente distinta, é reduzido.

3.1.1.1 CONSTRUÇÃO DE UMA SMC

Algebricamente, as SMC são construídas através de um polinômio que indica as respectivas operações que devem ser realizadas com o conteúdo de suas variáveis (este polinômio será aqui denominado de polinômio gerador). Os coeficientes deste polinômio estão restritos aos valores 0 ou 1. As operações aritméticas realizadas com estes números são do tipo mod2. O polinômio binário de grau n é denotado por C(x):

$$C(x) = C_n . x^n + C_{n-1} . x^{n-1} + ... + C_0 \qquad (30)$$

onde os coeficientes $C_n = C_0 = 1$, necessariamente. No primeiro caso para que o grau seja n e no segundo para a realimentação do registrador. Este polinômio será representado por um vetor binário $C=\{C_n, C_{n-1},..., C_0\}$, bem como pela sua notação octal. A indicação da base aparecerá quando houver a possibilidade de uma interpretação incorreta no contexto. Para ilustrar estes aspectos de notação examine-se os exemplos a seguir.

Os polinômios $x^5 + x^4 + x^2 + x + 1$ e $x^6 + x^5 + x^3 + x^2 + 1$ serão representados, respectivamente, pelos vetores {1, 1, 0, 1, 1, 1} e {1, 1, 0, 1, 1, 0, 1} ou também pela respectiva notação em octal [67] e [155]. Uma seqüência s_i qualquer é dita gerada pelo polinômio $C_i(x)$ se tomado qualquer segmento de tamanho n de s_i e substituído em $C_i(x)$ obtém-se como resultado zero. Algebricamente este fato pode ser escrito da seguinte forma:

$$C(x) = x^n + C_{n-1} . x^{n-1} + ... + 1 = 0 \qquad (31)$$

As SMC podem ser construídas através de registradores de deslocamento, como se representa na figura a seguir.

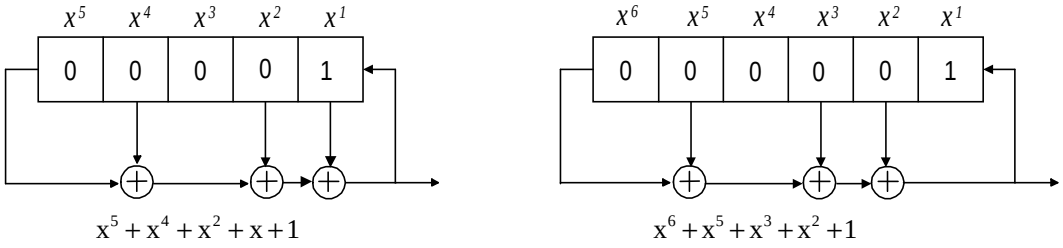

Fig. 1 Registradores de deslocamento para a construção de uma SMC

Os registradores de deslocamento exibem certas propriedades das seqüências de forma mais imediata. Estas propriedades são inerentes aos registradores e assim são transferidas diretamente às seqüências. Se o conteúdo de cada uma das células dos registradores acima fosse zero, então a saída seria uma seqüência de zeros, daí conclui-se que o conteúdo dos registradores nunca deverá passar pelo estado nulo. Outras propriedades, não tão imediatas, podem ser obtidas.

As SMC's são aquelas em que o conteúdo do registrador passa por todos os estados possíveis, exceto o nulo. Como necessariamente haverá repetição dos estados anteriores após isto, o período desta classe de códigos é $N = 2^n - 1$.

O conteúdo inicial do registrador determina a fase inicial da seqüência. Neste trabalho este conteúdo inicial será adotado sempre como {0,0,0,0,...1}.

O processo para se gerar uma SMC é muito simples, no entanto, existem apenas alguns polinômios que são capazes de construir uma SMC. Estes polinômios capazes de gerar uma SMC são conhecidos pelo nome de polinômios primitivos.

3.1.1.2 PROPRIEDADES DAS SMC'S

As seqüências de máximo comprimento possuem as seguintes propriedades:

Seja a seqüência binária b construída a partir de um polinômio primitivo C(x), nestas circunstâncias pode-se verificar que:

1- Possue período $N=2^n-1$

2- Existem N seqüências não nulas geradas por C(x), que são ciclicamente equivalentes.

3- Dados dois inteiros distintos $1 \le i, j \le N$, existe apenas um inteiro k, distinto destes dois últimos, $1 \le k \le N$, tal que:

$$T^i b \oplus T^j b = T^k b \tag{32}$$

4- $$wH(s) = 2^{n-1} = \tfrac{1}{2}(N+1) \tag{33}$$

5- Para seqüências polarizadas

$$\theta_b(\ell) = \begin{cases} N, & \text{se } \ell = 0 \\ -1, & \text{se } \ell \neq 0 \end{cases} \tag{34}$$

onde N é igual ao período da seqüência. Esta propriedade mostra que existem apenas dois valores para a função de auto correlação periódica.

6- De todas as N seqüências possíveis de serem geradas por C(x), há exatamente uma para a qual vale:

$$\tilde{b}_i = \tilde{b}_{2i} \text{ para todo } i \in Z. \tag{35}$$

Esta seqüência será denominada de seqüência característica e será denotada por $\tilde{b}$ e a fase desta seqüência será chamada de fase característica.

7- Assumindo-se que a seqüência b[q] não seja nula, onde q é um inteiro, b[q] terá um período igual a N/mdc(N,q), e será construída a partir de um polinômio $C'(x)$, cujas raízes são a q-ésimas potências das raízes de C(x).

Quando mdc(N,q)=1, b[q] também será uma SMC de período N. Neste caso a decimação é denominada própria. O polinômio $C'(x)$ será um polinômio primitivo distinto de C(x), exceto quando b estiver em sua fase característica e q=2 (considera-se sempre q=qmodN para efeitos de decimação)**.**

Uma característica da decimação por 2, está no fato de que esta gera sempre a própria seqüência da qual foi decimada, deslocada por um fator k (na fase característica k=0). Realizando-se todas a decimações possíveis, tal que mdc(N,q)=1 com q menor que N, obtém-se todas as SMC de grau n.

8- Se o mdc(N,q)=1 e a=b[q], então para todo j, i inteiros não negativos tem-se:

$$\tilde{b}[2^j q] = \tilde{b}[2^j q \bmod N] = \tilde{a}$$

e (36)

$$b[2^j q] = b[2^j q \bmod N] = T^i a$$

Existe uma decimação de particular interesse: aquela que gera a seqüência recíproca da que está sendo decimada, que é a decimação de ordem N-1. Combinando esta decimação com a propriedade 8, obtém-se uma outra decimação capaz também de gerar a seqüência recíproca à decimada, que é a decimação de ordem: $\frac{1}{2}(N-1) = 2^{n-1} - 1$.

9- As quantidades de 1's e 0's numa SMC são, respectivamente, iguais a 2^{n-1}, $2^{n-1} - 1$.

Esta propriedade é denominada de balanceamento, isto é, o número de 1's e 0's difere de apenas um.

10- Em todas as SMC existe apenas um bloco de 1's de comprimento n e um bloco de 0's de comprimento n-1.

11- Tomando-se um número $0 < k < n-1$, existe uma quantidade de blocos de 0's e 1's de comprimento k igual a 2^{n-k-2}

12- O número de SMC's de um dado grau corresponde ao número de polinômios primitivos deste grau, HOLMES[7], e é dado por:

$$\lambda(n) = \frac{\varphi(2^n - 1)}{n} \tag{37}$$

onde $\lambda(n)$ é a função de Euler, que representa o número de positivos inteiros menores do que n e primos com o mesmo. Este número é calculável por:

se $m = \prod_{i=1}^{k} p_i^{\alpha_i}$ onde p_i é primo e α_i inteiro, então:

$$\varphi(m) = \begin{cases} 1 & m = 1 \\ \prod_{i=1}^{k} (p_i - 1) p_i^{\alpha_i - 1} & m > 1 \end{cases} \tag{38}$$

por exemplo:

$n = 6 \Rightarrow m = 2^6 - 1 = 63 = 3^2 \times 7^1 \Rightarrow \varphi(63) = 2 \times 3^1 \times 6 \times 7^0 = 36$ e assim $\lambda(6) = 36/6 = 6$ SMC's.

3.1.1.3 PROPRIEDADES DAS FUNÇÕES DE AUTO CORRELAÇÃO E CORRELAÇÃO CRUZADA PARA SMC'S[5]

Como definido anteriormente a função de correlação cruzada periódica, entre duas seqüências é dada pela expressão:

$$\theta_{a,b} = \sum_{j=0}^{N-1} a(j).b(j+\ell) = C_{a,b}(\ell) + C_{a,b}(\ell - N) \tag{39}$$

A auto correlação é definida pela mesma expressão, quando os índices a e b são iguais. Assumindo-se que a e b são duas SMC's, polarizadas, distintas e de comprimento $N=2^n-1$, seguem-se as seguintes propriedades:

1- $\theta_{a,b}(\ell) = \theta_{a,b}(\ell + N)$ (40)

2- $\left|\theta_{a,b}(\ell)\right| \leq N$ (41)

3- $\theta_{a,b}(\ell)$ é sempre um inteiro ímpar (42)

4- $\theta_{a,b}(\ell)+1$ é sempre um múltiplo de 8 (43)

Exceto quando a e b são seqüências recíprocas, quando então $\theta_{a,b}(\ell)+1$ é múltiplo de 4

5- $\sum_{\ell=0}^{N-1} \theta(a,b)(\ell) = 1$ (44)

Com esta propriedade tem-se que para um valor grande de N, o valor médio de $\theta_{a,b}(\ell)$ é muito próximo de zero.

6- $\sum_{\ell=0}^{N-1} \theta_{a,b}^2(\ell) = N^2 + N - 1 = 2^{2n} - 2^n - 1$ (45)

Constata-se pois que o valor médio quadrático da função de correlação cruzada é muito próximo 2^n, e que $|\theta_{a,b}(\ell)| > 2^{n/2} - 1$, para pelo menos um valor de ℓ.

3.1.1.4 ESPECTRO DE CORRELAÇÃO CRUZADA

Duas SMC's a e b de mesmo grau, possuem as seguintes propriedades relativas ao espectro de correlação cruzada:

1- O espectro de correlação cruzada de duas SMC's a e b quaisquer, é o mesmo que o de $(T^i a,\ T^j b)$.

2- O espectro de (a, a[q])=(b, b[q]) para quaisquer a, b e q, onde q é um inteiro modN qualquer.

3- Se as decimações q e q' são tais que q.q'=1modN então os espectros de (a, a[q])=(a, a[q']).

Teorema 1

A correlação cruzada de duas SMC's distintas a e b de período $N=2^n-1$, assume apenas três valores, quando a e b são tais que, b=a[q]; n não é uma potência de 2; q assume um dos seguintes valores $2^k + 1$ ou $2^{2k} - 2^k - 1$ e sendo e=mdc(n,k) tal que n/e é ímpar. Seguem-se os respectivos valores, bem como o número de ocorrências dos mesmos num período:

$$\theta(a,b)(\ell)=\begin{cases} -1+2^{(n+e)/2} & \text{ocorre } 2^{(n-e-1)}+2^{(n-e-2)/2} \text{ vezes} \\ -1 & \text{ocorre } 2^n-2^{n-e}-1 \text{ vezes} \\ -1-2^{(n+e)/2} & \text{ocorre } 2^{(n-e-1)}-2^{(n-e-2)/2} \text{ vezes} \end{cases} \quad (46)$$

Desta fórmula cabe destacar o fato de que se **e** é grande a correlação toma grandes valores, todavia poucas vezes, se **e** é pequeno a correlação assume valores menores, porém muitas vezes. No que se segue adotar-se-á seguinte expressão:

$$t(n) = 1+2^{\lfloor (n+2)/2 \rfloor} \quad (47)$$

onde $\lfloor \alpha \rfloor$ representa a parte inteira do argumento.

Definição 1

Denominam-se pares preferenciais às SMC a e b, de mesmo grau n, não múltiplo de 4, que possuam espectro de correlação cruzada apenas com os valores: -1, -t(n), t(n) - 2.

Teorema 2

Se a e b são duas SMC's, onde o grau n das mesmas é múltiplo de 4, e se

b=a[-1+2$^{(n+2)/2}$]=a[t(n)-2] então o espectro de correlação cruzada assume apenas quatro valores:

$$\theta(a,b)(\ell)=\begin{cases}-1+2^{(n+2)/2} & \text{ocorre } (2^{n-1}+2^{(n-2)/2})/3 \text{ vezes}\\ -1+2^{n/2} & \text{ocorre } 2^{n/2} \text{ vezes}\\ -1 & \text{ocorre } 2^{(n-1)}+2^{(n-2)/2}-1 \text{ vezes}\\ -1-2^{n/2} & \text{ocorre } (2^{n}-2^{n/2})/3 \text{ vezes}\end{cases} \quad (48)$$

Comparando-se estes resultados com os do Teorema 1, observa-se que são mais interessantes do que aqueles, quando ***e*** é maior que três. Outros resultados que advém deste último são:

Se n é par:

$$-t(n)+4 \le \theta(a,b)(\ell) \le t(n)-2 \quad (49)$$

e se a e b são recíprocos tem-se:

$$\left|\theta(a,b)(\ell)\right| \le 2^{(n+2)/2} \quad (50)$$

Denotando θ_c como o limite máximo para a magnitude da correlação cruzada entre duas SMC's a e b de período $N=2^n - 1$, com n maior ou igual a três, os resultados anteriores podem ser sintetizados da seguinte forma:

1- Quando n é ímpar ou 2mod4, $\theta_c \ge t(n)$ para pares preferenciais

2- Quando n é par, $\theta_c \ge t(n) - 2$ para a e b recíprocos

3- Quando n é múltiplo de quatro, $\theta_c \ge t(n) - 2$ para a e b seguindo o teorema 2

3.1.2 SEQÜÊNCIAS DE GOLD

3.1.2.1 CONSTRUÇÃO DA FAMÍLIA

As seqüências de Gold formam um conjunto (família) que consiste de N+2 seqüências. Cada uma possue um período $N=2^n-1$, onde n é o número de células dos registradores utilizados para a obtenção das seqüências. Este grupo é construído em duas etapas através do uso de dois registradores de deslocamento, atuando em paralelo, conforme figura 2 adiante. Cada registrador possue realimentações que geram uma SMC.

A primeira etapa consiste em inicializar-se um dos registradores com zeros enquanto o outro passa por todos os estados possíveis, exceto o nulo. Somando-se as saídas obtidas nos dois registradores gerar-se-á a SMC correspondente ao segundo registrador.

A segunda etapa consiste em inicializar-se o primeiro registrador com um conteúdo não nulo qualquer, enquanto o outro é inicializado com todos os estados possíveis, inclusive o nulo. Somando-se as saídas obtidas de ambos os registradores obtém-se as 2^n seqüências restantes da família.

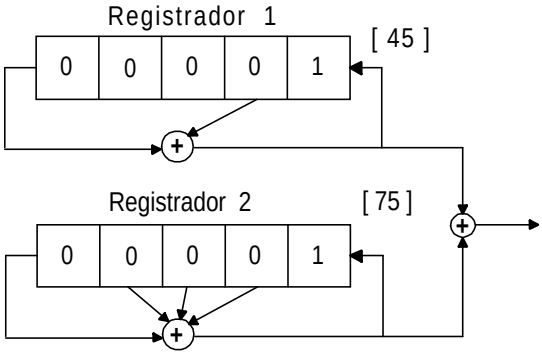

Fig. 2 Registradores de deslocamento para a construção de Família de Gold

Algebricamente, este procedimento pode ser descrito pela expressão a seguir, onde a e b são SMC's.

$$G(a,b) = \{a, b, a \oplus b, a \oplus Tb, a \oplus T^2b, a \oplus T^3b, \ldots, a \oplus T^{N-1}b\} \qquad (51)$$

A propriedade mais importante desta família é que tomando-se um par qualquer de seqüências da mesma, tem-se que os picos para a auto correlação e correlação cruzada

periódicas estão limitados aos máximos valores obtidos para a correlação cruzada de a e b, isto é, as propriedades de correlação do conjunto dependem de a e b e tem-se:

$$\theta_c = \max\left\{\left|\theta_{a,b}(\ell)\right|; 0 \le \ell \le N-1\right\} = \theta_a = \max\left\{\left|\theta_i(\ell)\right|; 1 \le \ell \le N-1 \text{ e } i = a, b\right\} \quad (52)$$

Destes resultados tem-se, nos piores casos, valores de pico semelhantes às SMC's.

Definição 2

O conjunto G(a,b) é denominado de conjunto de seqüências de Gold se as seqüências a e b formarem um par preferencial de SMC's (conforme Definição 1).

Assim para a seqüências de Gold a correlação cruzada entre as seqüências da família resulta em três valores, que são aqueles relativos aos pares preferenciais, onde o pico é igual a t(n).

Quando n é ímpar, então {a, a[2^k+1]} formam um par preferencial, visto que mdc(n,k)=1.

Verifica-se que o Teorema 1 é válido para todas as decimações de valor 2^k+1. Uma implicação destes resultados é que {a, a[t(n)]} é um par preferencial desde que n não seja um múltiplo de 4. Assim G(a,a[t(n)]) será uma família de Gold, com pico de correlação cruzada igual a t(n) e seu espectro variará entre três valores.

Tem-se pois que para as seqüências de Gold:

$$x, y \in G(a, b) \Rightarrow \theta(x, y)(\ell) \in \{-1, -t(n), t(n) - 2\} \quad (53)$$

e

$$z \in G(a, b) \Rightarrow \theta(z)(\ell) \in \{-1, -t(n), t(n) - 2\} \quad , \forall \ell \neq 0 \bmod N \quad (54)$$

3.1.3 FAMÍLIA GOLD LIKE E GOLD BCH DUAL

Estas famílias apresentam resultados similares aos obtidos pelas seqüências de Gold e a sua construção segue o mesmo procedimento.

3.1.3.1 CONSTRUÇÃO DA FAMÍLIA

Seja a uma SMC de período $N=2^n-1$, onde n é um inteiro par. Construa-se primeiro o conjunto $b^{(k)}$, k=0,1,2,.. onde $b^{(k)}$ é obtido pela decimação q de $T^k a$, com q inteiro, obedecendo a relação mdc(q, N)=3. Este conjunto conterá três seqüências de período N'=N/3.

A próxima etapa consiste na operação XOR, bit a bit, de a com cada uma das três seqüências geradas, para todos os deslocamentos possíveis destas. Esta construção gera uma família, que conterá N+1 seqüências de período N. A expressão a seguir exibe estes procedimentos.

$$\begin{aligned} GL(a,q) = \{ & a, a \oplus b^{(0)}, a \oplus Tb^{(0)}, a \oplus T^2 b^{(0)}, \ldots, a \oplus T^{N'-1} b^{(0)}, \\ & a \oplus b^{(1)}, a \oplus Tb^{(1)}, a \oplus T^2 b^{(1)}, \ldots, a \oplus T^{N'-1} b^{(1)}, \\ & a \oplus b^{(2)}, a \oplus Tb^{(2)}, a \oplus T^2 b^{(2)}, \ldots, a \oplus T^{N'-1} b^{(2)} \} \end{aligned} \quad (55)$$

3.1.3.2 GOLD LIKE

Dá-se o nome de Gold-Like, ao conjunto de seqüências geradas tal como em (55), onde com q=t(n). Quando n é múltiplo de 4 o mdc(t(n),N)=3 e então é possível a obtenção da família. Os resultados para a correlação cruzada periódica restringem-se a apenas cinco valores, sendo o maior valor em módulo igual a t(n). O valores para a correlação cruzada periódica assumem um valor dentre os seguintes:

$$\{-1, -t(n), t(n)-2, -s(n), s(n)-2\} \quad (56)$$

onde s(n) é calculável por:

$$s(n) = 1 + 2^{n/2} = \tfrac{1}{2}(t(n)+1) \quad (57)$$

3.1.3.3 GOLD BCH DUAL

Estas seqüências utilizam o mesmo processo de construção em (55), onde o valor para a decimação é igual a 3; desta forma quando n é par o mdc(3,N)=3. Como na família anterior esta também possue N+1 seqüências de período N. Os valores para a correlação cruzada restringem-se também a apenas cinco valores, que são:

$$\{-1, -t(n), t(n)-2, -s(n), s(n)-2\}. \quad (58)$$

Observação: quando n é ímpar, a[3] é uma SMC e assim {a, a[3]} formam um par preferencial recaindo-se, neste caso, na família de Gold.

3.1.4 FAMÍLIAS DE KASAMI

3.1.4.1 CONJUNTO PEQUENO DE KASAMI

Esta família é gerada a partir de uma SMC a de grau n par, sobre a qual realiza-se uma decimação de ordem $q=s(n)=2^{n/2}+1$, gerando-se uma nova seqüência b=a[s(n)]. A seqüência b é uma SMC de grau n/2 e consequentemente com período igual a $2^{n/2}-1$. A construção da família segue-se com a operação XOR bit a bit de a e b, para todos os deslocamentos possíveis entre as mesmas. Este procedimento é o a seguir indicado:

$$Kp(a) = \{a, a \oplus b, a \oplus Tb, a \oplus T^2 b, a \oplus T^3 b, \ldots, a \oplus T^{2^{n/2}-2} b\} \quad (59)$$

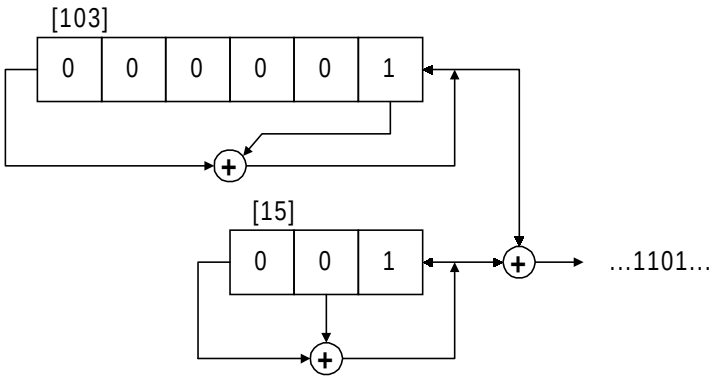

Fig. 3 Registradores de deslocamento para a construção da família Kasami Pequeno

Os valores para a correlação cruzada periódica entre as seqüências desta família restringem-se a apenas três valores que são:

$$\{-1, -s(n), s(n)-2\} \tag{60}$$

A característica principal desta família consiste no valor máximo do módulo de sua correlação cruzada periódica que é $2^{n/2}+1$. Este valor é aproximadamente metade daquele encontrado para as seqüências da família de Gold.

No entanto o número de seqüências desta família é $2^{n/2}$, bem inferior à família de Gold.

O valor da correlação cruzada periódica do conjunto pequeno de Kasami é muito próximo ao limite de WELCH, que quando aplicado à um grupo de $2^{n/2}$ seqüências de comprimento $2^{n/2}-1$ resulta em:

$$\theta_{MAX} > 2^{n/2} - 1 \tag{61}$$

Considerando o fato de que a correlação cruzada periódica entre seqüências binárias de comprimento ímpar é um número inteiro ímpar, o limite anterior pode ser reescrito como se segue:

$$\theta_{MAX} \geq 2^{n/2} + 1 \tag{62}$$

Para esta última relação, o conjunto pequeno de Kasami é um conjunto ótimo.

3.1.4.2 CONJUNTO GRANDE DE KASAMI

Para construir-se este conjunto são necessárias três seqüências a, b e c. A primeira deve ser uma SMC de grau n par; a segunda obtida de forma análoga àquela realizada no conjunto pequeno de Kasami e a terceira é construída por uma decimação de ordem t(n) da primeira. As três seqüências são pois: a, b=a[s(n)] e c=a[t(n)]. Com estas três seqüências, realiza-se a

operação XOR bit a bit para todos os deslocamentos possíveis entre as três seqüências. Este procedimento gerará então o conjunto grande de Kasami.

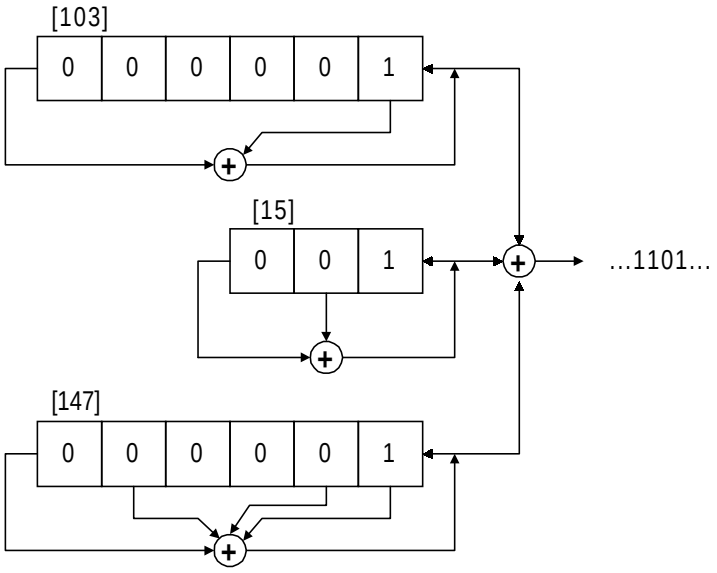

Fig. 4 Registradores de deslocamento para a construção da família Kasami Grande

Existem dois resultados possíveis para esta família:

1- Se n=2mod4.

$$Kg(a) = G(a,c) \bigcup \left[\bigcup_{i=0}^{2^{n/2}-2} \left\{ T^i b \oplus G(a,c) \right\} \right] \tag{63}$$

2- Se n=0mod4

$$Kg(a) = GL(a,t(n)) \bigcup \left[\bigcup_{i=0}^{2^{n/2}-2} \left\{ T^i b \oplus GL(a,t(n)) \right\} \right] \bigcup \left\{ c^{(j)} \oplus T^k b : 0 \le j \le 2; 0 \le k \le (2^{n/2}-1)/3 \right\} \tag{64}$$

Os valores para a função de correlação cruzada periódica são {-1, -t(n), t(n)-2, -s(n), s(n)-2} e o número de elementos deste conjunto é $2^{n/2}(2^n+1)$ para n=2mod4 ou $2^{n/2}(2^n+1)$-1 para n=0mod4.

Esta família contém a família de Gold (ou Gold-Like) bem como o conjunto pequeno de Kasami. Este conjunto mantém os mesmos resultados para a correlação cruzada que as das famílias anteriores, com um aumento significativo no número de seqüências da família.

3.1.5 SEQÜÊNCIAS DE HADAMARD[8]

As seqüências de Hadamard tem assumido uma importância cada vez maior no universo das telecomunicações principalmente por sua ortogonalidade e facilidade de construção. São obtidas através das linhas e/ou colunas das matrizes de Hadamard. As matrizes de Hadamard são denotadas por H_m onde m indica o número de linhas (colunas). Esta família de seqüências apesar de linear difere das anteriores em alguns aspectos, entre eles: o comprimento que é par, pela forma de construção que não é baseada em registradores de deslocamento e/ou polinômios característicos e porque, de uma maneira geral, estão vinculadas a sistemas síncronos. No entanto estas seqüências são utilizadas em sistemas de telefonia móvel, como também podem servir de base para a construção de seqüências não lineares, como as seqüências de Bent. Descreve-se a seguir as características das mesmas, bem como o tipo mais conhecido.

Definição 3

Uma matriz de Hadamard de ordem m, é uma matriz m x m, H_m, onde todos seus elementos são -1 ou +1 e tal que:

$$H_m H_m^T = H_m^T H_m = mI_m \qquad (65)$$

onde I_m indica a matriz identidade de ordem m e o expoente T uma transposição. Esta expressão estabelece que quaisquer duas linhas (ou colunas) de H_m são ortogonais.

Definição 4

Uma matriz retangular mxn, H_{mxn}, consistindo de elementos -1 e +1, é dita uma matriz de Hadamard retangular (ou incompleta) se:

$$H_{mxn}H_{mxn}^{T} = nI_{m} \tag{66}$$

Definição 5

Duas matrizes H_1 e H_2 são matrizes de Hadamard equivalentes, se:

$$H_{2} = PH_{1}Q \tag{67}$$

onde P e Q são matrizes de permutação, isto é, matrizes com elementos -1 ou +1 com o objetivo de permutar as linhas e/ou colunas de H.

Existem vários métodos para a construção das matrizes de Hadamard, tais como os de Williamson, Baumert-Hall, Goethals-Seidel etc. Expor-se-á neste trabalho um dos métodos mais utilizados para a obtenção destas, mais especificamente as de ordem 2^n, conhecidas como matrizes de Hadamard tipo Sylvester.

$$H(k+1)=\begin{Vmatrix} H(k) & H(k) \\ H(k) & -H(k) \end{Vmatrix} \tag{68}$$

onde

$$H(1)\in\{\pm D_1,\pm D_2,\pm D_3,\pm D_4\} \tag{69}$$

$$D_1 = \begin{Vmatrix} +1 & -1 \\ +1 & +1 \end{Vmatrix},\ D_2 = \begin{Vmatrix} +1 & +1 \\ +1 & -1 \end{Vmatrix},\ D_3 = \begin{Vmatrix} -1 & +1 \\ +1 & +1 \end{Vmatrix} \text{ e } D_4 = \begin{Vmatrix} +1 & +1 \\ -1 & +1 \end{Vmatrix} \tag{70}$$

Comumente, esta construção é encontrada com o nome de matrizes de Walsh-Hadamard ou matrizes de Walsh; qualquer uma das denominações pode ser considerada correta pois a matrizes de Walsh são um caso particular das matrizes de Hadamard.

A definição genérica para estas matrizes é realizada sobre corpos matemáticos e denotada por H(p,h) onde h é a ordem da matriz e p indica a base do corpo matemático ao qual se refere. Nestas condições tem-se a seguinte expressão para a matriz de Hadamard generalizada:

$$H\ H^{*} = h\ I_{h} \qquad (71)$$

onde H^{*} é a transposta conjugada da matriz H.

As matrizes de Walsh são definidas para o caso em que p=2, e $h=2^{n}$.

3.2 SEQÜÊNCIAS NÃO LINEARES[9]

A designação seqüências não-lineares é, em princípio, inadequada pois o adjetivo refere-se ao método empregado para a construção e não à seqüência. No entanto para que a linguagem fique mais simples tratar-se-á as seqüências geradas por operações não lineares simplesmente por seqüências não lineares.

As seqüências não-lineares caracterizam-se por possuírem um método de construção mais complexo e um equivalente linear muito longo em comparação com às lineares de mesmo grau. Equivalente linear é um valor que representa o menor número células necessárias para a construção de uma determinada seqüência através de operações lineares. Cabe ressaltar que toda seqüência pode sempre ser construída por um gerador com operações lineares. A aplicação principal destas seqüências está relacionada com sistemas que exigem sigilo e baixa probabilidade de interceptação.

A forma mais conveniente para trabalhar-se com códigos não-lineares é através da função traço, que mapeia elementos de $GF(2^{n})$ num subcorpo $GF(2^{j})$, onde n é um inteiro divisível por j.

A função traço (vide item 5 do apêndice) é definida por:

$$tr_j^n(\alpha) = \sum_{i=0}^{(n/j)-1} \alpha^{2^{j.i}} \qquad (72)$$

onde α é um elemento primitivo de GF(2^n). Esta função pode ser utilizada de uma maneira geral para definir qualquer seqüência de código, linear ou não.

3.2.1 SEQÜÊNCIAS GMW[10]

Estas seqüências são devidas à Gordon, Mills e Welch (GMW) e possuem propriedades similares às SMC's.

Considere um inteiro n=j.k, e a seqüência $\{b_i\}$ definida por:

$$b_i = tr_1^j\left\{ \left[tr_j^n(\alpha^i) \right]^r \right\} \qquad (73)$$

onde α é um elemento primitivo de GF(2^n) e r um inteiro qualquer relativamente primo à 2^j-1 no intervalo $1 \le r < 2^j - 1$. Quando r=1 a seqüência $\{b_i\}$ definida por (73) nada mais é que uma SMC. Os valores das funções definidas pela expressão anterior são denominadas como seqüências GMW.

A parte interna da função traço $tr_j^n(\alpha^i)$ pode ser interpretada como uma SMC de período 2^n -1, com elementos em GF(2^j). Os elementos zero nesta seqüência tem uma característica especial, com relação a distribuição dos zeros, que é descrita a seguir. Seja a seqüência $\{b_i'\}$ dada por:

$$b_i' = tr_j^m(\alpha^i) \qquad (74)$$

Então para cada T=(2n-1)/(2j-1) símbolos consecutivos de $\{b_i'\}$, haverá (2n-j-1)/(2j-1) zeros (esta característica é útil na demonstração das propriedades de correlação periódica das GMW).

As GMW's possuem as mesmas propriedades de correlação cruzada periódica que as SMC's, no entanto possuem um equivalente linear maior. O equivalente linear L de uma GMW, dada por (73), é:

$$L = j(n / j)^{w} \tag{75}$$

onde w é o número de uns da representação de r na base 2.

Uma seqüência $\{b_i\}$ de período 2^n-1, é chamada de k-upla balanceada, se o número de ocorrências N_C de uma k-upla c sobre GF(2), num período da mesma, é dado por 2^{n-k}. Com esta definição uma SMC de grau n é uma n-upla balanceada.

Seja então uma GMW $\{b_i\}$. O número N_C é dado por:

$$N_c = \begin{cases} 2^{(n-k)}, & \text{para} \quad c \neq 0, \quad 1 \leq k \leq n / j \\ 2^{(n-k)} - 1, & \text{para} \quad c = 0, \quad 1 \leq k \leq n / j \end{cases} \tag{76}$$

Um outro resultado importante é que para qualquer decimação própria de uma GMW, ou uma escolha qualquer de r na fórmula de geração, obtém-se uma seqüência GMW distinta.

O número de GMW ciclicamente distintas, para um n e j fixos, é dado por:

$$N_{GMW} = N_P(n).N_p(j) \tag{77}$$

onde Np(n) é o número de polinômios primitivos de grau n sobre GF(2).

Comparando-se as GMW's e SMC's tem-se que ambas possuem as mesmas propriedades de correlação cruzada periódicas, no entanto as GMW tem um equivalente linear maior e um conjunto de seqüências ciclicamente distintas de mesmo grau, superior (as GMW's distintas, de mesmo grau, eventualmente podem possuir equivalentes lineares de tamanhos diferentes). Estas características das GMW conferem uma maior segurança ao sistema quando comparadas as SMC's.

3.2.2 SEQÜÊNCIAS DE BENT[11,12]

3.2.2.1 INTRODUÇÃO

As seqüências de Bent são códigos construídos a partir de funções de Bent, definidas por ROTHAUS[13], como se segue.

Definição 6

Seja P(x) uma função que mapeia um espaço vetorial V_n de dimensão n (GF(2^n)) de n-uplas em GF(2), sobre um espaço V_1 de dimensão 1 (GF(2)). P(x) será uma função de Bent se todos os coeficientes da Transformada de Fourier da função $(-1)^{P(x)}$ forem iguais a 1. Os coeficientes de Fourier $c(\lambda)$ são calculados pela expressão:

$$c(\lambda) = \frac{1}{2^{n/2}} \sum_{x \in V_n} (-1)^{P(x)} . (-1)^{\langle \lambda, x \rangle} \qquad (78)$$

onde λ e $x \in V_n$ e $\langle \lambda, x \rangle$ é o produto escalar entre os dois vetores; nestas circunstâncias pode-se escrever[10,11]:

$$(-1)^{P(x)} = \frac{1}{2^{n/2}} \sum_{\lambda \in V_n} c(\lambda) . (-1)^{\langle \lambda, x \rangle} \qquad (79)$$

Assim se $c(\lambda) = 1$ para todo x, $\lambda \in V_n$ a função P(x) será uma função de Bent.

A função P(x) pode ser interpretada como uma função Booleana e x como um vetor pertencente a um espaço vetorial V_n. As funções de Bent possuem inúmeras propriedades gerais; a seguir apresentam-se algumas que podem ser verificadas em ROTHAUS[13]:

1- $2^{n/2} c(\lambda)$ é o número de zeros menos o número de uns da função $P(x)+\langle \lambda, x \rangle$.

2- Se P(x) é uma função de Bent então $c(\lambda)$ também será, isto é, a transformada de uma função de Bent também é uma função de Bent.

3- P(x) é uma função de Bent se e somente se $(-1)^{P(x+y)}$ é uma matriz de Hadamard para todo $y \in GF(2^n)$.

4- Se P(x) uma função de Bent então n é par.

5- Se P(x) sobre V_n e Q(y) sobre V_m são funções de Bent então P(x)+Q(y) sobre V_{n+m} também é uma função de Bent.

ROTHAUS[13] apresentou duas grandes classes de funções de Bent, com as respectivas comprovações, colocadas a seguir:

1- Sejam $x, y \in V_k$ e P(x) um polinômio arbitrário sobre V_k. Então o polinômio Q(x,y) sobre V_{2k} dado por:

$$Q(x,y) = \langle x,y \rangle + P(x) \tag{80}$$

será uma função de Bent.

2- Sejam A(x), B(x) e C(x) funções de Bent sobre V_{2k}, e $y, z \in V_1$, então o polinômio:

$$\begin{aligned} Q(x,y,z) = {} & A(x)B(x) + B(x)C(x) + \\ & + C(x)A(x) + [A(x) + B(x)]y + [A(x) + C(x)]z + yz \end{aligned} \tag{81}$$

é uma função de Bent sobre V_{2k+2}.

Com estas duas classes podem ser construídas, rapidamente, várias funções de Bent. Observe-se que a primeira classe pode ser compreendida como um caso particular da segunda.

As funções de Bent possuem uma estreita relação com as matrizes de Hadamard, assim pode-se definir uma outra forma para as funções de Bent através da transformada de Hadamard[14]. As funções de Bent podem ser analisadas e construídas de diversas outras formas, tais como nos co-conjuntos de primeira ordem de Reed-Muller, através da álgebra

das matrizes de Kronecker etc. Em YARLAGADDA[15] faz-se uma análise e síntese de seqüências de Bent por diversos métodos, enfocando aquelas de comprimento 2^n.

Neste trabalho serão analisadas as linhas de construção desenvolvidas por SIMOM[11], OLSEN[12] onde foram exibidas formas de obtenção de famílias de seqüências de Bent com propriedades de correlação bastante atraentes para aplicações envolvendo sistemas de comunicação SS.

3.2.2.2 FILOSOFIA DA CONSTRUÇÃO[11,12]

Descreve-se a seguir o método de construção apresentado em SIMON[11].

Seja α um elemento primitivo de GF(2^d), onde d é um inteiro divisível por 4 e seja x a representação do conteúdo de um gerador de SMC, na configuração de Galois, tendo o polinômio mínimo de α como o polinômio característico do gerador. Seja ainda $\{\phi_1,...,\phi_{d/2}\}$ uma base qualquer de GF($2^{d/2}$) sobre GF(2) e selecione-se um elemento ε qualquer de GF(2^d) que não pertença a um Corpo menor. Constrói-se a matriz M, com dimensão d/2×d, tal que o elemento $m_{i,j}$ é dado por

$$m_{i,j} = Tr_1^d(\varepsilon\phi_i\alpha^{j-1}) \tag{82}$$

e seja ainda s^t um vetor d-dimensional não contido no subespaço linear formado pelas linhas de M. Nestas circunstâncias as $2^{d/2}$ funções não lineares da forma:

$$r_z(x) = (-1)^{f_z(M.x)+s^t.x} \tag{83}$$

onde $f_z(.)$ são funções de Bent, produzem seqüências com correlações cruzadas periódicas e auto correlações periódicas fora de fase limitadas em magnitude por $(1+2^{d/2})$.

Em OLSEN[12] demonstra-se que a função:

$$f_z(x) = x_1^t.x_2 + g(x_2) + z^t.x \tag{84}$$

é uma função de Bent, onde $x \in GF(2^d)$, $x = [x_1\, x_2]^t$ com x_1 e x_2 de mesma dimensão, g(.) é uma função arbitrária e z é uma variável utilizada para a seleção de seqüências (e que determina o número delas numa dada família).

Para o equivalente linear das seqüências desta família pode ser estabelecido um limite inferior[11] dado por:

$$L \geq \begin{cases} 20 & d = 8 \\ \binom{d/2}{d/4} 2^{d/4} + d + \frac{1}{2}\sum_{i=2}^{d/4-1} \binom{d/2}{i} 2^i & d \geq 8 \end{cases} \qquad (85)$$

que fornece, por exemplo, um equivalente linear maior ou igual a 202 para seqüências de Bent de grau 12.

APÊNDICE- ELEMENTOS DE ÁLGEBRA

1- Grupos

Um grupo é um conjunto de elementos que satisfazem os axiomas de AX1 à AX4 abaixo, e para os quais está definida uma e apenas uma operação binária (operação dita binária é aquela aplicada à dois elementos quaisquer, independentemente se são números inteiros, complexos etc.). Sejam a, b, c, ... elementos de um grupo e uma operação binária definida para o grupo, que pode também ser representada por uma função de duas variáveis (f(a,b)=c). As operações binárias que serão utilizadas são as da adição (a + b=c) e/ou multiplicação (a . b=c, ab=c).

Axiomas

AX1 (Fechamento)

Quando a operação binária é aplicada a quaisquer dois elementos do grupo obtém-se um terceiro elemento também do grupo.

AX2 (Lei Associativa)

Dados três elementos quaisquer do grupo, a ordem na qual a operação binária é aplicada a eles não é relevante (e assim não há a necessidade de colocação de parênteses).

AX3 Existe o elemento identidade pertence ao grupo.

Para a operação da adição o elemento identidade será denominado de zero e denotado por 0. Para a operação da multiplicação o elemento identidade será denominado de um e denotado por 1.

Assim tem-se: $a + 0=a$, $a . 1=a$

AX4 Todo o elemento do grupo possui um elemento inverso.

Para a operação da adição o elemento inverso de a será denotado por -a. Para a operação da multiplicação elemento inverso de a será denotado por a^{-1}.

Assim tem-se: $a + (- a)=0$, $a . (a^{-1})=1$.

Teorema: O elemento identidade de um grupo é único e o elemento inverso de cada elemento do grupo também é único.

Se a operação binária do grupo for comutativa então o grupo é dito ser Abeliano ou comutativo.

Exemplo: Seja o seguinte grupo {0, 1, 2, 3, 4} (que são números mod5) para o qual está definida a operação binária da adição.

O elemento identidade do grupo é o 0. O elemento inverso do elemento 2 é 3, pois $2 + 3 =5=0$ mod5.

Num grupo que possua apenas um elemento este será a identidade. Um grupo que possua dois elementos, terá a identidade e o outro elemento será inverso dele próprio. Estes grupos são necessariamente Abelianos.

2- Anéis

Um anel é um conjunto para o qual estão definidas duas operações binárias, sendo uma a adição e a outra a multiplicação e onde valem os axiomas de AX5 a AX8.

AX5

Todo anel é um grupo Abeliano sobre a adição.

AX6

Para quaisquer dois elementos de um anel, o seu produto existe e é um elemento do anel.

AX7

Vale a lei associativa para a multiplicação.

AX8

Vale a lei distributiva.

O anel é dito ser comutativo se a multiplicação for comutativa.

3- Corpos

Um corpo é um anel que forma um grupo Abeliano sobre a multiplicação, excetuando-se o elemento zero.

Os corpos estudados serão aqueles com um número de elementos finito, denominados de corpos de Galois e denotados por GF(q), onde q é um inteiro que representa o número de

elementos do corpo. Os elementos de um corpo podem ser números, polinômios, vetores etc.

Exemplos:

GF(7)={0,1,2,3,4,5,6} é um corpo com 7 elementos, onde deve ser considerada a aritmética mod7, assim 3+5= 1mod7.

GF(2)={0,1} é um corpo com 2 elementos, onde deve ser considerada a aritmética mod2, assim 1+1= 0mod2.

Define-se ordem de um elemento x pertencente a um corpo finito como sendo a potência na qual seja elevado resulte 1, isto é, $x^t=1$, a ordem de x é t, e será denotada como ord(x)=t.

Define-se como sendo um elemento primitivo de GF(q), o elemento x cuja ord(x)=q.

Todos os elementos de GF(q) são potências de um elemento primitivo e todo GF(q) possui pelo menos um elemento primitivo. O elemento primitivo é denominado também como elemento gerador do corpo.

4- Polinômios

Corpos de polinômios são construídos com coeficientes pertencentes à GF(2) e baseados em polinômios que não possuam raízes pertencentes à GF(2).

Exemplo:

Seja o polinômio de $x^3 + x + 1$ sobre o qual será construído um GF(8) de polinômios cujos coeficientes estão em GF(2).

x representa o elemento primitivo.

Na tabela abaixo os elementos da segunda coluna são obtidos através do resto da divisão entre os elementos da primeira coluna e do polinômio acima adotado.

x^0	1
x^1	x
x^2	x^2
x^3	x+1
x^4	x^2+x
x^5	x^2+x+1
x^6	x^2+1

pois, por exemplo: $x^3 = (x^3 + x + 1).1 + x + 1$ (observe-se que x+x=0x=0, com os coeficientes pertencendo à GF(2)).

O corpo é constituído dos elementos da segunda coluna mais o 0.

Diz-se que um corpo é um subcorpo se ele está contido em outro corpo. Assim GF(2) é um subcorpo de GF(2^3).

x^7=1 e qualquer potência maior que 7 pode ser obtida com o auxílio deste detalhe, assim x^{15}=x^{14}.x=x.

5- Função Traço

Sejam dois corpos F=GF(q) e K=GF(q^n). Define-se a função traço de K sobre F pela expressão:

$$Tr_F^K(x) = x + x^q + x^{q^2} + \ldots + x^{q^{n-1}}$$

onde x é um elemento de K.

Exemplo: Sejam F=GF(2), K=GF(2^3) e o polinômio $x^3 + x + 1$. A tabela a seguir ilustra o cálculo da função traço de algumas potências de x (é necessário que os valores da tabela do item 4 sejam levados em consideração).

	Tr_F^K
1	$1 + 1 + 1 = 1$
x^1	$x + x^2 + x^4 = 0(x + x^2) = 0$
x^2	$x^2 + x^4 + x^8 = x^2.(1 + x^2 + x^6) = x^2.(0(x^2+1)) = 0$
x^3	$x^3 + x^6 + x^{12} = x^3.(1 + x^3 + x^9) = x^3.(1 + x^3(1+ x^6)) = ... = 1$
x^4	$x^4 + x^8 + x^{16} = x^4 + x^8.(1+ x^8) = x^4.+ x(1+ x) = 0x^4 = 0$
x^5	$x^5 + x^{10} + x^{20} = x^5 + x^{10}.(1+ x^{10}) = x^5 + x^3(1 + x^3) = ... = 1$
x^6	$x^6 + x^{12} + x^{24} = x^6 + x^{12}.(1+ x^{12}) = x^6 + x^5(1 + x^5) = ... = 1$

Observe-se que o resultado do cálculo da função traço sempre resulta num elemento do subcorpo F.

Com esta função traço constrói-se uma SMC's; assim no exemplo acima a SMC gerada com relação ao polinômio $x^3 + x + 1$ é:

SMC={1, 0, 0, 1, 0, 1, 1}.

Cada bit da seqüência pode ser expresso através da função traço.

$b_i = Tr_F^K(x^i) = Tr(x^i)$, onde x representa um elemento primitivo do corpo.

Quando K e F forem conhecidos os mesmos serão omitidos.

<u>Propriedades da função traço</u>

Sejam os elementos a e b do corpo K e o subcorpo F.

a) $Tr(a) \in F$

b) $Tr(a + b) = Tr(a) + Tr(b)$

c) $Tr(\lambda.a) = \lambda.Tr(a)$ onde $\lambda \in F$

d) $Tr(a^q) = Tr(a)$ onde q é o número de elementos em F

Seja $\{b_i\}$ uma SMC qualquer e $\{b_{d.i}\}$ uma seqüência obtida de $\{b_i\}$ através de uma decimação d, onde o índice i varia de 0 até $N=2^n-1$, n é o grau da SMC e N o comprimento da seqüência.

Sejam $a_i = (-1)^{b_i}$ e $a_{di} = (-1)^{b_{di}}$ as seqüências anteriores em sua forma polarizada.

A correlação cruzada periódica pode ser escrita através da função traço como se segue:

$$\theta(\ell) = \sum_{i=0}^{N} (-1)^{Tr(x^i)+Tr(x^{d.i+\ell})} = \sum_{i=0}^{N} (-1)^{Tr(x^i+x^{d.i+\ell})} = \sum_{y \in GF(2^n)} (-1)^{Tr(y+cy^d)} - (-1)^0$$

onde $c = x^{\ell}$ e $y = x^i$.

Para obter-se o espectro de correlação cruzada periódica deve-se então analisar a função $Tr(y + cy^d)$, isto é, com que freqüência ela assume os valores 0 ou 1.

Se n é impar e d assumindo algum valor na forma:

$$d = 2^k + 1, \text{ou } d = 4^k - 2^k + 1$$

onde k é um inteiro, o espectro de correlação cruzada assume três valores, que são:

$$-1, -1 + 2^{(n+1)/2}, -1 - 2^{(n+1)/2}$$

Com estes resultados pode-se, por exemplo, construir seqüências de Gold, que é uma família onde a correlação cruzada assume os três valores anteriores. Assim através da função traço é possível uma análise algébrica das seqüências de código, o que possibilita a previsão de resultados de forma mais sistemática.

Em SCHOLTZ[17]podem ser encontradas expressões formais para a geração de inúmeras famílias de seqüências, em termos da função Traço.

REFERÊNCIAS BIBLIOGRÁFICAS

1. PICKHOLTZ, R. L.; SCHILLING, D. L.; MILSTEIN, L. B. Theory of Spread Spectrum Communications -A Tutorial. IEEE Transactions on Commmunications, v. COM-30, n. 5, p. 855-884, May. 1982.

2. DIXON, R. C. Spread Spectrum Systems. 2. ed. John Wiley & Sons, 1984.

3. PURSLEY, M. B. Spread-Spectrum Multiple-Access Communications, in Multi-User Communication Systems. G. Longo (editor), Vienna and New York: Springer-Verlag, p. 139-199, 1981.

4. JESZENSKY, P. J. E. Uma Motivação para o Estudo de Seqüências de Códigos. Notas de Aula do Curso PEE-710 Comunicação por Espalhamento Espectral. Departamento de Engenharia Eletrônica da Escola Politécnica da Universidade de São Paulo, p. 1-40, fev. 1992.

5. SARWATE, D. V.; PURSLEY, AND M. B. Crosscorrelation Properties of Pseudorandom and Related Sequences. Proceedings of the IEEE, v. 68, n. 5, p. 593-619, May 1980.

6. WELCH, L. R. Lower Bounds on the Maximum Crosscorrelation of Signals. IEEE Transactions on Information Theory, v. IT-20, n. 3, p. 397-399, May 1974.

7. HOLMES, J. K. Coherent Spread Spectrum Systems. John Wiley & Sons, 1982.

8. AGAIAN, S. S. Hadamard Matrices and Their Applications. Lecture Notes in Mathematics 1168. Springer-Verlag, 1980

9. MARTINEZ, A. A. G.; JESZENSKY, P. J. E. Geradores Não Lineares de Seqüências para uso em Sistemas Spread Spectrum, 13º Simpósio Brasileiro de Telecomunicações, Anais p. 125-130, set. 1995.

10. SCHOLTZ, R. A.; WELCH, L. R. GMW Sequences. IEEE Transactions on Information Theory, v. IT-30, n. 3, p. 548-553, May 1984.

11. SIMON, M. K. et al. Spread Spectrum Communications. Computer Science Press, v.1, 1985.

12. OLSEN, J. D.; SCHOLTZ, R. A.; WELCH, L. R. Bent-Functions Sequences. IEEE Transactions on Information Theory. v. IT-28, n. 6, Nov. 1982.

13. ROTHAUS, O. S. On "Bent" Functions. Journal of Combinatorial Theory. (A) 20, p. 300-305, 1976.

14. MACWILLIAMS, F. J.; SLOANE, N. J. A. The Theory of Error-Correcting Codes. North-Holland, Mathematical Library. v. 16, 1992.

15. YARLAGADDA, R.; HERSHEY, J. E. Analysis and Synthesis of Bent Sequences. IEE Proceedings. v. 136, Pt. E, n. 2. Mar 1989.

16. JESZENSKY, P. J. E. Notas de Aula do Curso PEE-710 Comunicação por Espalhamento Espectral: Teoria Básica sobre Seqüências de Códigos. Departamento de Engenharia Eletrônica da Escola Politécnica da Universidade de São Paulo. p 1-21, mar. 1994.

17. SCHOLTZ, R. A. Criteria for Sequence Set Design in CDMA Communications. The Tenth International Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes, San Juan, Puerto Rico, May 10-14, 1993.