

ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO  
DEPARTAMENTO DE ENGENHARIA ELETRÔNICA  
ÁREA DE SISTEMAS ELETRÔNICOS

SEQÜÊNCIAS DE CÓDIGOS PARA USO EM COMUNICAÇÃO POR  
ESPALHAMENTO ESPECTRAL

Angel Antonio Gonzalez Martinez

**SÃO PAULO**  
1997

Angel Antonio Gonzalez Martinez

SEQÜÊNCIAS DE CÓDIGOS PARA USO EM COMUNICAÇÃO POR  
ESPALHAMENTO ESPECTRAL

Dissertação apresentada à Escola  
Politécnica da Universidade de  
São Paulo para a obtenção do  
título de Mestre em Engenharia  
Elétrica.

Área de Concentração :  
Sistemas Eletrônicos.

Orientador :  
Dr. Paul Jean Etienne Jeszensky.

**SÃO PAULO**  
1997

Gonzalez Martinez, Angel Antonio

Seqüências de Códigos para uso em Comunicação por Espalhamento Espectral.

São Paulo 1997

p. 161

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo.  
Departamento de Engenharia Eletrônica -Área de Sistemas Eletrônicos.

1. Spread Spectrum 2. CDMA 3. Seqüências de Códigos

Universidade de São Paulo. Escola Politécnica . Departamento de Engenharia  
Eletrônica - Área de Sistemas Eletrônicos.

À meu pai, pelo incentivo e  
apoio em todos os momentos.

## **AGRADECIMENTOS**

Ao amigo e orientador Prof. Dr. Paul Jean Etienne Jeszensky pelas incansáveis horas dedicadas em apoio a realização deste trabalho, pelo estímulo e incentivo permanentes.

À CAPES pelo auxílio na forma de bolsa e a FAPESP pelos recursos fornecidos para a realização do Projeto Temático: "Comunicação por Espalhamento Espectral".

À todos os demais que direta ou indiretamente colaboraram para a elaboração deste trabalho.

## RESUMO

Apresenta-se neste trabalho uma revisão dos principais conceitos referentes às seqüências de código tendo como aplicação principal a sua utilização em Sistemas por Espalhamento Espectral de Seqüência Direta (SS/DS-Spread Spectrum Direct Sequence).

Tendo em vista esta aplicação principal caracterizam-se inicialmente os sistemas tipo SS/DS. A partir desta caracterização é possível estabelecer alguns critérios de desempenho que são então utilizados para comparar as diversas famílias de seqüências neste uso específico.

Desta forma, apresentam-se em seguida as principais famílias de códigos geradas linear e não linearmente, assim como suas propriedades mais importantes.

O trabalho conclue com alguns indicativos de desempenho para cada família e critérios objetivos para a seleção de seqüências a serem utilizadas num dado sistema.

É importante salientar que optou-se neste trabalho por uma descrição informativa e livre, ao invés de uma axiomática e formal. Evidentemente esta última forma seria possível, porém o texto ficaria proibitivamente volumoso e os conceitos importantes poderiam ser ofuscados pelo rigor. Desta forma todas propriedades mencionadas ao longo do texto são sempre encaminhadas para referências específicas onde as demonstrações podem ser encontradas.

## ABSTRACT

In this work we explain the main topics concerning code sequences for use in Spread Spectrum Systems of Direct Sequence type (SS/DS-Spread Spectrum Direct Sequence).

With this goal in mind, first SS/DS systems are described in some detail and performance criteria are established for comparison of various families of sequences.

Next families of sequences are introduced (generated in linear and non linear form) and their most important characteristics exposed.

The work is concluded with some performance indicators for each family and an objective criterion for sequence selection is presented.

It is important to emphasize the exposition option for this work: free and informative instead of axiomatic and formal. Clearly this later form would be possible, but the work would lose the desirable hands-on emphasis and some important practical aspects would be masked by formal aspects. With this intention all demonstrations are guided to proper references where the correspondent demonstration can be found.

## LISTAS DE ALGUMAS ABREVIACES UTILIZADAS

- ALOHA             uma expresso de amor ou boas vindas, em lngua Havaiana.
- AWGN            Additive White Gaussian Noise
- BCH              Bose-Chaudhuri-Hocquenghem
- BPSK             Binary Phase Shifty Keying
- CD-CSMA        Code Division-Carrier Sense Multiple Access
- CDMA            Code Division Multiple Access
- dH                Distncia de Hamming
- DS                Direct Sequence
- FDMA            Frequency Division Multiple Access
- FDP              Funo Densidade de Probabilidade
- FH/SS            Frequency Hopping/Spread Spectrum
- GF                Galois Field (Corpo de Galois)
- GMW             Gordon-Mills-Welch
- LAN              Local Area Network
- MFSK            M-Frequency Shifty Keying
- MPSK            M-Phase Shifty Keying
- MQAM            M-Quadrature Amplitude Modulation

- MSK Minimum Shift Keying
- O-CDMA Optical CDMA
- OOC Optical Orthogonal Codes
- PC Personal Computer
- QPSK Quaternary Phase Shift Keying
- SMC Sequências de Máximo Comprimento
- SNR Signal to Noise Ratio
- SS Spread Spectrum
- TDMA Time Division Multiple Access
- TH/SS Time Hopping/Spread Spectrum
- wH Peso (weight) de Hamming

## ÍNDICE

1 INTRODUÇÃO.....	1
1.1 OBJETIVO .....	1
1.2 DESCRIÇÃO DO DESENVOLVIMENTO DO TRABALHO.....	1
1.3 DESCRIÇÃO DOS CAPÍTULOS .....	2
1.4 RESULTADOS ALCANÇADOS/CONTRIBUIÇÕES.....	3
2 SISTEMAS DE COMUNICAÇÃO SPREAD SPECTRUM (SS).....	4
2.1 PRINCÍPIOS .....	4
2.2 IMUNIDADE À INTERFERÊNCIAS NUM SISTEMA TIPO DS/SS.....	6
2.3 SISTEMAS CDMA .....	11
2.3.1 INTRODUÇÃO.....	11
2.3.2 SISTEMAS CDMA-DS/SS ASSÍNCRONOS .....	12
2.3.3 ANÁLISE DA INTERFERÊNCIA DE MÚLTIPLO ACESSO.....	18
3 SEQÜÊNCIAS BINÁRIAS, PRINCÍPIOS GERAIS E CARACTERÍSTICAS.....	27
3.1 ALGUMAS DEFINIÇÕES E PROPRIEDADES BÁSICAS.....	27
3.2 LIMITES PARA AS FUNÇÕES DE CORRELAÇÃO.....	31
3.3 FAMÍLIAS DE SEQÜÊNCIAS .....	33
3.3.1 SEQÜÊNCIAS LINEARES .....	33
3.3.1.1 SEQÜÊNCIAS DE MÁXIMO COMPRIMENTO (SMC).....	33
3.3.1.1.1 CONSTRUÇÃO DE UMA SMC .....	34
3.3.1.1.2 PROPRIEDADES DAS SMC'S .....	36
3.3.1.1.3 PROPRIEDADES DAS FUNÇÕES DE AUTO CORRELAÇÃO E CORRELAÇÃO CRUZADA PARA SMC'S.....	39
3.3.1.1.4 ESPECTRO DE CORRELAÇÃO CRUZADA.....	40
3.3.1.2 SEQÜÊNCIAS DE GOLD.....	42

3.3.1.2.1 CONSTRUÇÃO DA FAMÍLIA .....	42
3.3.1.3 FAMÍLIA GOLD LIKE E GOLD BCH DUAL.....	44
3.3.1.3.1 CONSTRUÇÃO DA FAMÍLIA .....	44
3.3.1.3.2 GOLD LIKE .....	45
3.3.1.3.3 GOLD BCH DUAL.....	45
3.3.1.4 FAMÍLIAS DE KASAMI .....	46
3.3.1.4.1 CONJUNTO PEQUENO DE KASAMI .....	46
3.3.1.4.2 - CONJUNTO GRANDE DE KASAMI.....	47
3.3.1.5 SEQÜÊNCIAS DE HADAMARD .....	49
3.3.2 SEQÜÊNCIAS NÃO LINEARES.....	51
3.3.2.1 SEQÜÊNCIAS GMW.....	52
3.3.2.2 SEQÜÊNCIAS DE BENT .....	53
3.3.2.2.1 INTRODUÇÃO.....	53
3.3.2.2.2 FILOSOFIA DA CONSTRUÇÃO .....	56
4 MÉTODOS DE SIMULAÇÃO.....	58
4.1 DIAGRAMAS DE CONSTRUÇÃO DE SEQÜÊNCIAS .....	58
4.1.1 SMC .....	59
4.1.2 GOLD .....	60
4.1.3 GOLD LIKE .....	61
4.1.4 GOLD - BCH DUAL.....	62
4.1.5 KASAMI PEQUENO.....	63
4.1.6 KASAMI GRANDE.....	64
4.1.7 HADAMARD.....	65
4.1.8 GMW .....	66
4.1.9 BENT.....	67
4.2 PROCEDIMENTOS E RESULTADOS PARA AS SIMULAÇÕES.....	68
4.2.1 SMC .....	68
4.2.1.1 PROPRIEDADES GERAIS.....	68

4.2.1.2 PROPRIEDADES DE CORRELAÇÃO PERIÓDICA .....	74
4.2.2 GOLD .....	87
4.2.2.1 PROPRIEDADES GERAIS.....	87
4.2.3 GOLD LIKE .....	94
4.2.4 GOLD BCH DUAL.....	98
4.2.5 KASAMI PEQUENO.....	101
4.2.6 KASAMI GRANDE.....	104
4.2.7 GMW .....	107
4.2.8 SEQÜÊNCIAS DE BENT.....	111
4.3 CRITÉRIO PARA A SELEÇÃO DE SEQÜÊNCIAS EM SISTEMAS	
ASSÍNCRONOS .....	114
4.3.1 INTRODUÇÃO.....	114
4.3.2 DETERMINAÇÃO DE UMA QUANTIDADE DE SEQÜÊNCIAS A	
SER PROCURADA .....	114
4.3.3 SIMULATED ANNEALING.....	116
4.3.3.1 INTRODUÇÃO .....	116
4.3.3.2 DESCRIÇÃO .....	116
4.3.3.3 CONSIDERAÇÕES.....	119
4.3.4 TABELA COMPARATIVA DE SEQÜÊNCIAS .....	123
4.3.5 CONCLUSÕES .....	126
ANEXO .....	127
REFERÊNCIAS BIBLIOGRÁFICAS.....	146
APÊNDICE .....	151

## **1 INTRODUÇÃO**

### **1.1 OBJETIVO**

O objetivo principal deste trabalho é o de apresentar as principais famílias de seqüências de códigos utilizadas em sistemas de comunicação por espalhamento espectral (SS-Spread Spectrum), descrevendo suas propriedades e características, bem como a forma de construção e critérios de análise e seleção de seqüências.

### **1.2 DESCRIÇÃO DO DESENVOLVIMENTO DO TRABALHO**

O trabalho inicia-se com uma descrição dos princípios de funcionamento de um sistema de comunicação por espalhamento espectral, onde é destacado o alvo de interesse principal, neste caso o estudo das seqüências de código empregadas na etapa de espalhamento. Adotou-se para tanto o sistema SS de seqüência direta (DS).

Sobre as seqüências de código, descreve-se a sua influência sobre o processo de transmissão de dados, onde são examinadas as características especiais conferidas ao sistema devidas ao espalhamento, tais como imunidade à ruído, multiplexação em código (CDMA) etc. Descrito o funcionamento do sistema e caracterizada a importância das seqüências no mesmo, inicia-se o estudo de seqüências binárias, sendo inicialmente abordados os princípios gerais destacando-se as características intrínsecas das mesmas, para em seguida buscar-se aquelas que são relevantes ao sistema mencionado anteriormente.

Abordados os tópicos principais relativos às seqüências binárias, inicia-se o desenvolvimento de processos de construção das famílias de seqüências mais conhecidas. Esses processos de construção foram realizados com o auxílio do software *Mathematica*.

Com as famílias construídas é feita uma verificação das propriedades teóricas através de simulações em computador por meio de programas especialmente desenvolvidos neste trabalho.

## **1.3 DESCRIÇÃO DOS CAPÍTULOS**

### **Capítulo 2**

Princípios de Comunicação por Espalhamento Espectral.

Neste item é descrito o funcionamento de sistemas SS dando-se enfoque maior aos de sequência direta.

Sistemas CDMA

Descrevem-se os princípios básicos de um sistema CDMA/DS assíncrono

### **Capítulo 3**

Sequências Binárias

Princípios Gerais

Em linha gerais são exibidas as características das sequências binárias, enfocando-se em seguida aquelas mais utilizadas na aplicação de comunicação por espalhamento espectral.

Famílias

São expostos os meios de construção das famílias com suas características principais e, finalmente, alguns métodos para a seleção de sequências a serem utilizadas num dado sistema.

### **Capítulo 4**

São desenvolvidos todos os programas utilizados neste trabalho, juntamente com os comentários necessários a compreensão dos mesmos.

### **Anexo**

Neste anexo são apresentados, de forma resumida, os programas desenvolvidos para as simulações realizadas.

### **Referências Bibliográficas**

Neste item são apresentadas as referências utilizadas ao longo do texto e as referências recomendadas para um aprofundamento em certos tópicos.

### **Apêndice**

No apêndice são apresentados alguns elementos de álgebra e resultados adicionais sobre a decimação de seqüências.

## **1.4 RESULTADOS ALCANÇADOS/CONTRIBUIÇÕES**

Neste trabalho foi alcançado o objetivo de fornecer um texto, entre os raros em nosso idioma, sobre seqüências de códigos para uso em comunicação por espalhamento espectral.

Os códigos mais conhecidos foram expostos e foram criados algoritmos que possibilitam um estudo amplo das relações entre as famílias de códigos e o desempenho dos mesmos em sistemas de comunicação por espalhamento espectral de seqüência direta assíncronos.

## 2 SISTEMAS DE COMUNICAÇÃO SPREAD SPECTRUM (SS)

### 2.1 PRINCÍPIOS<sup>1</sup>

Um sistema de comunicação por Espalhamento Espectral<sup>2</sup> (Spread Spectrum-SS) de sequência direta (Direct Sequence-DS), consiste na modulação de uma portadora por uma sequência de código digital, cuja taxa de bits é muito superior a da informação. Esta modulação provoca um aumento da banda utilizada pelo sinal durante a transmissão da informação. Este processo de alargamento da banda confere propriedades especiais ao sistema, entre as quais destacam-se: uma alta imunidade a ruídos e a interferências intencionais; uma baixa probabilidade de interceptação e a possibilidade de multiplexação por divisão em código.

As primeiras propriedades conferem confiabilidade, segurança e sigilo aos dados transmitidos, isto por si só, torna a utilização deste método recomendável a uma larga classe de sistemas de transmissão, enquanto que a última propicia um melhor aproveitamento do espectro de frequências. Isto se deve a sua possível aplicação em sistemas de múltiplo acesso. O CDMA<sup>3</sup> (Code Division Multiple Access) é um método de multiplexação por divisão em código onde tem-se vários usuários ocupando simultaneamente a mesma banda. Isto é possível porque os dados de cada usuário são espalhados de tal forma que a soma das interferências de todos os demais usuários sobre um em particular pode ser tornada tolerável. A figura 2.1 ilustra o princípio de funcionamento do sistema para um único usuário.

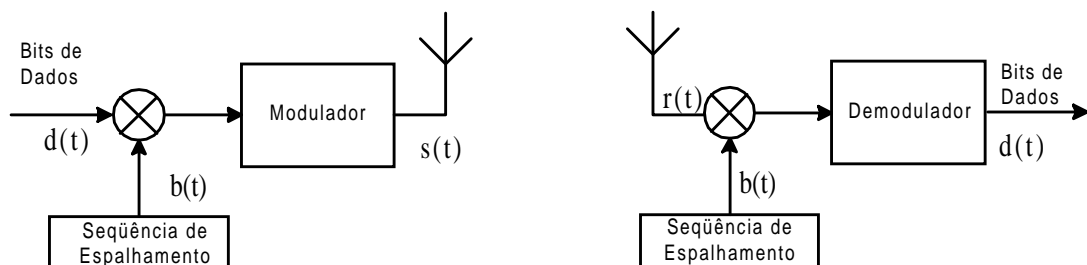


Fig. 2.1 Princípio de funcionamento do sistema Spread Spectrum

Os dados  $d(t)$  são multiplicados pela sequência de espalhamento  $b(t)$ , o que acarreta o espalhamento ou alargamento da banda, e o resultado deste produto é então modulado para a transmissão. No receptor o sinal de entrada  $r(t)$  é multiplicado por  $b(t)$ , com o que seu efeito de espalhamento desaparece e o sinal retorna ao seu estado original. Constata-se ainda que eventuais interferências na entrada do receptor serão espalhadas pelo código local  $b(t)$  atenuando o seu efeito nocivo sobre a recepção. Na figura 2.2 à esquerda, exibe-se o esboço do espectro de  $d(t)$  antes de ser multiplicado por  $b(t)$  e à direita o espectro após a multiplicação (escalas normalizadas).

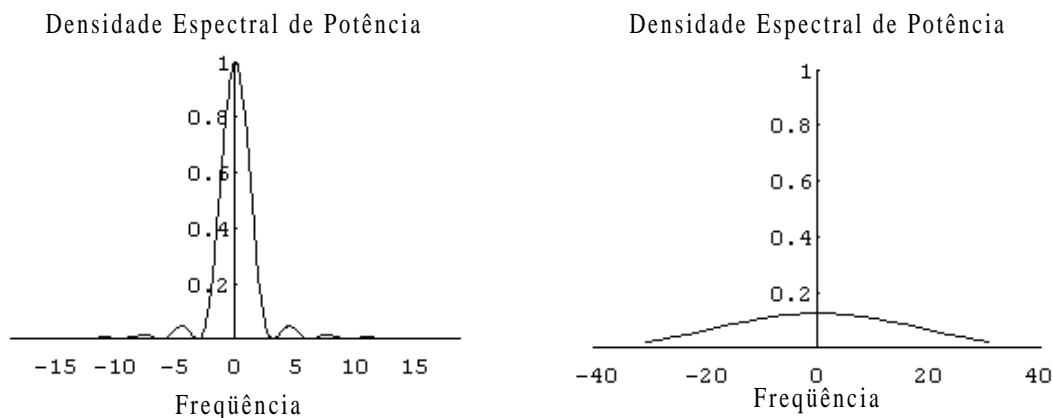


Fig. 2.2 Efeito do espalhamento-Alargamento da banda.

O processo de modulação é independente da sequência; por este motivo a técnica de Espalhamento Espectral pode ser associada a diversos métodos de modulação (como por exemplo, BPSK, QPSK, MSK etc). Existem ainda outras técnicas de espalhamento espectral, das quais destacam-se:

- Frequency Hopping (FH/SS): que consiste em deslocamentos da frequência da portadora por incrementos discretos seguindo um padrão governado por uma sequência de código. Assim o transmissor salta de uma frequência para outra, dentro de um conjunto previamente determinado, sendo a ordem com que uma frequência é utilizada determinada pela sequência de código adotada.

- Time Hopping (TH/SS): muito similar aos sistemas de modulação pulsada esta técnica consiste basicamente na utilização de uma seqüência de código que determinará instantes para as transmissões por surtos.

Alguns sistemas utilizam ainda uma forma híbrida combinando pelo menos duas das três formas vistas (DS, FH e TH). As principais aplicações de sistemas SS estão ligadas, originariamente, às comunicações táticas militares anti-interferência. O seu uso em atividades civis vem crescendo em setores como, por exemplo, o da telefonia celular, o de localização de móveis através de satélites etc.

Neste trabalho apresenta-se um estudo das principais seqüências binárias utilizadas por esta técnica de transmissão. Para este estudo o método utilizado foi o DS, por ser o mais largamente utilizado.

## 2.2 IMUNIDADE À INTERFERÊNCIAS NUM SISTEMA TIPO DS/SS

A principal característica de sistemas SS é a sua imunidade a interferências, sejam estas intencionais ou não. As interferências intencionais caracterizam-se por sinais de potência finita elevada, numa determinada posição do espectro do sinal transmitido, para assegurar que as mesmas causarão falhas na recepção. Este tipo de interferência pode ter um efeito destrutivo grande na demodulação do sinal útil. Em sistemas tipo SS, há uma certa imunidade a este tipo de interferência.

Considere-se um meio de transmissão com D sinais equiprováveis, de mesma energia, representados num espaço N-dimensional tal que:

$$s_i(t) = \sum_{k=1}^N s_{i,k} \cdot \psi_k(t) \quad 1 \leq i \leq D; 0 \leq t \leq T \quad (2.1)$$

onde:

$$s_{i,k} = \int_0^T s_i(t) \psi_k(t) dt \quad (2.2)$$

e

$\{\psi_k(t); 1 \leq k \leq N\}$  é uma base ortonormal, isto é:

$$\int_0^T \psi_n(t) \psi_m(t) dt = \delta_{n,m} \stackrel{\Delta}{=} \begin{cases} 1 & n = m \\ 0 & n \neq m \end{cases} \quad (2.3)$$

A energia média de um sinal é calculável por:

$$\int_0^T s_i^2(t) dt = \sum_{k=1}^N s_{i,k}^2 = E_s; \quad 1 \leq i \leq D \quad (2.4)$$

Sinais interferentes intencionais, denominados de "jammer", podem ser escritos na forma:

$$J(t) = J_{out}(t) + \sum_{k=1}^N J_k \psi_k(t); \quad 0 \leq t \leq T \quad (2.5)$$

onde  $J_{out}(t)$  representa a parte do sinal não representável no espaço de sinais considerado (isto é, ortogonal aos vetores da base). O sinal  $J(t)$  é independente dos sinais desejados e tem por finalidade corromper a informação transmitida. A energia da interferência efetiva é dada por:

$$\int_0^T [J(t) - J_{out}(t)]^2 dt = \sum_{k=1}^N J_k^2 \equiv E_J \quad (2.6)$$

O sinal na entrada no receptor, num ambiente contaminado pela presença de um "jammer", é dado por:

$$r(t) = s_i(t) + J(t) \quad (2.7)$$

Este sinal é correlacionado com o conjunto de  $D$  sinais conhecidos no receptor. Na saída do  $i$ -ésimo correlator ter-se-á:

$$U_i \equiv \int_0^T r(t) \cdot s_i(t) dt = \sum_{k=1}^N (s_{i,k}^2 + J_k s_{i,k}) \quad (2.8)$$

A esperança condicionada deste sinal, será dada por:

$$E(U_i | s_i) = \sum_{k=1}^N s_{i,k}^2 = E_s \quad (2.9)$$

pois supondo os sinais equiprováveis e de mesma energia, pode-se escrever:

$$E(U_i) = \frac{E_s}{D} \quad (2.10)$$

e assim o segundo termo de  $U_i$  possui média zero. Analogamente, obtém-se o seguinte resultado para a variância:

$$\text{var}(U_i | s_i) = \sum_{k,\ell} J_k J_\ell s_{i,k} s_{i,\ell} = \sum_{k=1}^N J_k^2 s_{i,k}^2 = \frac{E_s}{N} E_J \quad (2.11)$$

e portanto:

$$\text{var}(U_i) = \frac{E_s}{N \cdot D} E_J \quad (2.12)$$

Uma possível medida de desempenho é a relação sinal/ruído, definida por:

$$\text{SNR} = \frac{E^2(U)}{\text{var}(U)} = \frac{E_s}{E_J} \times \frac{N}{D} \quad (2.13)$$

Este resultado é independente da maneira como o "jammer" distribui sua energia pelo espectro. O termo  $N/D$  na equação acima é denominado de ganho de processamento e pode ser escrito em função da banda como<sup>1</sup>:

$$G_P = \frac{N}{D} \cong \frac{2B_{ss}T}{2B_D T} = \frac{B_{ss}}{B_D} \quad (2.14)$$

onde  $B_{ss}$  é a largura de banda do sinal SS e  $B_D$  é a largura necessária para transmitir-se o sinal de dados sem espalhamento. Ilustra-se na figura 2.3 a seguir o processo descrito.

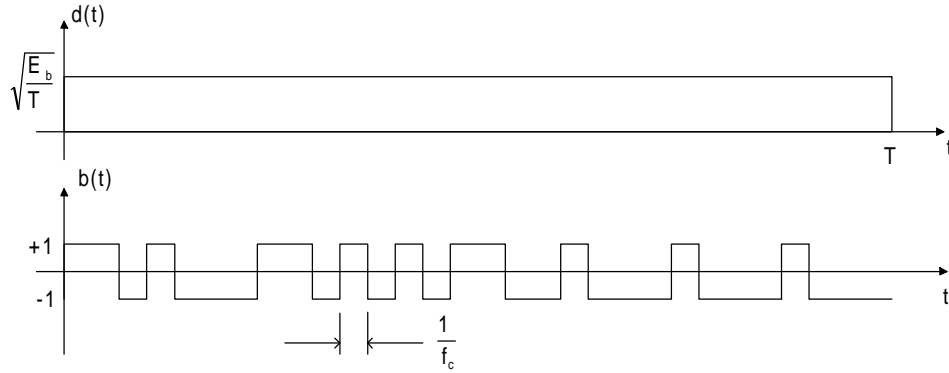


Fig. 2.3 Sinal de dados e seqüência de espalhamento

O sinal recebido na presença de um "jammer", em banda base, é:

$$r(t) = d(t).c(t) + J(t), \quad 0 \leq t \leq T, \quad (2.15)$$

O receptor de correlação para o bit considerado realiza a operação:

$$U = \int_0^T r(t).c(t)dt \quad (2.16)$$

O integrando pode ser expandido para uma melhor visualização do processo.

$$r(t).c(t) = d(t).c^2(t) + J(t).c(t) = d(t) + J(t).c(t) \quad (2.17)$$

pois quando  $b(t)$  é multiplicado por si mesmo (o que pressupõe o sincronismo estabelecido) sua influência desaparece sobre o sinal de dados; no entanto ele passa a influenciar o sinal interferente  $J(t)$  fazendo com que o espectro deste seja espalhado e consequentemente sua interferência nociva atenuada. Para a probabilidade de erro de um símbolo pode-se escrever:

$$P_s = \sum_{k=1}^D P(s_k)P(\epsilon/s_k) \quad (2.18)$$

onde  $P(\epsilon/s_k)$  representa a probabilidade de erro do símbolo  $s_k$ , condicionada à sua transmissão. No caso de mensagens equiprováveis esta expressão simplifica-se para:

$$P_s = \frac{1}{D} \sum_{k=1}^D P(\epsilon/s_k) \quad (2.19)$$

Admitindo-se que todos os símbolos tenham a mesma probabilidade de erro, esta última expressão simplifica-se para  $P(\varepsilon/s_k)$ . Considerando-se um caso binário, quando um símbolo equivale a um bit de informação e portanto  $E_b=E_s$ , uma fórmula simplificada para o cálculo da probabilidade de erro de um símbolo, onde são considerados o teorema do limite central, a dimensão do espaço  $N$  como sendo grande, e uma aproximação Gaussiana, é dada por:

$$P_e = P(U < 0) \cong Q\left(\sqrt{\frac{E_b}{E_j} \cdot \frac{N}{D}}\right) \quad (2.20)$$

onde  $E_b$  é a energia de bit de informação,  $E_j$  é a energia do sinal interferente e  $N$  o comprimento da seqüência de espalhamento (também dimensão do espaço vetorial) e a função  $Q(.)$  é calculável por:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \cdot \int_x^{\infty} e^{-y^2/2} dy \quad (2.21)$$

Esta aproximação evidencia o fato de que, quanto maior a dimensão da seqüência de espalhamento utilizada, maior será a imunidade do sistema em relação às interferências. Esta característica está portanto diretamente ligada ao ganho de processamento do sinal e, conseqüentemente, à relação entre bandas. Nos exemplos aqui considerados os códigos utilizados para o espalhamento estavam em perfeito sincronismo, tanto em frequência quanto em fase. Os problemas oriundos da falta de sincronismo não são objeto de estudo neste trabalho.

## 2.3 SISTEMAS CDMA

### 2.3.1 INTRODUÇÃO

Com a necessidade crescente de ampliação da faixa para as rádio-comunicações e os limites tecnológicos atuais para a sua ampliação, os sistemas multiusuário ganham atualmente destaque. Neste contexto sistemas CDMA são promissores e estão sendo considerados para utilização em diversas aplicações, como a telefonia móvel, redes de transmissão de dados, entre outros.

Sistemas CDMA são aqueles nos quais vários usuários são multiplexados por código, isto é, cada um possui sua sequência binária própria e é através desta que o receptor poderá identificá-lo e extrair a informação enviada. A principal característica deste método de transmissão é a possibilidade de termos vários usuários utilizando um mesmo meio de comunicação, numa mesma frequência simultaneamente e isto é possível devido ao espalhamento realizado pelo código utilizado. Assim a eventual interferência provocada pelos outros sinais presentes no receptor é atenuada a níveis aceitáveis.

Outros sistemas de múltiplo acesso utilizados são o FDMA (Frequency Division Multiple Access) e o TDMA (Time Division Multiple Access). Em sistemas FDMA os usuários do sistema transmitem simultaneamente, porém em bandas de frequência disjuntas, enquanto que no TDMA os usuários ocupam a mesma banda, no entanto transmitem sequencialmente no tempo. Os sistemas de múltiplo acesso estão atualmente sendo utilizados também em redes de dados locais (LAN's de cabos coaxiais, fibras ópticas, rádio frequência etc). Pode-se citar como exemplos: CD-CSMA (Code Division Carrier Sense Multiple Access); ALOHA DS/SSMA que é um sistema que transmite por pacotes; CDMA-Óptico via códigos opticamente ortogonais (OOC-Optical Orthogonal Codes) etc.

### 2.3.2 SISTEMAS CDMA-DS/SS ASSÍNCRONOS<sup>3, 4</sup>

Num sistema CDMA-DS/SS vários sinais assíncronos ocupam simultaneamente o mesmo canal. Cada sinal emprega uma sequência de assinatura (código de espalhamento) distinta dos demais usuários do sistema. Esta sequência é escolhida de tal forma que possua certas propriedades de correlação desejáveis, como por exemplo uma correlação fora de fase muito pequena quando comparada com a de fase. Existem algumas famílias de códigos que possuem esta propriedade, entre outras, o que vem a incrementar o desempenho do sistema e serão detalhadas posteriormente. O principal objetivo de sistemas desta classe é de ser capaz de separar os sinais SS no receptor, embora estes ocupem simultaneamente a mesma banda.

Neste item descrever-se-á os princípios básicos deste sistema, exemplificando com os meios de comunicação mais usuais; por fim, coloca-se em evidência uma abordagem mais detalhada para a medida de desempenho do sistema. Na modulação em sequência binária direta por espalhamento espectral, o sinal de banda básica tem a forma:

$$x(t) = \sum_{j=-\infty}^{\infty} x_j \psi(t - jT_c) \quad (2.22)$$

onde  $\{x_j\}$  representa uma sequência periódica binária, cujos elementos pertencem à  $\{+1, -1\}$ ,  $\psi(\cdot)$  é um sinal limitado no intervalo  $[0, T_c]$ , no qual vale a relação normalizante:

$$\frac{1}{T_c} \int_0^{T_c} \psi^2(t) dt = 1 \quad (2.23)$$

A forma mais comum para o sinal  $\psi$  é a de um pulso retangular de duração igual a  $T_c$ . Esta forma de onda é designada como forma de onda do chip.

$$\psi(t) = p_{T_c}(t) = \begin{cases} 1, & 0 < t \leq T_c \\ 0, & \text{caso contrário.} \end{cases} \quad (2.24)$$

Outras formas de onda podem ser utilizadas e é o que ocorre por exemplo na modulação MSK (Minimum Shift Keying) onde é utilizado um pulso senoidal que também obedece a relação (2.23). A forma de onda deve ser adotada em conformidade com o processo de modulação utilizado. Neste trabalho será utilizado o sistema de modulação PSK (Phase Shift Keying) e a forma de onda adotada será a de um pulso retangular. Um sinal de dados binário é representável pela equação:

$$b(t) = \sum_{\ell=-\infty}^{\infty} b_{\ell} p_T(t - \ell T) \quad (2.25)$$

onde  $p_T(t)$  é um pulso retangular de duração  $T$  e  $d = b_{\ell}$  é uma seqüência binária de dados pertencentes a  $\{+1, -1\}$  para todo  $j$ .

A seqüência  $b = \{b_j\}$  em (2.22) é a seqüência de assinatura, que possui período igual a  $N$ , inteiro, e satisfaz portanto à condição  $b_j = b_{j+N}$ . A duração de um bit de dados será  $T = NT_c$ . Assim a faixa ocupada pelo sinal transmitido em banda base,  $s(t) = d(t) \cdot b(t)$ , é  $N$  vezes maior que a do sinal de dados  $d(t)$ .

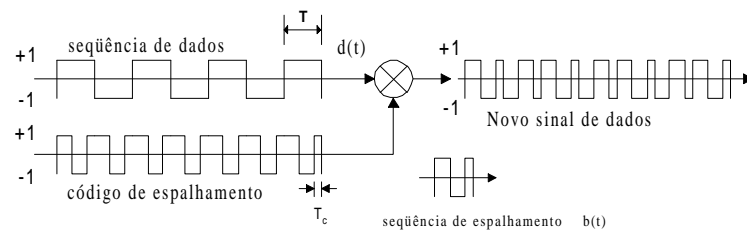


Fig. 2.4 Multiplicação da seqüência de dados pela de Espalhamento

Na figura 2.4 representa-se o sinal de dados  $d(t)$  e o código de espalhamento  $b(t)$  (neste caso  $N=5$  e a saída é a multiplicação dos dois sinais antes da modulação). O sinal SS em seqüência direta transmitido tem a seguinte forma:

$$s(t) = A x(t) b(t) \cos(\omega_c t + \theta) \quad (2.26)$$

onde  $\omega_c$  é a frequência da portadora e  $\theta$  uma fase arbitrária. Num sistema CDMA com K-usuários há K equações como esta e assim pode-se escrever para o k-ésimo usuário:

$$s_k = A a_k(t) b_k(t) \cos(\omega_c t + \theta_k) \quad (2.27)$$

onde  $k \in \{1, 2, \dots, K\}$  e  $b_k$  é a assinatura do k-ésimo usuário (o  $b(t)$  específico). As fases dos sinais são diferentes pois os transmissores não estão em sincronismo, em princípio. No receptor do sistema são recebidos simultaneamente os K sinais, mais um AWGN (Additive White Gaussian Noise), além de haver um atraso entre os vários sinais.

A figura 2.5 ilustra o modelamento adotado para o sistema e a partir deste pode-se estabelecer o equacionamento correspondente.

$$r(t) = n(t) + \sum_{k=1}^K s_k(t - \tau_k) \quad (2.28)$$

onde  $n(t)$  é um AWGN com densidade espectral  $N_0/2$  e  $\tau_k$  é o atraso relativo do k-ésimo sinal. Substituindo (2.27) em (2.28) obtém-se:

$$r(t) = n(t) + \sum_{k=1}^K A_k a_k(t - \tau_k) b_k(t - \tau_k) \cos(\omega_c t - \phi_k) \quad (2.29)$$

onde  $\phi_k = \theta_k + \omega_c \tau_k$  e  $A_k$  representa a amplitude do sinal. Sem perda de generalidade, assumir-se-á que o atraso relativo ao usuário  $i$  e o seu respectivo ângulo de fase são nulos. Isto significa que para este usuário há um perfeito sincronismo, implicando que em (2.29)  $\tau_i = \phi_i = 0$ , e consequentemente os atrasos e diferenças de fases dos demais usuários serão referidos a este. Ademais, para evitar-se o "near-far problem", assumir-se-á também que as amplitudes  $A_k$  na entrada do receptor são constantes e assim  $A_k = A$  no que se segue.

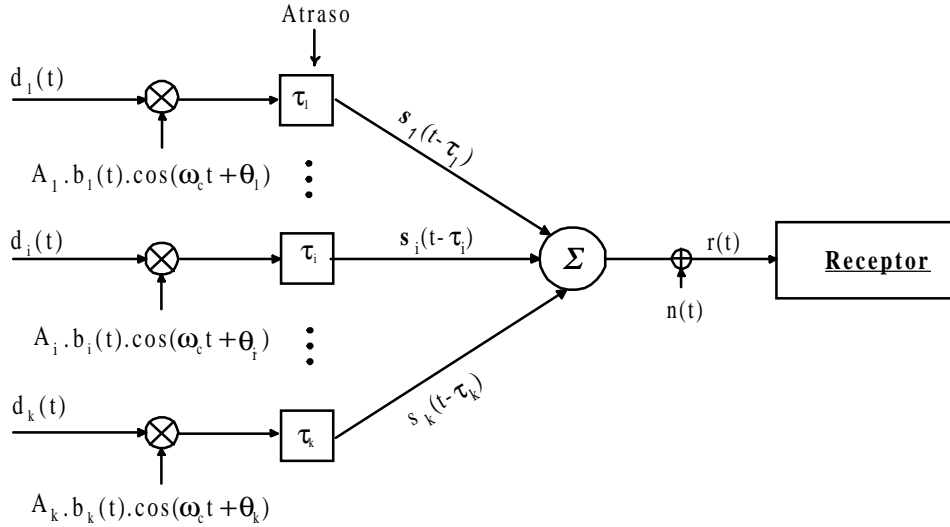


Fig. 2.5 Representação de um sistema CDMA assíncrono.

O receptor de correlação está sincronizado para captar a informação de um sinal  $i$  específico, para tanto deverá selecionar o código correspondente a este sinal e multiplicá-lo pelo sinal  $r(t)$  à entrada do sistema, resultando na saída:

$$Z_i = \int_0^T r(t) a_i(t) \cos(\omega_c t) dt \quad (2.30)$$

pois foi assumido  $\varphi_i = \tau_i = 0$ . Substituindo (2.28) em (2.30) segue-se:

$$Z_i = \eta_i + \sum_{k=1}^K \int_0^T s_k(t - \tau_k) a_i(t) \cos(\omega_c t) dt \quad (2.31)$$

onde a primeira parcela de (2.31) é uma variável aleatória devida ao ruído, descrita por:

$$\eta_i = \int_0^T n(t) a_i(t) \cos(\omega_c t) dt \quad (2.32)$$

Se  $\omega_c \gg T^{-1}$  (frequência da portadora e do dado, respectivamente) pode-se ignorar as componentes de frequências múltiplas da fundamental (harmônicas), resultantes da integração efetuada em (2.30). Assim, levando estes fatores em consideração ao substituir-se (2.27) em (2.31) resulta:

$$Z_i = \eta_i + \frac{1}{2} A \int_0^T b_i(t) dt + \sum_{\substack{k=1 \\ k \neq i}}^K \frac{1}{2} A [f_{k,i}(\tau_k) + \hat{f}_{k,i}(\tau_k)] \cos(\varphi_k) \quad (2.33)$$

onde as funções  $f_{k,i}$  e  $\hat{f}_{k,i}$  são definidas por.

$$f_{k,i}(\tau) = \int_0^\tau b_k(t - \tau) a_k(t - \tau) a_i(t) dt \quad (2.34)$$

$$\hat{f}_{k,i}(\tau) = \int_\tau^T b_k(t - \tau) a_k(t - \tau) a_i(t) dt \quad (2.35)$$

Nestas duas últimas expressões, o fator  $d_k$  representa um bit da seqüência de dados do usuário interferente, nos intervalos de  $0 < t \leq \tau$  e  $\tau < t \leq T$ , sendo que o valor de  $d_k$  não pode variar nestes intervalos. Em função desta observação as fórmulas podem ser reescritas da seguinte forma:

$$f_{k,i}(\tau) = b_{-1}^{(k)} \int_0^\tau a_k(t - \tau) a_i(t) dt \quad (2.36)$$

$$\hat{f}_{k,i}(\tau) = b_0^{(k)} \int_\tau^T a_k(t - \tau) a_i(t) dt \quad (2.37)$$

onde  $b_{-1}^{(k)}$  e  $b_0^{(k)}$  representam, respectivamente, o valor do bit da seqüência  $k$  no primeiro e segundo subintervalos de integração do dado  $b_0^{(i)}$  a ser demodulado. Com a observação destas funções, sobressai o interesse pelas seguintes:

$$R_{k,i}(\tau) = \int_0^\tau a_k(t - \tau) a_i(t) dt \quad (2.38)$$

$$\hat{R}_{k,i}(\tau) = \int_\tau^T a_k(t - \tau) a_i(t) dt \quad (2.39)$$

Estas são conhecidas como funções de correlação cruzada parciais de tempo contínuo. O efeito da interferência normalizada do usuário  $k$  sobre o usuário  $i$  pode ser calculado através da expressão:

$$I_{k,i}(\underline{b}_k, \tau, \varphi) = T^{-1} [b_{-1}^{(k)} R_{k,i}(\tau) + b_0^{(k)} \hat{R}_{k,i}(\tau)] \cos(\varphi) \quad (2.40)$$

onde  $\underline{b}_k = (b_{-1}^{(k)}, b_0^{(k)})$  representa um vetor de dois bits de dados consecutivos da informação transmitida pelo  $k$ -ésimo sinal interferente. A fórmula (2.33) pode ser escrita agora como:

$$Z_i = \eta_i + \frac{1}{2}AT\{b_0^{(i)} + \sum_{\substack{k=1 \\ k \neq i}}^K I_{k,i}(\underline{b}_k, \tau_k, \varphi_k)\} \quad (2.41)$$

A primeira parcela é devida ao AWGN; a segunda é o sinal que se deseja demodular e a última representa a interferência de múltiplo acesso dos  $K-1$  usuários adicionais do sistema sobre o  $i$ -ésimo usuário. A dificuldade principal inerente a este sistema é a interferência de múltiplo acesso que deve ser minimizada a níveis aceitáveis para um bom desempenho. Devido a isso há um maior interesse no estudo da última parcela de (2.41). Afim de simplificar a notação escrever-se-á para a interferência total de múltiplo acesso:

$$V_{k,i} = \sum_{\substack{k=1 \\ k \neq i}}^K I_{k,i}(\underline{b}_k, \tau_k, \varphi_k) \quad (2.42)$$

Nos receptores de correlação a decisão de qual pulso foi enviado (se positivo ou negativo) é realizada através da observação de  $Z_i$  no instante  $t=T$ ; isto é, se  $Z_i > 0$  o receptor decide que um pulso positivo foi enviado, caso contrário decide pelo negativo.

A medida de desempenho considerada é a probabilidade de erro de bit. Posteriormente escrever-se-á esta probabilidade como uma função gaussiana da relação sinal/ruído (SNR), que será dependente da correlação cruzada discreta entre as seqüências, afim de exibir como se pode otimizar o desempenho do sistema através da seleção criteriosa dos códigos de espalhamento:

$$Q(\text{SNR}) = \frac{1}{\sqrt{2\pi}} \int_{\text{SNR}}^{\infty} e^{-y^2/2} dy \quad (2.43)$$

### 2.3.3 ANÁLISE DA INTERFERÊNCIA DE MÚLTIPLO ACESSO

A análise será efetuada através da equação (2.40), que mede a interferência de um usuário  $k$  qualquer sobre um usuário  $i$  específico. Define-se como correlação cruzada periódica de tempo contínuo à função:

$$\mathfrak{R}_{k,i}(\tau) = \int_0^T a_k(t - \tau) a_i(t) dt \quad (2.44)$$

Assume-se que o tempo de um chip  $T_C$  é submúltiplo do período  $T$  do sinal de dados, isto é,  $T = NT_C$  com  $N$  representando o número de chips da sequência e que o atraso  $\tau$  é tal que  $-\infty < \tau < \infty$ ; assim  $\mathfrak{R}_{k,i}(\tau) = \int_0^T a_k(t - \tau) a_i(t) dt$ . Comparando-se (2.44) com as equações de correlação cruzada parcial de tempo contínuo (2.38) e (2.39) tem-se a relação:

$$\hat{R}_{k,j}(\tau) + R_{k,j}(\tau) = \int_0^T a_k(t - \tau) a_i(t) dt = \mathfrak{R}_{k,i}(\tau) \quad 0 < \tau \leq T \quad (2.45)$$

Retornando-se à equação (2.40), que permite calcular a interferência de um usuário sobre o outro, pode-se estabelecer os seguintes casos:

$$b_0^{(k)} = b_{-1}^{(k)} \quad (2.46)$$

Para este caso a (2.40) simplifica-se para:

$$I_{k,i}(\underline{b}_k, \tau, \varphi) = [T^{-1} b_0^{(k)} \cos(\varphi)] \mathfrak{R}_{k,i}(\tau) \quad (2.47)$$

Desta forma pode-se obter um limite máximo para a interferência:

$$|I_{k,i}(\underline{b}_k, \tau, \varphi)| \leq |I_{k,i}(\underline{b}_k, \tau, 0)| = T^{-1} |\mathfrak{R}_{k,i}(\tau)| \quad (2.48)$$

Seguindo o mesmo raciocínio quando:

$$b_0^{(k)} \neq b_{-1}^{(k)} \quad (2.49)$$

$$I_{k,i}(\underline{b}_k, \tau, \varphi) = [T^{-1} b_0^{(k)} \cos(\varphi)] \{ \hat{R}_{k,i}(\tau) - R_{k,i}(\tau) \} \quad (2.50)$$

O último fator desta expressão é definido como função de auto correlação cruzada ímpar de tempo contínuo:

$$\hat{\mathfrak{R}}_{k,i}(\tau) = \hat{R}_{k,i}(\tau) - R_{k,i}(\tau), \quad 0 \leq \tau \leq T \quad (2.51)$$

e obedece a seguinte relação:

$$\hat{\mathfrak{R}}_{k,i}(\tau) = -\hat{\mathfrak{R}}_{k,i}(T - \tau) \quad (2.52)$$

Analogamente para a função  $\mathfrak{R}_{k,i}(\tau)$  tem-se:

$$\mathfrak{R}_{k,i}(\tau) = \mathfrak{R}_{k,i}(T - \tau) \quad (2.53)$$

Retornando para a interferência de múltiplo acesso, neste caso a equação (2.40) terá uma forma análoga ao caso anterior, como se segue:

$$I_{k,i}(\underline{b}_k, \tau, \varphi) = [T^{-1} \cdot b_0^{(k)} \cos(\varphi)] \hat{\mathfrak{R}}_{k,i}(\tau) \quad (2.54)$$

Em consequência, o limite para este caso pode ser escrito como:

$$|I_{k,i}(\underline{b}_k, \tau, \varphi)| \leq |I_{k,i}(\underline{b}_k, \tau, 0)| = T^{-1} |\hat{\mathfrak{R}}_{k,i}(\tau)| \quad (2.55)$$

Neste cálculo determinou-se os limites com relação a variável  $\varphi$ . Analisam-se a seguir estes limites para a interferência de múltiplo acesso devido à variável  $\underline{d}_k$  referida na equação (2.40).

$$\begin{aligned} \max \left\{ |I_{k,i}(\underline{b}_k, \tau, \varphi)| \right\} &= T^{-1} |\cos(\varphi)| \cdot \max \left\{ |\mathfrak{R}_{k,i}(\tau)|, |\hat{\mathfrak{R}}_{k,i}(\tau)| \right\} \\ &= T^{-1} |\cos(\varphi)| \cdot \left\{ |\hat{R}_{k,i}(\tau)| + |R_{k,i}(\tau)| \right\} \end{aligned} \quad (2.56)$$

Assim, se  $R_{k,i}$  e  $\hat{R}_{k,i}$  possuírem o mesmo sinal, tem-se o primeiro caso descrito anteriormente, caso contrário tem-se o segundo.

Analisando o vetor  $\underline{b}_k$  pode-se também determinar um limite inferior para a interferência, dado pela seguinte equação:

$$I_{k,i}(\underline{b}_k, \tau, \varphi) = -T^{-1} \cdot |\cos(\varphi)| \cdot \left\{ \left| \hat{R}_{k,i}(\tau) \right| + \left| R_{k,i}(\tau) \right| \right\} \quad (2.57)$$

Comparando-se agora as duas análises, isto é, aquela referente à  $\varphi$  e ao vetor  $\underline{b}_k$  obter-se-á a seguinte relação para a interferência de múltiplo acesso entre usuários:

$$-T^{-1} \cdot \left\{ \left| \hat{R}_{k,i}(\tau) \right| + \left| R_{k,i}(\tau) \right| \right\} \leq I_{k,i}(\underline{b}_k, \tau, \varphi) \leq T^{-1} \cdot \left\{ \left| \hat{R}_{k,i}(\tau) \right| + \left| R_{k,i}(\tau) \right| \right\} \quad (2.58)$$

Observe-se que adotou-se  $|\cos(\varphi)|=1$

(isto é,  $I_{k,i}(\underline{b}_k, \tau, \varphi) = -T^{-1} \cdot |\cos(\varphi)| \cdot \left\{ \left| \hat{R}_{k,i}(\tau) \right| + \left| R_{k,i}(\tau) \right| \right\}$ ) e que esta relação (2.58) é válida para todo  $\tau$ .

Com esta análise determinam-se os limites para a interferência de múltiplo acesso, como função do argumento. A última etapa da análise será baseada nas funções de correlação cruzada, onde tem-se uma gama maior de condições a serem levadas em consideração. Em síntese, os resultados para a máxima interferência de múltiplo acesso entre usuários, recairão no estudo das funções a seguir. Após a determinação dos limites para esta interferência, poder-se-á determinar a probabilidade de erro máxima do sistema e consequentemente o desempenho do mesmo.

$$\mathfrak{R}_{\max}(k, i) = \max \left\{ \left| \hat{R}_{k,j}(\tau) \right| + \left| R_{k,j}(\tau) \right| : 0 \leq \tau \leq T \right\} \quad (2.59)$$

ou de outra forma:

$$\mathfrak{R}_{\max}(k, i) = \max \left\{ \left| \mathfrak{R}_{k,j}(\tau) \right|, \left| \hat{\mathfrak{R}}_{k,j}(\tau) \right| : 0 \leq \tau \leq T \right\} \quad (2.60)$$

Antes de continuar a análise de (2.59) e (2.60) serão descritos, de forma sucinta, alguns resultados adicionais.

Para o cálculo do valor médio quadrático da interferência de múltiplo acesso consideram-se os vetores  $\underline{d}_k \in [-1, 1]$  de forma equiprovável;  $\varphi_k \in [0, 2\pi[$  com uma função densidade de probabilidade (FDP) uniforme neste intervalo e  $\tau_k \in [0, T[$ , também com uma FDP uniforme. Como estas variáveis aleatórias são independentes:

$$E\{I_{k,i}(\underline{b}_k, \tau_k, \varphi_k)\} = 0 \quad (2.61)$$

Esta é a esperança da interferência de múltiplo acesso. Já para a variância pode-se escrever:

$$\begin{aligned} \sigma_{k,i}^2 &= \text{Var}\{I_{k,i}(\underline{b}_k, \tau_k, \varphi_k)\} \\ &= \frac{1}{2} T^{-3} \int_0^T [R_{k,i}^2(\tau) + \hat{R}_{k,i}^2(\tau)] d\tau \end{aligned} \quad (2.62)$$

e que depende apenas de  $\tau$ . Este valor é muito importante pois através dela pode-se calcular a relação sinal/ruído para o  $i$ -ésimo receptor, definida por:

$$\text{SNR}_i = E\{Z_i | b_0^{(i)} = +1\} \left[ \text{Var}\{Z_i | b_0^{(i)} = +1\} \right]^{-1/2} \quad (2.63)$$

Evidentemente  $I_{k,i}(\underline{b}_k, \tau_k, \varphi_k)$  não depende de  $\underline{b}_0^{(i)}$  e assim (2.41) e (2.61) implicam em:

$$E\{Z_i | b_0^{(i)} = +1\} = E\{\eta_i\} + \frac{1}{2} AT \left[ 1 + \sum_{k \neq i} E\{I_{k,i}(\underline{b}_k, \tau_k, \varphi_k)\} \right] = \frac{1}{2} AT \quad (2.64)$$

Somando-se a isso o fato de que  $I_{k,i}(\underline{b}_k, \tau_k, \varphi_k)$  e  $I_{j,i}(\underline{b}_j, \tau_j, \varphi_j)$  são independentes para  $k \neq j$ , obtém-se a variância<sup>4</sup>:

$$\begin{aligned} \text{Var}\{Z_i | b_0^{(i)} = +1\} &= \text{Var}\{\eta_i\} + \left(\frac{1}{2} AT\right)^2 \sum_{k \neq i} \text{Var}\{I_{k,i}(\underline{b}_k, \tau_k, \varphi_k)\} \\ &= \frac{1}{4} N_0 T + \frac{1}{4} A^2 T^2 \sum_{k \neq i} \sigma_{k,i}^2 \end{aligned} \quad (2.65)$$

Donde se conclui que a relação sinal ruído pode ser escrita da seguinte forma:

$$\text{SNR}_i = \left\{ \frac{N_0}{A^2 T} + \sum_{k \neq i} \sigma_{k,i}^2 \right\}^{-1/2} \quad (2.66)$$

A SNR serve como uma medida do desempenho do sistema para a maioria dos casos. Neste caso foi realizado um modelamento relativamente simples, que é atrativo devido à facilidade de seu cálculo. Estes resultados são válidos quando a forma de onda

do chip é retangular. No entanto quando isto não ocorrer as alterações serão pequenas, tendo apenas o acréscimo de um fator multiplicativo na variância e por este motivo não serão tratados aqui. Retornando à análise das funções de correlação cruzada, foi visto que para obter-se a magnitude máxima da interferência de múltiplo acesso, restava analisar a equação (2.59) e/ou (2.60), o que também dará subsídios para o cálculo da variância (2.62). As equações para a correlação cruzada parcial de tempo contínuo podem ser desenvolvidas para  $\tau = \ell T_c$ , onde  $\ell$  é um número inteiro que denotará o deslocamento entre as seqüências. Assim:

$$\begin{aligned} R_{k,i}(\ell T_c) &= \int_0^{\ell T_c} a_k(t - \ell T_c) a_i(t) dt = \\ &= \sum_{j=0}^{\ell-1} a_k(j - \ell) a_i(j) \int_0^{T_c} \psi^2(t) dt = \left\{ \sum_{j=0}^{\ell-1} a_k(j - \ell) a_i(j) \right\} T_c \end{aligned} \quad (2.67)$$

$$\begin{aligned} \hat{R}_{k,i}(\ell T_c) &= \int_{\ell T_c}^T a_k(t - \ell T_c) a_i(t) dt = \\ &= \sum_{j=\ell}^{N-1} a_k(j - \ell) a_i(j) \int_0^{T_c} \psi^2(t) dt = \left\{ \sum_{j=0}^{N-\ell-1} a_k(j) a_i(j + \ell) \right\} T_c \end{aligned} \quad (2.68)$$

Neste desenvolvimento a forma de onda do sinal foi normalizada, exibindo que ela possui uma componente multiplicativa no cálculo da interferência de múltiplo acesso. Destas equações surge a necessidade de algumas novas definições:

$$C_{k,i}(\ell) = \begin{cases} \sum_{j=0}^{N-1-\ell} a_k(j) a_i(j + \ell), & 0 \leq \ell \leq N-1 \\ \sum_{j=0}^{N-1+\ell} a_k(j - \ell) a_i(j), & 1-N \leq \ell < 0 \\ 0, & |\ell| > N \end{cases} \quad (2.69)$$

Esta expressão é conhecida como função de correlação cruzada aperiódica discreta. Analogamente desenvolvendo as expressões (2.44) e (2.51) obter-se-á as funções de correlação cruzada periódica par e ímpar discretas, que estão definidas a seguir. Assim fica evidenciada a necessidade do estudo das seqüências e suas

propriedades, pois elas interferem diretamente na magnitude da interferência de múltiplo acesso. Define-se como função de correlação cruzada periódica par à expressão:

$$\theta_{k,i}(\ell) = \sum_{j=0}^{N-1} a_k(j) a_i(j + \ell) \quad (2.70)$$

Fazendo-se uma extensão na definição de  $C_{k,i}(\ell)$ , tornando-a também periódica, verifica-se que:

$$\theta_{k,i} = C_{k,i}(\ell) + C_{k,i}(\ell - N) \quad (2.71)$$

Esta função será também denominada correlação cruzada periódica, quando não houver possibilidade de engano. Analogamente, define-se a função de correlação cruzada periódica ímpar:

$$\hat{\theta}_{k,i} = C_{k,i}(\ell) - C_{k,i}(\ell - N) \quad (2.72)$$

Estas funções para  $k=i$  recebem na sua denominação o prefixo auto, tornando-se auto correlação cruzada periódica par e ímpar respectivamente, e nestes casos na fórmula será indicado apenas um índice.

A análise da máxima interferência de múltiplo acesso é dada pelas seguintes expressões:

$$\begin{aligned} \mathfrak{R}_{\max}(k,i) &= \max \left\{ \left| \mathfrak{R}_{k,j}(\tau) \right|, \left| \hat{\mathfrak{R}}_{k,j}(\tau) \right| : 0 \leq \tau \leq T \right\} \\ &= T_c \max \left\{ \left| \theta_{k,j}(\ell) \right|, \left| \hat{\theta}_{k,j}(\ell) \right| : \ell = 0, 1, \dots, N-1 \right\} \end{aligned} \quad (2.73)$$

e

$$\begin{aligned} I_{\max}(k,i) &= \max_{\underline{b}_k} I_{k,i}(\underline{b}_k, \tau, \varphi) = T^{-1} \mathfrak{R}_{\max}(k,i) \\ &= \frac{T_c}{T} \max \left\{ \left| \theta_{k,j}(\ell) \right|, \left| \hat{\theta}_{k,j}(\ell) \right| \right\} = N^{-1} \max \left\{ \left| \theta_{k,j}(\ell) \right|, \left| \hat{\theta}_{k,j}(\ell) \right| \right\} \end{aligned} \quad (2.74)$$

Com esta última equação determina-se o pior caso, isto é, onde existiria a maior interferência no sistema. Esta forma é útil para uma avaliação rápida do desempenho do sistema, estabelecendo antecipadamente um limite máximo que poderá ser atingido. Pode-se compará-lo com o pior caso, para todos os usuários, por exemplo, para detectar-se seqüências inconvenientes. Note-se que o cálculo para esta avaliação é realizado na forma discreta. O objetivo é o de examinar as relações entre as várias seqüências discretas para a obtenção dos resultados. A dificuldade reside no comprimento das seqüências pois, dependendo do caso, poderá resultar num número excessivo de iterações. Assim tem-se que associar o comprimento às limitações de banda e o grau de imunidade à interferências desejado. Sabe-se que quanto maior a seqüência maior a imunidade à interferência (inclusive as de múltiplo acesso), no entanto isso causa um aumento da banda ocupada. Tem-se pois a necessidade de assumir um compromisso banda “versus” imunidade.

Os picos de correlação cruzada ocorrem poucas vezes, isto é, existem poucos valores para o atraso no tempo e de fase para os quais ocorre  $I_{\max}(k,i)$ . Assim, para a maioria das aplicações, é mais útil a avaliação do sistema através do desempenho médio do que do desempenho de pior caso. A principal medida é definida pela relação sinal/ruído como visto em (2.63) e (2.66).

Como já mencionado anteriormente analisar-se-á apenas o caso onde a forma de onda para o chip é retangular. Neste caso tem-se a seguinte fórmula<sup>3, 4</sup> para a variância:

$$\sigma_{k,i}^2 = \left( \frac{T_c}{T} \right)^3 \{2\mu_{k,i}(0) + \mu_{k,i}(1)\} / 6 = (6.N^3)^{-1} \{2\mu_{k,i}(0) + \mu_{k,i}(1)\} \quad (2.75)$$

onde a função  $\mu_{k,i}(n) = \sum_{\ell=1-N}^{N-1} C_{k,i}(\ell)C_{k,i}(\ell+n)$  é definida por:

$$\mu_{k,i}(n) = \sum_{\ell=1-N}^{N-1} C_{k,i}(\ell)C_{k,i}(\ell+n) \quad (2.76)$$

Substituindo este resultado na expressão (2.66) tem-se a SNR e com ela pode-se obter a probabilidade de erro de bit dada por (2.43).

$$\text{SNR}_i = \left\{ \left( 6N^3 \right)^{-1} \sum_{\substack{k=1 \\ k \neq i}}^K \{ 2\mu_{k,i}(0) + \mu_{k,i}(1) \} + \frac{N_0}{A^2 T} \right\}^{-1/2} \quad (2.77)$$

$$P_e = Q(\text{SNR}) \quad (2.78)$$

O fator  $\mu_{k,i}$  depende de correlações cruzadas entre as seqüência  $k$  e  $i$ . Denominando-se:

$$\beta_{k,i} = \{ 2\mu_{k,i}(0) + \mu_{k,i}(1) \} \quad (2.79)$$

Pode-se provar<sup>4</sup> que:

$$\beta_{k,i} = 2N^2 + 4 \sum_{\ell=1}^{N-1} C_k(\ell) C_i(\ell) + \sum_{\ell=1-N}^{N-1} C_k(\ell) C_i(\ell+1) \quad (2.80)$$

Observa-se então que esta última expressão pode ser calculada através de auto correlações apenas. Assim para o cálculo  $\text{SNR}_i$  necessita-se do conhecimento de  $K$  auto correlações apenas, enquanto que na forma anterior, expressão (2.76), tinha-se que conhecer  $K(K-1)/2$  correlações cruzadas parciais.

Como o valor médio de  $\mu_{k,i}(0)$  é  $N^2$  e o de  $\mu_{k,i}(1)$  é zero<sup>4</sup> segue-se a aproximação:

$$\text{SNR}_i \approx \left\{ \frac{K-1}{3N} + \frac{N_0}{A^2 T} \right\}^{-1/2} \quad (2.81)$$

onde  $K$  é o número de usuários,  $N$  o comprimento da seqüência e  $N_0/2$  a densidade espectral de potência do AWGN.

### **3 SEQUÊNCIAS BINÁRIAS, PRINCÍPIOS GERAIS E CARACTERÍSTICAS<sup>5</sup>**

#### **3.1 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.

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, conseqüentemente o conhecimento destas operações é fundamental.

As seqüências binárias serão representadas por um vetor  $\vec{x} = \{x_0, x_1, \dots, x_{N-1}\}$ , 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  $\langle x, y \rangle = x_0 \cdot y_0 + \dots + x_{N-1} \cdot y_{N-1}$ . 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,  $T^2 x = \{x_2, x_3, \dots, x_{N-1}, x_0, x_1\}$ , 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 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  $N$  possui  $N$  fases distintas.

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

$$(T^k w)_i = (T^{-k} x)_{N-1-i} = (T^{N-k} x)_{N-1-i} \quad (3.01)$$

onde o índice externo ao parênteses, na expressão 3.01), 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:

$$x = \{x_0, x_1, \dots, x_{N-1}\} \quad (3.02)$$

$y$  será igual a:

$$y = \{x_0, x_q, x_{2q}, \dots, x_{((N-1).q)}\} \quad (3.03)$$

onde os índices de  $y$  são  $\text{mod}N$ ; portanto  $(N-1)q \text{ mod}N=N-q$ , 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 (ver apêndice A2 para detalhes adicionais sobre decimação).

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

$$\theta_{x,y}(\ell) = \langle x, T^\ell y \rangle, \ell \in Z \quad (3.04)$$

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

$$\theta_{x,y}(\ell) = \sum_{i=0}^{N-1} x_i \cdot y_{i+\ell}, \quad \ell \in Z \quad (3.05)$$

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

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

$$|\theta_{x,y}(\ell)| \leq \|x\| \cdot \|T^\ell y\| \leq \|x\| \cdot \|y\| \quad (3.06)$$

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  $\ell$ .

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

$$\theta(x, T^k y)(\ell) = \theta(x, y)(\ell + k) \quad (3.07)$$

$$\theta(T^i x, T^k y)(\ell) = \theta(x, y)(\ell + k - i) \quad (3.08)$$

$$\theta(T^k x)(\ell) = \theta(x)(\ell) \quad (3.09)$$

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:

$$\theta_x(0) = \langle x, x \rangle \quad (3.10)$$

$$\theta_x(\ell) = \theta_x(\ell + N) \quad (3.11)$$

$$\theta_x(\ell) = \theta_x(-\ell) \quad (3.12)$$

$$|\theta_x(\ell)| \leq \|x\|^2 = \langle x, x \rangle = \theta_x(0) \quad (3.13)$$

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

$$\sum x = \sum_{i=0}^{N-1} x_i \quad (3.14)$$

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

$$\sum_{\ell=0}^{N-1} \theta(x, y)(\ell) = \left( \sum x \right) \left( \sum y \right) \quad (3.15)$$

$$\sum_{\ell=0}^{N-1} \theta(x)(\ell) = \left| \left( \sum x \right) \right|^2 \quad (3.16)$$

### 3.2 LIMITES PARA AS FUNÇÕES DE CORRELAÇÃO<sup>4,5</sup>

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:

$$\sum_{\ell=0}^{N-1} \theta_{w,y}(\ell) \cdot [\theta_{x,z}(\ell + n)] = \sum_{\ell=0}^{N-1} \theta_{w,x}(\ell) \cdot [\theta_{y,z}(\ell + n)] \quad (3.17)$$

Desta relação obtém-se as seguintes:

para z=y:

$$\sum_{\ell=0}^{N-1} \theta_{w,y}(\ell) \cdot [\theta_{x,y}(\ell + n)] = \sum_{\ell=0}^{N-1} \theta_{w,x}(\ell) \cdot [\theta_y(\ell + n)] \quad (3.18)$$

e desta última, fazendo-se  $w=x$ :

$$\sum_{\ell=0}^{N-1} \theta_{x,y}(\ell) \cdot [\theta_{x,y}(\ell + n)] = \sum_{\ell=0}^{N-1} \theta_x(\ell) \cdot [\theta_y(\ell + n)] \quad (3.19)$$

e agora se  $n=0$ :

$$\sum_{\ell=0}^{N-1} |\theta_{x,y}(\ell)|^2 = \sum_{\ell=0}^{N-1} \theta_x(\ell) \theta_y(\ell) \quad (3.20)$$

Das identidades anteriores pode-se derivar um limite inicial para a correlação cruzada periódica aplicando a desigualdade de Cauchy, expressão (3.06), tem-se:

$$|\theta(x,y)(\ell)| \leq [\theta(x)(0) \cdot \theta(y)(0)]^{1/2} \quad (3.21)$$

Aplicando-se agora a desigualdade de Cauchy à equação (3.20) tem-se:

$$\sum_{\ell=0}^{N-1} |\theta_{x,y}(\ell)|^2 \leq \left( \sum_{\ell=0}^{N-1} |\theta_x(\ell)|^2 \right)^{1/2} \left( \sum_{\ell=0}^{N-1} |\theta_y(\ell)|^2 \right)^{1/2} \quad (3.22)$$

Desta forma pode-se chegar a um limite superior, bem como a um inferior, para as funções de correlação cruzada. Reescrevendo-se novamente (3.20) segue-se:

$$\sum_{\ell=0}^{N-1} |\theta_{x,y}(\ell)|^2 = \theta_x(0) \theta_y(0) + \sum_{\ell=1}^{N-1} \theta_x(\ell) \theta_y(\ell) \quad (3.23)$$

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

$$\sum_{\ell=0}^{N-1} |\theta_{x,y}(\ell)|^2 \leq \theta_x(0) \cdot \theta_y(0) + \left( \sum_{\ell=1}^{N-1} |\theta_x(\ell)|^2 \right)^{1/2} \cdot \left( \sum_{\ell=1}^{N-1} |\theta_y(\ell)|^2 \right)^{1/2} \quad (3.24)$$

e para o limite inferior:

$$\sum_{\ell=0}^{N-1} |\theta_{x,y}(\ell)|^2 \geq \theta_x(0) \cdot \theta_y(0) - \left( \sum_{\ell=1}^{N-1} |\theta_x(\ell)|^2 \right)^{1/2} \cdot \left( \sum_{\ell=1}^{N-1} |\theta_y(\ell)|^2 \right)^{1/2} \quad (3.25)$$

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 autocorrelação fora de fase, respectivamente, por  $\theta_c$  e  $\theta_a$ , isto é:

$$\theta_c = \max\{\theta_{x,y}(\ell); 0 \leq \ell \leq N-1, x, y \in X \text{ e } x \neq y\} \quad (3.26)$$

$$\theta_a = \max\{\theta_x(\ell); 1 \leq \ell \leq N-1, x \in X\} \quad (3.27)$$

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

$$\left(\frac{\theta_c^2}{N}\right) + \frac{N-1}{N(K-1)} \left(\frac{\theta_a^2}{N}\right) \geq 1 \quad (3.28)$$

Definindo-se agora  $\theta_{\max} = \max\{\theta_a, \theta_c\}$ , segue um outro limite importante, WELCH<sup>6</sup>:

$$\theta_{\max} \geq N \left[ \frac{K-1}{N.K-1} \right]^{1/2} \quad (3.29)$$

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

### 3.3 FAMÍLIAS DE SEQÜÊNCIAS

#### 3.3.1 SEQÜÊNCIAS LINEARES

##### 3.3.1.1 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 autocorrelação

que colaboram, em grande parte, para a etapa de sincronismo de alguns sistemas de comunicação.

Quanto as 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.

#### 3.3.1.1.1 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  $C(x)$ :

$$C(x) = C_n \cdot x^n + C_{n-1} \cdot x^{n-1} + \dots + C_0 \quad (3.30)$$

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  $C = \{C_n, C_{n-1}, \dots, C_0\}$ , 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 sequência  $s_i$  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:

$$C(x) = x^n + C_{n-1} \cdot x^{n-1} + \dots + 1 = 0 \quad (3.31)$$

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

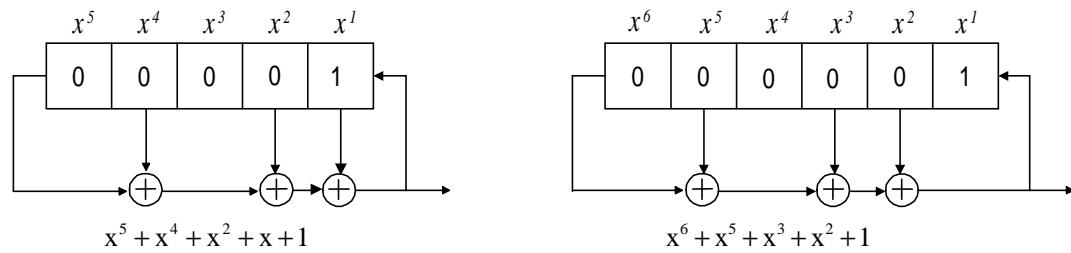


Fig. 3.1 Registradores de deslocamento para a construção de uma SMC

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  $\{0,0,0,0,\dots,1\}$ .

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.

### 3.3.1.1.2 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- Possui período  $N=2^n-1$

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

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

$$T^i_s \oplus T^j_s = T^k_s \quad (3.32)$$

$$4- wH(s) = 2^{n-1} = \frac{1}{2}(N+1) \quad (3.33)$$

5- Para seqüências polarizadas

$$\theta_s(\ell) = \begin{cases} N, & \text{se } \ell = 0 \\ -1, & \text{se } \ell \neq 0 \end{cases} \quad (3.34)$$

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:

$$\tilde{s}_i = \tilde{s}_{2i} \text{ para todo } i \in Z. \quad (3.35)$$

Esta seqüência será denominada de seqüência característica e será denotada por  $\tilde{s}_i = \tilde{s}_{2i}$  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  $N/\text{mdc}(N,q)$ , e será construída a partir de um polinômio  $C'(x)$ , cujas raízes são a  $q$ -ésimas potências das raízes de  $C(x)$ .

Quando  $\text{mdc}(N,q)=1$ ,  $b[q]$  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  $q=q \bmod N$  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 as decimações possíveis, tal que  $\text{mdc}(N,q)=1$  com  $q$  menor que  $N$ , obtém-se todas as SMC de grau  $n$ .

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

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

$$e \quad (3.36)$$

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

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<sup>7</sup>, e é dado por:

$$\lambda(n) = \frac{\varphi(2^n - 1)}{n} \quad (3.37)$$

onde  $\lambda(n) = \frac{\varphi(2^n - 1)}{n}$  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:

$$\begin{aligned} \text{se } m &= \prod_{i=1}^k p_i^{\alpha_i} \text{ onde } p_i \text{ é primo e } \alpha_i \text{ inteiro, então:} \\ \varphi(m) &= \begin{cases} 1 & m = 1 \\ \prod_{i=1}^k (p_i - 1)p_i^{\alpha_i - 1} & m > 1 \end{cases} \end{aligned} \quad (3.38)$$

por exemplo:

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

### 3.3.1.1.3 PROPRIEDADES DAS FUNÇÕES DE AUTO CORRELAÇÃO E CORRELAÇÃO CRUZADA PARA SMC'S<sup>5</sup>

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

$$\theta_{k,i} = \sum_{j=0}^{N-1} a_k(j) \cdot a_i(j + \ell) = C_{k,i}(\ell) + C_{k,i}(\ell - N) \quad (3.39)$$

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 com  $N=2^n-1$ , seguem-se as seguintes propriedades:

$$1- \theta_{a,b}(\ell) = \theta_{a,b}(\ell + N) \quad (3.40)$$

$$2- |\theta_{a,b}(\ell)| \leq N \quad (3.41)$$

$$3- \theta_{a,b}(\ell) \text{ é sempre um inteiro ímpar} \quad (3.42)$$

$$4- \theta_{a,b}(\ell) + 1 \text{ é sempre um múltiplo de 8} \quad (3.43)$$

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

$$5- \sum_{\ell=0}^{N-1} \theta(a,b)(\ell) = 1 \quad (3.44)$$

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.

$$6- \sum_{\ell=0}^{N-1} [\theta(a,b)(\ell)]^2 = N^2 + N - 1 = 2^{2n} - 2^n - 1 \quad (3.45)$$

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  $\ell$ .

#### 3.3.1.1.4 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 mod  $N$  qualquer.

3- Se as decimações  $q$  e  $q'$  são tais que  $q.q'=1 \text{ mod } N$  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  $e=\text{mdc}(n,k)$  tal que  $n/e$  é ímpar. Seguem-se os respectivos valores, bem como o número de ocorrências dos mesmos num período:

$$\theta(a, b)(\ell) = \begin{cases} -1 + 2^{(n+e)/2} & \text{ocorre } 2^{(n-e-1)} + 2^{(n-e-2)/2} & \text{vezes} \\ -1 & \text{ocorre } 2^n - 2^{n-e} - 1 & \text{vezes} \\ -1 - 2^{(n+e)/2} & \text{ocorre } 2^{(n-e-1)} - 2^{(n-e-2)/2} & \text{vezes} \end{cases} \quad (3.46)$$

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:

$$t(n) = 1 + 2^{\lfloor (n+2)/2 \rfloor} \quad (3.47)$$

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:

$$\theta(a, b)(\ell) = \begin{cases} -1 + 2^{(n+2)/2} & \text{ocorre } (2^{n-1} + 2^{(n-2)/2}) / 3 & \text{vezes} \\ -1 + 2^{n/2} & \text{ocorre } 2^{n/2} & \text{vezes} \\ -1 & \text{ocorre } 2^{(n-1)} + 2^{(n-2)/2} - 1 & \text{vezes} \\ -1 - 2^{n/2} & \text{ocorre } (2^n - 2^{n/2}) / 3 & \text{vezes} \end{cases} \quad (3.48)$$

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

Se n é par:

$$-t(n) + 4 \leq \theta(a, b)(\ell) \leq t(n) - 2 \quad (3.49)$$

e se a e b são recíprocos tem-se:

$$|\theta(a, b)(\ell)| \leq 2^{(n+2)/2} \quad (3.50)$$

Denotando  $\theta_c$  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  $2 \bmod 4$ ,  $\theta_c \geq t(n)$  para pares preferenciais

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

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

### 3.3.1.2 SEQUÊNCIAS DE GOLD

#### 3.3.1.2.1 CONSTRUÇÃO DA FAMÍLIA

As seqüências de Gold formam um conjunto (família) que consiste de  $N+2$  seqüências. Cada uma possui 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 3.2 adiante. Cada registrador possui 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.

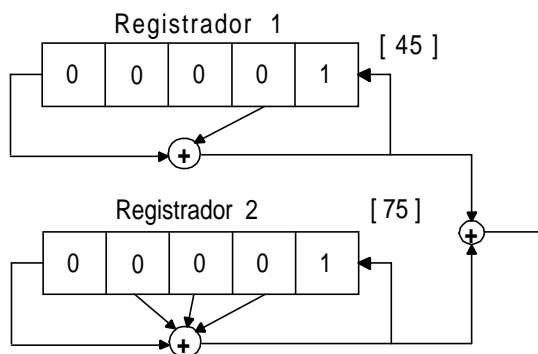


Fig. 3.2 Registradores de deslocamento para a construção de Família de Gold

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

$$G(a, b) = \{a, b, a \oplus b, a \oplus Tb, a \oplus T^2b, a \oplus T^3b, \dots, a \oplus T^{N-1}b\} \quad (3.51)$$

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:

$$\theta_c = \max\{\theta_{a,b}(\ell); 0 \leq \ell \leq N-1\} = \theta_a = \max\{\theta_i(\ell); 1 \leq \ell \leq N-1 \text{ e } i=a, b\} \quad (3.52)$$

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  $\text{mdc}(n, k) = 1$ .

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:

$$x, y \in G(a, b) \Rightarrow \theta(x, y)(\ell) \in \{-1, -t(n), t(n) - 2\} \quad (3.53)$$

e

$$z \in G(a, b) \Rightarrow \theta(z)(\ell) \in \{-1, -t(n), t(n) - 2\}, \forall \ell \neq 0 \bmod N \quad (3.54)$$

### 3.3.1.3 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.

#### 3.3.1.3.1 CONSTRUÇÃO DA FAMÍLIA

Seja  $a$  uma SMC de período  $N=2^n-1$ , onde  $n$  é um inteiro par. Construa-se primeiro o conjunto  $b^{(k)}$ ,  $k=0,1,2,\dots$  onde  $b^{(k)}$  é obtido pela decimação  $q$  de  $T^k a$ , com  $q$  inteiro, obedecendo a relação  $\text{mdc}(q, N)=3$ . Este conjunto conterà 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 conterà  $N+1$  seqüências de período  $N$ . A expressão a seguir exhibe estes procedimentos.

$$\begin{aligned} GL(a, q) = \{ & a \oplus b^{(0)}, a \oplus T b^{(0)}, a \oplus T^2 b^{(0)}, \dots, a \oplus T^{N'-1} b^{(0)}, \\ & a \oplus b^{(1)}, a \oplus T b^{(1)}, a \oplus T^2 b^{(1)}, \dots, a \oplus T^{N'-1} b^{(1)}, \\ & a \oplus b^{(2)}, a \oplus T b^{(2)}, a \oplus T^2 b^{(2)}, \dots, a \oplus T^{N'-1} b^{(2)} \} \end{aligned} \quad (3.55)$$

#### 3.3.1.3.2 GOLD LIKE

Dá-se o nome de Gold-Like, ao conjunto de seqüências geradas tal como em (3.55), onde com  $q=t(n)$ . Quando  $n$  é múltiplo de 4 o  $\text{mdc}(t(n), N)=3$  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  $t(n)$ . Os valores para a correlação cruzada periódica assumem um valor dentre os seguintes:

$$\{-1, -t(n), t(n)-2, -s(n), s(n)-2\} \quad (3.56)$$

onde  $s(n)$  é calculável por:

$$s(n) = 1 + 2^{n/2} = \frac{1}{2} (t(n) + 1) \quad (3.57)$$

### 3.3.1.3.3 GOLD BCH DUAL

Estas seqüências utilizam o mesmo processo de construção em (3.55), onde o valor para a decimação é igual a 3; desta forma quando  $n$  é par o  $\text{mdc}(3, N) = 3$ . Como na família anterior esta também possui  $N+1$  seqüências de período  $N$ . Os valores para a correlação cruzada restringem-se também a apenas cinco valores, que são:

$$\{-1, -t(n), t(n)-2, -s(n), s(n)-2\}. \quad (3.58)$$

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.

### 3.3.1.4 FAMÍLIAS DE KASAMI

#### 3.3.1.4.1 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:

$$Kp(a) = \{a, a \oplus b, a \oplus Tb, a \oplus T^2b, a \oplus T^3b, \dots, a \oplus T^{2^{n/2}-2}b\} \quad (3.59)$$

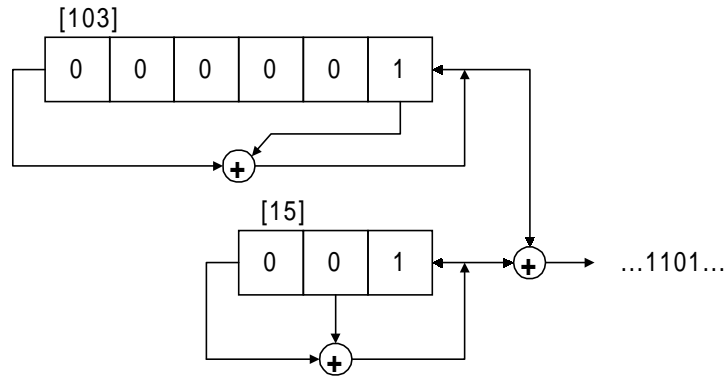


Fig. 3.3 Registradores de deslocamento para a construção da família Kasami Pequeno

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

$$\{-1, -s(n), s(n)-2\} \quad (3.60)$$

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:

$$\theta_{\text{MAX}} > 2^{n/2} - 1 \quad (3.61)$$

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:

$$\theta_{\text{MAX}} \geq 2^{n/2} + 1 \quad (3.62)$$

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

#### **3.3.1.4.2 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.

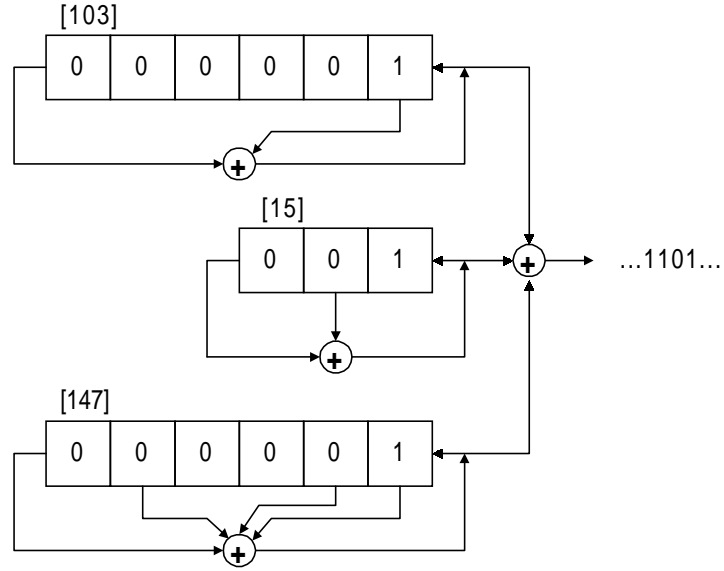


Fig. 3.4 Registradores de deslocamento para a construção da família Kasami Grande

Existem dois resultados possíveis para esta família:

1- Se  $n \equiv 2 \pmod{4}$ .

$$Kg(a) = G(a, c) \cup \left[ \bigcup_{i=0}^{2^{n/2}-2} \{T^i b \oplus G(a, c)\} \right] \quad (3.63)$$

2- Se  $n \equiv 0 \pmod{4}$

$$Kg(a) = GL(a, t(n)) \cup \left[ \bigcup_{i=0}^{2^{n/2}-2} \{T^i b \oplus GL(a, t(n))\} \right] \cup \{c^{(i)} \oplus T^k b : 0 \leq j \leq 2; 0 \leq k \leq (2^{n/2}-1)/3\} \quad (3.64)$$

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  $n \equiv 2 \pmod{4}$  ou  $2^{n/2}(2^n+1)-1$  para  $n \equiv 0 \pmod{4}$ .

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.

### 3.3.1.5 SEQUÊNCIAS DE HADAMARD<sup>8</sup>

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  $m \times m$ ,  $H_m$ , onde todos seus elementos são -1 ou +1 e tal que:

$$H_m H_m^T = H_m^T H_m = mI_m \quad (3.65)$$

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  $m \times n$ ,  $H_{m \times n}$ , consistindo de elementos -1 e +1, é dita uma matriz de Hadamard retangular (ou incompleta) se:

$$H_{m \times n} H_{m \times n}^T = nI_m \quad (3.66)$$

#### Definição 5

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

$$H_2 = PH_1Q \quad (3.67)$$

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.

$$H(k+1) = \begin{bmatrix} H(k) & H(k) \\ H(k) & -H(k) \end{bmatrix} \quad (3.68)$$

onde

$$H(1) \in \{\pm D_1, \pm D_2, \pm D_3, \pm D_4\} \quad (3.69)$$

$$D_1 = \begin{bmatrix} +1 & -1 \\ +1 & +1 \end{bmatrix}, D_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}, D_3 = \begin{bmatrix} -1 & +1 \\ +1 & +1 \end{bmatrix}, e D_4 = \begin{bmatrix} +1 & +1 \\ -1 & +1 \end{bmatrix} \quad (3.70)$$

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 as 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:

$$H H^* = h I_h \quad (3.71)$$

onde  $H^*$  é a transposta conjugada da matriz  $H$ .

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

### 3.3.2 SEQÜÊNCIAS NÃO LINEARES<sup>9</sup>

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 apêndice A1) é definida por:

$$\text{tr}_j^n(\alpha) = \sum_{i=0}^{(n/j)-1} \alpha^{2^{ji}} \quad (3.72)$$

onde  $\alpha$  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.

#### 3.3.2.1 SEQÜÊNCIAS GMW<sup>10</sup>

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:

$$b_i = \text{tr}_1^j \left\{ \left[ \text{tr}_j^n (\alpha^i) \right]^r \right\} \quad (3.73)$$

onde  $\alpha$  é um elemento primitivo de  $\text{GF}(2^n)$  e  $r$  um inteiro qualquer relativamente primo à  $2^j-1$  no intervalo  $1 \leq r < 2^j-1$ . Quando  $r=1$  a seqüência  $\{b_i\}$  definida por (3.73) 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  $\text{tr}_j^n (\alpha^i)$  pode ser interpretada como uma SMC de período  $2^n-1$ , com elementos em  $\text{GF}(2^j)$ . 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:

$$b_i' = \text{tr}_j^m (\alpha^i) \quad (3.74)$$

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 (3.73), é:

$$L = j(n/j)^w \quad (3.75)$$

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  $\text{GF}(2)$ , 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:

$$N_c = \begin{cases} 2^{(n-k)}, & \text{para } c \neq 0, \quad 1 \leq k \leq n/j \\ 2^{(n-k)} - 1, & \text{para } c = 0, \quad 1 \leq k \leq n/j \end{cases} \quad (3.76)$$

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:

$$N_{\text{GMW}} = N_p(n) \cdot N_p(j) \quad (3.77)$$

onde  $N_p(n)$  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.

### 3.3.2.2 SEQÜÊNCIAS DE BENT<sup>11,12</sup>

#### 3.3.2.2.1 INTRODUÇÃO

As seqüências de Bent são códigos construídos a partir de funções de Bent, definidas por ROTH AUS<sup>13</sup>, 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:

$$c(\lambda) = \frac{1}{2^{n/2}} \sum_{x \in V_n} (-1)^{P(x)} \cdot (-1)^{\langle \lambda, x \rangle} \quad (3.78)$$

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

$$(-1)^{P(x)} = \frac{1}{2^{n/2}} \sum_{\lambda \in V_n} c(\lambda) \cdot (-1)^{\langle \lambda, x \rangle} \quad (3.79)$$

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 ROTHBAUS<sup>13</sup>:

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<sup>13</sup> 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:

$$Q(x, y) = \langle x, y \rangle + P(x) \quad (3.80)$$

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:

$$Q(x, y, z) = A(x)B(x) + B(x)C(x) + C(x)A(x) + [A(x) + B(x)]y + [A(x) + C(x)]z + yz \quad (3.81)$$

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<sup>14</sup>. 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<sup>15</sup> 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<sup>11</sup>, OLSEN<sup>12</sup> 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.

### 3.3.2.2 FILOSOFIA DA CONSTRUÇÃO<sup>11,12</sup>

Descreve-se a seguir o método de construção apresentado em SIMON<sup>11</sup>.

Seja  $\alpha$  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  $\alpha$  como o polinômio característico do gerador. Seja ainda  $\{\phi_1, \dots, \phi_{d/2}\}$  uma base qualquer de  $GF(2^{d/2})$  sobre  $GF(2)$  e selecione-se um elemento  $\epsilon$  qualquer de  $GF(2^d)$  que não pertença a um Corpo menor. Constrói-se a matriz  $M$ , com dimensão  $d/2 \times d$ , tal que o elemento  $m_{i,j}$  é dado por

$$m_{i,j} = \text{Tr}_1^d(\epsilon \phi_i \alpha^{j-1}) \quad (3.82)$$

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:

$$r_z(x) = (-1)^{f_z(M \cdot x) + s^t \cdot x} \quad (3.83)$$

onde  $f_z(\cdot)$  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<sup>12</sup> demonstra-se que a função:

$$f_z(x) = x_1^t \cdot x_2 + g(x_2) + z^t \cdot x \quad (3.84)$$

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<sup>11</sup> dado por:

$$L \geq \begin{cases} 20 & d = 8 \\ \left( \frac{d/2}{d/4} \right) 2^{d/4} + d + \frac{1}{2} \sum_{i=2}^{d/4-1} \binom{d/2}{i} 2^i & d \geq 8 \end{cases} \quad (3.85)$$

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

## **4 MÉTODOS DE SIMULAÇÃO**

Os resultados que serão apresentados, foram obtidos através de simulações realizadas por computadores, em plataformas baseadas em estações de trabalho SUN e PC, utilizando-se principalmente do software *Mathematica* versão 2.2 em ambiente Unix e Windows.

### **4.1 DIAGRAMAS DE CONSTRUÇÃO DE SEQUÊNCIAS**

Descreve-se a seguir, em termos de diagramas de blocos, a metodologia utilizada para a geração das várias famílias de códigos descritas no capítulo anterior.

### 4.1.1 SMC

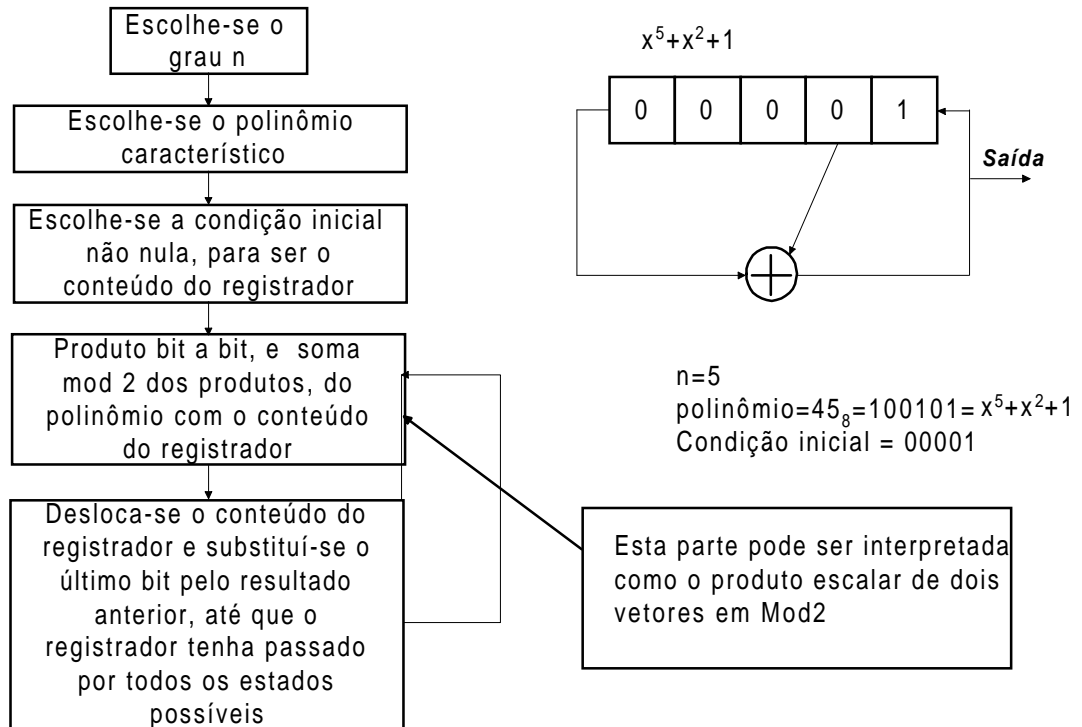


Fig. 4.1 Diagrama de Construção de uma SMC

### 4.1.2 GOLD

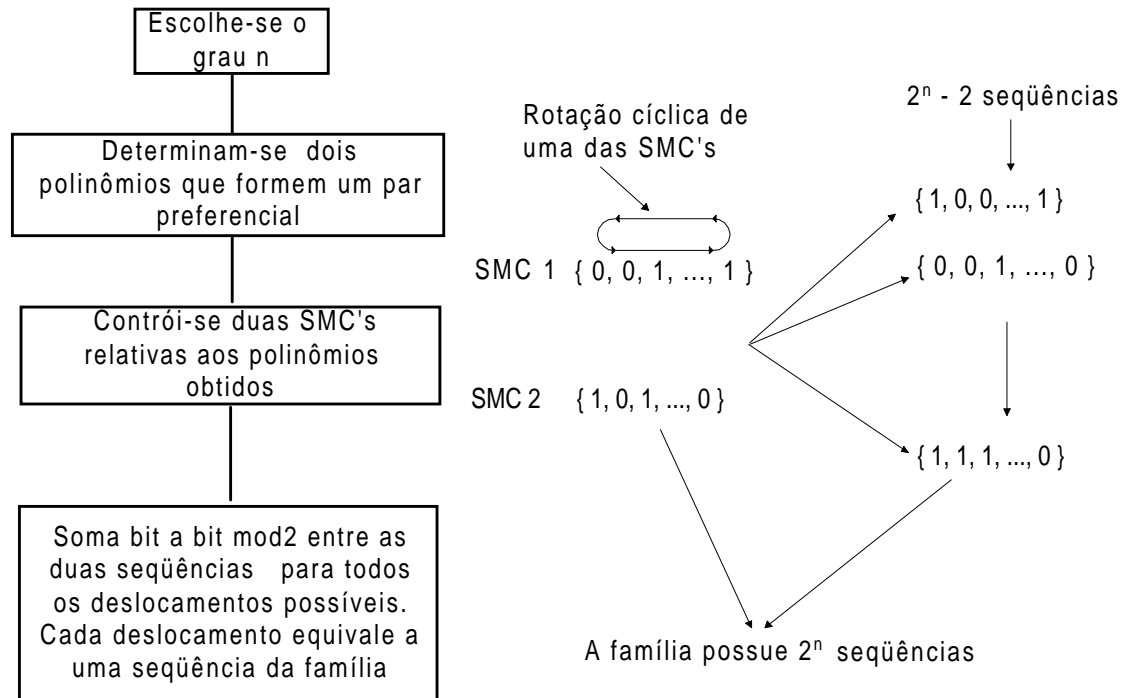
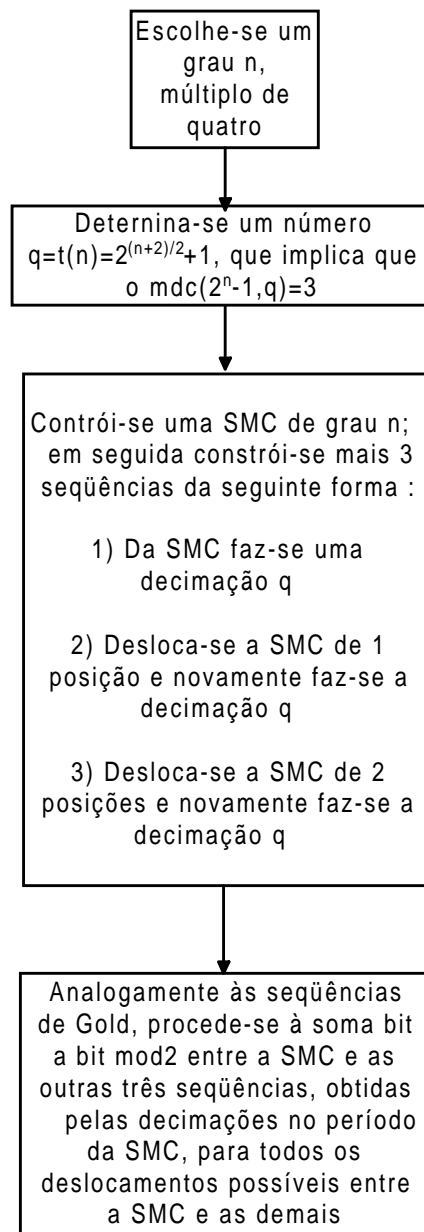


Fig. 4.2 Diagrama de Construção de Famílias de Seqüências de Gold

### 4.1.3 GOLD LIKE



Ex :

$n = 4$  , polinômio = [23] = {1,0,0,1,1} -> { 1,0,0,1}

$$q = 2^{(4+2)/2} + 1 = 9$$

Seqüência = {1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1}

Decimação 1

{0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1}

Seqüência deslocada de uma posição para a esquerda

{1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1}

Decimação 2

{1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1}

Seqüência deslocada de duas posições para a esquerda

{1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1}

Decimação 3

{0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1}

Como as seqüências geradas pelas decimações tem um terço do período da SMC, serão geradas ao todo um número de seqüências igual ao período e incluindo-se a SMC, tem-se que o número de seqüências total da família é igual a  $2^n = 16$

{{1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1},  
 {1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0},  
 {1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1},  
 {1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1},  
 {0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1},  
 {0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0},  
 {0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0},  
 {0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0},  
 {1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0},  
 {0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1},  
 {0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0},  
 {1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0},  
 {1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1},  
 {0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1},  
 {1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0},  
 {0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1}}

Fig. 4.3 Diagrama de Construção de Famílias de Seqüências de Gold Like

#### 4.1.4 GOLD BCH DUAL

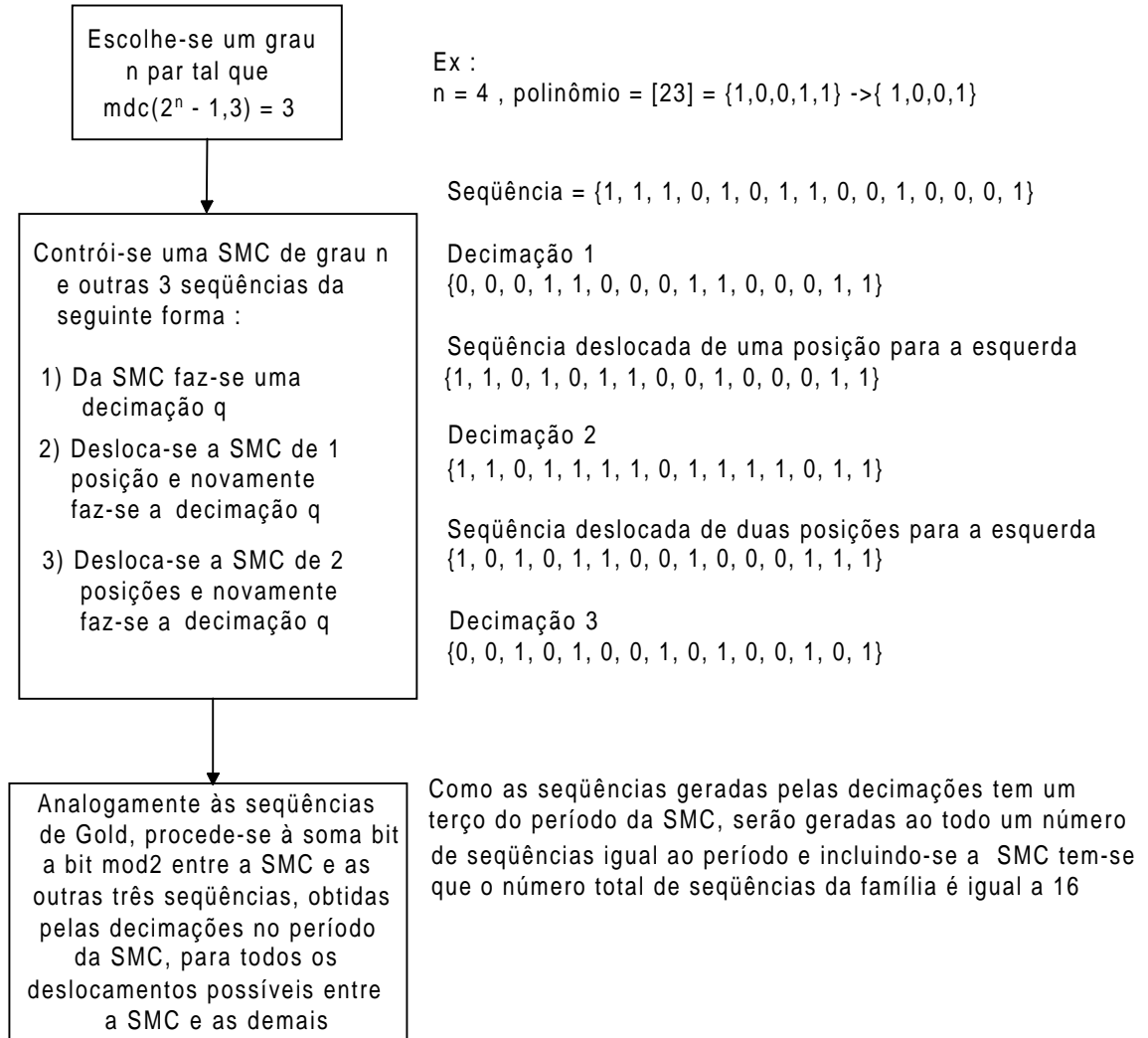


Fig. 4.4 Diagrama de Construção de Famílias de Seqüências de Gold-BCH Dual

#### 4.1.5 KASAMI PEQUENO

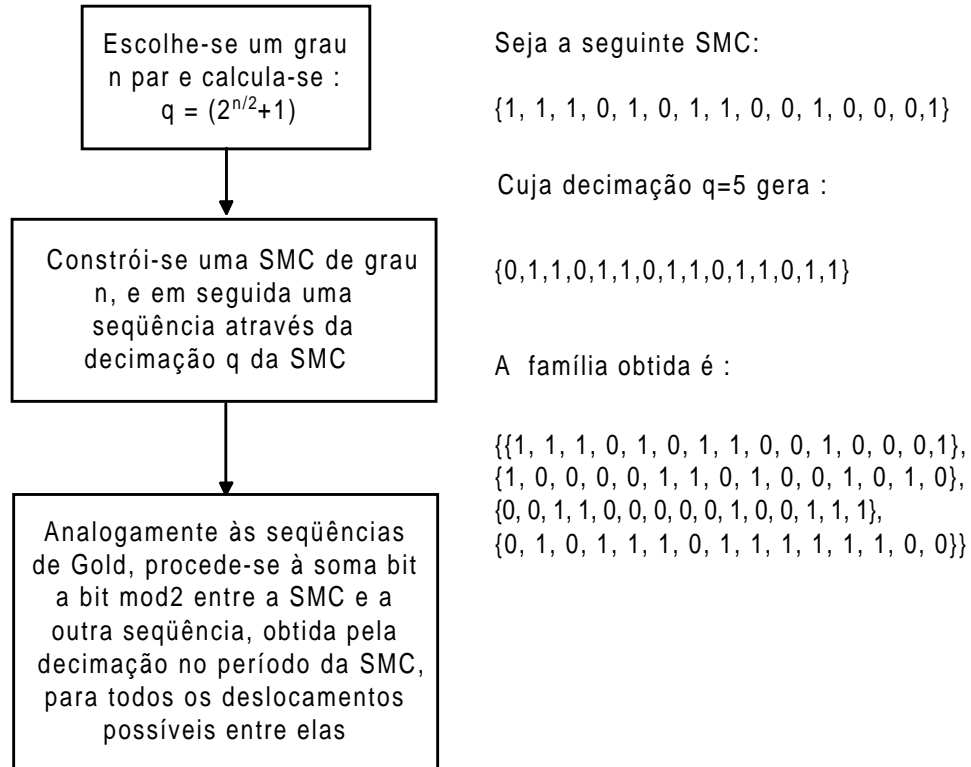


Fig. 4.5 Diagrama de Construção de Famílias de Seqüência Kasami Pequeno

#### 4.1.6 KASAMI GRANDE

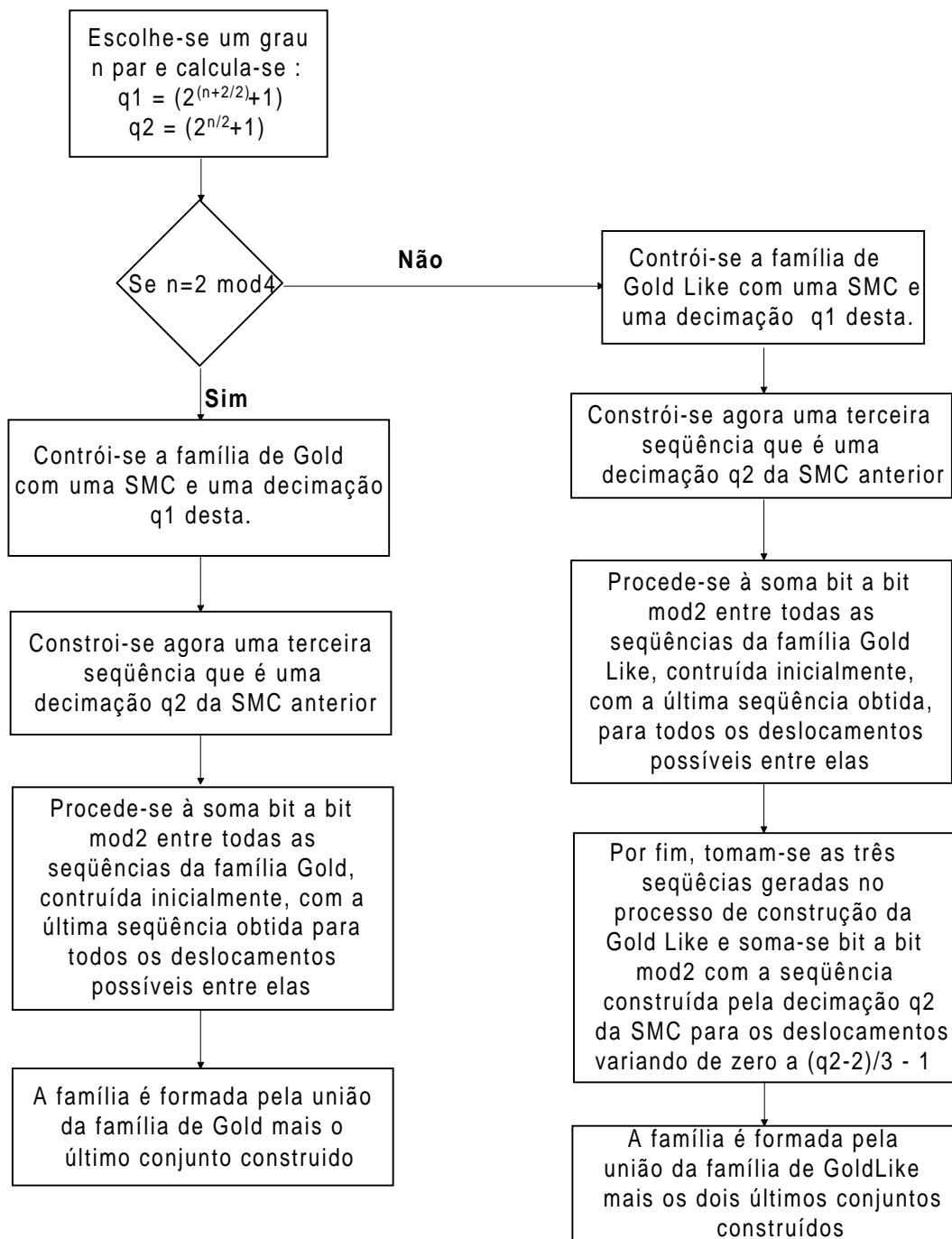


Fig. 4.6 Diagrama de Construção de Famílias de Seqüências Kasami Grande

### 4.1.7 HADAMARD

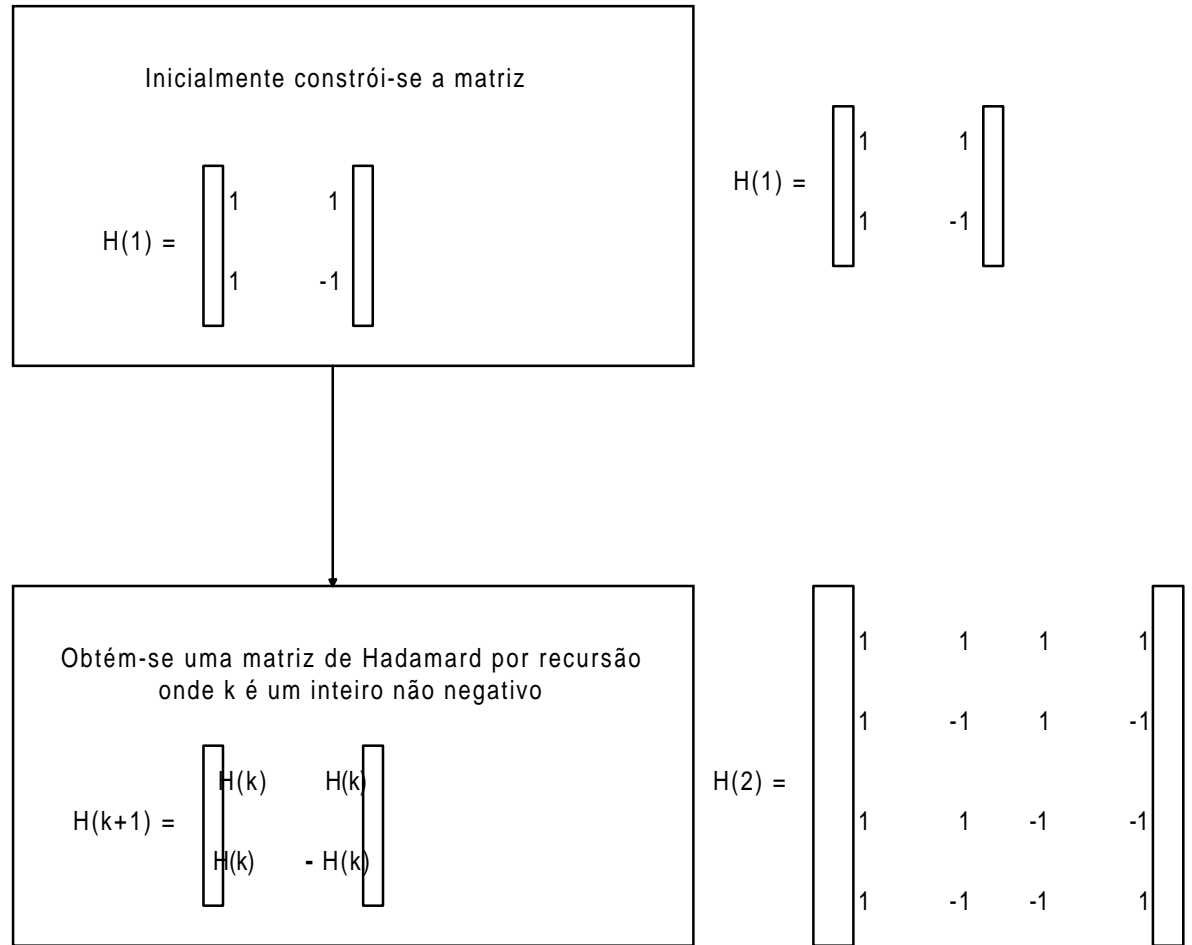


Fig. 4.7 Diagrama de Construção de Famílias de seqüências de Hadamard

### 4.1.8 GMW

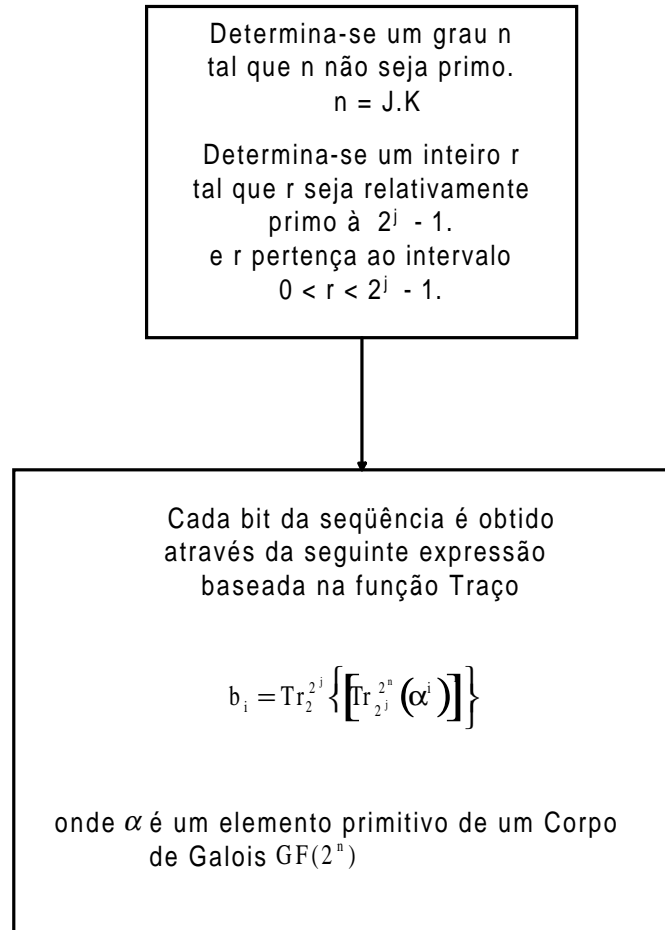


Fig. 4.8 Diagrama de Construção de Famílias de Seqüências GMW

#### 4.1.9 BENT

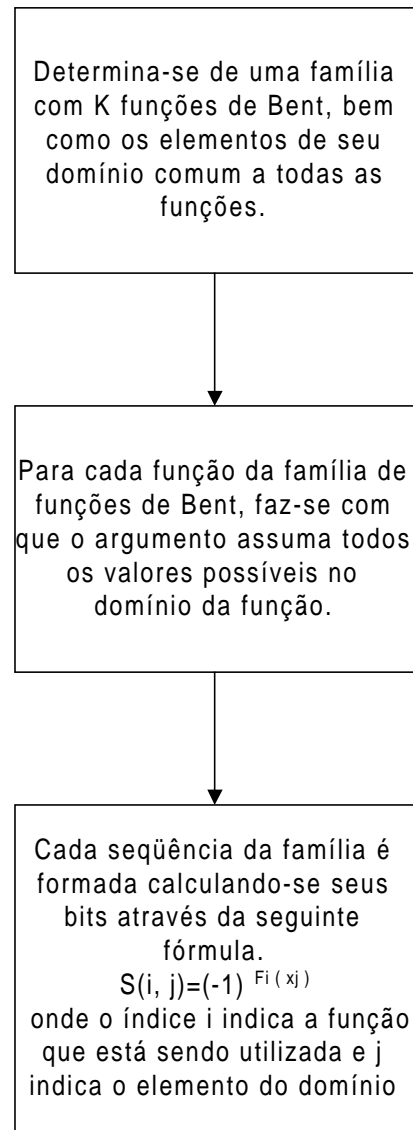


Fig. 4.9 Diagrama de Construção de Famílias de Seqüências de Bent

## 4.2 PROCEDIMENTOS E RESULTADOS PARA AS SIMULAÇÕES

As simulações e cálculos deste capítulo foram realizadas através de funções que estão expostas no anexo deste trabalho. Estas funções são algoritmos elaborados para serem utilizadas no programa *Mathematica* e foram destacadas em negrito, sendo que as funções próprias do *Mathematica* foram escritas em itálico. A descrição da utilização e do algoritmo podem ser consultadas no anexo.

### 4.2.1 SMC

Por conveniência de exposição as propriedades das SMC's serão reescritas

#### 4.2.1.1 PROPRIEDADES GERAIS

1- O período  $N$  de uma SMC tem o seguinte valor  $N=2^n - 1$ .

No diagrama da figura 4.1, tem-se um algoritmo que pode ser implementado através de um registrador de deslocamento e de uma porta XOR, com um número de entradas correspondente ao de realimentações. A sequência será de máximo comprimento se o conteúdo do registrador passar por todos os estados possíveis, exceto o nulo.

A periodicidade desta sequência pode ser verificada com a função **FasesCoincidentes[ ]** que compara as duas sequências verificando a existência de coincidência de fase entre as mesmas.

Por exemplo seja:

$$\text{seq1} = \text{SMC}[\{1,0,0,0,0,1\}] = \{1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1\}$$

$$\text{FasesCoincidentes}[\text{seq1}, \text{seq1}] = \{0\};$$

Como era esperado, só poderia haver uma fase coincidente no período, pois se houvesse mais de uma significaria que o período é menor do que o comprimento da sequência que está sendo analisada.

Seja um caso em que a sequência é formada por vários períodos de uma sequência menor.

$seq2 = \{1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1\}$

**FasesCoincidentes**[seq2,seq2]={0, 5, 10}

A diferença entre fases é 5 e existem 3 coincidências; portanto a sequência possui comprimento ímpar.

Para sequências em que o comprimento é um número primo não há possibilidade de ocorrer um período menor que o comprimento, exceto no caso em que todos os bits da sequência são iguais.

Em síntese, se como resultado da função **FasesCoincidentes**[seq1,seq2] fosse obtido:

{ } então seq1 é diferente de seq2

{n} então seq1=seq2 deslocada de n casas para a esquerda e o período de seq1/seq2 é igual ao comprimento.

{n1, n2, ...ni} então seq1 e seq2 são sequências iguais exceto pelo deslocamento e o período é menor que o comprimento.

onde seq1 e seq2 são sequências binárias que possuem o mesmo comprimento e os n's são números inteiros não negativos.

2- Existem N sequências não nulas geradas por C(x) (polinômio característico - responsável pelas realimentações), que são ciclicamente equivalentes.

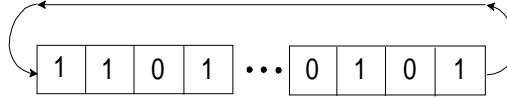


Fig. 4.10 Seqüências Ciclicamente Equivalentes

As seqüências ciclicamente equivalentes são aquelas que são obtidas pela simples rotação da seqüência de origem. Isso equivale a carregar o registrador de deslocamento com um conteúdo inicial diferente. Para cada posição relativa da seqüência é dito que a mesma está numa determinada fase. Neste trabalho é considerada como fase inicial a seqüência na qual o registrador de deslocamento é inicializado com  $\{0,0,0,\dots,0,0,0,1\}$ .

Seja uma seqüência de período  $2^n-1=63$ , grau  $n=6$ , para este caso existiriam 63 seqüências distintas, mas ciclicamente equivalentes.

3- Dados dois inteiros distintos  $1 \leq i, j \leq N$ , existe apenas um inteiro  $k$ , distinto destes dois últimos,  $1 \leq k \leq N$ , tal que:  $T^i b \oplus T^j b = T^k b$ , onde  $b$  é uma SMC.

Seja então a seguinte SMC de grau 4.

$$\text{seq1} = \text{SMC}[\{1, 0, 0, 1\}] = \{1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1\}$$

para  $i=5$  e  $j=7$  obtém-se o valor  $k=14$ . A função  $\text{prop3}$  foi elaborada para a comprovação desta propriedade, ou seja determinar  $k$  na expressão anterior. Neste caso:

$$\text{prop3}[\text{seq1}, 5, 7] = \{14\}$$

A seguir se comprovará a propriedade para todos os deslocamentos possíveis:

Com a seguinte expressão  $\text{Table}[\{i, j, \text{prop3}[\text{ss1}, i, j]\}, \{i, 0, 14\}, \{j, 0, 14\}]$  obtém-se uma tabela que exhibe as coincidências entre seqüências, verificando-se então a propriedade para o grupo.

Inicialmente varia-se  $j$  e em seguida  $i$ . Cada grupo equivale à  $\{i, j, \{k\}\}$ .

Nota-se não há um valor de  $k$  para os casos em  $i=j$ .

Desta propriedade tem-se que a soma de uma SMC com ela própria deslocada é a mesma sequência com uma fase distinta.

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

Dada uma SMC não polarizada esta propriedade pode ser comprovada através da simples soma de seus bits, ou aplicando o produto escalar sobre ela própria.

Seja então a seguinte SMC [103]

$seq1 = \mathbf{Smc}[\{1,0,0,0,0,1\}] = \{1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1\}$

$$seq1.seq1=32$$

onde o ponto representa no *Mathematica* o produto escalar entre duas listas (vetores).

Para seqüências não polarizadas este número indica o número de 1's da seqüência. Se fosse polarizada indicaria seu comprimento.

## 5 - Distribuição dos blocos de bits.

A seguir coloca-se a seqüência num gráfico, onde nas abscissas tem-se a posição relativa do bit.

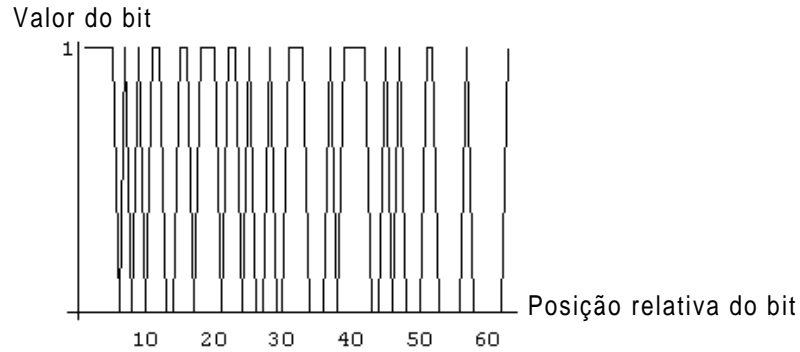


Fig. 4.11 Representação gráfica de uma SMC.

Observando o gráfico detalhadamente nota-se a existência de 8 grupos de apenas um 1 (são os picos mais estreitos no gráfico), quatro de apenas dois 1's, dois de três 1's, um de quatro 1's e um de seis 1's, sendo que este último é encontrado unindo-se o início com o final. Para os zeros tem-se 8 de um 0, quatro de dois 0's, dois de três 0's, um de quatro 0's e um de cinco 0's. Esta relação pode ser constatada em todas as SMC de grau 6, independente do polinômio primitivo que a gerou, e pode ser generalizada para qualquer grau.

O número de 1's é igual a:  $2^{n-1}$  e o número de 0's é igual a:  $2^{n-1} - 1$

A distribuição correspondente é:

um grupo de  $n$  1's (não ocorre o grupo de  $n$  0's)

um grupo de  $(n-1)$  0's.

e para os demais  $2^{n-k-2}$  grupos de  $k$  dígitos iguais, onde  $0 < k < n-1$

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

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

Esta seqüência é denominada de seqüência característica e denotada por  $\tilde{b}_i$ . A fase desta seqüência é chamada de fase característica.

Para comprovar a ocorrência desta propriedade utiliza-se a seguinte função:

**fseq**[seqüência]

que retorna o número de fases onde ocorre a coincidência com a decimação 2.

Seja novamente a seqüência [103]

**seq1**=**SMC**[{1,0,0,0,0,1}]= {1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1}

Da função **fseq** tem-se:

**fseq**[seq1]= {61}

Este resultado significa que a fase característica desta SMC, relativa a posição inicialmente atribuída é 61. Assim rotacionando ciclicamente a mesma de 61 posições para a esquerda e em seguida decimando-a por 2, obtém-se a mesma seqüência.

Se a seqüência utilizada não fosse uma SMC obter-se-iam outros resultados.

Por exemplo:

**seq2**= {1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1}

**fseq**[seq2]= {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15}

Obviamente o resultado esperado para este caso particular, pois para qualquer deslocamento ou para qualquer decimação deve-se obter a mesma seqüência.

**seq3**= {1,1,0,0,1,0,0,0,1,1,0,1,0}

**fseq[seq3]={ }**

Neste caso significando que não existe uma fase tal que uma decimação por 2 da sequência gere a própria.

Esta função pode ser usada para outras decimações, que não 2, que está como "default".

Deste resultado tem-se que uma decimação 2 de uma SMC gera a própria sequência deslocada por fator k.

#### 4.2.1.2 PROPRIEDADES DE CORRELAÇÃO PERIÓDICA

##### Auto Correlação Periódica

A auto correlação periódica de uma SMC é calculada com a expressão seguinte:

$$\theta_x(\ell) = \sum_{i=0}^{N-1} x_i \cdot x_{i+\ell}, \quad \ell \in \mathbb{Z}$$

onde x representa a SMC.

Este resultado é, no caso da SMC, dado por:

$$\theta_x(\ell) = \begin{cases} N, & \text{se } \ell = 0 + N.k \\ -1, & \text{se } \ell \neq 0 + N.k \end{cases} \quad k = 0, 1, \dots$$

Quando o deslocamento é zero ou um múltiplo do período o valor da auto correlação periódica **Normalizada** (tratar-se-á sempre com correlações normalizadas ) é igual ao período **N** e para todos os outros deslocamentos a auto correlação periódica é igual a **-1**.

Para efetuar-se o cálculo da auto correlação periódica de uma sequência seguem-se os procedimentos abaixo.



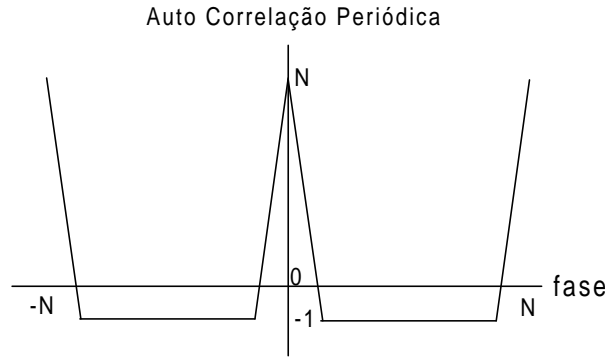


Fig. 4.12 Auto Correlação Periódica para uma SMC

### **Correlação Cruzada Periódica**

O cálculo da correlação cruzada periódica será efetuado através da função:

**CorrelacaoPeriodica**[seq1, seq2, d ]

onde seq1 e seq2 são duas seqüências diferentes e d é o deslocamento à esquerda da seq2, o qual é 0 se omitido.

Sejam então:

seq1=**Polarize**[SMC[ { 1,1,0,1,1,0}]] e

seq2=**Polarize**[SMC[ { 1,0,0,0,0,1}]]

**CorrelacaoPeriodica**[seq1,seq2]=15

Para calcular os valores relativos a todos deslocamentos possíveis num período utiliza-se a seguinte expressão:

correlacoes=**Table**[**CorrelacaoPeriodica**[seq1,seq2,d],{d,0,**Length**[seq1]-1}]

correlacoes={15, 7, -1, -9, -1, -1, -1, -9, 7, 15, -1, -1, -1, 7, -1, -1, -1, -1, 15, -9, -9, -9, -9, 7, -9, -1, -9, -1, 7, -1, -9, -9, -1, -1, -9, 7, -1, -9, 7, 23, -1, 7, -9, -1, -9, 15, -1, 7, -1, -1, -9, -9, 7, -1, -1, -1, -9, -1, 7, -9, 23, 7, -1}



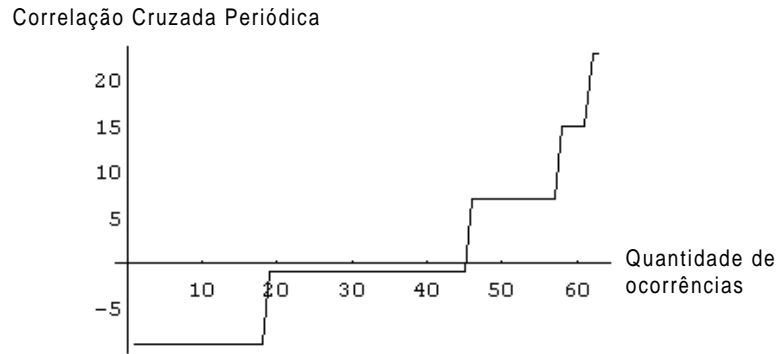


Fig. 4.14: Gráfico de Pesos da Correlação Cruzada Periódica (SMC)

Os pesos de cada valor podem ser obtidos com as seguintes funções:

a)  $\text{valores} = \text{Union} [\text{correlações}] = \{-9, -1, 7, 15, 23\}$

b)  $\text{Table} [ \{ \text{valores}[[i]], \text{Count} [\text{correlacoes}, \text{valores}[[i]]] \}, \{i, 1, \text{Length} [\text{valores}]] ]$

$\{\{-9, 18\}, \{-1, 27\}, \{7, 12\}, \{15, 4\}, \{23, 2\}\}$

Esta lista exibe que o valor -9 resultou em 18 deslocamentos, o valor -1 em 27, o 7 em 12, o 15 em 4 e o 23 em 2.

Pode-se obter as posições em que um determinado valor de correlação ocorreu utiliza-se a seguinte função:

$\text{Flatten} [ \text{Position} [\text{correlações}, -9] ] = \{4, 8, 20, 21, 22, 23, 25, 27, 31, 32, 35, 38, 43, 45, 51, 52, 57, 60\}$

Os valores máximo e o mínimo podem ser obtidos com as seguintes funções:

máximo =  $\text{Max} [\text{correlacoes}] = 23$

mínimo =  $\text{Min} [\text{correlacoes}] = -9$

### Auto Correlação Aperiódica

A expressão a seguir calcula a auto correlação aperiódica, bem como a correlação cruzada aperiódica. Quando o parâmetro da função for nulo obter-se-á um resultado igual ao obtido pela correlação cruzada periódica.

$$C_{k,i}(\ell) = \begin{cases} \sum_{j=0}^{N-1-\ell} a_k(j) a_i(j+\ell) & , \quad 0 \leq \ell \leq N-1 \\ \sum_{j=0}^{N-1+\ell} a_k(j-\ell) a_i(j) & , \quad 1-N \leq \ell < 0 \\ 0 & , \quad |\ell| > N \end{cases}$$

Seja então seq1=**Polarize**[SMC[{1,1,0,0,1,1}]]

**CorrelacaoAperiodica**[ seq1, seq1, 4]=-1

autocorrelacoesaperiodicas=Table[**CorrelacaoAperiodica**[ seq1, seq1, d],{d,-(Length[seq1]-1), (Length[seq1]-1)}

Observe-se que aqui o intervalo utilizado para o cálculo foi de -(N-1) à (N-1).

{1, -2, 1, 0, -1, -4, -1, 0, 1, 0, 1, 2, 3, -2, 1, 0, -1, -6, -7, 6, 1, 0, 1, -6, -9, 4, -1, 0, -1, 0, -1, 0, -1, 0, -5, 8, 5, -2, -1, -2, -7, 6, 5, 0, -1, -2, 1, -4, -3, -2, -1, -2, -1, 0, 3, 0, -1, -2, 1, -2, 63, -2, 1, -2, -1, 0, 3, 0, -1, -2, -1, -2, -3, -4, 1, -2, -1, 0, 5, 6, -7, -2, -1, -2, 5, 8, -5, 0, -1, 0, -1, 0, -1, 0, -1, 0, -1, 4, -9, -6, 1, 0, 1, 6, -7, -6, -1, 0, 1, -2, 3, 2, 1, 0, 1, 0, -1, -4, -1, 0, 1, -2, 1}

Representando graficamente a lista acima, obtém-se:

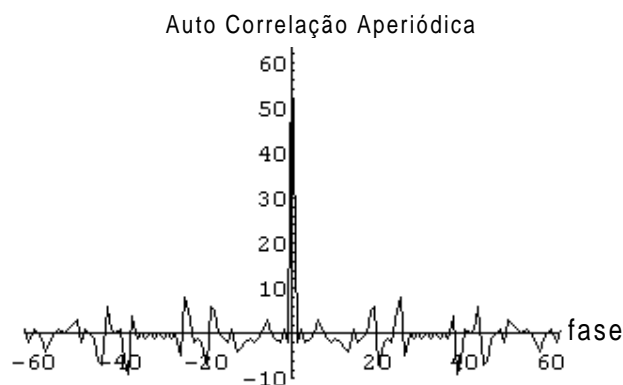


Fig. 4.15 Gráfico da Auto Correlação Aperiódica

Obteve-se um gráfico simétrico em relação à origem, como esperado.

Os valores resultantes são:  $\{-9, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 8, 63\}$

Com as seguintes ocorrências:  $\{-9, 2\}, \{-7, 4\}, \{-6, 4\}, \{-5, 2\}, \{-4, 4\}, \{-3, 2\}, \{-2, 18\}, \{-1, 26\}, \{0, 26\}, \{1, 18\}, \{2, 2\}, \{3, 4\}, \{4, 2\}, \{5, 4\}, \{6, 4\}, \{8, 2\}, \{63, 1\}$

Para o intervalo considerado, o gráfico é simétrico e assim tem-se quantidades pares para todos os valores exceto para o valor 63 que corresponde exatamente ao deslocamento 0 quando a auto correlação aperiódica equivale à periódica.

No gráfico a seguir são plotadas os valores dos pesos

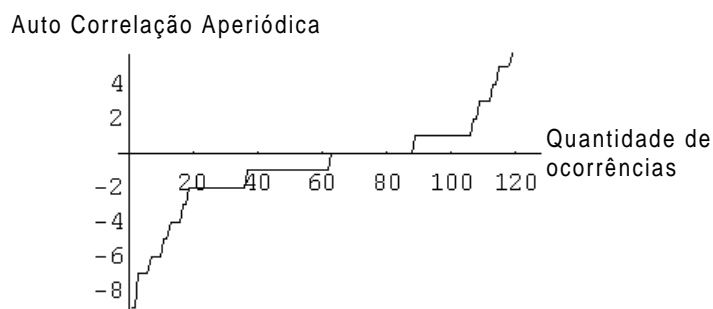


Fig. 4.16 Gráfico de Pesos da Auto Correlação Aperiódica (SMC)

### **Correlação Cruzada Aperiódica**

Sejam então novamente  $\text{seq1} = \text{Polarize}[\text{SMC}[\{1,1,0,1,1,0\}]]$  e  $\text{seq2} = \text{Polarize}[\text{SMC}[\{1,0,0,0,0,1\}]]$

$\text{correape} = \text{Table} [ \text{CorrelacaoAperiodica} [ \text{seq1}, \text{seq2}, l], \{1, 0, \text{Length} [\text{seq1}] - 1\}]$

$\text{correape} = \{-1, 14, -1, 0, 1, -14, 5, 0, 1, -4, -3, 10, -1, 0, 3, 0, -1, 2, 13, 14, 1, -12, 1, 4, 9, 6, -5, -2, 11, -10, 1, -4, 1, -6, -3, -14, 1, 4, 1, -6, -7, -8, 3, 4, 5, -12, -1, -2, 5, 2, -1, -2, -1, -2, 1, -2, -1, -4, -1, 0, 1, -2, 1\}$

Valores Resultantes:  $\{-14, -12, -10, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, 14\}$

Com as seguintes ocorrências:  $\{\{-14, 2\}, \{-12, 2\}, \{-10, 1\}, \{-8, 1\}, \{-7, 1\}, \{-6, 2\}, \{-5, 1\}, \{-4, 3\}, \{-3, 2\}, \{-2, 6\}, \{-1, 9\}, \{0, 5\}, \{1, 11\}, \{2, 2\}, \{3, 2\}, \{4, 3\}, \{5, 3\}, \{6, 1\}, \{9, 1\}, \{10, 1\}, \{11, 1\}, \{13, 1\}, \{14, 2\}\}$

### **Equivalente Linear**

O equivalente linear L é um número que indica a quantidade de células do menor conjunto possível formado por um registrador de deslocamento, com as respectivas conexões lineares, capaz de reconstruir a sequência dada.

Para a obtenção desse número referente à uma dada sequência pode-se seguir os seguintes passos.

a) Seja dada uma sequência qualquer, por exemplo:

$\text{seq1} = \text{SMC} [ \{1, 1, 0, 0, 1, 1\} ] = \{1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1\}$

b) A seguir obtém-se o polinômio correspondente à sequência

$$\text{polinomioseq1} = \text{Sum} [ \text{seq1}[[n]] z^{(\text{Length} [\text{seq1}]-n)}, \{n, 1, \text{Length} [\text{seq1}]\}] = 1 + z^6 + z^7 + z^8 + z^9 + z^{12} + z^{15} + z^{17} + z^{19} + z^{22} + z^{23} + z^{25} + z^{30} + z^{34} + z^{36} + z^{37} + z^{39} + z^{40} + z^{41} + z^{42} + z^{43} + z^{44} + z^{46} + z^{48} + z^{49} + z^{50} + z^{54} + z^{55} + z^{58} + z^{59} + z^{60} + z^{62}.$$

c) Obtenção do polinômio gerador

1) Obtém-se máximo divisor comum entre polinomioseq1 e  $z^{(\text{Length}[\text{seq1}]-1)}$

$$\text{poliMDC} = \text{PolynomialGCD} [\text{polinomioseq1}, z^{\text{Length} [\text{seq1}]-1}, \text{Modulus} \rightarrow 2] = 1 + z + z^2 + z^3 + z^6 + z^9 + z^{11} + z^{13} + z^{16} + z^{17} + z^{19} + z^{24} + z^{28} + z^{30} + z^{31} + z^{33} + z^{34} + z^{35} + z^{36} + z^{37} + z^{38} + z^{40} + z^{42} + z^{43} + z^{44} + z^{48} + z^{49} + z^{52} + z^{53} + z^{54} + z^{56} + z^{57}$$

2) Efetua-se o quociente entre  $z^{\text{Length}[\text{seq1}]-1}$  e poliMDC módulo 2

$$\text{Polinômio\_Gerador} = \text{PolynomialMod} [\text{PolynomialQuotient} [z^{\text{Length}[\text{seq1}]-1}, \text{poliMDC}, z], 2] = 1 + z + z^4 + z^5 + z^6.$$

Obs.: O polinômio gerado é o recíproco daquele que está sendo usado neste trabalho, pelo fato de que aqui está sendo adotada uma sistemática diferente da costumeiramente utilizada. Para obter-se o polinômio utilizado deve-se agora dividir o resultado obtido por  $z^{\text{Exponent}(\text{Polinômio\_Gerador})}$  e multiplicar cada expoente por -1. O método aqui adotado utiliza funções do programa **Mathematica** e portanto possuirá uma característica distinta.

$$\text{coeficientes} = \text{CoefficientList} [\text{Polinômio\_Gerador}, z]$$

$$\text{Reverse} [\text{coeficientes}]$$

$$\text{Polinômio\_Gerador} = \text{Sum} [\text{coeficientes}[[i]] z^{(i-1)}, \{i, 1, \text{Length}[\text{coeficientes}]\}]$$

d) Equivalente Linear

O equivalente linear é igual ao grau do polinômio gerador. Este pode ser obtido através da função do *Mathematica* *Exponent*[].

$$L = \text{Exponent}[\text{Polinômio\_Gerador}, z] = 6$$

No anexo há uma função para o cálculo direto do equivalente linear, que poderia ter sido usada aqui. No entanto optou-se por esta forma para exibir os detalhes da função, pois os mesmos são etapas importantes em outras fases deste trabalho.

Seja então a seguinte sequência seq1 = **SMC** [ { 1, 1, 0, 0, 1, 1 } ]

$$\text{EquivalenteLinear} [\text{seq1}] = 6$$

### **Cálculo da Interferência de Múltiplo Acesso**<sup>3,4</sup>

Dado um grupo de usuários, onde cada usuário possui uma sequência de código distinta num sistema CDMA assíncrono (vide capítulo 2) tem-se as seguintes relações de interesse:

$$\mu_{k,i}(n) = \sum_{\ell=1-N}^{N-1} C_{k,i}(\ell) C_{k,i}(\ell + n)$$

$$\text{SNR}_i = \left\{ \left( 6N^3 \right)^{-1} \sum_{\substack{k=1 \\ k \neq i}}^K \left\{ 2\mu_{k,i}(0) + \mu_{k,i}(1) \right\} + \frac{N_0}{A^2 T} \right\}^{-1/2}$$

$$\beta_{k,i} = 2\mu_{k,i}(0) + \mu_{k,i}(1)$$

O parâmetro  $\beta_{k,i}$ , que representa a interferência do usuário k sobre o usuário i, é a parte que será destacada adiante.

Para exemplificar seja uma família de sequências composta por 6 SMC's de grau seis.

$$[103], [141] - [147], [163] - [155], [133]$$

SMC103=**SMC**[{1,0,0,0,0,1}] SMC103p=Polarize[SMC103];

SMC141=**SMC**[{1,1,0,0,0,0}] SMC141p=Polarize[SMC141];

SMC147=**SMC**[{1,1,0,0,1,1}] SMC147p=Polarize[SMC147];

SMC163=**SMC**[{1,1,1,0,0,1}] SMC163p=Polarize[SMC163];

SMC155=**SMC**[{1,1,0,1,1,0}] SMC155p=Polarize[SMC155];

SMC133=**SMC**[{1,0,1,1,0,1}] SMC133p=Polarize[SMC133];

familiap={SMC103p, SMC141p, SMC147p, SMC163p, SMC155p, SMC133p}

Após construir-se o grupo acima, realiza-se o cálculo do  $\beta_{k,i}$ ,  $\mu_{k,i}(0)$ ,  $\mu_{k,i}(1)$ . A lista a seguir exhibe os valores destes parâmetros, sendo que a primeira linha refere-se à SMC103p com as demais cinco, a segunda linha refere-se a SMC141p com as demais quatro e assim por diante.

```
{
  {{8534, 4359, -184}, {7750, 3959, -168}, {7710, 3999, -288}, {8478, 4319, -160},
  {7606, 3959, -312}}, {{7582, 3903, -224}, {8102, 4103, -104}, {8358, 4263, -168},
  {8414, 4287, -160}},
  {{8694, 4567, -440}, {7830, 3991, -152}, {8494, 4431, -368}},
  {{7934, 4063, -192}, {8950, 4471, 8}},
  {{9078, 4615, -152}}
}
```

Para construir-se esta lista utilizou-se a seguinte rotina:

*Table*[ {**Beta***ij*[ familiap[[i]], familiap[[j]]],

**funcaoMi**[familiap[[i]], familiap[[j]]],

**funcaoMi**[familiap[[i]], familiap[[j]],1}],

{i, 1, *Length*[familiap]-1},{j, i+1, *Length*[familiap]}}

Sejam então as matrizes de betas apresentadas a seguir, onde betas1 refere-se a interferência dos demais usuários sobre a primeira seqüência, betas2 refere-se a interferência dos demais usuários sobre a segunda seqüência e assim por diante (note-se que não existe interferência de uma seqüência sobre ela própria, evidentemente).

betas1={8534, 7750, 7710, 8478, 7606}, Média=8015,6

betas2={8534, 7582, 8102, 8358, 8414}, Média=8198

betas3={7750, 7582, 8694, 7830, 8494}, Média=8070

betas4={7710, 8102, 8694, 7934, 8950}, Média=8278

betas5={8478, 8358, 7830, 7934, 9078}, Média=8335,6

betas6={7606, 8414, 8494, 8950, 9078}, Média=8508,4

Média dos betas=8234,27 (observe-se que o valor médio de  $\beta_{k,i}$  para seqüências randômicas é igual a  $2N^2=7938$ )

$SNR_1=6,11834$   $Q(SNR_1)=\text{FuncaoQ}[SNR_1]=4,73*10^{-10}$

$SNR_2=6,04989$   $Q(SNR_2)=\text{FuncaoQ}[SNR_2]=7,25*10^{-10}$

$SNR_3=6,09768$   $Q(SNR_3)=\text{FuncaoQ}[SNR_3]=5,38*10^{-10}$

$SNR_4=5,96549$   $Q(SNR_4)=\text{FuncaoQ}[SNR_4]=1,22*10^{-09}$

$SNR_5=5,99975$   $Q(SNR_5)=\text{FuncaoQ}[SNR_5]=9,88*10^{-10}$

$$\text{SNR}_6=5,93851 \quad Q(\text{SNR}_6)=\text{FuncaoQ}[\text{SNR}_6]=1,44*10^{-09}$$

Este exemplo ilustra um sistema assíncrono onde a cada usuário é atribuída uma sequência de comprimento de 63 e o número de usuários é igual a seis (que é aproximadamente 10% do comprimento da sequência). Neste sistema a probabilidade de erro limitante é de  $1,44*10^{-09}$ .

1 - tipo da sequência=SMC

2 - Critério de seleção=não aleatório

3 -  $n=6$

4 -  $N=63$

5 -  $2N^2=7938$

6 - usuários=6

7 -  $(\text{usuários}/N)\%=9,52$

8 - beta médio=8234,27

9 - Probabilidade de erro limitante= $1,44*10^{-09}$

{SMC, "Não Aleatório", 6; 63; 7938; 6; 9,52; 8234,27;  $1,44*10^{-9}$ }

para o grau 7 obtém-se

{SMC; "Aleatório"; 7; 127; 32258; 18; 14,2; 32248,04;  $1,32*10^{-6}$ }

Pelos resultados obtidos, que podem ser verificados para outros graus também, constata-se que as SMC's são sequências próximas ao que se espera de sequências ideais. As propriedades de correlação (principalmente as de auto correlação periódica)

são boas, quando comparadas com as de outras famílias de seqüências como as aqui tratadas.

Estas seqüências são fáceis de se gerar (o algoritmo é pequeno e ocupa pouca memória do sistema) e devido a sua característica de auto correlação periódica fora de fase assumir um só valor, tem-se uma facilidade adicional para o sincronismo.

#### 4.2.2 GOLD

Esta família de seqüências é formada através da soma mod2 (bit a bit) entre um par preferencial de SMC's, para todos os deslocamentos possíveis entre as mesmas e desta forma o número de elementos desta família é igual ao comprimento mais 2.

No tocante aos valores do espectro de correlação cruzada periódica as seqüências de Gold apresentam valores idênticos aos obtidos para as SMC's geradoras.

##### 4.2.2.1 PROPRIEDADES GERAIS

Inicialmente ilustra-se a construção de grupos de pares preferenciais para um exemplo de grau 6.

###### a) Obtenção dos polinômios

$\text{polis} = \mathbf{Primitivos}[6] = \{ \{1, 0, 0, 0, 0, 1\}, \{1, 0, 1, 1, 0, 1\}, \{1, 1, 0, 0, 0, 0\}, \{1, 1, 0, 0, 1, 1\}, \{1, 1, 0, 1, 1, 0\}, \{1, 1, 1, 0, 0, 1\} \}.$

Obs.: Cada vetor acima representa um polinômio de grau 6 em ordem decrescente de seus coeficientes, com o elemento independente não representado.

###### b) Seleção de pares preferenciais

Calcula-se a auto correlação cruzada periódica entre as SMC's geradas pelos polinômios acima e verifica-se aqueles grupos em que obtém-se apenas três valores distintos.

```

correlacoes=Table[Union[Table[CorrelacaoPeriodica[Polarize[Smc[polis[[i]]]
],Polarize[Smc[polis[[j]]]],l],{1,1,2^Length[polis[[1]]}]],{i,1,6},{j,1,6}]

correlacoes={

{{-1, 63}, {-17, -1, 15}, {-13, -9, -5, -1, 3, 7, 11, 15}, {-17, -1, 15}, {-9, -1, 7,
15, 23}, {-9, -1, 7, 15, 23}},

{{-17, -1, 15}, {-1, 63}, {-9, -1, 7, 15, 23}, {-9, -1, 7, 15, 23}, {-13, -9, -5, -1, 3,
7, 11, 15}, {-17, -1, 15}},

{{-13, -9, -5, -1, 3, 7, 11, 15}, {-9, -1, 7, 15, 23}, {-1, 63}, {-9, -1, 7, 15, 23}, {-
17, -1, 15}, {-17, -1, 15}},

{{-17, -1, 15}, {-9, -1, 7, 15, 23}, {-9, -1, 7, 15, 23}, {-1, 63}, {-17, -1, 15}, {-
13, -9, -5, -1, 3, 7, 11, 15}},

{{-9, -1, 7, 15, 23}, {-13, -9, -5, -1, 3, 7, 11, 15}, {-17, -1, 15}, {-17, -1, 15}, {-
1, 63}, {-9, -1, 7, 15, 23}},

{{-9, -1, 7, 15, 23}, {-17, -1, 15}, {-17, -1, 15}, {-13, -9, -5, -1, 3, 7, 11, 15}, {-
9, -1, 7, 15, 23}, {-1, 63}}

}

```

Na lista acima selecionam-se os grupos de três valores. A primeira linha representa as correlações da primeira seqüência com as demais inclusive a própria. A segunda linha é referente a segunda seqüência e assim sucessivamente. Os conjuntos com apenas dois valores equivalem às auto correlações periódicas pois correspondem a SMC's. Deve-se observar, por exemplo, que o fato da seqüência 1 formar um par preferencial com as seqüências 2 e 4, não significa necessariamente que as seqüências 2 e 4 formem um par preferencial.

Por exemplo, selecionando-se os polinômios correspondentes ao segundo conjunto da linha um tem-se:

$$\{1, 0, 0, 0, 0, 1\} \text{ e } \{1, 0, 1, 1, 0, 1\}$$

Constrói-se a família:

$$\text{FamiliaGold} = \mathbf{Gold}[\{1, 0, 0, 0, 0, 1\}, \{1, 0, 1, 1, 0, 1\}];$$

### **Auto Correlação Periódica**

$\text{auto} = \text{Table}[\mathbf{CorrelacaoPeriodica}[\mathbf{Polarize}[\text{FamiliaGold}[[i]]], \mathbf{Polarize}[\text{FamiliaGold}[[j]]], f], \{i, 1, 64\}, \{j, i+1, 65\}, \{f, 0, 62\}];$

$$\text{Union}[\text{auto}] = \{-17, -1, 15, 63\}$$

### **Correlação Cruzada Periódica**

Calculando-se todas correlações cruzadas periódicas entre todas as seqüências desta família para todos os deslocamentos, obtém-se os valores:

$\text{correlacoes} =$

$= \text{Table}[\mathbf{CorrelacaoPeriodica}[\mathbf{Polarize}[\text{FamiliaGold}[[i]]], \mathbf{Polarize}[\text{FamiliaGold}[[j]]], f], \{i, 1, 64\}, \{j, i+1, 65\}, \{f, 0, 62\}];$

$$\text{Union}[\text{Flatten}[\text{correlacoes}]] = \{-17, -1, 15\}$$

A seguinte relação é utilizada para a verificação dos valores esperados para a correlação cruzada periódica entre as seqüências da família de Gold.

$$\theta_{u,v}(\ell) = N - 2\text{wt}(u \oplus T^\ell v)$$

Sejam duas SMC's  $a$  e  $b$  de mesmo grau, então

$$u = a + T^i b \quad \text{e} \quad v = a + T^j b$$

$$\theta_{u,v}(\ell) = \begin{cases} -1 & \text{para } \ell = 0 \text{ ou } \ell = j-i \\ N - 2\text{wt}(a \oplus T^{k-w}b) = \theta_{a,b}(k-w) & \text{outros casos} \end{cases}$$

onde  $i, j, k$  e  $w$  são inteiros.

Com isto fica evidente que o espectro de correlação cruzada periódica para as seqüências de Gold sempre será composto pelos valores do espectro da correlação cruzada periódica das SMC's. O mesmo se aplica à função de auto correlação periódica. Este é um resultado genérico e independe do grau das SMC's (Gold é um caso particular).

### **Correlação Cruzada Aperiódica**

Toda a correlação cruzada aperiódica está limitada por:

$$|C_{i,j}(\ell)| \leq \sqrt{C_{i,j}(0) \cdot C_{i,j}(0)} \leq N$$

A expressão a seguir possibilita o cálculo de um limite inferior para a máxima correlação cruzada aperiódica e/ou auto correlação aperiódica entre um grupo de  $K$  usuários, independentemente das seqüências que estão sendo usadas.

Sejam definidos os seguintes parâmetros:

$$C_c = \text{Max} \{ |C_{i,j}(\ell)| : 0 \leq \ell \leq N-1 \}$$

$$C_a = \text{Max} \{ |C_i(\ell)| : 0 < \ell \leq N-1 \}$$

$$C_{\text{max}} = \text{Max} \{ |C_c|, |C_a| \}$$

$K$  o número de usuários (seqüências)

onde  $i$  e  $j$  são elementos do grupo de usuários. Nestas circunstâncias pode-se escrever:

$$\frac{(2N-1)}{N} \cdot \left( \frac{(C_c)^2}{N} \right) + \frac{2(N-1)}{N(K-1)} \cdot \left( \frac{(C_a)^2}{N} \right) \geq 1$$

e esta última implica em:

$$(C_{\max})^2 \geq \frac{N^2(K-1)}{(2NK-K-1)}$$

Este resultado é similar ao da equação (3.28), válida para o caso periódico. Ver JESZENSKY<sup>4</sup>.

Os gráficos a seguir exibem o comportamento desta expressão, para os casos onde o comprimento é de 63 e 1000, e com K variando de zero até um valor igual ao comprimento da seqüência:

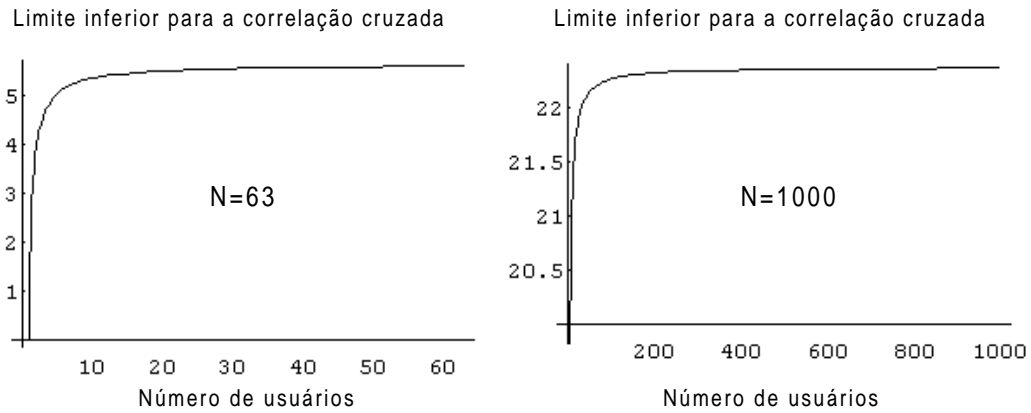


Fig.

#### 4.17 Limite de Welch.

O valor assintótico destas curvas é  $\sqrt{0,5N}$ , e essa tendência é muito rápida, pois observa-se que com um pequeno número de usuários atinge-se um valor próximo a este limite.

Para a família de Gold, exibe-se a seguir alguns dos valores obtidos para a correlação cruzada aperiódica.

grau 5

$\{-7, -6, -4, -3, -1, 0, 1, 2, 3, 5, 6, 7, 8\}$

grau 6

$\{-19, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 14, 16, 17\}$

grau 7

$\{-23, -18, -17, -16, -15, -14, -13, -12, -11, -10, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}$

O gráfico a seguir representa a correlação cruzada aperiódica para o grau 7, entre duas seqüências de Gold (selecionou-se para este exemplo as seqüências de números 10 e 45 ao acaso). A família foi gerada pelos polinômios [211] e [217].

Foram seguidos os seguintes passos:

fam=**Gold**[{1, 0, 0, 0, 1, 0, 0},{1, 0, 0, 0, 1, 1, 1}];

fampp=**Polarize**[fam];

seq1=fampp[[10]]; seq2=fampp[[45]];

correlacao=**Table**[**CorrelacaoAperiodica**[seq1,seq2,f],{ f, -*Length*[seq1]+ 1, *Length*[seq1] - 1}]

coordenadas=**Table**[{i,correlacao[[i+127]]},{i,-126,126}]

**ListPlot**[coordenadas, *PlotJoined*->*True*, *PlotRange*->{{-126,126},{-21,127}}]

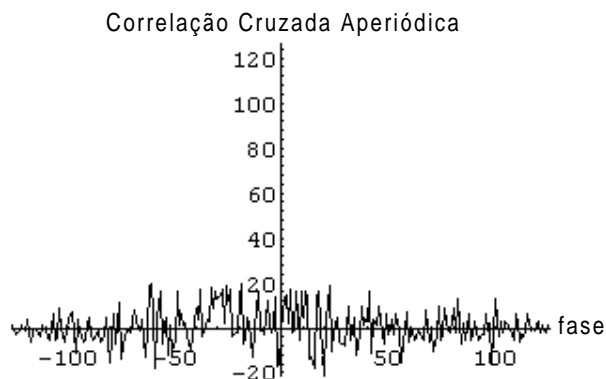


Fig. 4.18 Correlação Cruzada Aperiódica-grau 7

O valor máximo é igual a 20 e o mínimo -23

### **Equivalente Linear**

O exemplo a seguir ilustra o cálculo do equivalente linear para todas as seqüências de uma família de Gold (FamiliaGold) de grau seis:

$Table[EquivalenteLinear[FamiliaGold[[i]]],\{i,1,Length[FamiliaGold]\}]=\{6, 6, 12, 12, ..., 12\}$

Como era de se esperar, as seqüências de Gold possuem um equivalente linear igual a  $2n=12$ , exceto, é claro, para as SMC's geradoras.

### **Cálculo da Interferência de Múltiplo Acesso**

Analogamente ao realizado para as SMC's, selecionou-se aleatoriamente 6 seqüências de Gold, com grau 6, de uma família de comprimento 65 e calculou-se a interferência multiusuário.

$betas1=\{6206, 9350, 7858, 9510, 6842\}$ , Média=7953,2

$betas2=\{6206, 6478, 7466, 7742, 7162\}$ , Média=7010,8

$betas3=\{9350, 6478, 8034, 8870, 8058\}$ , Média=8158,0

betas4={7858, 7466, 8034, 7834, 6686}, Média=7575,6

betas5={9510, 7742, 8870, 7834, 7274}, Média=8246,0

betas6={6842, 7162, 8058, 6686, 7274}, Média=7204,4

Média dos betas=7691,33 (observe-se que o valor médio de  $\beta_{k,i}$  para seqüências randômicas é igual a  $2N^2=7938$ )

A maior soma dos betas ocorreu para betas5, logo a Pe limitante será calculada através deste grupo.

$$Pe=8,08 * 10^{-10}$$

Observe-se que mesmo com a escolha aleatória das seqüências o resultado obtido foi melhor do que aquele encontrado para as SMC's.

#### 4.2.3 GOLD LIKE

As seqüências Gold Like, a princípio, apresentam a desvantagem de só existirem para graus múltiplos de quatro. No entanto, o número de famílias é proporcionalmente superior às de Gold, pois para cada SMC é possível construir-se uma família com  $N+1=2^n$  seqüências. Por exemplo, para o grau 8 existem 16 SMC, logo é possível obter-se 16 famílias de seqüências, onde cada família possui  $2^8=256$  elementos, sendo que cada seqüência possui  $2^8-1=255$  bits. Outra vantagem desta família é que não há a necessidade de pesquisar-se por seqüências preferenciais, pois para qualquer família construída obtém-se sempre os mesmos valores para o espectro de correlação cruzada periódica. Os limites para a correlação cruzada periódica são idênticos às de Gold, no entanto os valores do espectro de correlação cruzada periódica são constituídos por 5 valores distintos.

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

onde  $s(n)$  e  $t(n)$  são calculáveis por:

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

Gera-se, por exemplo, uma família Gold Like utilizando-se a função:

$\text{Famigl} = \text{GoldLike}[\{1, 1, 1, 1, 0, 0, 1, 1\}];$

$\text{Famigl} = \text{Polarize}[\text{Famigl}];$

onde o argumento é equivalente a um polinômio primitivo de grau 8, que pode ser obtido pela função **Primitivos**[8]. Esta família possui 256 seqüências.

As auto correlações periódicas, bem como as correlações cruzadas periódicas, podem ser calculadas como descrito a seguir:

### Auto Correlações Periódicas

$\text{Table}[\text{CorrelacaoPeriodica}[\text{Famigl}[[i]], \text{Famigl}[[i]], f], \{i, 1, \text{Length}[\text{Famigl}]\}, \{f, 0, \text{Length}[\text{Famigl}[[i]]]-1\}]$

No exemplo foram obtidos os seguintes valores:

$\{-33, -17, -1, 15, 31, 255\}$

O valor 255 corresponde ao deslocamento zero entre as seqüências.

### Correlação Cruzada Periódica

$\text{Table}[\text{CorrelacaoPeriodica}[\text{Famigl}[[i]], \text{Famigl}[[j]], f], \{i, 1, \text{Length}[\text{Famigl}]\}, \{j, 1, \text{Length}[\text{Famigl}]\}, \{f, 0, \text{Length}[\text{Famigl}[[i]]]-1\}]$

No exemplo foram obtidos os seguintes valores:

$\{-33, -17, -1, 15, 31\}$

### Auto Correlação Aperiódica

*Table[ CorrelacaoAperiodica[ Famigl[[ i ]], Famigl[[ i ]], f ], {i, 1, Length[Famigl]}, {f, 0, Length[Famigl[[i]]]-1}]*

No exemplo foram obtidos os seguintes valores:

{-33, -28, -22, -19, -18, -17, -16, -15, -14, -13, -12, -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 28, 30, 255}

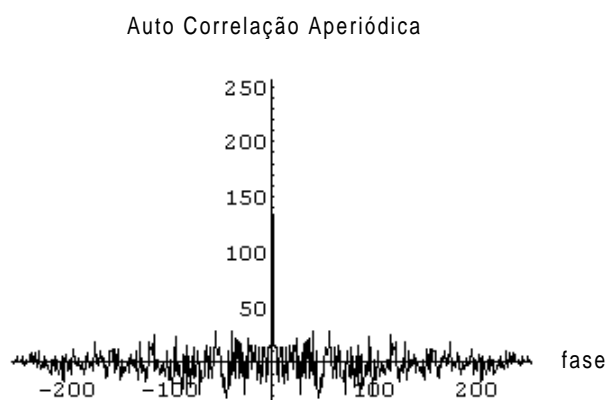


Fig. 4.19a Auto Correlação Aperiódica-Gold Like grau 8

e excluindo o valor na origem, tem-se:

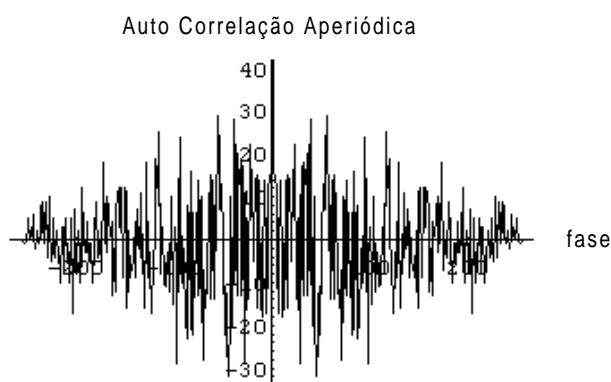


Fig. 4.19b Auto Correlação Aperiódica-Gold Like grau 8

### Correlação Cruzada Aperiódica

*Table[ CorrelacaoAperiodica[ Famigl[[ i ]], Famigl[[ j ]], f ], {i, 1, Length[Famigl]}, {j, 1, Length[Famigl]}, {f, 0, Length[Famigl[[i]]]-1}]*

No exemplo foram obtidos os seguintes valores:

{-30, -27, -24, -23, -22, -21, -19, -18, -17, -16, -15, -14, -13, -12, -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 31, 34}

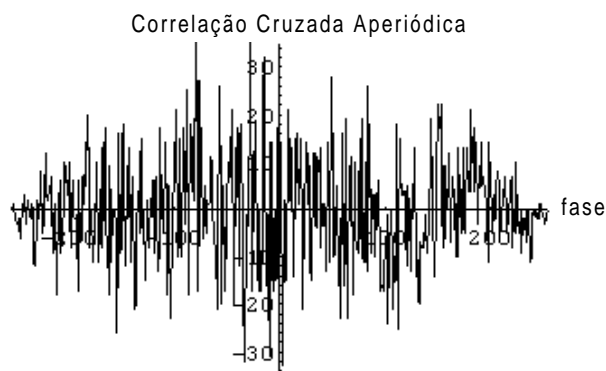


Fig. 4.20 Correlação Cruzada Aperiódica-Gold Like grau 8

### Equivalente Linear

O equivalente linear, neste exemplo, é igual a  $2n=16$

Para calcular-se o equivalente linear para toda a família seja o exemplo.

*gl2=GoldLike[{1, 1, 1, 1, 0, 0, 1, 1}];*

*Table[EquivalenteLinear[gl2[[i]]], {i, 1, Length[gl2]}]=*

*= {8, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16}*

### **Cálculo da Interferência de Múltiplo Acesso**

Analogamente ao realizado para as SMC's, selecionou-se aleatoriamente 6 seqüências Gold Like, com grau 8, de uma família de comprimento 256 e calculou-se a interferência multiusuário.

betas1={144898, 132638, 136462, 128002, 127422}, Média=133884.

betas2={144898, 134266, 129154, 125926, 109418}, Média=128732.

betas3={132638, 134266, 136750, 144810, 128390}, Média=135371.

betas4={136462, 129154, 136750, 146690, 124950}, Média=134801.

betas5={128002, 125926, 144810, 146690, 124250}, Média=133936.

betas6={127422, 109418, 128390, 124950, 124250}, Média=122886.

Média dos betas=131602. (observe-se que o valor médio de  $\beta_{k,i}$  para seqüências randômicas é igual a  $2N^2=130050$ )

A maior soma dos betas ocorreu para betas5, logo a  $P_e$  limitante será calculada através deste grupo.

$$P_e=1,54*10^{-29}.$$

O melhor resultado para a  $P_e$  já era esperado, pois manteve-se o número de usuários e aumentou-se o comprimento das seqüências.

#### **4.2.4 GOLD BCH DUAL**

Esta família é semelhante à anterior e por isso obtém-se um algoritmo praticamente idêntico. A diferença é que existem também para valores de graus pares não múltiplos de quatro.

O grau deve obedecer a seguinte restrição:

$$\text{gdc}(3, 2^n - 1) = 3, \quad \forall \quad n \quad \text{par}$$

Os valores para as auto correlações periódicas e correlações cruzadas periódicas são dados por:

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

onde

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

A vantagem portanto deste grupo é que existe um número maior de possibilidades para a construção de famílias. Seja um polinômio primitivo representado por  $\{1, 1, 0, 0, 0, 0\}$ .

A família Gold BCH Dual pode ser construída através da seguinte função:

famibch=**GoldBCHdual**[{1, 1, 0, 0, 0, 0}];

famibch=Polarize[famibch];

O número de seqüências da família é igual ao da Gold Like, isto é,  $2^n$ .

*Length*[famibch]=64

Os pesos para as seqüências desta família são:

{24, 28, 32, 36, 40}

### **Auto Correlação Periódica.**

{-17, -9, -1, 7, 15, 63}

onde o valor 63 refere-se ao deslocamento zero. Estes valores podem ser calculados através das seguintes funções:

*Table[ CorrelacaoPeriodica[ famibch[[ i ]], famibch[[ i ]], f ], {i, 1, Length[famibch]}, {f, 0, Length[famibch][[i]]-1}]*

Analogamente obtém-se os valores para a correlação cruzada periódica, aperiódica e auto correlação periódica. No exemplo foram obtidos os seguintes valores:

### **Correlação Cruzada Periódica**

{-17, -9, -1, 7, 15}

### **Auto Correlação Aperiódica**

{-14, -13, -11, -10, -9, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 17, 63}

### **Correlação Cruzada Aperiódica**

{-20, -12, -9, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14}

### **Equivalente Linear**

Analogamente à família Gold, esta família também possui um equivalente linear igual a  $2n$ , exceto para a SMC pertencente a família.

### **Cálculo da Interferência de Múltiplo Acesso**

Analogamente ao realizado para as SMC's, selecionou-se aleatoriamente 6 seqüências de Gold Like, com grau 6, de uma família de comprimento 64 e calculou-se a interferência multiusuário.

betas1={7022, 7090, 7746, 7110, 7958}, Média=7385.2

betas2={7022, 8946, 8570, 7046, 7958}, Média=7908.4

betas3={7090, 8946, 7182, 7282, 7522}, Média=7604.4

betas4={7110, 8570, 7182, 7866, 7634}, Média=7672.4

betas5={7110, 7046, 7282, 7866, 8670}, Média=7594.8

betas6={7958, 7958, 7522, 7634, 8670}, Média=7948.4

Média dos betas=7685.6 (observe-se que o valor médio de  $\beta_{k,i}$  para seqüências randômicas é igual a  $2N^2=7938$ ).

A maior soma dos betas ocorreu para betas6, logo a Pe limitante será calculada através deste grupo.

$$Pe=4,02*10^{-10}.$$

Este resultado para a Pe é pouco melhor ao obtido com as SMC e as de Gold.

#### 4.2.5 KASAMI PEQUENO

Dentre as famílias até o momento analisadas, esta é a que possui os menores valores para o espectro de correlação cruzada periódica; no entanto o número de elementos da família é inferior às anteriores. O valor máximo para a auto correlação periódica é  $s(n)$ , e este valor é muito próximo ao limite de Welch, o que faz com que esta família possa ser considerada ótima sob o aspecto de espectro de correlação cruzada periódica.

O número de elementos na família é igual a  $2^{n/2}$  e para cada SMC de grau par pode-se construir uma família, sendo que cada seqüência terá comprimento  $2^n - 1$ . Este grupo apresenta uma vantagem adicional que é a de possuir um equivalente linear superior quando comparado às SMC's.

Os valores para as auto correlações periódicas e correlações cruzadas periódicas são dados por:

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

onde

$$s(n) = 2^{n/2} + 1$$

Seja então,  $n = 6$ :

**Primitivos**[6]={ {1, 0, 0, 0, 0, 1}, {1, 0, 1, 1, 0, 1}, {1, 1, 0, 0, 0, 0}, {1, 1, 0, 0, 1, 1}, {1, 1, 0, 1, 1, 0}, {1, 1, 1, 0, 0, 1} }

famikp=**KasamiPequeno**[ {1, 0, 0, 0, 0, 1} ];

famikp=Polarize[famikp];

Os pesos para as seqüências desta família são:

$$\{28, 32, 36\}$$

Os valores para a auto correlação periódica são:

$$\{-9, -1, 7, 63\}$$

onde o valor 63 refere-se ao deslocamento zero.

Estas correlações podem ser calculadas através das seguintes funções:

*Table*[ **CorrelacaoPeriodica**[ Famikp[[ i ]], Famikp[[ i ]], f ], {i, 1, *Length*[Famikp]}, {f, 0, *Length*[Famikp[[i]]]-1} ]

Analogamente obtém-se os valores para a correlação cruzada periódica, aperiódica e auto correlação periódica.

Correlação Cruzada Periódica= $\{-9, -1, 7\}$

Auto Correlação Aperiódica= $\{-10, -8, 0, 5, 6, 7, 9\}$

Correlação Cruzada Aperiódica= $\{-13, -9, -8, -4, -1, 5, 6\}$

Esta família possui um equivalente linear  $3n/2=9$ .

Este equivalente pode ser obtido pela função:

$L=Table[ \text{EquivalenteLinear}[ \text{famikp}[[i]] ],\{i,1,Length[\text{famikp}]]\}=\{6, 9, 9, 9, 9, 9, 9, 9\}$

O primeiro elemento possui valor 6 e corresponde ao equivalente linear da sequência de máximo comprimento correspondente ao polinômio primitivo.

### **Cálculo da Interferência de Múltiplo Acesso**

Analogamente ao realizado para as SMC's, selecionou-se aleatoriamente 6 sequências de Kasami pequeno, com grau 6, de uma família de 8 sequências e calculou-se a interferência multiusuário.

$\text{betas1}=\{6870, 7530, 9206, 6426, 8098\}, \text{Média}=7626$

$\text{betas2}=\{6870, 7098, 7782, 7898, 7450\}, \text{Média}=7419.6$

$\text{betas3}=\{7530, 7098, 6674, 6462, 6878\}, \text{Média}=6928.4$

$\text{betas4}=\{9206, 7782, 6674, 7026, 7642\}, \text{Média}=7666$

$\text{betas5}=\{6426, 7898, 6462, 7026, 5686\}, \text{Média}=6699.6$

$\text{betas6}=\{8098, 7450, 6878, 7642, 5686\}, \text{Média}=7150.8$

Média dos betas=7248.4 (observe-se que o valor médio de  $\beta_{k,i}$  para seqüências randômicas é igual a  $2N^2=7938$ )

A maior soma dos betas ocorreu para betas4, logo a Pe limitante será calculada através deste grupo.

$$Pe=1,97*10^{-10}.$$

Esta família apresentou resultados semelhantes aos anteriores de mesmo grau.

#### 4.2.6 KASAMI GRANDE

Esta família pode ser considerada como uma ampliação das famílias de Kasami Pequeno, Gold e Gold Like pois é criada sobre estas. O número de seqüências desta família é consideravelmente maior que todas as famílias examinadas anteriormente. Pode-se construir uma família para cada SMC de grau par, mantendo-se os mesmos valores para a correlação cruzada periódica do que àqueles obtidos na famílias de Gold. O número de seqüências desta família é igual à:

$$2^{n/2} (2^n + 1) \quad n \equiv 2 \pmod{4}$$

$$2^{n/2} (2^n + 1) - 1 \quad n \equiv 0 \pmod{4}$$

Os valores para as auto correlações periódicas e correlações cruzadas periódicas são dados por:

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

onde  $s(n)$  e  $t(n)$  são calculáveis por:

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

Seja por exemplo  $n=6$ . Gera-se a família Kasami Grande utilizando a seguinte função:

Famikg= **KasamiGrande**[{1, 0, 0, 0, 0, 1}];

onde o argumento é equivalente a um polinômio primitivo de grau 6, que pode ser obtido pela função **Primitivos**[6]. Polarizando-se a família:

Famikg=Polarize[Famikg];

A quantidade de uns em cada seqüência da família é igual a um dos valores a seguir:

*Union[ Table[ Count[Famikg[[i]],1],{i, 1, Length[Famikg]}] ]*

{24, 28, 32, 36, 40}

Esta família possui  $2^{n/2}(2^n + 1) = 520$  seqüências.

As auto correlações periódicas bem como as correlações cruzadas periódicas podem ser calculadas utilizando-se a seguinte função:

### **Auto Correlações**

*Table[ CorrelacaoPeriodica[ Famikg[[ i ]], Famikg[[ i ]], f ], {i, 1, Length[Famikg]}, {f, 0, Length[Famikg[[i]]]-1}]*

No exemplo foram obtidos os valores:

{-17, -9, -1, 7, 15, 63}

O valor 63 é para o deslocamento zero entre as seqüências.

### **Correlação Cruzada Periódica**

*Table[ CorrelacaoPeriodica[ Famikg[[ i ]], Famikg[[ j ]], f ], {i, 1, Length[Famikg]}, {j, 1, Length[Famikg]}, {f, 0, Length[Famikg[[i]]]-1}]*

No exemplo foram obtidos os valores:

{-17, -9, -1, 7, 15}

### **Auto Correlação Aperiódica**

*Table[ CorrelacaoAperiodica[ Famikg[[ i ]], Famikg[[ i ]], f ], {i, 1, Length[Famikg]}, {f, 0, Length[Famikg[[i]]]-1}]*

No exemplo anterior os valores obtidos foram:

{-24, -22, -21, -20, -19, -18, -17, -16, -15, -14, -13, -12, -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23, 63}

### **Correlação Cruzada Aperiódica**

*Table[ CorrelacaoAperiodica[ Famikg[[ i ]], Famikg[[ j ]], f ], {i, 1, Length[Famikg]}, {j, 1, Length[Famikg]}, {f, 0, Length[Famikg[[i]]]-1}]*

No exemplo anterior os valores obtidos foram:

{-24, -22, -21, -20, -19, -18, -17, -16, -15, -14, -13, -12, -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23}

O equivalente linear para as seqüências desta família é calculável por:

$L=Table[EquivalenteLinear[Famikg[[i]]],\{i,1,Length[Famikg]\}]$

e onde obtém-se os valores {6, 9, 12, 15}

### **Cálculo da Interferência de Múltiplo Acesso**

Analogamente ao realizado para as SMC's, selecionou-se aleatoriamente 6

seqüências de Kasami grande, com grau 6, de uma família de 520 seqüências e calculou-se a interferência multiusuário.

$$\text{betas1}=\{6430, 8902, 6194, 8730, 6682\}, \text{ Média}=7387.6$$

$$\text{betas2}=\{6430, 6550, 8314, 6370, 7962\}, \text{ Média}=7125.2$$

$$\text{betas3}=\{8902, 6550, 7346, 11002, 8674\}, \text{ Média}=8494.8$$

$$\text{betas4}=\{6194, 8314, 7346, 6190, 7806\}, \text{ Média}=7170$$

$$\text{betas5}=\{8730, 6370, 11002, 6190, 6710\}, \text{ Média}=7800.4$$

$$\text{betas6}=\{6682, 7962, 8674, 7806, 6710\}, \text{ Média}=7566.8$$

Média dos betas=7590,8 (observe-se que o valor médio de  $\beta_{k,i}$  para seqüências randômicas é igual a  $2N^2=7938$ ).

A maior soma dos betas ocorreu para betas3, logo a Pe limitante será calculada através deste grupo  $Pe=1,39*10^{-9}$ .

#### 4.2.7 GMW

As seqüências GMW são seqüências não lineares que possuem valores para o espectro de correlação cruzada periódica e aperiódica coincidentes às SMC's; sua principal vantagem está no equivalente linear que é superior.

A construção das seqüências é baseada na função traço:

$$b_i = \text{Tr}_2^{2^j} ([\text{Tr}_2^{2^n}(\alpha^i)]^r)$$

O grau da seqüência n deve ser um número não primo, isto é:

$$n=J.K \quad \text{onde J e K são números inteiros.}$$

O parâmetro  $r$  que está no intervalo  $0 < r < 2^J - 1$  é um inteiro qualquer relativamente primo à  $2^J - 1$  e está ligado ao grau de não linearidade da seqüência. A cada valor distinto de  $r$  pode-se gerar a mesma seqüência deslocada, ou não, ou uma seqüência distinta. O parâmetro  $\alpha$  é um elemento primitivo do Corpo de Galois  $GF(2^n)$ . O número de seqüências distintas para um determinado grau é determinado por:

$$N_{GMW} = N_p(n) \cdot N_p(J)$$

onde  $N_p(g)$  é o número de polinômios primitivos de grau  $g$ .

Pode-se gerar uma seqüência através da seguinte função:

$seq = \text{GMW}[\text{polinômio}, J, r]$ ; o polinômio deve ser primitivo e expresso na variável  $x$ .

Exemplo:

Sejam as seguintes representações dos polinômios primitivos de grau 6:

**Primitivos**[6] = { {1, 0, 0, 0, 0, 1}, {1, 0, 1, 1, 0, 1}, {1, 1, 0, 0, 0, 0}, {1, 1, 0, 0, 1, 1}, {1, 1, 0, 1, 1, 0}, {1, 1, 1, 0, 0, 1} }

Para cada uma destas representações, constrói-se o polinômio na variável  $x$ , a seguir apresentado:

$pol = \{ x^6 + x + 1, x^6 + x^4 + x^3 + x + 1, x^6 + x^5 + 1, x^6 + x^5 + x^2 + x + 1, x^6 + x^5 + x^3 + x^2 + 1, x^6 + x^5 + x^4 + x + 1 \}$

$seqs = \text{Table}[\text{GMW}[pol[[i]]], 3, 3], \{i, 1, 6\}];$

Para ilustrar o cálculo das correlações selecionaram-se dois elementos da família acima construída, sendo estes equivalentes àqueles gerados pelos polinômios primitivos de grau 6,  $x^6 + x^5 + x^2 + x + 1$  e  $x^6 + x + 1$ , com  $J=3$  e  $r=3$ :

Sejam então:

$$\text{seq1} = \text{GMW}[x^6 + x^5 + x^2 + x + 1, 3, 3] = \{0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0\}$$

A auto correlação periódica gera valores idênticos aos obtidos por uma SMC:

$$\{-1, 63\}$$

$$\text{seq2} = \text{GMW}[x^6 + x + 1, 3, 3] = \{1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0\}$$

A correlação cruzada periódica entre estas duas seqüências gera o conjunto de valores:

$$\{-13, -9, -5, -1, 7, 11, 15\}$$

A Auto Correlação Aperiódica

$$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 63\} \quad \text{para a seq1}$$

$$\{-11, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 10, 63\} \quad \text{para a seq2}$$

A Correlação Cruzada Aperiódica gera o conjunto de valores:

$$\{-14, -13, -12, -11, -9, -8, -7, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 6, 7, 9, 10, 12\}$$

O cálculo do equivalente linear para esta classe de seqüências é obtido através expressão:

$$L = J(n/J)^w$$

onde w é o número de uns da representação, em base 2, do parâmetro r.

Assim no exemplo acima ter-se-á:

$$L=3.(6 / 3 )^2=12$$

que também pode ser obtida pela função genérica

$$L=\text{EquivalenteLinear}[ \text{seq1} ]=12$$

### **Cálculo da Interferência de Múltiplo Acesso**

Analogamente ao realizado nos exemplos anteriores, selecionaram-se aleatoriamente 6 seqüências de GMW, com grau 6, de uma família de 12, e calculou-se a interferência multiusuário.

$$\text{betas1}=\{7218, 10318, 7590, 7330, 7902\}, \text{Média}=8071.6$$

$$\text{betas2}=\{7218, 7538, 7482, 10942, 6938\}, \text{Média}=8023.6$$

$$\text{betas3}=\{10318, 7538, 7910, 7466, 8006\}, \text{Média}=8247.6$$

$$\text{betas4}=\{7590, 7482, 7910, 7602, 10382\}, \text{Média}=8193.2$$

$$\text{betas5}=\{7330, 10942, 7466, 7602, 7258\}, \text{Média}=8119.6$$

$$\text{betas6}=\{7902, 6938, 8006, 10382, 7258\}, \text{Média}=8097.2$$

Média dos betas=8125.47 (observe-se que o valor médio de  $\beta_{k,i}$  para seqüências randômicas é igual a  $2N^2=7938$ )

A maior soma dos betas ocorreu para betas3, logo a Pe limitante será calculada através deste grupo e vale  $Pe=8.11*10^{-10}$ .

### **4.2.8 SEQÜÊNCIAS DE BENT**

Serão construídas seqüências de Bent seguindo o processo adotado em SIMON<sup>10</sup>. Esta família possui propriedades de correlação e equivalente linear melhores do que as famílias anteriores.

As seqüências de Bent aqui geradas possuem um grau  $n$  múltiplo de quatro e comprimento  $2^n - 1$ . A seguir é exibido um exemplo, como em SIMON<sup>10</sup>, juntamente com as ferramentas utilizadas nas simulações para a comparação dos resultados. Adotar-se-á inicialmente  $n$  múltiplo de quatro. A função de Bent adotada é a seguinte:

$$F_z(\mathbf{X}) = \mathbf{X}_1 \cdot \mathbf{X}_2 + G(\mathbf{X}_2) + z^t \mathbf{X}.$$

onde  $\mathbf{X}$  é um vetor de  $V_{n/2}$ , com coordenadas de valores pertencentes a  $\{0, 1\}$  e  $\mathbf{X}_1$  e  $\mathbf{X}_2$  correspondem às metades distintas de  $\mathbf{X}$  originando vetores de  $V_{n/4}$ .

O parâmetro  $z$  é um vetor de  $V_{n/2}$  que tem for finalidade selecionar uma função de Bent distinta na família.

A função  $G(\mathbf{X}_2)$  é uma função Booleana arbitrária; com ela pode-se gerar famílias de funções de Bent distintas.

O vetor  $\mathbf{X}$  é calculado através de um mapeamento linear do espaço vetorial  $V_n$  para o espaço vetorial  $V_{n/2}$ ; esse mapeamento linear é realizado com a função Traço.

Assim tem-se:

$$\mathbf{X} = \mathbf{M} \cdot \mathbf{x}$$

onde  $\mathbf{x}$  é um vetor do espaço  $V_n$ , que será obtido do conteúdo de um registrador de deslocamentos na configuração de Galois<sup>5</sup> construído para gerar uma SMC de grau  $n$ .

$\mathbf{M}$  é uma matriz de ordem  $n/2 \times n$  calculada por:

$$m_{i,j} = \text{Tr}_2^{2^n} (\varepsilon_0 \phi_i \alpha^{j-1})$$

$\varepsilon_0$  é um elemento arbitrário de  $\text{GF}(2^n)$  que não esteja em  $\text{GF}(2^{n/2})$ .

$\phi_i$  é um elemento de uma base arbitrária de  $\text{GF}(2^{n/2})$ .

$\alpha$  é um elemento primitivo de  $\text{GF}(2^n)$ .

Finalmente, para a construção da seqüência usa-se a seguinte expressão:

$$\text{Seq}_z = (-1)^{F_z(\mathbf{M} \cdot \mathbf{x}) + \mathbf{s}^t \cdot \mathbf{x}}$$

O índice  $z$  determina a função de Bent que está sendo utilizada para o cálculo da seqüência.

O parâmetro  $\mathbf{s}^t$  é um vetor arbitrário de  $V_n$  que não deve ser igual a nenhuma das linhas de  $\mathbf{M}$ ; este parâmetro é responsável pelo balanceamento da seqüência.

Exemplo:

Seja  $x^{12} + x^6 + x^4 + x + 1$  um polinômio primitivo para  $n=12$ , que será representado por  $\text{pc} = \{1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1\}$ .

$$\varepsilon_0 = \alpha$$

$$\phi_i = \{ \alpha^{65i}, i=0, 1, 2, 3, 4, 5 \}$$

$$m_{i,j} = \text{Tr}_2^{2^{12}} (\alpha^{65(i-1)+(j-1)+1})$$

Obs.: o índice aparece subtraído de um pois o mesmo variará de 1 até 6.

$$\mathbf{M} = \text{Table}[\text{Traco}[x^{65(i-1)+j}, x^{12} + x^6 + x^4 + x + 1], \{i, 1, 6\}, \{j, 1, 12\}]$$

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

O vetor  $s^t$  não pode coincidir com nenhuma linha desta matriz, bem como não deve ser nulo.

Adotar-se-á  $s^t = \{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1\}$ .

Para a função  $G(\mathbf{X}_2)$  adotar-se-á, arbitrariamente, a função lógica E entre seus bits.

$$G(\mathbf{X}_2) = \mathbf{X}_2[1] \cdot \mathbf{X}_2[2] \cdot \mathbf{X}_2[3].$$

e z variará de 0 à  $2^{n/2}$ .

Bent = Table[ **bent01**[ pc, d], {d, 0, 63}];

Com esta última expressão constrói-se uma família de Bent com 64 seqüências, cuja correlação cruzada periódica fora de fase tem por valor máximo  $2^{n/2} + 1 = 65$  que equivale a aproximadamente 16% do comprimento da seqüência  $N = 4095$ . Em SIMON<sup>10</sup> tem-se uma implementação física deste exemplo. Para se construir outra família pode-se mudar a função  $G(\mathbf{X}_2)$  para qualquer outra função Booleana.

O equivalente linear para esta família é estimada pela expressão (3.85) e fornece, neste exemplo,  $L \geq 202$ . Calculando-se o equivalente linear para algumas seqüências da família acima obteve-se:

$$L = \text{EquivalenteLinear}[\text{seq0}] = 232$$

Os resultados desta item aparecem na tabela comparativa apresentada em 4.3.4

### 4.3 CRITÉRIO PARA A SELEÇÃO DE SEQUÊNCIAS EM SISTEMAS ASSÍNCRONOS

#### 4.3.1 INTRODUÇÃO

O critério a seguir exibido tem por objetivo selecionar um grupo de seqüências, dentro de uma família de forma que a interferência de múltiplo acesso seja minimizada.

O número de seqüências a ser selecionado deve ser determinado em função de parâmetros do sistema no qual serão utilizados. O parâmetro que será utilizado para a determinação da quantidade de seqüências será a probabilidade de erro de bit.

#### 4.3.2 DETERMINAÇÃO DE UMA QUANTIDADE DE SEQUÊNCIAS A SER PROCURADA

As considerações a seguir aplicam-se para sistemas DS-SS assíncronos e servem como uma primeira aproximação para a determinação da ordem de grandeza dos parâmetros envolvidos.

Com a expressão a seguir, que é uma aproximação gaussiana, determina-se uma a probabilidade de erro em função de uma relação sinal ruído estipulada.

$$P_e = Q(\text{SNR}) = \frac{1}{\sqrt{2\pi}} \cdot \int_{\text{SNR}}^{\infty} e^{-y^2/2} dy$$

Por exemplo, para uma probabilidade de  $1,0 \cdot 10^{-6}$  deve-se ter no mínimo  $\text{SNR}_{\text{mínima}} = 4,8$ .

Com este último dado, pode-se através da aproximação indicada a seguir, estipular um número de usuários em função do comprimento das seqüências a serem utilizadas.

Da expressão (2.81) tem-se:

$$\text{SNR} \approx \frac{1}{\sqrt{\frac{K-1}{3N} - \frac{N_0}{2E_b}}} \approx \frac{1}{\sqrt{\frac{K-1}{3N}}}$$

desprezando-se, na última aproximação, os ruídos que não são de multiacesso.

Desta última vem:

$$K \approx \frac{3N}{(\text{SNR})^2} + 1 \quad \text{ou} \quad N \approx \frac{(K-1)(\text{SNR})^2}{3}$$

Se  $N=2^n-1$  (como no caso das SMC's)

$$n \approx \log_2 \left( \frac{(K-1)(\text{SNR})^2}{3} + 1 \right)$$

Para seqüências de comprimento 63 (grau 6), o número de usuários seria limitado à 9, para a probabilidade de erro especificada.

Assim deve-se determinar 9 seqüências dentro da família especificada que atendam a esta restrição (observe-se que neste caso particular não poderiam ser SMC's, pois para este grau existem apenas 6 SMC's ).

Estas expressões visam apenas dar uma estimativa inicial para a quantidade a ser selecionada, pois aqui não se está considerando um sistema específico. Num sistema específico, onde o número máximo de usuários é pré-determinado e a  $P_e$  é especificada, deve-se estimar inicialmente o comprimento da seqüência necessária a partir das equações anteriores.

### 4.3.3 SIMULATED ANNEALING<sup>16</sup>

#### 4.3.3.1 INTRODUÇÃO

Neste item é exposto um critério para a seleção de seqüências dentro de uma família, de forma que seja minimizada a interferência de múltiplo acesso para o caso em que o tempo de bit é um múltiplo do tempo de chip.

O critério a seguir é formulado de maneira empírica, pois o número de combinações de seqüências atinge um número cuja a ordem de grandeza é extremamente elevada e inviabilizando a busca ótima. Por exemplo, considerando-se uma família de Gold de grau 6, que possui 65 seqüências, para selecionar-se 10 destas, teria-se que testar 127.805.525.001 combinações até que fosse encontrada a melhor. Infelizmente este número torna o processo da otimização proibitivo, sendo assim necessário criarem-se métodos de subotimização na busca de um grupo de seqüências onde sejam encontrados valores aceitáveis.

O método de "Simulated Annealing" é uma técnica genérica para a minimização do número de combinações na otimização de sistemas, onde a quantidade de iterações necessárias para a determinação do ponto ótimo atinge valores proibitivos. O ponto ótimo não é encontrado, a não ser por acaso. No entanto são evitados os casos inaceitáveis ou pouco aceitáveis. A seguir é colocada uma descrição do método adaptada à busca de seqüências.

#### 4.3.3.2 DESCRIÇÃO

Seja dado um grupo qualquer de seqüências, denominado de família, com um número M de seqüências.

$$\text{família} = \{ \text{seq1}, \text{seq2}, \dots, \text{seqM} \}$$

### **Inicialização**

Esta etapa consiste na determinação de valores para alguns parâmetros que controlam o fluxo do algoritmo.

a) Selecionam-se aleatoriamente  $K$  das  $M$  seqüências da família, formando-se uma subfamília.

$$\text{subfamília} = \{\text{seqi1}, \text{seqi2}, \text{seqi3}, \dots, \text{seqiK}\}$$

b) Calculam-se os betas (interferência de múltiplo acesso) para este subconjunto de  $K$  seqüências, para todas as combinações possíveis, construindo-se uma matriz quadrada de ordem  $K-1$  (denominada de matriz dos betas), onde a primeira linha refere-se a primeira seqüência da subfamília, e assim sucessivamente (não são considerados os casos da interferência de uma seqüência sobre ela própria, evidentemente). Procede-se em seguida a soma dos elementos de cada linha, obtendo-se uma matriz coluna (denominada de matriz de soma dos betas), onde cada elemento de uma linha equivale a soma dos elementos da linha correspondente da matriz dos betas e representa então a interferência sobre aquele usuário devida aos  $(K-1)$  restantes.

Após este passo inicializa-se o parâmetro  $\text{MaxBeta}$  com o maior valor da matriz de soma dos betas. Este parâmetro será utilizado para tomada decisão por ocasião da substituição por uma nova seqüência. Armazena-se também o valor referente ao índice da seqüência onde ocorreu o maior valor para a soma dos betas no parâmetro  $\text{MaxIndice}$ .

c) Da matriz dos betas determina-se o menor e o maior valor e calcula-se a diferença entre os mesmos. Com o módulo desta diferença multiplicado por uma constante, inicializa-se o parâmetro  $T$  que será responsável pela probabilidade de efetuar-se uma substituição por uma nova seqüência. A constante de multiplicação deve

ser tal que o parâmetro  $T$  torne-se muito maior que a diferença entre os betas máximo e mínimo encontrados.

d) Determina-se um valor inicial para os demais parâmetros:  $\text{NumSubstituicoes\_0} = \text{NumSubstituicoes} = 10M$ ; manter-se-á este valor igual a 10% do número de iterações quando o mesmo for omitido. Este parâmetro será responsável pela redução do fator  $T$ , isto é, quando ocorrer um número de substituições igual a  $\text{NumSubstituicoes}$  diminui-se  $T$ , por exemplo, de 10%, assim  $T \rightarrow 0,9T$ .

e) Para finalizar o processo de otimização podem-se adotar vários critérios como, por exemplo, número de iterações, tempo de processamento etc. Adotou-se aqui o número de iterações, e assim inicializou-se o parâmetro  $\text{NumItera}$ , com um número da ordem de, aproximadamente, de 100M; assim após efetuarem-se 100M buscas finaliza-se o processo.

### **Processo (Ciclo de Otimização)**

f) Seleciona-se aleatoriamente uma seqüência  $j$  do conjunto formado pelas seqüências que não foram inicialmente selecionadas, isto é,  $\text{seq}_j \in \text{família}$  e  $\notin \text{subfamília}$ .

g) Guarda-se a subfamília numa matriz temporária; em seguida substitui-se a seqüência referente ao  $\text{MaxIndice}$  obtido no item b) pela  $\text{seq}_j$ .

h) Repetem-se os cálculos efetuados no item b) e compara-se o novo  $\text{MaxBeta}$  com o anterior e tomam-se uma das seguintes decisões:

- se o novo  $\text{MaxBeta}$  for menor que  $\text{MaxBeta}$  anterior mantém-se a substituição já efetuada bem como o valor para o  $\text{MaxBeta}$ .

- caso contrário gera-se um número aleatório, entre zero e um, denominado de  $\text{NumAle}$ . Se  $\text{NumAle}$  for menor que  $e^{-(\text{MaxBeta})/T}$ , mantém-se a substituição já

efetuada, bem como o valor para MaxBeta; por outro lado se isso não ocorrer desfaz-se a substituição e guarda-se no parâmetro MaxBeta, o valor anteriormente calculado.

i) Decrementa-se de um o parâmetro NumSubstituicoes; se com isso NumSubstituicoes=0 então faz-se  $T \rightarrow 0.9T$  e NumSubstituicoes=NumSubstituicoes\_0 (10M).

j) Decrementa-se de um o parâmetro NumItera; se NumItera=0 finaliza-se o algoritmo, caso contrário inicia-se o processo a partir do item f).

#### 4.3.3.3 CONSIDERAÇÕES

Observe-se que o número de iterações desta rotina NumItera deve ser suficientemente superior ao NumSubstituicoes para proporcionar uma redução significativa no parâmetro T. Este algoritmo supõe que o número de iterações que serão realizadas possui uma elevada ordem de grandeza quando comparado ao número de seqüências da família. Quando o número de iterações a ser realizado não for proporcionalmente elevado (isto incluiria, por exemplo, os casos onde o comprimento da seqüência é muito grande e o tempo para a realização dos cálculos é proibitivo) deve-se reduzir a ordem de grandeza do parâmetro T para, por exemplo, um valor igual à diferença entre os betas máximo e mínimo ou menor ainda.

Neste caso o número de substituições deve ser, por exemplo, 1/20 ou 1/10 do número de iterações.

Portanto, antes de atribuir-se valores ao parâmetro T e ao número de substituições, deve-se ter uma perspectiva do número de iterações, do tempo necessário para realizar cada iteração e analisar-se os valores da expressão  $e^{-X/T}$  que fornecerá a relação entre X e T mais adequada para cada caso.

Os valores das seqüências onde ocorreu o menor MaxBeta e onde ocorreu a maior MaxBeta devem ser armazenados para verificar-se o ganho.

A seguir é exposta a tela principal do programa, que foi realizado para a seleção de seqüências por este critério.

Seja então um exemplo numérico com 9 seqüências de uma família de Gold de grau 6 (65 seqüências no total). A família foi gerada utilizando-se a função **Gold** e os polinômios  $\{1, 0, 0, 0, 0, 1\}$  e  $\{1, 0, 1, 1, 0, 1\}$ , numa ordenação conforme expressão (3.51). As seqüências inicialmente selecionadas foram: 3, 5, 7, 9, 10, 20, 30, 40 e 50. Na tabela adiante:

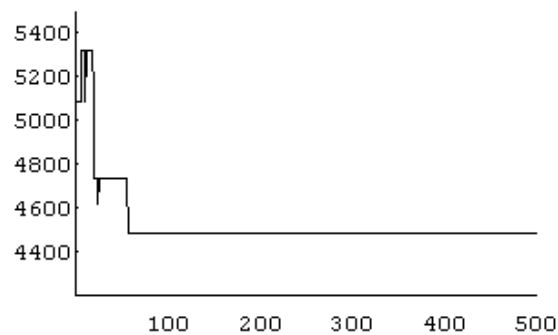
- cada linha corresponde a um conjunto de 9 seqüências testadas;
- BetaMin corresponde ao menor valor de Beta da matriz total;
- BetaMax corresponde ao maior valor de Beta da matriz total (não necessariamente na mesma linha do BetaMin);
- SomaMaxBeta corresponde à linha desta matriz em que a soma é maximizada (corresponde ao pior caso da utilização daquelas 9 seqüências);

- T é um parâmetro variável que decai, neste exemplo, de 10% de seu valor anterior (fixado inicialmente em 3000 neste caso) a cada 20% do número total de iterações (500 neste caso).

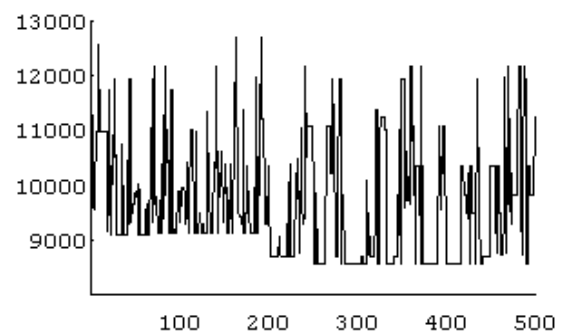
NumItera	BetaMin	BetaMax	SomaMaxBeta	T
0	5078	11266	74696	3000
10	5318	10986	62284	3000
20	4730	9838	60320	3000
30	4730	9086	57584	3000
40	4730	10466	57592	3000
50	4730	9778	56296	3000
60	4486	9498	60536	3000
70	4486	12178	62032	3000
80	4486	9666	59888	3000
90	4486	11726	60736	3000
100	4486	9930	60280	2700
110	4486	11014	57504	2700
120	4486	9122	58512	2700
130	4486	11334	61056	2700
140	4486	12178	60504	2700
150	4486	9962	58864	2700
160	4486	11098	61664	2700
170	4486	11362	59544	2700
180	4486	9122	58764	2700
190	4486	12678	62932	2700
200	4486	8698	53704	2430
210	4486	9070	58624	2430
220	4486	8698	58568	2430
230	4486	10010	63968	2430
240	4486	12174	58248	2430
250	4486	8578	55368	2430
260	4486	8578	56272	2430
270	4486	11918	58576	2430
280	4486	10914	61080	2430
290	4486	8578	54760	2430
300	4486	8578	54760	2187
310	4486	8726	59968	2187
320	4486	11362	60984	2187
330	4486	11014	60080	2187
340	4486	8718	55424	2187
350	4486	11918	58576	2187
360	4486	11726	58992	2187
370	4486	12174	58248	2187
380	4486	8578	54760	2187
390	4486	10382	59968	2187
400	4486	8578	55368	1968
410	4486	8578	55368	1968
420	4486	9838	54832	1968
430	4486	9486	59040	1968
440	4486	8718	55424	1968
450	4486	10338	56392	1968
460	4486	8738	57912	1968
470	4486	11222	59144	1968
480	4486	12174	58248	1968
490	4486	10338	56392	1968
500	4486	11222	59144	1771

- Ponto Ótimo (menor SomaMaxBeta): iteração 200;
- Sequências seleccionadas neste passo: 8, 27, 31, 34, 44, 46, 53, 57 e 62;
- Observe-se que esta iteração não corresponde ao mínimo dos BetaMax.

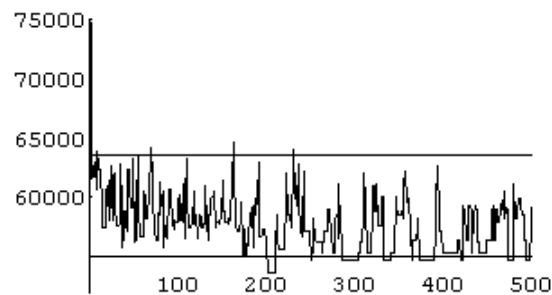
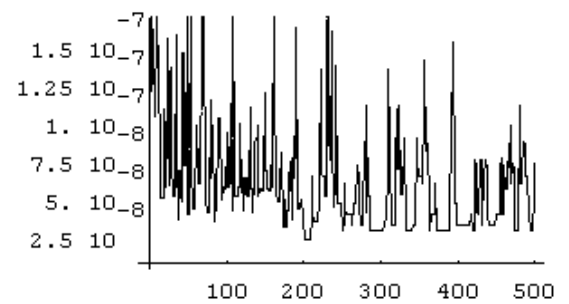
Variação do beta mínimo



Variação do beta máximo



SomaMaxBeta

Probabilidade de erro de bit  
(coluna SomaMaxBeta)

- Valor Médio =  $2N^2 = 63504 \rightarrow Pe = 5.8 \cdot 10^{-7}$  (para seqüências aleatórias)

Considerando-se seqüências escolhidas ao acaso e uma aproximação por seqüências aleatórias o desempenho médio é o acima calculado.

- Máximo da SomaMaxBeta = 74696  $\rightarrow Pe = 3.7 \cdot 10^{-6}$  (iteração 0)

Não se otimizando a escolha de seqüências o resultado para a probabilidade de

erro de bit poderia ser, no pior caso, o valor calculado.

- Mínimo da SomaMaxBeta=53704  $\rightarrow$   $Pe=6.3 \cdot 10^{-8}$  (iteração 200)

Com a escolha das seqüências por este método pode-se garantir que o pior desempenho será sempre melhor que o valor acima.

#### 4.3.4 TABELA COMPARATIVA DE SEQÜÊNCIAS

Seguindo a linha exposta em KÄRKKÄINEN<sup>17</sup> constrói-se a tabela a seguir selecionando-se seqüências aleatórias dentro das respectivas famílias. Com relação a tabela exibida na referência, foram acrescentados resultados obtidos com famílias não lineares, bem como ampliou-se a mesma, adicionando-se duas colunas para exibir o equivalente linear e o número de seqüências na família (nesta tabela  $\theta_c$  corresponde ao pico da correlação cruzada periódica, em módulo, e F denota o número de seqüências da família).

Verifica-se assim que a geração não linear das seqüências não trouxe, dentro dos exemplos apresentados, nenhuma deterioração em relação ao desempenho já conhecido com as famílias geradas de forma linear. Nos exemplos apresentados, verifica-se ainda que o desempenho das seqüências GMW é melhor do que o valor médio esperado com seqüências randômicas, enquanto nas de Bent é pior. Estas diferenças são, no entanto, muito pequenas e observadas num universo não representativo da família, de forma que é prematuro, senão errôneo, estender esta observação. Outro fato que aparece destes resultados é que sendo  $E\{\beta_{i,x}\} = 2N^2$  pode-se, em princípio, pesquisar dentre todas as seqüências de uma dada família aquelas para as quais este parâmetro seja o menor possível. O número de pesquisas a efetuar no entanto é proibitivo: a determinação de U seqüências de código ótimas, a partir de uma família de M seqüências de comprimento N, corresponde a determinar  $P_{ei}$  mínima,  $N^U \binom{M}{U}$  vezes (para N=511, M=513 e U=50, por exemplo, o número de alternativas possíveis é de  $\cong 10^{205}$ !).

Observa-se no entanto que este cálculo pode ser aproximado para a determinação de  $\mu_{i,x}(0)$  apenas, já que a influência de  $\mu_{i,x}(1)$  pode ser desprezada numa primeira avaliação.

[illegible]

#### 4.3.5 CONCLUSÕES

A escolha de seqüências de código para espalhamento espectral é ainda um campo aberto onde devem ser realizados estudos mais aprofundados para a determinação de critérios de escolha mais precisos.

Dentre as famílias lineares destaca-se a de Kasami Pequeno, não pela quantidade de seqüências, mas pelos seus valores de correlação periódica. Comparando-a com o limite de WELCH são de início as mais recomendáveis; inconvenientes, no entanto, se houver a necessidade de um grande número de usuários. Neste caso deve-se optar por outras famílias.

Dentre as famílias não lineares, destacam-se as seqüências de Bent tanto sob o aspecto de correlação periódica quanto de equivalente linear.

As SMC's são as seqüências que individualmente, apresentam as melhores características, pois sob o aspecto de correlação periódica, balanceamento e distribuição dos seus bits são quase ideais. Apresentam, no entanto, inconvenientes no que diz respeito ao número de seqüências da família (em comparação com outras famílias) e, principalmente, no seu equivalente linear. Esta última observação não recomenda seu uso em sistemas onde o "sigilo" é importante, por exemplo.

Uma última observação, muito importante, diz respeito à aplicabilidade dos resultados obtidos. A sua aplicação limita-se ao caso de seqüências de códigos tais que  $T = NT_c$ , onde  $T$  é a duração de um bit de dados,  $T_c$  é a duração de um chip da seqüência e  $N$  o comprimento da mesma. Em situações diferentes desta os resultados gerais devem ser adaptados. Por exemplo, considerando-se correlações cruzadas aperiódicas de segmentos das seqüências utilizadas ao invés de correlações cruzadas aperiódicas como definidas em (2.69).

## **ANEXO:**

### **PROGRAMAS DESENVOLVIDOS NO MATHEMATICA**

#### **A1- FUNÇÕES DO PROGRAMA MATHEMATICA MAIS UTILIZADAS**

Table- gera uma lista.

Length- retorna o número de elementos de uma lista.

ListPlot- constrói um gráfico com os elementos de uma lista.

Sum- retorna a soma dos elementos de uma lista.

Module- constrói blocos independentes de programa.

Mod- retorna o módulo de um número em relação a uma base dada.

PolynomialPowerMod- retorna o módulo de um polinômio em função de outro.

#### **A2- GERAÇÃO DE SEQUÊNCIAS LINEARES**

##### **SMC**

```

Smc[CoefdoPoli_] := Module[{ grau, CondIni, CRD, SmcdeSaida, Bit },
  (*CoefdoPoli=coeficientes do polinômio primitivo, menos o último*)
  grau = Length[CoefdoPoli];
  CondIni = Table[0, { grau }];
  CondIni = ReplacePart[CondIni, 1, -1];
  CRD = CondIni;
  SmcdeSaida = Table[0, { 2^grau-1 }];
  Do[
    Bit = Mod[CoefdoPoli.CRD, 2];
    SmcdeSaida[[i]] = Bit;
    CRD = ReplacePart[ RotateLeft[CRD, 1], Bit, -1 ],
    { i, 1, 2^grau-1 }
  ];
  SmcdeSaida
];

```

Descrição funcional

a) Sintaxe

Smc[ { 1, 0, ..., 1 } ]

b) Parâmetro

CoefdoPoli\_: é uma matriz linha entre chaves que contém os coeficientes do polinômio primitivo gerador da sequência, de tal forma que se inicie da potência mais alta até a mais baixa, excluindo-se a potência zero. Estes coeficientes devem ser 0 ou 1.

Exemplo: Seja o seguinte polinômio primitivo ,  $x^6 + x + 1$ .

CoefdoPoli\_={ 1, 0, 0, 0, 0, 1 }

Como o polinômio é do grau 6 a matriz deve conter seis elementos, sendo que o primeiro da esquerda para a direita é o coeficiente de maior grau, que efetivamente será sempre 1, e o último elemento representa o coeficiente de x.

Obs.: A função não faz nenhuma espécie de verificação, logo se o parâmetro não for correto obter-se-ão resultados errados.

### c) Resultado

Como resultado obter-se-á a seqüência de máximo comprimento na forma de uma matriz linha, que no exemplo acima é:

{1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1}

## GOLD

⚡ Gold[poli1\_, poli2\_] := Module[{ grau, tamanho, smc1, smc2, familia, seq },

grau = Length[poli1];

tamanho = 2^grau - 1;

(\* A função Smc[ ] precisa estar carregada \*)

smc1 = Smc[poli1];

smc2 = Smc[poli2];

familia = Table[0, {tamanho + 2}];

familia[[1]] = smc1;

familia[[2]] = smc2;

Do[

seq = Mod[smc1 + RotateLeft[smc2, i], 2];

familia[[3 + i]] = seq,

{i, 0, tamanho - 1}

];

familia

];

Obs.: Para que esta função opere, há a necessidade de carregar-se a função geradora de Smc.

### Descrição funcional

#### a) Sintaxe

Gold[ { 1, 0, ..., 1 }, { 1, 0, ..., 1 } ]

#### b) Parâmetro

poli1\_, poli2\_: são matrizes linha entre chaves que contém os coeficientes dos polinômios primitivos, sendo que estes polinômios devem formar um par preferencial, para que venham a gerar uma das famílias de seqüências de Gold.

Exemplo:

Sejam os seguintes polinômios primitivos  $x^6 + x + 1$  e  $x^6 + x^5 + x^2 + x + 1$

$\text{poli1\_} = \{ 1, 0, 0, 0, 0, 1 \}$ ,  $\text{poli2\_} = \{ 1, 1, 0, 0, 1, 1 \}$

Como os polinômios são de grau 6, cada parâmetro deve ser uma matriz com seis elementos, sendo que o primeiro da esquerda para a direita é o coeficiente de maior grau, que efetivamente será sempre 1, e o último elemento representa o coeficiente de  $x$ .

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

#### c) Resultado

Como resultado obter-se-á a uma família de seqüências na forma de uma matriz linha, onde cada elemento desta matriz é uma outra matriz que contém uma seqüência, que no exemplo acima é:

```
Gold[{ 1, 0, 0, 0, 0, 1 }, { 1, 1, 0, 0, 1, 1 }] =
{
{ 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1,
1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1 },
{ 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1,
0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1 },
{ 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0,
1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 },
{ 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1,
1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0 }, ...,
{ 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1 }
}
```

onde as duas primeiras seqüências são as SMC's geradoras.

#### GOLDLIKE

```
⚡ GoldLike[poli1_] := Module[{ grau, tamanho, smcpoli1, q, seq01, seq02, seq03, familia, seq },
    grau = Length[poli1];
    tamanho = 2^grau - 1;
    (* A função Smc[ ] e Decimação devem estar carregadas *)
    smcpoli1 = Smc[poli1];
    (* Gerando as demais seqüências através de decimação *)
    q = 2^((grau+2)/2)+1;
    seq01 = Decimacao[smcpoli1, q];
    seq02 = Decimacao[RotateLeft[smcpoli1, 1], q];
    seq03 = Decimacao[RotateLeft[smcpoli1, 2], q];
    familia = Table[0, { tamanho+1 }];
```

```

familia[[1]]=smcpoli1;
Do[
    seq=Mod[smcpoli1 + RotateLeft[seq01,i],2];
    familia[[2+i]]=seq,
    {i,0,tamanho/3-1}
];
Do[
    seq=Mod[smcpoli1 + RotateLeft[seq02,i],2];
    familia[[tamanho/3+2+i]]=seq,
    {i,0,tamanho/3-1}
];
Do[
    seq=Mod[smcpoli1 + RotateLeft[seq03,i],2];
    familia[[2*tamanho/3+2+i]]=seq,
    {i,0,tamanho/3-1}
];
familia
];

```

#### Descrição funcional

##### a) Sintaxe

GoldLike[ { 1,0,...,1 } ]

##### b) Parâmetro

poli1\_: é uma matriz linha entre chaves que contém os coeficientes do polinômio primitivo, onde o grau do mesmo deve ser múltiplo de quatro

Exemplo: Seja o seguinte polinômio primitivos  $x^4 + x^3 + x + 1$  e

poli1\_={ 1, 1, 0, 1}.

Como o polinômio é de grau 4 o parâmetro deve ser uma matriz com quatro elementos, sendo que o primeiro da esquerda para a direita é o coeficiente de maior grau, que efetivamente será sempre 1, e o último elemento representa o coeficiente de x.

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

##### c) Resultado

Como resultado obter-se-á a uma família de seqüências na forma de uma matriz linha, onde cada elemento desta matriz é uma outra matriz que contém uma seqüência, que no exemplo acima é:

GoldLike[{1,1,0,1}]=

{{0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1}, {1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1},

```
{1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0}, {0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0},
{0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1}, {0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1},
{1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1}, {0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0},
{0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1}, {1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1},
{0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0}, {0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0},
{1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1}, {1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0},
{1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0}, {1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0}}
```

### **GOLD BCH DUAL**

⚡ GoldBCHdual[poli1\_]:=

```
Module[{grau,tamanho,smcpoli1,q,seq01,seq02,seq03,familia,seq},
grau=Length[poli1];
tamanho=2^grau-1;
(* A função Smc[ ] e Decimação devem estar carregadas *)
smcpoli1=Smc[poli1];
(* Gerando as demais seqüências através de decimação *)
q=3;
seq01=Decimacao[smcpoli1,q];
seq02=Decimacao[RotateLeft[smcpoli1,1],q];
seq03=Decimacao[RotateLeft[smcpoli1,2],q];
familia=Table[0,{tamanho+1}];
familia[[1]]=smcpoli1;
Do[
seq=Mod[smcpoli1 + RotateLeft[seq01,i],2];
familia[[2+i]]=seq,
{i,0,tamanho/3-1}
];
Do[
seq=Mod[smcpoli1 + RotateLeft[seq02,i],2];
familia[[tamanho/3+2+i]]=seq,
{i,0,tamanho/3-1}
];
Do[
seq=Mod[smcpoli1 + RotateLeft[seq03,i],2];
familia[[2*tamanho/3+2+i]]=seq,
{i,0,tamanho/3-1}
];
```

```
];
familia
];
```

#### b) Parâmetro

poli1\_: é uma matriz linha entre chaves que contém os coeficientes do polinômio primitivo, onde o grau n do mesmo deve obedecer a seguinte restrição:

$$\text{mdc}(2^n-1,3)=3$$

Exemplo: Seja o seguinte polinômio primitivos  $x^4 + x^3 + x + 1$  e

poli1\_={ 1, 1, 0, 1}.

Como o polinômio é de grau 4 o parâmetro deve ser uma matriz com quatro elementos, sendo que o primeiro da esquerda para a direita é o coeficiente de maior grau, que efetivamente será sempre 1, e o último elemento representa o coeficiente de x.

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

#### c) Resultado

Como resultado obter-se-á uma família de seqüências na forma de uma matriz linha, onde cada elemento desta matriz é uma outra matriz que contém uma seqüência, que no exemplo acima é:

```
GoldBCHdual[{1,1,0,1}]=
{{1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0}, {1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1},
{0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0}, {1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1},
{0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0}, {0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1},
{1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1}, {0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0},
{1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1}, {0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0},
{0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1}, {0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0},
{1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1}, {0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0},
{1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1}, {1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0}}
```

#### KASAMI PEQUENO

```
⌘KasamiPequeno[poli1_]:=Module[{grau,tamanho,smcpoli1,q,seq01,familia,seq},
grau=Length[poli1];
tamanho=2^grau-1;
(* A função Smc[ ] e Decimação devem estar carregadas *)
smcpoli1=Smc[poli1];
(* Gerando as demais seqüências através de decimação *)
q=2^(grau/2)+1;
seq01=Decimacao[smcpoli1,q];
familia=Table[0,{q-1}];
```

```

familia[[1]]=smcpoli1;
Do[
    seq=Mod[smcpoli1 + RotateLeft[seq01,i],2];
    familia[[2+i]]=seq,
    {i,0,q-3}
];
familia
];

```

#### Descrição funcional

##### a) Sintaxe

KasamiPequeno[ { 1,0,...,1 }]

##### b) Parâmetro

poli1\_: é uma matriz linha entre chaves que contém os coeficientes do polinômio primitivo, onde o grau n do mesmo deve ser um número par.

Exemplo: Seja o seguinte polinômio primitivos  $x^4 + x^3 + x + 1$  e

poli1\_={ 1, 1, 0, 1 }.

Como o polinômio é de grau 4 o parâmetro deve ser uma matriz com quatro elementos, sendo que o primeiro da esquerda para a direita é o coeficiente de maior grau, que efetivamente será sempre 1, e o último elemento representa o coeficiente de x.

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

##### c) Resultado

Como resultado obter-se-á uma família de seqüências na forma de uma matriz linha, onde cada elemento desta matriz é uma outra matriz que contém uma seqüência, que no exemplo acima é:

```

KasamiPequeno[{1,1,0,1}]=
{{1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0}, {0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1},
{1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1}, {0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0}}

```

#### KASAMI GRANDE

```

KasamiGrande[poli1_] := Module[{grau,tamanho,tamanhodafamilia,smcpoli1,q,
    seq01,seq02,seq03,seq04,familia,seq,i,j},
    grau=Length[poli1];
    tamanho=2^grau-1;
    (* A função Smc[ ] e Decimação devem estar carregadas *)
    smcpoli1=Smc[poli1];
    (* Gerando as demais seqüências através de decimação *)
    q1=2^((grau+2)/2)+1;

```

```

q2=2^(grau/2)+1;
(* If [condição, Verdadeiro, Falso]*)
(* A parte verdadeira corresponde a Gold e a falsa a Gold Like *)
If[Mod[grau,4]==2,
  seq01=Decimacao[smcpoli1,q1];
  seq02=Decimacao[smcpoli1,q2];
  tamanhodafamilia=(2^grau+1)(2^(grau/2));
  familia=Table[0,{tamanhodafamilia}];
  familia[[1]]=smcpoli1;
  familia[[2]]=seq01;
  (* Gerando a família de Gold *)
  Do[
    seq=Mod[smcpoli1 + RotateLeft[seq01,i],2];
    familia[[3+i]]=seq,
    {i,0,tamanho-1}
  ];
  (* Família de Gold Gerada *)
  (* Fazendo a combinação das seqüências da família de Gold *)
  (* com a outra seqüência para todos os deslocamentos possíveis *)
  Do[
    Do[
      seq=Mod[familia[[j]] + RotateLeft[seq02,i],2];
      familia[[tamanho+2 + (j-1)*(q2-2)+1 + i]]=seq,
      {i,0,q2-3}
    ],
    {j,1,tamanho+2}
  ],
  (* Gold Like *)
  tamanhodafamilia=((2^grau+1)*(2^(grau/2)))-1;
  familia=Table[0,{tamanhodafamilia}];
  familia[[1]]=smcpoli1;
  seq01=Decimacao[smcpoli1,q1];
  seq02=Decimacao[RotateLeft[smcpoli1,1],q1];
  seq03=Decimacao[RotateLeft[smcpoli1,2],q1];
  Do[

```

```

seq=Mod[smcpoli1 + RotateLeft[seq01,i],2];
familia[[2+i]]=seq,
{i,0,tamanho/3-1}
];
Do[
seq=Mod[smcpoli1 + RotateLeft[seq02,i],2];
familia[[tamanho/3+2+i]]=seq,
{i,0,tamanho/3-1}
];
Do[
seq=Mod[smcpoli1 + RotateLeft[seq03,i],2];
familia[[2*tamanho/3+2+i]]=seq,
{i,0,tamanho/3-1}
];
(* Combinando Gold Like com todas as combinações possíveis *)
seq04=Decimacao[smcpoli1,q2];
Do[
Do[
seq=Mod[familia[[j]] + RotateLeft[seq04,i],2];
familia[((tamanho+1) + ((j-1)*(q2-2))+1 + i)]=seq,
{i,0,q2-3}
],
{j,1,tamanho+1}
];
(* Combinando as seqüências geradas em Gold Like *)
(* com a decimação de Kasami pequeno *)
Do[
seq=Mod[ seq01 + RotateLeft[seq04,i],2];
familia[((tamanho+1)*(q2-1))+1+i]=seq,
{i,0,(q2-2)/3-1}
];
Do[
seq=Mod[ seq02 + RotateLeft[seq04,i],2];
familia[((tamanho+1)*(q2-1))+((q2-2)/3)+1+i]=seq,
{i,0,(q2-2)/3-1}
];

```

```

];
Do[
    seq=Mod[ seq03 + RotateLeft[seq04,i],2];
    familia[(((tamanho+1)*(q2-1))+(2*((q2-2)/3))+1+i)]=seq,
    {i,0,(q2-2)/3-1}
];
];
(* Família Gerada *)
familia
];

```

Descrição funcional

a) Sintaxe

KasamiGrande[{ 1,0,...,1}]

b) Parâmetro

poli1\_: é uma matriz linha entre chaves que contém os coeficientes do polinômio primitivo, onde o grau n do mesmo deve ser um número par.

Exemplo: Seja o seguinte polinômio primitivos  $x^4 + x^3 + x + 1$  e

poli1\_={ 1, 1, 0, 1 }.

Como o polinômio é de grau 4 o parâmetro deve ser uma matriz com quatro elementos, sendo que o primeiro da esquerda para a direita é o coeficiente de maior grau, que efetivamente será sempre 1, e o último elemento representa o coeficiente de x.

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

c) Resultado

Como resultado obter-se-á uma família de seqüências na forma de uma matriz linha, onde cada elemento desta matriz é uma outra matriz que contém uma seqüência, que no exemplo acima é:

```

KasamiGrande[{1,1,0,1}]=
{{1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0}, {1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1},
{1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0}, {0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0},
{0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1}, {0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1},
{1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1}, {1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0},
{0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0}, {0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1},
{0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1}, {0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0},
{0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1}, {1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1},
{1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0}, {1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0},
{0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1}, {1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1},

```

{0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0}, {0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0},  
 {1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0}, {0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1},  
 {0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1}, {1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1},  
 {0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0}, {1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1},  
 {0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1}, {1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0},  
 {1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0}, {0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0},  
 {1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1}, {1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0},  
 {0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0}, {1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1},  
 {0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0}, {1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0},  
 {0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1}, {0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1},  
 {1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1}, {0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0},  
 {1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1}, {0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1},  
 {1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0}, {1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1},  
 {0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0}, {1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1},  
 {1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0}, {0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0},  
 {1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1}, {1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1},  
 {0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1}, {1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0},  
 {1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0}, {0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0},  
 {1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1}, {0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0},  
 {1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0}, {0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1},  
 {0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1}, {1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1},  
 {0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0}, {0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1},  
 {1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1}, {0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0},  
 {1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0}, {1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0},  
 {0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1}

### HADAMARD

$$H(k+1) = \begin{pmatrix} H(k) & H(k) \\ H(k) & -H(k) \end{pmatrix} \quad \text{com} \quad H(1) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

```

Hadamard[k_:1]:=Module[{anterior={{1,1},{1,-1}},posterior={{1,1},{1,-1}}},
  Do[
    posterior[[1,1]]=anterior;
    posterior[[1,2]]=anterior;
    posterior[[2,1]]=anterior;
    posterior[[2,2]]=-anterior;
    anterior[[1,1]]=posterior[[1,1]];
  ]

```

```

anterior[[1,2]]=posterior[[1,2]];
anterior[[2,1]]=posterior[[2,1]];
anterior[[2,2]]=posterior[[2,2]],
{i,1,k-1}];
PaddedForm[MatrixForm[posterior],2]
]

```

Descrição funcional

a) Sintaxe

Hadamard[ k ]

onde k é um inteiro positivo maior ou igual a 1.

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

c) Resultado

Obtém-se uma visualização da matriz Hadamard.

### **A3- GERAÇÃO DE SEQUÊNCIAS NÃO LINEARES**

#### **GMW**

```

↳ GMW[poly_, J_, r_:1]:
= Module[{i,k,grau,expoente,tamanhodaseq,seqgmw,parteinterna},
grau=Exponent[poly,x];
tamanhodaseq=2^grau-1;
seqgmw=Table[1,{tamanhodaseq}];
Do[
    parteinterna=PolynomialMod[Sum[PolynomialPowerMod[
        PolynomialPowerMod[x,i,{poly,2}]],(2^J)^k,{poly,2}],
        {k,0,(grau/J)-1}],2];
    seqgmw[[i]]=PolynomialMod[Sum[PolynomialPowerMod[
        PolynomialPowerMod[parteinterna,r,{poly,2}],
        2^k,{poly,2}],{k,0,J-1}],2],
    {i,1,tamanhodaseq}];
seqgmw
]

```

Descrição funcional

a) Sintaxe

GMW [  $x^n + x^{n-1} + \dots + 1$ , J, r]

b) Parâmetro

poly\_: é um polinômio primitivo, tal que o grau n do mesmo deve ser um número múltiplo de J.

Exemplo: seja o seguinte polinômio primitivo

$$\text{poly} = x^6 + x^5 + x^2 + x + 1$$

$$J=3, r=3 \text{ e } n=6.$$

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

### c) Resultado

Como resultado obter-se-á uma seqüência na forma de uma matriz linha:

$$\text{GMW}[x^6+x^5+x^2+x+1, 3, 3]=$$

{0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0}

### BENT

Para construir-se funções de Bent, deve-se inicialmente calcular a matriz m. A seguir tem-se o exemplo utilizado no texto para ilustrar esta etapa.

$$m = \text{Table}[\text{Traco}[x^{(65(i-1)+j)}, x^{12+x^6+x^4+x+1}], \{i, 6\}, \{j, 12\}]$$

$$m = \{ \{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0\}, \\ \{0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1\}, \\ \{1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0\}, \\ \{1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0\}, \\ \{1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1\}, \\ \{0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1\} \\ \}$$

pc={1,0,0,1,0,1,0,0,0,0,1} polinômio característico utilizado no exemplo.

$$\text{bent}[\text{polcar\_d\_}] := \text{Module}[\{tp, ts, crd, chor, smc, x, x1, x2, g, fb, zx, sx, sbent, bij\},$$

$$tp = \text{Length}[\text{polcar}];$$

$$ts = 2^{tp-1};$$

$$crd = \text{ReplacePart}[\text{Table}[0, \{tp\}], 1, -1];$$

$$sbent = \text{Table}[0, \{ts\}];$$

$$s = \{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1\};$$

$$z = \text{IntegerDigits}[d, 2, 6];$$

$$\text{Do}[\{$$

$$x = \text{Mod}[m.crd, 2],$$

$$x1 = \text{Take}[x, \text{Length}[x]/2],$$

$$x2 = \text{Take}[x, -\text{Length}[x]/2],$$

$$g = x2[[1]] x2[[2]] x2[[3]],$$

```

fb=x1.x2,
zx=z.x,
sx=s.crd,
bij=Mod[sx+zx+fb+g,2],
sbent[[i]]=bij,
ubrd=crd[[tp]],
      crd=RotateRight[Mod[ crd+(ubrd polcar),2 ]],
      crd=ReplacePart[ crd,ubrd,1],
    },{i,1,ts}];
sbent
(*Save["Bent2",sbent]*)
]

```

#### a) Sintaxe

```
bent [{1,0,0,1,0,1,0,0,0,0,1}, 5 ]
```

#### b) Parâmetro

polcar\_: é um polinômio primitivo, utilizado para cálculo de m.

d\_: é um inteiro, que variará no subcorpo  $GF(2^{n/2})$ ; para cada valor é gerada uma seqüência.

Exemplo:

```
bent [{1,0,0,1,0,1,0,0,0,0,1}, 5 ]
```

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

#### c) Resultado

Como resultado obter-se-á uma seqüência na forma de uma matriz linha com 4095 elementos.

### **A4- FUNÇÕES AUXILIARES**

```

Decimacao[sequencia_,q_:1]:=Module[{seq,i,j},
  seq=Table[0,{Length[sequencia]}];
  Do[
    j=Mod[1+ i q,Length[sequencia]];
    seq[[i]]=sequencia[[ j ]],
    {i,1,Length[sequencia]}
  ];
  seq
];

```

Descrição funcional

## a) Sintaxe

Decimacao[{1,1,0,0...,0},3]

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

## c) Resultado

Obtém-se uma seqüência que é uma decimação da original e com comprimento igual ao original.

↯Polarize[x\_]:=(-1)^x;

Descrição funcional

## a) Sintaxe

Polarize[{1,1,0,0...,0}]

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

## c) Resultado

Obtém-se uma seqüência polarizada, isto é, de 1's e -1's

↯FasesCoincidentes[Seq1\_, Seq2\_]:= Module[{nada, j, fcoincidentes={ }},

j=0;

Do[

If[Seq1==RotateLeft[Seq2, j], fcoincidentes=Append[fcoincidentes, j],  
nada=j];

j=j+1,

{Length[Seq2]}

];

fcoincidentes

]

Descrição funcional

## a) Sintaxe

FasesCoincidentes[Seqüência1, Seqüência2]

onde Seqüência1 e Seqüência2 são quaisquer duas seqüências binárias entre chaves, polarizadas ou não.

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

## c) Resultado

Obtém-se um conjunto de números que indicam quantas vezes a Seqüência2 foi deslocada para a esquerda até coincidir com a Seqüência1. Se o conjunto for vazio significa que as duas seqüências são distintas.

Nota: Esta função também é útil para a verificação da periodicidade de uma seqüência.

```
⌘ Pesos[Seq1_,Seq2_]:=Module[{i,j=0,somamod2,resultado={}},
```

```
Do[
```

```
    somamod2=Mod[ Seq1 + RotateLeft[Seq2,j],2];
```

```
    peso=Sum[somamod2[[i]],{i,1,Length[somamod2]}];
```

```
    resultado=Append[resultado,peso],
```

```
    {j,0,Length[Seq1]-1}
```

```
];
```

```
resultado
```

```
]
```

Descrição funcional

a) Sintaxe

Pesos[Seqüência1, Seqüência2]

onde Seqüência1 e Seqüência2 são quaisquer duas seqüências binárias entre chaves.

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados. As seqüências devem possuir o mesmo número de elementos.

b) Descrição

Esta função executa a operação XOR bit a bit entre as seqüências, obtendo uma nova seqüência que indica o grau de "diferença" entre as duas seqüências; em seguida estes bits são somados. Esta operação é repetida para todos os deslocamentos possíveis entre as seqüências.

c) Resultado

Obtém-se um conjunto de números que podem ser interpretados como o grau de "diferença" entre as seqüências.

```
⌘ prop3[seq_,i_:0,j_:0]:=Module[{seqi,seqj,k,somamod2,resultado={}},
```

```
    seqi=RotateLeft[seq,i];
```

```
    seqj=RotateLeft[seq,j];
```

```
    somamod2=Mod[seqi+seqj,2];
```

```
Do[
```

```
    If[somamod2==RotateLeft[seq,k],resultado=Append[resultado,k],]
```

```
    {k,0,Length[seq]-1}
```

```
];
```

```
resultado
```

```
]
```

Descrição funcional

## a) Sintaxe

Prop3[Seqüência1, deslocamento1, deslocamento2]

onde Seqüência1 é uma seqüência binária e deslocamento1 e deslocamento2 são inteiros.

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

## c) Resultado

Obtém-se um conjunto de números.

↯ CorrelacaoPeriodica[x\_,y\_,l\_:0]:=x.RotateLeft[y,l];

Descrição funcional

## a) Sintaxe

CorrelacaoPeriodica[{1,1,-1,-1,...,-1},{-1,1,-1,1,...,-1},l]

## b) Parâmetros

x e y devem ser duas seqüências polarizadas e l um número inteiro que indicará o deslocamento entre as duas seqüências. O parâmetro l é zero quando omitido.

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

## c) Resultado

Obtém-se um valor que é a correlação cruzada periódica entre as seqüências polarizadas x e y para um deslocamento l entre elas.

↯ CorrelacaoAperiodica[x\_, y\_,l\_:0]:=Module[{tamanho,soma},

tamanho=Length[x];

If[l >= 0 && l<=tamanho, soma=Sum[ x[[i]] y[[i+l]],{i,1,tamanho-l}],;

If[l >= -(tamanho) && l<0,soma=Sum[ x[[i-l]] y[[i]],{i,1,tamanho+l}],;

soma

]

Descrição funcional

## a) Sintaxe

CorrelacaoAperiodica[{1,1,-1,-1,...,-1},{-1,1,-1,1,...,-1},l]

## b) Parâmetros

x e y devem ser duas seqüências polarizadas e l um número inteiro que indicará o deslocamento entre as duas seqüências. O parâmetro l é zero quando omitido.

Obs.: A função não faz nenhuma espécie de verificação, logo se os parâmetros não forem corretos obter-se-ão resultados errados.

## c) Resultado

Obtém-se um valor que é a correlação cruzada aperiódica entre as seqüências polarizadas x e y para um deslocamento l entre elas.

#### **A5- FUNÇÕES COMPLEMENTARES**

↪ `funcaoMi[seq1_,seq2_,n_:0]:=Module[{ },Sum[(CorrelacaoAperiodica[seq1,seq2,i]`

onde seq1 e seq2 são duas seqüências polarizadas e n um inteiro, que neste trabalho assumiu valores 0 ou 1

↪ `Betaij[seq1_,seq2_]:=Module[{ },(2funcaoMi[seq1,seq2] + funcaoMi[seq1,seq2,1])]`

Esta função calcula a interferência de múltiplo acesso.

Os parâmetros seq1 e seq2 são seqüências polarizadas.

↪ `EquivalenteLinear[seq_]:=Module[{comprimento,poliseq,poligeral,mdcpoli,poligerador,i},  
comprimento=Length[seq];  
poliseq=Sum[seq[[i]]*z^(comprimento-i),{i,1,comprimento}];  
poligeral=z^comprimento - 1;  
mdcpoli=PolynomialGCD[poligeral,poliseq,Modulus->2];  
poligerador=PolynomialQuotientMod[poligeral,mdcpoli,z,2];  
Exponent[poligerador,z]  
]`

Esta função retorna um inteiro, que representa o equivalente linear de seq, onde seq é uma seqüência não polarizada.

↪ `Primitivos[grau_]:=Module[{cyclo,fator01,fator02,sep01,sep02},  
cyclo=Cyclotomic[2^grau-1,x];  
fator01=Factor[cyclo,Modulus->2];  
fator02=FactorList[fator01];  
sep01=Table[fator02[[i,1]],{i,1,Length[fator02]}];  
sep02=Table[CoefficientList[sep01[[i]],x],{i,1,Length[sep01]}];  
sep03=Table[Delete[sep02[[i]],1],{i,1,Length[sep02]}];  
sep04=Table[Reverse[sep03[[i]]],{i,1,Length[sep03]}]  
]`

Esta função retorna os polinômios primitivos de um determinado grau, na forma de uma lista de coeficientes.

Obs.: O parâmetro grau é um número inteiro.

```

Traco[y1_,y2_]:=Module[{g,n},
  g=Exponent[y2,x]-1;
  PolynomialMod[
    Sum[PolynomialPowerMod[y1,2^n,{y2,2}],
      {n,0,g}],2]
]

```

Esta função calcula o traço de  $y1$  em relação a um polinômio primitivo  $y2$ .

Tanto  $y1$  como  $y2$ , devem ser escritos em função de  $x$ , por exemplo:

$$y1 = x^2 + x.$$

$$y2 = x^3 + x + 1.$$

As funções vistas neste anexo interagem entre si, sendo necessário que todas sejam implementadas num arquivo único e assim carregadas no software *Mathematica*.

## **REFERÊNCIAS BIBLIOGRÁFICAS**

1. PICKHOLTZ, R. L.; SCHILLING, D. L.; MILSTEIN, L. B. Theory of Spread Spectrum Communications -A Tutorial. IEEE Transactions on Communications, 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 Sequências de Códigos. Notas de Aula do Curso de Comunicação por Espalhamento Espectral (PEE-710). 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 Sequências 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. ROTHBAUS, 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. FLANNERY, B. P.; TEUKOLSKY, S. A.; VETTERLING, W. T. Numerical Recipes. William H. Press, Cambridge University Press. p. 326-334, 1988.

17. KÄRKKÄINEN, KARI H. A. Mean-Square Cross-Correlation as Performance Measure for Spreading Code Families. IEEE Second International Symposium on Spread Spectrum Techniques and Applications (ISSSTA'92). Yokohama, Japan, Nov-Dec 1992.

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

### **BIBLIOGRAFIA RECOMENDADA**

ADAMS, C. M.; TAVARES, S. E. Generating and Counting Binary Bent Sequences. IEEE Transactions on Information Theory, v. IT-36, n. 5, p. 1170-1173, Sept. 1990.

BEKIR, N. E.; SCHOLTZ, R. A.; WELCH, L. R. Partial-Periodic Correlation Properties of PN Sequences. National Telecommunications Conf. Rec. v. 3, p. 35.1.1-35.1.4, 1978.

COOK, C. E.; MARSH, H. S. An Introduction to Spread Spectrum. IEEE Communications Magazine. v. 21, n. 2, p. 8-16, Mar. 1983.

DIXON, R. C. Spread Spectrum Systems. ed2 John Wiley & Sons, 1984.

GOLD, R. Optimal Binary Sequences for Spread Spectrum Multiplexing. IEEE Transactions on Information Theory. v. IT-13, n. 5, p. 619-621, Oct. 1967.

GOLD, R. Maximal Recursive Sequences with 3-Valued Recursive Crosscorrelation Functions. IEEE Transactions on Information Theory. v. IT-14, n. 1, p. 154-156, Jan. 1968.

GOLOMB, S. W. Correlation Properties of Periodic and Aperiodic Sequences, and Applications to Multi-Users Systems in New Concepts in Multi-User Communication. NATO Advanced Study Institutes Series. J. K. Skwirzynski (editor), Sijthoff Noordhoff International Publishers. p. 161-197, 1981.

GOLOMB, S. W. Shift Register Sequences. Aegean Park Press, Laguna Hills-CA, 1982.

HELLESETH, T. Some Results About the Cross-Correlation Function between Two Maximal Linear Sequences. *Discrete Mathematics*, n. 16, p. 209-232, 1976.

JESZENSKY, P. J. E. Calculation of the Bit Error Probability in a Direct Sequence Spread Spectrum Systems with Code Division Multiple Access. *International Telecommunications Symposium. Symposium Record* p. 12.3.1-12.3.5, Sept. 1990.

JESZENSKY, P. J. E. Introdução à Técnica de Comunicação por Espalhamento Espectral (Spread Spectrum). Mini Curso B apresentado no 9º Simpósio Brasileiro de Telecomunicações. p. 1-61, Sept. 1991.

JESZENSKY, P. J. E. Uma Revisão sobre Geradores Lineares de Sequências para Comunicação por Espalhamento Espectral. 9º Simpósio Brasileiro de Telecomunicações. p. 11.4.1-11.4.6, set. 1991.

KUMAR, P. V., SCHOLTZ, R. A. Bounds on the Linear Span of Bent Sequences. *IEEE Transactions on Information Theory*. v. IT-29, n. 6, p. 854-862, Nov. 1983.

LEHNERT, J. S.; PURSLEY, M. B. Error Probabilities for Binary Direct-Sequence Spread-Spectrum Communications with Random Sequence Signatures. *IEEE Transactions on Communications*. v. COM-35, n. 1, p. 87-98, Jan. 1987.

MCELIECE, R. J. *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, 1987.

NAZARI, N.; ZIEMER, R. E. Computationally Efficient Bounds for the Performance of Direct-Sequence Spread Spectrum Multiple-Access Communications Systems in Jamming Environments. *IEEE Transactions on Communications*. v. COM-36, n. 5, p. 577-587, May. 1988.

NO, J. S.; KUMAR, P. V. A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and Large Linear Span. *IEEE Transactions on Information Theory*. v. IT-35, n. 2, p. 371-379, Mar. 1989.

OLSEN, J. D.; SCHOLTZ, R. A.; WELCH, L. R. Bent Function Sequences. *IEEE Transactions on Information Theory*. v. IT-28, n. 6, p. 858-864, Nov. 1982.

PAPOULIS, A. *Probability, Random Variables, and Stochastic Processes*. McGraw-Hill International Book Co. ed2, 1984.

PURSLEY, M. B.; SARWATE, D. V. Bounds on Aperiodic Cross-Correlation for Binary Sequences. *Electronics Letters*, v. 12, n. 12, p. 304-305, 10<sup>th</sup> June 1976.

PURSLEY, M. B.; SARWATE, D. V. Evaluation of Correlation Parameters for Periodic Sequences. *IEEE Transactions on Information Theory*. v. IT-23, p. 508-513, July 1977.

PURSLEY, M. B. Performance Evaluation for Phase-Coded Spread Spectrum Multiple-Access Communication-Part I: System Analysis. IEEE Transactions on Communications, v. COM-25, n 8, p. 795-799, Aug. 1977.

PURSLEY, M. B.; SARWATE, D. V. Performance Evaluation for Phase-Coded Spread Spectrum Multiple-Access Communication-Part II: Code Sequence Analysis. IEEE Transactions on Communications. v. COM-25, n. 8, p. 800-803, Aug. 1977.

PURSLEY, M. B.; ROEFS, H. F. A. Numerical Evaluation of Correlation Parameters for Optimal Phases of Binary Shift-Register Sequences. IEEE Transactions on Communications, v. COM-27, n 10, p. 1597-1604, Oct. 1979.

PURSLEY, M. B.; SARWATE D. V.; STARK, W. E. Error Probability for Direct-Sequence Spread Spectrum Multiple Access Communications: Part I: Upper and Lower Bounds. IEEE Transactions on Communications. v. COM-30, n. 5, p. 975-984, May. 1982.

ROEFS, H. F.; PURSLEY, M. B. Correlation Parameters of Random Binary Sequences. Electronics Letters, v. 13, n. 16, p. 488-489, 4<sup>th</sup> Aug. 1977.

SARWATE, D. V.; PURSLEY, M. B. New Correlation Identities for Periodic Sequences. Electronics Letters, v. 13, n. 2, p. 48-49, 20<sup>th</sup> January 1977.

SARWATE, D. V. Bounds on Crosscorrelation and Autocorrelation of Sequences. IEEE Transactions on Information Theory, v. IT-25, n. 6, p. 720-724, Nov. 1979.

SARWATE, D. V. Sets of Complementary Sequences. Electronics Letters, v. 19, n. 18, p. 711-712, 10<sup>th</sup> June 1983.

SARWATE, D. V. Mean Square Correlation of Shift Register Sequences. IEE Proceedings. v. 131, Part F, n. 2, p. 101-106, Apr. 1984.

SARWATE, D. V.; PURSLEY, M. B.; BASAR, T. Ü. Partial Correlation Effects in Direct-Sequence Spread-Spectrum Multiple-Access Communication Systems. IEEE Transactions on Communications. v. COM-32, n. 5, p. 567-573, May. 1984.

SARWATE, D. V. An Upper Bound on the Aperiod Autocorrelation Function for a Maximal-Lenght Sequence. IEEE Transactions on Information Theory, v. IT-30, n. 4, p. 685-687, July 1984.

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

TORRIERE, D. J. Principles of Secure Communication Systems. Artech House, 1985.

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.

ZIEMER, R. E.; PETERSON, R. L. Digital Communications and Spread Spectrum Systems. MacMillan Publishing Co., 1985.

## **APÊNDICE:**

### **A1 - 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  $a, b, c, \dots$  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 ( $a \cdot b=c, ab=c$ ).

#### 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:  $a + 0 = a$ ,  $a \cdot 1 = a$

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:  $a + (-a) = 0$ ,  $a \cdot (a^{-1}) = 1$ .

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 Abelianos 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  $2 + 3 = 5 = 0 \text{ mod } 5$ .

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 Abelianos 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 Abelianiano 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  $3+5=1 \text{ mod } 7$ .

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

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  $\text{ord}(x)=t$ .

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

Todos os elementos de  $\text{GF}(q)$  são potências de um elemento primitivo e todo  $\text{GF}(q)$  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  $\text{GF}(2)$  e baseados em polinômios que não possuam raízes pertencentes à  $\text{GF}(2)$ .

Exemplo:

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

$x$  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:

$$\text{Tr}_F^K(x) = x + x^q + x^{q^2} + \dots + x^{q^{n-1}}$$

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).

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

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 sequência pode ser expresso através da função traço.

$$b_i = \text{Tr}_F^K(x^i) = \text{Tr}(x^i), \text{ onde } x \text{ representa um elemento primitivo do corpo.}$$

Quando K e F forem conhecidos os mesmos serão omitidos.

#### Propriedades da função traço

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

$$a) \text{Tr}(a) \in F$$

$$b) \text{Tr}(a + b) = \text{Tr}(a) + \text{Tr}(b)$$

$$c) \text{Tr}(\lambda \cdot a) = \lambda \cdot \text{Tr}(a) \text{ onde } \lambda \in F$$

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

Seja  $\{b_i\}$  uma SMC qualquer e  $\{b_{di}\}$  uma sequência 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 sequência.

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:

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

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

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

Se  $n$  é ímpar 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.

## A2 - DECIMAÇÃO DE SEQUÊNCIAS<sup>18</sup>

Seja  $\{a_n\}$  uma sequência arbitrária de comprimento  $p$ . Denomina-se decimação  $k$  da sequência original à sequência  $\{c_n\}$  tal que  $c_n = a_{kn}$  para todo  $n$ . Por exemplo: 110110... é uma decimação 2 possível da sequência 10100010100010.... É evidente que se  $k$  dividir  $p$  então  $\{c_n\}$  terá um período de, no máximo,  $p/k$  (no exemplo anterior  $p=6$ ,  $k=2$  e o período da sequência decimada é 3), e portanto se  $p$  e  $k$  são primos entre si o período resultante será  $p$ . Genericamente, o período da sequência decimada é dada por  $p/\text{mdc}(p,k)$ . Seja então  $\{a_n\}$  uma SMC com  $p=(2^n-1)$ , nestas condições demonstra-se que:

- a decimação  $a_{kn}$  de  $a_n$  é uma SMC se, e somente se,  $k$  e  $p$  forem primos entre si;
- todas as SMC's de período  $p=(2^n-1)$  podem ser construídas por decimação de  $\{a_n\}$ ;
- o polinômio primitivo correspondente à sequência obtida por decimação  $k$  é tal que suas raízes são a potência  $k$ -ésima das raízes do polinômio original. Os números que antecedem os polinômios na notação octal referem-se exatamente a esta propriedade. Assim se  $\alpha$  é raiz de 1-[103] então  $\alpha^5$  será raiz de 5-[147], e desta forma a sequência gerada pelo polinômio [147] pode ser obtida por uma decimação 5 da sequência correspondente ao polinômio [103];
- duas sequências produzidas por decimação, com  $j$  e  $k$  primos em relação a  $(2^n-1)$ , são ciclicamente distintas se, e somente se,  $j \not\equiv 2^i k \pmod{(2^n-1)}$  para todo inteiro  $i$ .

Por exemplo:  $n=4$ ;  $p=(2^4-1)=15=3 \times 5 \Rightarrow \lambda(n)=2$  que é o número de SMC's que existem para este grau. Dada uma delas a outra pode ser obtida por uma decimação

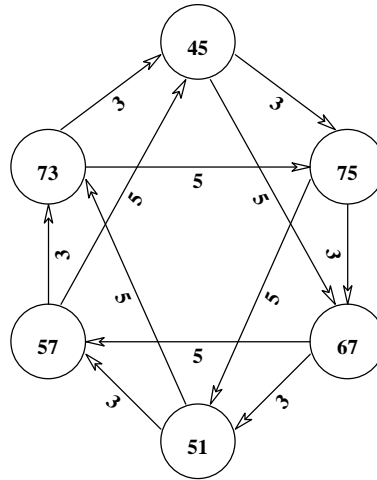
conveniente. As decimações possíveis são: 1; 2; ..... 14; 15. Destas devem ser descartadas todas as que tem fatores comuns com 15. Restam pois as alternativas 2; 4; 7; 8; 11; 13; 14. e para estas pode-se construir a tabela indicada a seguir.

k	$k \times 2^i$		
	$i = 1$	$i = 2$	$i = 4$
2	2	4	8
4	4	8	16
7	7	14	$28 \equiv 13$
8	8	$16 \equiv 1$	$32 \equiv 2$
11	11	$22 \equiv 7$	$44 \equiv 14$
13	13	$26 \equiv 11$	$52 \equiv 7$
14	14	$28 \equiv 13$	$56 \equiv 11$

Observa-se então que as decimações 2; 4 e 8 são impróprias (conduzem a fases diferentes da mesma seqüência), enquanto as decimações 7; 11; 13 e 14 conduzem à outra seqüência procurada (conforme o valor ter-se-á fases distintas da mesma seqüência). Destes resultados pode-se ainda inferir:

- se  $k$  é uma decimação própria da seqüência, as decimações  $2^i k \bmod (2^n - 1)$  levam a fases diferentes da mesma seqüência, para  $i=1; 2; \dots; n-1$ ;
- todas as decimações pares levam a fases diferentes da mesma seqüência;
- decimações próprias só são obtidas com  $k$  ímpar e obedecendo ao teorema enunciado.

Exemplo final:  $n=5$ ;  $p=(2^n-1)=31$  e  $\lambda(5)=6$ . Representando-os graficamente tem-se:



Os números nas interligações indicam as decimações, onde então de cada seqüência ilustra-se a construção de mais duas, com  $k=3$  e  $5$ . Observa-se que partindo da seqüência  $[73]$  pode-se obter a seqüência  $[57]$ , por exemplo, por decimações sucessivas de  $5$ ;  $5$  e  $3$ ; e como  $5 \times 5 \times 3 = 75 = 13 \pmod{31}$  o mesmo resultado é obtido com uma decimação  $13$ . Observação:  $[51]$ ;  $[57]$  e  $[73]$  são recíprocos de  $[45]$ ;  $[75]$  e  $[67]$ , respectivamente.

Sistematizando o processo de decimação, seja para este último exemplo a tabela a seguir representada.

$C_0$	$1_{**}^*$	2	4	8	$16^*$
$C_1$	$3_{***}^*$	6	12	24	17
$C_2$	$5_{**}^*$	10	20	$9^*$	18
$C_3$	7	14	28	$25_{**}^*$	$19^*$
$C_4$	11	22	$13_{***}^*$	$26^*$	21
$C_5$	$15_{***}^*$	30	29	$27^*$	23

Os elementos desta tabela constituem-se dos números de 1 a 30 ( $2^n - 2$ ) e indicam as decimações possíveis de uma dada seqüência. Numa linha os números sucessivos são sempre o dobro do anterior  $\pmod{31}$ , de forma que todas as decimações desta linha são

equivalentes, conforme teorema anterior (a menos da fase da seqüência resultante). A primeira linha desta tabela é constituída de potências sucessivas de 2, de 1 até  $2^{n-1}$ . A próxima linha inicia-se com o menor número inteiro de 1 a 30, ainda não coberto pelas linhas anteriores, e assim sucessivamente. Desta forma, com esta tabela, tem-se uma construção sistemática para todas as SMC's de um determinado grau. Nesta tabela (ver também o diagrama anterior), a título de exemplo, indicam-se por:

$N^*$  decimações sucessivas de 3, a partir do elemento 1. Na ordem percorrem-se os elementos 1; 3; 9; 27; 19; 26 e 16 (que corresponde a uma fase diferente da seqüência de partida);

$N^{**}$  decimações sucessivas de 5, a partir do elemento 1. Na ordem percorrem-se os elementos 1; 5; 25 e retorna-se a 1.

$N^{***}$  decimações sucessivas de 5, a partir do elemento 3. Na ordem percorrem-se os elementos 3; 15; 13 e retorna-se a 3.

Ao conjunto de conjuntos  $C_0; C_1; \dots$ , acrescido de  $\{0\}$ , dá-se o nome de coconjunto ciclotômico de grau  $n$  (estudos nesta área remontam ao ano de 1800 com Gauss).