André Seichi Ribeiro Kuramoto

Metodologias de seleção de seqüências de espalhamento para sistemas DS/CDMA quase síncronos

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

São Paulo
2005

André Seichi Ribeiro Kuramoto

Metodologias de seleção de seqüências de espalhamento para sistemas DS/CDMA quase síncronos

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

Área de concentração:
Sistemas Eletrônicos

Orientador:
Prof. Dr. Paul Jean Etienne Jeszensky

São Paulo
2005

Ficha Catalográfica

Kuramoto, André Seichi Ribeiro

Metodologias de seleção de seqüências de espalhamento para sistemas DS/CDMA quase síncronos. São Paulo, 2005. 261 p.

Dissertação (Mestrado) — Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Telecomunicações e Controle.

1. Espalhamento espectral. 2. Seqüências de espalhamento. 3. CDMA. 4. Quase síncrono. 5. Múltipla taxa. I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Telecomunicações e Controle. II. Área de Sistemas Eletrônicos.

Aos meus pais.

Agradecimentos

Meus sinceros agradecimentos ao professor Dr. Paul Jean E. Jeszensky pela paciência e dedicação no trabalho de orientação e pela motivação e constante apoio para a realização desta dissertação. Ao professor Dr. Taufik Abrão pelas horas dedicadas às discussões sobre o tema da dissertação e ao constante incentivo que muito contribuiram. Aos colegas do Laboratório de Comunicações e Sinais (LCS) do Departamento de Engenharia de Telecomunicações e Controle da Escola Politécnica da Universidade de São Paulo (EPUSP): Vanderlei A. da Silva, Bruno A. Angélico, Ivan R. S. Casella e Elvis M. G. Stancanelli; ao colega Fernando Ciriaco Dias Neto do Laboratório de Telecomunicações do Departamento de Engenharia Elétrica da Universidade Estadual de Londrina (UEL) pelas informações técnicas compartilhadas. À minha família e à Karina Miceli pelo constante incentivo e apoio. Às minhas amigas Edilma e Aline Stümer pelo conhecimento compartilhado.

Resumo

Este trabalho apresenta um estudo sobre alguns métodos propostos de obtenção de famílias de seqüências adequadas para a função de espalhamento em sistemas QS-CDMA. Neste estudo, são consideradas seqüências binárias, polifásicas e uma família de seqüências ternárias recentemente proposta na literatura. Especial atenção é dada às famílias de seqüências binárias. Para algumas destas famílias, são apresentadas figuras de desempenho em termos de taxa de erro de bit para um sistema de comunicação móvel QS-CDMA com recepção convencional em canal Rayleigh multipercurso. Tais figuras auxiliam a avaliação destas famílias de seqüências binárias.

Na literatura, poucos trabalhos são encontrados sobre seqüências adequadas a sistemas QS-CDMA de taxa de dados variável (multitaxa). Neste trabalho, avalia-se a utilização das seqüências binárias previamente estudadas em um sistema QS-CDMA multitaxa do tipo múltiplos códigos de espalhamento. Para o sistema QS-CDMA multitaxa do tipo múltiplos ganhos de processamento é proposta uma metodologia de seleção de seqüências.

As conclusões deste trabalho envolvem a classificação das metodologias de obtenção das famílias de seqüências em termos de complexidade do método, características das famílias de seqüências resultantes, desempenhos proporcionados em um sistema QS-CDMA e a aplicabilidade em um sistema QS-CDMA multitaxa.

Abstract

This work presents a study on some proposed methods of obtaining families of appropriate sequences for the spreading function in QS-CDMA systems. In this study, binary and poliphase sequences and a family of ternary sequences recently proposed in the literature are considered. Special attention is given to the families of binary sequences. For some of these families, performance illustrations are presented in terms of bit error rate for a QS-CDMA mobile communication system with conventional reception in multipath Rayleigh fading channel. Such illustrations aid the evaluation of these families of binary sequences.

In the literature they are found few works on appropriate sequences for QS-CDMA systems with variable data rates (multirate). In this work, it was evaluated the use of the binary sequences previously studied in a multirate QS-CDMA system with multiple code scheme. For the multirate QS-CDMA system with multiple processing gains a methodology of sequence selection was proposed.

The conclusions of this work involve the classification of the methodologies of obtaining the families of sequences in terms of: complexity of the method, characteristic of the resulting families of sequences, proportionate performance in a QS-CDMA system and the applicability in a multirate QS-CDMA system.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

1G Primeira geração.

2G Segunda geração.

3G Terceira geração.

4G Quarta geração.

AMPS *Advanced Mobile Phone System*.

ANATEL Agência Nacional de Telecomunicações.

AWGN Ruído aditivo branco Gaussiano (*additive white Gaussian noise*).

BER Taxa de erro de bit (*bit error rate*).

BPSK *Binary phase-shift keying*.

BW Largura de banda (*band width*).

CDMA Acesso múltiplo por divisão de códigos (*code division multiple access*).

DFT Transformada discreta de Fourier (*discret Fourier transform*).

DS/CDMA CDMA de seqüência direta (*direct sequence* CDMA).

EAC Autocorrelação par (*even autocorrelation*).

ECC Correlação cruzada par (*even cross-correlation*).

ERB Estação rádio base.

ESA *European Space Agency*.

FDMA Acesso múltiplo por divisão de freqüências (*frequency division multiple access*).

GPS *Global Positioning System*.

GSM *Global System for Mobile Communication*.

IMT-2000 *International Mobile Telecommunication*-2000.

IS-95 *Interim Standard*-95.

ITU *International Telecommunication Union*.

LCZ Zona de correlação reduzida (*low correlation zone*).

MAI Interferência de múltiplo acesso (*multiple access interference*).

MC *Multi-code*.

MM *Multi-modulation*.

MPG *Multi processing gain*.

MPSK *M-ary phase-shift keying*.

MQAM *M-ary quadrature amplitude modulation*.

MRC Combinador de razão máxima (*maximum ratio combiner*).

MuD Detector multiusuário (*multi-user-detector*).

OAC Autocorrelação ímpar (*odd autocorrelation*).

OCC Correlação cruzada ímpar (*odd cross-correlation*).

pdf Função densidade de probabilidade (*probability density function*).

PIC Cancelador de interferência paralelo (*parallel interference canceller*).

PIC-HD PIC com decisão abrupta (*parallel interference canceller with hard decision*).

QS-CDMA DS/CDMA quase síncrono (*quasi-synchronous* DS/CDMA).

SA Recozimento simulado (*simulated annealing*).

SI Auto-interferência (*self-interference*).

SII Auto-interferência intersimbólica (*self intersymbol interference*).

SCI Auto-interferência de um mesmo símbolo (*self current-symbol interference*).

SMC Seqüência de máximo comprimento.

SNIR Relação sinal-ruído-interferência (*signal-to-noise plus interference ratio*).

SNIRT SNIR alvo (*signal-to-noise plus interference ratio target*).

TDMA Acesso múltiplo por divisão de tempo (*time division multiple access*).

TSP Problema do caixeiro viajante (*traveling salesman problem*).

VCR *Variable chip rate*.

WCDMA *Wideband* CDMA.

WH *Walsh-Hadamard*.

ZCZ Zona de correlação nula (*zero correlation zone*).

Lista de Símbolos

Nas expressões matemáticas, os símbolos principais e de maior ocorrência estão listados abaixo.

símbolo	descrição
T_c	período de *chip*.
Load	carregamento do sistema dado por $\frac{U}{N}$.
U	número de usuários ativos no sistema.
N	comprimento da seqüência.
T	período do símbolo de informação.
G	ganho de processamento dado por $\frac{T}{T_c}$.
P	potência do sinal recebido.
$\alpha_{\mathcal{L}}$	ganho do canal para o componente multipercurso $\mathcal{L}$.
$\tau_{u,\mathcal{L}}$	atraso absoluto do $\mathcal{L}$-ésimo componente multipercurso do u-ésimo usuário em um sistema de taxa única.
$\tau_{u,j,\mathcal{L}}$	atraso absoluto do $\mathcal{L}$-ésimo componente multipercurso do u-ésimo usuário do serviço j em um sistema que utiliza o esquema MPG.
$\phi_{k,\ell}$	deslocamento de fase devido ao atraso $\tau_{k,\ell}$.
$\phi_{k,i,\ell}$	deslocamento de fase devido ao atraso $\tau_{k,i,\ell}$.
b_k	símbolo de informação do k-ésimo usuário em um sistema de taxa única.
$b_{k,h}$	símbolo de informação do h-ésimo canal do k-ésimo usuário em um sistema que utiliza o esquema MC.
$b_{k,i}$	símbolo de informação do k-ésimo usuário do serviço i em um sistema que utiliza o esquema MPG.
D	número de correlacionadores (*fingers*) do Rake.
$I_{k,\ell}$	MAI sobre o ℓ-ésimo componente multipercurso do k-ésimo usuário em um sistema de taxa única.

continua...

símbolo	descrição
$I_{k,h,\ell}$	MAI sobre o ℓ-ésimo componente multipercurso do h-ésimo canal do k-ésimo usuário em um sistema que utiliza o esquema MC.
$I_{k,i,\ell}$	MAI sobre o ℓ-ésimo componente multipercurso do k-ésimo usuário do serviço i em um sistema que utiliza o esquema MPG.
$SI_{k,\ell}$	SI sobre o ℓ-ésimo componente multipercurso do k-ésimo usuário em um sistema de taxa única.
$SI_{k,h,\ell}$	SI sobre o ℓ-ésimo componente multipercurso do h-ésimo canal do k-ésimo usuário em um sistema que utiliza o esquema MC.
$SI_{k,i,\ell}$	SI sobre o ℓ-ésimo componente multipercurso do k-ésimo usuário do serviço i em um sistema que utiliza o esquema MPG.
$SII_{k,\ell}$	SII sobre o ℓ-ésimo componente multipercurso do k-ésimo usuário em um sistema de taxa única.
$\varphi_{u,\mathcal{L}}$	fase relativa das portadoras do sinal de interesse e do sinal interferente ($\varphi_{u,\mathcal{L}} = \phi_{u,\mathcal{L}} - \phi_{k,\ell}$).
$\varphi_{u,j,\mathcal{L}}$	fase relativa das portadoras do sinal de interesse e do sinal interferente ($\varphi_{u,j,\mathcal{L}} = \phi_{u,j,\mathcal{L}} - \phi_{k,i,\ell}$).
$\tau_{u,\mathcal{L}}$	atraso relativo entre o sinal de interesse e o sinal interferente ($\tau_{u,\mathcal{L}} = \tau_{u,\mathcal{L}} - \tau_{k,\ell}$).
$\tau_{u,j,\mathcal{L}}$	atraso relativo entre o sinal de interesse e o sinal interferente ($\tau_{u,j,\mathcal{L}} = \tau_{u,j,\mathcal{L}} - \tau_{k,i,\ell}$).
Δ_ℓ	atraso do ℓ-ésimo componente multipercurso dado um perfil atraso-potência.
$\gamma_{\mathcal{L}}$	atraso relativo entre o componente multipercurso de interesse e um componente multipercurso interferente ($\gamma_{\mathcal{L}} = \Delta_{\mathcal{L}} - \Delta_\ell$).
$\tau_{\max}$	erro máximo de sincronismo, dado pela maior diferença entre os atrasos dos $\mathcal{L}$-ésimos componentes multipercurso de dois usuários ($\max\{\lvert\tau_{u,\mathcal{L}}\rvert\}$).

continua...

símbolo	descrição
L_{CZ}	zona de correlação reduzida.
Z_{CZ}	zona de correlação nula.
$\mathbb{T}^i\mathbf{x}$	deslocamento cíclico para a esquerda de i posições da seqüência $\mathbf{x}$.
$\{s_t\}$	seqüência $\mathbf{s}$. No texto, algumas vezes as chaves { } serão omitidas para simplificar a notação.
$s_k(t)$	sinal transmitido pelo k-ésimo usuário em um sistema de taxa única.
$s_{k,h}(t)$	sinal transmitido por meio do h-ésimo canal do k-ésimo usuário em um sistema que utiliza o esquema MC.
$s_{k,i}(t)$	sinal transmitido pelo k-ésimo usuário do serviço i em um sistema que utiliza o esquema MPG.
$c_k(t)$	sinal relativo à seqüência de espalhamento utilizada pelo k-ésimo usuário em um sistema de taxa única.
$c_{k,h}(t)$	sinal relativo à seqüência de espalhamento utilizada no h-ésimo canal pelo k-ésimo usuário em um sistema que utiliza o esquema MC.
$c_{k,i}(t)$	sinal relativo à seqüência de espalhamento utilizada pelo k-ésimo usuário do serviço i em um sistema que utiliza o esquema MPG.
$r(t)$	sinal recebido na estação rádio base.
$z_{k,\ell}$	saída do ℓ-ésimo correlacionador do k-ésimo usuário em um sistema de taxa única.
$z_{k,h,\ell}$	saída do ℓ-ésimo correlacionador do h-ésimo canal do k-ésimo usuário em um sistema que utiliza o esquema MC.
$z_{k,i,\ell}$	saída do ℓ-ésimo correlacionador do k-ésimo usuário do serviço i em um sistema que utiliza o esquema MPG.
y_k	saída do combinador do k-ésimo usuário em um sistema de taxa única.
$y_{k,h}$	saída do combinador do h-ésimo canal do k-ésimo usuário em um sistema que utiliza o esquema MC.

continua...

símbolo	descrição
$y_{k,i}$	saída do combinador do k-ésimo usuário do serviço i em um sistema que utiliza o esquema MPG.
$SNIR_{k,\ell}$	SNIR na saída do ℓ-ésimo correlacionador do k-ésimo usuário em um sistema de taxa única.
$SNIR_{k,h,\ell}$	SNIR na saída do ℓ-ésimo correlacionador do h-ésimo canal do k-ésimo usuário em um sistema que utiliza o esquema MC.
$SNIR_{k,i,\ell}$	SNIR na saída do ℓ-ésimo correlacionador do k-ésimo usuário do serviço i em um sistema que utiliza o esquema MPG.
$n(t)$	sinal relativo ao AWGN.
$n_{k,\ell}$	sinal relativo ao AWGN processado para o ℓ-ésimo correlacionador do k-ésimo usuário em um sistema de taxa única.
$n_{k,h,\ell}$	sinal relativo ao AWGN processado para o ℓ-ésimo correlacionador do h-ésimo canal do k-ésimo usuário em um sistema que utiliza o esquema MC.
$n_{k,i,\ell}$	sinal relativo ao AWGN processado para o ℓ-ésimo correlacionador do k-ésimo usuário do serviço i em um sistema que utiliza o esquema MPG.
$\Re\{x\}$	parte real de x.
N_0	densidade espectral de potência bilateral de $n(t)$.
$\delta(t)$	função delta de Dirac.
$\mathcal{R}_{u,k}(\tau)$	função de correlação parcial par entre $c_u(t)$ e $c_k(t)$.
$\tilde{\mathcal{R}}_{u,k}(\tau)$	função de correlação parcial ímpar entre $c_u(t)$ e $c_k(t)$.
$\mathcal{R}_{u,g,k,h}(\tau)$	função de correlação parcial par entre $c_{u,g}(t)$ e $c_{k,h}(t)$.
$\tilde{\mathcal{R}}_{u,g,k,h}(\tau)$	função de correlação parcial ímpar entre $c_{u,g}(t)$ e $c_{k,h}(t)$.
$C_{u,k}(d)$	função de correlação aperiódica entre as seqüências $\mathbf{c}_u$ e $\mathbf{c}_k$.
$C_{u,g,k,h}(d)$	função de correlação aperiódica entre as seqüências $\mathbf{c}_{u,g}$ e $\mathbf{c}_{k,h}$.
$\theta(\mathbf{c}_i, \mathbf{c}_j, d)$	(ou $\theta_{i,j}(d)$) função de correlação periódica par entre as seqüências $\mathbf{c}_i$ e $\mathbf{c}_j$.

continua...

símbolo	descrição
$\Theta(\mathbf{c}_i, \mathbf{c}_j, d)$	(ou $\Theta_{i,j}(d)$) função de correlação periódica ímpar entre as seqüências $\mathbf{c}_i$ e $\mathbf{c}_j$.
T	período de bit.
K	número de seqüências em um conjunto.
$\phi(.)$	função de Euler.
$GF(p)$	corpo D mod p, onde D é o conjunto fundamental e p um número primo.
$Tr_m^n(\alpha)$	função traço, apêndice B.1.8.
ord(α)	ordem do elemento α.
mdc(x, y)	máximo divisor comum entre x e y.
$\lfloor x \rfloor$	maior inteiro menor ou igual a x.
$\lceil x \rceil$	menor inteiro maior ou igual a x.
BER_k	taxa de erro de bit para o k-ésimo usuário em um sistema de taxa única.
$BER_{k,h}$	taxa de erro de bit para o h-ésimo canal do k-ésimo usuário em um sistema que utiliza o esquema MC.
$BER_{k,i}$	taxa de erro de bit para o k-ésimo usuário do serviço i em um sistema que utiliza o esquema MPG.
$\overline{BER}$	taxa de erro de bit média.

1 Introdução

O sistema de telefonia móvel celular comercial começou a operar na América em 1983 com o sistema *Advanced Mobile Phone System* (AMPS). Projeções indicavam que os telefones celulares seriam utilizados apenas por uma pequena parcela da população, a qual não superaria um milhão de usuários nos Estados Unidos até 1990. Porém, já no início da década de 90, os EUA contavam com mais de cinco milhões de usuários; em 2002 eles já eram quase 140 milhões. Nesse mesmo ano, no mundo todo, eram mais de um bilhão de usuários de telefonia sem fio (*wireless telephony*), superando o número de telefones fixos (WHALEN, 2002). Segundo a ANATEL (Agência Nacional de Telecomunicações), em agosto de 2003 o número de telefones celulares no Brasil ultrapassou o número de telefones fixos: $40,09$ milhões de celulares contra $39,10$ milhões de telefones fixos.

Os primeiros sistemas celulares, ou sistemas de primeira geração (1G), utilizavam tecnologia analógica de acesso múltiplo por divisão de freqüência (*frequency division multiple access*, FDMA) para prover os canais de voz. Tais sistemas eram bastante restritivos: possuíam cobertura limitada, baixa capacidade, reduzida eficiência em potência e banda e baixa qualidade de voz. Na segunda metade da década de 1980, os sistemas de segunda geração (2G) foram desenvolvidos utilizando tecnologia digital. O primeiro sistema de 2G introduzido nos EUA utilizava a técnica de acesso múltiplo por divisão de tempo (*time division multiple access*, TDMA), a qual foi, em 1990, adotada para o *Global System for Mobile Communication* (GSM) na Europa. Em meados de 1990, a técnica de acesso múltiplo por divisão de códigos (*code division multiple access*, CDMA) surgiu como o segundo tipo de sistemas de 2G, o qual foi chamado de *Interim Standard-95* (IS-95). Hoje, a indústria está caminhando para sistemas de maior capacidade que suportam altas taxas de transmissão e aplicações multimídia. Assim, surgem os sistemas de terceira geração (3G), utilizando também a técnica de multiplexação CDMA e os antigos FDMA e TDMA vão sendo abandonados.

Em 1990, a seção de padronização do ITU (*International Telecommunication Union*) iniciou seus trabalhos visando o futuro dos sistemas de comunicações móveis terrestres, os quais resultaram no padrão *International Mobile Telecommunication* -2000 (IMT-2000). O número 2000 foi adicionado ao nome do padrão porque previa-se que seus serviços estariam disponíveis por volta do ano 2000. Porém, tais serviços começaram a operar somente durante o ano de 2002.

Como especificado no padrão, os sistemas de 3G integram diferentes serviços para diferentes áreas de cobertura. Por exemplo, um usuário de baixíssima mobilidade dentro de um escritório coberto por uma "picocélula", pode ter disponível uma taxa de dados maior que $2,048 Mbps$. Para um pedestre coberto por uma "microcélula", a taxa de dados pode ser superior a $384 kbps$ e, para um usuário com mobilidade veicular operando em uma macrocélula, a taxa de dados é de, no mínimo, $144 kbps$. A figura 1.1 ilustra a hierarquia de um sistema de 3G.

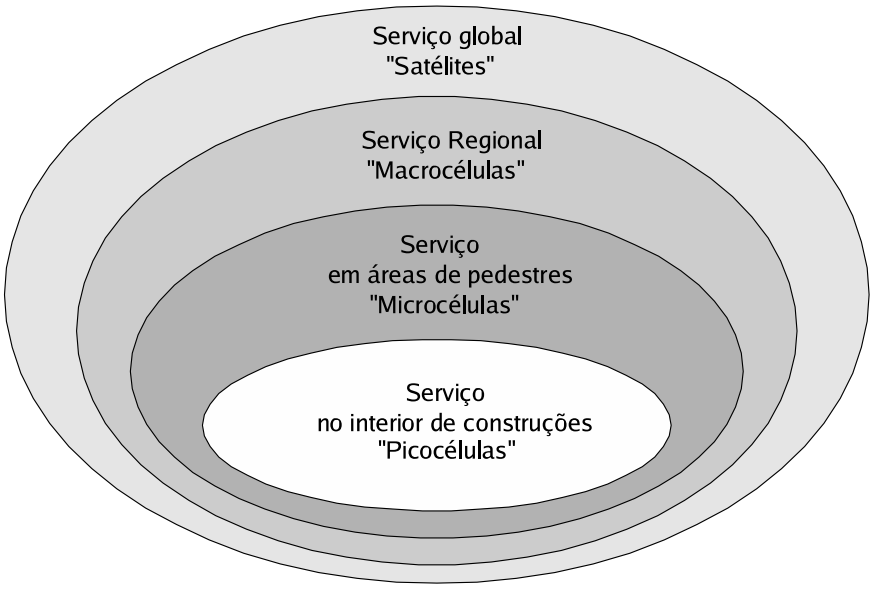

Figura 1.1: Hierarquia das áreas de serviços, conforme IMT-2000.

Nos últimos anos, os sistemas de comunicação móvel estão exigindo elevadas taxas de dados e também taxa de dados variáveis para integrar serviços variados como o de voz, de comunicação de dados e de multimídia. Disponibilizar tais serviços exige um sistema de elevada capacidade. Para utilizar o espectro disponível de forma eficiente, o sistema deve maximizar a taxa de dados (ou a capacidade, ou ainda o desempenho). Assim, importantes critérios utilizados na avaliação de sistemas de comunicação móvel são a probabilidade de erro na comunicação e a eficiência espectral, ou seja, a

capacidade do sistema para uma determinada largura de banda.

A técnica de multiplexação por divisão de código (*code-division multiple access*, CDMA) por seqüência direta (*direct sequence CDMA*, DS/CDMA) permite que um número de usuários utilize simultaneamente um mesmo canal de comunicação, modulando seus sinais por diferentes seqüências, ou códigos de espalhamento. No receptor, o sinal original de um dado usuário é recuperado correlacionando-se o sinal recebido com a correspondente seqüência de espalhamento (SIMON et al., 1994).

O sinal transmitido em um canal de rádio móvel terrestre é propagado do transmissor para o receptor através de diversos caminhos devido aos fenômenos de refração e reflexão em diferentes meios e obstáculos (STUBER, 2001), como mostra a figura 1.2. Tal fenomeno é chamado de propagação multipercurso. A propagação multipercurso fará com que, no canal reverso de um sistema de telefonia móvel celular DS/CDMA, réplicas dos sinais transmitidos pelos usuários ativos cheguem com diferentes atrasos no receptor da estação rádio base (ERB). Os sinais dos usuários não demodulados e suas réplicas podem provocar a interferência de múltiplo acesso (*multiple access interference*, MAI) e as réplicas do sinal do usuário de interesse podem provocar a auto-interferência (*self-interference*, SI). A MAI e a SI são resultados dos atrasos aleatórios entre os sinais dos usuários ativos e suas réplicas, os quais tornam impossível a manutenção da ortogonalidade entre todas as formas de onda de códigos de espalhamento. A MAI torna-se substancial quando o número de usuários cresce e/ou quando as disparidades de potência entre usuários ativos tornam-se significativas (efeito *near-far*) (PICKHOLTZ; MILSTEIN; SCHILLING, 1991).

O desempenho dos sistemas CDMA é limitado principalmente pela MAI e pela SI, as quais podem ser controladas através da escolha adequada de seqüências de espalhamento com boas propriedades de correlação. Adicionalmente, a MAI pode ter seu efeito minimizado através do controle de potência de todos os sinais recebidos dos usuários ativos no sistema, de forma a manter as potências recebidas as mais próximas possíveis.

Se todos os usuários transmitirem sincronizadamente, ou quase, pode-se obter a condição dos sinais de todos os usuários estarem chegando ao receptor da ERB com diferenças de atrasos confinadas em um intervalo de tempo definido, dependendo das características do canal de comunicação. Esse sistema, chamado de DS/CDMA quase síncrono (ou *quasi-synchronous DS/CDMA*, QS-CDMA), tem a capacidade de mini-

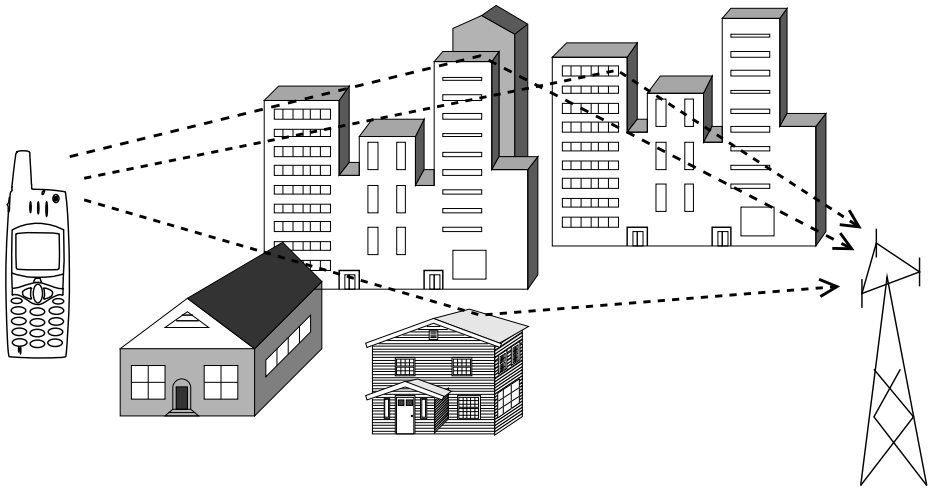

Figura 1.2: Propagação multipercurso.

mizar drasticamente a MAI e a SI através da utilização de conjuntos de seqüências com boas propriedades de correlação (MASSEY; MITTELHOLZER, 1991) (GAUDENZI; ELIA; VIOLA, 1992).

Assim, em um sistema QS-CDMA, a característica de quase ortogonalidade entre as seqüências de espalhamento designadas para os usuários ativos é explorada de forma a minimizar a interferência maximizando a capacidade do sistema.

O estudo de conjuntos de seqüências de espalhamento para sistemas CDMA é justificável, pois suas propriedades de correlação e características, como comprimento e número de seqüências disponíveis, definem limites de eficiência espectral e de desempenho e, portanto, limites de capacidade do sistema os quais podem ser otimizados com a alteração do conjunto de seqüências utilizado.

Como indicado na figura 1.1, os satélites de comunicação podem prover serviços sobre uma vasta área para usuários móveis ou fixos. A ESA (*European Space Agency*) propôs, para um sistema de comunicação terrestre via satélite anterior ao de 3G, sincronizar o canal reverso para que os sinais de todos os usuários cheguem alinhados no satélite (MASSEY; MITTELHOLZER, 1991). O sincronismo no canal reverso proposto em (GAUDENZI; ELIA; VIOLA, 1992) consiste em transmitir um *clock* de referência juntamente com a estrutura do sinal CDMA, através de um código dedicado (chamado *master code*), modulado por uma freqüência de referência precisa. A estrutura desse sinal, chamado de sinal mestre (*master signal*), é similar a outros sinais que acessam a rede. Durante o estabelecimento do sincronismo, cada usuário transmite seu sinal

sincronizadamente com o *master signal*. O sinal recebido pelo satélite é retransmitido ao usuário imediatamente (sinal *echo*). A partir da diferença de tempo entre o momento em que o sinal foi enviado pelo usuário e a recepção do *echo*, estima-se e compensa-se o atraso de propagação. Uma vez estabelecido o sincronismo, continua-se o processamento para compensar variações do atraso de propagação. Essa técnica de sincronismo é chamada de malha fechada local, pois cada unidade móvel possui sua própria malha de sincronismo. Dessa forma, o *jitter* temporal nesse sistema é restrito a poucas dezenas ou mesmo unidades de chip. Em casos práticos, esse pode ser mantido abaixo de $0,3$ chips para uma taxa de chip de $1Mchip/s$ (GAUDENZI; ELIA; VIOLA, 1992). Monitorando-se a potência do *master signal* também pode-se implementar um controle de potência de malha aberta, reduzindo assim o efeito *near-far*[1].

Assim como em muitos casos práticos, o reuso de freqüência é aplicado nesse sistema para aumentar a capacidade e o conjunto de códigos utilizáveis. Nesse caso, é necessário um mínimo isolamento entre feixes adjacentes. Em um satélite multi-feixes, pode-se designar diferentes famílias de códigos para diferentes feixes. Dessa forma, a interferência causada por um feixe adjacente reutilizando a mesma freqüência de portadora é atenuada pela isolação entre os feixes e também pelas boas propriedades de correlação entre seqüências de famílias distintas (GAUDENZI; ELIA; VIOLA, 1992).

No sistema celular de telefonia móvel terrestre, pode-se obter o sincronismo no canal reverso utilizando também um *master signal* que contenha a informação do *clock* de referência, figura 1.3. Assim como no sistema via satélite, os usuários recebem o *master signal* de referência, com o qual transmitem de forma sincronizada. Em uma microcélula, as distâncias envolvidas são pequenas ($100m$ a $1000m$) e, portanto, a ERB receberá os sinais de todos os usuários com pequenas diferenças de atraso de propagação (muito menores que um período de símbolo), mesmo quando há um usuário na borda da célula e outro muito próximos à ERB. Por exemplo (KAJIWARA; NAKAGAWA, 1994), assumindo-se um sistema microcelular CDMA de 2G com taxa de bit de $9,6kbps$ (modulação BPSK) e uma taxa de chip de $9,6 \times 10^3 \times 127 \approx 1,2Mchips/s$ (seqüência de espalhamento com comprimento de $127chips$), o atraso de propagação corresponde a $2 \sim 8chips$ para células de $300 \sim 1000m$ de raio, respectivamente.

Outra aplicação em telefonia móvel, a qual os usuários tentam transmitir sincroni-

[1] Esse efeito ocorre no canal reverso (da estação móvel para a ERB) quando sinais de estações móveis são "sufocados" por sinais fortes provenientes de estações móveis mais próximas à ERB.

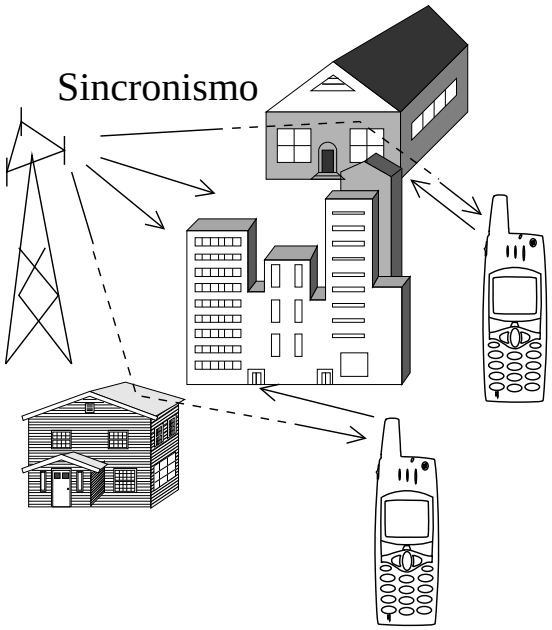

Figura 1.3: Aplicação do QS-CDMA em telefonia móvel.

zadamente, utiliza o *clock* derivado do sistema local de posicionamento global (*Global Positioning System*, GPS). Os receptores móveis equipados com receptores GPS, permitem à ERB receber os sinais dos vários usuários com atrasos relativos mantidos em uma fração de período de símbolo (ILTIS, 1996) (ILTIS; MAILAENDER, 1996). Em (ILTIS; MAILAENDER, 1996), duas abordagens são consideradas: a) o usuário desconhece a distância da ERB; b) a distância da ERB é conhecida pelo usuário. Definindo o período de chip como T_c, o raio da célula como r_{cel}, e um erro temporal máximo no clock do GPS por T_{GPS}. Para o caso a), a diferença temporal entre um usuário localizado a uma distância $d = 0$ e outro usuário no perímetro da célula, com $d = r_{cel}$, é $\pm\frac{r_{cel}}{2c_{light}}$, onde $c_{light} = 3\times10^8 m/s$ representa a velocidade da luz no vácuo. Considerando o pior caso de alinhamento de *clock*, o erro temporal total dado em períodos de chip é:

$$\Delta = \pm\frac{1}{T_c}\left(\frac{r_{cel}}{2c_{light}} + 2T_{GPS}\right) \tag{1.1}$$

Esse erro pode ser reduzido se for assumido que o usuário possa estimar o atraso de percurso para a ERB (caso b). Utilizando o serviço de estimação de posição do GPS, o usuário pode estimar o atraso de percurso e compensá-lo. Nesse caso, define-se P_{GPS} como o erro na estimativa de posicionameto do GPS, o que significa que qualquer usuário conhece sua posição com erro de $\pm P_{GPS}$ metros. O erro temporal resultante

para a ERB passa a ser $\pm\frac{P_{GPS}}{c_{light}}$. Novamente, para o pior caso de alinhamento de *clock*, o erro temporal dado em períodos de chip é:

$$\Delta = \pm\frac{1}{T_c}\left(\frac{P_{GPS}}{c_{light}} + 2T_{GPS}\right) \tag{1.2}$$

Considerando $T_c = 8,14\times10^{-7}s$, o que corresponde a uma taxa de chip do sistema 2G de $1,2MHz$, $T_{GPS} = \pm0,5\times10^{-6}s$, $P_{GPS} = 15m$, e $r_{cel} = 2km$ (macrocélula), obtém-se um erro temporal, conforme o caso a), de $\Delta = \pm5,3$ chips, e $\Delta = \pm1,3$ chips, conforme o caso b) (ILTIS; MAILAENDER, 1996).

A técnica de multiplexação CDMA também pode ser utilizada em redes de pacotes, permitindo que usuários transmitam simultaneamente. Tal situação foi discutida em (SAITO et al., 1998) utilizando o protocolo ALOHA. O protocolo ALOHA foi proposto pela Universidade do Hawaii em 1970, para permitir a comunicação entre o Centro de Computação da Universidade do Havaí e seus terminais, distantes geograficamente. A principal característica desse protocolo é que cada terminal, assim que receber a mensagem da fonte, transmite-a imediatamente. Se houver colisão com a transmissão de um outro terminal, cada terminal envolvido na colisão retransmitirá sua mensagem em tempos aleatórios na tentativa de se evitar novas colisões. O terminal detecta se obteve ou não sucesso em sua transmissão através de uma informação da Central por um outro canal auxiliar (LIMA, 1996). Uma modificação do ALOHA é conhecida como *slotted* ALOHA. Nesse protocolo, as mensagens são enviadas em um *slot* de tempo entre dois pulsos de sincronismo, sendo que a transmissão iniciará somente no começo de um *slot* de tempo. Dessa forma, a taxa de colisões pode ser reduzida para a metade (HARADA; PRASAD, 2002). Para transmitir o pacote com sucesso, deve-se garantir apenas um pacote no *slot* de tempo, como mostra a figura 1.4. Se dois ou mais pacotes são gerados no mesmo *slot* de tempo, ocorrerá colisão.

Multiplexando os terminais com a técnica CDMA (CDMA ALOHA), o sistema será capaz de transmitir pacotes simultaneamente. Uma vez que no *sloted* ALOHA os terminais estão sincronizados, o sistema QS-CDMA é perfeitamente aplicável para minimizar a interferência MAI e com isso, aumentar o desempenho (SAITO et al., 1998).

Existem outras aplicações para o sistema QS-CDMA, incluindo um sistema de telefonia móvel celular de quarta geração (4G) proposto recentemente. Esse sistema, chamado de LAS-CDMA, é brevemente discutido no apêndice D.

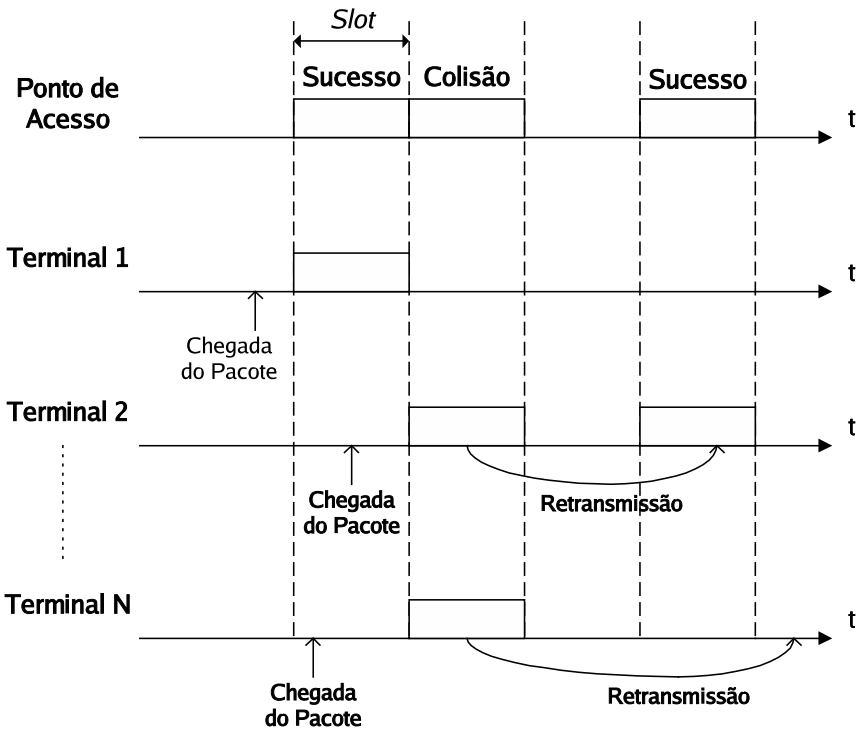

Figura 1.4: *Slotted* ALOHA.

Neste trabalho, são apresentados alguns métodos propostos de obtenção de famílias de seqüências adequadas para a função de espalhamento em sistemas QS-CDMA. As famílias estudadas aqui são: QS, OQS, Lin-Chang, LCZ-GMW binária, LCZ-GMW polifásica, ZCZ binária, ZCZ quadrifásica, PS, SP e LAS. Para estudar os métodos de obtenção de algumas dessas famílias, é necessário compreender também os métodos de construção e as características das seqüências de máximo comprimento (SMC) e seqüências GMW e da família Gold. A família de seqüências No complementa o estudo, pois essa representa a generalização de SMC e seqüências GMW, da família Gold e da família pequena de Kasami.

Dentre as famílias de seqüências analisadas neste trabalho, especial atenção é dada às famílias de seqüências binárias: QS, OQS, Lin-Chang, LCZ-GMW binária e ZCZ binária. Para estas, são apresentadas figuras de desempenho, em termos de taxa de erro de bit, de um sistema de comunicação móvel QS-CDMA. Para essa análise de desempenho, foi considerada recepção convencional e canal Rayleigh multipercurso.

Conforme já mencionado, os sistemas de comunicação móvel estão exigindo taxa de dados variável para integrar serviços variados. Entretanto, existem poucos trabalhos

sobre seqüências adequadas a sistemas QS-CDMA de taxa de dados variável (multitaxa). Neste trabalho, é proposta uma metodologia para seleção de seqüências adequadas a sistemas QS-CDMA multitaxa do tipo múltiplos ganhos de processamento (*multi-processing gain*, MPG). A família de seqüências obtida com esse método é avaliada comparativamente com a família de seqüências OVSF, a qual é composta de seqüências Walsh-Hadamard, por meio de figuras de desempenho de um sistema QS-CDMA multitaxa.

A seguir, a seção 1.1 apresenta o modelo do sistema adotado para auxiliar o estudo das famílias de seqüências. A seção 1.1.1 apresenta os critérios de seleção de seqüências para sistemas QS-CDMA, baseados no modelo de sistema adotado anteriormente. Alguns limites teóricos para as funções de correlação de seqüências são discutidos na seção 1.2. O estudo das metodologias de obtenção de famílias de seqüências binárias encontra-se no capítulo 2, juntamente com uma comparação de suas características e desempenhos proporcionados quando aplicadas em um sistema QS-CDMA de taxa única de dados. O capítulo 3 traz uma breve discussão sobre sistemas CDMA multitaxa, além de figuras de desempenho de sistema QS-CDMA multitaxa do tipo múltiplos códigos (*multi-code*, MC) utilizando algumas famílias de seqüências previamente estudadas. Ainda nesse capítulo é proposto um método de seleção de seqüências para sistemas QS-CDMA MPG. Por fim, o capítulo 4 apresenta as conclusões deste trabalho, bem como propostas de trabalhos futuros. Os apêndices C, E e D complementam o estudo com famílias de seqüências polifásicas, sistemas QS-CDMA com detecção multiusuário do tipo cancelamento de interferência paralelo e o sistema LAS-CDMA e as seqüências ternárias, respectivamente.

Neste trabalho, algumas demonstrações foram incluídas, e detalhadas, apesar de poderem ser encontradas na literatura aberta. A motivação para esse procedimento foi a de buscar a completeza do texto e, adicionalmente, pelo fato de várias delas estarem disponíveis em uma forma muito compacta e dispersa.

1.1 Modelagem do sistema QS-CDMA

As seqüências de espalhamento são definidas como:

$$\mathbf{c}_i = \{c_{i,0}\, c_{i,1} \ldots c_{i,N-1}\} \tag{1.3}$$

onde i representa a i-ésima seqüência do conjunto; N o comprimento da seqüência de espalhamento; e $c_{i,j}$ é o chip j da i-ésima seqüência, tal que $\sum_{j=0}^{N-1} |c_{i,j}| = N$.

A razão entre o período do símbolo de informação T e o período de chip T_c é chamada de ganho de processamento $G = \frac{T}{T_c}$. Neste trabalho, todos os chips de uma seqüência espalham cada um dos símbolos de informação, logo $G = N$.

O carregamento do sistema $Load = \frac{U}{N}$ relaciona o número de usuários ativos U no sistema com o comprimento N das seqüências utilizadas.

Em um sistema QS-CDMA, o sinal transmitido pelo k-ésimo usuário pode ser dado por:

$$s_k(t) = \sqrt{2P} b_k(t) c_k(t) cos(\omega_c t) \tag{1.4}$$

onde P é a potência do sinal transmitido, a qual será considerada igual para todos os usuários; $b_k(t)$ é um sinal BPSK (*binary phase shift keying*) representando a informação e $c_k(t)$ o sinal relativo à seqüência de espalhamento dado por:

$$c_k(t) = \sum_{m=-\infty}^{\infty} p(t - mT_c) \underline{c}_{k,m} \tag{1.5}$$

onde $\underline{c}_{k,m} = c_{k,m(\text{mod } N)}$ é o m-ésimo chip da seqüência de espalhamento de comprimento N utilizada pelo k-ésimo usuário; $p(t)$ é a formatação de pulso retangular de amplitude unitária no intervalo $[0; T_c)$ e zero fora.

O sinal recebido na estação rádio base, figura 1.5, será:

$$r(t) = \sum_{u=1}^{U} \sum_{\mathcal{L}=1}^{L} \alpha_{\mathcal{L}}(t) s_u(t - \tau_{u,\mathcal{L}}) + n(t) \tag{1.6}$$

onde U é o número de usuários ativos no sistema; $\alpha_{\mathcal{L}}(t)$ representa o ganho do canal para o componente multipercurso $\mathcal{L}$; $\tau_{u,\mathcal{L}}$ é o atraso absoluto do $\mathcal{L}$-ésimo componente multipercurso do u-ésimo usuário e $n(t)$ é o ruído aditivo branco Gaussiano (*additive white Gaussian noise,* AWGN).

A saída do ℓ-ésimo correlacionador do k-ésimo usuário, analisada apenas em um símbolo de informação (sem perda de generalidade considera-se o intervalo $0 \leq t < T$, onde $T = NT_c$ é o período de símbolo e $\tau_{k,\ell} = 0$) será:

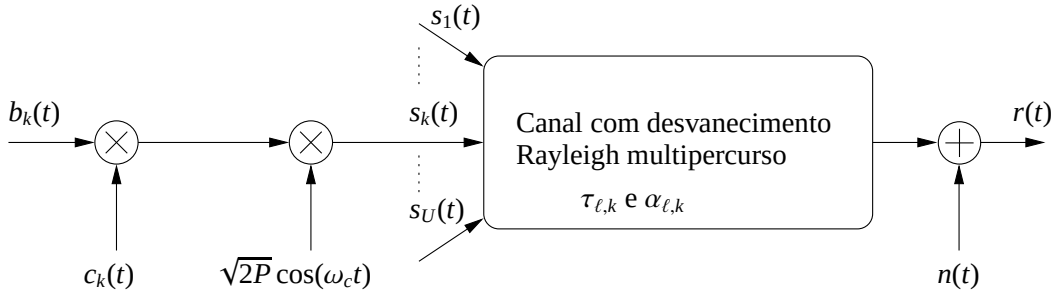

Figura 1.5: Sinal transmitido, canal e sinal recebido.

$$\begin{aligned} z_{k,\ell} &= \int_0^T r(t)c_k^*(t)cos(\omega_c t - \phi_{k,\ell})dt \\ &= \sqrt{2P}\int_0^T \alpha_\ell(t)b_k(t)c_k(t)c_k^*(t)cos^2(\omega_c t - \phi_{k,\ell})dt + I_{k,\ell} + S\,I_{k,\ell} + n_{k,\ell}(t) \end{aligned} \tag{1.7}$$

onde o primeiro termo representa o sinal de interesse, o segundo a MAI, o terceiro a SI e o último o AWGN processado; $\phi_{k,\ell} = \omega_c \tau_{k,\ell}$ é o deslocamento de fase devido ao atraso $\tau_{k,\ell}$. Foram consideradas as estimativas perfeitas de atraso $\hat{\tau}_{k,\ell}$ e fase $\hat{\phi}_{k,\ell}$ no receptor, logo $\hat{\tau}_{k,\ell} = \tau_{k,\ell}$ e $\hat{\phi}_{k,\ell} = \phi_{k,\ell}$. Será considerado que o ganho de canal $\alpha_\ell(t)$ é constante no intervalo de integração T (ou período do símbolo de informação). Logo, $\alpha_\ell(t) = \alpha_\ell$. Rearranjando a equação anterior, tem-se:

$$z_{k,\ell} = \sqrt{\frac{P}{2}}\alpha_\ell T b_k^{(0)} + I_{k,\ell} + S\,I_{k,\ell} + n_{k,\ell}(t) \tag{1.8}$$

onde $b_k^{(0)} \in \{-1; 1\}$ é a informação de interesse.

Considerando recepção Rake com D correlacionadores (*fingers*), figura 1.6, e combinador de razão máxima (*maximum ratio combiner*, MRC), figura 1.7, tem-se:

$$\begin{aligned} y_k &= \sum_{\ell=1}^{D} \Re\{z_{k,\ell}\hat{\alpha}_\ell\} \\ \hat{b}_k^{(0)} &= \text{sign}(y_k) \end{aligned} \tag{1.9}$$

onde $\hat{\alpha}_\ell$ é a estimativa do ganho de canal, a qual foi considerada perfeita, e $\hat{b}_k^{(0)}$ é a informação de interesse estimada.

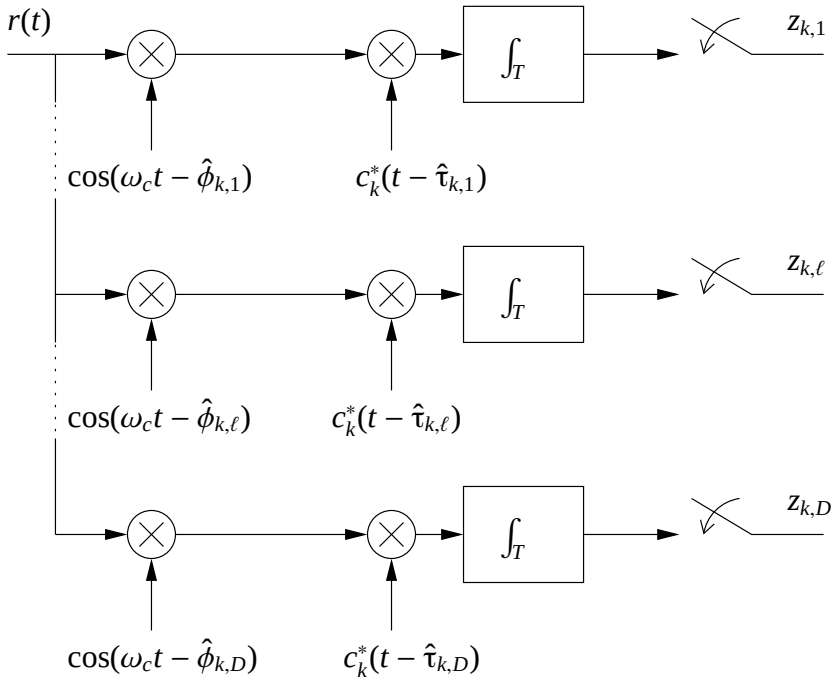

Figura 1.6: Receptor Rake.

A MAI sobre o ℓ-ésimo correlacionador do k-ésimo usuário será:

$$
\begin{aligned}
I_{k,\ell} &= \sum_{(u=1,\ u\neq k)}^{U} \sum_{\mathcal{L}=1}^{L} \sqrt{2P} \cdot \\
&\cdot \int_0^T \alpha_{\mathcal{L}}(t) b_u(t-\tau_{u,\mathcal{L}}) c_u(t-\tau_{u,\mathcal{L}}) c_k^*(t) cos(\omega_c t - \phi_{u,\mathcal{L}}) cos(\omega_c t - \phi_{k,\ell}) dt \\
&= \sum_{(u=1,\ u\neq k)}^{U} \sum_{\mathcal{L}=1}^{L} \sqrt{2P}\alpha_{\mathcal{L}} \cdot \\
&\cdot \int_0^T b_u(t-\tau_{u,\mathcal{L}}) c_u(t-\tau_{u,\mathcal{L}}) c_k^*(t) \frac{1}{2} \left(cos(\varphi_{u,\mathcal{L}}) + cos(2\omega_c t - (\phi_{u,\mathcal{L}} - \phi_{k,\ell}))\right) dt \\
&= \sum_{(u=1,\ u\neq k)}^{U} \sum_{\mathcal{L}=1}^{L} \sqrt{\frac{P}{2}} \alpha_{\mathcal{L}} \int_0^T b_u(t-\tau_{u,\mathcal{L}}) c_u(t-\tau_{u,\mathcal{L}}) c_k^*(t) dt\ cos(\varphi_{u,\mathcal{L}})
\end{aligned}
\tag{1.10}
$$

onde $\tau_{u,\mathcal{L}} = \tau_{u,\mathcal{L}} - \tau_{k,\ell}$ é o atraso relativo entre o sinal de interesse (sinal do ℓ-ésimo componente multipercurso do k-ésimo usuário) e o sinal interferente (sinal do $\mathcal{L}$-ésimo componente multipercurso do u-ésimo usuário); $\varphi_{u,\mathcal{L}} = \phi_{u,\mathcal{L}} - \phi_{k,\ell}$ é a fase relativa entre as portadoras do sinal de interesse e do sinal interferente. Os termos que correspondem ao atraso relativo e à fase relativa não possuem os índices do sinal de interesse para

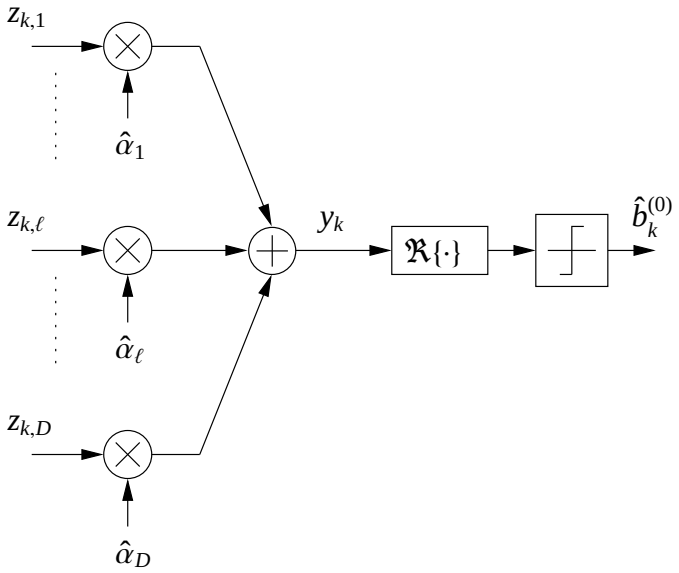

Figura 1.7: Combinador MRC.

simplificar a notação.

Será considerada a fase relativa $\varphi_{u,\mathcal{L}}$ com função densidade de probabilidade (*probability density function, pdf*) uniforme definida no intervalo $[0; 2\pi)$ e o atraso relativo $\tau_{u,\mathcal{L}}$ com *pdf* uniforme definida no intervalo $[-\tau_{\max} + \gamma_{\mathcal{L}}; \tau_{\max} + \gamma_{\mathcal{L}}]$, onde $\gamma_{\mathcal{L}} = \Delta_{\mathcal{L}} - \Delta_\ell$ e $\tau_{\max}$ é o erro máximo de sincronismo, dado pela maior diferença entre os atrasos dos $\mathcal{L}$-ésimos componentes multipercurso de dois usuários. As variáveis Δ_ℓ assumem apenas valores positivos e múltiplos de T_c e representam os atrasos dos componentes multipercurso dado um perfil atraso-potência determinístico, figura 1.8. Observe que $\gamma_{\mathcal{L}}$ também não possui o índice do componente multipercurso de interesse para simplificar a notação. Considera-se também, os símbolos de informação $b = -1$ e $b = 1$ equiprováveis.

Analogamente à MAI, a SI sobre o ℓ-ésimo correlacionador do k-ésimo usuário será:

$$SI_{k,\ell} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \sqrt{\frac{P}{2}}\alpha_{\mathcal{L}} \int_0^T b_k(t-\tau_{k,\mathcal{L}})c_k(t-\tau_{k,\mathcal{L}})c_k^*(t)dt\ cos(\varphi_{k,\mathcal{L}}) \tag{1.11}$$

O AWGN processado para o ℓ-ésimo correlacionador do k-ésimo usuário é dado por:

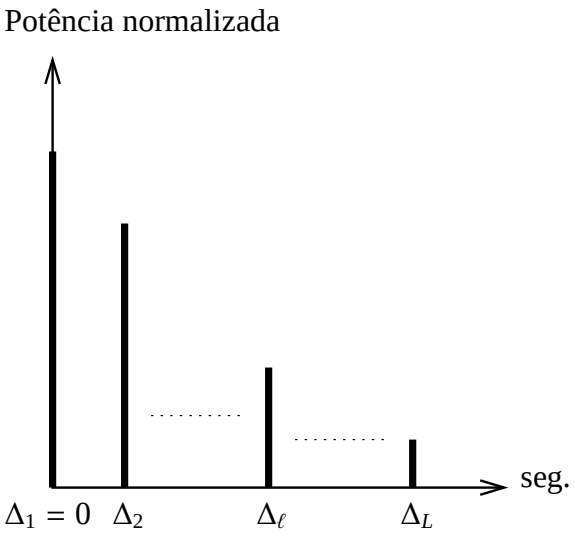

Figura 1.8: Perfil atraso-potência determinístico.

$$\begin{aligned} n_{k,\ell}(t) &= \int_0^T n(t)c_k^*(t)cos(\omega_c t - \phi_{k,\ell})dt \\ &= \sum_{m=0}^{N-1} \underline{c}_{k,m}^* \int_{mT_c}^{(m+1)T_c} n(t)cos(\omega_c t - \phi_{k,\ell})dt \end{aligned} \tag{1.12}$$

Será calculada a relação sinal-ruído-interferência (*signal-to-noise plus interference ratio*, SNIR) na saída do ℓ-ésimo correlacionador do k-ésimo usuário:

$$SNIR_{k,\ell} = \frac{\text{potência do sinal de interesse}}{\text{potência da MAI, da SI e do AWGN processado}} \tag{1.13}$$

onde a potência do sinal de interesse será:

$$\mathbb{E}_\alpha \left\{ \left(\sqrt{\frac{P}{2}} \alpha_\ell T b_k^{(0)} \right)^2 \right\} = \frac{P}{2} T^2 \mathbb{E}_\alpha \{\alpha_\ell^2\} \tag{1.14}$$

A potência do AWGN processado será:

$$\mathbb{E}\left\{(n_{k,\ell}(t))^2\right\} = \mathbb{E}\left\{ \left(\sum_{m=0}^{N-1} \underline{c}_{k,m}^* \int_{mT_c}^{(m+1)T_c} n(t)cos(\omega_c t)dt \right)^2 \right\}$$

$$
\begin{aligned}
&= \mathbb{E}\left\{\sum_{m=0}^{N-1}\left(|\underline{c}_{k,m}|^2\int_{mT_c}^{(m+1)T_c}\int_{mT_c}^{(m+1)T_c} n(t)n(u)cos(\omega_c t)cos(\omega_c u)\,dt\,du+\right.\right.\\
&\quad\left.\left.+\sum_{p=0}^{N-1}\underline{c}^*_{k,m}\underline{c}^*_{k,p}\int_{mT_c}^{(m+1)T_c}\int_{pT_c}^{(p+1)T_c} n(t)n(u)cos(\omega_c t)cos(\omega_c u)\,dt\,du\right)\right\}\\
&= \sum_{m=0}^{N-1}\left(\int_{mT_c}^{(m+1)T_c}\int_{mT_c}^{(m+1)T_c}\frac{N_0}{2}\delta(t-u)cos(\omega_c t)cos(\omega_c u)\,dt\,du\right)\\
&= \sum_{m=0}^{N-1}\frac{N_0\,T_c}{4}\\
&= \frac{N_0\,T}{4} \qquad (1.15)
\end{aligned}
$$

Como φ, b, τ e α são variáveis aleatórias independentes, a potência da MAI e da SI sobre o ℓ-ésimo correlacionador do k-ésimo usuário serão:

$$
\begin{aligned}
\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,\ell})^2\right\} &= \mathbb{E}_\alpha\left\{\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{\mathbb{E}_\varphi\left\{(I_{k,\ell})^2\right\}\right\}\right\}\right\}\\
\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(S\,I_{k,\ell})^2\right\} &= \mathbb{E}_\alpha\left\{\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{\mathbb{E}_\varphi\left\{(S\,I_{k,\ell})^2\right\}\right\}\right\}\right\} \qquad (1.16)
\end{aligned}
$$

Inicialmente, será calculada a potência da MAI, a qual pode ser reescrita como:

$$
I_{k,\ell} = \sum_{(u=1,\ u\neq k)}^{U}\sum_{\mathcal{L}=1}^{L}\sqrt{\frac{P}{2}}\alpha_{\mathcal{L}}J_{u,\mathcal{L}}\,cos(\varphi_{u,\mathcal{L}}) \qquad (1.17)
$$

onde $J_{u,\mathcal{L}} = \int_0^T b_u(t-\tau_{u,\mathcal{L}})c_u(t-\tau_{u,\mathcal{L}})c_k^*(t)dt$. Realizando a média na variável $\varphi_{u,\mathcal{L}}$:

$$
\begin{aligned}
\mathbb{E}_\varphi\left\{(I_{k,\ell})^2\right\} &= \sum_{(u=1,\ u\neq k)}^{U}\sum_{\mathcal{L}=1}^{L}\frac{P}{2}\alpha^2_{\mathcal{L}}J^2_{u,\mathcal{L}}\int_0^{2\pi}cos^2(\varphi_{u,\mathcal{L}})\frac{1}{2\pi}\,d\varphi_{u,\mathcal{L}}\\
&= \sum_{(u=1,\ u\neq k)}^{U}\sum_{\mathcal{L}=1}^{L}\frac{P}{4}\alpha^2_{\mathcal{L}}J^2_{u,\mathcal{L}} \qquad (1.18)
\end{aligned}
$$

Realizando a média na variável b_u:

$$
\mathbb{E}_b\left\{\mathbb{E}_\varphi\left\{(I_{k,\ell})^2\right\}\right\} = \sum_{(u=1,\ u\neq k)}^{U}\sum_{\mathcal{L}=1}^{L}\frac{P}{4}\alpha^2_{\mathcal{L}}\mathbb{E}_b\left\{J^2_{u,\mathcal{L}}\right\} \qquad (1.19)
$$

Reescrevendo $J_{u,\mathcal{L}}$:

$$\begin{aligned} J_{u,\mathcal{L}} &= \int_0^T b_u(t-\tau_{u,\mathcal{L}})c_u(t-\tau_{u,\mathcal{L}})c_k^*(t)dt \\ &= \begin{cases} \left(b_u^{(-1)}\mathcal{R}_{u,k}(\tau_{u,\mathcal{L}}) + b_u^{(0)}\tilde{\mathcal{R}}_{u,k}(\tau_{u,\mathcal{L}})\right) & \text{, para } \tau_{u,\mathcal{L}} \geq 0 \\ \left(b_u^{(0)}\mathcal{R}_{u,k}(\tau_{u,\mathcal{L}}) + b_u^{(1)}\tilde{\mathcal{R}}_{u,k}(\tau_{u,\mathcal{L}})\right) & \text{, para } \tau_{u,\mathcal{L}} < 0 \end{cases} \end{aligned} \tag{1.20}$$

onde $b_u^{(-1)}$, $b_u^{(0)}$ e $b_u^{(1)}$ são as informações do usuário interferente que participam da integração e as funções $\mathcal{R}_{u,k}(\tau_{u,\mathcal{L}})$ e $\tilde{\mathcal{R}}_{u,k}(\tau_{u,\mathcal{L}})$ são chamadas de funções de correlação cruzada parcial par e ímpar, respectivamente, definidas como:

$$\begin{aligned} \mathcal{R}_{u,k}(\tau) &= \int_0^{\underline{\tau}} c_u(t-\underline{\tau})c_k^*(t)\,dt \\ \tilde{\mathcal{R}}_{u,k}(\tau) &= \int_{\underline{\tau}}^T c_u(t-\underline{\tau})c_k^*(t)\,dt, \text{ com } \underline{\tau} = \tau \text{ para } \tau \geq 0 \text{ e } \underline{\tau} = T+\tau \text{ para } \tau < 0 \end{aligned} \tag{1.21}$$

Observa-se que, para $\tau < 0$, $\mathcal{R}_{u,k}(\tau)$ e $\tilde{\mathcal{R}}_{u,k}(\tau)$ são equivalentes a $\mathcal{R}_{u,k}(T+\tau)$ e $\tilde{\mathcal{R}}_{u,k}(T+\tau)$, respectivamente.

Assim, tem-se:

$$\begin{aligned} \mathbb{E}_b\left\{J_{u,\mathcal{L}}^2\right\} &= \begin{cases} \mathbb{E}_b\left\{\left(b_u^{(-1)}\mathcal{R}_{u,k}(\tau_{u,\mathcal{L}}) + b_u^{(0)}\tilde{\mathcal{R}}_{u,k}(\tau_{u,\mathcal{L}})\right)^2\right\}, & \tau_{u,\mathcal{L}} \geq 0 \\ \mathbb{E}_b\left\{\left(b_u^{(0)}\mathcal{R}_{u,k}(\tau_{u,\mathcal{L}}) + b_u^{(1)}\tilde{\mathcal{R}}_{u,k}(\tau_{u,\mathcal{L}})\right)^2\right\}, & \tau_{u,\mathcal{L}} < 0 \end{cases} \\ &= \frac{1}{2}\left\{\left(\mathcal{R}_{u,k}(\tau_{u,\mathcal{L}}) + \tilde{\mathcal{R}}_{u,k}(\tau_{u,\mathcal{L}})\right)^2 + \right. \\ &+ \left.\left(\mathcal{R}_{u,k}(\tau_{u,\mathcal{L}}) - \tilde{\mathcal{R}}_{u,k}(\tau_{u,\mathcal{L}})\right)^2\right\} \\ &= \left\{\left(\mathcal{R}_{u,k}(\tau_{u,\mathcal{L}})\right)^2 + \left(\tilde{\mathcal{R}}_{u,k}(\tau_{u,\mathcal{L}})\right)^2\right\} \end{aligned} \tag{1.22}$$

O próximo passo é realizar a média na variável $\tau_{u,\mathcal{L}}$:

$$\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{\mathbb{E}_\varphi\left\{(I_{k,\ell})^2\right\}\right\}\right\} = \sum_{(u=1,\ u\neq k)}^{U}\sum_{\mathcal{L}=1}^{L}\frac{P}{4}\alpha_{\mathcal{L}}^2\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{J_{u,\mathcal{L}}^2\right\}\right\} \tag{1.23}$$

onde:

$$\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{J^2_{u,\mathcal{L}}\right\}\right\} = \frac{1}{2\tau_{\max}}\int_{-\tau_{\max}+\gamma_\mathcal{L}}^{\tau_{\max}+\gamma_\mathcal{L}}\left[\left(\mathcal{R}_{u,k}(\tau_{u,\mathcal{L}})\right)^2+\left(\tilde{\mathcal{R}}_{u,k}(\tau_{u,\mathcal{L}})\right)^2\right]d\tau_{u,\mathcal{L}} \tag{1.24}$$

Fazendo $-\tau_{\max}+\gamma_\mathcal{L}$ e $\tau_{\max}+\gamma_\mathcal{L}$ múltiplos de T_c, tem-se $\frac{-\tau_{\max}+\gamma_\mathcal{L}}{T_c}=\upsilon_1$ e $\frac{\tau_{\max}+\gamma_\mathcal{L}}{T_c}=\upsilon_2$ números inteiros. Como os sinais $c_u(t)$ são periódicos com período NT_c, tem-se que:

$$\begin{aligned}
\mathcal{R}_{u,k}(\upsilon_1 T_c) &\equiv \mathcal{R}_{u,k}((\upsilon_1 \bmod N)T_c)\\
\mathcal{R}_{u,k}(\upsilon_2 T_c) &\equiv \mathcal{R}_{u,k}((\upsilon_2 \bmod N)T_c)\\
\tilde{\mathcal{R}}_{u,k}(\upsilon_1 T_c) &\equiv \tilde{\mathcal{R}}_{u,k}((\upsilon_1 \bmod N)T_c)\\
\tilde{\mathcal{R}}_{u,k}(\upsilon_2 T_c) &\equiv \tilde{\mathcal{R}}_{u,k}((\upsilon_2 \bmod N)T_c)
\end{aligned} \tag{1.25}$$

Assim, pode-se reescrever (1.24) como:

$$\begin{aligned}
\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{J^2_{u,j,\mathcal{L}}\right\}\right\} = \frac{1}{2\tau_{\max}}&\sum_{m=\upsilon_1}^{\upsilon_2-1}\cdot\\
&\cdot\int_{(m \bmod N)T_c}^{((m \bmod N)+1)\,T_c}\left[\left(\mathcal{R}_{u,k}(\tau_{u,\mathcal{L}})\right)^2+\left(\tilde{\mathcal{R}}_{u,k}(\tau_{u,\mathcal{L}})\right)^2\right]d\tau_{u,\mathcal{L}}
\end{aligned} \tag{1.26}$$

O desenvolvimento da integral da expressão acima é apresentado no apêndice A.1. Com esse resultado, tem-se:

$$\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{J^2_{u,j,\mathcal{L}}\right\}\right\} = \frac{1}{2\tau_{\max}}\sum_{m=\upsilon_1}^{\upsilon_2-1}\rho_{u,k}(m \bmod N) \tag{1.27}$$

onde:

$$\begin{aligned}
\rho_{u,k}(m) = \frac{T_c^3}{3}&\left(C_{u,k}(m-N+1)C_{u,k}(m-N)+C_{u,k}(m+1)C_{u,k}(m)+\right.\\
+\;&\left.C^2_{u,k}(m-N)+C^2_{u,k}(m)+C^2_{u,k}(m-N+1)+C^2_{u,k}(m+1)\right)
\end{aligned} \tag{1.28}$$

e

$$C_{u,k}(d) = \begin{cases} \sum_{v=0}^{N-d-1} c_{u,v} c_{k,v+d}^* & 0 \leq d \leq N-1 \\ \sum_{v=0}^{N+d-1} c_{u,v-d} c_{k,v}^* & 1-N \leq d < 0 \\ 0 & |d| \geq N \end{cases} \tag{1.29}$$

onde $\mathbf{c}_k = \{c_{k,1}, c_{k,2}, ..., c_{k,N}\}$ e $\mathbf{c}_u = \{c_{u,1}, c_{u,2}, ..., c_{u,N}\}$.

Finalmente, realiza-se a média na variável $\alpha_{\mathcal{L}}$:

$$\begin{aligned} \mathbb{E}_\alpha \left\{ \mathbb{E}_\tau \left\{ \mathbb{E}_b \left\{ \mathbb{E}_\varphi \left\{ (I_{k,i,\ell})^2 \right\} \right\} \right\} \right\} &= \sum_{(u=1,\ u\neq k)}^{U} \sum_{\mathcal{L}=1}^{L} \frac{P}{8\tau_{max}} \mathbb{E}_\alpha\{\alpha_{\mathcal{L}}^2\} \cdot \\ &\quad \cdot \sum_{m=\upsilon_1}^{\upsilon_2-1} \rho_{u,k}(m \bmod N) \end{aligned} \tag{1.30}$$

Portanto, a potência da MAI sobre o ℓ-ésimo correlacionador do k-ésimo usuário será:

$$\mathbb{E}_{\alpha,\varphi,b,\tau} \left\{ (I_{k,i,\ell})^2 \right\} = \sum_{(u=1,\ u\neq k)}^{U} \sum_{\mathcal{L}=1}^{L} \frac{P}{8\tau_{max}} \mathbb{E}_\alpha\{\alpha_{\mathcal{L}}^2(t)\} \sum_{m=\upsilon_1}^{\upsilon_2-1} \rho_{u,k}(m \bmod N) \tag{1.31}$$

Será calculada a potência da SI como em (1.16). Inicialmente, calcula-se $\mathbb{E}_\varphi \left\{ (S\,I_{k,\ell})^2 \right\}$, onde $S\,I_{k,\ell}$ é dado por (1.11):

$$\mathbb{E}_\varphi \left\{ (S\,I_{k,\ell})^2 \right\} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \frac{P}{4} \alpha_{\mathcal{L}}^2 J_{k,\mathcal{L}}^2 \tag{1.32}$$

onde $J_{k,\mathcal{L}}$ é dado por:

$$\begin{aligned} J_{k,\mathcal{L}} &= \int_0^T b_k(t-\tau_{k,\mathcal{L}}) c_k(t-\tau_{k,\mathcal{L}}) c_k(t)^* dt \\ &= \begin{cases} b_k^{(-1)} \mathcal{R}_{k,k}(\tau_{k,\mathcal{L}}) + b_k^{(0)} \tilde{\mathcal{R}}_{k,k}(\tau_{k,\mathcal{L}}), & \tau_{k,\mathcal{L}} \geq 0 \\ b_k^{(0)} \mathcal{R}_{k,k}(\tau_{k,\mathcal{L}}) + b_k^{(1)} \tilde{\mathcal{R}}_{k,k}(\tau_{k,\mathcal{L}}), & \tau_{k,\mathcal{L}} < 0 \end{cases} \end{aligned} \tag{1.33}$$

onde:

$$\begin{aligned}\mathcal{R}_{k,k}(\tau) &= \int_0^{\underline{\tau}} c_k(t-\underline{\tau})c_k^*(t)\,dt \\ \tilde{\mathcal{R}}_{k,k}(\tau) &= \int_{\underline{\tau}}^{T} c_k(t-\underline{\tau})c_k^*(t)\,dt, \text{ com } \underline{\tau} = \tau \text{ para } \tau \geq 0 \text{ e } \underline{\tau} = T+\tau \text{ para } \tau < 0\end{aligned} \tag{1.34}$$

são as funções de autocorrelação parciais par e ímpar, respectivamente. Observa-se que, para $\tau < 0$, $\mathcal{R}_{k,k}(\tau)$ e $\tilde{\mathcal{R}}_{k,k}(\tau)$ são equivalentes a $\mathcal{R}_{k,k}(T+\tau)$ e $\tilde{\mathcal{R}}_{k,k}(T+\tau)$, respectivamente.

Realizando a média para o símbolo de informação b_k:

$$\mathbb{E}_b\left\{\mathbb{E}_\varphi\left\{(S\,I_{k,\ell})^2\right\}\right\} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \frac{P}{4}\alpha_{\mathcal{L}}^2(t)\mathbb{E}_b\left\{J_{k,\mathcal{L}}^2\right\} \tag{1.35}$$

onde $\mathbb{E}_b\left\{J_{k,\mathcal{L}}^2\right\}$:

$$\mathbb{E}_b\left\{J_{k,\mathcal{L}}^2\right\} = \left(\mathcal{R}_{k,k}(\tau_{k,\mathcal{L}})\right)^2 + \left(\tilde{\mathcal{R}}_{k,k}(\tau_{k,\mathcal{L}})\right)^2 \tag{1.36}$$

Considera-se o perfil atraso-potência determinístico, assim, $\tau_{k,\mathcal{L}} = \tau_{k,\ell} - \tau_{k,\mathcal{L}} = \Delta_\ell - \Delta_{\mathcal{L}}$ é uma constante e não uma variável aleatória. Adicionalmente, $\tau_{k,\mathcal{L}}$ assume apenas valores múltiplos de T_c, impostos pelo perfil atraso-potência do canal. Assim, do apêndice A.2, pode-se reescrever:

$$\begin{aligned}\mathcal{R}_{k,k}(\tau_{k,\mathcal{L}}) &= T_c C_{k,k}\left(\frac{\tau_{k,\mathcal{L}}}{T_c} - N\right) \\ \tilde{\mathcal{R}}_{k,k}(\tau_{k,\mathcal{L}}) &= T_c C_{k,k}\left(\frac{\tau_{k,\mathcal{L}}}{T_c}\right)\end{aligned} \tag{1.37}$$

Realizando a média na variável $\alpha_{\mathcal{L}}$:

$$\mathbb{E}_\alpha\left\{\mathbb{E}_b\left\{\mathbb{E}_\varphi\left\{(S\,I_{k,\ell})^2\right\}\right\}\right\} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \frac{P}{4}\mathbb{E}_\alpha\left\{\alpha_{\mathcal{L}}^2\right\}\left(\left(T_c C_{k,k}\left(\frac{\tau_{k,\mathcal{L}}}{T_c} - N\right)\right)^2 + \left(T_c C_{k,k}\left(\frac{\tau_{k,\mathcal{L}}}{T_c}\right)\right)^2\right) \tag{1.38}$$

A potência da SI é, portanto, dada por:

$$\mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,\ell})^2\right\} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \frac{P}{4}\mathbb{E}_{\alpha}\left\{\alpha_{\mathcal{L}}^2(t)\right\}\left(\left(T_c C_{k,k}(\frac{\tau_{k,\mathcal{L}}}{T_c} - N)\right)^2 + \left(T_c C_{k,k}(\frac{\tau_{k,\mathcal{L}}}{T_c})\right)^2\right) \tag{1.39}$$

Então, obtém-se a relação sinal-ruído-interferência (SNIR) na saída do ℓ-ésimo correlacionador do k-ésimo usuário:

$$SNIR_{k,\ell} = \frac{\frac{P}{2}T^2\mathbb{E}_{\alpha}\{\alpha_{\ell}^2\}}{\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,\ell})^2\right\} + \mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,\ell})^2\right\} + \frac{N_0 T}{4}} \tag{1.40}$$

onde $\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,\ell})^2\right\}$ é dado pela equação (1.31) e $\mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,\ell})^2\right\}$ é dado pela equação (1.39).

Como as energias de símbolo recebido $E_b = P \cdot T$ foram admitidas iguais para todos os usuários:

$$SNIR_{k,\ell} = \frac{E_b\ \mathbb{E}_{\alpha}\{\alpha_{\ell}^2\}}{\frac{2}{T}\left\{\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,\ell})^2\right\} + \mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,\ell})^2\right\}\right\} + \frac{N_0}{2}} \tag{1.41}$$

Para maximizar o desempenho do sistema para todos os usuários, deve-se maximizar a SNIR na saída de todos os correlacionadores de todos os usuários.

A seguir serão apresentadas algumas definições que auxiliarão o estudo de seqüências de espalhamento adequadas para sistemas QS-CDMA.

Seja $d \in \mathbb{Z}$. Define-se função de correlação cruzada periódica par (*even cross-correlation*, ECC), figura 1.9, como:

$$\theta(\mathbf{c}_i, \mathbf{c}_j, d) = \theta_{i,j}(d) = \begin{cases} C_{i,j}(d) + C_{j,i}^*(N-d), & 0 \leq d < N \\ C_{i,j}(d) + C_{j,i}^*(-N-d), & -N < d < 0 \end{cases} \tag{1.42}$$

e função de correlação cruzada periódica ímpar (*odd cross-correlation*, OCC), figura 1.10, como:

$$\Theta(\mathbf{c}_i, \mathbf{c}_j, d) = \Theta_{i,j}(d) = \begin{cases} C_{i,j}(d) - C_{j,i}^*(N-d), & 0 \leq d < N \\ C_{i,j}(d) - C_{j,i}^*(-N-d), & -N < d < 0 \end{cases} \tag{1.43}$$

onde $C_{i,j}(d)$ é a função de correlação aperiódica dada por (1.29) e reescrita a seguir:

$$C(\mathbf{c}_i, \mathbf{c}_j, d) = C_{i,j}(d) = \begin{cases} \sum_{m=0}^{N-d-1} c_{i,m} c_{j,m+d}^*, & 0 \leq d < N \\ \sum_{m=0}^{N+d-1} c_{i,m-d} c_{j,m}^*, & -N < d < 0 \\ 0 & |d| \geq N \end{cases} \tag{1.44}$$

onde $i \neq j$; $*$ denota o complexo conjugado; d representa o deslocamento entre as seqüências de espalhamento. Em (1.42) e (1.43), quando $i = j$, define-se a função de autocorrelação par (*even autocorrelation*, EAC) e ímpar (*odd autocorrelation*, OAC), respectivamente.

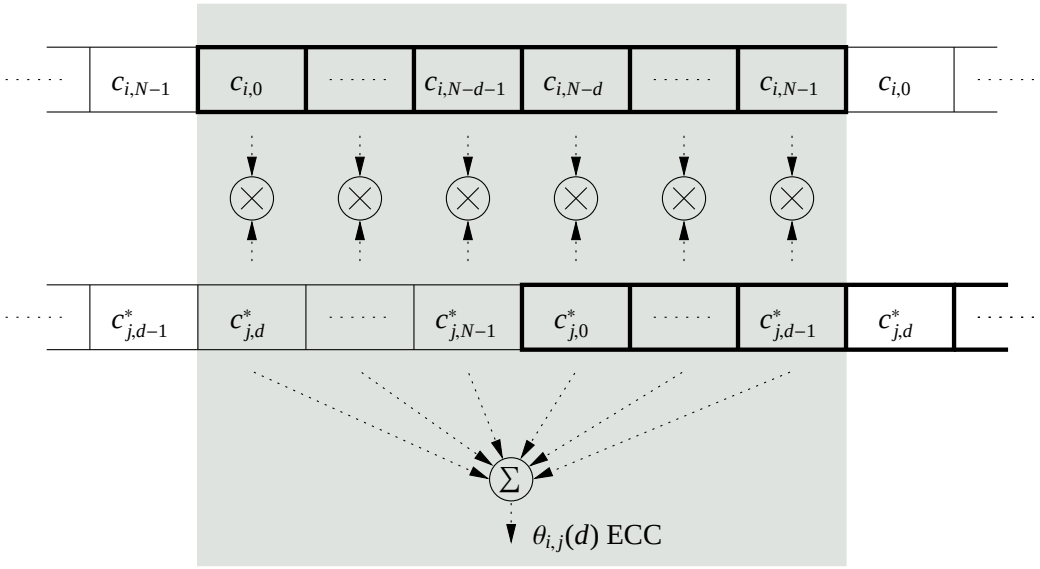

Figura 1.9: Função de correlação periódica par.

É fácil verificar a propriedade:

$$C_{i,j}(-d) = C_{j,i}^*(d) \tag{1.45}$$

De (1.42) e (1.45) tem-se a propriedade:

$$\theta_{i,j}(-d) = C_{i,j}(-d) + C_{j,i}^*(-N + d) = C_{j,i}^*(d) + C_{i,j}(N - d) = \theta_{j,i}^*(d) \tag{1.46}$$

Analogamente, de (1.43) e (1.45) tem-se a propriedade:

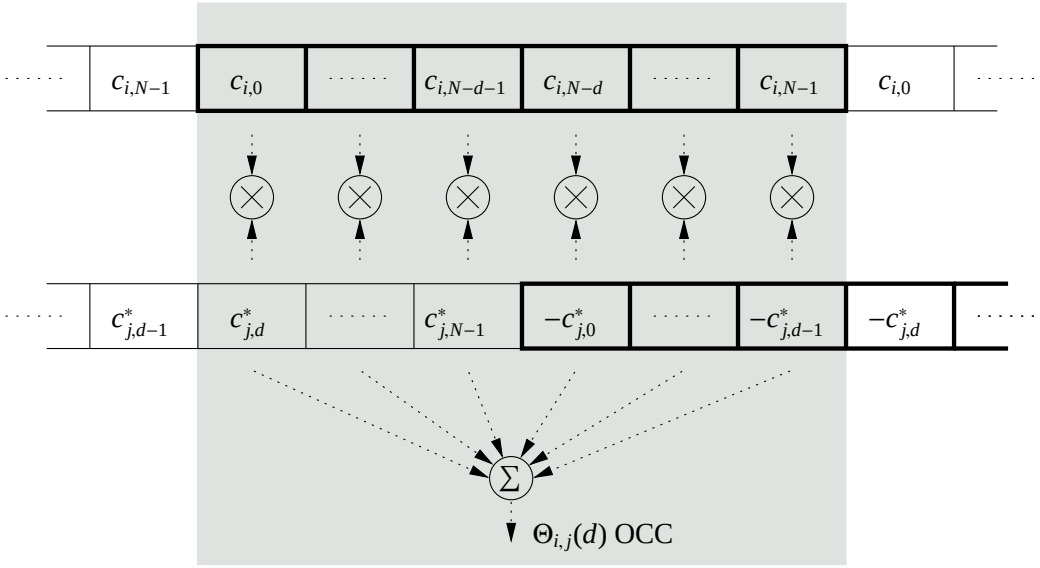

Figura 1.10: Função de correlação periódica ímpar.

$$\Theta_{i,j}(-d) = C_{i,j}(-d) - C^*_{j,i}(-N+d) = C^*_{j,i}(d) - C_{i,j}(N-d) = \Theta^*_{j,i}(d) \tag{1.47}$$

De (1.42) e (1.44), tem-se:

$$\theta_{i,j}(d) = \sum_{m=0}^{N-1} c_{i,m} c_{j,m+d(\bmod N)}, \quad \text{para} \ \ |d| < N \tag{1.48}$$

1.1.1 Critério de seleção de seqüências para sistemas QS-CDMA

Observando (1.18) e (1.20) verifica-se que a potência da MAI provocada sobre o ℓ-correlacionador do k-ésimo usuário será função da potência do sinal transmitido, do valor médio quadrático dos coeficientes de desvanecimento do canal e das funções de correlação parciais ponderadas pelos símbolos de informação. O apêndice A.2 mostra que pode-se reescrever a função de correlação parcial (1.21) em termos da função de correlação aperiódica (1.44):

$$\begin{aligned}
\mathcal{R}_{u,k}(\tau) &= T_c C_{u,k}(d-N) + \left[C_{u,k}(d-N+1) - C_{u,k}(d-N)\right](\tau - dT_c), \\
\tilde{\mathcal{R}}_{u,k}(\tau) &= T_c C_{u,k}(d) + \left[C_{u,k}(d+1) - C_{u,k}(d)\right](\tau - dT_c),
\end{aligned}$$

$$0 \leq dT_c \leq \tau < (d+1)T_c < NT_c \tag{1.49}$$

A soma e a subtração dessas funções de correlação parcial podem ser expressas em termos da função de correlação periódica par, $\theta_{i,j}(\tau)$ (1.42), e ímpar, $\Theta_{i,j}(\tau)$ (1.43), respectivamente:

$$\begin{aligned}
\mathcal{R}_{u,k}(\tau) - \tilde{\mathcal{R}}_{u,k}(\tau) &= T_c\left(\Theta_{u,k}(d)\right) + (\tau - dT_c)\left(\Theta_{u,k}(d+1) - \Theta_{u,k}(d)\right), \\
\mathcal{R}_{u,k}(\tau) + \tilde{\mathcal{R}}_{u,k}(\tau) &= T_c\left(\theta_{u,k}(d)\right) + (\tau - dT_c)\left(\theta_{u,k}(d+1) - \theta_{u,k}(d)\right) \\
& \qquad 0 \leq dT_c \leq \tau < (d+1)T_c < NT_c
\end{aligned} \tag{1.50}$$

Fazendo $\tau = rT_c$ e $T_c = \frac{T}{N}$ em (1.50), tem-se:

$$\begin{aligned}
\mathcal{R}_{u,k}(rT_c) - \tilde{\mathcal{R}}_{u,k}(rT_c) &= T\left(\frac{\Theta_{u,k}(d)}{N}\right) + T(r-d)\left(\frac{\Theta_{u,k}(d+1)}{N} - \frac{\Theta_{u,k}(d)}{N}\right), \\
\mathcal{R}_{u,k}(rT_c) + \tilde{\mathcal{R}}_{u,k}(rT_c) &= T\left(\frac{\theta_{u,k}(d)}{N}\right) + T(r-d)\left(\frac{\theta_{u,k}(d+1)}{N} - \frac{\theta_{u,k}(d)}{N}\right) \\
& \qquad 0 \leq d \leq r < (d+1) < N
\end{aligned} \tag{1.51}$$

De (1.51) e (1.20), tem-se, na situação de bits consecutivos iguais, $b_u^{(-1)} = b_u^{(0)}$, a potência da MAI dependente da função de correlação cruzada periódica par e, na situação de bits consecutivos opostos, $b_u^{(-1)} = -b_u^{(0)}$, a potência da MAI dependente da função de correlação cruzada periódica ímpar. Considerando bits equiprováveis, a função de correlação cruzada periódica par e a função de correlação cruzada periódica ímpar são igualmente importantes para a determinação da potência da MAI.

Fazendo a mesma análise para a potência da SI, equações (1.32) e (1.33), verifica-se que na situação de bits consecutivos iguais, $b_k^{(-1)} = b_k^{(0)}$, a potência da SI depende da função de autocorrelação periódica par. Na situação de bits consecutivos opostos, $b_u^{(-1)} = -b_u^{(0)}$, a potência da SI depende da função de autocorrelação periódica ímpar. Assim, novamente, considerando bits equiprováveis, a função de autocorrelação periódica par e a função de autocorrelação periódica ímpar são igualmente importantes para a determinação da potência da SI.

Então, para minimizar a potência da MAI e da SI e, em conseqüência, maximizar o desempenho do sistema, deve-se obter conjuntos de seqüências de espalhamento que

resultem em reduzidos valores para as funções de correlação periódica par e ímpar.

Como o atraso relativo $\tau_{u,\mathcal{L}}$ em (1.20) possui *pdf* uniforme definida no intervalo $[-\tau_{\max}+\gamma_{\mathcal{L}}; \tau_{\max}+\gamma_{\mathcal{L}}]$, a potência da MAI dependerá das funções de correlação cruzada periódica par $\theta_{u,k}(d)$ e ímpar $\Theta_{u,k}(d)$ apenas para[2] $|d| \leq \left\lceil \max\left\{\left|-\frac{\tau_{\max}}{T_c}+\frac{\gamma_{\mathcal{L}}}{T_c}\right|; \left|\frac{\tau_{\max}}{T_c}+\frac{\gamma_{\mathcal{L}}}{T_c}\right|\right\}\right\rceil = \left\lceil \frac{\tau_{\max}}{T_c}+\frac{\Delta_L}{T_c}\right\rceil$, onde Δ_L é o espalhamento máximo multipercurso. Analogamente, como $\tau_{k,\mathcal{L}}$ em (1.33) não será maior que Δ_L, a potência da SI dependerá das funções de autocorrelação periódica par $\theta_{k,k}(d)$ e ímpar $\Theta_{k,k}(d)$ apenas para $|d| \leq \left\lceil \frac{\Delta_L}{T_c}\right\rceil$.

Dado que o erro máximo de sincronismo $\tau_{\max}$ e o espalhamento máximo multipercurso Δ_L podem ser pequenos, as potências da MAI e da SI podem ser reduzidas utilizando-se conjuntos de seqüências que resultam em valores reduzidos para $\theta_{u,k}(d)$ e $\Theta_{u,k}(d)$, com $|d| \leq \left\lceil \frac{\tau_{\max}}{T_c}+\frac{\Delta_L}{T_c}\right\rceil$, e $\theta_{k,k}(d)$ e $\Theta_{k,k}(d)$, com $|d| \leq \left\lceil \frac{\Delta_L}{T_c}\right\rceil$, para quaisquer seqüências $\mathbf{c}_u$ e $\mathbf{c}_k$ pertencentes ao conjunto.

Será mostrado na seção 1.2 que quanto menor for o intervalo em que as funções de correlação assumem valores reduzidos, maior é o limite superior teórico para o número de seqüências do conjunto.

No próximo capítulo, serão apresentadas várias famílias de seqüências que resultam em funções de correlação cruzada periódica par reduzida. Obter expressões para as funções de correlação periódica par para uma dada família de seqüências é mais fácil do que obter expressões para as funções de correlação periódica ímpar. Existem poucos trabalhos publicados sobre funções de correlação periódica ímpar de seqüências.

Conforme será mostrado, a maioria das seqüências de comprimento ímpar é obtida a partir das seqüências de máximo comprimento (SMC), também conhecidas como *m-sequences*. As propriedades das funções de correlação periódica par das SMC são conhecidas. Com esse conhecimento, são obtidas expressões para as funções de correlação cruzada periódica par para seqüências obtidas a partir das SMC.

Analogamente, as seqüências de comprimento par são, em sua maioria, obtidas a partir de seqüências complementares, das quais apenas as propriedades de correlação periódica par são conhecidas. Então, obter expressões para as funções de correlação periódica par das seqüências de comprimento par é imediato.

Observe a diferença entre as funções de correlação periódicas par e ímpar:

[2] $\lceil x \rceil$ representa o menor inteiro maior ou igual a x.

$$\theta_{i,j}(d) - \Theta_{i,j}(d) = \begin{cases} 2C^*_{j,i}(N-d), & 0 \leq d < N \\ 2C^*_{j,i}(-N-d), & -N < d < 0 \end{cases} \tag{1.52}$$

Para $d = \pm 1$ essa diferença será no máximo 2, em módulo, e para $d = \pm 2$ a diferença será no máximo 4, em módulo. Então, para valores de d reduzidos, se a função de correlação periódica par assumir valores reduzidos, a função de correlação periódica ímpar também assumirá valores reduzidos. Isso significa que, para sistemas QS-CDMA, pode ser suficiente utilizar conjuntos de seqüências que resultam valores reduzidos apenas para as funções de correlação periódica par, a fim de minimizar as potências da MAI e da SI e, consequentemente, maximizar a SNIR e o desempenho do sistema. Essa constatação auxilia o estudo de seqüências, visto que pouco foi publicado sobre as funções de correlação periódica ímpar de seqüências.

A seção seguinte apresentará alguns limites teóricos para as funções de correlação. Esses limites mostram quão pequenos podem ser os valores assumidos pelas funções de correlação das seqüências de um conjunto.

1.2 Limites teóricos

Conforme foi mostrado na seção anterior, é desejável obter seqüências que resultam em valores reduzidos para as funções de autocorrelação e de correlação cruzada. Inicialmente em (WELCH, 1974), foi apresentado um limite que estabelece quão reduzidos podem ser os valores da função de correlação cruzada periódica par e da função de autocorrelação periódica par para um conjunto A de K seqüências compostas de elementos complexos tal que $\theta(\mathbf{u}, \mathbf{u}, 0) = N$, com $\mathbf{u} \in A$. Esse limite é chamado de limite de Welch e é dado por:

$$\left(\frac{\theta_{\max}}{N}\right)^2 \geq \frac{K-1}{KN-1} \tag{1.53}$$

onde:

$$\theta_{\max} = \max\{\theta_c, \theta_a\}$$

$$\theta_c = \max\{|\theta(\mathbf{u}, \mathbf{v}, d)| : \mathbf{u} \neq \mathbf{v},\ |d| < N\}$$

$$\theta_a = \max\{|\theta(\mathbf{u}, \mathbf{u}, d)| : 0 < |d| < N\} \tag{1.54}$$

onde $\mathbf{u}, \mathbf{v} \in A$.

Para as funções de correlação aperiódica, o limite de Welch é dado por:

$$\left(\frac{C_{\max}}{N}\right)^2 \geq \frac{K-1}{K(2N-1)-1} \tag{1.55}$$

onde:

$$\begin{aligned} C_{\max} &= \max\{C_c, C_a\} \\ C_c &= \max\{|C(\mathbf{u}, \mathbf{v}, d)| : \mathbf{u} \neq \mathbf{v},\ |d| < N\} \\ C_a &= \max\{|C(\mathbf{u}, \mathbf{u}, d)| : 0 < |d| < N\} \end{aligned} \tag{1.56}$$

A demonstração do limite de Welch utiliza-se de um teorema do produto escalar (WELCH, 1974) o que a torna relativamente longa. Em (MASSEY, 1991), apresentou-se uma forma elementar de derivar o limite de Welch.

Em (SARWATE, 1979), Sarwate faz a observação que se um conjunto de seqüências possui boas propriedades de correlação cruzada, as propriedades de autocorrelação não serão muito boas. Essa observação qualitativa é verificada com limites inferiores que relacionam as funções de correlação cruzada e de autocorrelação. Para as funções de correlação periódica par, o limite de Sarwate é dado por:

$$\left(\frac{\theta_c^2}{N}\right) + \frac{N-1}{N(K-1)}\left(\frac{\theta_a^2}{N}\right) \geq 1 \tag{1.57}$$

Para as funções de correlação aperiódica, o limite de Sarwate é dado por:

$$\frac{(2N-1)}{N}\left(\frac{C_c^2}{N}\right) + \frac{2(N-1)}{N(K-1)}\left(\frac{C_a^2}{N}\right) \geq 1 \tag{1.58}$$

Fazendo $\theta_{\max} = \max\{\theta_c, \theta_a\}$ em (1.57) e $C_{\max} = \max\{C_c, C_a\}$ em (1.58), obtém-se os limites de Welch (1.53) e (1.55), respectivamente. Assim, tem-se que os limites de Welch são casos particulares dos limites de Sarwate.

O limite de (1.57) mostra que não é possível obter conjuntos de seqüências ideais. Considera-se ideais os conjuntos de seqüências tais que:

$$\begin{aligned} |\theta(\mathbf{u},\mathbf{v},d)| &= 0, \quad \text{para} \quad \mathbf{u} \neq \mathbf{v},\ |d| < N \\ |\theta(\mathbf{u},\mathbf{u},d)| &= 0, \quad \text{para} \quad 0 < |d| < N \end{aligned} \tag{1.59}$$

Isso não é suficiente para afirmar que conjuntos ideais, quando utilizados em sistemas DS/CDMA, eliminam totalmente a MAI e SI. Deve-se considerar a função de correlação ímpar na determinação da MAI e da SI, como mostrado na seção anterior.

Além de (SARWATE, 1979) apresentar limites para as funções de correlação periódica par e aperiódica, esse apresenta também um limite que relaciona as funções de correlação periódica ímpar:

$$\left(\frac{\Theta_c^2}{N}\right) + \frac{N-1}{N(K-1)}\left(\frac{\Theta_a^2}{N}\right) \geq 1 \tag{1.60}$$

onde:

$$\begin{aligned} \Theta_{\max} &= \max\{\Theta_c, \Theta_a\} \\ \Theta_c &= \max\{|\Theta(\mathbf{u},\mathbf{v},d)| : \mathbf{u} \neq \mathbf{v},\ |d| < N\} \\ \Theta_a &= \max\{|\Theta(\mathbf{u},\mathbf{u},d)| : 0 < |d| < N\} \end{aligned} \tag{1.61}$$

Em sistemas QS-CDMA, os sinais chegam ao receptor confinados em um intervalo de tempo. Assim, as seqüências utilizadas no sistema serão observadas quase sincronizadas. Então, é suficiente que o conjunto seja ideal ou resulte em valores reduzidos de correlação apenas para uma faixa de deslocamentos. Conforme já mencionado, para a função de correlação cruzada, é desejável que a faixa seja $|d| \leq \left\lceil \frac{1}{T_c}(\tau_{\max} + \Delta_L) \right\rceil$, onde $\tau_{\max} + \Delta_L$ representa o maior atraso observado entre sinais de usuários distintos em um sistema QS-CDMA. Para a função de autocorrelação, é desejável que a faixa seja $0 < |d| \leq \left\lceil \frac{\Delta_L}{T_c} \right\rceil$, onde Δ_L representa o maior atraso observado entre os multipercursos de um mesmo usuário (espalhamento máximo multipercurso). Assim, para analisar os conjuntos de seqüências adequados para sistemas QS-CDMA, definem-se zonas (faixas) nas quais as funções de correlação são reduzidas.

A zona de correlação cruzada periódica par reduzida para um conjunto A de seqüências é definida como:

$$L_{CCZ} = \max\{\mathcal{Z} : |\theta(\mathbf{u}, \mathbf{v}, d)| \leq \theta_{cCZ}, \ \ \forall \mathbf{u}, \mathbf{v} \in A, \ \ \mathbf{u} \neq \mathbf{v}, \ \ |d| \leq \mathcal{Z}\} \tag{1.62}$$

A zona de autocorrelação periódica par reduzida é definida como:

$$L_{ACZ} = \max\{\mathcal{Z} : |\theta(\mathbf{u}, \mathbf{u}, d)| \leq \theta_{aCZ}, \forall \mathbf{u} \in A, 0 < |d| \leq \mathcal{Z}\} \tag{1.63}$$

e a zona de correlação reduzida (*low correlation zone,* LCZ) é definida como:

$$L_{CZ} = \min\{L_{CCZ}, L_{ACZ}\} \tag{1.64}$$

Quando $\theta_m = \max\{\theta_{cCZ}, \theta_{aCZ}\} = 0$, (1.62) define a zona de correlação cruzada nula (Z_{CCZ}) e (1.63) define a zona de autocorrelação nula (Z_{ACZ}). Conseqüentemente, (1.64) define a zona de correlação nula (*zero correlation zone,* ZCZ).

Os conjuntos que possuem $\theta_m = 1$ e $L_{CZ} = 0$ são chamados de conjuntos quase ortogonais e os que possuem $\theta_m = 1$ e $L_{CZ} > 0$ são chamados de conjuntos quase ortogonais generalizados. Em contrapartida, os conjuntos que possuem $\theta_m = 0$ e $Z_{CZ} = 0$ são chamados de conjuntos ortogonais e os que possuem $\theta_m = 0$ e $Z_{CZ} > 0$ são chamados de conjuntos ortogonais generalizados.

A partir das observações anteriores, tem-se que as funções de correlação devem ser consideradas apenas no intervalo $|d| \leq L_{CZ}$ ou $|d| \leq Z_{CZ}$, para a análise dos conjuntos de seqüências aplicadas em sistemas QS-CDMA.

Em (TANG; FAN; MATSUFUJI, 2000) e (TANG; FAN, 2001a) foram apresentados os limites para as funções de correlação para o intervalo $|d| \leq L_{CZ}$:

$$\begin{aligned} \theta^2_{mCZ} &\geq N\frac{KL_{CZ} + K - N}{KL_{CZ} + K - 1} \\ C^2_{mCZ} &\geq N^2\frac{(K-1)(L_{APCZ}+1) - N + 1}{(KL_{APCZ})(N + L_{APCZ})} \\ \Theta^2_{mCZ} &\geq N\frac{KL_{OPCZ} + K - N}{(KL_{OPCZ} + K - 1)} \end{aligned} \tag{1.65}$$

onde, $\theta_{mCZ} = \max\{\theta_{cCZ}, \theta_{aCZ}\}$ e analogamente à L_{CZ}, definem-se:

$$
\begin{aligned}
&L_{APCZ} = \\
&= \max\{\mathcal{Z} : |C(\mathbf{u},\mathbf{v},d)| \leq C_{mCZ}, \text{ onde } (|d| \leq \mathcal{Z} \text{ e } \mathbf{u} \neq \mathbf{v}) \text{ ou } (0 < |d| \leq \mathcal{Z} \text{ e } \mathbf{u} = \mathbf{v})\} \\
&L_{OPCZ} = \\
&= \max\{\mathcal{Z} : |\Theta(\mathbf{u},\mathbf{v},d)| \leq \Theta_{mCZ}, \text{ onde } (|d| \leq \mathcal{Z} \text{ e } \mathbf{u} \neq \mathbf{v}) \text{ ou } (0 < |d| \leq \mathcal{Z} \text{ e } \mathbf{u} = \mathbf{v})\}
\end{aligned}
\tag{1.66}
$$

Os limites de (1.65) são chamados de limites de Tang-Fan.

Recentemente em (PENG; FAN, 2002) e (PENG; FAN, 2003a) foram derivados limites que relacionam as funções de correlação periódica par e aperiódica para seqüências binárias, respectivamente, considerando a zona de correlação reduzida (LCZ). Em (PENG; FAN, 2003b), o limite que relaciona a função de autocorrelação periódica par com a função de correlação cruzada periódica par considerando a LCZ foi generalizado para seqüências compostas de elementos complexos de módulos unitários. Esse é dado por:

$$
\frac{1}{K}\left(1 - \frac{1}{L_{CZ}+1}\right)\theta_{aCZ}^2 + \left(1 - \frac{1}{K}\right)\theta_{cCZ}^2 \geq N - \frac{N^2}{K(L_{CZ}+1)} \tag{1.67}
$$

Fazendo $L_{CZ} = N-1$, $\theta_{aCZ} = \theta_a$ e $\theta_{cCZ} = \theta_c$ em (1.67), obtém-se o limite de Sarwate (1.57) para as funções de correlação periódica par. Fazendo $\theta_m = \max\{\theta_{cCZ}, \theta_{aCZ}\}$ e $L_{CZ} = N-1$ em (1.67), obtém-se o limite de Welch (1.53) para as funções de correlação periódica par.

Como o limite de Sarwate para as funções de correlação periódica par (1.57) é um caso particular de (1.67), este é chamado de limite de Sarwate generalizado. Neste trabalho, é dada maior atenção às funções de correlação periódica par, pois a maioria das metodologias de seleção de seqüências aqui discutidas objetivam obter conjuntos de seqüências que resultam em reduzidos valores de correlação periódica par. Assim, a seção seguinte apresenta a demonstração do limite de Sarwate generalizado apenas para as funções de correlação periódica par.

1.2.1 Limite de Sarwate generalizado

Considere q um inteiro positivo maior que 1, o conjunto dos números inteiros menores que q, $Z_q = \{0, 1, ..., q-1\}$, os elementos complexos de módulo unitário, $W_q^n = e^{\frac{\sqrt{-1}2\pi}{q}n}$, e o conjunto de q elementos W_q, $E = \{W_q^0, W_q^1, ..., W_q^{q-1}\}$. Considere a seqüência $\mathbf{x} = (x_0, x_1, ..., x_{N-1}) \in E^N$ de comprimento N. Quando $q = 2$ a seqüência $\mathbf{x}$ é binária.

Para derivar o limite de Sarwate generalizado serão demonstradas 4 propriedades de correlação (Lema 1.2.1 a 1.2.4).

Lema 1.2.1 *Para qualquer seqüência* $\mathbf{x} \in E^N$ *e qualquer inteiro* $d = 0, 1, ..., N-1$ *tem-se:*

$$\sum_{\mathbf{y} \in E^N} |\theta(\mathbf{x}, \mathbf{y}, d)|^2 = Nq^N \tag{1.68}$$

A prova é apresentada a seguir (PENG; FAN, 2003a).

Sejam $\mathbf{x} = \{W_q^{u_0}, W_q^{u_1}, ..., W_q^{u_{N-1}}\}$ e $\mathbf{y} = \{W_q^{v_0}, W_q^{v_1}, ..., W_q^{v_{N-1}}\}$, onde $u_i, v_i \in Z_q$ com $i = 0, 1, ..., N-1$. Tem-se que:

$$\begin{aligned}
\sum_{\mathbf{y} \in E^N} |\theta(\mathbf{x}, \mathbf{y}, d)|^2 &= \sum_{\mathbf{y} \in E^N} \theta(\mathbf{x}, \mathbf{y}, d)\theta^*(\mathbf{x}, \mathbf{y}, d) \\
&= \sum_{\mathbf{y} \in E^N} \left(\sum_{i=0}^{N-1} W_q^{u_i - v_{i+d}} \right) \left(\sum_{j=0}^{N-1} W_q^{-u_j + v_{j+d}} \right) \\
&= \sum_{i,j=0}^{N-1} W_q^{u_i - u_j} H(i, j, d)
\end{aligned} \tag{1.69}$$

onde

$$H(i, j, d) = \sum_{\mathbf{y} \in E^N} W_q^{-v_{i+d} + v_{j+d}} \tag{1.70}$$

Existe um total de q^N seqüências $\mathbf{y} \in E^N$. Observando dois elementos quaisquer v_{i+d} e v_{j+d} das seqüências $\mathbf{y} = \{v_0, v_1, ..., v_{i+d}, ..., v_{j+d}, ...v_{N-1}\}$, existem q^2 combinações distintas de elementos v_{i+d} e v_{j+d}. Então, percorrendo todas as q^N seqüências $\mathbf{y} \in E^N$, observa-se cada uma das q^2 combinações distintas de elementos v_{i+d} e v_{j+d} se repetirem

q^{N-2} vezes, totalizando as $q^2 q^{N-2} = q^N$ seqüências. Assim, se $i \neq j$ em (1.70):

$$H(i, j, d) = q^{N-2} \sum_{r,s=0}^{q-1} W_q^{-r+s} = 0 \tag{1.71}$$

Se $i = j$ em (1.70):

$$H(i, j, d) = \sum_{\mathbf{y} \in E^N} W_q^0 = q^N \tag{1.72}$$

De (1.69) tem-se:

$$\sum_{\mathbf{y} \in E^N} |\theta(\mathbf{x}, \mathbf{y}, d)|^2 = \sum_{i,j=0}^{N-1} W_q^{u_i - u_j} H(i, j, d) = \sum_{k=0}^{N-1} W_q^0 H(k, k, d) + \sum_{i,j=0,\ i \neq j}^{N-1} W_q^{u_i - u_j} H(i, j, d) \tag{1.73}$$

Substituindo (1.71) e (1.72) em (1.73):

$$\sum_{\mathbf{y} \in E^N} |\theta(\mathbf{x}, \mathbf{y}, d)|^2 = \sum_{i,j=0}^{N-1} W_q^{u_i - u_j} H(i, j, d) = N q^N \tag{1.74}$$

Assim, prova-se o Lema 1.2.1.

Considere elementos $w_i \geq 0$, com $i = 0, 1, ..., L_{CZ}$, considere também $\sum_{i=0}^{L_{CZ}} w_i = 1$ e $\mathbf{w} = (w_0, w_1, ..., w_{L_{CZ}})$. Define-se o operador deslocamento cíclico como:

$$\mathbb{T}^i \mathbf{x} = (x_i, x_{i+1}, ..., x_0, x_{N-1}, ..., x_{N-i}) \tag{1.75}$$

O número de seqüências em um conjunto A será denotado por $|A|$. Considere $\mathbf{x} \in E^N$ e $A, B \subseteq E^N$, com $|A| > 0$ e $|B| > 0$. Define-se:

$$F(A, B) = \frac{1}{|A||B|} \sum_{\mathbf{x} \in A} \sum_{\mathbf{y} \in B} \sum_{s=0}^{L_{CZ}} \sum_{t=0}^{L_{CZ}} | < \mathbb{T}^s \mathbf{x}, \mathbb{T}^t \mathbf{y} > |^2 w_s w_t \tag{1.76}$$

onde $< \mathbf{x}, \mathbf{y} >= \sum_{i=0}^{N-1} x_i y_i^*$.

Lema 1.2.2 *Para qualquer* $\mathbf{x} \in E^N$ *e* $A \subseteq E^N$*:*

$$F(\{\mathbf{x}\}, E^N) = F(A, E^N) = F(E^N, E^N) = N \tag{1.77}$$

Segue a prova do Lema 1.77 (PENG; FAN, 2003a).

$$F(\{\mathbf{x}\}, E^N) = \frac{1}{|1||q^N|} \sum_{\mathbf{y} \in E^N} \sum_{s=0}^{L_{CZ}} \sum_{t=0}^{L_{CZ}} | < \mathbb{T}^s \mathbf{x}, \mathbb{T}^t \mathbf{y} > |^2 w_s w_t \tag{1.78}$$

Observe que:

$$< \mathbb{T}^s \mathbf{x}, \mathbb{T}^t \mathbf{y} >= \begin{cases} \theta(\mathbf{x}, \mathbf{y}, t-s) & \text{se } \ s \leq t; \\ \theta(\mathbf{x}, \mathbf{y}, N+t-s) & \text{caso contrário.} \end{cases} \tag{1.79}$$

Substituindo (1.79) em (1.78):

$$\begin{aligned} F(\{\mathbf{x}\}, E^N) \ &= \ \frac{1}{q^N} \Bigg[\sum_{0 \leq s \leq t \leq L_{CZ}} \sum_{\mathbf{y} \in E^N} |\theta(\mathbf{x}, \mathbf{y}, t-s)|^2 w_s w_t + \\ &+ \ \sum_{0 \leq t \leq s < L_{CZ}} \sum_{\mathbf{y} \in E^N} |\theta(\mathbf{x}, \mathbf{y}, N-s+t)|^2 w_s w_t \Bigg] \end{aligned} \tag{1.80}$$

Substituindo (1.68) em (1.80):

$$F(\{\mathbf{x}\}, E^N) \ = \ \frac{1}{q^N} \left[\sum_{0 \leq s \leq t \leq L_{CZ}} N q^N w_s w_t + \sum_{0 \leq t \leq s < L_{CZ}} N q^N w_s w_t \right] = N \tag{1.81}$$

Observe que $F(\{\mathbf{x}\}, E^N)$ não depende de $\mathbf{x}$. Assim, prova-se o Lema 1.77.

Lema 1.2.3 *Para $C \subseteq E^N$ tem-se $F(C, C) \geq N$*

Segue a prova do Lema 1.2.3 (PENG; FAN, 2003a).

Inicialmente, será verificado que:

$$F(A, B) = \frac{1}{|A||B|} \sum_{X \in U(A)} \sum_{Y \in U(B)} \sum_{i,j=0}^{N-1} f(i, j, s; X) f^*(i, j, t; Y) \tag{1.82}$$

onde $U(\mathbf{x}) = \{\mathbb{T}^i\mathbf{x} | i = 0, 1, ..., L_{CZ}\}$, $U(A) = \bigcup_{\mathbf{x}\in A} U(\mathbf{x})$, $X = \mathbb{T}^s\mathbf{x} = (x_s, x_{s+1}, ..., x_{s+n-1})$ e $Y = \mathbb{T}^t\mathbf{y} = (y_t, y_{t+1}, ..., y_{t+n-1})$. Para qualquer $i = 0, 1, ..., N-1$, $j = 0, 1, ..., N-1$ e $s = 0, 1, ..., L_{CZ}$ define-se a função $f(i, j, s, X)$ sobre $U(E^N)$ como:

$$f(i, j, s; X) = x_{s+i}x_{s+j}w_s \tag{1.83}$$

Para qualquer $\mathbf{x} \in A$ e $\mathbf{y} \in B$, tem-se que:

$$\begin{aligned}
\sum_{X\in U(A)}\sum_{Y\in U(B)}\sum_{i,j=0}^{N-1} f(i, j, s; X)f^*(i, j, t; Y) &= \sum_{s,t=0}^{L_{CZ}}\sum_{i,j=0}^{N-1} f(i, j, s; \mathbb{T}^s\mathbf{x})f^*(i, j, t; \mathbb{T}^t\mathbf{y}) \\
&= \sum_{s,t=0}^{L_{CZ}}\sum_{i,j=0}^{N-1}(x_{s+i}x^*_{s+j}w_s)(y_{t+i}y^*_{t+j}w_t)^* \\
&= \sum_{s,t=0}^{L_{CZ}}(\sum_{i=0}^{N-1} x_{s+i}y^*_{t+i})(\sum_{j=0}^{N-1} x_{s+j}y^*_{t+j})^* w_s w_t \\
&= \sum_{s,t=0}^{L_{CZ}}|\sum_{i=0}^{N-1} x_{s+i}y^*_{s+j}|^2 w_s w_t \\
&= \sum_{s,t=0}^{L_{CZ}}| < \mathbb{T}^s x, \mathbb{T}^t y > |^2 w_s w_t
\end{aligned} \tag{1.84}$$

e substituindo esse resultado em $\sum_{\mathbf{x}\in A}\sum_{\mathbf{y}\in B}\sum_{s,t=0}^{L_{CZ}}| < \mathbb{T}^s x, \mathbb{T}^t y > |^2 w_s w_t$:

$$\begin{aligned}
\sum_{\mathbf{x}\in A}\sum_{\mathbf{y}\in B}\sum_{s,t=0}^{L_{CZ}}| < \mathbb{T}^s\mathbf{x}, \mathbb{T}^t\mathbf{y} > |^2 w_s w_t &= \sum_{\mathbf{x}\in A}\sum_{\mathbf{y}\in B}\sum_{X\in U(\mathbf{x})}\sum_{Y\in U(\mathbf{y})}\sum_{i,j=0}^{N-1} f(i, j, s; X)f^*(i, j, t; Y) \\
&= \sum_{X\in U(A)}\sum_{Y\in U(B)}\sum_{i,j=0}^{N-1} f(i, j, s; X)f^*(i, j, t; Y)
\end{aligned} \tag{1.85}$$

Substituindo (1.85) em (1.76), verifica-se (1.82).

Usando a desigualdade de Cauchy em (1.82):

$$\{|A||B|F(A, B)\}^2 = \left\{\sum_{i,j=0}^{N-1}\left(\sum_{X\in U(A)} f(i, j, s; X)\right)\left(\sum_{Y\in U(B)} f^*(i, j, t; Y)\right)\right\}^2$$

$$\begin{aligned} &\leq \sum_{i,j=0}^{N-1} \left| \sum_{X \in U(A)} f(i,j,s;X) \right|^2 \times \sum_{i,j=0}^{N-1} \left| \sum_{Y \in U(B)} f(i,j,s;Y) \right|^2 \\ &= |A|^2 F(A,A) |B|^2 F(B,B) \end{aligned} \tag{1.86}$$

Portanto:

$$\{F(A,B)\}^2 \leq F(A,A)F(B,B) \tag{1.87}$$

Fazendo $A = E^N$ e $B = C$ em (1.87), tem-se:

$$\{F(E^N,C)\}^2 \leq F(E^N,E^N)F(C,C) \tag{1.88}$$

De (1.77):

$$N^2 \leq NF(C,C) \tag{1.89}$$

Portanto:

$$F(C,C) \geq N \tag{1.90}$$

Assim, prova-se o Lema 1.2.3.

Lema 1.2.4 *Para $C \subseteq E^N$ e $|C| = K > 0$, tem-se:*

$$F(C,C) \leq \frac{N^2}{K} \sum_{s=0}^{L_{CZ}} w_s + \frac{1}{K} \left(1 - \sum_{s=0}^{L_{CZ}} w_s^2 \right) \theta_{aCZ}^2 + \left(1 - \frac{1}{K} \right) \theta_{cCZ}^2 \tag{1.91}$$

A prova é apresentada a seguir (PENG; FAN, 2003a).

Tem-se que:

$$F(C,C) = \frac{1}{|K||K|} \sum_{\mathbf{x} \in C} \sum_{\mathbf{y} \in C} \sum_{s=0}^{L_{CZ}} \sum_{t=0}^{L_{CZ}} | < \mathbb{T}^s \mathbf{x}, \mathbb{T}^t \mathbf{y} > | w_s w_t \tag{1.92}$$

Rearranjando os termos dos somatórios e lembrando que $< \mathbb{T}^s \mathbf{x}, \mathbb{T}^t \mathbf{y} >= \sum_{i=0}^{N-1} x_{i+s} y_{i+t} =$

$\theta(\mathbf{x}, \mathbf{y}, t-s)$:

$$\begin{aligned} K^2F(C,C) &= \sum_{\mathbf{x}\in C}\sum_{s=0}^{L_{CZ}}\theta^2(\mathbf{x},\mathbf{x},0)w_sw_s + \sum_{\mathbf{x}\in C}\sum_{s,t=0,\ s\neq t}^{L_{CZ}}\theta^2(\mathbf{x},\mathbf{x},t-s)w_sw_t \\ &+ \sum_{\mathbf{x},\mathbf{y}\in C,\ \mathbf{x}\neq\mathbf{y}}\sum_{s,t=0}^{L_{CZ}}\theta^2(\mathbf{x},\mathbf{y},t-s)w_sw_t \end{aligned} \tag{1.93}$$

Como $\theta^2(\mathbf{x},\mathbf{x},0) = N^2$, $\theta^2(\mathbf{x},\mathbf{x},t-s) \leq \theta^2_{aCZ}$, para $s \neq t$, e $\theta^2(\mathbf{x},\mathbf{y},t-s) \leq \theta^2_{cCZ}$, para $\mathbf{x} \neq \mathbf{y}$, pode-se obter a desigualdade:

$$\begin{aligned} K^2F(C,C) &= \sum_{\mathbf{x}\in C}\sum_{s=0}^{L_{CZ}}\theta^2(\mathbf{x},\mathbf{x},0)w_sw_s + \sum_{\mathbf{x}\in C}\sum_{s,t=0,\ s\neq t}^{L_{CZ}}\theta^2(\mathbf{x},\mathbf{x},t-s)w_sw_t \\ &+ \sum_{\mathbf{x},\mathbf{y}\in C,\ \mathbf{x}\neq\mathbf{y}}\sum_{s,t=0}^{L_{CZ}}\theta^2(\mathbf{x},\mathbf{y},t-s)w_sw_t \\ &\leq N^2\sum_{\mathbf{x}\in C}\sum_{s=0}^{L_{CZ}}w_s^2 + \theta^2_{aCZ}\sum_{\mathbf{x}\in C}\sum_{s,t=0,\ s\neq t}^{L_{CZ}}w_sw_t + \theta^2_{cCZ}\sum_{\mathbf{x},\mathbf{y}\in C,\ \mathbf{x}\neq\mathbf{y}}\left(\sum_{s=0}^{L_{CZ}}w_s\right)\left(\sum_{t=0}^{L_{CZ}}w_t\right) \end{aligned} \tag{1.94}$$

Lembrando que $\left(\sum_{s=0}^{L_{CZ}} w_s\right) = \left(\sum_{t=0}^{L_{CZ}} w_t\right) = 1$:

$$K^2F(C,C) \leq N^2K\sum_{s=0}^{L_{CZ}}w_s^2 + \theta^2_{aCZ}K\sum_{s,t=0,\ s\neq t}^{L_{CZ}}w_sw_t + \theta^2_{cCZ}K(K-1) \tag{1.95}$$

Assim, prova-se o Lema 1.2.4.

Dos Lemas 1.2.3 e 1.2.4 obtém-se o Teorema (PENG; FAN, 2003a):

Teorema 1.2.1 *Para $C \subseteq E^N$ e $|C| = K > 0$, tem-se que:*

$$N - \frac{N^2}{K}\sum_{s=0}^{L_{CZ}}w_s^2 \leq \frac{1}{K}\left(1 - \sum_{s=0}^{L_{CZ}}w_s^2\right)\theta^2_{aCZ} + \left(1 - \frac{1}{K}\right)\theta^2_{cCZ} \tag{1.96}$$

Para $\theta_{mCZ} = \max\{\theta_{aCZ}, \theta_{cCZ}\}$, obtém-se:

$$\theta_{mCZ}^2 \geq \frac{KN - N^2 \sum_{s=0}^{L_{CZ}} w_s^2}{K - \sum_{s=0}^{L_{CZ}} w_s^2} \tag{1.97}$$

Fazendo $w_s = \frac{1}{L_{CZ}+1}$, onde $s = 0, 1, ..., L_{CZ}$, tem-se $\sum_{s=0}^{L_{CZ}} w_s^2 = \frac{1}{L_{CZ}+1}$ e de (1.97):

$$\theta_{mCZ}^2 \geq \frac{KL_{CZ} + K - N}{KL_{CZ} + K - 1} N \tag{1.98}$$

Esse é o limite de Tang-Fan (TANG; FAN; MATSUFUJI, 2000) dado por (1.65).

Novamente, fazendo $w_s = \frac{1}{L_{CZ}+1}$ em (1.96), tem-se:

$$\frac{1}{K}\left(1 - \frac{1}{L_{CZ}+1}\right)\theta_{aCZ}^2 + \left(1 - \frac{1}{K}\right)\theta_{cCZ}^2 \geq N - \frac{N^2}{K(L_{CZ}+1)} \tag{1.99}$$

denominado limite de Sarwate generalizado (PENG; FAN, 2003a).

Fazendo $L_{CZ} = N - 1$, $\theta_{aCZ} = \theta_a$ e $\theta_{cCZ} = \theta_c$ em (1.99), tem-se:

$$\left(\frac{\theta_c^2}{N}\right) + \frac{N-1}{N(K-1)}\left(\frac{\theta_a^2}{N}\right) \geq 1 \tag{1.100}$$

definido como limite de Sarwate (SARWATE, 1979) dado por (1.57).

Fazendo $\theta_m = \max\{\theta_a, \theta_c\}$ em (1.100) obtém-se o limite de Welch (WELCH, 1974), o qual já foi apresentado por (1.53):

$$\left(\frac{\theta_{\max}}{N}\right)^2 \geq \frac{K-1}{KN-1} \tag{1.101}$$

Então, os limites de Tang-Fan, Sarwate e Welch para as funções de correlação periódica par são casos particulares do limite de Sarwate generalizado (1.99) apresentado aqui. Esse limite é adequado para avaliar seqüências quase ortogonais generalizadas e ortogonais generalizadas que são os principais objetos de estudo deste trabalho.

A figura 1.11 ilustra as relações entre o limite de Welch e o de Sarwate. Segundo Welch (1.53), um ponto $\{\frac{\theta_c^2}{N}, \frac{\theta_a^2}{N}\}$ nunca estará no interior da região hachurada. Em contrapartida, o limite de Sarwate (1.57) garante que um ponto $\{\frac{\theta_c^2}{N}, \frac{\theta_a^2}{N}\}$ nunca estará no interior da região sombreada (abaixo da reta $\left(\frac{\theta_c^2}{N}\right) + \frac{N-1}{N(K-1)}\left(\frac{\theta_a^2}{N}\right) = 1$). Assim, o limite de Sarwate é mais restritivo que o limite de Welch.

A figura 1.12 ilustra as relações entre os limites de Sarwate generalizado, Tang-

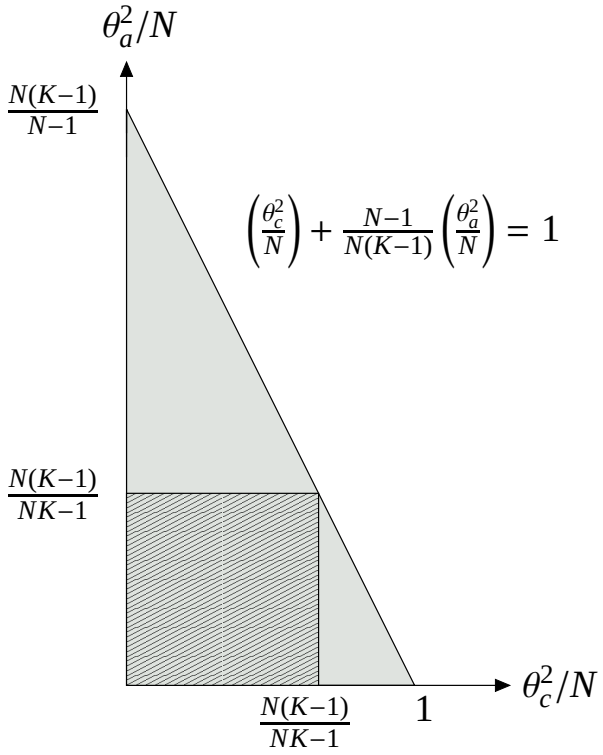

Figura 1.11: Esboço dos limites de Welch e Sarwate.

Fan, Welch e Sarwate. Segundo o limite de Tang-Fan (1.98), nenhum ponto $\{\frac{\theta_{cCZ}^2}{N}, \frac{\theta_{aCZ}^2}{N}\}$ estará no interior da região duplamente hachurada. O limite de Sarwate generalizado é mais restritivo, pois garante que nenhum ponto $\{\frac{\theta_{cCZ}^2}{N}, \frac{\theta_{aCZ}^2}{N}\}$ estará abaixo das retas $\frac{1}{K}\left(1 - \frac{1}{L_{CZ}+1}\right)\theta_{aCZ}^2 + \left(1 - \frac{1}{K}\right)\theta_{cCZ}^2 = N - \frac{N^2}{K(L_{CZ}+1)}$ definidas por L_{CZ}. Observe no gráfico que para $L_{CZ} = N - 1$ obtém-se o esboço do limite de Sarwate e Welch, conforme já mencionado.

O esboço do limite de Sarwate mostra que quanto menor a zona de correlação reduzida (LCZ), maior será a região com pontos $\{\frac{\theta_{cCZ}^2}{N}, \frac{\theta_{aCZ}^2}{N}\}$ com reduzidos valores de θ_{cCZ} e θ_{aCZ}. Na figura 1.12, observa-se também que aumentando-se a relação $\frac{N}{K}$, aumenta-se também a região com pontos $\{\frac{\theta_{cCZ}^2}{N}, \frac{\theta_{aCZ}^2}{N}\}$ com reduzidos valores de θ_{cCZ} e θ_{aCZ}. O que é intuitivo, pois para um dado comprimento N, quanto mais seqüências tiver um conjunto, haverá mais pares de seqüências que apresentam valores mais elevados de correlação. Essa característica será verificada nos conjuntos de seqüências que serão apresentados no próximo capítulo.

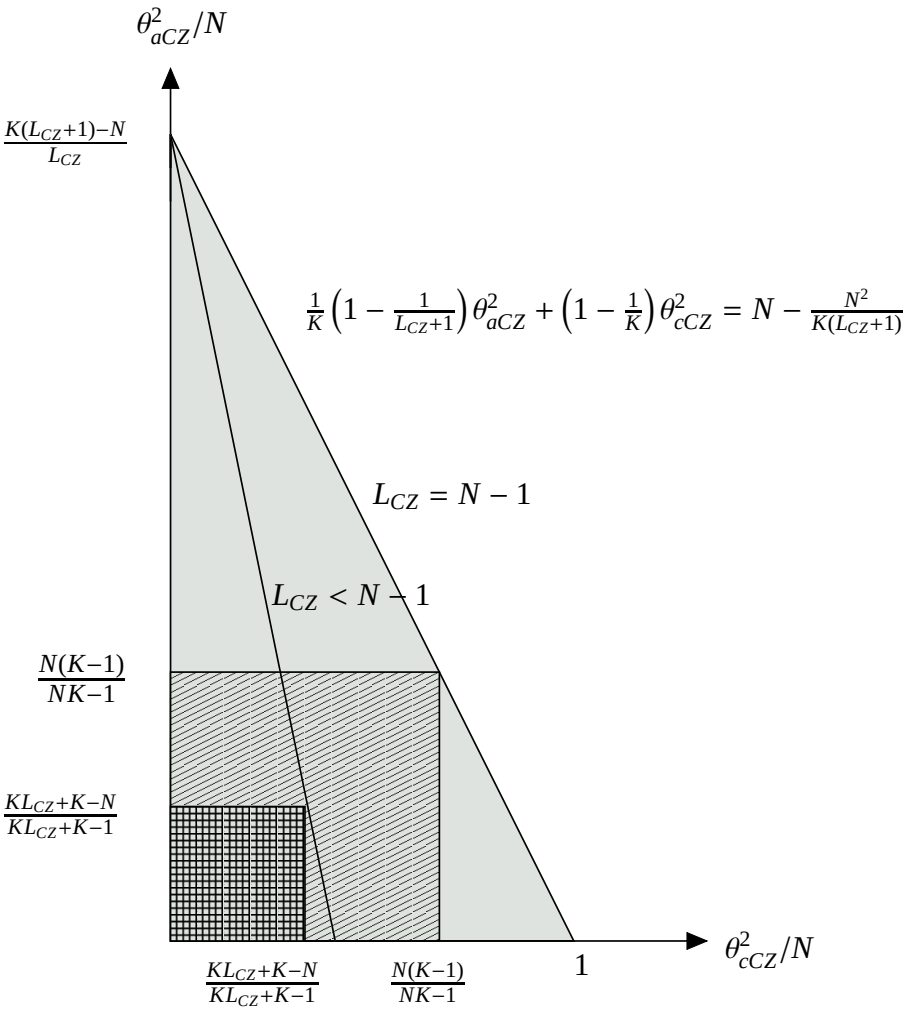

Figura 1.12: Esboço dos limites de Sarwate generalizado e Tang-Fan.

2 Métodos de seleção de seqüências adequadas para sistemas QS-CDMA

Este capítulo está dividido em três partes. A primeira parte descreve os seguintes métodos de obtenção de famílias de seqüências quase ortogonais generalizadas: QS, Lin-Chang e LCZ-GMW binária. São também apresentadas características dessas seqüências como: funções de correlação, número de seqüências em uma família e zona de correlação reduzida. Para auxiliar o estudo dessas famílias de seqüências, no apêndice B.1 é feita uma revisão sobre corpos finitos.

Inicialmente, serão descritas as seqüências de máximo comprimento (SMC) e a família de Gold, da qual é derivada a família QS. A seqüência GMW também é estudada, pois é a base para a construção das famílias Lin-Chang e LCZ-GMW binária. A primeira parte do capítulo 2 é encerrada com a família No. Essa família, apesar de não ser quase ortogonal generalizada, é apresentada porque representa a generalização de SMC, seqüências GMW e da família pequena de Kasami.

A segunda parte deste capítulo descreve as famílias de seqüências ortogonais generalizadas OQS e ZCZ binária. Antes de descrever a família ZCZ binária, são apresentadas as seqüências Walsh-Hadamard, pois essas são casos particulares da família ZCZ binária. O estudo de famílias de seqüências ortogonais ou quase ortogonais generalizadas é complementado com o apêndice C, o qual descreve a família quase ortogonal generalizada LCZ-GMW polifásica e as famílias ortogonais generalizadas ZCZ quadrifásica, PS e SP.

Finalmente, a terceira parte deste capítulo faz comparações entre as metodologias de obtenção de famílias de seqüências quase ortogonais e ortogonais generalizadas. Para auxiliar a avaliação das famílias de seqüências, são apresentadas figuras de de-

sempenho em termos de taxa de erro de bit para o sistema modelado no capítulo anterior.

2.1 Seqüências quase ortogonais e quase ortogonais generalizadas

2.1.1 Seqüências de Máximo Comprimento (SMC)

Nesta seção é investigada algumas propriedades da classe de seqüências denominadas *Seqüências de Máximo Comprimento* (SMC), também conhecidas como *m*-sequences. Essas seqüências possuem propriedades pseudo-aleatórias[1] muito importantes para aplicações em sistemas de comunicações. Inicialmente, tratar-se-á apenas das SMC binárias, ou seja, seus elementos estão no corpo fundamental[2] $GF(q)$, com $q = 2$.

Uma SMC de grau m é uma seqüência binária que satisfaz uma recorrência linear cujo polinômio característico de grau m é primitivo (MCELIECE, 1987). O polinômio primitivo de grau m é um polinômio mínimo do elemento α, o qual é raiz primitiva de um corpo $GF(2^m)$, apêndice (B.1). Todo polinômo primitivo é irredutível, apêndice (B.1), e do Teorema B.1.3 a seqüência definida por[3] $s_t = Tr_1^m(\theta\alpha^t)$ tem período[4] $N = \text{ord}(\alpha)$. A ordem do elemento α é $2^m - 1$ pois α é raiz primitiva de $GF(2^m)$. Assim, tem-se que o período da SMC é $2^m - 1$. A seguir, as principais propriedades da SMC são enunciadas.

2.1.1.1 Principais propriedades da SMC

Uma propriedade muito importante das SMC é a da distribuição dos blocos de comprimento r. Por exemplo, a seqüência 1110000110000 possui um bloco-1 de comprimento 3, dois blocos-0 de comprimento 4 e um bloco-1 de comprimento 2. Determinar a distribuição dos blocos em uma seqüência de período pequeno é fácil, basta contar. Verificar-se-á a seguir que as SMC possuem a distribuição dos blocos bem determi-

[1] propriedades que fazem as SMC se comportarem como seqüências cujos elementos são escolhidos aleatoriamente.

[2] $GF(p)$ é a notação usual para o corpo finito D mod p, onde D é o conjunto fundamental e p um número primo (apêndice B.1.3)

[3] $Tr_m^n(\alpha)$ representa a função traço de α, a qual mapeia elementos de $GF(2^n)$ em elementos de $GF(2^m)$ (apêndice B.1.8).

[4] $\text{ord}(\alpha)$ representa a ordem do elemento α (apêndice B.1.3).

nada.

Da recorrência linear (equação B.47) tem-se que a SMC é gerada da combinação de m termos anteriores, chamados de grânulo-m. Por exemplo: considere a SMC $(s_0, s_1, ..., s_{N-1})$; um grânulo-m é definido como:

$$(s_t, s_{t+1}, ..., s_{t+m-1}), \quad \text{para } t = 0, 1, ..., N-1 \tag{2.1}$$

onde os índices de (2.1) são tomados mod N, se necessário.

Pode-se identificar o período da seqüência quando houver uma repetição de um dos grânulos-m. Como a SMC tem período $N = 2^m - 1$, verifica-se que uma SMC contém $2^m - 1$ grânulos-m distintos. Tais grânulos-m são dados por todas as combinações de (2.1), exceto o $(0, 0, ..., 0)$, pois uma soma de zeros resultará sempre em zero e a seqüência definida pela recorrência linear (B.47) deixa de ser periódica.

Com isso prova-se um importante Teorema para as SMC:

Teorema 2.1.1 *Cada um dos* $2^m - 1$ *grânulos-m, exceto o* $(0, 0, ..., 0)$*, em uma SMC de período* $N = 2^m - 1$ *ocorre apenas uma vez.*

Observa-se na figura B.1 (apêndice) que o número de coeficientes a_i iguais a 1 da recorrência linear (ou do polinômio característico) para uma SMC deve ser par, pois, se for ímpar, o grânulo-m dado por 11...1 aplicado na recorrência linear (B.47) resultará sempre em 1 e a seqüência deixa de ser periódica.

Então, tem-se que uma SMC não tem nenhum bloco-0 de comprimento m e apenas um bloco-1 de comprimento m. O único bloco-1 de comprimento m está cercado (delimitado) por 0. Assim, a subseqüência 011...10 de comprimento $m + 2$ aparecerá apenas uma vez na SMC. Em conseqüência, aparecerão os grânulos 011...1 e 11...10. Se, na SMC, existir um bloco-1 de comprimento $m - 1$, este estará cercado por 0 e, em conseqüência, novamente, os grânulos 011...1 e 11...10 apareceriam novamente. Isso é contraditório ao Teorema 2.1.1, o que significa que em uma SMC não há blocos-1 de comprimento $m - 1$. Porém, ocorre um bloco-0 de comprimento $m - 1$, devido aos grânulos-m 100...0 e 00...01, os quais ocorrem em seqüência e apenas uma vez cada, conforme o Teorema 2.1.1.

Observe que os blocos de comprimento $r \leq m - 2$ aparecerão nos grânulos-m na forma:

$$\overbrace{0\underbrace{11\ldots1}_{r}0\underbrace{xx\ldots x}_{m-r-2}}^{m} \tag{2.2}$$

onde $x \in \{0,1\}$.

De (2.2) tem-se que o número de grânulos-m contendo um bloco-1 de comprimento $r \leq m-2$ é 2^{m-r-2}. Assim, o número de blocos-1 de comprimento $r \leq m-2$ em uma SMC é 2^{m-r-2}. Analogamente, o número de blocos-0 de comprimento $r \leq m-2$ em uma SMC é 2^{m-r-2}.

Com os comentários anteriores prova-se o Teorema da distribuição dos blocos em uma SMC:

Teorema 2.1.2 *A distribuição dos blocos em uma SMC de período N é dada pela Tabela 2.1.*

comprimento	blocos-0	blocos-1
1	2^{m-3}	2^{m-3}
2	2^{m-4}	2^{m-4}
$\vdots$	$\vdots$	$\vdots$
r	2^{m-r-2}	2^{m-r-2}
$\vdots$	$\vdots$	$\vdots$
$m-2$	1	1
$m-1$	1	0
m	0	1
Total:	2^{m-2}	2^{m-2}

Tabela 2.1: Distribuição dos blocos em uma SMC.

Observe na Tabela 2.1 que o número de elementos 1 em uma SMC supera em uma unidade o número de elementos 0. Então, uma SMC de período $N = 2^m - 1$ possui 2^{m-1} elementos 1 e $2^{m-1} - 1$ elementos 0.

As funções de correlação definidas na seção 1.1 consideram seqüências compostas de elementos de módulo unitário. Para se obter tal característica a partir de seqüências sobre $GF(p)$, faz-se:

$$c_t = \exp\left(\sqrt{-1}\frac{2\pi}{p}s_t\right) \tag{2.3}$$

Assim, $\mathbf{c} = \{c_t\}$ é uma seqüência composta de elementos tais que $|c_t| = 1$.

Outra propriedade importante da SMC é sobre a sua função de autocorrelação periódica par dada por:

$$\begin{aligned}\theta(\mathbf{c},\mathbf{c},\tau) &= \sum_{t=0}^{N-1}(-1)^{Tr(\theta\alpha^t)+Tr(\theta\alpha^{t+\tau})} \\ &= \sum_{t=0}^{N-1}(-1)^{Tr(\theta\alpha^t(1+\alpha^\tau))} \end{aligned} \tag{2.4}$$

onde foi utilizado a propriedade 2 do traço, seção B.1.8.

Se $\tau \equiv 0 \,(\mathrm{mod}\, N)$, $Tr(\theta\alpha^t(1+1)) = Tr(0) = 0$. Então, $\theta(\mathbf{c},\mathbf{c},\tau) = N$, para $\tau = 0 \,(\mathrm{mod}\, N)$.

Se $\tau \not\equiv 0 \,(\mathrm{mod}\, N)$, tem-se que $1+\alpha^\tau \neq 0$. Observe que $1+\alpha^\tau$ é um elemento α^σ de $GF(2^m)$, com $\sigma \in \{1,2,...,N-1\}$ e α o elemento primitivo do $GF(2^m)$. Adicionalmente, existe apenas um σ que satisfaz $1+\alpha^\tau = \alpha^\sigma$. Assim, $Tr(\theta\alpha^t(1+\alpha^\tau)) = Tr(\theta\alpha^{t+\sigma})$, ou seja, é uma SMC com fase $\theta\alpha^\sigma$. Como o número de elementos 1 em uma SMC supera em uma unidade o número de elementos 0, tem-se que $\theta(\mathbf{c},\mathbf{c},\tau) = -1$, para $\tau \neq 0 \,(\mathrm{mod}\, N)$.

Assim prova-se duas importantes propriedades da SMC. Uma para a função de autocorrelação da SMC, descrita pelo Teorema 2.1.3, e outra descrita pelo Teorema 2.1.4.

Teorema 2.1.3 *A função de autocorrelação periódica par de uma SMC é dada por:*

$$\theta(\boldsymbol{c},\boldsymbol{c},\tau) = \begin{cases} -1 & \text{se } \tau \not\equiv 0 \,(\mathrm{mod}\, N) \\ N & \text{se } \tau \equiv 0 \,(\mathrm{mod}\, N) \end{cases} \tag{2.5}$$

Nota-se que esse comportamento é válido também para uma seqüência de n elementos, os quais são variáveis aleatórias independentes e identicamente distribuídas.

Teorema 2.1.4 *Seja* (s_t) *uma SMC de período* $N = 2^m - 1$. *Então, para qualquer* $\tau \not\equiv 0 \,(\mathrm{mod}\, N)$ *existe um único inteiro* σ, *com* $1 \leq \sigma \leq N-1$, *tal que:*

$$s_t + s_{t+\tau} = s_{t+\sigma} \tag{2.6}$$

Por fim, será mostrado que existem exatamente[5] $\phi(2^m-1)/m$ SMC distintas de

[5] $\phi(.)$ representa a função de Euler (apêndice B.1.6).

período $2^m - 1$, bem como algumas formas de obtê-las.

Se duas SMC de mesmo período distinguem-se por apenas uma fase, ou translação, elas são equivalentes. De outra forma, foram geradas de uma mesma recorrência linear. Assim, para duas SMC serem distintas, ou uma não ser o resultado da translação da outra, elas devem ser geradas de recorrências lineares diferentes. Então, SMC distintas possuem seus respectivos polinômios característicos distintos.

Conclui-se, portanto, que o número de SMC distintas de mesmo período $N = 2^m - 1$ é dado pelo número de polinômios primitivos de grau m, pois os polinômios característicos das SMC devem ser primitivos. Esse número é dado pela função de Euler com argumento $2^m - 1$ dividido por m, $\phi(2^m - 1)/m$, seção B.1.6.

A SMC dada por $s_t = Tr(\theta\alpha^t)$, onde α é o elemento primitivo do corpo $GF(2^m)$ ou $D \bmod p$, com[6] $D = F_2[x]$ e $p(x)$ um polinômio primitivo de grau m, será distinta da SMC dada por $r_t = Tr(\theta\beta^t)$, onde β é o elemento primitivo do corpo $GF(2^m)$ ou $D \bmod h$, com $D = F_2[x]$ e $h(x)$ um polinômio primitivo de grau m, se e somente se $h(x)$ for distinto de $p(x)$.

Há outra forma de obter SMC distintas. Inicialmente, obtém-se os polinômios mínimos dos elementos do corpo $GF(2^m)$ que gerou a SMC. Para algum elemento α^d, entre outro(s) para $m > 2$, seu polinômio mínimo será de grau m e primitivo. Construindo um novo corpo $GF'(2^m)$ com esse polinômio primitivo, obtém-se uma SMC, distinta da original, pelo traço (foi assumido a fase $\theta = 1$ para simplificar a notação):

$$r_t = Tr(\beta^t) \tag{2.7}$$

onde β é o elemento primitivo do novo corpo $GF'(2^m)$, ou $\beta = \alpha^d$, com α o elemento primitivo do corpo original $GF(2^m)$. Assim:

$$r_t = Tr(\alpha^{dt}) \tag{2.8}$$

Conclui-se que basta decimar a SMC original de d para obter a nova SMC:

[6] $F_p[x]$ é o conjunto de polinômios no indeterminado x com coeficientes no corpo finito $F_p = \mathbb{Z} \bmod p$ (apêndice B.1.3).

$$r_t = s_{td}, \quad \text{para todo } t \geq 0 \tag{2.9}$$

Essa decimação, que resulta em outra SMC, é chamada de decimação própria.

Observe-se que, se d for tal que o polinômio mínimo de α^d for um polinômio primitivo de $GF(2^k)$ com $k < m$, a decimação conforme (2.9) resulta em uma SMC de período $N' = 2^k - 1$ menor que $N = 2^m - 1$. Agora, considere d tal que o polinômio mínimo de α^d não é um polinômio primitivo. Ou seja, α^d não gera um grupo cíclico $GF(2^m)^* = GF(2^m) - \{0\}$ e portanto não é raiz primitiva. Como α^d não gera um grupo cíclico $GF(2^m)^*$, a ordem de α^d é menor que $N = 2^m - 1$ e do Teorema B.1.3 tem-se que o período da seqüência gerada não será máximo $(2^m - 1)$ e, portanto, não será uma SMC. O período N' dessa seqüência cujo polinômio característico não é primitivo é diretamente obtido do Lema[7] B.1.1, $N' = \text{ord}(\alpha^d) = \text{ord}(\alpha)/\text{mdc}(d, \text{ord}(\alpha)) = N/\text{mdc}(d, N)$. Essa decimação, que resulta em outra seqüência que não é SMC, é chamada de decimação imprópria. O período da seqüência decimada é obtido do período da seqüência original e da decimação utilizada. Como resultado, tem-se que em uma decimação própria, o máximo divisor comum entre a decimação e o comprimento da SMC é 1, $\text{mdc}(d, N) = 1$. Assim, tem-se que as decimações próprias são elementos dos coconjuntos próprios do subgrupo $\{1, 2, 4, 8, ..., 2^m - 1\}$ e as decimações impróprias são elementos dos coconjuntos impróprios desse mesmo subgrupo.

2.1.1.2 Propriedades de correlação cruzada de SMC

Considere as duas SMC:

$$\begin{aligned} x_t &= Tr(\alpha^t) \\ y_t &= Tr(\alpha^{dt}) \end{aligned} \tag{2.10}$$

onde α é uma raiz primitiva de $GF(2^m)$ e d é qualquer inteiro na faixa $\{1, 2, ..., N - 1\}$ e primo relativo à N.

A função de correlação cruzada periódica par para essas duas SMC é dada por:

[7] $\text{mdc}(x, y)$ representa o máximo divisor comum entre x e y.

$$\theta(\mathbf{x}, \mathbf{y}, \tau) = \sum_{t=0}^{N-1} (-1)^{Tr(\alpha^{t-\tau} + \alpha^{dt})} \tag{2.11}$$

Substituindo $\alpha^{-\tau}$ por β e observando que na medida que t percorre de 0 a $N-1$, α^t percorre todos os elementos não nulos de $GF(2^m)$, obtém-se:

$$\theta(\mathbf{x}, \mathbf{y}, \tau) = \sum_{x \neq 0} (-1)^{Tr(\beta x + x^d)} \tag{2.12}$$

onde $\beta = \alpha^{-\tau}$.

Desenvolver a expressão (2.12) para obter o espectro de correlação[8] é uma tarefa complexa do ponto de vista matemático. Um resultado conhecido e muito importante foi obtido para $d = 2^e + 1$. Como visto anteriormente, uma decimação $d = 2^e + 1$ de uma SMC só resultará em outra SMC se $\text{mdc}(2^e + 1, 2^m - 1) = 1$. O apêndice B.2 mostra que $\text{mdc}(2^e + 1, 2^m - 1) = 1$ se e somente se $\text{mdc}(2e, m) = \text{mdc}(e, m)$.

Se $Tr(\beta x + x^d) = 0$ tiver M soluções em $GF(2^m)$, o argumento do somatório de (2.12) será 1 por $M - 1$ vezes, desconsiderando a solução $x = 0$, e -1 por $2^m - M$ vezes. Então, tem-se que $\theta(\mathbf{x}, \mathbf{y}, \tau) = (M - 1) - (2^m - M) = 2M - 2^m - 1$. Observa-se, portanto, que obtendo-se as soluções de:

$$F(x) = Tr(\beta x + x^d) = Tr(\beta x) + Tr(x^d) = 0 \tag{2.13}$$

caracteriza-se o espectro de correlação cruzada par discreta das SMC x_t e y_t previamente definidas.

A função $Tr(\beta x)$ é linear, então, pode ser representada por:

$$Tr(\beta x) = \mathbf{x} \cdot \mathbf{b} \tag{2.14}$$

onde $\mathbf{x}$ é a representação vetorial de x e $\mathbf{b} = (b_0, b_1, ..., b_{m-1})$ um vetor não nulo.

Em relação ao outro termo de (2.13), $Tr(x^d)$, pode-se fazer a expansão binária $d = d_0 + 2d_1 + 4d_2 + ... + 2^{m-1}d_{m-1}$, $d_k \in \{0; 1\}$ e então:

$$x^d = \prod_{k=0}^{m-1} (x^{2^k})^{d_k} \tag{2.15}$$

[8] número de ocorrências de cada valor assumidos por $\theta(\mathbf{x}, \mathbf{y}, \tau)$ para $0 \leq \tau < N$.

Observe que para qualquer inteiro k, o mapeamento $x \rightarrow x^{2^k}$ de $GF(2^m)$ no próprio corpo é linear (verificado na equação (B.27)):

$$\begin{aligned} x^{2^k} &= (x_0 + x_1\alpha + x_2\alpha^2 + ... + x_{m-1}\alpha^{m-1})^{2^k} \\ &= x_0 + x_1\alpha^{2^k} + x_2\alpha^{2^{k+1}} + ... + x_{m-1}\alpha^{2^k(m-1)} \end{aligned} \tag{2.16}$$

onde α é uma raiz primitiva de $GF(2^m)$.

Em representação vetorial de x, $\mathbf{x} = (x_0, x_1, ..., x_{m-1})$, o mapeamento será:

$$\mathbf{x} \rightarrow \mathbf{x}Q_k \tag{2.17}$$

onde Q_k é uma matriz $m \times m$ não singular e $\mathbf{x}Q_k$ é a representação vetorial de x^{2^k}. Então, cada componente da representação vetorial de x^{2^k} é uma função linear dos componentes de $\mathbf{x}$.

De (2.15) tem-se que $x \rightarrow x^d$ é o produto de $w(d)$ funções lineares de x, onde $w(d)$ denota o número de uns na expansão binária de d. Como o operador traço é simplesmente um produto escalar (2.14), tem-se que cada um dos m componentes da representaçao vetorial de $Tr(x^d)$ é uma função Booleana de grau no máximo $w(d)$ das m variáveis Booleanas $x_0, x_1, ..., x_{m-1}$. Por exemplo: para o caso de $d = 2^e + 1$, a expansão binária de d será:

$$d = d_0 + 2^e d_e, \quad \text{com } d_0 = d_e = 1 \tag{2.18}$$

Assim, $w(d) = 2$. E o $Tr(x^d)$:

$$\begin{aligned} Tr(x^d) &= Tr\left((x^{2^0})(x^{2^e})\right) \\ &= Tr\left((x_0 + x_1\alpha + ... + x_{m-1}\alpha^{m-1})(x_0 + x_1\alpha + ... + x_{m-1}\alpha^{m-1})^{2^e}\right) \\ &= Tr\left((x_0 + x_1\alpha + ... + x_{m-1}\alpha^{m-1})(x_0 + x_1\alpha^{2^e} + ... + x_{m-1}\alpha^{2^e(m-1)})\right) \\ &= Tr\left((x_0^2 + x_0x_1\alpha + ... + x_0x_{m-1}\alpha^{m-1}) + \right. \\ &+ (x_1x_0 + x_1^2\alpha + ... + x_1x_{m-1}\alpha^{m-1})\alpha^{2^e} + ... + \\ &+ \left.(x_{m-1}x_0 + x_{m-1}x_1\alpha + ... + x_{m-1}^2\alpha^{m-1})\alpha^{2^e(m-1)}\right) \end{aligned} \tag{2.19}$$

ou seja, uma função Booleana de grau no máximo 2 das variáveis Booleanas $x_0, x_1, ..., x_{m-1}$.

Para analisar o termo $Tr(x^d)$ de (2.13) na condição de $d = 2^e + 1$, é necessário utilizar algumas propriedades de polinômios quadráticos nos indeterminados $x_1, x_2, ..., x_m$ sobre um corpo finito. Essas propriedades estão demonstradas no Anexo B.3.

Conforme (2.13), para obter o espectro de correlação cruzada de x_t e y_t com $d = 2^e + 1$ em (2.10), deve-se calcular o número de soluções em $GF(2^m)$ da equação:

$$F(x) = Tr(x^{1+2^e}) + Tr(\beta x) = 0 \tag{2.20}$$

Do Corolário B.3.3, tem-se que o termo $Tr(x^{1+2^e})$ de $F(x) = 0$ pode ser transformado em $x_1x_2 + ... + x_{2s-1}x_{2s}$ ou $x_1x_2 + ... + x_{2s-1}x_{2s} + x_{2s+1}$ ou ainda $x_1x_2 + ... + x_{2s-1}x_{2s} + x_{2s-1} + x_{2s}$. O outro termo $Tr(\beta x)$ é linear (conforme (2.14)), assim, pode ser transformado em $a_1x_1 + a_2x_2 + ... + a_mx_m$. Então, $F(x) = 0$ será transformado em:

$$x_1x_2 + ... + x_{2s-1}x_{2s} + a_1x_1 + a_2x_2 + ... + a_mx_m = 0 \tag{2.21}$$

onde $x_1, x_2, ..., x_m$ assumem apenas os valores 0 e 1, pois são os coeficientes da representação vetorial de um elemento de $GF(2^m)$; $s = \lfloor r/2 \rfloor$, onde r é o *rank*[9] da forma quadrática representada por $Tr(x^{1+2^e})$. Observa-se que para um valor fixo de s, cada escolha de $(a_1, a_2, ..., a_m)$ resulta em uma equação (2.21) diferente. Assim, existem 2^m equações na forma de (2.21) para um valor fixo de s.

Considere o caso de $a_i = 1$ para algum $i > 2s$. Existem $2^m - 2^{2s}$ opções diferentes para $(a_1, a_2, ..., a_m)$. No total são 2^m opções de $(a_1, a_2, ..., a_m)$ e 2^{2s} opções em que $(a_1, a_2, ..., a_m) = (a_1, a_2, ..., a_{2s}, 0, 0, ..., 0)$, restando, então, $2^m - 2^{2s}$ opções em que $a_i = 1$ para algum $i > 2s$. Nesse caso, (2.21) poderá ser escrito como:

$$f(x_1, x_2, ..., x_{i-1}, x_{i+1}, ..., x_m) + x_i = 0 \tag{2.22}$$

onde x_i não é argumento de $f(.)$. Então, para cada escolha do argumento de $f(x_1, x_2, ..., x_{i-1}, x_{i+1}, ..., x_m)$, ou seja, os 2^{m-1} coeficientes x exceto o x_i, haverá exatamente um x_i que satisfaz (2.22), pois $f(x_1, x_2, ..., x_{i-1}, x_{i+1}, ..., x_m) = 0$ ou 1. Então, o número de

[9] *rank* de uma forma quadrática Q é definido como o número de variáveis no qual Q pode ser expresso através de transformações lineares não singulares de variáveis (apêndice B.3). O apêndice B.3 apresenta um resumo sobre formas quadráticas sobre um corpo finito.

soluções de (2.21) no caso de $a_i = 1$ para algum $i > 2s$ é 2^{m-1}.

Considere agora o caso $a_{2s+1} = a_{2s+2} = ... = a_m = 0$. Conforme já mencionado, existem 2^{2s} possibilidades para $(a_1, a_2, ..., a_m) = (a_1, a_2, ..., a_{2s}, 0, 0, ..., 0)$. Nesse caso, (2.21) resulta:

$$x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + a_1x_1 + a_2x_2 + ... + a_{2s}x_{2s} = 0 \tag{2.23}$$

Realizando-se a transformação:

$$y_1 = x_1 + a_2,\ y_2 = x_2 + a_1,\ y_3 = x_3 + a_4,\ y_4 = x_4 + a_3,\ etc. \tag{2.24}$$

tem-se:

$$\begin{aligned} y_1y_2 + y_3y_4 + ... + y_{2s-1}y_{2s} + a_1a_2 + a_3a_4 + ... + a_{2s-1}a_{2s} = 0 \\ y_1y_2 + y_3y_4 + ... + y_{2s-1}y_{2s} = a \end{aligned} \tag{2.25}$$

onde $a = a_1a_2 + a_3a_4 + ... + a_{2s-1}a_{2s}$.

Observa-se que em (2.25) a pode ser 1 ou 0. Considerando $a = 0$, tem-se a equação:

$$y_1y_2 + y_3y_4 + ... + y_{2s-1}y_{2s} = 0 \tag{2.26}$$

Define-se N_s o número de soluções $(y_1, y_2, ..., y_{2s})$ de (2.26). Observe que N_s representa o número de equações do tipo (2.21) com $a_{2s+1} = a_{2s+2} = ... = a_m = 0$ e $a_1a_2 + a_3a_4 + ... + a_{2s-1}a_{2s} = 0$. Fazendo a contagem exaustiva, obtém-se:

$$N_1 = 3, N_2 = 10, N_3 = 36, ... \tag{2.27}$$

Se N_s é o número de soluções para (2.26), então, N_{s+1} é o número de soluções para:

$$y_1y_2 + y_3y_4 + ... + y_{2s-1}y_{2s} = y_{2s+1}y_{2s+2} \tag{2.28}$$

Observe que na equação acima, $y_1y_2 + y_3y_4 + ... + y_{2s-1}y_{2s}$ será zero em N_s formas (por definição). Para cada uma dessas formas, $y_{2s+1}y_{2s+2}$ será zero em três formas, $0 \cdot 0$, $0 \cdot 1$ e $1 \cdot 0$. Em contrapartida, $y_1y_2 + y_3y_4 + ... + y_{2s-1}y_{2s}$ será 1 em $2^{2s} - N_s$ formas e $y_{2s+1}y_{2s+2}$ será 1 em apenas uma forma. Então, o número de soluções de (2.28) é:

$$\begin{aligned} N_{s+1} &= 3 \times N_s + (2^{2s} - N_s) \\ N_{s+1} &= 2N_s + 2^{2s} \end{aligned} \tag{2.29}$$

e o número de soluções N_s de (2.26) será:

$$N_s = 2N_{s-1} + 2^{2s-2} \tag{2.30}$$

Para obter uma expressão geral de N_s em termos de um N_{s-j} genérico, expande-se (2.30):

$$\begin{aligned} N_s &= 2N_{s-1} + 2^{2s-2} \\ &= 2(2N_{s-2} + 2^{2s-4}) + 2^{2s-2} \\ &= 4N_{s-2} + 2^{2s-2} + 2^{2s-3} \\ &= 4(2N_{s-3} + 2^{2s-6}) + 2^{2s-2} + 2^{2s-3} \\ &= 8N_{s-3} + 2^{2s-2} + 2^{2s-3} + 2^{2s-4} \\ &= 8(2N_{s-4} + 2^{2s-8}) + 2^{2s-2} + 2^{2s-3} + 2^{2s-4} \\ N_s &= 16N_{s-4} + 2^{2s-2} + 2^{2s-3} + 2^{2s-4} + 2^{2s-8} \end{aligned} \tag{2.31}$$

Observando-se o comportamento de N_s em (2.31), pode-se escrever:

$$N_s = 2^j N_{s-j} + 2^{2s} \sum_{i=2}^{j+1} 2^{-i} \tag{2.32}$$

Fazendo $j = s$, tem-se:

$$N_s = 2^s N_0 + 2^{2s} \sum_{i=2}^{s+1} 2^{-i} \tag{2.33}$$

De (2.30) e (2.27) tem-se $N_0 = N_1/2 - 1/2 = 3/2 - 1/2 = 1$. Assim:

$$N_s = 2^s + 2^{2s} \sum_{i=2}^{s+1} 2^{-i} \tag{2.34}$$

O termo $\sum_{i=2}^{s+1} 2^{-i} = \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + ... + \frac{1}{2^{s+1}}$ é uma série geométrica com termo inicial $b = \frac{1}{2^2}$, razão $r = \frac{1}{2}$ e termo final $\frac{1}{2^{s+1}} = \frac{1}{2^2}\frac{1}{2^{s-1}} = b \cdot r^{s-1}$. Uma série geométrica finita tem como resultado $\frac{b(1-r^s)}{1-r}$. Assim:

$$\sum_{i=2}^{s+1} 2^{-i} = \frac{2^{-2}(1 - 2^{-s})}{1 - 2^{-1}} = 2^{-1} - 2^{-1-s} \tag{2.35}$$

Substituindo (2.35) em (2.34) obtém-se:

$$\begin{aligned} N_s &= 2^s + 2^s(2^{-1} - 2^{-1-s}) \\ &= 2^s + 2^{2s-1} - 2^{s-1} \\ &= 2^{2s-1} + 2^s(1 - 2^{-1}) \\ N_s &= 2^{2s-1} + 2^{s-1} \end{aligned} \tag{2.36}$$

Se $N_s = 2^{2s-1} + 2^{s-1}$ é o número de soluções $(y_1, y_2, ..., y_{2s})$ para (2.26), o número de soluções $(y_1, y_2, ..., y_m)$ para a transformação (2.24) de (2.21) para o caso $a_{2s+1} = a_{2s+2} = ... = a_m = 0$ e $a = a_1a_2 + a_3a_4 + ... + a_{2s-1}a_{2s} = 0$ será $2^{m-2s}N_s = 2^{m-1} + 2^{m-s-1}$. Isso porque para cada solução $(y_1, y_2, ..., y_{2s})$ para (2.26), irão existir 2^{m-2s} soluções $(y_1, y_2, ..., y_m)$ de (2.21) para o caso $a_{2s+1} = a_{2s+2} = ... = a_m = 0$.

Considerando ainda o caso de $a_{2s+1} = a_{2s+2} = ... = a_m = 0$, porém agora com $a = 1$ em (2.25). Se existem N_s vetores $(y_1, y_2, ..., y_{2s})$ tais que $y_1y_2 + ... + y_{2s-1}y_{2s} = 0$, existem $2^{2s} - N_s = 2^{2s-1} - 2^{s-1}$ vetores $(y_1, y_2, ..., y_{2s})$ tais que $y_1y_2 + ... + y_{2s-1}y_{2s} = 1$. Assim, o número de equações do tipo (2.21) com $a_{2s+1} = a_{2s+2} = ... = a_m = 0$ e $a_1a_2 + a_3a_4 + ... + a_{2s-1}a_{2s} = 1$ será $2^{2s-1} - s^{s-1}$. Adicionalmente, o número de soluções $(y_1, y_2, ..., y_{2s})$ para (2.25) com $a_1 = 1$ será $2^{2s} - N_s = 2^{2s-1} - 2^{s-1}$. Em conseqüência, o número de soluções $(y_1, y_2, ..., y_m)$ de (2.21) para o caso $a_{2s+1} = a_{2s+2} = ... = a_m = 0$ e $a = a_1a_2 + a_3a_4 + ... + a_{2s-1}a_{2s} = 1$ será $2^{m-2s}(2^{2s} - N_s) = 2^{m-1} - 2^{m-s-1}$.

Relembrando o que foi feito até aqui para obter o número de soluções $F(x) = 0$,

equação (2.20). O problema foi separado em dois casos, com respeito aos coeficientes a_i de (2.21):

1. $a_i = 1$ para algum $i > 2s$.

2. $a_{2s+1} = a_{2s+2} = ... = a_m = 0$.

Para o primeiro caso, verificou-se que existem $2^m - 2^{2s}$ formas de escolher $(a_1, ..., a_m)$ em (2.21) que resultem em equações do tipo do caso 1. Adicionalmente, para cada uma dessas equações existem 2^{m-1} soluções.

Para o segundo caso, (2.21) foi transformado em $y_1y_2 + ... + y_{2s-1}y_{2s} = a$. Ainda no segundo caso, $y_1y_2 + ... + y_{2s-1}y_{2s} = a$ foi separado nos casos de $a = 0$ e $a = 1$. Para o caso de $a = 0$, verificou-se que existem $N_s = 2^{2s-1} + 2^{s-1}$ vetores $(y_1, y_2, ..., y_{2s})$ para os quais $y_1y_2 + ... + y_{2s-1}y_{2s} = 0$. Em conseqüência desse resultado, existem $2^{m-2s}N_s = 2^{m-1} + 2^{m-s-1}$ soluções para (2.21), no caso de $a = 0$. No caso de $a = 1$, verificou-se que existem $2^{2s} - N_s = 2^{2s-1} - 2^{s-1}$ vetores $(y_1, y_2, ..., y_{2s})$ para os quais $y_1y_2 + ... + y_{2s-1}y_{2s} = 1$. Em conseqüência desse resultado, existem $2^{m-2s}(2^{2s} - N_s) = 2^{m-1} - 2^{m-s-1}$ soluções para (2.21), no caso de $a = 1$.

A partir desses resultados, segue-se o Teorema:

Teorema 2.1.5 *O número de soluções de (2.21) segue a tabela abaixo:*

no. de soluções	*no. de equações*
2^{m-1}	$2^m - 2^{2s}$
$2^{m-1} + 2^{m-s-1}$	$2^{2s-1} + 2^{s-1}$
$2^{m-1} - 2^{m-s-1}$	$2^{2s-1} - 2^{s-1}$

Para determinar o espectro de $\theta(\mathbf{x}, \mathbf{y}, \tau)$ (2.12) no caso de $d = 1+2^e$, será necessário identificar o parâmetro s do Teorema 2.1.5. Do Corolário B.3.3 tem-se que $s = \lfloor r/2 \rfloor$ e r é o *rank* da forma quadrática:

$$Q_e(x) = Tr(x^{1+2^e}) \tag{2.37}$$

Conforme mostrado no início da seção, a decimação $d = 2^e + 1$ da SMC resultará em outra SMC se e somente se $\text{mdc}(m, 2e) = \text{mdc}(m, e)$. Para esse caso, tem-se:

$$rank(Q_e) = m - \text{mdc}(m, 2e) + 1 \tag{2.38}$$

Para provar (2.38) será calculado o tamanho do conjunto Y_e, definido por:

$$Y_e = \left\{ y \in GF(2^m) : Tr\left((x+y)^{2^e+1}\right) = Tr(x^{2^e+1}), \text{ para todo } x \in GF(2^m) \right\} \tag{2.39}$$

Observe que o conjunto Y_e é o conjunto de elementos $y \in GF(2^m)$ tais que a condição $Tr\left((x+y)^{2^e+1}\right) = Tr(x^{2^e+1})$, o qual de (2.37) equivale a $Q_e(x+y) = Q_e(x)$, é satisfeita para todo $x \in GF(2^m)$. Do Corolário B.3.4, tem-se que o número de elementos $y \in GF(2^m)$ que satisfaz $Q_e(x+y) = Q_e(x)$ para todo $x \in GF(2^m)$ é igual a 2^{m-r}, onde r é o *rank* de $Q_e(x)$. Ou seja, o tamanho do conjunto Y_e é 2^{m-r}. Então, determinando-se o tamanho do conjunto Y_e obtém-se o *rank* de $Q_e(x)$.

Faz-se a expansão de $Tr\left((x+y)^{2^e+1}\right)$:

$$\begin{aligned} Tr\left((x+y)^{2^e+1}\right) &= Tr\left((x+y)^{2^e}(x+y)\right) \\ &= Tr\left((x^{2^e}+y^{2^e})(x+y)\right) \\ &= Tr\left(x^{2^e+1} + x^{2^e}y + xy^{2^e} + y^{2^e+1}\right) \\ &= Tr(x^{2^e+1}) + Tr(x^{2^e}y) + Tr(xy^{2^e}) + Tr(y^{2^e+1}) \end{aligned} \tag{2.40}$$

Como $Tr(\alpha) = Tr(\alpha^{2^e})$, conforme a propriedade 4 da função traço (seção B.1.8), o termo $Tr(xy^{2^e})$ equivale a $Tr(x^{2^e}y^{2^{2e}})$. Assim, (2.40) torna-se:

$$Tr\left((x+y)^{2^e+1}\right) = Tr\left(x^{2^e+1} + x^{2^e}(y+y^{2^{2e}}) + y^{2^e+1}\right) \tag{2.41}$$

Então, a equação da definição (2.39):

$$Tr\left((x+y)^{2^e+1}\right) = Tr(x^{2^e+1}) \tag{2.42}$$

implica em:

$$Tr\left(x^{2^e}(y+y^{2^{2e}})\right) = Tr(y^{2^e+1}) \tag{2.43}$$

Portanto, o conjunto Y_e (2.39) é o conjunto de $y \in GF(2^m)$ tal que (2.43) é satisfeito para todo $x \in GF(2^m)$.

Observa-se que se $y+y^{2^{2e}} \neq 0$ em (2.43) e x percorrer todo o $GF(2^m)$ exceto o zero, o lado esquerdo de (2.43) equivale a uma SMC e, portanto, será "zero" $2^{m-1} - 1$ vezes e "um" 2^{m-1} vezes. Se x assumir também o valor zero, $Tr(0) = 0$, o lado esquerdo de (2.43) no total será zero 2^{m-1} vezes e um 2^{m-1} vezes. Mas o lado direito de (2.43) não depende de x, o que é uma contradição da equação. Conclui-se que se (2.43) é satisfeito para todo $x \in GF(2^m)$, deve-se ter:

$$y = y^{2^{2e}} \tag{2.44}$$

Dessa forma, o lado esquerdo de (2.43) é identicamente zero. Então, para (2.43) ser satisfeita para todo x:

$$Tr(y^{2^e+1}) = 0 \tag{2.45}$$

Com essa análise, tem-se que o conjunto Y_e de (2.39) é exatamente o conjunto de y que satisfaz $y = y^{2^{2e}}$ e $Tr(y^{2^e+1}) = 0$, (2.44) e (2.45), respectivamente.

Observe que se $y = y^{2^{2e}}$ pode-se afirmar que $y \in GF(2^{2e})$, pois o corpo ao qual y pertence é um grupo cíclico.

Utilizando a propriedade de corpos finitos (MCELIECE, 1987):

$$GF(p^m) \cap GF(p^n) = GF(p^{\text{mdc}(m,n)}) \tag{2.46}$$

tem-se que:

$$y \in GF(2^{\text{mdc}(2e,m)}) \tag{2.47}$$

Como $y \in GF(2^{2e})$, se $y \neq 0$, tem-se que $y^{2^{2e}-1} \equiv y^{0 \bmod 2^{2e}-1} = 1$. Escrevendo de outra forma, $y^{2^{2e}-1} = y^{(2^e+1)(2^e-1)} = y^{(2^e+1)2^e} y^{-(2^e+1)} = 1$ resultando em $y^{(2^e+1)2^e} = y^{(2^e+1)}$. Isso implica em $y^{(2^e+1)} \in GF(2^e)$, novamente porque o corpo é um grupo cíclico. Como y também pertence a $GF(2^m)$, de (2.46) tem-se:

$$y^{2^e+1} \in GF(2^{\text{mdc}(e,m)}) \tag{2.48}$$

Define-se:

$$\begin{aligned} g &= \text{mdc}(2e, m) \\ h &= \text{mdc}(e, m) \end{aligned} \tag{2.49}$$

Os corpos $GF(2^{\text{mdc}(2e,m)})$ e $GF(2^{\text{mdc}(e,m)})$ em (2.47) e (2.48), respectivamente, são iguais se $g = h$ e distintos se $g = 2h$.

Considere o caso de $g = h$, caso de interesse. Considere y percorrendo todos os elementos de $GF(2^h)$. Se $y = \alpha^i \in GF(2^h)$, com α uma raíz primitiva de $GF(2^h)$, y percorre todos os elementos não nulos de $GF(2^h)$. A ordem da raiz primitiva α é $2^h - 1$, pois as potências de uma raiz primitiva geram um grupo cíclico, nesse caso, as $2^h - 1$ potências de α geram o grupo cíclico $GF(2^h) - \{0\}$. Se $y = \alpha^i$, tem-se que $y^{2^e+1} = (\alpha^{2^e+1})^i$. Sabendo que a ordem de α é $\text{ord}(\alpha) = 2^h - 1$, do Lema B.1.1, a ordem de α^{2^e+1} será $\text{ord}(\alpha^{2^e+1}) = 2^h - 1/\text{mdc}(2^e + 1, 2^h - 1)$. Então, para obter $\text{ord}(\alpha^{2^e+1})$ calcula-se

$$\begin{aligned} &\text{mdc}(2^e + 1, 2^h - 1) = \text{mdc}(2^e + 1, 2^{\text{mdc}(e,m)} - 1) = \\ &= \text{mdc}(2^e + 1, \text{mdc}(2^e - 1, 2^m - 1))|\text{mdc}(2^e + 1, 2^e - 1) \end{aligned} \tag{2.50}$$

como:

$$\text{mdc}(2^e + 1, 2^e - 1) = 1 \tag{2.51}$$

(a prova de (2.51) encontra-se no apêndice B.2), tem-se que:

$$\begin{aligned} &\text{mdc}(2^e + 1, 2^h - 1)|1 \\ &\text{mdc}(2^e + 1, 2^h - 1) = 1 \end{aligned} \tag{2.52}$$

Portanto, a ordem de α^{2^e+1} será igual à ordem de α, $\text{ord}(\alpha^{2^e+1}) = 2^h - 1$. Assim,

na medida que $y = \alpha^i \in GF(2^h)$ percorre todos os elementos não nulos de $GF(2^h)$, $y^{2^e+1} = (\alpha^{2^e+1})^i$ também percorre todos os elementos não nulos de $GF(2^h)$. Como conseqüência, $Tr(y^{2^e+1})$ será uma SMC e, portanto, resultará zero $2^{h-1} - 1$ vezes e resultará 1 por 2^{h-1} vezes. Considerando também $y = 0$, $Tr(y^{2^e+1})$ será zero 2^{h-1} vezes e 1 por 2^{h-1} vezes. Então, exatamente a metade dos elementos de $GF(2^h)$ irão satisfazer $Tr(y^{2^e+1}) = 0$, (2.45). Conclui-se que o tamanho do conjunto Y_e, nesse caso de $g = h$, será 2^{h-1}, ou seja, existem 2^{h-1} elementos $y \in GF(2^m)$ que satisfazem $Q_e(x + y) = Q_e(x)$ para todo $x \in GF(2^m)$. Do Corolário B.3.4 tem-se que $2^{h-1} = 2^{m-r}$, assim $r = rank(Q_e) = m - h + 1 = m - \text{mdc}(2e, m) + 1$, no caso de $g = h$. Assim, (2.38) está provada.

Recapitular-se-á toda a metodologia utilizada para obter o histograma da função de correlação cruzada periódica par discreta $\theta(\mathbf{x}, \mathbf{y}, \tau)$ das duas SMC $x_t = Tr(\alpha^t)$ e $y_t = Tr(\alpha^{dt})$, com $d = 2^e + 1$, sendo que $\text{mdc}(2^e + 1, 2^m - 1) = 1$, o que, conforme apêndice B.2, é possível quando $\text{mdc}(2e, m) = \text{mdc}(e, m)$. A expressão de $\theta(\mathbf{x}, \mathbf{y}, \tau)$ (2.11) foi parametrizada por $\beta = \alpha^t$, com α uma raiz primitiva fixa de $GF(2^m)$ (2.12). Foi verificado que (2.12) é igual à $2M - 2^m - 1$, onde M é o número de soluções de $F(x) = 0$ dado por (2.20) e (2.21). O Teorema 2.1.5 mostrou que existem somente três valores para M de acordo com os valores que β assume, além disso, apresentou a quantidade de valores de β que resulta em cada um dos valores de M. Porém, o Teorema 2.1.5 apresenta esses resultados em função de $s = \lfloor \frac{r}{2} \rfloor$, onde r é o *rank* da forma quadrática $Tr(x^{2^e+1})$, definida por (2.37) como $Q_e(x)$. A expressão (2.38) determina o *rank* de Q_e como $m - g + 1$, onde $g = \text{mdc}(2e, m)$.

Observa-se que se m for par, esse poderá ser fatorado em $m = 2 \times m_f$. Nesse caso, $g = \text{mdc}(2e, m) = \text{mdc}(2e, 2m_f) = 2\text{mdc}(e, m_f)$ o que, independente do valor de $\text{mdc}(e, m_f)$, será par. Conseqüentemente, $m - g$ será também par, pois se $m/2$ e $g/2$ resultam em inteiros, $(m - g)/2 = m/2 + g/2$ também será um inteiro. Agora, considere m um número ímpar. Nesse caso, m não terá nenhum fator par, pois se tiver, esse será divisível por 2 e, conseqüentemente, m será divisível por 2 também, contrariando a hipótese de m ímpar. Como m não possui fatores pares, $g = \text{mdc}(2e, m)$ será também ímpar. Um número ímpar pode ser escrito como um número par menos 1. Por exemplo, nesse caso, $m = m_e - 1$ e $g = g_e - 1$, com m_e e g_e números pares. Assim, $m - g = (m_e - 1) - (g_e - 1) = m_e - g_e$ o que é, como no caso anterior, uma subtração de números pares, o que resulta em um número par. Concluindo, não importa se m é par ou ímpar, $m - g$ sempre resultará em par. Portanto, se $r = m - g + 1$, tem-se

$s = \lfloor \frac{r}{2} \rfloor = (m-g)/2 + \lfloor 1/2 \rfloor = (m-g)/2$. Ou seja, $s = (m-g)/2$.

Substituindo $s = (m-g)/2$ no Teorema 2.1.5:

no. de soluções (M)	no. de equações
2^{m-1}	$2^m - 2^{(m-g)}$
$2^{m-1} + 2^{m/2+g/2-1}$	$2^{m-g-1} + 2^{(m-g)/2-1}$
$2^{m-1} - 2^{m/2+g/2-1}$	$2^{m-g-1} - 2^{(m-g)/2-1}$

No desenvolvimento para obter o número de soluções de $F(x) = 0$ (2.20), dado pela tabela anterior, foi considerado o caso de $\beta = 0$. Lembrando que $\beta = \alpha^{-\tau}$, onde τ é o argumento da função de correlação, não faz sentido β assumir valor nulo, pois, nesse caso, tem-se $\tau = \infty$. Assim, deve-se identificar e desconsiderar o caso em que $\beta = 0$.

Quando $\beta = 0$, tem-se $F(x) = Tr(x^{2^e+1}) + Tr(\beta x) = Q_e(x) = Tr(x^{2^e+1}) = 0$. Do corolário B.3.3, tem-se que $Q_e(x) = Tr(x^{2^e+1})$ pode ser transformado em uma das 3 formas quadráticas:

$$\begin{aligned} x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + x_{2s+1} \quad & \text{(caso de } rank\, r = 2s+1\text{)} \\ x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} \quad & \text{(caso de } rank\, r = 2s\text{)} \\ x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + x_{2s-1} + x_{2s} \quad & \text{(caso de } rank\, r = 2s\text{)} \end{aligned} \tag{2.53}$$

Observe que $\text{mdc}(2^e+1, 2^m-1) = 1$ deve ocorrer para que $Tr(x^d)$, com $d = 2^e+1$, seja uma SMC e que isso só é possível para $\text{mdc}(2e, m) = \text{mdc}(e, m)$, ou seja, $g = h$ (apêndice B.2). Assim, de (2.38), tem-se que o *rank* de $Q_e(x)$ será $m - \text{mdc}(2e, m) + 1 = m - g + 1$, o que é um número ímpar, pois $m - g$ sempre será par (conforme já discutido anteriormente nesta seção). Então, $Q_e(x)$ pode ser transformado em $x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + x_{2s+1}$, com $r = 2s+1 = m-g+1$, ou ainda, $x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + a_1x_1 + a_2x_2 + ... + a_{2s+1}x_{2s+1} + ... + a_mx_m$, com $a_1 = a_2 = ... = a_{2s} = 0$, $a_{2s+1} = 1$ e $a_{2s+2} = a_{2s+3} = ... = a_m = 0$. Assim, pode-se reescrever $Q_e(x) = f(x_1, x_2, ..., x_{2s}, x_{2s+2}, ..., x_m) + x_{2s+1} = 0$. Essa forma quadrática já foi analisada em (2.22) e foi verificado que possui 2^{m-1} soluções.

Com essa análise pode-se afirmar que no caso de $\beta = 0$ existem 2^{m-1} soluções para $F(x) = 0$. Então, deve-se descontar uma equação, referente ao caso $\beta = 0$,

na qual $F(x) = 0$ apresenta 2^{m-1} soluções. Assim, o número de soluções de (2.20), desconsiderando a equação com $\beta = 0$, será:

no. de soluções (M)	no. de equações
2^{m-1}	$2^m - 2^{(m-g)} - 1$
$2^{m-1} + 2^{m/2+g/2-1}$	$2^{m-g-1} + 2^{(m-g)/2-1}$
$2^{m-1} - 2^{m/2+g/2-1}$	$2^{m-g-1} - 2^{(m-g)/2-1}$

Sabendo que $\theta(\mathbf{x}, \mathbf{y}, \tau) = 2M - 2^m - 1$, prova-se um dos principais teoremas para as SMC:

Teorema 2.1.6 *O espectro de correlação entre uma SMC de comprimento* $N = 2^m - 1$ *e sua decimação* $d = 2^e + 1$, *onde obrigatoriamente* $\text{mdc}(2^m - 1, 2^e + 1) = 1$, *será:*

$\theta(\boldsymbol{x}, \boldsymbol{y}, \tau)$	*no. de vezes*
-1	$2^m - 2^{(m-g)} - 1$
$-1 + 2^{(m+g)/2}$	$2^{m-g-1} + 2^{(m-g)/2-1}$
$-1 - 2^{(m+g)/2}$	$2^{m-g-1} - 2^{(m-g)/2-1}$

A função de correlação par periódica entre uma SMC e sua (2^e+1)-ésima decimação será no máximo $1 + 2^{(m+1)/2}$, em módulo, se $g = 1$. Porém, em sistemas DS/CDMA reais, são necessárias muito mais do que duas seqüências para alocar todos os usuários. Em (GOLD, 1967) foi mostrado que é possível construir mais seqüências mantendo-se os valores de correlação cruzada periódica das SMC. A demonstração dessa característica é imediata, conhecidas as características das SMC. As seqüências propostas em (GOLD, 1967), conhecidas como seqüências de Gold, são apresentadas na seção seguinte juntamente com sua boa característica de correlação cruzada par periódica.

2.1.2 Família Gold

Considere $d = 2^e + 1$ e $x \in GF(2^m)$. Seja a seqüência $s_t(x)$ de comprimento $N = 2^m - 1$:

$$s_t(x) = Tr(\alpha^t + x\alpha^{dt}),\ 0 \leq t \leq N - 1 \tag{2.54}$$

Para cada um dos 2^m valores de $x \in GF(2^m)$ existe uma seqüência $s_t(x)$ diferente. Adicionando o valor $x = \infty$, onde será denotado:

$$s_t(\infty) = Tr(\alpha^{dt}) \tag{2.55}$$

tem-se no total $2^m + 1$ seqüências.

Sejam x e y elementos de $\{GF(2^m),\ \infty\}$. A função de correlação cruzada par periódica entre as seqüências $s_t(x)$ e $s_t(y)$ será:

$$\theta_{x,y}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_t(x)+s_{t+\tau}(y)} \tag{2.56}$$

onde $s_t(x) + s_{t+\tau}(y) = Tr(\alpha^t + \alpha^{t+\tau} + x\alpha^{dt} + y\alpha^{dt+d\tau})$ e, assim como foi feito em toda a seção anterior, obter $\theta_{x,y}(\tau)$ é equivalente a obter o número de inteiros t no intervalo $0 \leq t \leq N-1$ tais que:

$$Tr((1+\alpha^\tau)\alpha^t + (x + y\alpha^{d\tau})\alpha^{dt}) = 0 \tag{2.57}$$

Definindo $A = 1 + \alpha^\tau$, $B = x + y\alpha^{d\tau}$ e $z = \alpha^t$ tem-se:

$$Tr(Az + Bz^d) = 0 \tag{2.58}$$

Conforme a seção 2.1.1.2, onde foi analisada a equação (2.13) que é do mesmo tipo de (2.58), os valores de $\theta_{x,y}(\tau)$ serão $-1, -1 \pm 2^{(m+g)/2}$, onde $g = \text{mdc}(2e, m)$, para A e B diferentes de zero.

Se $A = 0$ e $B = 0$, tem-se $\alpha^\tau = 1$ e $x + y\alpha^{d\tau} = 0$. Porém, isso ocorrerá se e somente se $\tau \equiv 0 \ (\text{mod}N)$ e $x = y$. Nesse caso, obviamente, $\theta_{x,y}(\tau) = N$ (autocorrelação par periódica).

Assim, duas seqüências, $s_t(x)$ e $s_t(y)$, dentre as $2^m + 1$ definidas como (2.54), com $x, y \in \{GF(2^m),\ \infty\}$ e $d = 2^e + 1$ resultam em:

$$\theta_{x,y}(\tau) = \begin{cases} -1 \\ -1 \pm 2^{(m+g)/2} \end{cases} \tag{2.59}$$

sendo que, no caso $\tau \equiv 0 \ (\text{mod}N)$ e $x = y$, $\theta_{x,y}(\tau) = N$.

Se $g = \text{mdc}(2e, m) = 1$, têm-se os menores valores de correlação cruzada periódica par para as seqüências **x** e **y**. Nesse caso, as $2^m + 1$ seqüências definidas como (2.54),

com $x \in \{GF(2^m), \infty\}$ e $d = 2^e + 1$, são chamadas seqüências Gold. O conjunto composto pelas $2^m + 1$ seqüências é chamado família Gold.

De (2.54), observa-se que $s_t(x) = Tr(\alpha^t) + Tr(x\alpha^{dt})$, que é a soma de duas SMC. Na condição de $d = 2^e + 1$, com $\text{mdc}(2^e, m) = 1$, o par de SMC é chamado de par preferencial.

Denotando uma SMC como $c_t = Tr(\alpha^{dt})$, a outra SMC, $Tr(x\alpha^{dt})$, com $x = \alpha^s$ e $s = 0, 1, ..., 2^{m-2}$, será c_{t+s}. Então, a família Gold é composta pelo par preferencial de SMC (casos em que $x = 0$ e $x = \infty$ em (2.54)) e pelas seqüências resultantes das somas de uma das SMC $\mathbf{a} = \{a_t\} = \{Tr(\alpha^t)\}$ com a outra SMC $\mathbf{b} = \{b_t\} = \{Tr(x\alpha^{dt})\}$ para os $2^m - 1$ deslocamentos. Assim, pode-se obter o conjunto Gold da seguinte forma:

$$\begin{aligned} G &= \{\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3, ..., \mathbf{g}_{2^m+1}\} \\ &= \{\mathbf{a}, \mathbf{b}, \mathbf{a} + \mathbb{T}\mathbf{b}, \mathbf{a} + \mathbb{T}^2\mathbf{b}, ..., \mathbf{a} + \mathbb{T}^{2^m-1}\mathbf{b}\} \end{aligned} \tag{2.60}$$

Observa-se que **b** é uma decimação d de **a**. Então, pode-se representar o conjunto Gold pelo polinômio primitivo que gerou o corpo $GF(2^m)$ (do qual α é elemento primitivo) e pelo polinômio mínimo de α^d. Por exemplo, para o par preferencial $\{\mathbf{a}, \mathbf{b}\}$, **a** foi obtida do corpo $GF(2^m)$ construído com o polinômio $1 + x^3 + x^5$ ([100101] em notação binária e [45] em notação octal), e **b** resultou da decimação $d = 11$ de **a**, ou seja, do polinômio mínimo de α^d: $1 + x + x^2 + x^4 + x^5$ ([111011] em notação binária e [73] em notação octal). Nesse caso, representa-se a família Gold como $Gold(45, 73)$.

A seção seguinte irá apresentar uma família de seqüências derivada da família Gold.

2.1.3 Família QS

Os conjuntos de seqüências QS propostos em (KUNO et al., 1994) (SAITO et al., 2001) são compostos de seqüências de Gold adequadamente escolhidas de forma que a função de correlação periódica par $\theta(\mathbf{a}, \mathbf{b}, d)$ assuma valores mínimos $\theta_{mCZ} = 1$ para $d \leq L_{CZ}$.

Em (KUNO et al., 1994), foi mostrado que para cada valor assumido pela função de correlação cruzada periódica par $\theta(\mathbf{a}, \mathbf{b}, d)$, para os mesmos valores de d, a ocorrência dos valores assumidos pela função de correlação cruzada periódica ímpar $\Theta(\mathbf{a}, \mathbf{b}, d)$

assemelha-se a uma função densidade de probabilidade Gaussiana. Adicionalmente, mostrou-se que a variância dessa densidade torna-se mínima quando o valor da função de correlação cruzada periódica par for mínimo, $\theta(\mathbf{a}, \mathbf{b}, d) = -1$. Portanto, para o conjunto de seqüências de Gold na condição de quase sincronismo, é razoável ajustar as fases de acordo com a função de correlação cruzada periódica par.

Em (SAITO et al., 2001), para conjuntos de seqüências QS, definiu-se para a função de correlação periódica par, $\theta(\mathbf{a}, \mathbf{b}, d)$, o parâmetro quase ortogonalidade na condição de quase sincronismo (*quasi-orthogonal on quasi-synchronous*), $QOQS(r)$, onde r relaciona-se com a zona de correlação reduzida da seguinte forma:

$$\theta(\mathbf{a}, \mathbf{b}, d) = -1 \text{ para } |d| \leq L_{CZ} = \frac{r-1}{2} \tag{2.61}$$

Aqui, um conjunto QS com $L_{CZ} = \frac{r-1}{2}$ será denotado por QS-r.

Para obter um conjunto de seqüências QS conforme (SAITO et al., 2001), inicialmente gera-se um conjunto de Gold conforme (2.60), onde as SMC são geradas conforme o registrador deslocameneto da figura B.1 com estado inicial 100...0. Eliminando-se do conjunto a seqüência $\mathbf{g}_2$, obtém-se um conjunto QS-1 com $L_{CZ} = 0$ (2.61). A partir desse conjunto, podem ser obtidos conjunto QS com $r > 1$. A metodologia para obter tais conjuntos consiste na procura exaustiva por seqüências do conjunto QS-1 que resultam em $\theta(\mathbf{a}, \mathbf{b}, d) = -1$ para $0 < |d| \leq \frac{r-1}{2}$, onde $\mathbf{a}, \mathbf{b} \in$ QS-1. As seqüências que apresentarem essa característica irão compor o conjunto QS-r.

Conforme descrito na seção 2.1.2, um conjunto de Gold é gerado a partir de duas SMC. Mas nem todas as combinações de SMC irão gerar conjuntos de Gold com a possibilidade de selecionar seqüências QS-r. Em (SAITO et al., 2001), os conjuntos de Gold com $N = 31$ foram separados em duas classes: conjuntos de Gold de Classe I, dos quais é possível obter um conjunto de seqüências QS-3 e os conjuntos de Gold de Classe II, dos quais não é possível obter um conjunto de seqüências QS-3.

- Classe I : $Gold(45, 47)$, $Gold(45, 73)$, $Gold(47, 51)$, $Gold(47, 67)$, $Gold(51, 67)$, $Gold$ $(51, 75)$, $Gold(67, 75)$.
- Classe II: $Gold(45, 67)$, $Gold(45, 75)$, $Gold(47, 73)$, $Gold(51, 73)$, $Gold(73, 75)$.

Por exemplo, um conjunto de seqüências QS-3 de comprimento $N = 31$ obtido do conjunto $Gold(45, 73)$ pode ser composto pelas seqüências $\{\mathbf{g}_1, \mathbf{g}_{12}, \mathbf{g}_{17}, \mathbf{g}_{18}, \mathbf{g}_{19},$

$\mathbf{g}_{27}$, $\mathbf{g}_{30}$, $\mathbf{g}_{31}\}$ ou pelas seqüências $\{\mathbf{g}_4$, $\mathbf{g}_5$, $\mathbf{g}_6$, $\mathbf{g}_7$, $\mathbf{g}_{10}$, $\mathbf{g}_{14}$, $\mathbf{g}_{15}$, $\mathbf{g}_{21}\}$, onde $\mathbf{g}_i$ com $i = 1, 2, 3, ..., 2^n + 1$ são as seqüências geradas conforme (2.60). Em (SAITO et al., 2001), um conjunto $QS - r$ é representado por Q_i, onde i é o menor índice das seqüências Gold que compõem o conjunto.

Para a condição de $r = 5$, o conjunto de seqüências QS pode ser formado pelas seqüências $\{\mathbf{g}_1$, $\mathbf{g}_{12}$, $\mathbf{g}_{17}$, $\mathbf{g}_{19}\}$, ou pelas seqüências $\{\mathbf{g}_4$, $\mathbf{g}_5$, $\mathbf{g}_{10}$, $\mathbf{g}_{15}\}$ do mesmo conjunto $Gold(45, 73)$. A tabela 2.2 sintetiza alguns conjuntos de seqüências QS (SAITO et al., 2001).

Tabela 2.2: Conjuntos de seqüências QS.

Conjunto Gold	N	r	**Conjunto QS-r**	**Seqüências do conjunto Gold**
	7	1	Q_1	todas exceto $\mathbf{g}_2$
$Gold(13, 15)$	7	3	Q_1	$\{\mathbf{g}_1, \mathbf{g}_7\}$
	7	3	Q_3	$\{\mathbf{g}_3, \mathbf{g}_9\}$
	31	1	Q_1	todas exceto $\mathbf{g}_2$
	31	3	Q_1	$\{\mathbf{g}_1, \mathbf{g}_{12}, \mathbf{g}_{17}, \mathbf{g}_{18}, \mathbf{g}_{19}, \mathbf{g}_{27}, \mathbf{g}_{30}, \mathbf{g}_{31}\}$
$Gold(45, 73)$	31	3	Q_4	$\{\mathbf{g}_4, \mathbf{g}_5, \mathbf{g}_6, \mathbf{g}_7, \mathbf{g}_{10}, \mathbf{g}_{147}, \mathbf{g}_{15}, \mathbf{g}_{21}\}$
	31	5	Q_1	$\{\mathbf{g}_1, \mathbf{g}_{12}, \mathbf{g}_{17}, \mathbf{g}_{19}\}$
	31	5	Q_4	$\{\mathbf{g}_4, \mathbf{g}_5, \mathbf{g}_{10}, \mathbf{g}_{15}\}$
$Gold(203, 277)$	127	5	Q_1	$\{\mathbf{g}_1, \mathbf{g}_7, \mathbf{g}_{12}, \mathbf{g}_{13}, \mathbf{g}_{31}, \mathbf{g}_{33}, \mathbf{g}_{69}, \mathbf{g}_{111}\}$

As figuras 2.1.a e 2.1.b exemplificam as funções de correlação periódica para duas seqüências do conjunto QS-5 com $N = 127$. A figura 2.2 apresenta a ocorrência de valores de correlação cruzada periódica ímpar $\Theta(\mathbf{a}, \mathbf{b}, d)$, com $\mathbf{a}$ e $\mathbf{b}$ seqüências do conjunto QS-5 com $N = 127$, $\mathbf{a} \neq \mathbf{b}$ e $|d| \leq 2$. Nesse caso, observa-se que a ocorrência de valores elevados de correlação cruzada periódica ímpar é pequena.

2.1.3.1 Características das seqüências QS

O número de seqüências em um conjunto QS-r varia com o valor de r. Observa-se que, de modo geral, um incremento de 2 no valor de r, diminui aproximadamente $\frac{1}{4}$ do número de seqüências no conjunto na maioria dos casos. Em (SAITO et al., 2001) foi investigado o tamanho e a quantidade de conjuntos de seqüências QS para $N = 7, 31, 127, 511$. Esses dados são parcialmente mostrados na tabela 2.3.

Os conjuntos de seqüências QS de mesmo N, r e tamanho K podem ter propriedades de correlação cruzada periódica ímpar diferentes. Por exemplo, para $N = 31$ e $r = 5$ existem 2 conjuntos, Q_1 e Q_4, com 4 seqüências cada, extraídas do conjunto

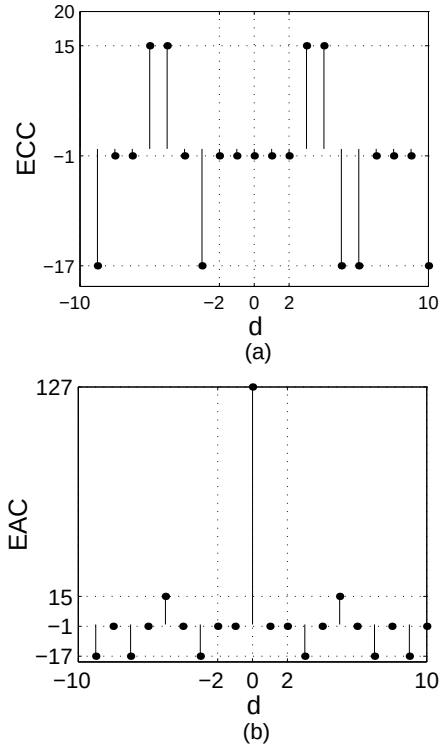

Figura 2.1: Exemplo para a (a) função de correlação cruzada periódica par e para a (b) função de autocorrelação periódica par de seqüências QS-5 com $N = 127$.

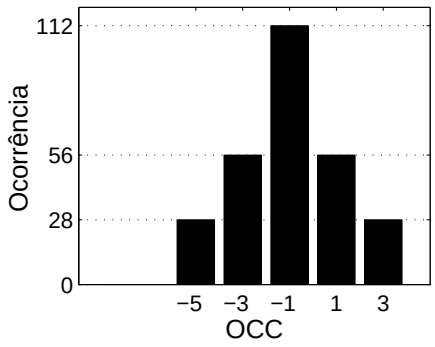

Figura 2.2: Histograma da função de correlação cruzada periódica ímpar no intervalo $-2 \leq |d| \leq 2$ para o subconjunto Q_1 do conjunto QS-5 com $N = 127$.

Gold$(45, 73)$. Verifica-se a maior ocorrência de valores de correlação cruzada periódica ímpar $\Theta(\mathbf{a}, \mathbf{b}, d)$ de maior magnitude no conjunto Q_1 em relação ao conjunto Q_4 com $|d| \leq 1$ e também $|d| \leq 2$. Portanto, o receptor convencional utilizando o conjunto Q_4 terá melhor desempenho quando comparado ao receptor utilizando o conjunto Q_1 na condição de erro de sincronismo $\tau_{\max} \leq 1$ e $\tau_{\max} \leq 2$ (KURAMOTO; ABRÃO; JESZENSKY, 2004c). A distribuição dos valores de correlação cruzada periódica ímpar

Tabela 2.3: Tamanho do conjunto de seqüências QS de acordo com r e N.

r	N	**quantidade de conjuntos**	**tamanho**, K
3	7	2	2
	31	2	8
	127	2	32
	511	2	128
5	31	2	4
	127	4	8
	511	4	32
7	127	4	4
	511	8	8
9	127	2	4
	511	8	4

são mostrados na figura 2.3.

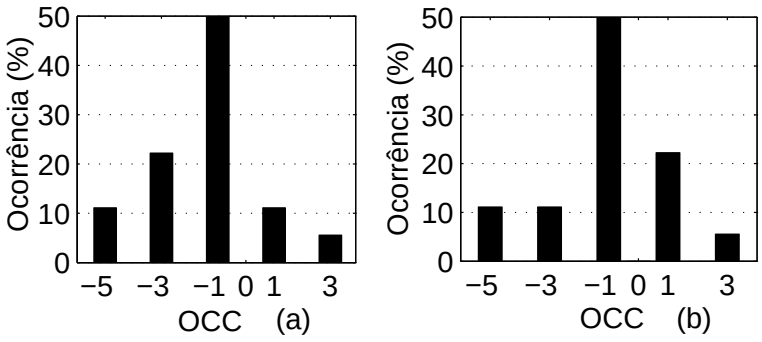

Figura 2.3: Ocorrência de valores de correlação cruzada periódica ímpar $\Theta(\mathbf{a}, \mathbf{b}, d)$ para o conjunto de seqüências QS-5 obtido do conjunto de Gold $Gold(45, 73)$: (a) Q_1 e (b) Q_4, com $|d| \leq 2$.

A seção 2.2.1 descreverá o conjunto de seqüências ortogonais generalizadas OQS, o qual também é derivado de conjuntos Gold. A metodologia de construção desse conjunto é semelhante à metodologia apresentada nesta seção.

2.1.4 Seqüências GMW

As seqüências GMW foram propostas em (SCHOLTZ; WELCH, 1984) baseados em estudos de Gordon, Mills e Welch (GMW) (GORDON; MILLS; WELCH, 1962). Essas seqüências são de fundamental importância no estudo de seqüências adequadas para sistemas QS-CDMA, pois as GMW apresentam uma faixa de deslocamentos bem de-

terminada, na qual a função de correlação cruzada par periódica assume valor -1 (em módulo é o menor valor de correlação possível).

As seqüências GMW são definidas como (SCHOLTZ; WELCH, 1984):

$$a_t = Tr_1^m \left\{ [Tr_m^n(\alpha^t)]^r \right\} \tag{2.62}$$

onde α é um elemento primitivo de $GF(2^n)$ e r um inteiro primo relativo à $2^m - 1$, definido em $1 \leq r < 2^m - 1$. O período da seqüência será $N = 2^n - 1$, pois $Tr_m^n(\alpha^t)$ é uma recorrência linear, a qual seu período é dado pela ordem de α. Como α é um elemento primitivo de $GF(2^n)$, a ordem de α é $2^n - 1$; em outras palavras, α^t percorre todos os elementos não nulos de $GF(2^n)$.

Observe que se $r = 1$, da propriedade 4 do traço (seção B.1.8), a seqüência GMW é uma SMC. Assim, pode-se afirmar que as seqüências GMW representam a generalização das SMC.

Com o objetivo de analisar a seqüência GMW em termos de sua construção e funções de correlação periódica, define-se $\mathcal{T}$ como:

$$\mathcal{T} = \frac{2^n - 1}{2^m - 1} \tag{2.63}$$

Então, escreve-se (2.62) em forma matricial, sendo que a seqüência GMW $\{a_t\}$ é dada pela concatenação das linhas da matriz:

$$\mathbf{A} = \begin{bmatrix} Tr_1^m \left\{ \left[Tr_m^n(\alpha^0) \right]^r \right\} & Tr_1^m \left\{ \left[Tr_m^n(\alpha^1) \right]^r \right\} & \dots & Tr_1^m \left\{ \left[Tr_m^n(\alpha^{\mathcal{T}-1}) \right]^r \right\} \\ Tr_1^m \left\{ \left[Tr_m^n(\alpha^{\mathcal{T}}) \right]^r \right\} & Tr_1^m \left\{ \left[Tr_m^n(\alpha^{\mathcal{T}+1}) \right]^r \right\} & \dots & Tr_1^m \left\{ \left[Tr_m^n(\alpha^{2\mathcal{T}-1}) \right]^r \right\} \\ Tr_1^m \left\{ \left[Tr_m^n(\alpha^{2\mathcal{T}}) \right]^r \right\} & Tr_1^m \left\{ \left[Tr_m^n(\alpha^{2\mathcal{T}+1}) \right]^r \right\} & \dots & Tr_1^m \left\{ \left[Tr_m^n(\alpha^{3\mathcal{T}-1}) \right]^r \right\} \\ \vdots & \vdots & \ddots & \vdots \\ Tr_1^m \left\{ \left[Tr_m^n(\alpha^{(2^m-2)\mathcal{T}}) \right]^r \right\} & Tr_1^m \left\{ \left[Tr_m^n(\alpha^{(2^m-2)\mathcal{T}+1}) \right]^r \right\} & \dots & Tr_1^m \left\{ \left[Tr_m^n(\alpha^{(2^m-1)\mathcal{T}}) \right]^r \right\} \end{bmatrix} \tag{2.64}$$

Observe que a ordem de $\alpha^{\mathcal{T}}$ é 2^m, pois:

$$(\alpha^{\mathcal{T}})^{2^m} = (\alpha^{\mathcal{T}})^{2^m-1+1} = (\alpha^{\mathcal{T}})^{2^m-1}(\alpha^{\mathcal{T}})^1 = \left(\alpha^{\frac{2^n-1}{2^m-1}}\right)^{2^m-1}(\alpha^{\mathcal{T}})^1 = (\alpha^{2^n-1})(\alpha^{\mathcal{T}})$$

$$= \alpha^{\mathcal{T}} \tag{2.65}$$

Assim, verifica-se que $\alpha^{\mathcal{T}} \in GF(2^m)$ e pode-se aplicar a propriedade 3 da função traço (seção B.1.8) em $Tr_1^m\left\{\left[Tr_m^n(\alpha^{k\mathcal{T}+i})\right]^r\right\}$:

$$Tr_1^m\left\{\left[Tr_m^n(\alpha^{k\mathcal{T}+i})\right]^r\right\} = Tr_1^m\left\{\alpha^{rk\mathcal{T}}\left[Tr_m^n(\alpha^i)\right]^r\right\} \tag{2.66}$$

Aplicando tal propriedade a todos os elementos de (2.64), tem-se:

$$\mathbf{A} = \begin{bmatrix} Tr_1^m\left\{\alpha^{0r\mathcal{T}}\left[Tr_m^n(\alpha^0)\right]^r\right\} & Tr_1^m\left\{\alpha^{0r\mathcal{T}}\left[Tr_m^n(\alpha^1)\right]^r\right\} & \cdots & Tr_1^m\left\{\alpha^{0r\mathcal{T}}\left[Tr_m^n(\alpha^{\mathcal{T}-1})\right]^r\right\} \\ Tr_1^m\left\{\alpha^{r\mathcal{T}}\left[Tr_m^n(\alpha^0)\right]^r\right\} & Tr_1^m\left\{\alpha^{r\mathcal{T}}\left[Tr_m^n(\alpha^1)\right]^r\right\} & \cdots & Tr_1^m\left\{\alpha^{r\mathcal{T}}\left[Tr_m^n(\alpha^{\mathcal{T}-1})\right]^r\right\} \\ Tr_1^m\left\{\alpha^{2r\mathcal{T}}\left[Tr_m^n(\alpha^0)\right]^r\right\} & Tr_1^m\left\{\alpha^{2r\mathcal{T}}\left[Tr_m^n(\alpha^1)\right]^r\right\} & \cdots & Tr_1^m\left\{\alpha^{2r\mathcal{T}}\left[Tr_m^n(\alpha^{\mathcal{T}-1})\right]^r\right\} \\ \vdots & \vdots & \ddots & \vdots \\ Tr_1^m\left\{\alpha^{(2^m-2)r\mathcal{T}}\left[Tr_m^n(\alpha^0)\right]^r\right\} & Tr_1^m\left\{\alpha^{(2^m-2)r\mathcal{T}}\left[Tr_m^n(\alpha^1)\right]^r\right\} & \cdots & Tr_1^m\left\{\alpha^{(2^m-2)r\mathcal{T}}\left[Tr_m^n(\alpha^{\mathcal{T}-1})\right]^r\right\} \end{bmatrix} \tag{2.67}$$

Observando os elementos da matriz (2.67) em colunas, pode-se escrever os elementos em seqüência de cada coluna como:

$$Tr_1^m\left\{\alpha^{kr\mathcal{T}}[\theta]^r\right\} \tag{2.68}$$

com $k = 0, 1, 2, ..., 2^m - 2$ e $\theta \in GF(2^m)$ constante, onde $\theta = Tr_m^n(\alpha^j) = \alpha^{d\mathcal{T}}$, $j = 0, 1, 2, ..., \mathcal{T} - 1$ e $d = 0, 1, 2, ..., 2^m - 2, \infty$. Note que (2.68) é uma SMC $\{u_{k+d}\} = \{Tr_1^m\left\{\alpha^{kr\mathcal{T}}\alpha^{dr\mathcal{T}}\right\}\} = \{Tr_1^m\left\{\alpha^{(k+d)r\mathcal{T}}\right\}\}$ cuja fase d é definida por θ.

Observe que o inteiro r é expoente de elementos $\alpha^{k\mathcal{T}} \in GF(2^m)$, assim, esse é definido $0 \leq r < 2^m - 1$. Além disso, a SMC dada por $u_k = Tr_1^m\left\{\alpha^{kr\mathcal{T}}\right\}$, com $k = 0, 1, 2, ..., 2^m - 2$, é a decimação r da SMC dada por $u_k = Tr_1^m\left\{\alpha^{k\mathcal{T}}\right\}$. O comprimento da seqüência decimada é $N_2 = N_1/\text{mdc}(r, 2^m - 1)$ (Lema B.1.1), onde N_1 é o comprimento da seqüência original. Assim, r deve satisfazer $\text{mdc}(r, 2^m - 1) = 1$, para que a SMC decimada tenha o mesmo comprimento da SMC original.

Então, para obter uma GMW basta obter uma semente SMC e calcular fases θ apropriadas. O conjunto de fases $\theta = Tr_m^n(\alpha^j) = \alpha^{d\mathcal{T}}$ será dado pela seqüência s composta pelos expoentes d de $\alpha^{\mathcal{T}}$:

$$s = (s_0, s_1, s_2, ..., s_{\mathcal{T}-1}) \tag{2.69}$$

onde $s_j = d$, com $Tr_m^n(\alpha^j) = \alpha^{d\mathcal{T}}$ onde d poderá assumir os valores $d = 0, 1, 2, ..., 2^m - 2$ e ∞; este último ocorre quando $Tr_m^n(\alpha^j) = 0$. Então, quando $s_j = \infty$, $Tr_m^n(\alpha^j) = 0$ e, portanto, todos os elementos da j-ésima coluna de (2.67) serão zero.

A SMC dada por $u_k = Tr_1^m\left\{\alpha^{kr\mathcal{T}}\right\} = Tr_1^m\left\{(\alpha^{r\mathcal{T}})^k\right\}$ com α um elemento primitivo de $GF(2^n)$ construído com o polinômio primitivo $f(x)$ pode ser escrita como $u_k = Tr_1^m\left\{(\beta)^k\right\}$ com β um elemento primitivo de $GF(2^m)$ construído com o polinômio mínimo de $\alpha^{r\mathcal{T}}$, o qual é primitivo, pois mdc$(r, 2^m - 1) = 1$, e de grau m, pois, como foi mostrado anteriormente, a ordem de $\alpha^{r\mathcal{T}}$ é 2^m.

Então, na construção da GMW, em vez de definir o elemento primitivo α de $GF(2^n)$ e r, serão definidos os elementos primitivos α de $GF(2^n)$ e β de $GF(2^m)$.

Dessa forma, a seqüência GMW pode ser escrita como:

$$\mathbf{A} = \begin{bmatrix} u_{s_0} & u_{s_1} & u_{s_2} & ... & u_{s_{\mathcal{T}-1}} \\ u_{1+s_0} & u_{1+s_1} & u_{1+s_2} & ... & u_{1+s_{\mathcal{T}-1}} \\ u_{2+s_0} & u_{2+s_1} & u_{2+s_2} & ... & u_{2+s_{\mathcal{T}-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ u_{2^m-2+s_0} & u_{2^m-2+s_1} & u_{2^m-2+s_2} & ... & u_{2^m-2+s_{\mathcal{T}-1}} \end{bmatrix} \tag{2.70}$$

Observa-se que, assim como anteriormente, quando $s_j = \infty$, ou seja, $Tr_m^n(\alpha^j) = 0$, todos os elementos da coluna referente à s_j em (2.70) serão zero. Isso significa que $u_{k+s_j} = 0$, quando $s_j = \infty$.

2.1.4.1 Propriedades de correlação de seqüências GMW construídas de um mesmo polinômio primitivo

Considere a seqüência **a** dada por (2.70) e outra GMW, denotada por **b**, construída com o mesmo polinômio primitivo de grau n, porém, a semente SMC é obtida de outro polinômio primitivo de grau m. Tal polinômio dá origem à SMC **v** distinta de **u**, pois foram obtidas de polinômios primitivos distintos de graus m. Essa outra seqüência GMW **b**, construída a partir da SMC **v**, com deslocamento de $\tau = \tau_0\mathcal{T} + \tau_1$ para a esquerda, pode ser escrita, na forma matricial, como:

$$\mathbf{B}^{\tau} = \begin{bmatrix} v_{\tau_0+s_{\tau_1}} & v_{\tau_0+s_{\tau_1+1}} & v_{\tau_0+s_{\tau_1+2}} & \cdots & v_{\tau_0+s_{\tau_1+\mathcal{T}-1}} \\ v_{\tau_0+1+s_{\tau_1}} & v_{\tau_0+1+s_{\tau_1+1}} & v_{\tau_0+1+s_{\tau_1+2}} & \cdots & v_{\tau_0+1+s_{\tau_1+\mathcal{T}-1}} \\ v_{\tau_0+2+s_{\tau_1}} & v_{\tau_0+2+s_{\tau_1+1}} & v_{\tau_0+2+s_{\tau_1+2}} & \cdots & v_{\tau_0+2+s_{\tau_1+\mathcal{T}-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{\tau_0+2^m-2+s_{\tau_1}} & v_{\tau_0+2^m-2+s_{\tau_1+1}} & v_{\tau_0+2^m-2+s_{\tau_1+2}} & \cdots & v_{\tau_0+2^m-2+s_{\tau_1+\mathcal{T}-1}} \end{bmatrix} \tag{2.71}$$

A expressão geral para a correlação cruzada periódica par entre seqüências GMW construídas com um mesmo polinômio primitivo de grau n foi obtida em (GAMES, 1984) e (LIN; CHANG, 1997). Para simplificar a notação, faz-se $\theta_{\mathbf{ab}}(\tau) = \theta(\mathbf{a}, \mathbf{b}, \tau)$:

$$\begin{aligned}
\theta_{\mathbf{ab}}(\tau) &= \sum_{i=0}^{2^n-2} (-1)^{a_i+b_{i+\tau}} \\
&= (-1)^{u_{s_0} v_{(\tau_0+s_{\tau_1})}} + (-1)^{u_{s_1} v_{(\tau_0+s_{\tau_1+1})}} + \ldots + (-1)^{u_{s_{(\mathcal{T}-1)}} v_{(\tau_0+s_{(\tau_1+\mathcal{T}-1)})}} + \\
&+ (-1)^{u_{(1+s_0)} v_{(\tau_0+1+s_{\tau_1})}} + (-1)^{u_{(1+s_1)} v_{(\tau_0+1+s_{(\tau_1+1)})}} + \ldots + (-1)^{u_{(1+s_{\mathcal{T}-1})} v_{(\tau_0+1+s_{(\tau_1+\mathcal{T}-1)})}} + \\
&+ \ldots + \\
&+ (-1)^{u_{(2^m-2+s_0)} v_{(\tau_0+2^m-2+s_{\tau_1})}} + (-1)^{u_{(2^m-2+s_1)} v_{(\tau_0+2^m-2+s_{(\tau_1+1)})}} + \ldots + (-1)^{u_{(2^m-2+s_{\mathcal{T}-1})} v_{(\tau_0+2^m-2+s_{(\tau_1+\mathcal{T}-1)})}} \\
&= \theta_{\mathbf{uv}}(\tau_0 + s_{\tau_1} - s_0) + \theta_{\mathbf{uv}}(\tau_0 + s_{\tau_1+1} - s_1) + \theta_{\mathbf{uv}}(\tau_0 + s_{\tau_1+2} - s_2) + \ldots + \\
&+ \theta_{\mathbf{uv}}(\tau_0 + s_{\tau_1+\mathcal{T}-1} - s_{\mathcal{T}-1}) \\
&= \sum_{j=0}^{\mathcal{T}-1} \theta_{\mathbf{uv}}(\tau_0 + s_{\tau_1+j} - s_j)
\end{aligned} \tag{2.72}$$

Conforme a definição de s_k, tem-se que $s_{i\mathcal{T}+j}$ é o expoente de $\alpha^{\mathcal{T}}$ do resultado de $Tr_m^n(\alpha^{i\mathcal{T}+j})$. Da propriedade do traço $Tr_m^n(\alpha^{i\mathcal{T}+j}) = \alpha^{i\mathcal{T}} Tr_m^n(\alpha^j)$ tem-se que $s_{i\mathcal{T}+j} = i + s_j$. Aplicando essa propriedade em (2.72) tem-se:

$$\begin{aligned}
\theta_{\mathbf{ab}}(\tau) &= \sum_{j=0}^{\mathcal{T}-1} \theta_{\mathbf{uv}}(s_{\tau_0\mathcal{T}+\tau_1+j} - s_j) \\
&= \sum_{j=0}^{\mathcal{T}-1} \theta_{\mathbf{uv}}(s_{\tau+j} - s_j)
\end{aligned} \tag{2.73}$$

Observe que a função de correlação cruzada periódica de seqüências GMW é completamente definida pela função de correlação cruzada periódica das SMC sementes

das GMW.

Um Lema apresentado em (LIN; CHANG, 1997) obtido dos Teoremas 1 e 2 de (GAMES, 1984), os quais foram derivados de resultados de (SINGER, 1938) é extremamente útil na caracterização da função de correlação cruzada periódica de seqüências GMW.

Lema 2.1.1 *Se* $\tau \neq (0 \bmod \mathcal{T})$*, na seqüência* $(s_\tau - s_0, s_{\tau+1} - s_1, ..., s_{\tau+\mathcal{T}-1} - s_{\mathcal{T}-1}) \bmod (2^m - 2)$ *o elemento* $\infty - \infty$ *aparecerá* $2^{n-2m-1}/(2^m - 1)$ *vezes, o elemento* ∞ *aparecerá* 2^{n-2m+1} *vezes e os elementos* $\{0, 1, 2, ..., 2^m - 2\}$ *aparecerão* 2^{n-2m} *vezes cada um. Se* $\tau = d\mathcal{T}$*, o elemento* $\infty - \infty$ *aparecerá* $(2^{n-m} - 1)/(2^m - 1)$ *vezes e o elemento d aparecerá* 2^{n-m} *vezes.*

Com esse Lema, pode-se reescrever (2.73) como:

$$\theta_{\mathbf{ab}}(\tau) = \begin{cases} \frac{2^{n-2m}-1}{2^m-1}\theta_{\mathbf{uv}}(\infty - \infty) + 2^{n-2m+1}\theta_{\mathbf{uv}}(\infty) + 2^{n-2m}\sum_{k=0}^{2^m-2}\theta_{\mathbf{uv}}(k), & \tau \neq (0 \bmod \mathcal{T}) \\ \frac{2^{n-m}-1}{2^m-1}\theta_{\mathbf{uv}}(\infty - \infty) + 2^{n-m}\theta_{\mathbf{uv}}(d), & \tau = d\mathcal{T} \end{cases}$$

onde:

$$\begin{aligned} \theta_{\mathbf{uv}}(\infty - \infty) &= \sum_{i=0}^{2^m-2}(-1)^{u_i + v_{(i+\infty-\infty)}} \\ &= \sum_{i=0}^{2^m-2}(-1)^{u_{(i+\infty)} + v_{(i+\infty)}} \\ &= \sum_{i=0}^{2^m-2}(-1)^{0+0} \\ &= 2^m - 1 \end{aligned} \tag{2.74}$$

$$\begin{aligned} \theta_{\mathbf{uv}}(\infty) &= \sum_{i=0}^{2^m-2}(-1)^{u_i + v_{(i+\infty)}} \\ &= \sum_{i=0}^{2^m-2}(-1)^{u_i + 0} \end{aligned}$$

$$= \sum_{i=0}^{2^m-2} (-1)^{u_i} \tag{2.75}$$

Como a SMC é balanceada[10]:

$$\begin{aligned} \theta_{\mathbf{uv}}(\infty) &= \sum_{i=0}^{2^m-2} (-1)^{u_i} \\ &= -1 \end{aligned} \tag{2.76}$$

e

$$\begin{aligned} \sum_{k=0}^{2^m-2} \theta_{\mathbf{uv}}(k) &= \sum_{k=0}^{2^m-2} \sum_{i=0}^{2^m-2} (-1)^{u_i+v_{i+k}} \\ &= \sum_{i=0}^{2^m-2} (-1)^{u_i} \sum_{k=0}^{2^m-2} (-1)^{v_{i+k}} \end{aligned} \tag{2.77}$$

Lembrando novamente que a SMC é balanceada:

$$\begin{aligned} \sum_{k=0}^{2^m-2} \theta_{\mathbf{uv}}(k) &= (-1)(-1) \\ &= 1 \end{aligned} \tag{2.78}$$

Substituindo (2.74), (2.76) e (2.78) em (2.74), tem-se:

$$\theta_{\mathbf{ab}}(\tau) = \begin{cases} -1, & \text{para } \tau \neq (0 \bmod \mathcal{T}) \\ 2^{n-m} - 1 + 2^{n-m}\theta_{\mathbf{uv}}(d), & \text{para } \tau = d\mathcal{T} \end{cases} \tag{2.79}$$

Para (2.74), (2.76) e (2.78) ocorrerem não é necessário que as sementes **u** e **v** sejam SMC. Observe que se as sementes **u** e **v** forem balanceadas, não SMC, o resultados obtido em (2.74), (2.76) e (2.78) serão os mesmos e, conseqüentemente, a função de correlação cruzada periódica par será similar à apresentada em (2.74), a menos de

[10] para seqüências de comprimento ímpar, será adotado o termo balanceada às seqüências que possuirem 2^{m-1} elementos 1 e $2^{m-1} - 1$ elementos 0. Para seqüências de comprimento par, o termo balanceada será adotado às seqüências que possuirem o mesmo número de elementos 0 e 1.

$\theta_{\mathbf{uv}}(d)$, a qual será a correlação cruzada entre seqüências balanceadas (o que representa um conjunto que contém as SMC, porém, muito maior). Essa observação foi apresentada pela primeira vez em (LIN; CHANG, 1997), como uma proposta de seqüências adequadas para sistemas QS-CDMA, por apresentar a faixa $\mathcal{T}$ de correlação mínima (-1). Esse conjunto de seqüências será discutido em seções subseqüentes.

A expressão para a função de autocorrelação periódica par para a seqüência GMW **a** é obtida com o mesmo procedimento utilizado na caracterização da função de correlação cruzada periódica par:

$$\begin{aligned} \theta_{\mathbf{aa}}(\tau) &= \sum_{i=0}^{2^n-2}(-1)^{a_i+a_{(i+\tau)}} \\ &= \sum_{j=0}^{\mathcal{T}-1}\theta_{\mathbf{uu}}(\tau_0 + s_{\tau_1+j} - s_j) \end{aligned} \tag{2.80}$$

Utilizando a propriedade $s_{i\mathcal{T}+j} = i + s_j$, tem-se:

$$\begin{aligned} \theta_{\mathbf{aa}}(\tau) &= \sum_{j=0}^{\mathcal{T}-1}\theta_{\mathbf{uu}}(s_{\tau_0\mathcal{T}+\tau_1+j} - s_j) \\ &= \sum_{j=0}^{\mathcal{T}-1}\theta_{\mathbf{uu}}(s_{\tau+j} - s_j) \end{aligned} \tag{2.81}$$

Com o Lema 2.1.1, pode-se escrever:

$$\theta_{\mathbf{aa}}(\tau) = \begin{cases} \frac{2^{n-2m}-1}{2^m-1}\theta_{\mathbf{uu}}(\infty-\infty) + 2^{n-2m+1}\theta_{\mathbf{uu}}(\infty) + 2^{n-2m}\sum_{k=0}^{2^m-2}\theta_{\mathbf{uu}}(k), & \tau \neq (0 \bmod \mathcal{T}) \\ \frac{2^{n-m}-1}{2^m-1}\theta_{\mathbf{uu}}(\infty-\infty) + 2^{n-m}\theta_{\mathbf{uu}}(d), & \tau = d\mathcal{T} \end{cases}$$

onde:

$$\theta_{\mathbf{uu}}(\infty-\infty) = \sum_{i=0}^{2^m-2}(-1)^{u_i+u_{(i+\infty-\infty)}}$$

$$\begin{aligned} &= \sum_{i=0}^{2^m-2} (-1)^{u_{(i+\infty)}+u_{(i+\infty)}} \\ &= \sum_{i=0}^{2^m-2} (-1)^{0+0} \\ &= 2^m - 1 \end{aligned} \tag{2.82}$$

$$\begin{aligned} \theta_{\mathbf{uu}}(\infty) &= \sum_{i=0}^{2^m-2} (-1)^{u_i+u_{(i+\infty)}} \\ &= \sum_{i=0}^{2^m-2} (-1)^{u_i+0} \\ &= \sum_{i=0}^{2^m-2} (-1)^{u_i} \\ &= -1 \end{aligned} \tag{2.83}$$

$$\begin{aligned} \sum_{k=0}^{2^m-2} \theta_{\mathbf{uu}}(k) &= \sum_{k=0}^{2^m-2} \sum_{i=0}^{2^m-2} (-1)^{u_i+u_{(i+k)}} \\ &= \sum_{i=0}^{2^m-2} (-1)^{u_i} \sum_{k=0}^{2^m-2} (-1)^{u_{(i+k)}} \\ &= 1 \end{aligned} \tag{2.84}$$

e

$$\theta_{\mathbf{uu}}(d) = -1 \text{ , para } d \neq 0 \bmod 2^m - 1 \tag{2.85}$$

pois a seqüência **u** é SMC.

Substituindo (2.82), (2.83) , (2.84) e (2.85) em (2.82), tem-se:

$$\theta_{\mathbf{aa}}(\tau) = \begin{cases} -1 & \text{, para } \tau \neq 0 \bmod 2^m - 1 \\ N & \text{, para } \tau = 0 \bmod 2^m - 1 \end{cases} \tag{2.86}$$

Observe que a função de autocorrelação de seqüências GMW é idêntica à função de autocorrelação de SMC.

2.1.4.2 Número de seqüências GMW de um dado comprimento

O número de seqüências GMW $a_t = Tr_1^m\{[Tr_m^n(\alpha^t)]^r\}$, construídas de um mesmo polinômio primitivo de grau n, será dado pelo número de seqüências semente SMC distintas de grau m, pois duas GMW são distintas devido às sementes serem distintas. De forma equivalente, duas GMW são distintas se as decimações r, com r inteiro definido em $1 \leq r < 2^m - 1$ e primo relativo com $2^m - 1$, adotadas na construção de cada seqüência pertencerem a coconjuntos distintos. Essa afirmação é facilmente explicada, pois o polinômo mínimo de um elemento primitivo β de um corpo $GF(2^m)$ (nesse caso primitivo de $GF(2^m)$) será distinto de um polinômio mínimo de mesmo grau de β^r, se e somente se r, definido em $1 \leq r < 2^m - 1$, pertencer a outro coconjunto. Adicionalmente, este outro polinômio mínimo será primitivo de grau m se e somente se a ordem de β^r for $2^m - 1$, ou seja, se β^r for raiz primitiva de um corpo $GF(2^m)$. Para concluir, do Lema B.1.1, a ordem de β^r, dada por $\text{ord}(\beta^r) = t/\text{mdc}(r,t)$, onde $t = \text{ord}(\beta) = 2^m - 1$, será $2^m - 1$ se e somente se $\text{mdc}(r,t) = \text{mdc}(r, 2^m - 1) = 1$, ou seja, r deve ser primo relativo a $2^m - 1$.

O número de SMC distintas de grau m é dado por $\phi(2^m - 1)/m$, assim, o número de GMW distintas obtidas do mesmo polinômio primitivo de grau n será:

$$K(m) = \phi(2^m - 1)/m \tag{2.87}$$

com m fator de n.

Será adotada a nomenclatura família de seqüências GMW a um conjunto de seqüências GMW obtidas de um mesmo polinômio primitivo de grau n.

Uma família será distinta de outra se os polinômios primitivos de grau n forem distintos. Então, o número de famílias GMW é dado pelo número de polinômios primitivos de grau n, $K(n) = \phi(2^n - 1)/n$. Assim, o total de seqüências GMW de grau n, considerando todas as famílias, será:

$$K(m) \times K(n) \tag{2.88}$$

Entretanto, a boa propriedade de correlação cruzada, equação (2.79), vale apenas para seqüências de uma mesma família, ou seja, construídas de um mesmo polinômio primitivo de grau n, conforme a demonstração.

A seção seguinte apresenta as seqüências de Lin-Chang, as quais são interpretadas como a generalização das seqüências GMW.

2.1.5 Família Lin-Chang

As seqüências Lin-Chang foram propostas em (LIN; CHANG, 1997). Os autores desse artigo observaram que para obter seqüências que resultam em uma função de correlação cruzada par periódica $\theta_{\mathbf{ab}}(\tau) = -1$ para uma faixa τ semelhante à apresentada em (2.79), pode-se utilizar o método de construção das seqüências GMW de uma mesma família e adotar uma seqüência semente balanceada, não necessariamente uma SMC. Então, são chamadas de seqüências Lin-Chang às seqüências construídas com o mesmo método de construção de seqüências GMW, porém as seqüências sementes não precisam ser SMC, desde que sejam balanceadas.

2.1.5.1 Propriedades de correlação de seqüências Lin-Chang

Observe que se as sementes **u** e **v** forem balanceadas, não necessariamente SMC, os resultados obtidos em (2.74), (2.76) e (2.78) serão os mesmos e, conseqüentemente, a função de correlação cruzada periódica par apresentada em (2.74) também será similar, dada por:

$$\theta_{\mathbf{ab}}(\tau) = \begin{cases} -1, & \text{para } \tau \neq (0 \bmod \mathcal{T}) \\ 2^{n-m} - 1 + 2^{n-m}\theta_{\mathbf{uv}}(d), & \text{para } \tau = d\mathcal{T} \end{cases} \tag{2.89}$$

onde **u** e **v** agora são seqüências balanceadas (não necessariamente SMC).

Lembre-se de que essa expressão para a função de correlação cruzada par periódica foi obtida considerando seqüências obtidas de um mesmo polinômio primitivo de grau n.

A função de autocorrelação de seqüências Lin-Chang é obtida de (2.82), com a diferença que **u** é uma seqüência balanceada que pode não ser SMC. No caso de **u** ser SMC, a seqüência Lin-Chang é uma seqüência GMW e, portanto, a função de autocorrelação periódica será dada por (2.86). No caso de **u** não ser SMC, não ocorrerá (2.85). Assim, obtém-se a função de autocorrelação periódica par da substituição de (2.82), (2.83) e (2.84) em (2.82):

$$\theta_{\mathbf{aa}}(\tau) = \begin{cases} -1, & \text{para } \tau \neq (0 \bmod \mathcal{T}) \\ 2^{n-m} - 1 + 2^{n-m}\theta_{\mathbf{uu}}(d), & \text{para } \tau = d\mathcal{T}, \tau \neq (0 \bmod 2^n - 1) \\ N & \tau = (0 \bmod 2^n - 1) \end{cases} \tag{2.90}$$

onde $\theta_{\mathbf{uu}}(d) = \sum_{i=0}^{2^m-2}(-1)^{u_i+u_{(i+d)}}$.

2.1.5.2 Limite superior e inferior da função de autocorrelação periódica par para seqüências Lin-Chang

Para as seqüências descritas anteriormente, os valores assumidos pela função de autocorrelação periódica par estão bem estabelecidos. Em (LIN; CHANG, 1997) não foram apresentados os valores máximos e mínimos da função de autocorrelação par periódica fora da origem para as seqüências Lin-Chang. Para obtê-los, basta calcular os valores máximos e mínimos da função de autocorrelação par periódica fora da origem para as seqüências sementes.

A condição de $\tau = d\mathcal{T}$ com $\tau \neq (0 \bmod 2^n - 1)$ em (2.90) implica em $d \neq (0 \bmod 2^m - 1)$. Observe que, para $d \neq (0 \bmod 2^m - 1)$, $\{u_i\}$ e $\{u_{(i+d)}\}$ podem diferir em 2 elementos no mínimo, nesse caso $u_i + u_{(i+d)} = 1$. Conseqüentemente, concordarão em $2^m - 3$ elementos, nesse caso $u_i + u_{(i+d)} = 0$. Assim:

$$\begin{aligned} \theta_{\mathbf{uu}}(d) &= \sum_{i=0}^{2^m-2}(-1)^{u_i+u_{(i+k)}} \\ &= 2^m - 3 - 2 \\ &= 2^m - 5 \end{aligned} \tag{2.91}$$

Por outro lado, ainda para $d \neq (0 \bmod 2^m - 1)$, $\{u_i\}$ e $\{u_{(i+d)}\}$ podem concordar em 1 elemento no mínimo. Conseqüentemente, irão diferir em $2^m - 2$ elementos. Assim:

$$\begin{aligned} \theta_{\mathbf{uu}}(d) &= \sum_{i=0}^{2^m-2}(-1)^{u_i+u_{(i+k)}} \\ &= 1 - (2^m - 2) \\ &= 3 - 2^m \end{aligned} \tag{2.92}$$

Somente para $m \geq 3$ tem-se mais de 1 polinômio primitivo de grau m. Somente para $m \geq 3$ ter-se-á um conjunto com mais de uma seqüência. Assim, de (2.91) e (2.92):

$$\max\{\theta_{\mathbf{uu}}\} = 2^m - 5 \quad \text{e} \quad \min\{\theta_{\mathbf{uu}}\} = 3 - 2^m \tag{2.93}$$

Com esses resultados obtém-se o maior e menor valor de autocorrelação da seqüência **a** quando **u** não é SMC, para $\tau = d\mathcal{T}, \tau \neq (0 \bmod 2^n - 1)$ e $m \geq 3$:

$$\begin{aligned}
\max\{\theta_{\mathbf{aa}}(\tau)\} &= \max\{2^{n-m} - 1 + 2^{n-m}\theta_{\mathbf{uu}}(d)\} \\
&= 2^{n-m} - 1 + 2^{n-m}\max\{\theta_{\mathbf{uu}}\} \\
&= 2^{n-m} - 1 + 2^{n-m}(2^m - 5) \\
&= 2^n - 4 \cdot 2^{n-m} - 1 \qquad (2.94) \\
\min\{\theta_{\mathbf{aa}}(\tau)\} &= \min\{2^{n-m} - 1 + 2^{n-m}\theta_{\mathbf{uu}}(d)\} \\
&= 2^{n-m} - 1 + 2^{n-m}\min\{\theta_{\mathbf{uu}}\} \\
&= 2^{n-m} - 1 + 2^{n-m}(3 - 2^m) \\
&= -(2^n - 4 \cdot 2^{n-m}) - 1 \qquad (2.95)
\end{aligned}$$

Assim, os limites para a função de autocorrelação par periódica para $\tau = d\mathcal{T}, \tau \neq (0 \bmod 2^n - 1)$ e $m \geq 3$ serão:

$$-(2^n - 4 \cdot 2^{n-m}) - 1 \leq \theta_{\mathbf{aa}}(\tau) \leq 2^n - 4 \cdot 2^{n-m} - 1, \quad \text{para} \quad \tau = d\mathcal{T}, \tau \neq (0 \bmod 2^n - 1) \tag{2.96}$$

2.1.5.3 Número de seqüências Lin-Chang de um dado comprimento

Assim como para as seqüências GMW, o número de seqüências Lin-Chang construídas de um mesmo polinômio primitivo de grau n será dado pelo número de seqüências sementes disponíveis. Duas seqüências Lin-Chang são distintas se as respectivas sementes forem distintas. Como as sementes devem ser balanceadas e não necessariamente SMC, o número de sementes balanceadas de comprimento $2^m - 1$ será $\frac{\binom{2^m-1}{2^{(m-1)}}}{2^m-1}$. Portanto, o número de seqüências Lin-Chang construídas de um mesmo polinômio primitivo de

grau n, ou seja, o tamanho de uma família Lin-Chang de grau n, será dado por:

$$K(m) = \frac{\binom{2^m-1}{2^{(m-1)}}}{2^m - 1} \tag{2.97}$$

onde m é fator de n.

Observa-se que o tamanho da família Lin-Chang pode ser muito maior que o tamanho da família GMW. Por exemplo, para $m = 3, 4$ e 5, têm-se 5, 429 e 9694845 seqüências, respectivamente, em uma família Lin-Chang contra 3, 3 e 6, seqüências, respectivamente, em uma família GMW.

O número de famílias Lin-Chang é dado pelo número de polinômios primitivos de grau n, $K(n) = \phi(2^n - 1)/n$, assim como para as famílias GMW. O total de seqüências Lin-Chang de grau n, considerando todas as famílias, será:

$$\frac{\binom{2^m-1}{2^{(m-1)}}}{2^m - 1} \times \phi(2^n - 1)/n \tag{2.98}$$

É importante destacar que a boa propriedade de correlação cruzada, equação (2.89), vale apenas para seqüências de uma mesma família, ou seja, construídas de um mesmo polinômio primitivo de grau n.

2.1.5.4 Considerações sobre as características das seqüências Lin-Chang

Conforme demonstrado, para $0 < |\tau| < \frac{2^n-1}{2^m-1}$ ou $|\tau| \neq (0 \bmod \frac{2^n-1}{2^m-1})$, todos os valores assumidos pelas funções de correlação periódica par para as seqüências Lin-Chang de uma mesma família são mínimos e iguais a -1, figura 2.4.a e 2.4.b. Porém, dentro da mesma faixa τ os valores de correlação cruzada periódica ímpar não são mínimos, figura 2.5.

Observando as equações (2.97) e (2.89), verifica-se que existe um compromisso entre a faixa de deslocamentos τ em que as funções de correlação periódica par assumem valor -1 e o número de seqüências distintas na família (LIN; CHANG, 1997). Para obter o carregamento máximo com o conjunto Lin-Chang adota-se $n = 2m$, reduzindo, em conseqüência, a faixa de atrasos onde as funções de correlação periódica par assumem valor -1.

A função correlação cruzada periódica par pode assumir valores elevados quando

$\tau = d\mathcal{T}$, dependendo das fases das seqüências sementes, de outra forma, da função correlação cruzada periódica par entre as sementes $\theta_{\mathbf{uv}}(d)$, conforme a equação (2.89). Tal característica é exemplificada na figura 2.4.a. Isso implica em alta interferência entre usuários quando existirem sinais de usuários sincronizados ou quase com atrasos confinados em pequenas frações de chip. Para solucionar esse problema, basta ajustar as fases das sementes u e v para que $\theta_{\mathbf{uv}}(0) = -1$. Assim, $\theta_{\mathbf{ab}}(0) = -1$, conforme (2.89). Isso pode ser um trabalho difícil quando existem várias sementes para serem ajustadas.

Na condição de $\tau \neq 0$, o valor da função de autocorrelação periódica par para seqüências Lin-Chang geradas a partir de seqüências do tipo SMC (seqüências de máximo comprimento), reduz-se a -1, pois nesse caso a seqüência gerada é uma seqüência GMW (LIN; CHANG, 1997) (SCHOLTZ; WELCH, 1984). Quando as seqüências sementes não são SMC, a função de autocorrelação da seqüência Lin-Chang apresenta, adicionalmente ao valor -1, outros picos os quais seus valores limites são dados por (2.96), figura 2.4.b.

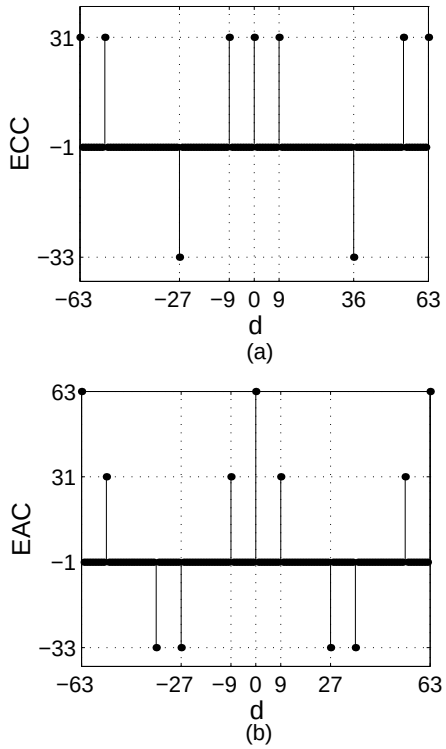

Figura 2.4: Exemplo para a (a) função de correlação cruzada periódica par e para a (b) função de autocorrelação periódica par de seqüências do conjunto Lin-Chang com $n = 2m$ e $N = 63$.

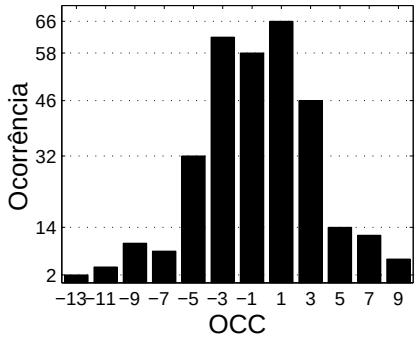

Figura 2.5: Histograma da função de correlação cruzada periódica ímpar no intervalo $0 < |\tau| < 9$ para o conjunto Lin-Chang com $n = 2m$ e $N = 63$.

A próxima seção descreve as seqüências LCZ-GMW binárias as quais, assim como as seqüências Lin-Chang, são obtidas de forma similar às seqüências GMW.

2.1.6 Família LCZ-GMW binária

A zona de correlação reduzida (*low correlation zone*, LCZ) representa o intervalo $|\tau| \leq \mathcal{Z}$ em que as funções de correlação periódica par $\theta_{i,j}(\tau)$ assumem valores reduzidos dados por θ_m (exceto para $i = j$ e $\tau = 0$). As seqüências que apresentam essa característica são chamadas de seqüências LCZ, conforme já mencionado na seção 1.2. As seqüências LCZ com $\theta_m = 1$ são chamadas de seqüências quase ortogonais generalizadas. Assim, pode-se afirmar que as seqüências QS (seção 2.1.3) são seqüências LCZ com $L_{CZ} = \frac{r-1}{2}$ e $\theta_m = 1$. É desejável que em sistemas QS-CDMA as seqüências utilizadas no sistema possuam a zona de correlação reduzida para, dessa forma, reduzir a interferência de múltiplo acesso e a auto-interferência.

Em (LONG; ZHANG, 1995) foram propostas seqüências LCZ binárias (sobre $GF(2)$) construídas a partir de um par de seqüências GMW. Para especificar tal conjunto de seqüências e não confundir com outros conjuntos LCZ como o QS, será adotada a nomenclatura LCZ-GMW.

A proposta apresentada em (LONG; ZHANG, 1995) foi estendida para o caso de seqüências p-árias, ou seja, sobre $GF(p)$ em (TANG; FAN, 2001b). Esse caso é apresentado no apêndice C.1. Uma família LCZ-GMW p-ária (ou LCZ-GMW polifásica) possui características de LCZ semelhantes às binárias. Lembrando a seção 2.1.1.1, as funções de correlação entre seqüências $\mathbf{a} = \{a_0, a_1, ..., a_{N-1}\}$ e $\mathbf{b} = \{b_0, b_1, ..., b_{N-1}\}$,

onde $a_i, b_i \in GF(p)$ ou a_i e b_i pertencem a um subconjunto do conjunto dos números inteiros, são calculadas entre seqüências $\tilde{\mathbf{a}} = \{\tilde{a}_0, \tilde{a}_1, ..., \tilde{a}_{N-1}\}$ e $\tilde{\mathbf{b}} = \{\tilde{b}_0, \tilde{b}_1, ..., \tilde{b}_{N-1}\}$, onde $\tilde{a}_i = \exp\left(\frac{j2\pi}{p} a_i\right)$ e $\tilde{b}_i = \exp\left(\frac{j2\pi}{p} b_i\right)$.

O método de geração de seqüências LCZ-GMW binárias, com $L_{CZ} = \mathcal{T} - 1 = \frac{2^n-1}{2^m-1} - 1$ e $\theta_m = 1$ proposta em (LONG; ZHANG, 1995) e (TANG; FAN, 2001b) é justificado com uma demonstração da função de correlação periódica bastante extensa. Aqui, será justificado o método de geração de seqüências LCZ-GMW e demonstrada a função de correlação periódica para seqüências LCZ-GMW binárias de uma forma bastante clara e direta.

Observe a função de correlação periódica dada pela equação (2.74) reproduzida aqui:

$$\theta_{\mathbf{ab}}(\tau) = \begin{cases} \frac{2^{n-2m}-1}{2^m-1}\theta_{\mathbf{uv}}(\infty - \infty) + 2^{n-2m+1}\theta_{\mathbf{uv}}(\infty) + 2^{n-2m}\sum_{k=0}^{2^m-2}\theta_{\mathbf{uv}}(k), & \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{para } \tau \neq (0 \bmod \mathcal{T}) & (2.99) \\ \frac{2^{n-m}-1}{2^m-1}\theta_{\mathbf{uv}}(\infty - \infty) + 2^{n-m}\theta_{\mathbf{uv}}(d), \qquad \text{para } \tau = d\mathcal{T} & \end{cases}$$

onde **u** e **v** serão SMC quando **a** e **b** forem seqüências GMW. Quando **a** e **b** forem seqüências Lin-Chang, **u** e **v** serão seqüências balanceadas, não necessariamente SMC.

Para que $\theta_{\mathbf{ab}}(\tau)$ resulte em -1 para $\tau = 0$ e $\mathbf{a} \neq \mathbf{b}$, deve-se obter:

$$\theta_{\mathbf{uv}}(0) = \sum_{i=0}^{2^m-2}(-1)^{u_i + v_{(i+0)}} = -1 \tag{2.100}$$

e para que $\theta_{\mathbf{ab}}(\tau)$ resulte em -1 para $\tau \neq (0 \bmod \mathcal{T})$, deve-se obter:

$$\begin{aligned} \theta_{\mathbf{uv}}(\infty) &= \sum_{i=0}^{2^m-2}(-1)^{u_i} \\ &= -1 \end{aligned} \tag{2.101}$$

e

$$\sum_{k=0}^{2^m-2}\theta_{\mathbf{uv}}(k) = \sum_{k=0}^{2^m-2}\sum_{i=0}^{2^m-2}(-1)^{u_i + v_{i+k}}$$

$$\begin{aligned} &= \sum_{i=0}^{2^m-2}(-1)^{u_i}\sum_{k=0}^{2^m-2}(-1)^{v_{i+k}} \\ &= (-1)(-1) \\ &= 1 \end{aligned} \tag{2.102}$$

Com essas três condições satisfeitas, obtêm-se seqüências LCZ-GMW binárias **a** e **b** com o método de geração de seqüências GMW (ou Lin-Chang), considerando agora as seqüências **u** e **v** como as sementes de **a** e **b**, respectivamente. A função de correlação par periódica será:

$$\theta_{\mathbf{ab}}(\tau) = \begin{cases} 2^{n-m} - 1 + 2^{n-m}\theta_{\mathbf{uv}}(d), & \text{para } \tau \neq 0 \text{ e } \tau = d\mathcal{T} \\ -1, & c.c. \end{cases} \tag{2.103}$$

sendo que $\theta_{\mathbf{ab}}(\tau) = N$ para $\tau = 0$ e $\mathbf{a} = \mathbf{b}$.

Fazendo $\mathbf{u} = \mathbf{x} + \mathbb{T}^{\ell_1}\mathbf{y}$ e $\mathbf{v} = \mathbf{x} + \mathbb{T}^{\ell_2}\mathbf{y}$, em (2.100) ter-se-á:

$$\theta_{\mathbf{uv}}(0) = \sum_{i=0}^{2^m-2}(-1)^{u_i+v_{(i+0)}} = \sum_{i=0}^{2^m-2}(-1)^{x_i+y_{(i+\ell_1)}+x_i+y_{(i+\ell_2)}} = \sum_{i=0}^{2^m-2}(-1)^{y_{(i+\ell_1)}+y_{(i+\ell_2)}} = \theta_{\mathbf{yy}}(\ell_2 - \ell_1) \tag{2.104}$$

Em (2.101) ter-se-á:

$$\theta_{\mathbf{uv}}(\infty) = \sum_{i=0}^{2^m-2}(-1)^{u_i} = \sum_{i=0}^{2^m-2}(-1)^{x_i+y_{(i+\ell_1)}} = \theta_{\mathbf{xy}}(\ell_1) \tag{2.105}$$

e em (2.102) ter-se-á:

$$\sum_{k=0}^{2^m-2}\theta_{\mathbf{uv}}(k) = \sum_{i=0}^{2^m-2}(-1)^{u_i}\sum_{k=0}^{2^m-2}(-1)^{v_{i+k}} = \theta_{\mathbf{xy}}(\ell_1)\,\theta_{\mathbf{xy}}(\ell_2) \tag{2.106}$$

Então, para que $\theta_{\mathbf{uv}}(0) = \theta_{\mathbf{yy}}(\ell_2 - \ell_1)$ resulte em -1 (condição dada por (2.100)), basta que **y** seja SMC. Para que $\theta_{\mathbf{uv}}(\infty) = \theta_{\mathbf{xy}}(\ell_1)$ resulte em -1 (condição dada por (2.101)) e $\sum_{k=0}^{2^m-2}\theta_{\mathbf{uv}}(k) = \theta_{\mathbf{xy}}(\ell_1)\ \theta_{\mathbf{xy}}(\ell_2)$ resulte em 1 (condição dada por (2.102)), deve-se garantir $\theta_{\mathbf{xy}}(\ell_1) = -1$ e $\theta_{\mathbf{xy}}(\ell_2) = -1$.

Com as observações anteriores, ficam estabelecidos os seguintes critérios para

obtenção de seqüências LCZ-GMW:

1. As sementes devem ser do tipo $\mathbf{u} = \mathbf{x} + \mathbb{T}^{\ell}\mathbf{y}$, com $\mathbf{x}$ e $\mathbf{y}$ SMC;
2. $\theta_{\mathbf{xy}}(\ell) = -1$;

Observa-se que ao conjunto gerado a partir das sementes do tipo $\mathbf{u} = \mathbf{x} + \mathbb{T}^{\ell}\mathbf{y}$, com $\mathbf{x}$ e $\mathbf{y}$ SMC, pode-se acrescentar uma seqüência gerada por uma SMC, $\mathbf{x}$ ou $\mathbf{y}$.

Para o caso de $\mathbf{u} = \mathbf{x}$ e $\mathbf{v} = \mathbf{x} + \mathbb{T}^{\ell_2}\mathbf{y}$, em (2.100) ter-se-á:

$$\theta_{\mathbf{uv}}(0) = \sum_{i=0}^{2^m-2}(-1)^{u_i+v_{(i+0)}} = \sum_{i=0}^{2^m-2}(-1)^{x_i+x_i+y_{(i+\ell_2)}} = \sum_{i=0}^{2^m-2}(-1)^{y_{(i+\ell_2)}} \tag{2.107}$$

Em (2.101) ter-se-á:

$$\theta_{\mathbf{uv}}(\infty) = \sum_{i=0}^{2^m-2}(-1)^{u_i} = \sum_{i=0}^{2^m-2}(-1)^{x_i} \tag{2.108}$$

e em (2.102) ter-se-á:

$$\sum_{k=0}^{2^m-2}\theta_{\mathbf{uv}}(k) = \sum_{i=0}^{2^m-2}(-1)^{u_i}\sum_{k=0}^{2^m-2}(-1)^{v_{i+k}} = \sum_{i=0}^{2^m-2}(-1)^{x_i}\,\theta_{\mathbf{xy}}(\ell_2) \tag{2.109}$$

Então, para que as condições dadas pelas equações (2.100) e (2.101) sejam satisfeitas, basta que $\mathbf{x}$ e $\mathbf{y}$ sejam seqüências balanceadas. Para que a condição dada pela equação (2.102) seja satisfeita, basta que $\theta_{\mathbf{xy}}(\ell_2) = -1$ e $\mathbf{x}$ seja balanceada.

Para o caso de $\mathbf{u} = \mathbf{x} + \mathbb{T}^{\ell_1}\mathbf{y}$ e $\mathbf{v} = \mathbf{x}$, em (2.100) ter-se-á:

$$\theta_{\mathbf{uv}}(0) = \sum_{i=0}^{2^m-2}(-1)^{u_i+v_{(i+0)}} = \sum_{i=0}^{2^m-2}(-1)^{x_i+y_{(i+\ell_1)}+x_i} = \sum_{i=0}^{2^m-2}(-1)^{y_{(i+\ell_1)}} \tag{2.110}$$

Em (2.101) ter-se-á:

$$\theta_{\mathbf{uv}}(\infty) = \sum_{i=0}^{2^m-2}(-1)^{u_i} = \sum_{i=0}^{2^m-2}(-1)^{x_i+y_{(i+\ell_1)}} = \theta_{\mathbf{xy}}(\ell_1) \tag{2.111}$$

e em (2.102) ter-se-á:

$$\sum_{k=0}^{2^m-2} \theta_{\mathbf{uv}}(k) = \sum_{i=0}^{2^m-2} (-1)^{u_i} \sum_{k=0}^{2^m-2} (-1)^{v_{i+k}} = \theta_{\mathbf{xy}}(\ell_1) \sum_{k=0}^{2^m-2} (-1)^{x_k} \tag{2.112}$$

Então, para que a condição dada pela equação (2.100) seja satisfeita, basta que **y** seja uma seqüência balanceada. Para que a condição dada pela equação (2.101) seja satisfeita, basta que $\theta_{\mathbf{xy}}(\ell_1) = -1$ e para que a condição dada pela equação (2.102) seja satisfeita, basta que $\theta_{\mathbf{xy}}(\ell_1) = -1$ e **x** seja também uma seqüência balanceada.

Como as SMC são balanceadas, a característica LCZ é verificada para o conjunto composto por seqüências geradas a partir das sementes $\mathbf{u} = \mathbf{x} + \mathbb{T}^{\ell}\mathbf{y}$, as quais satisfazem os critérios 1 e 2, e a partir de uma das SMC, **x** ou **y**.

A seguir é apresentado um algoritmo para gerar um família LCZ-GMW conforme as observações anteriores:

Algoritmo 2.1.1 *Algoritmo de geração de uma família de seqüências LCZ-GMW:*

1. *Obter duas SMC* $\boldsymbol{x}$ *e* $\boldsymbol{y}$*;*
2. *Obter um conjunto de deslocamentos* $\{\ell_1, \ell_2, ..., \ell_{K-1}\}$ *tal que:*

$$\theta_{\boldsymbol{xy}}(\ell_1) = \theta_{\boldsymbol{xy}}(\ell_2) = ... = \theta_{\boldsymbol{xy}}(\ell_{K-1}) = -1 \tag{2.113}$$

3. *Gerar o conjunto de sementes A:*

$$A = \left\{\boldsymbol{x}, \boldsymbol{x} + \mathbb{T}^{\ell_1}\boldsymbol{y}, \boldsymbol{x} + \mathbb{T}^{\ell_2}\boldsymbol{y}, ..., \boldsymbol{x} + \mathbb{T}^{\ell_{K-1}}\boldsymbol{y}\right\} \tag{2.114}$$

4. *Utilizar o método de geração de seqüências GMW (ou Lin-Chang) com as sementes do conjunto A.*

O algoritmo proposto em (LONG; ZHANG, 1995) e (TANG; FAN, 2001b) não é exatamente igual ao que foi apresentado aqui, porém, é fácil justificar porque ambos resultam em conjuntos de seqüências LCZ-GMW iguais. O algoritmo proposto em (LONG; ZHANG, 1995) e (TANG; FAN, 2001b) é apresentado a seguir:

Algoritmo 2.1.2 *Algoritmo de geração de uma família de seqüências LCZ-GMW proposto em (LONG; ZHANG, 1995) e (TANG; FAN, 2001b):*

1. *Obter duas seqüências GMW* $\boldsymbol{a'}$ *e* $\boldsymbol{b'}$ *a partir das SMC* $\boldsymbol{x}$ *e* $\boldsymbol{y}$*, respectivamente;*

2. *Obter um conjunto de deslocamentos* $\{\ell_1, \ell_2, ..., \ell_{K-1}\}$ *tal que:*

$$\theta_{\boldsymbol{xy}}(\ell_1) = \theta_{\boldsymbol{xy}}(\ell_2) = ... = \theta_{\boldsymbol{xy}}(\ell_{K-1}) = -1 \tag{2.115}$$

3. *Gerar o conjunto LCZ-GMW:*

$$\left\{\boldsymbol{a'}, \boldsymbol{a'} + \mathbb{T}^{\ell_1 \mathcal{T}}\boldsymbol{b'}, \boldsymbol{a'} + \mathbb{T}^{\ell_2 \mathcal{T}}\boldsymbol{b'}, ..., \boldsymbol{a'} + \mathbb{T}^{\ell_{K-1} \mathcal{T}}\boldsymbol{b'}\right\} \tag{2.116}$$

Para verificar que os dois algoritmos apresentados são equivalentes, considere duas seqüências GMW **a'** e **b'** dadas pela concatenação das linhas das matrizes **A'** e **B'**, respectivamente, como em (2.70):

$$\mathbf{A'} = \begin{bmatrix} x_{s_0} & x_{s_1} & x_{s_2} & \cdots & x_{s_{\mathcal{T}-1}} \\ x_{1+s_0} & x_{1+s_1} & x_{1+s_2} & \cdots & x_{1+s_{\mathcal{T}-1}} \\ x_{2+s_0} & x_{2+s_1} & x_{2+s_2} & \cdots & x_{2+s_{\mathcal{T}-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{2^m-2+s_0} & x_{2^m-2+s_1} & x_{2^m-2+s_2} & \cdots & x_{2^m-2+s_{\mathcal{T}-1}} \end{bmatrix} \tag{2.117}$$

e

$$\mathbf{B'} = \begin{bmatrix} y_{s_0} & y_{s_1} & y_{s_2} & \cdots & y_{s_{\mathcal{T}-1}} \\ y_{1+s_0} & y_{1+s_1} & y_{1+s_2} & \cdots & y_{1+s_{\mathcal{T}-1}} \\ y_{2+s_0} & y_{2+s_1} & y_{2+s_2} & \cdots & y_{2+s_{\mathcal{T}-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y_{2^m-2+s_0} & y_{2^m-2+s_1} & y_{2^m-2+s_2} & \cdots & y_{2^m-2+s_{\mathcal{T}-1}} \end{bmatrix} \tag{2.118}$$

onde **x** e **y** são SMC.

A seqüência $\mathbf{a} = \mathbf{a'} + \mathbb{T}^{\ell\mathcal{T}}\mathbf{b'}$ do terceiro item do algoritmo de (LONG; ZHANG, 1995) e (TANG; FAN, 2001b) será, em sua forma matricial **A** dada por:

$$\mathbf{A} = \begin{bmatrix} x_{s_0} + y_{s_0+\ell} & x_{s_1} + y_{s_1+\ell} & \cdots & x_{s_{\mathcal{T}-1}} + +y_{s_{\mathcal{T}-1}+\ell} \\ x_{1+s_0} + y_{1+s_0+\ell} & x_{1+s_1} + y_{1+s_1+\ell} & \cdots & x_{1+s_{\mathcal{T}-1}} + y_{1+s_{\mathcal{T}-1}+\ell} \\ x_{2+s_0} + y_{2+s_0+\ell} & x_{2+s_1} + y_{2+s_1+\ell} & \cdots & x_{2+s_{\mathcal{T}-1}} + y_{2+s_{\mathcal{T}-1}+\ell} \\ \vdots & \vdots & \ddots & \vdots \\ x_{2^m-2+s_0} + y_{2^m-2+s_0+\ell} & x_{2^m-2+s_1} + y_{2^m-2+s_1+\ell} & \cdots & x_{2^m-2+s_{\mathcal{T}-1}} + y_{2^m-2+s_{\mathcal{T}-1}+\ell} \end{bmatrix} \tag{2.119}$$

Esse resultado é uma seqüência gerada como uma GMW (ou Lin-Chang) a partir da semente $\mathbf{x} + \mathbb{T}^\ell\mathbf{y}$ como no algoritmo proposto nesta seção. Portanto, os algoritmos são equivalentes e resultam no mesmo conjunto LCZ-GMW, desde que as SMC utilizadas sejam iguais.

2.1.6.1 Propriedades de correlação de uma família LCZ-GMW

Conforme foi mostrado, uma família LCZ-GMW é construída de tal forma a apresentar uma zona de correlação reduzida com $L_{CZ} = \mathcal{T} - 1 = \frac{2^n-1}{2^m-1} - 1$. A função de correlação será dada por (2.103).

Observa-se que se o par de SMC **x** e **y** utilizado na construção de uma família LCZ-GMW for um par preferencial, tem-se **u** e **v** seqüências de Gold. Como os valores de correlação entre seqüências de Gold são bem definidos, na equação (2.103), tem-se $\theta_{\mathbf{uv}}$ bem definidos e, conseqüentemente, obtém-se os valores possíveis de correlação dessa família LCZ-GMW.

2.1.6.2 Número de seqüências LCZ-GMW de um dado comprimento

Em (TANG; FAN, 2001b) foram obtidas expressões para o tamanho de família LCZ-GMW para dois casos especiais. Ainda não foi obtida uma expressão geral para o tamanho exato de uma família LCZ-GMW. Porém, o limite de Tang-Fan (1.98) é uma medida razoável:

$$K \leq \frac{N^2 - 1}{(L_{CZ} + 1)(N - 1)} \tag{2.120}$$

onde N é o comprimento das seqüências, L_{CZ} define a zona de correlação reduzida e K é o número de seqüências na família.

Para, $m = 3$ e $n = 6$ tem-se $N = 63$, $L_{CZ} = 8$ $K = 4$. A desigualdade (2.120) fornece $K < 7,1111$. Esse limite é aplicável para qualquer família LCZ (quase ortogonal generalizada), não apenas à família LCZ-GMW analisada neste trabalho.

Especificamente para as seqüências LCZ-GMW, foi derivado em (TANG; FAN, 2001b) o limite inferior para a relação $\frac{K\,L_{CZ}}{N+1}$, dado por:

$$1 \geq \frac{K\,L_{CZ}}{N+1} \geq \begin{cases} 50\% & \text{para } m \text{ ímpar} \\ 75\% & \text{para } m \equiv 2 \pmod 4 \end{cases} \tag{2.121}$$

onde $N = 2^n - 1$ e $L_{CZ} = \mathcal{T} - 1 = \frac{2^n-1}{2^m-1} - 1$, com m fator de n assim como para as seqüências GMW.

2.1.6.3 Sumário das características das seqüências LCZ-GMW

As funções de autocorrelação e correlação cruzada periódica par assumem valor -1 para $0 < |\tau| < \mathcal{T}$ e $|\tau| < \mathcal{T}$, respectivamente, onde $\mathcal{T} = \frac{2^n-1}{2^m-1}$, m e n são inteiros, os quais representam o grau dos polinômios primitivos utilizados na construção das seqüências GMW que originam o conjunto LCZ-GMW binário. O comprimento das seqüências LCZ-GMW binárias é dado por $N = 2^n - 1$. As figuras 2.6.a e 2.6.b exemplificam as características das funções de correlação periódica par para seqüências LCZ-GMW binária com $n = 2m$ e $N = 63$. Ao contrário das funções de correlação periódica par, os valores da função de correlação periódica ímpar para o conjunto LCZ-GMW binário não são mínimos para $|\tau| < \mathcal{T}$, figura 2.7.

De acordo com (TANG; FAN; MATSUFUJI, 2000), para um conjunto LCZ-GMW composto de seqüências de comprimento N, existe um compromisso entre o tamanho K do conjunto e o valor de L_{CZ}: $\frac{KL_{CZ}}{N+1} \leq 1$. Quanto maior o valor de L_{CZ}, menor é o valor de K. Assim, o carregamento máximo para um conjunto de seqüências LCZ-GMW de comprimento N é obtido quando $n = 2m$, condição em que L_{CZ} é mínimo.

A próxima seção descreve as seqüências de No, as quais representam a generalização de SMC, seqüências GMW e seqüências da família pequena de Kasami (KASAMI, 1968).

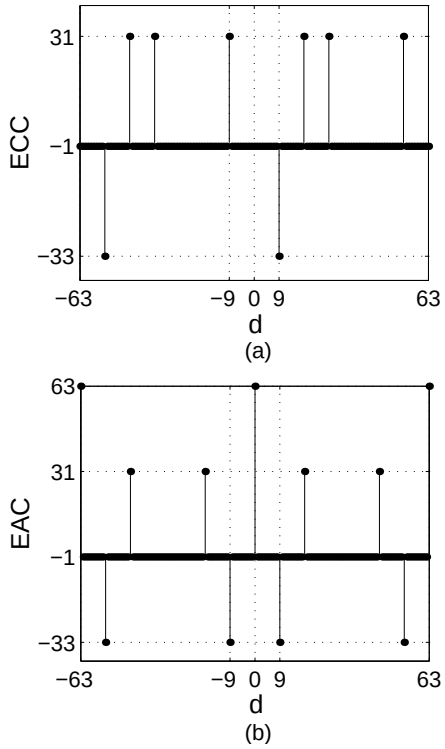

Figura 2.6: Exemplo para a (a) função de correlação cruzada periódica par e para a (b) função de autocorrelação periódica par de seqüências do conjunto LCZ-GMW com $n = 2m$ e $N = 63$.

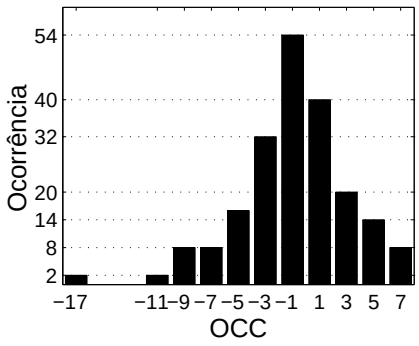

Figura 2.7: Histograma da função de correlação cruzada periódica ímpar do conjunto LCZ-GMW com $n = 2m$ e $N = 63$ e $|\tau| < 9$.

2.1.7 Família No

As seqüências de No foram propostas em (NO; KUMAR, 1989) como seqüências com propriedades ótimas de correlação periódica par e elevado equivalente linear.

O equivalente linear representa o número de células necessárias no circuito que implementa uma recorrência linear (B.47), figura B.1, para gerar a seqüência. É claro

que para as SMC, o número de células necessárias é m, onde m é o grau do polinômio primitivo. Para as seqüências não SMC de uma família de Gold, o número de células necessárias é $2m$, pois para a construção dessas seqüências são necessárias duas SMC. Para as seqüências GMW e Lin-Chang, esse número não é simples de ser obtido como no caso das SMC ou das seqüências de Gold, pois a construção de seqüências GMW e Lin-Chang envolvem operações não lineares que não permitem escrever a seqüência como um simples traço como a SMC (Teorema B.1.2). A medida do equivalente linear é importante para verificar a probabilidade de interceptação do sistema, ou a robustez contra a "quebra" da seqüência (código) ou do sigilo das informações moduladas por tais seqüências. Este trabalho não tem o objetivo de estudar a probabilidade de interceptação do sistema e, portanto, o equivalente linear das seqüências não será analisado.

As seqüências de No não foram propostas para sistemas QS-CDMA, porém, serão apresentadas aqui por representarem a generalização de SMC, seqüências GMW e da família pequena de Kasami (KASAMI, 1968).

As seqüências de uma família No são dadas por:

$$s_i(t) = Tr_1^m \left\{ \left[Tr_m^n(\alpha^{2t}) + \gamma_i \alpha^{\mathcal{T}t} \right]^r \right\} \tag{2.122}$$

onde $m = n/2$; r é um inteiro definido no intervalo $0 \leq r < 2^m - 1$ que satisfaz $\text{mdc}(r, 2^m - 1) = 1$; $\mathcal{T} = \frac{2^n-1}{2^m-1}$ como para as seqüências GMW e Lin-Chang sendo que nesse caso ($m = n/2$) tem-se $\mathcal{T} = 2^m + 1$. O comprimento da seqüência será $N = 2^n - 1$, pois com t variando de 0 a $2^n - 2$, tem-se α^{2t} percorrendo todos os elementos não nulos de $GF(2^n)$.

Para cada elemento γ, o qual pertence a $GF(2^m)$, obtém-se uma seqüência distinta de uma família No. Então, tem-se que o número de seqüências de uma família é dado por $K(m) = 2^m$, o que representa o número de elementos de $GF(2^m)$. Observe que os elementos γ_i de $GF(2^m)$ são $\alpha^{\mathcal{T}i}$, $i = 0, 1, 2, .., 2^m - 2$, além do elemento nulo.

O resultado de $Tr_m^n\{\alpha^{2t}\}$ em (2.122) pertence ao subcorpo $\{0, 1, \alpha^{\mathcal{T}}, \alpha^{\mathcal{T}2}, ..., \alpha^{\mathcal{T}(2^m-2)}\} \subset GF(2^m) \subset GF(2^n)$, pois a função traço mapeia elementos do corpo $GF(2^n)$ em elementos do subcorpo $GF(2^m)$.

Considere o argumento de $Tr_1^m\{.\}$ de (2.122). Esse pode ser visto como uma seqüência:

$$u_t = \left\{ Tr_m^n \left\{ \alpha^{2t} \right\} + \gamma_i \alpha^{\mathcal{T} t} \right\} \tag{2.123}$$

Pode-se interpretar $\left\{ \gamma_i \alpha^{\mathcal{T} t} \right\}$ como uma seqüência de comprimento $2^m - 1$, pois para um valor fixo de γ_i, com $\gamma_i \neq 0$, $\alpha^{\mathcal{T} t}$ percorre todos os elementos de $GF(2^m)$ exceto o nulo.

Sabe-se que $\{ Tr_m^n \{ \alpha^t \} \}$ é a definição de uma SMC que contém elementos sobre $GF(2^m)$, pois α^t percorre todos os elementos de $GF(2^n)$ e a função traço mapeia esses elementos em $GF(2^m)$. Assim, a porção $\left\{ Tr_m^n \left\{ \alpha^{2t} \right\} \right\}$ de u_t pode ser interpretada como uma decimação 2 da SMC anterior. Da propriedade do traço, $\left\{ Tr_m^n \left\{ \alpha^{2t} \right\} \right\} = \{ Tr_m^n \{ \alpha^t \} \}$, tem-se que $\left\{ Tr_m^n \left\{ \alpha^{2t} \right\} \right\}$ será a mesma SMC.

Quando $\gamma_i = 0$ em (2.122), tem-se:

$$s_i(t) = Tr_1^m \left\{ \left[Tr_m^n \left(\alpha^{2t} \right) \right]^r \right\} \tag{2.124}$$

que é uma seqüência GMW.

Observe que o inteiro r é expoente de elementos de $GF(2^m)$. Logo, esse é definido $0 \leq r < 2^m - 1$. Além disso, devido aos mesmos motivos apontados na seção 2.1.4 (seqüências GMW), r deve satisfazer $\text{mdc}(r, 2^m - 1) = 1$.

2.1.7.1 Família pequena e família grande de Kasami

Considerando o caso de $r = 1$ em (2.122), tem-se:

$$s_i(t) = Tr_1^m \left\{ \left[Tr_m^n \left(\alpha^{2t} \right) + \gamma_i \alpha^{\mathcal{T} t} \right]^1 \right\} \tag{2.125}$$

das propriedades da função traço:

$$Tr_1^n \{ \beta_1 + \beta_2 \} = Tr_1^n \{ \beta_1 \} + Tr_1^n \{ \beta_2 \} \tag{2.126}$$

e

$$Tr_1^m \{ Tr_m^n (\beta_i) \} = Tr_1^n \{ \beta_i \}, \quad \text{com } \beta_i \in GF(2^n) \tag{2.127}$$

tem-se que:

$$\begin{aligned} s_i(t) &= Tr_1^m \left\{ \left[Tr_m^n \left(\alpha^{2t} \right) + \gamma_i \alpha^{\mathcal{T} t} \right]^1 \right\} \\ &= Tr_1^m \left\{ Tr_m^n \left(\alpha^{2t} \right) \right\} + Tr_1^m \left\{ \gamma_i \alpha^{\mathcal{T} t} \right\} \\ &= Tr_1^n \left\{ \alpha^{2t} \right\} + Tr_1^m \left\{ \gamma_i \alpha^{\mathcal{T} t} \right\} \end{aligned} \tag{2.128}$$

O primeiro termo do lado direito de (2.128), $Tr_1^n \left\{ \alpha^{2t} \right\}$, é uma SMC de grau n (da definição de SMC de grau n, $Tr_1^n \left\{ \alpha^{2t} \right\}$, onde α^t percorre todo $GF(2^n)$). Conforme já foi indicado, da propriedade da função traço $Tr_m^n \left(\beta^{2^i} \right) = Tr_m^n (\beta)$ com $\beta \in GF(2^n)$, tem-se que $\left\{ Tr_1^n \left\{ \alpha^{2t} \right\} \right\}$ será a mesma SMC $\left\{ Tr_1^n \{ \alpha^t \} \right\}$.

O segundo termo de (2.128) é uma SMC de grau m, pois $\alpha^{\mathcal{T} t}$, $0 \leq t \leq N-1$ percorre todos os elementos de $GF(2^m)$ na medida que t varia, como já foi mencionado. O elemento γ_i que aparece multiplicando $\alpha^{\mathcal{T} t}$ apenas insere uma fase (ou deslocamento) na SMC de grau m, pois esse se mantém constante para cada seqüência No.

Então, tem-se uma SMC de grau n somada a uma SMC de grau $m = n/2$ deslocada conforme γ_i. Considerando todos os deslocamentos na medida que γ_i percorre $GF(2^m)$ exceto o elemento nulo, tem-se um conjunto conhecido como família pequena de Kasami (KASAMI, 1968). Adicionalmente, se o valor de r for $r = 2^i$, $i = 0, 1, 2, ...$, com $r < 2^m - 1$, o conjunto gerado é também uma família pequena de Kasami, pois, pela definição da função traço, $Tr_1^m \left(\beta^{2^i} \right) = Tr_1^m (\beta)$.

Considere agora, além da família pequena de Kasami, o conjunto composto por seqüências de Gold geradas através da SMC definida pelo elemento primitivo $\alpha \in GF(2^m)$ e da SMC definida pelo elemento primitivo $\beta = \alpha^{2^e+1}$, com $\text{mdc}(2e, m) = 1$, excluindo as SMC que originaram tal conjunto. Considere também um conjunto composto por seqüências de outra família pequena de Kasami gerada da SMC definida pelo elemento primitivo $\beta = \alpha^{2^e+1}$ e da mesma SMC de grau m definida pelo elemento primitivo $\alpha^{\mathcal{T}}$. Adicionando esses 2 conjuntos ao conjunto pequeno de Kasami anterior, obtém-se a família grande de Kasami, a qual apresentará, adicionalmente aos valores de correlação da família pequena de Kasami (que serão apresentados na seção seguinte), valores de correlação da família de Gold.

2.1.7.2 Propriedades de correlação de seqüências de No

Seja n, $n > 0$ e par, $N = 2^n - 1$, $m = n/2$ e $\mathcal{T} = 2^m + 1$. A família de seqüências de No será:

$$S = \{s_i(t) | 0 \leq t \leq N-1, 1 \leq i \leq 2^m\} \tag{2.129}$$

composta por 2^m seqüências binárias dadas por (2.122).

A função de correlação par periódica entre a i-ésima e a j-ésima seqüência da família é dada por:

$$\theta_{i,j}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_i(t+\tau)+s_j(t)}, \qquad 0 \leq \tau \leq N-1 \tag{2.130}$$

Para as seqüências de uma família de No é válido o teorema:

Teorema 2.1.7 *A função de correlação periódica par para a família de seqüências definida em (2.129) assume apenas os seguintes valores:*

$$\begin{aligned} \theta_{i,j}(\tau) \quad &\in \quad \{-2^m - 1, -1, 2^m - 1\}, \\ &\forall \ i, \ j, \ \tau \quad \text{com} \quad 1 \leq i, j \leq 2^m \quad \text{e} \quad 0 \leq \tau \leq N-1 \end{aligned} \tag{2.131}$$

com a restrição de $i \neq j$ ou $\tau \neq 0$. No caso $i = j$ e $\tau = 0$ tem-se, obviamente, $\theta_{i,j}(\tau) = N$.

A prova do Teorema 2.1.7 segue abaixo.

Sejam t_1 e t_2 os dígitos da expansão de t na base $\mathcal{T}$ onde $0 \leq t \leq N-1$:

$$t = \mathcal{T} t_1 + t_2, \qquad 0 \leq t_1 \leq 2^m - 2, \qquad 0 \leq t_2 \leq \mathcal{T} - 1 \tag{2.132}$$

Note que:

$$Tr_m^n(\alpha^{2(\mathcal{T}t_1+t_2)}) \quad = \quad \sum_{j=0}^{1} (\alpha^{2(\mathcal{T}t_1+t_2)})^{2^{mj}}$$

$$\begin{aligned} &= \alpha^{2\mathcal{T}t_1}\alpha^{2t_2} + \alpha^{2\mathcal{T}t_1 2^m}\alpha^{2t_2 2^m} \\ &= \alpha^{2\mathcal{T}t_1}\alpha^{2t_2} + \alpha^{2(2^m 2^m + 2^m)t_1}\alpha^{2t_2 2^m} \\ &= \alpha^{2\mathcal{T}t_1}\alpha^{2t_2} + \alpha^{2(2^{n/2}2^{n/2} + 2^m)t_1}\alpha^{2t_2 2^m} \\ &= \alpha^{2\mathcal{T}t_1}\alpha^{2t_2} + \alpha^{2(2^n + 2^m)t_1}\alpha^{2t_2 2^m} \\ &= \alpha^{2\mathcal{T}t_1}\alpha^{2t_2} + \left(\alpha^{2^n}\right)^{2t_1}\alpha^{2.2^m t_1}\alpha^{2t_2 2^m} \end{aligned} \tag{2.133}$$

como α é um elemento primitivo de $GF(2^n)$, tem-se que $\alpha^{2^i} = \alpha$. Assim:

$$\begin{aligned} Tr_m^n(\alpha^{2(\mathcal{T}t_1+t_2)}) &= \alpha^{2\mathcal{T}t_1}\alpha^{2t_2} + \alpha^{2t_1}\alpha^{2.2^m t_1}\alpha^{2t_2 2^m} \\ &= \alpha^{2\mathcal{T}t_1}\alpha^{2t_2} + \alpha^{2(2^m+1)t_1}\alpha^{2t_2 2^m} \\ &= \alpha^{2\mathcal{T}t_1}\alpha^{2t_2} + \alpha^{2\mathcal{T}t_1}\alpha^{2t_2 2^m} \\ &= \alpha^{2\mathcal{T}t_1}\left(\alpha^{2t_2} + \alpha^{2t_2 2^m}\right) \end{aligned} \tag{2.134}$$

da definição da função traço e de (2.134) tem-se que:

$$Tr_m^n(\alpha^{2(\mathcal{T}t_1+t_2)}) = \alpha^{2\mathcal{T}t_1}Tr_m^n(\alpha^{2t_2}) \tag{2.135}$$

Pode-se observar também que:

$$\begin{aligned} \alpha^{\mathcal{T}^2 t_1} &= \alpha^{(2^m+1)^2 t_1} = \alpha^{(2^{2m}+2.2^m+1)t_1} \\ &= \left(\alpha^{2^{\frac{2n}{2}}}\right)^{t_1}\alpha^{(2.2^m+1)t_1} = \left(\alpha^{2^n}\right)^{t_1}\alpha^{(2.2^m+1)t_1} \\ &= \alpha^{t_1+(2.2^m+1)t_1} = \alpha^{t_1(2.2^m+2)} = \alpha^{2(2^m+1)t_1} \\ &= \alpha^{2\mathcal{T}t_1} \end{aligned} \tag{2.136}$$

Com as identidades (2.135) e (2.136), as seqüências da família No podem ser escritas como:

$$s_i(t) = Tr_1^m\left\{\alpha^{2r\mathcal{T}t_1}\left[Tr_m^n(\alpha^{2t_2}) + \gamma_i\alpha^{\mathcal{T}t_2}\right]^r\right\} \tag{2.137}$$

Conseqüentemente, o expoente de cada termo da função de correlação periódica discreta (2.130) pode ser escrito como:

$$s_i(t+\tau) + s_j(t) = Tr_1^m \left\{ \alpha^{2r\mathcal{T}t_1} f_1(t_2) \right\} \tag{2.138}$$

onde definiu-se:

$$f_1(t) = \left[Tr_m^n(\alpha^{2(t+\tau)}) + \gamma_i \alpha^{\mathcal{T}(t+\tau)} \right]^r + \left[Tr_m^n(\alpha^{2t}) + \gamma_j \alpha^{\mathcal{T}t} \right]^r, \quad 0 \le t \le N-1 \tag{2.139}$$

Vale lembrar que, para caracterizar a função de correlação periódica discreta, basta caracterizar a seqüência $s_i(t+\tau) + s_j(t)$ definida por (2.138), ou seja, verificar a ocorrência de "zeros" e "uns" dessa seqüência.

Para um valor fixo de t_2, $0 \le t_2 \le \mathcal{T}-1$ tal que $f_1(t_2) \neq 0$, a seqüência $s_i(t+\tau)+s_j(t)$ em função de t_1 e com t_2 constante representa a definição clássica de SMC através da função traço, pois $\alpha^{\mathcal{T}i}$, $i = 0, 1, 2, ..., n$, são elementos de $GF(2^m)$. Essa SMC tem comprimento $2^m - 1$ e sua fase é determinada pelo valor de $f_1(t_2)$. É óbvio que, quando $f_1(t_2) = 0$, ter-se-á uma seqüência de $2^m - 1$ zeros em vez da SMC. A figura 2.8 ilustra a discussão desse parágrafo.

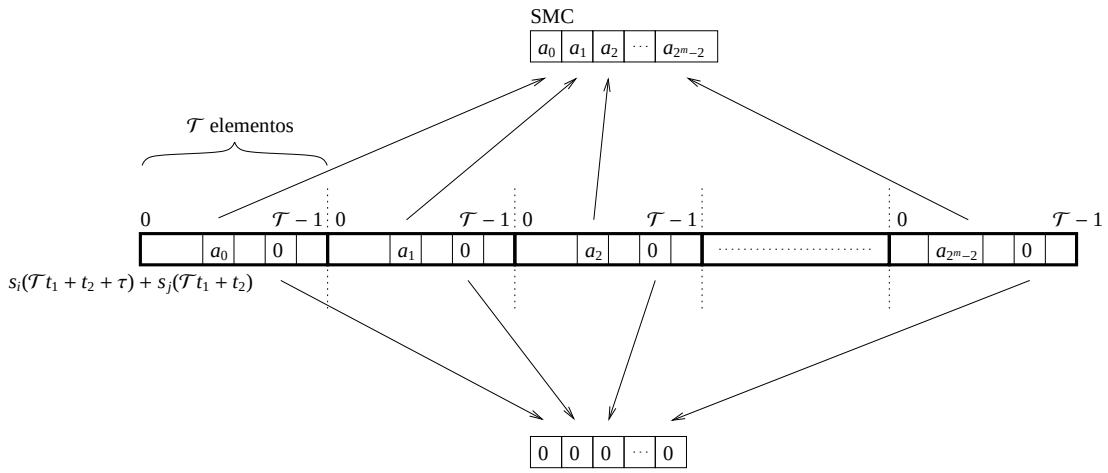

Figura 2.8: Característica do expoente de cada termo da soma da função de correlação periódica discreta.

Para contar quantos zeros existem na soma de seqüências $s_i(t+\tau) + s_j(t)$, define-se z_1 como o número de valores de t_2 para o qual $f_1(t_2) = 0$.

O problema da contagem de zeros será separado em duas condições:

1. $f_1(t_2) = 0$;

2. $f_1(t_2) \neq 0$.

Na primeira condição, quando tem-se $f_1(t_2) = 0$, a soma de seqüências $s_i(t+\tau) + s_j(t)$ terá esse "zero" repetido para todos $t = t_1\mathcal{T} + t_2$, com t_2 fixo. Como t_1 varia de 0 a $2^m - 2$, ter-se-á, portanto, $2^m - 1$ zeros na seqüência $s_i(t+\tau) + s_j(t)$ para cada $f_1(t_2) = 0$. Considerando todos os valores t_2 para o qual $f_1(t_2) = 0$, ter-se-á $z_1(2^m - 1)$ zeros na seqüência $s_i(t+\tau) + s_j(t)$.

Na segunda condição, observa-se que se $f_1(t_2) = 0$ ocorre z_1 vezes, conseqüentemente, $f_1(t_2) \neq 0$ ocorre $\mathcal{T} - z_1$ vezes, lembrando que $\mathcal{T} = 2^m + 1$ é o número de diferentes valores que t_2 pode assumir (2.132). Conforme já indicado anteriormente, quando $f_1(t_2) \neq 0$, a seqüência $s_i(t+\tau) + s_j(t)$ com $t = t_1\mathcal{T} + t_2$ e t_2 constante será uma SMC de comprimento $2^m - 1$. Na seção 2.1.1.1 mostrou-se que o número de zeros em uma SMC de comprimento $2^m - 1$ é dado por $2^{m-1} - 1$. Então, nesse caso ($f_1(t_2) \neq 0$), tem-se $(\mathcal{T} - z_1) \times (2^{m-1} - 1)$ "zeros" na seqüência $s_i(t+\tau) + s_j(t)$.

Combinando as duas condições $f_1(t_2) = 0$ e $f_1(t_2) \neq 0$, a seqüência $s_i(t+\tau) + s_j(t)$ assumirá valor zero $z_1(2^m - 1) + (\mathcal{T} - z_1)(2^{m-1} - 1)$ vezes.

Pode-se observar que elementos "uns" na seqüência $s_i(t+\tau) + s_j(t)$ só ocorrem quando $f_1(t_2) \neq 0$. Existem $\mathcal{T} - z_1$ valores de t_2 para os quais $f_1(t_2) \neq 0$. Com essa restrição ($f_1(t_2) \neq 0$), a seqüência $s_i(t+\tau) + s_j(t)$ será sempre SMC. Sabe-se que o número de "uns" em uma SMC de comprimento $2^m - 1$ é dado por 2^{m-1} (seção 2.1.1.1). Então, o total de "uns" em $s_i(t+\tau) + s_j(t)$ é $(\mathcal{T} - z_1)2^{m-1}$.

Com esses resultados, tem-se que a função de correlação par periódica é do tipo:

$$\begin{aligned} \theta_{i,j}(\tau) &= z_1(2^m - 1) + (\mathcal{T} - z_1)(2^{m-1} - 1) - (\mathcal{T} - z_1)2^{m-1} \\ &= 2^m(z_1 - 1) - 1 \end{aligned} \tag{2.140}$$

Para terminar a prova do Teorema 2.1.7 basta mostrar que z_1 assume apenas os valores 0, 1 ou 2, com γ_i e γ_j percorrendo todo $GF(2^m)$ e t variando na faixa $0 \leq t \leq N - 1$ descartando, é claro, a condição de $\gamma_i = \gamma_j$ e $t = 0$, pois, nesse caso, $\theta_{i,j}(t) = N$. Para tal demonstração, pode-se observar que de (2.139) tem-se:

$$f_1(t+\mathcal{T}) = \left[Tr_m^n\left(\alpha^{2(t+\mathcal{T}+\tau)}\right) + \gamma_i\alpha^{\mathcal{T}(t+\mathcal{T}+\tau)}\right]^r + \left[Tr_m^n\left(\alpha^{2(t+\mathcal{T})}\right) + \gamma_j\alpha^{\mathcal{T}(t+\mathcal{T})}\right]^r, 0 \le t \le N-1 \tag{2.141}$$

O termo $\gamma_i\alpha^{\mathcal{T}(t+\mathcal{T}+\tau)}$ que aparece em (2.141) pode ser escrito como:

$$\begin{aligned}\gamma_i\alpha^{\mathcal{T}(t+\mathcal{T}+\tau)} &= \gamma_i\alpha^{\mathcal{T}(t+\tau)+\mathcal{T}^2} = \gamma_i\alpha^{\mathcal{T}(t+\tau)}\alpha^{(2^m+1)^2} = \gamma_i\alpha^{\mathcal{T}(t+\tau)}\alpha^{2^{2m}+2.2^m+1} = \\ &= \gamma_i\alpha^{\mathcal{T}(t+\tau)}\alpha^{2^n+2.2^m+1} = \gamma_i\alpha^{\mathcal{T}(t+\tau)}\alpha^{2^n}\alpha^{2.2^m+1} = \gamma_i\alpha^{\mathcal{T}(t+\tau)}\alpha^{1}\alpha^{2.2^m+1} = \\ &= \gamma_i\alpha^{\mathcal{T}(t+\tau)}\alpha^{2.2^m+2} = \gamma_i\alpha^{\mathcal{T}(t+\tau)}\alpha^{2.\mathcal{T}}\end{aligned} \tag{2.142}$$

Analogamente, o termo $\gamma_j\alpha^{\mathcal{T}(t+\mathcal{T})}$ de (2.141) pode ser escrito como:

$$\gamma_j\alpha^{\mathcal{T}(t+\mathcal{T})} = \gamma_j\alpha^{\mathcal{T}t}\alpha^{2.\mathcal{T}} \tag{2.143}$$

O termo $Tr_m^n(\alpha^{2(t+\mathcal{T}+\tau)})$ que também aparece em (2.141) pode ser escrito como:

$$\begin{aligned}Tr_m^n(\alpha^{2(t+\mathcal{T}+\tau)}) &= \sum_{j=0}^{1}\left(\alpha^{2(t+\mathcal{T}+\tau)}\right)^{2^{mj}} \\ &= \alpha^{2(t+\mathcal{T}+\tau)} + \alpha^{2(t+\mathcal{T}+\tau)2^m} = \\ &= \alpha^{2\mathcal{T}}\alpha^{2(t+\tau)} + \alpha^{2\mathcal{T}2^m}\alpha^{2(t+\tau)2^m} \\ &= \alpha^{2\mathcal{T}}\alpha^{2(t+\tau)} + \alpha^{2(2^m+1)2^m}\alpha^{2(t+\tau)2^m} \\ &= \alpha^{2\mathcal{T}}\alpha^{2(t+\tau)} + \alpha^{2(2^{2m}+2^m)}\alpha^{2(t+\tau)2^m} \\ &= \alpha^{2\mathcal{T}}\alpha^{2(t+\tau)} + \alpha^{2(2^n+2^m)}\alpha^{2(t+\tau)2^m} \\ &= \alpha^{2\mathcal{T}}\alpha^{2(t+\tau)} + \left(\alpha^{2^n}\right)^2\alpha^{2.2^m}\alpha^{2(t+\tau)2^m} \\ &= \alpha^{2\mathcal{T}}\alpha^{2(t+\tau)} + \alpha^{2}\alpha^{2.2^m}\alpha^{2(t+\tau)2^m} \\ &= \alpha^{2\mathcal{T}}\alpha^{2(t+\tau)} + \alpha^{2\mathcal{T}}\alpha^{2(t+\tau)2^m} \\ &= \alpha^{2\mathcal{T}}\left(\alpha^{2(t+\tau)} + \alpha^{2(t+\tau)2^m}\right) \\ &= \alpha^{2\mathcal{T}}Tr\left(\alpha^{2(t+\tau)}\right)\end{aligned} \tag{2.144}$$

Analogamente, o termo $Tr_m^n(\alpha^{2(t+\mathcal{T})})$ de (2.141) pode ser escrito como:

$$Tr_m^n(\alpha^{2(t+\mathcal{T})}) = \alpha^{2\mathcal{T}} Tr_m^n(\alpha^{2t}) \tag{2.145}$$

Assim, substituindo (2.142) a (2.145) em (2.141):

$$\begin{aligned} f_1(t+\mathcal{T}) &= \left[\alpha^{2\mathcal{T}}\left(Tr_m^n\left(\alpha^{2(t+\tau)}\right) + \gamma_i \alpha^{\mathcal{T}(t+\tau)}\right)\right]^r + \left[\alpha^{2\mathcal{T}}\left(Tr_m^n\left(\alpha^{2(t)}\right) + \gamma_j \alpha^{\mathcal{T}(t)}\right)\right]^r \\ &= \alpha^{2r\mathcal{T}} f_1(t), 0 \le t \le N-1 \end{aligned} \tag{2.146}$$

onde $f_1(t)$ é dado por (2.139).

Lembrando que z_1 denota o número de valores de t_2 para o qual $f_1(t_2) = 0$ com $0 \le t_2 \le \mathcal{T} - 1$. Se z_2 denota o número de vezes que $f_1(t) = 0$ com t variando em $0 \le t \le N-1 = 2n-1 = 2^{2m}-1 = (2^m-1)(2^m+1) = (2^m-1)\mathcal{T}$, tem-se que:

$$z_1 = \frac{z_2}{2^m - 1} \tag{2.147}$$

Ou seja, se $f_1(t_2) = 0$, então $f_1(t_2+\mathcal{T}) = 0$, conforme resultado da equação (2.146), e também $f_1(t) = 0$, com $t = t_1\mathcal{T} + t_2$ e $t_1 = 0, 1, 2, ..., 2^m - 2$. Observe que t_1 assume $2^m - 1$ valores diferentes para cada t_2 tal que $f_1(t_2) = 0$. Então, se existem z_1 valores de t_2 tal que $f_1(t_2) = 0$, existem $(2^m - 1)z_1$ valores de t tais que $f_1(t) = 0$. Assim, o resultado acima (2.147) é obtido. Define-se:

$$f_2(t) = Tr_m^n\left\{\alpha^{2t}\left(1 + \alpha^{2\tau}\right)\right\} + \alpha^{\mathcal{T}t}\left(\gamma_i \alpha^{\mathcal{T}\tau} + \gamma_j\right), 0 \le t \le N-1 \tag{2.148}$$

o que equivale à definição de $f_1(t)$ (2.139) com $r = 1$. Como mdc$(r, 2^m - 1) = 1$:

$$f_2(t) = 0 \Leftrightarrow f_1(t) = 0, \qquad 0 \le t \le N-1 \tag{2.149}$$

Então, em vez de contar o número de "zeros" de $f_1(t)$, contar-se-á o número de "zeros" de $f_2(t)$.

Seja $x = \alpha^t$. Então, x percorre todos os elementos diferentes de zero de $GF(2^n)$ na medida que t percorre o intervalo de 0 a $N-1$. Reescrevendo $f_2(.)$ agora em função de x:

$$\begin{aligned} f_2(x) &= Tr_m^n\left\{x^2\left(1+\alpha^{2\tau}\right)\right\} + x^{2^m+1}\left(\gamma_i\alpha^{\mathcal{T}\tau}+\gamma_j\right) \\ &= x^2\left(1+\alpha^{2\tau}\right) + x^{2^{m+1}}\left(1+\alpha^{2\tau}\right)^{2^m} + x^{2^m+1}\left(\gamma_i\alpha^{\mathcal{T}\tau}+\gamma_j\right) \\ &= x^2\left\{y^2\left(1+\alpha^{2\tau}\right)^{2^m} + y\left(\gamma_i\alpha^{\mathcal{T}\tau}+\gamma_j\right) + \left(1+\alpha^{2\tau}\right)\right\} \end{aligned} \quad (2.150)$$

onde $y = x^{2^m-1}$.

A função $f_2(.)$ é dada pela multiplicação de x^2 por um polinômio quadrático em y. Para determinar quantas vezes $f_2(x) = 0$, o problema será separado em dois casos:

1. $\tau = 0, \gamma_i \neq \gamma_j$;
2. $\tau \neq 0$.

No primeiro caso, tem-se:

$$\begin{aligned} f_2(x) &= x^2\left\{y^2(1+1)^{2^m} + y\left(\gamma_i+\gamma_j\right) + (1+1)\right\} \\ &= x^2 y\left(\gamma_i+\gamma_j\right) \end{aligned} \quad (2.151)$$

Assim, $f_2(x)$ nunca assumirá valor nulo. Então, $z_1 = 0$ e $z_2 = 0$, resultando em:

$$\theta_{i,j}(0) = -2^m - 1, \qquad \text{para } i \neq j \quad (2.152)$$

No segundo caso, $f_2(x) = 0$ se e somente se o polinômio quadrático for zero, ou seja se $y = \alpha^{t_2(2^m-1)}$ for raiz do polinômio. Como o polinômio quadrático está sobre $GF(2^n)$, pode-se ter 0, 1, ou 2 raízes em $GF(2^n)$.

Se não existir raiz, ou seja, se não existir t_2 tal que $y = \alpha^{t_2(2^m-1)}$ seja raiz do polinômio, $f_2(.)$ não assumirá valor zero nesse caso ($\tau \neq 0$) e, portanto, $z_1 = z_2 = 0$.

Se existir uma raiz, ou seja, $y = \alpha^{t_2(2^m-1)}$ for raiz do polinômio para algum $\alpha \in GF(2^n)$, então, $\alpha^{t_2(2^m-1)}$, com $t_2 = 1, 2, ..., 2^{n/2} - 1$, serão também raízes do polinômio. Assim ter-se-á $2^{n/2} - 1 = 2^m - 1$ valores de t_2 tais que $f_2(t_2) = 0$, ou seja, $z_2 = 2^m - 1$ e, portanto, $z_1 = 1$.

Se existirem duas raizes, ou seja, $y_1 = \alpha_1^{t_2(2^m-1)}$ e $y_2 = \alpha_2^{t_2(2^m-1)}$, com α_1 e $\alpha_2 \in$

$GF(2^n)$ e $\alpha_1 \neq \alpha_2^{2^J}$, $J = 0, 1, 2, ..., 2^m - 1$, ou seja, α_1 e α_2 não são conjugados, então, $\left(\alpha_1^{t_2(2^m-1)}\right)^k = \alpha_1^{t_2(2^m-1)k}$ e $\left(\alpha_2^{t_2(2^m-1)}\right)^k = \alpha_2^{t_2(2^m-1)k}$, com $k = 1, 2, ..., 2^{n/2} - 1$, serão também raízes do polinômio. Assim ter-se-á $2(2^{n/2} - 1) = 2(2^m - 1)$ valores de t_2 tais que $f_2(t_2) = 0$, ou seja, $z_2 = 2(2^m - 1)$ e, portanto, $z_1 = 2$. Então, no segundo caso, $t \neq 0$, z_1 pode assumir os valores 0, 1 e 2.

Mostrou-se que z_1 assume apenas os valores 0, 1 e 2, o que resulta, de (2.140), em:

$$\begin{aligned} \theta_{i,j}(\tau) \quad &\in \quad \{-2^m - 1, -1, 2^m - 1\}, \\ &\forall \ i, \ j, \ \tau \quad \text{com} \quad 1 \leq i, j \leq 2^m \quad \text{e} \quad 0 \leq \tau \leq N - 1 \end{aligned} \tag{2.153}$$

assim, o Teorema 2.1.7 está provado.

2.1.7.3 Número de seqüências No de um dado comprimento

O número de seqüências de comprimento $N = 2^n - 1$ em uma família No, ou o tamanho de uma família No, será:

$$K(m) = 2^m \tag{2.154}$$

com $n = 2m$, pois, como já mencionado, para cada elemento $\gamma \in GF(2^m)$ em (2.122), obtém-se uma seqüência distinta de uma família No.

O número de famílias No é dado pelo número de polinômios primitivos de grau n dado por $\phi(2^n - 1)/n$, pois para cada corpo $GF(2^n)$, tem-se uma família No distinta.

Então, o total de seqüências No, considerado-se todas as famílias, será:

$$2^m \times \phi(2^n - 1)/n \tag{2.155}$$

2.1.8 Sumário das seqüências quase ortogonais

Foram apresentadas as SMC, seqüências Gold, QS, GMW, Lin-Chang, LCZ-GMW e No. Os métodos de obtenção das seqüências de Gold, QS, Lin-Chang, LCZ-GMW e No são baseados nas características das SMC e GMW.

A função de correlação par periódica $\theta_{i,j}(\tau)$ de um par preferencial de SMC apre-

senta apenas três valores para $i \neq j$ e, adicionalmente, valor N para $i = j$ e $\tau = 0$. Utilizando-se dessa propriedade, deriva-se a família de seqüências de Gold. Selecionando-se seqüências de uma família de Gold que resultam em valores reduzidos para a função de correlação par periódica em torno da origem, obtém-se um subconjunto com zona de correlação par periódica reduzida (LCZ). Esse subconjunto de Gold é denominado família de seqüências QS.

Observando-se a função de correlação cruzada par periódica de seqüências GMW de comprimento $N = 2^n - 1$ construídas de um mesmo polinômio primitivo de grau n, verifica-se que para essa função apresentar $\theta_{i,j}(\tau) = -1$ para $\tau \neq 0 \pmod{\mathcal{T}}$, com $\mathcal{T}$ definido anteriormente, não é necessário que as seqüências sementes sejam SMC. Caso as seqüências forem apenas balanceadas, não necessariamente SMC, essa característica também é obtida. O conjunto de seqüências geradas conforme as seqüências GMW de um mesmo polinômio primitivo de grau n, porém com sementes balanceadas, não necessariamente SMC, é chamado de família Lin-Chang. Adicionalmente, se a função de correlação cruzada par periódica na origem entre as sementes resultar em -1, as respectivas seqüências Lin-Chang possuirão uma zona de correlação par periódica reduzida (LCZ) dada por $L_{CZ} = \mathcal{T} - 1$, com $\mathcal{T}$ conforme definido anteriormente.

Observando-se ainda a função de correlação cruzada par periódica de seqüências GMW de comprimento $N = 2^n - 1$ construídas de um mesmo polinômio primitivo de grau n, obtém-se outra condição em que ocorre zona de correlação reduzida dada por $L_{CZ} = \mathcal{T} - 1$. Agora, as sementes são obtidas de SMC. Esse outro conjunto de seqüências LCZ, cujo método de geração é baseado no método de geração de seqüências GMW obtidas de um mesmo polinômio primitivo de grau n, é chamado de família LCZ-GMW.

Por fim, foi apresentada a família No. Essa família sempre possuirá uma seqüência GMW. Em casos particulares, essa família recai na família pequena de Kasami. Dessa forma, mostra-se que as seqüências No representam a generalização de SMC, seqüências GMW e seqüências da família pequena de Kasami. A família No não apresenta LCZ, porém, apresenta apenas 3 valores de correlação par periódica para $i \neq j$ e, adicionalmente, valor N para $i = j$ e $\tau = 0$.

A Figura 2.1.8 representa, em termos de conjuntos, as famílias de seqüências sobre $GF(2)$ apresentadas aqui.

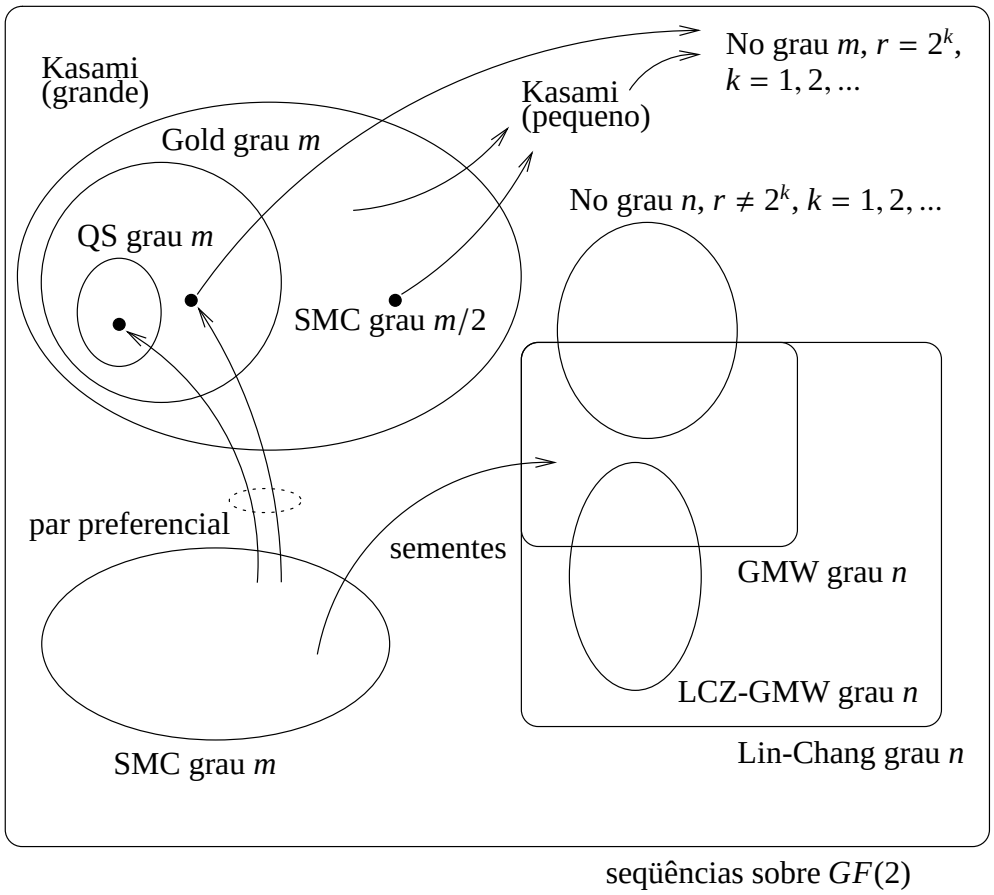

Figura 2.9: O universo de seqüências sobre $GF(2)$ e as famílias de seqüências apresentadas.

A partir de um par preferencial de SMC é obtida uma família de Gold a qual contém o par preferêncial. De uma família de Gold obtém-se um subconjunto de seqüências que resultam em LCZ chamado de família QS. A família grande de Kasami contém uma família de Gold. A família pequena de Kasami é composta pelas seqüências da família grande de Kasami que não pertencem à família de Gold. A família No de grau n, com $r = 2^k$ e $k = 1, 2, ...$, é composta pelas seqüências da família pequena de Kasami e a SMC de grau $m/2$, a qual gera a família pequena de Kasami.

As seqüências GMW construídas de um mesmo polinômio primitivo de grau n, as quais constituem uma família GMW, são obtidas das SMC de grau m, com m fator de n. A família Lin-Chang é composta por todas as seqüências da família GMW e por outras que resultam em uma função de correlação cruzada periódica par semelhante à da família GMW. As seqüências LCZ-GMW são compostas por seqüências GMW e Lin-Chang que resultam em LCZ. A família No de grau n, com $r \neq 2^k$ e $k = 1, 2, ...$,

possui uma seqüência GMW e outras que resultam em apenas três valores de $\theta_{i,j}(\tau)$ para $i \neq j$ e, adicionalmente, valor N para $i = j$ e $\tau = 0$.

A próxima seção apresentará as famílias de seqüências ortogonais generalizadas OQS e ZCZ. Serão também apresentadas as seqüências Walsh-Hadamard, as quais são casos particulares das seqüências ZCZ.

2.2 Seqüências ortogonais e ortogonais generalizadas

2.2.1 Família OQS

A família OQS (*orthogonal QS-sequence*) foi proposta em (SAITO et al., 2001). Essa família possui zona de correlação zero, característica desejável para sistemas QS-CDMA.

A metodologia de construção de uma família OQS é semelhante à construção de uma família QS. A partir de uma família de seqüências de Gold de comprimento $N = 2^n - 1$ construídas conforme descrito na seção 2.1.3, são inseridos chips $c = 0$ ou $c = 1$ após o i-ésimo chip e antes do $(i + 1)$-ésimo chip de todas as seqüências do conjunto, resultando em uma família de seqüência de comprimento $N = 2^n$. Esse conjunto é chamado de Gold ortogonal (*orthogonal Gold*) e denotado por $OGold(X, Y, c, i)$, onde X e Y representam, em notação octal, os polinômios primitivos utilizado na construção da família de Gold. A família OQS-r é obtida da busca exaustiva por seqüências do conjunto Gold ortogonal $OGold(X, Y, c, i)$ que resultam em:

$$\theta(\mathbf{x}, \mathbf{y}, d) = \begin{cases} 0 & \text{para } \mathbf{x} \neq \mathbf{y} \text{ e } |d| \leq Z_{CZ} = \frac{r-1}{2} \\ 0 & \text{para } \mathbf{x} = \mathbf{y} \text{ e } 0 < |d| \leq Z_{CZ} = \frac{r-1}{2} \\ N & \text{para } \mathbf{x} = \mathbf{y} \text{ e } d = 0 \end{cases} \tag{2.156}$$

Em (SAITO et al., 2001), foi observado que nem todas as famílias $OGold(X, Y, c, i)$ podem produzir conjuntos OQS com grande número de seqüência. Esse artigo investigou as famílias de seqüências de Gold ortogonal de comprimento $N = 32$ que podem produzir famílias OQS compostas de 8 seqüências e $Z_{CZ} = 1$. Essas famílias de Gold ortogonal são: $OGold(45, 47, c, 18)$, $OGold(45, 73, c, 18)$, $OGold(47, 51, c, 12)$, $OGold(47, 67, c, 12)$, $OGold(51, 67, c, 17)$, $OGold(51, 75, c, 17)$ e $OGold(65, 75, c, 27)$, com $c = 1$ ou $c = 0$.

2.2.2 Seqüências Walsh-Hadamard

As seqüências $\mathbf{c}_i$ de Walsh-Hadamard (WH) são obtidas das linhas (ou colunas) da matriz quadrada de Hadamard H_n (PROAKIS, 1995):

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}, \qquad H_0 = [1]$$

$$\mathbf{c}_i = \{h_{i,0} h_{i,1} ... h_{i,2^n-1}\} \tag{2.157}$$

onde $\mathbf{c}_i$ representa a i-ésima seqüência do conjunto Walsh-Hadamard composto de elementos h_i bipolarizados $\{+1, -1\}$ obtidos da i-ésima linha da matriz H_n.

É fácil verificar que a função de correlação periódica par na origem para as seqüências Walsh-Hadamard de comprimento 2, obtidas de H_1, assume valor zero. Para seqüências $\mathbf{c}_i$ e $\mathbf{c}_j$ de comprimento 4, obtidas de H_2, a função de correlação cruzada par periódica será:

$$\theta(\mathbf{c}_i, \mathbf{c}_j, 0) = \begin{cases} \theta(\mathbf{a}, \mathbf{b}, 0) + \theta(\mathbf{a}, \mathbf{b}, 0), & \text{para } |i-j| \leq 2 \\ \theta(\mathbf{a}, \mathbf{b}, 0) - \theta(\mathbf{a}, \mathbf{b}, 0), & \text{para } |i-j| > 2 \end{cases} \tag{2.158}$$

onde $\mathbf{a}$ e $\mathbf{b}$ são seqüências de comprimento 2 obtidas de H_1. Para $|i-j| \leq 2$ é fácil ver que $\mathbf{a} \neq \mathbf{b}$ e $\theta(\mathbf{a}, \mathbf{b}, 0) = 0$. Assim, $\theta(\mathbf{c}_i, \mathbf{c}_j, 0) = 0$.

Genericamente, para seqüências de comprimento $N = 2^n$ obtidas de H_n, a função de correlação cruzada periódica par na origem será:

$$\theta(\mathbf{c}_i, \mathbf{c}_j, 0) = \begin{cases} \theta(\mathbf{a}, \mathbf{b}, 0) + \theta(\mathbf{a}, \mathbf{b}, 0), & \text{para } |i-j| \leq N/2 \\ \theta(\mathbf{a}, \mathbf{b}, 0) - \theta(\mathbf{a}, \mathbf{b}, 0), & \text{para } |i-j| > N/2 \end{cases} \tag{2.159}$$

onde $\mathbf{a}$ e $\mathbf{b}$ são seqüências de comprimento $N/2$ obtidas de H_{n-1}. Para $|i-j| \leq N/2$ é fácil ver que $\mathbf{a} \neq \mathbf{b}$ e, nesse caso, $\theta(\mathbf{a}, \mathbf{b}, 0) = 0$, pois $\mathbf{a}$ e $\mathbf{b}$ são ortogonais (linhas de H_{n-1}). Assim, $\theta(\mathbf{c}_i, \mathbf{c}_j, 0) = 0$.

Fora da origem não existe uma expressão geral para as funções de correlação. Observa-se que o conjunto possui seqüências ciclicamente equivalentes e seqüências com período menor que $N = 2^n$. Essa característica é devido ao método de construção, onde cada seqüência de comprimento N do conjunto é uma concatenação de seqüências

de comprimento $N/2$. Assim, as funções de correlação fora da origem podem assumir valores elevados.

Como as seqüências Walsh-Hadamard são obtidas das linhas (ou colunas) de H_n, a qual é uma matriz quadrada $2^n \times 2^n$, o número de seqüências em um conjunto Walsh-Hadamard será $K = 2^n$.

A próxima seção apresentará um método de construção de seqüências semelhante ao método de construção das seqüências Walsh-Hadamard, porém, com esse método obtém-se seqüências adequadas para sistemas QS-CDMA. A seção 3.3.1 descreverá um método de seleção de seqüências Walsh-Hadamard para sistemas DS/CDMA síncronos multitaxa do tipo MPG.

2.2.3 Família ZCZ binária

Analogamente à LCZ, a zona de correlação zero (*zero correlation zone*, ZCZ) representa o intervalo $|\tau| \leq Z_{CZ}$ em que a função de correlação periódica par $\theta_{i,j}(\tau)$ assume valor nulo (exceto para $i = j$ e $\tau = 0$). As seqüências que apresentam essa característica são chamadas de seqüências ZCZ ou ortogonais generalizadas. Um conjunto de seqüências que possuem a característica ZCZ é chamado de família ZCZ. Por exemplo, uma família OQS é uma família ZCZ. Porém, para simplificar a notação, a nomenclatura ZCZ será utilizada para a família de seqüências propostas em (FAN; KUROYANAGI; DENG, 1999) e (DENG; FAN, 2000).

Em (DENG; FAN, 2000) foi observado que conjuntos de seqüências mutuamente ortogonais, construídos conforme o Teorema 13 de (TSENG; LIU, 1972), possuem a característica ZCZ. O estudo de conjuntos de seqüências complementares mutuamente ortogonais foi iniciado por Tseng e Liu em (TSENG; LIU, 1972), motivado por trabalhos sobre séries complementares, principalmente o trabalho de Golay de 1961 (GOLAY, 1961). Séries complementares são seqüências finitas de mesmo comprimento tal que a soma de suas funções de autocorrelação periódica par $\theta(\mathbf{a}, \mathbf{a}, d)$, para qualquer d diferente de zero, resulta em zero. São chamados de complementares mutuamente ortogonais os conjuntos de seqüências tais que tanto a soma de suas funções de autocorrelação periódica par quanto a soma de suas funções de correlação cruzada periódica par resultam em zero, para qualquer d diferente de zero.

A construção de uma família ZCZ utiliza-se de um procedimento recorrente. Parte-

se de um conjunto de seqüências complementares mutuamente ortogonais chamado de conjunto base e, então, por meio de uma recorrência linear obtém-se conjuntos com maior número de seqüências de maior comprimento e maior zona de correlação zero. O método de construção é apresentado a seguir.

Seja F^n uma matriz geradora do conjunto ZCZ composto por K seqüências de comprimento N. A matriz ou conjunto base $n = 0$ de ordem m, utilizado para a geração de um conjunto ZCZ é dado por:

$$F^0 = \begin{bmatrix} F_{11}^0 & F_{12}^0 \\ F_{21}^0 & F_{22}^0 \end{bmatrix} = \begin{bmatrix} -X^m & Y^m \\ -\bar{Y}^m & \bar{X}^m \end{bmatrix}_{2\times 2^{m+1}} \tag{2.160}$$

com

$$\begin{aligned} [X^0, Y^0] &= [1, 1] \\ [X^m, Y^m] &= [X^{m-1}Y^{m-1}, (-X^{m-1})Y^{m-1}] \end{aligned} \tag{2.161}$$

onde $-\mathbf{a}$ denota a seqüência composta por elementos opostos aos da seqüência $\mathbf{a}$; $\bar{\mathbf{a}}$ denota a forma reversa da seqüência $\mathbf{a}$:

$$\mathbf{a} = [a_1, a_2, ..., a_N]$$

$$-\mathbf{a} = [-a_1, -a_2, ..., -a_N] \tag{2.162}$$

$$\bar{\mathbf{a}} = [a_N, a_{N-1}, ..., a_1] \tag{2.163}$$

A matriz F^0 (matriz ou conjunto base) é um conjunto ZCZ de tamanho $K = 2$ e $Z_{CZ} = 2^{m-1}$, composto por seqüências de comprimento $N = 2^{m+1}$, conforme definido em (FAN; KUROYANAGI; DENG, 1999).

A partir do conjunto base F^0, um conjunto ZCZ de $n = 1$, F^1, pode ser construído utilizando a seguinte fórmula:

$$
\begin{aligned}
F^1 &= \begin{bmatrix} F^1_{11} & F^1_{12} & F^1_{13} & F^1_{14} \\ F^1_{21} & F^1_{22} & F^1_{23} & F^1_{24} \\ F^1_{31} & F^1_{32} & F^1_{33} & F^1_{34} \\ F^1_{41} & F^1_{42} & F^1_{43} & F^1_{44} \end{bmatrix} \\
&= \begin{bmatrix} F^0_{11}F^0_{11} & F^0_{12}F^0_{12} & (-F^0_{11})F^0_{11} & (-F^0_{12})F^0_{12} \\ F^0_{21}F^0_{21} & F^0_{22}F^0_{22} & (-F^0_{21})F^0_{21} & (-F^0_{22})F^0_{22} \\ (-F^0_{11})F^0_{11} & (-F^0_{121})F^0_{12} & F^0_{11}F^0_{11} & F^0_{12}F^0_{12} \\ (-F^0_{21})F^0_{21} & (-F^0_{22})F^0_{22} & F^0_{21}F^0_{21} & F^0_{22}F^0_{22} \end{bmatrix}
\end{aligned} \tag{2.164}
$$

onde $F^n_{i_1 j_1} F^n_{i_2 j_2}$ denota a concatenação da seqüência $F^n_{i_1 j_1}$ com a seqüência $F^n_{i_2 j_2}$:

$$
\begin{aligned}
F^n_{i_1 j_1} &= \left[a_1, a_2, ..., a_{\frac{2^{n+m-1}+1}{2}} \right] \\
F^n_{i_2 j_2} &= \left[c_1, c_2, ..., c_{\frac{2^{n+m-1}+1}{2}} \right] \\
F^n_{i_1 j_1} F^n_{i_2 j_2} &= \left[a_1, a_2, ..., a_{\frac{2^{2n+2m+1}}{2}}, c_1, c_2, ..., c_{\frac{2^{2n+2m+1}}{2}} \right]
\end{aligned} \tag{2.165}
$$

Generalizando, a partir de um conjunto ZCZ F^{n-1}, um conjunto maior F^n pode ser construído por meio da recorrência:

$$
F^n = \begin{bmatrix} F^n_{11} & ... & F^n_{1K} & F^n_{1(K+1)} & ... & F^n_{1(2K)} \\ F^n_{21} & ... & F^n_{2K} & F^n_{2(K+1)} & ... & F^n_{1(2K)} \\ ... & & & & & \\ ... & & & & & \\ F^n_{(2K-1),1} & ... & F^n_{(2K-1),K} & F^n_{(2K-1),(K+1)} & ... & F^n_{(2K-1),(2K)} \\ F^n_{(2K),1} & ... & F^n_{(2K),K} & F^n_{(2K)(K+1)} & ... & F^n_{(2K),(2K)} \end{bmatrix}_{2^{n+1} \times 2^{2n+m+1}} \tag{2.166}
$$

onde o tamanho do conjunto F^{n-1} é $K = 2^n$, para $n > 0$. $F^n_{i,j}$ e $F^n_{(i+M),(j+M)}$, com $1 \leq i, j \leq K$, é dado por:

$$\begin{array}{llll}
F^n_{i,1} = F^{n-1}_{i,1}F^{n-1}_{i,1} & F^n_{i,2} = F^{n-1}_{i,2}F^{n-1}_{i,2} & \ldots & F^n_{i,K} = F^{n-1}_{i,K}F^{n-1}_{i,K} \\
F^n_{i,(1+K)} = (-F^{n-1}_{i,1})F^{n-1}_{i,1} & F^n_{i,(1+(K+1))} = (-F^{n-1}_{i,2})F^{n-1}_{i,2} & \ldots & F^n_{i,(2K)} = (-F^{n-1}_{i,K})F^{n-1}_{i,K} \\
F^n_{(i+K),1} = F^n_{1,(i+K)} & F^n_{(i+K),2} = F^n_{i,(1+(K+1))} & \ldots & F^n_{(i+K),K} = F^n_{1,(2K)} \\
F^n_{(i+K),(1+K)} = F^n_{i,1} & F^n_{(i+K),(1+(K+1))} = F^n_{i,2} & \ldots & F^n_{(i+K),(2K)} = F^n_{i,K}
\end{array} \tag{2.167}$$

A matriz F^n é um conjunto ZCZ de tamanho $K = 2^{n+1}$ e $Z_{CZ} = 2^{n+m-1}$ composto de seqüência comprimento $N = 2^{2n+m+1}$.

Pode-se construir um conjunto ZCZ composto de seqüências de menor comprimento, simplesmente dividindo cada uma das seqüências pela metade. Como exemplo:

$$\begin{aligned}
F^1 &= \begin{bmatrix} F^1_{11} & F^1_{12} & F^1_{13} & F^1_{14} \\ F^1_{21} & F^1_{22} & F^1_{23} & F^1_{24} \\ F^1_{31} & F^1_{32} & F^1_{33} & F^1_{34} \\ F^1_{41} & F^1_{42} & F^1_{43} & F^1_{44} \end{bmatrix} \\
A^1 &= \begin{bmatrix} F^1_{11} & F^1_{12} \\ F^1_{21} & F^1_{22} \\ F^1_{31} & F^1_{32} \\ F^1_{41} & F^1_{42} \end{bmatrix} \\
B^1 &= \begin{bmatrix} F^1_{13} & F^1_{14} \\ F^1_{23} & F^1_{24} \\ F^1_{33} & F^1_{34} \\ F^1_{43} & F^1_{44} \end{bmatrix}
\end{aligned} \tag{2.168}$$

onde F^1 é o conjunto ZCZ original, A^1 e B^1 são os novos conjuntos ZCZ.

Dividindo novamente pela metade as seqüências dos novos conjuntos A^1 e B^1, obtêm-se novos conjuntos de menor comprimento. Assim, t divisões sucessivas de cada uma das seqüências de um conjunto ZCZ geram conjuntos ZCZ de tamanho $K = 2^{n+1}$ composto por seqüências de comprimento $N = 2^{2n+m+1-t}$ e $Z_{CZ} = 2^{n+m-t-1}$. Para $n > 0$, deve-se ter $t \leq n$ e, para $n = 0$, deve-se ter $t \leq m$.

2.2.3.1 Características do conjunto ZCZ

Observa-se que no conjunto ZCZ, metade das seqüências são ciclicamente equivalentes à outra metade das seqüências do conjunto. Essa característica é facilmente observada em (2.164). As seqüências obtidas da metade superior da matriz são ciclicamente equivalentes às seqüências obtidas da metade inferior da matriz.

Ainda observando (2.164), para $m = 0$ e $n = t$, tem-se um conjunto ZCZ com $N = K$ e $Z_{CZ} = 0$ composto por seqüências Walsh-Hadamard construídas como mostrado em (2.157), porém, com $H_0 = -1$. Assim, mostra-se que os conjuntos de seqüências Walsh-Hadamard são casos particulares de conjuntos de seqüências ZCZ.

As figuras 2.10.a e 2.10.b exemplificam a característica de zona de correlação nula das funções de correlação periódica par de seqüências do conjunto ZCZ. Na figura 2.11, ao contrário das funções de correlação periódica par, observa-se que a função de correlação cruzada periódica ímpar não é ótima para $|\tau| \leq Z_{CZ}$.

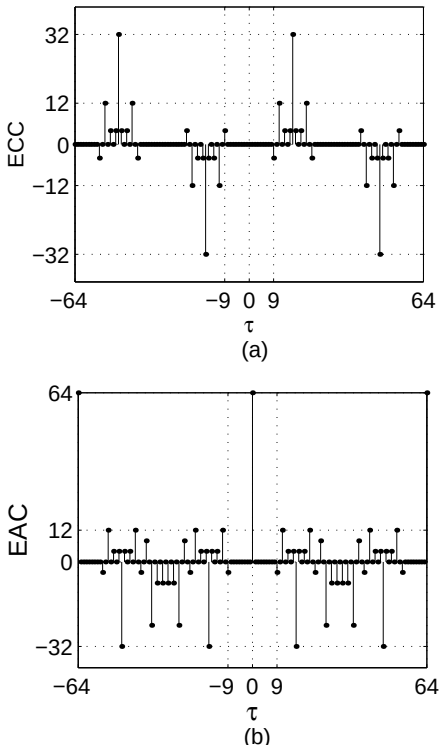

Figura 2.10: Exemplo para a (a) função de correlação periódica cruzada par e para a (b) função de autocorrelação periódica par de seqüências do conjunto ZCZ com $n = 1$, $m = 4$, $t = 1$ e $N = 64$.

Existe um compromisso entre o valor Z_{CZ} da zona de correlação nula e o número

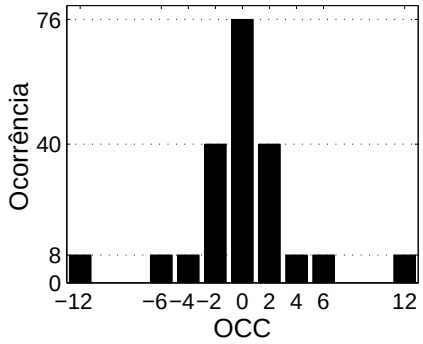

Figura 2.11: Histograma da função de correlação cruzada periódica ímpar no intervalo $|\tau| < 9$ para o conjunto ZCZ com $n = 4$, $m = 1$, $t = 1$ e $N = 64$.

de seqüências K de comprimento N disponíveis no conjunto. Fazendo $\theta_{mCZ} = 0$ e $L_{CZ} = Z_{CZ}$ em (1.98), obtém-se a relação:

$$N \geq K(Z_{CZ} + 1) \tag{2.169}$$

No apêndice C.2 é apresentada a metodologia de construção de seqüências ZCZ quadrifásicas.

2.3 Comparação das características das seqüências para QS-CDMA

A tabela 2.4 sintetiza, para as famílias de seqüências binárias estudadas e adequadas a sistemas QS-CDMA, as principais características: comprimento das seqüências N, número de seqüências na família K e zona de correlação reduzida/zero.

A figura 2.12 apresenta uma comparação entre número de seqüências K na família e a zona de correlação reduzida/zero para as famílias QS, Lin-Chang, LCZ-GMW e ZCZ de seqüências binárias de comprimento $N = 511$, no caso das seqüências de comprimento ímpar, e $N = 512$ no caso das seqüências de comprimento par. O número de seqüências com comprimento $N = 511$ em cada família QS-r foi obtido de (SAITO et al., 2001). Não foram realizadas verificações sobre esses números devido ao enorme tempo de processamento computacional, pois envolvem inúmeros testes, visto que as seqüências das famílias QS-r resultam da procura exaustiva no conjunto de Gold (2.60) excluída a seqüência $\mathbf{g}_2$. Em (SAITO et al., 2001), não foram apresentados números

Tabela 2.4: Comprimento das seqüências N, número de seqüências na família K e zona de correlação reduzida/zero para as seqüências binárias estudadas adequadas para sistemas QS-CDMA.

Família	N	K^a	LCZ/ZCZ^b
QS-r	2^n-1	-	$\frac{r-1}{2}$
Lin-Chang	2^n-1	$\frac{\binom{2^m-1}{2(m-1)}}{2^m-1}$	$\frac{2^n-1}{2^m-1}-1$
LCZ-GMW	2^n-1	-	$\frac{2^n-1}{2^m-1}-1$
OQS-r	2^n	-	$\frac{r-1}{2}$
ZCZ	$2^{2n+m+1-t}$	2^{n+1}	$2^{n+m-t-1}$

[a] Para as famílias QS, LCZ-GMW e OQS, não existe uma expressão geral do número de seqüências.
[b] Para seqüencias da família Lin-Chang, a função de correlação cruzada periódica par $\theta(\mathbf{a},\mathbf{b},d)$ pode assumir valores elevados para $d=0$ se a correlação cruzada periódica par entre as sementes não for -1, seção 2.1.5 eq. (2.89).

de seqüências das famílias OQS-r de comprimento $N=511$. Aqui, esses números também não foram obtidos com o mesmo argumento utilizado para a família QS-r. Por exemplo, para a família Gold sem a seqüência $\mathbf{g}_2$ de comprimento $N=511$ existem $\binom{512}{4}\cong 2,82\times10^9$ combinações de 4 seqüências e $\binom{512}{128}\cong 2,46\times10^{123}$ combinações de 128 seqüências. Para obter uma família OQS-r composta por 4 seqüências de comprimento 512 pode ser necessário testar $\binom{512}{4}\times 2\times 512\cong 2,88\times10^{12}$ combinações de 4 seqüências, pela possível necessidade de testar as 512 posições para o chip (+1 ou -1) que deve ser inserido. Na figura 2.12 foi também adicionado o limite de Tang-Fan (1.98):

$$K \geq \frac{N}{L_{CZ}+1} \tag{2.170}$$

Para obter as famílias QS, Lin-Chang e LCZ-GMW com $N=511$, foi adotado $n=6$. Para as famílias Lin-Chang e LCZ-GMW m deve ser fator de n. Para $m=\frac{n}{2}=3$ tem-se a condição de maximização do número K de seqüências nas famílias. No caso de $m=\frac{n}{3}=2$, obtém-se apenas uma seqüência Lin-Chang e uma seqüência LCZ-GMW. O número de seqüências disponíveis no conjunto LCZ-GMW deve ser obtido verificando a função de correlação cruzada periódica entre as SMC sementes, conforme mostram os algoritmos da seção 2.1.6. Para a família ZCZ, foram adotados os parâmetros da tabela 2.5.

A partir da figura 2.12, pode-se verificar que a família de seqüências QS resulta em um número de seqüências K muito menor que o limite de Tang-Fan. Assim, a relação entre o maior valor de K possível e o comprimento N das seqüências para um

Tabela 2.5: Parâmetros de construção das famílias ZCZ com $N = 512$.

K	ZCZ	n	m	t
4	64	1	6	0
8	32	2	4	0
16	16	3	2	0
32	8	4	1	1
64	4	5	1	3
128	2	6	1	5
256	1	7	1	7

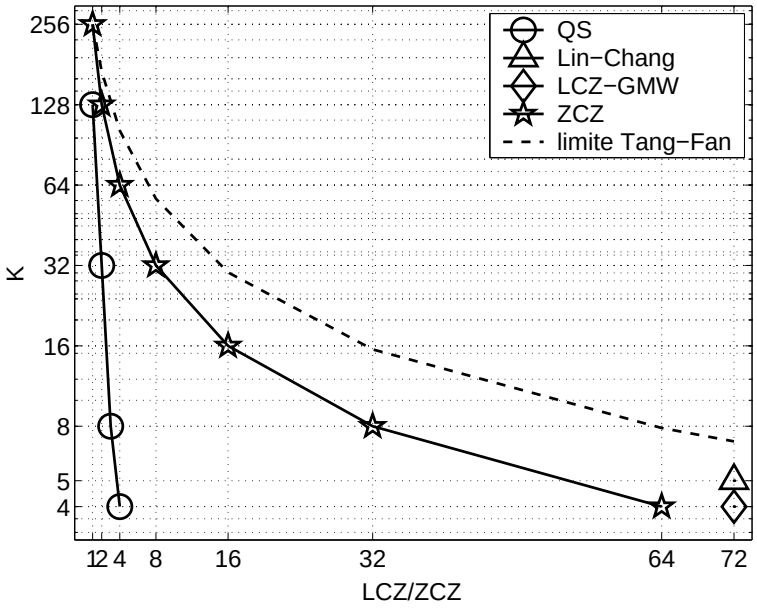

Figura 2.12: Comparação entre número de seqüências K na família e a zona de correlação reduzida/zero para as famílias de seqüências binárias estudadas adequadas a sistemas QS-CDMA de comprimento $N = 511$ ou $N = 512$.

dado valor $L_{CZ} > 0$, $\frac{\max\{K\}}{N}$, para essas famílias é reduzida. Em contrapartida, para as famílias Lin-Chang, LCZ-GMW e ZCZ o valor de K está próximo do limite de Tang-Fan e, portanto, $\frac{\max\{K\}}{N}$ assume um valor mais elevado.

As famílias de seqüências Lin-Chang e LCZ-GMW não são flexíveis, ou seja, existem apenas seqüências de comprimento $N = 2^n - 1$, para valores de n não primos. É possível obter famílias com mais de uma seqüência apenas para $m > 2$. Consequentemente, n terá que ser maior que 4. Portanto, os comprimentos de seqüências Lin-Chang e LCZ-GMW possíveis são $N = 63, 255, 511, 1023, 4095, ...$ Adicionalmente, para comprimentos de seqüências $N \leq 1023$, não é possível variar a LCZ (ou m) para aumentar ou diminuir o número K de seqüências da família. Seqüências Lin-

Chang e LCZ de comprimento $N = 63$ implicam em $n = 6$, o qual possui como fatores $m = 3$ e $m = 2$. Como é necessário $m > 2$ para obter mais de uma seqüência no conjunto, m pode assumir apenas o valor 3. No caso de $n = 8$, $n = 9$ e $n = 10$, m pode assumir apenas os valores 2, 9 e 5, respectivamente. As tabelas 2.6, 2.7, 2.8 e 2.9 apresentam o número de seqüências e a zona de correlação reduzida/zero para as famílias QS, Lin-Chang, LCZ-GMW e ZCZ com $N \leq 1024$ possíveis de serem obtidas. Para a família OQS, foi obtido apenas um conjunto (tabela 2.10) devido à complexidade do método de construção já mencionada. Os conjuntos QS da tabela 2.6 foram obtidos de (SAITO et al., 2001). Dessas tabelas, conclui-se que a família de seqüências ZCZ é a mais flexível.

Tabela 2.6: Conjuntos de seqüências QS possíveis com $N \leq 1024$.

		Número de seqüências					
		2	4	8	32	128	
LCZ	1	7		31	127	511	N (comprimento das seqüências)
	2		31	127	511		
	3		127	511			
	4		511				

Tabela 2.7: Conjuntos de seqüências Lin-Chang possíveis com $N \leq 1024$.

		Número de seqüências			
		5	429	9694845	
LCZ[a]	8	63			N (comprimento das seqüências)
	16		255		
	72	511			
	32			1023	

[a] Para seqüencias da família Lin-Chang, a função de correlação cruzada periódica par $\theta(\mathbf{a}, \mathbf{b}, d)$ pode assumir valores elevados para $d = 0$ se a correlação cruzada periódica par entre as sementes não for -1, seção 2.1.5 eq. (2.89).

Tabela 2.8: Conjuntos de seqüências LCZ-GMW possíveis com $N \leq 1024$.

		Número de seqüências			
		4	6	16	
LCZ	8	63			N (comprimento das seqüências)
	16		255		
	72	511			
	32			1023	

Tabela 2.9: Conjuntos de seqüências ZCZ possíveis com $N \leq 1024$.

		Número de seqüências								
		4	8	16	32	64	128	256	512	
ZCZ	1	8	16	32	64	128	256	512	1024	N (comp. das seqs.)
	2	16	32	64	128	256	512	1024		
	4	32	64	128	256	512	1024			
	8	64	128	256	512	1024				
	16	128	256	512	1024					
	32	256	512	1024						
	64	512	1024							
	128	1024								

Tabela 2.10: Conjunto de seqüências OQS obtido com $N \leq 1024$.

		Número de seqüências[a] 8	
ZCZ	1	32	N (comprimento das seqüências)

[a]Devido à complexidade do método de construção de seqüências OQS, foi obtida apenas a família apresentada na tabela.

2.3.1 Desempenho de sistemas de taxa única

Nesta seção, são apresentados resultados em termos de taxa de erro de bit (BER) de sistemas QS-CDMA utilizando diferentes conjuntos de seqüências. Considera-se recepção Rake MRC com diversidade $D = 4$, taxa chip de $3,84$ $Mchip/s$ e canal com desvanecimento multipercurso Rayleigh com perfil atraso potência do modelo COST207 (STUBER, 2001) dado pela tabela 2.11.

Se nas equações (1.10) e (1.11) da modelagem do sistema QS-CDMA os somatórios $\sum_j$, $\sum_u$ e $\sum_{\mathcal{L}}$ compreenderem um grande número de termos, de (YAO, 1977) pode-se afirmar que a *pdf* resultante para a MAI adicionada à SI tenderá a uma Gaus-

Tabela 2.11: Perfil atraso-potência do modelo de canal COST207 (STUBER, 2001).

ℓ	Δ_ℓ	$\mathbb{E}\{\alpha_\ell^2\}$
1	$0T_c$	$0,189$
2	$1T_c$	$0,379$
3	$2T_c$	$0,239$
4	$6T_c$	$0,095$
5	$9T_c$	$0,061$
6	$19T_c$	$0,037$

siana. Fazendo-se essa aproximação, obtém-se uma expressão analítica para o desempenho aproximado do *k*-ésimo usuário, em termos de taxa de erro de bit (BER), por meio de (PROAKIS, 1995):

$$BER_k = \frac{1}{2}\sum_{\ell=1}^{D} \Upsilon_\ell \left[1 - \sqrt{\frac{SNIR_{k,\ell}}{2 + SNIR_{k,\ell}}}\right] \tag{2.171}$$

$$\Upsilon_\ell = \prod_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{D} \frac{SNIR_{k,\ell}}{SNIR_{k,\ell} - SNIR_{k,\mathcal{L}}} \tag{2.172}$$

A avaliação de desempenho é realizada observando a BER média ($\overline{BER}$) dada pela média aritmética das BER de todos os usuários ativos no sistema.

Inicialmente, são apresentadas figuras de desempenho $\overline{BER}\times\tau_{\max}$ comparativas entre resultados de simulação Monte-Carlo e resultados obtidos com a expressão analítica (2.171) para o sistema modelado na seção 1.1. Adicionalmente, essas figuras apresentam o limite de BER, o qual é dado por (2.171) com $SNIR_{k,\ell} = \frac{2E_b\mathbb{E}\{\alpha_{k,\ell}\}}{N_0}$. O procedimento de simulação Monte-Carlo é descrito no apêndice F e o simulador de canal é descrito no apêndice G.

A figura 2.13 apresenta a comparação entre o resultado analítico e o resultado da simulação Monte-Carlo para o conjunto de seqüências QS derivado do conjunto $Gold(203, 277)$. Desse conjunto de Gold, obtêm-se 4 subconjuntos compostos de 8 seqüências QS-5 de comprimento $N = 127$ (SAITO et al., 2001). Arbitrariamente, escolheu-se o subconjunto Q_1, uma vez que todos os 4 subconjuntos apresentam propriedades de correlação similares.

A figura 2.14 apresenta a comparação entre o resultado analítico e o resultado da simulação Monte-Carlo para a família Lin-Chang com $m = 3$ e $n = 2m$. O polinômio primitivo utilizado para a construção do corpo $GF(2^6)$ foi $x^6 + x^5 + x^2 + x + 1$. As 5 sementes ciclicamente distintas escolhidas para gerar as 5 seqüências Lin-Chang de comprimento $N = 63$ foram: {1 0 1 1 0 1 0}, {0 0 0 1 1 1 1}, {0 0 1 0 1 1 1}, {0 0 1 1 1 0 1} e {1 1 0 1 1 0 0}. As fases das sementes foram escolhidas ao acaso e, portanto, não estão ajustadas para gerar seqüências Lin-Chang que resultam na função de correlação cruzada periodica par na origem $\theta(\mathbf{a}, \mathbf{b}, 0) = -1$, para $\mathbf{a} \neq \mathbf{b}$. Ajustando-se as fases das sementes para que ocorra $\theta(\mathbf{a}, \mathbf{b}, 0) = -1$, obtém-se as 4 seqüências LCZ-GMW binárias mais uma seqüência Lin-Chang.

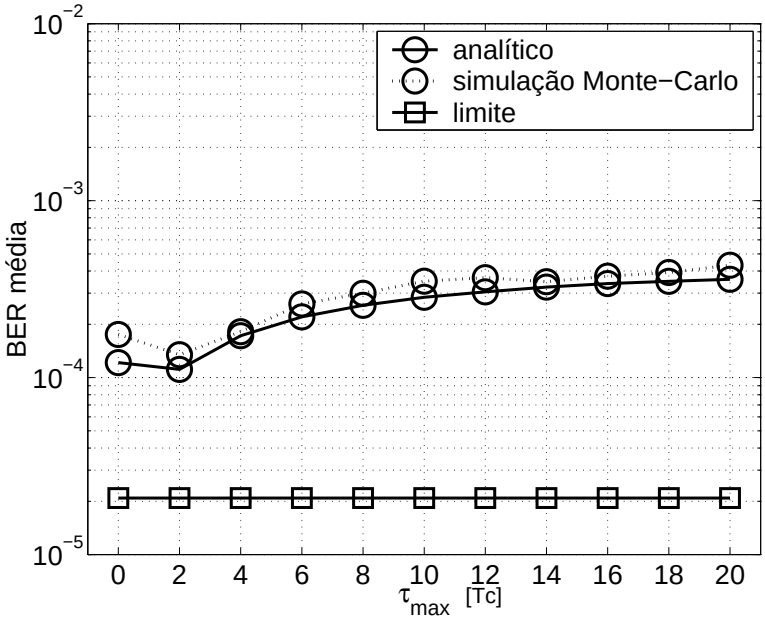

Figura 2.13: Desempenho $\overline{BER} \times \tau_{\max}$ do receptor Rake MRC utilizando o conjunto de seqüências QS; $\frac{E_b}{N_0} = 16dB$.

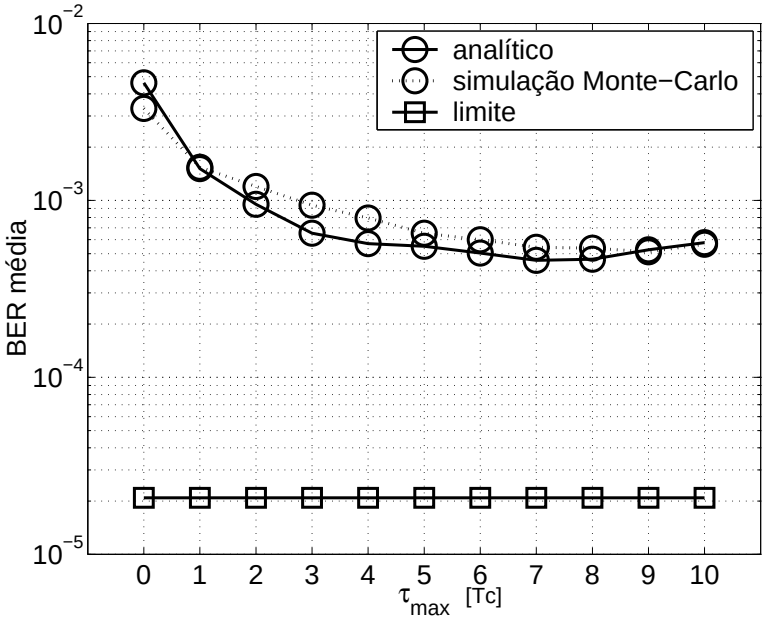

Figura 2.14: Desempenho $\overline{BER} \times \tau_{\max}$ do receptor Rake MRC utilizando a família Lin-Chang; $\frac{E_b}{N_0} = 16dB$.

A figura 2.15 apresenta a comparação entre o resultado analítico e o resultado da simulação Monte-Carlo para família LCZ-GMW binária com $m = 3$ e $n = 2m$. Para a construção do corpo $GF(2^6)$, foi utilizado o polinômio primitivo $1 + x + x^6$. Essa

família é composta de 4 seqüências de comprimento $N = 63$.

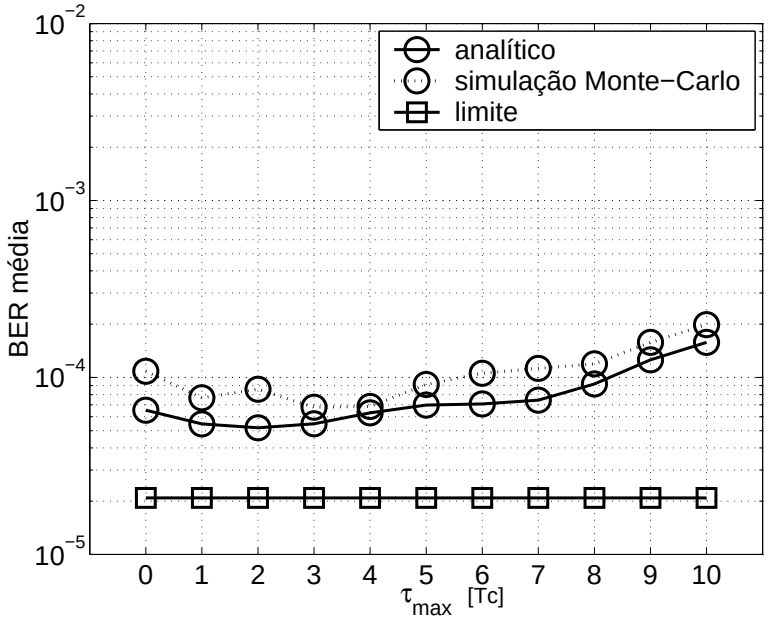

Figura 2.15: Desempenho $\overline{BER} \times \tau_{\max}$ do receptor Rake MRC utilizando a família LCZ-GMW binária; $\frac{E_b}{N_0} = 16dB$.

A figura 2.16 apresenta a comparação entre o resultado analítico e o resultado da simulação Monte-Carlo para a família ZCZ binária com $m = 4$, $n = 1$ e $t = 1$, resultando em um conjunto de 4 seqüências de comprimento $N = 64$ e $Z_{CZ} = 8$.

Observando-se as figuras 2.13 a 2.16, tem-se que a aproximação Gaussiana utilizada para obter a expressão analítica da $\overline{BER}$ do sistema QS-CDMA modelado é razoável, pois os resultados analíticos são próximos dos simulados. Assim, os resultados apresentados a seguir são obtidos apenas da expressão analítica dada por (2.171).

A seguir serão apresentados resultados de $\overline{BER} \times \frac{E}{N_0}$ e $\overline{BER} \times \tau_{\max}$ para os conjuntos de seqüências obtidos apresentados na tabela 2.12.

Tabela 2.12: Conjuntos de seqüências binárias adequados para sistemas QS-CDMA analisados.

Conjunto	$N = 31$ ou 32	$N = 63$ ou 64	$N = 127$ ou 128	$N = 255$ ou 256	$N = 511$ ou 512
QS	obtido	não existe	obtido	não existe	não obtido
OQS	obtido	não existe	não obtido	não existe	não obtido
Lin-Chang	não existe	obtido	não existe	obtido	obtido
LCZ-GMW	não existe	obtido	não existe	obtido	obtido
ZCZ	obtido	obtido	obtido	obtido	obtido

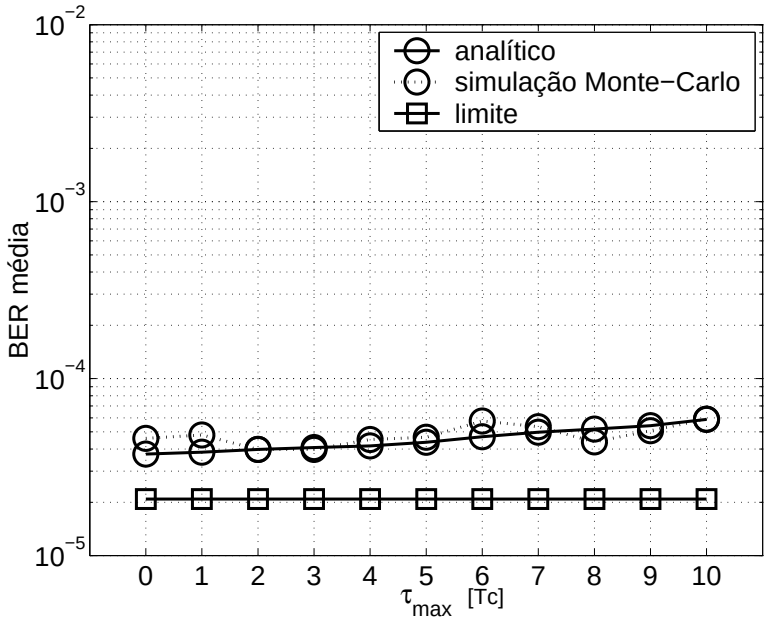

Figura 2.16: Desempenho $\overline{BER} \times \tau_{\max}$ do receptor Rake MRC utilizando a família ZCZ binária; $\frac{E_b}{N_0} = 16dB$.

Considerando $N \leq 1024$, apenas para $N = 511$ ou 512 existem conjuntos de seqüências para todas as famílias binárias adequadas para QS-CDMA estudadas. Porém, não foram obtidos os conjuntos QS com $N = 511$ e os conjuntos OQS com $N = 512$ e $N = 128$. Os métodos de construção de tais conjuntos são complexos e necessitam de um elevado tempo de processamento. Assim, serão realizadas comparações entre os conjuntos de mesmo N e não haverá uma comparação simultânea para todos os conjuntos. Os conjuntos QS analisados foram obtidos de (SAITO et al., 2001) e o conjunto OQS analisado foi obtido por procura exaustiva.

As características e parâmetros de construção dos conjuntos QS, OQS, Lin-Chang, LCZ-GMW e ZCZ são apresentados nas tabelas 2.13, 2.16, 2.14, 2.15 e 2.17, respectivamente.

A família Lin-Chang com $N = 255$ possui 429 seqüências. Para ser possível uma comparação com as outras famílias que apresentam um número reduzido de seqüências, foram escolhidas aleatoriamente $K = 6$ seqüências Lin-Chang para compor o conjunto de $N = 255$ analisado.

Os resultados de $\overline{BER} \times \frac{E}{N_0}$ consideram $\tau_{\max} = 4T_c$ e os resultados de $\overline{BER} \times \tau_{\max}$ consideram $\frac{E_b}{N_0} = 16dB$.

Tabela 2.13: Conjuntos de seqüências QS analisados.

N	31		127		
K	4	8	4	8	32
LCZ	2	1	3	2	1
r	5	3	7	5	3
conjunto Gold	$Gold(45, 73)$		$Gold(203, 277)$		
seqüências	$\mathbf{g}_1$	$\mathbf{g}_1$	$\mathbf{g}_1$	$\mathbf{g}_1$	$\mathbf{g}_1$
	$\mathbf{g}_{12}$	$\mathbf{g}_{12}$	$\mathbf{g}_{13}$	$\mathbf{g}_7$	$\mathbf{g}_8$
	$\mathbf{g}_{17}$	$\mathbf{g}_{17}$	$\mathbf{g}_{69}$	$\mathbf{g}_{12}$	$\mathbf{g}_{16}$
	$\mathbf{g}_{19}$	$\mathbf{g}_{18}$	$\mathbf{g}_{111}$	$\mathbf{g}_{13}$	$\mathbf{g}_{18}$
		$\mathbf{g}_{19}$		$\mathbf{g}_{31}$	$\mathbf{g}_{21}$
		$\mathbf{g}_{27}$		$\mathbf{g}_{33}$	$\mathbf{g}_{26}$
		$\mathbf{g}_{30}$		$\mathbf{g}_{69}$	$\mathbf{g}_{28}$
		$\mathbf{g}_{31}$		$\mathbf{g}_{111}$	$\mathbf{g}_{34}$
					$\mathbf{g}_{38}$
					$\mathbf{g}_{41}$
					$\mathbf{g}_{44}$
					$\mathbf{g}_{52}$
					$\mathbf{g}_{55}$
					$\mathbf{g}_{58}$
					$\mathbf{g}_{62}$
					$\mathbf{g}_{66}$
					$\mathbf{g}_{70}$
					$\mathbf{g}_{73}$
					$\mathbf{g}_{75}$
					$\mathbf{g}_{79}$
					$\mathbf{g}_{84}$
					$\mathbf{g}_{88}$
					$\mathbf{g}_{90}$
					$\mathbf{g}_{95}$
					$\mathbf{g}_{97}$
					$\mathbf{g}_{100}$
					$\mathbf{g}_{102}$
					$\mathbf{g}_{104}$
					$\mathbf{g}_{106}$
					$\mathbf{g}_{112}$
					$\mathbf{g}_{118}$
					$\mathbf{g}_{127}$

Tabela 2.14: Conjuntos de seqüências Lin-Chang analisados.

N	63	255	511
K	5	6[a]	5
LCZ	8	16	72
n	6	8	9
m	3	4	3
pol. primitivo de grau n	$x^6 + x + 1$	$x^8 + x^4 + x^3 + x^2 + 1$	$x^9 + x^4 + 1$
sementes	1001011	101010101010101	1001011
	1101100	110011001100110	1101100
	1010110	111111110000000	1010110
	1110001	111100001111000	1110001
	0100111	111000111000110	0100111
		111110000011100	

[a] foram escolhidas 6 seqüências quaisquer dentre as 429 existentes.

Tabela 2.15: Conjuntos de seqüências LCZ-GMW binária analisados.

N	63	255	511
K	4	6	4
LCZ	8	16	72
n	6	8	9
m	3	4	3
pol. primitivo de grau n	$x^6 + x + 1$	$x^8 + x^4 + x^3 + x^2 + 1$	$x^9 + x^4 + 1$
pol. primitivo de grau m	$x^3 + x + 1$	$x^4 + x + 1$	$x^3 + x + 1$
	$x^3 + x^2 + 1$	$x^4 + x^3 + 1$	$x^3 + x^2 + 1$

Tabela 2.16: Conjuntos de seqüências OQS analisados.

N	32
K	8
ZCZ	1
r	3
conjunto Gold ortogonal	$OGold(45, 73, -1, 7)$
seqüências	$\mathbf{g}_1$
	$\mathbf{g}_{12}$
	$\mathbf{g}_{17}$
	$\mathbf{g}_{18}$
	$\mathbf{g}_{19}$
	$\mathbf{g}_{27}$
	$\mathbf{g}_{30}$
	$\mathbf{g}_{31}$

Tabela 2.17: Conjuntos de seqüências ZCZ analisados.

N	32			64				128					256					512				
K	4	8	16	4	8	16	32	4	8	16	32	64	4	8	16	32	64	4	8	16	32	64
ZCZ	4	2	1	8	4	2	1	16	8	4	2	1	32	16	8	4	2	64	32	16	8	4
n	1	2	3	1	2	3	4	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
m	2	1	1	3	1	1	1	4	2	1	1	1	5	3	1	1	1	6	4	2	1	1
t	0	1	3	0	0	2	4	0	0	1	3	5	0	0	0	2	4	0	0	0	1	3

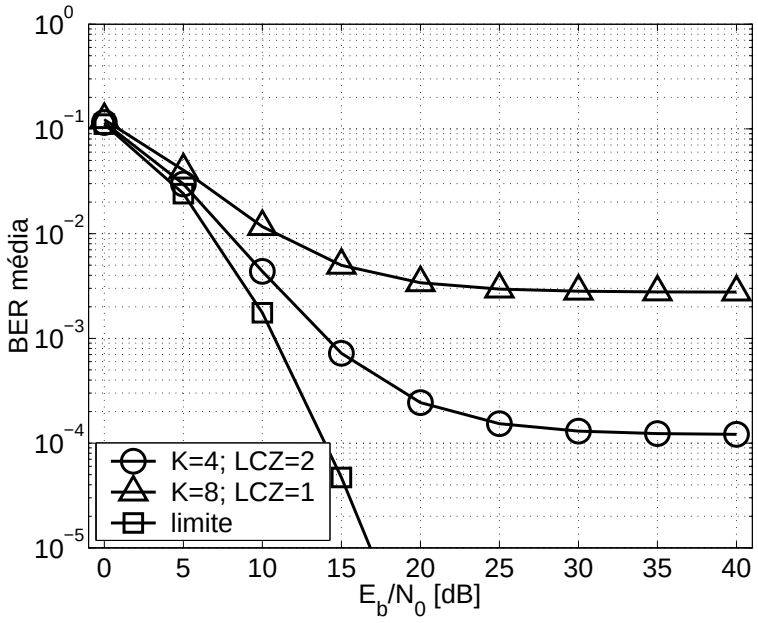

Figura 2.17: $\overline{BER} \times \frac{E}{N_0}$ para a família de seqüências QS com $N = 31$ obtidas do conjunto $Gold(45, 73)$ e $\tau_{\max} = 4T_c$.

Das figuras 2.17, 2.18 e 2.19, tem-se que os conjuntos ZCZ com $K = 4$ e $K = 8$ seqüências de comprimento $N = 32$ resultam em melhores desempenhos comparados aos conjuntos QS e OQS de mesmo número de seqüências e comprimento, pois a zona de correlação reduzida/nula para o conjunto ZCZ é maior. Essa característica provê aos conjuntos ZCZ uma maior resistência ao erro de sincronismo quando comparado aos conjuntos QS e OQS. Tal afirmação pode ser confirmada por meio das figuras 2.20, 2.21 e 2.22. Os conjuntos ZCZ com $K = 4$ e $K = 8$ apresentam uma degradação de desempenho com o aumento de $\tau_{\max}$ mais retardada do que os conjuntos QS de mesmo K. Os conjuntos QS-3 e OQS-3, ambos com $K = 8$ seqüências, apresentam desempenhos similares aos observados nas figuras 2.17, 2.18, 2.20 e 2.21.

Os conjuntos Lin-Chang com $N = 63$ e $N = 511$ são compostos por 4 seqüências LCZ-GMW e pela seqüência derivada da semente SMC {0100111}. Assim, os desempenhos obtidos com os conjuntos Lin-Chang e LCZ-GMW são semelhantes, sendo que, para o conjuntos Lin-Chang, a $\overline{BER}$ é um pouco maior por possuir uma seqüência a mais que o conjunto LCZ-GMW (figuras 2.23, 2.24, 2.26 e 2.27). O desempenho obtido com o conjunto ZCZ com $N = 64$ e $K = 4$ (figura 2.25) é superior aos obtidos com os conjuntos Lin-Chang e LCZ-GMW com $N = 63$. As zonas de correlação reduzida/nula para os conjuntos Lin-Chang, LCZ-GMW e ZCZ são iguais, entretanto, o

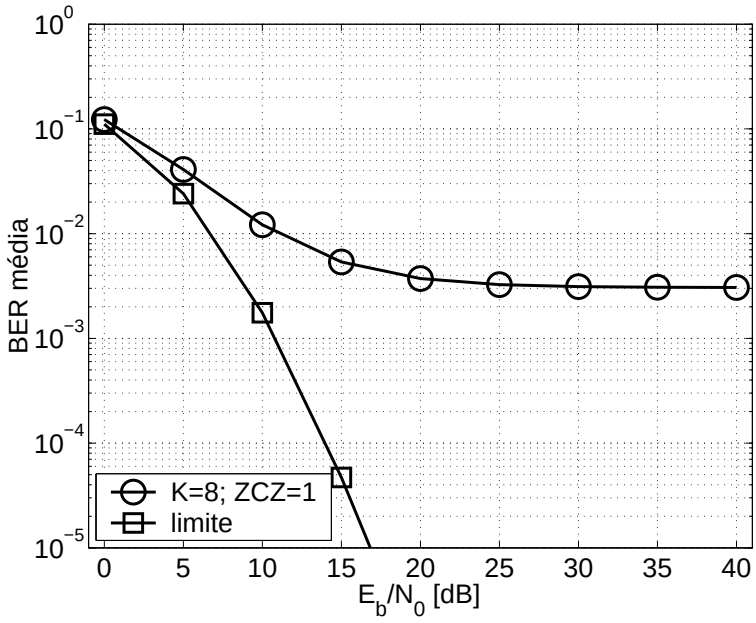

Figura 2.18: $\overline{BER} \times \frac{E}{N_0}$ para a família de seqüências OQS com $N = 32$ obtidas do conjunto $Gold(45, 73)$ e $\tau_{\max} = 4T_c$.

desempenho para o conjunto ZCZ é menos degradado com o aumento de $\tau_{\max}$ (figura 2.28). Essa diferença de desempenho é devido às funções de correlação periódica par fora da zona de correlação reduzida/nula e às funções de correlação periódica ímpar apresentarem características distintas.

Assim como a comparação entre as famílias ZCZ de comprimento $N = 32$ e QS de comprimento $N = 31$, a família ZCZ de comprimento $N = 128$ apresenta desempenho superior à família QS de comprimento $N = 127$. Comparando a figura 2.29 com a figura 2.30 e a figura 2.31 com a figura 2.32, para $K = 4$, $K = 8$ e $K = 32$, a afirmação anterior é confirmada. Novamente, observa-se que o desempenho para as famílias ZCZ com $K = 4$ e $K = 8$ é pouco degradado como aumento de $\tau_{\max}$ comparado com o desempenho para as famílias QS com $K = 4$ e $K = 8$.

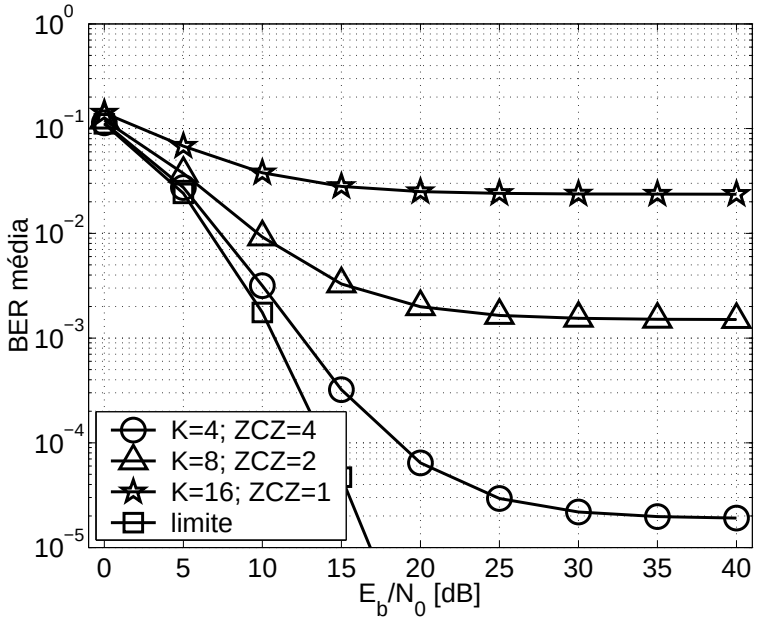

Figura 2.19: $\overline{BER} \times \frac{E}{N_0}$ para a família de seqüências ZCZ binária com $N = 32$ e $\tau_{\max} = 4T_c$.

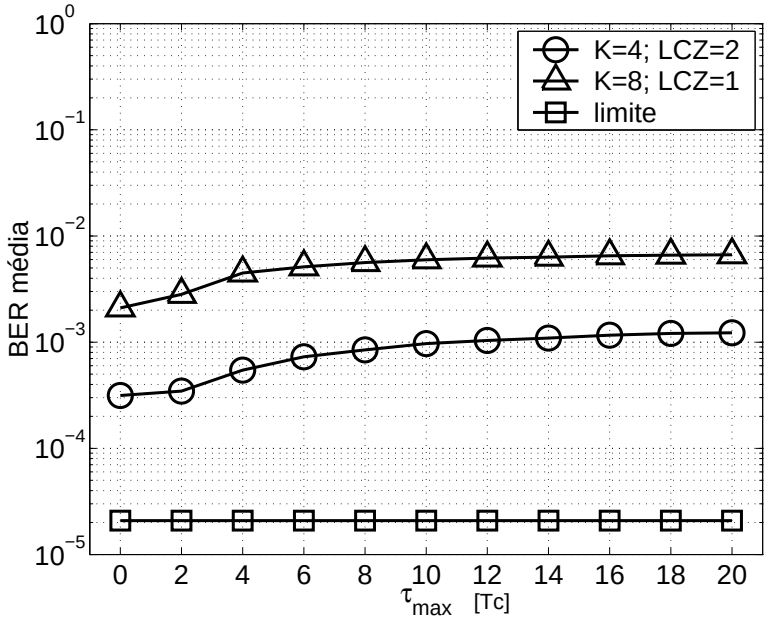

Figura 2.20: $\overline{BER} \times \tau_{\max}$ para a família de seqüências QS com $N = 31$ obtidas do conjunto $Gold(45, 73)$ e $\frac{E_b}{N_0} = 16dB$.

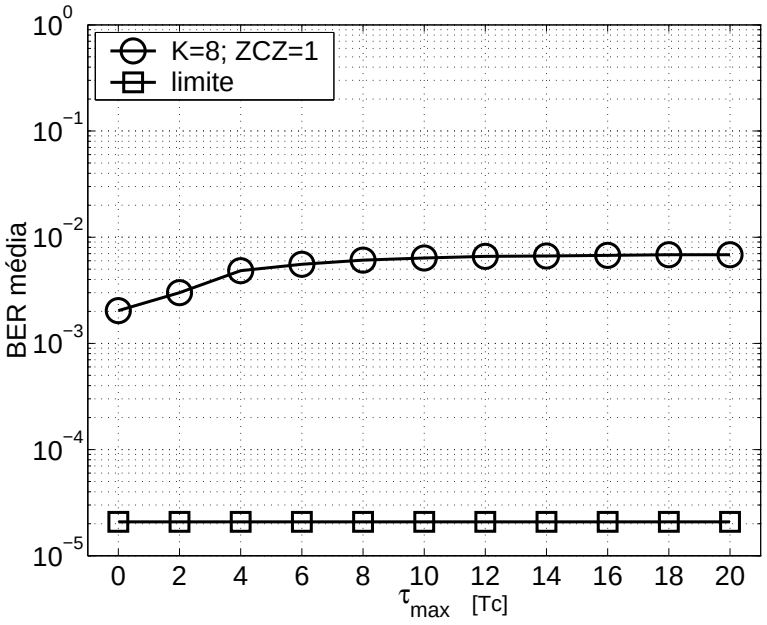

Figura 2.21: $\overline{BER} \times \tau_{\max}$ para a família de seqüências OQS com $N = 32$ obtidas do conjunto $Gold(45, 73)$ e $\frac{E_b}{N_0} = 16dB$.

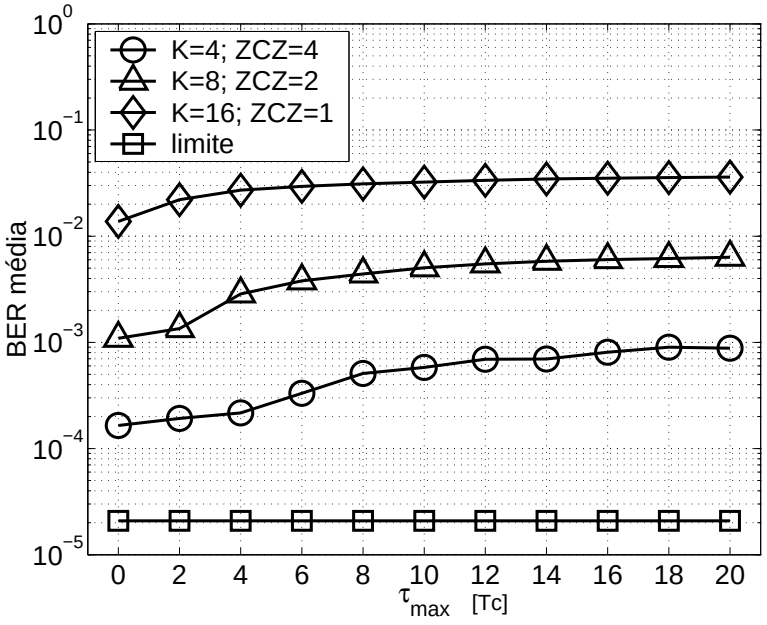

Figura 2.22: $\overline{BER} \times \tau_{\max}$ para a família de seqüências ZCZ binária com $N = 32$ e $\frac{E_b}{N_0} = 16dB$.

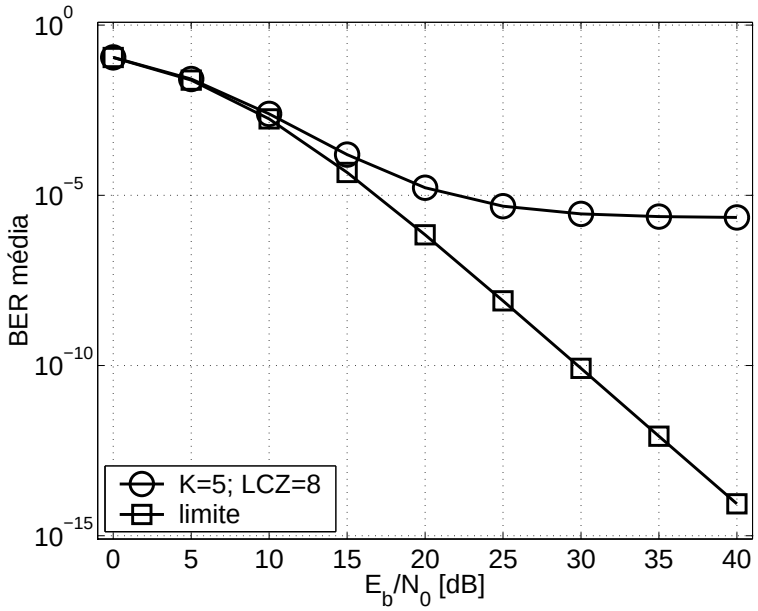

Figura 2.23: $\overline{BER} \times \frac{E}{N_0}$ para a família de seqüências Lin-Chang com $N = 63$ obtidas com $1 + x + x^6$, $m = 3$ e $\tau_{\max} = 4T_c$.

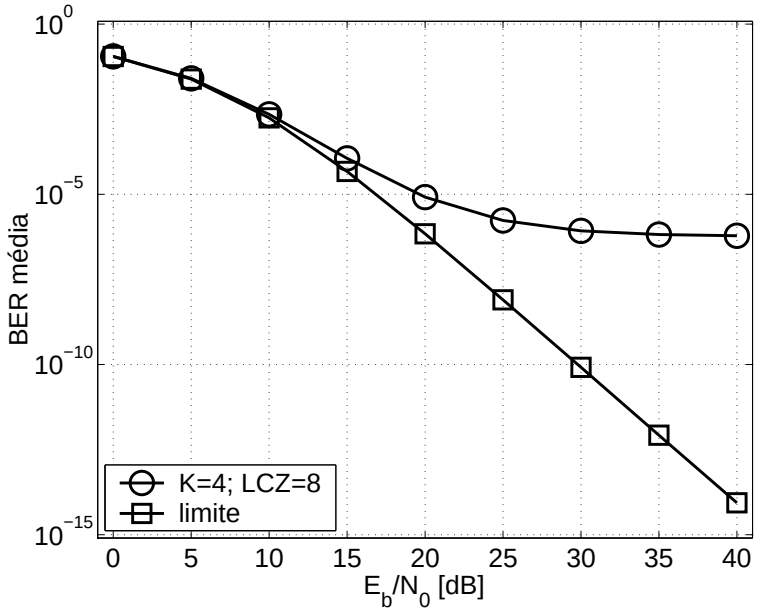

Figura 2.24: $\overline{BER} \times \frac{E}{N_0}$ para a família de seqüências LCZ-GMW binária com $N = 63$ obtidas com $1 + x + x^6$, $1 + x + x^3$, $1 + x^2 + x^3$ e $\tau_{\max} = 4T_c$.

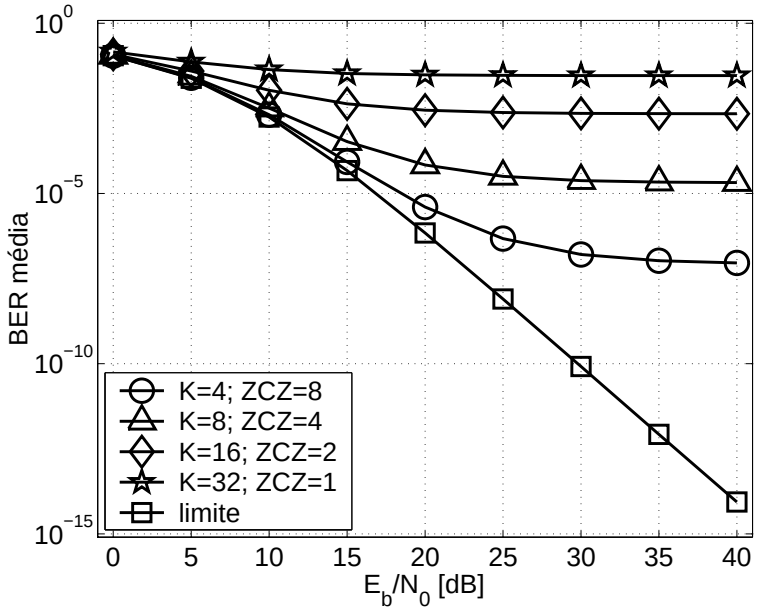

Figura 2.25: $\overline{BER} \times \frac{E}{N_0}$ para a família de seqüências ZCZ binária com $N = 64$ e $\tau_{\max} = 4T_c$.

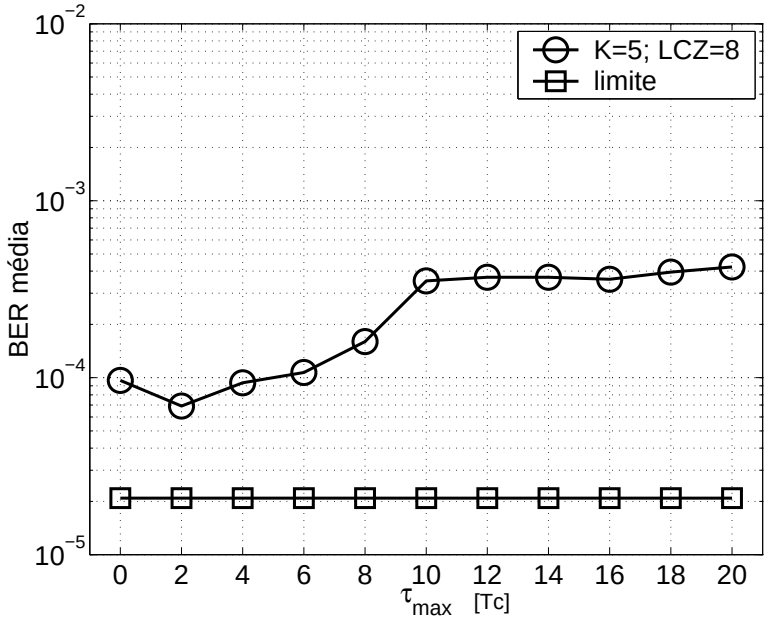

Figura 2.26: $\overline{BER} \times \tau_{\max}$ para a família de seqüências Lin-Chang com $N = 63$ obtidas com $1 + x + x^6$, $m = 3$ e $\frac{E_b}{N_0} = 16dB$.

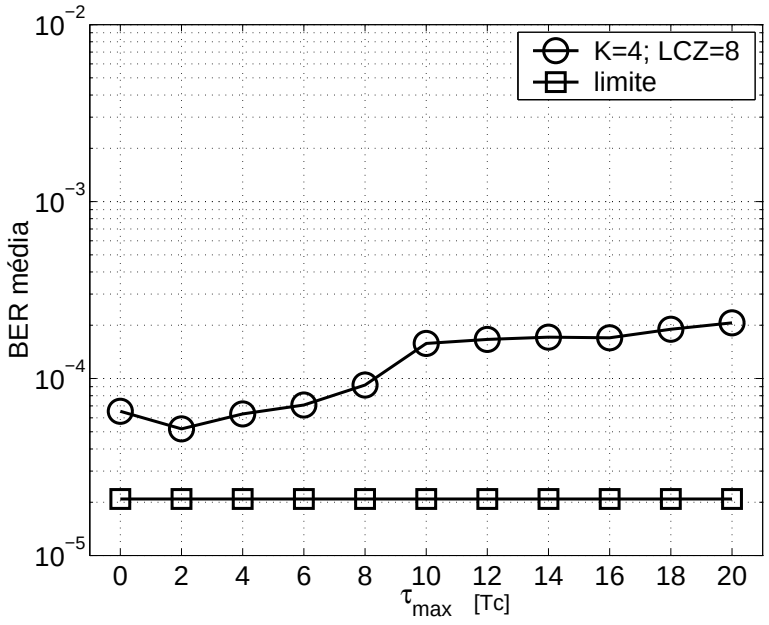

Figura 2.27: $\overline{BER} \times \tau_{\max}$ para a família de seqüências LCZ-GMW binária com $N = 63$ obtidas com $1 + x + x^6$, $1 + x + x^3$, $1 + x^2 + x^3$ e $\frac{E_b}{N_0} = 16dB$.

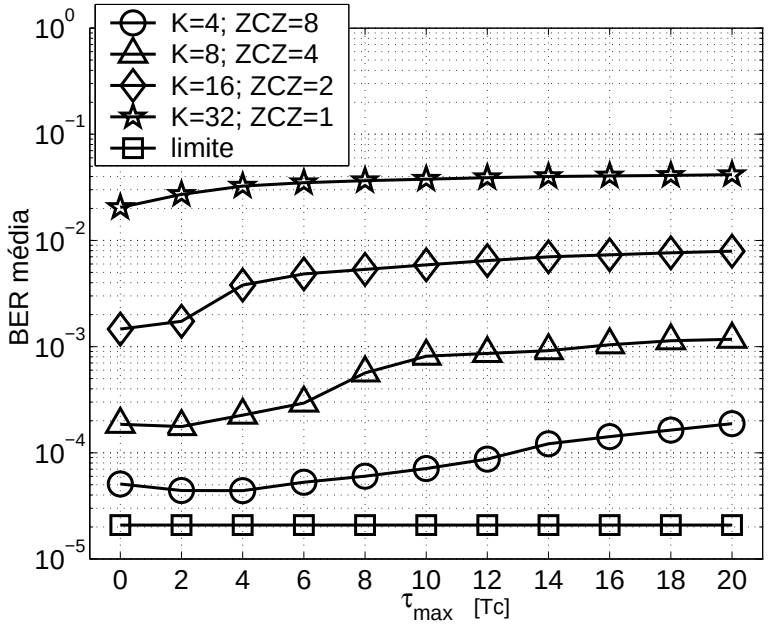

Figura 2.28: $\overline{BER} \times \tau_{\max}$ para a família de seqüências ZCZ binária com $N = 64$ e $\frac{E_b}{N_0} = 16dB$.

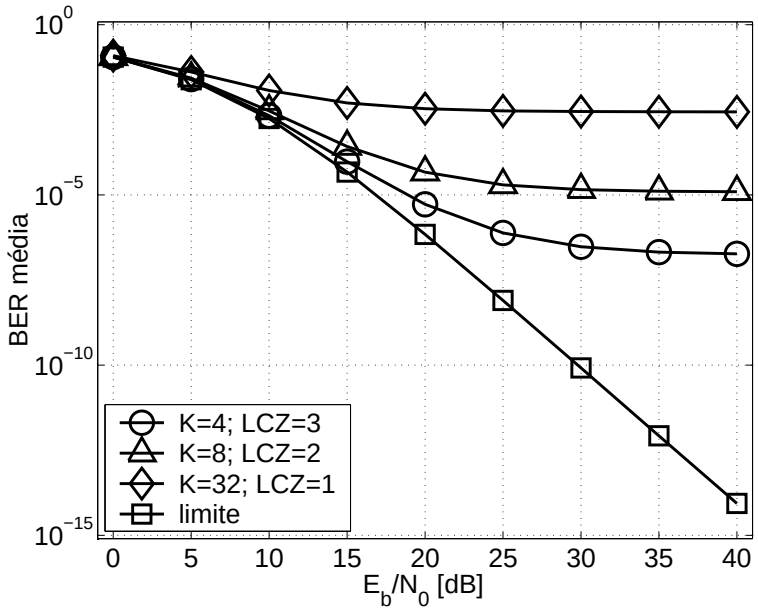

Figura 2.29: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências QS com $N = 127$ obtidas do conjunto $Gold(203, 277)$ e $\tau_{\max} = 4T_c$.

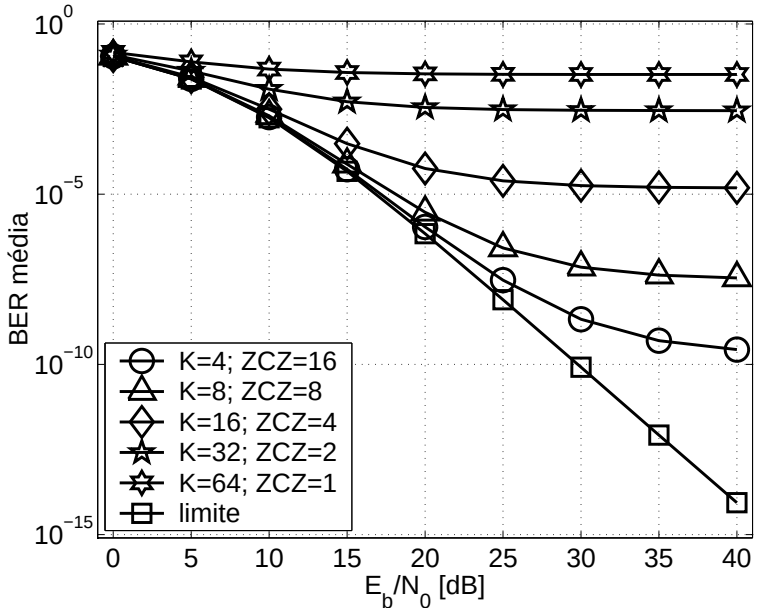

Figura 2.30: $\overline{BER} \times \frac{E}{N_0}$ para a família de seqüências ZCZ binária com $N = 128$ e $\tau_{\max} = 4T_c$.

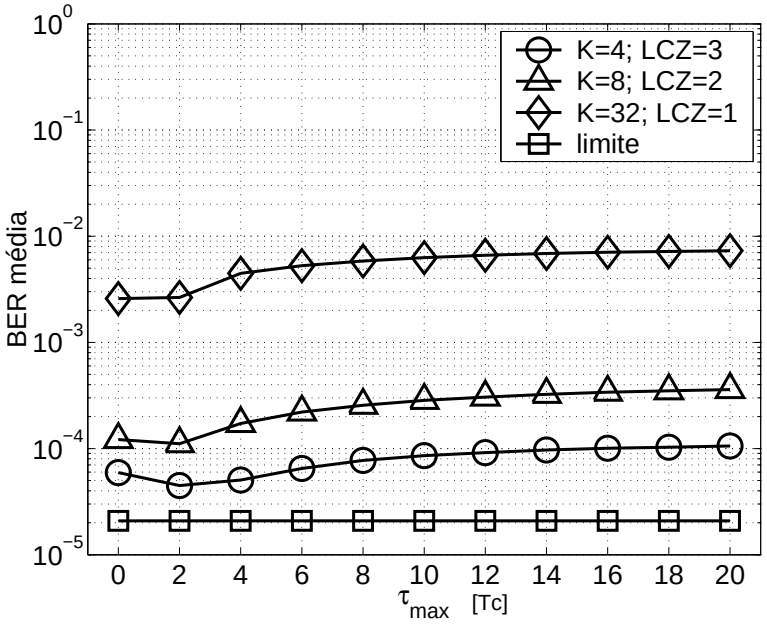

Figura 2.31: $\overline{BER} \times \tau_{\max}$ para a família de seqüências QS com $N = 127$ obtidas do conjunto $Gold(203, 277)$ e $\frac{E_b}{N_0} = 16dB$.

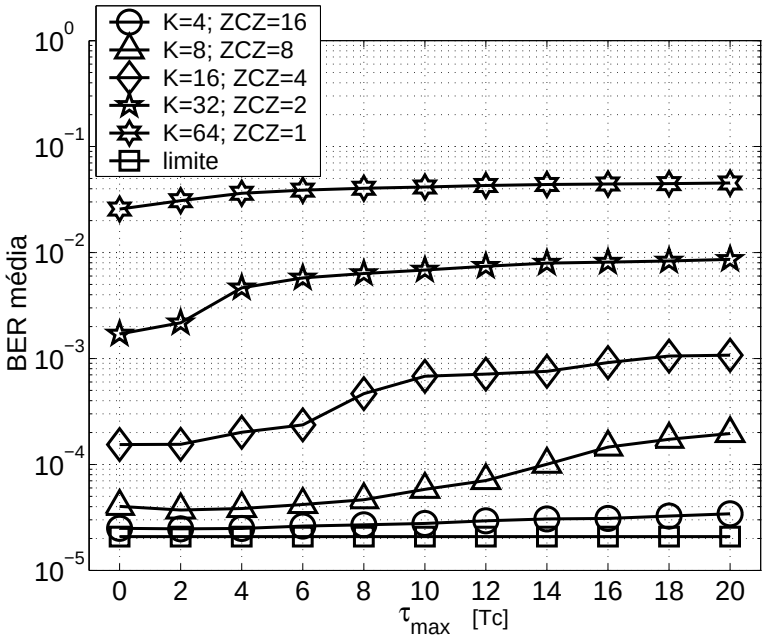

Figura 2.32: $\overline{BER} \times \tau_{\max}$ para a família de seqüências ZCZ binária com $N = 128$ e $\frac{E_b}{N_0} = 16dB$.

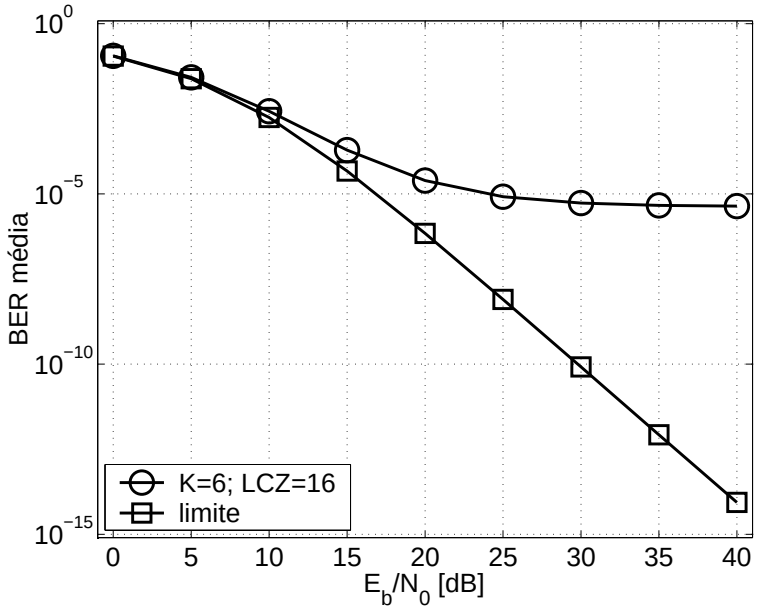

Figura 2.33: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências Lin-Chang com $N = 255$ obtidas com $1 + x^2 + x^3 + x^4 + x^8$, $m = 4$ e $\tau_{\max} = 4T_c$.

Como as sementes para as 6 seqüências Lin-Chang de comprimento $N = 255$ foram escolhidas aleatoriamente, não é possível garantir que a função de correlação cruzada periódica par resulte em valor nulo na origem. Em (LIN; CHANG, 1997) não foi proposto nenhum método sistemático para a escolha das sementes das seqüências Lin-Chang. Quando as sementes são de comprimento pequeno a busca exaustiva é viável, como no caso de $m = 3$, que resulta em sementes de comprimento $2^m - 1 = 7$. Porém, quando $m = 4$, caso de $N = 255$, as sementes possuem comprimento $2^m - 1 = 15$ e, portanto, existem $\binom{15}{8}/15 = 429$ sementes balanceadas. Então, o total de combinações de 6 sementes das 429 para todas as fases será $\binom{429}{6} \times 15 \times 6 \cong 7,52 \times 10^{14}$. Assim, a procura exaustiva torna-se inviável, fazendo com que o método de seleção de seqüências proposto em (LIN; CHANG, 1997) (método de obtenção de seqüências Lin-Chang) seja ineficiente. Comparando as figuras 2.33 e 2.34, pode-se concluir que a escolha aleatória de 6 sementes não gerou 6 seqüências Lin-Chang otimizadas. Isso porque a família LCZ-GMW está contida na família Lin-Chang e o desempenho obtido com a família LCZ-GMW foi muito superior. Observando as figura 2.36 e 2.37 fica claro que a escolha aleatória de 6 sementes resultou em seqüências Lin-Chang com $\theta(\mathbf{a}, \mathbf{b}, 0) \neq 0$, pois a $\overline{BER}$ para $\tau_{\max} = 0$ é maior para a família Lin-Chang comparada com a $\overline{BER}$ para a família LCZ-GMW.

O desempenho obtido com a família ZCZ de $N = 256$ e $K = 8$, figura 2.35, foi

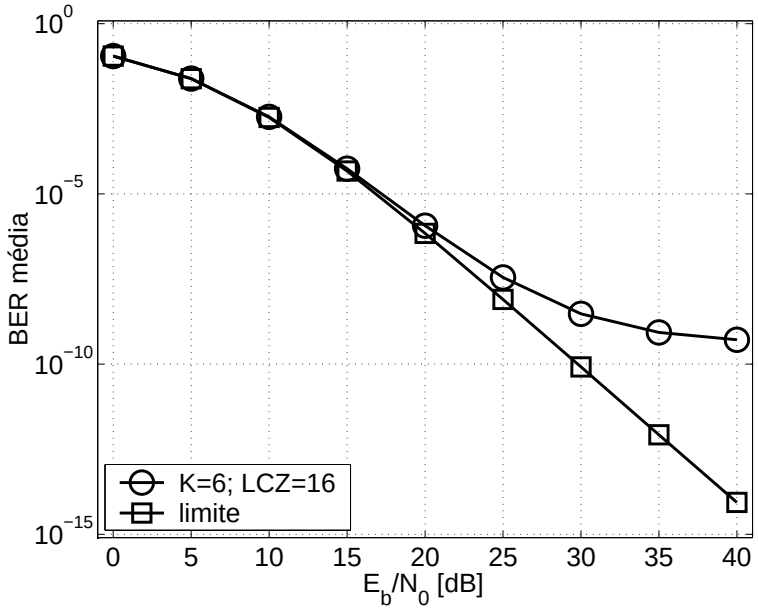

Figura 2.34: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências LCZ-GMW binárias com $N = 255$ obtidas com $1 + x^2 + x^3 + x^4 + x^8$, $1 + x + x^4$, $1 + x^3 + x^4$ e $\tau_{\max} = 4T_c$.

superior ao obtido com as famílias Lin-Chang e LCZ-GMW com $N = 255$ e $K = 6$. Adicionalmente, a família ZCZ mostra-se menos sensível ao erro de sincronismo comparada às famílias Lin-Chang e LCZ-GMW, figuras 2.36, 2.37 e 2.38.

Para as famílias Lin-Chang com $N = 511$ e $K = 5$, LCZ-GMW com $N = 511$ e $K = 4$ e ZCZ com $N = 512$ e $K = 4$, os desempenhos obtidos são semelhantes (figuras 2.39, 2.40 e 2.41). Essas famílias também se apresentam resistentes ao erro de sincronismo (figuras 2.42, 2.43 e 2.44).

Com base nas figuras de resultado apresentadas anteriormente, foi elaborado um quadro de comparação qualitativa entre as famílias QS, Lin-Chang, LCZ-GMW, OQS e ZCZ. Não é possível fazer uma comparação quantitativa entre todas essas famílias com a intenção de classificá-las. Conforme já mencionado, para $N \leq 1024$ apenas para $N = 511$ ou 512 é possível obter todas essas famílias. Entretanto, as famílias QS e OQS não foram obtidas devido a complexidade dos métodos de geração. Dos resultados obtidos nesta análise, pode-se afirmar que a família de seqüências estudada que apresenta o melhor conjunto de características é a família ZCZ, seguida das famílias Lin-Chang e LCZ-GMW, as quais possuem características semelhantes, pois a família LCZ-GMW está contida na família Lin-Chang. As famílias QS e OQS apresentaram as piores características dentre as famílias estudadas, destacando-se a falta de flexibilidade, a

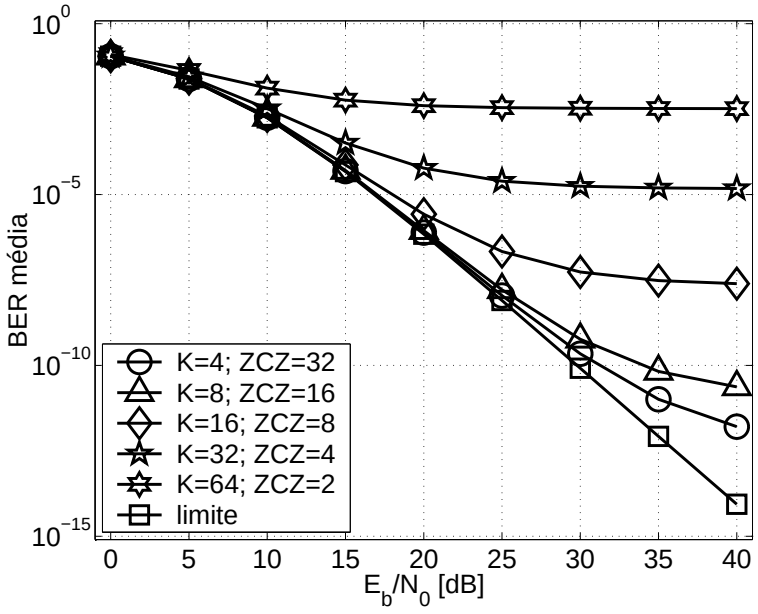

Figura 2.35: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências ZCZ com $N = 256$ e $\tau_{\max} = 4T_c$.

complexidade de geração dos conjuntos de seqüências e a baixa relação $\frac{\max\{K\}}{N}$.

Tabela 2.18: Comparação qualitativa das famílias de seqüências binárias estudadas adequadas para sistemas QS-CDMA.

Família	**relação** $\frac{\max\{K\}}{N}$	**flexível**	**resistente ao erro de sincronismo**	**desempenho proporcionado**
QS	insuficiente	não	não	razoável
Lin-Chang	razoável	não	sim	bom
LCZ-GMW	razoável	não	sim	bom
OQS	insuficiente	não	não	razoável
ZCZ	razoável	sim	sim	bom

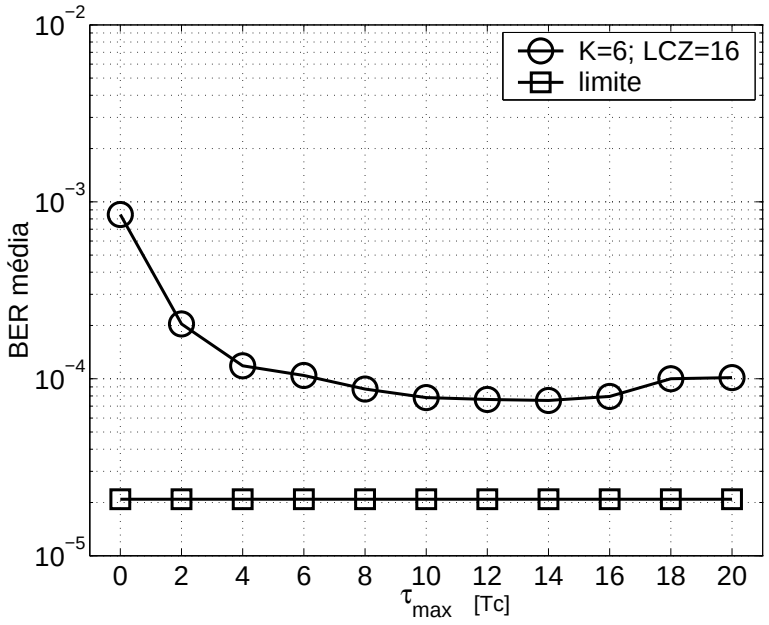

Figura 2.36: $\overline{BER} \times \tau_{\max}$ para a família de seqüências Lin-Chang com $N = 255$ obtidas com $1 + x^2 + x^3 + x^4 + x^8$, $m = 4$ e $\frac{E_b}{N_0} = 16dB$.

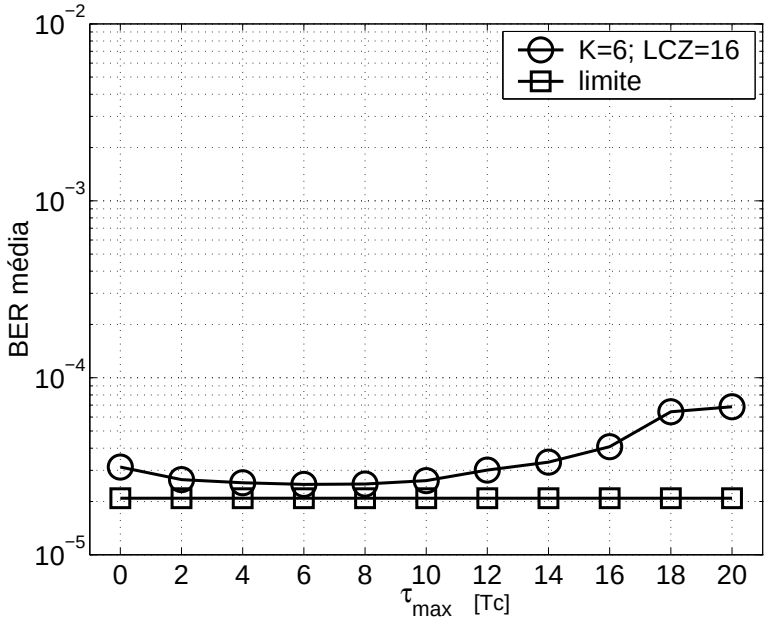

Figura 2.37: $\overline{BER} \times \tau_{\max}$ para a família de seqüências LCZ-GMW binária com $N = 255$ obtidas com $1 + x^2 + x^3 + x^4 + x^8$, $1 + x + x^4$, $1 + x^3 + x^4$ e $\frac{E_b}{N_0} = 16dB$.

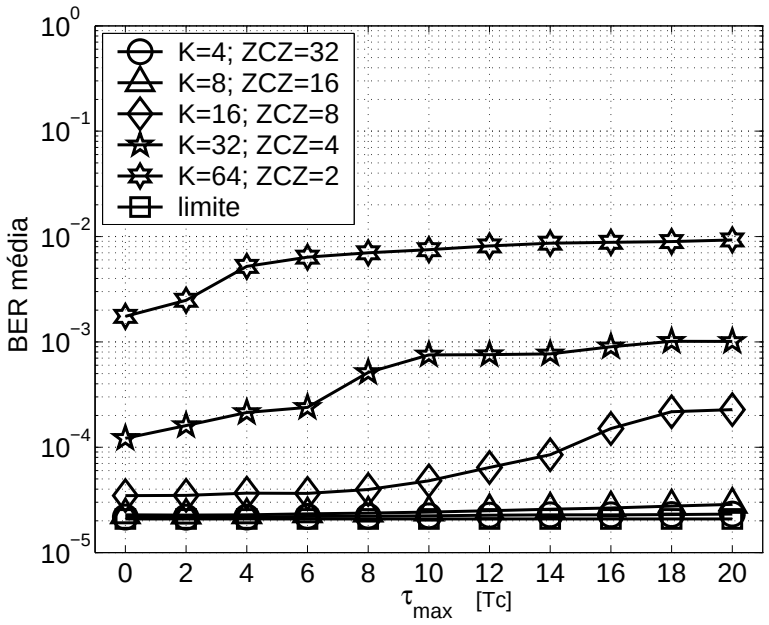

Figura 2.38: $\overline{BER} \times \tau_{\max}$ para a família de seqüências ZCZ binária com $N = 256$ e $\frac{E_b}{N_0} = 16dB$.

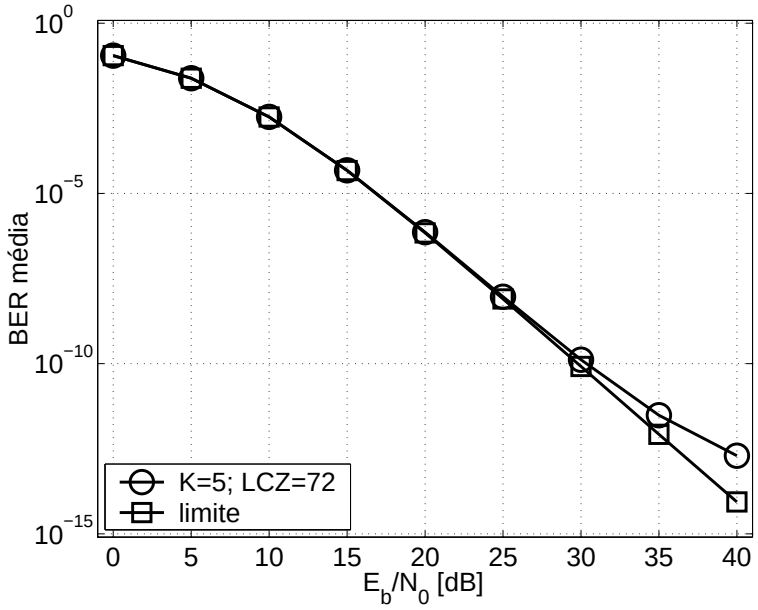

Figura 2.39: $\overline{BER} \times \frac{E}{N_0}$ para a família de seqüências Lin-Chang com $N = 511$ obtidas com $1 + x^4 + x^9$, $m = 3$ e $\tau_{\max} = 4T_c$.

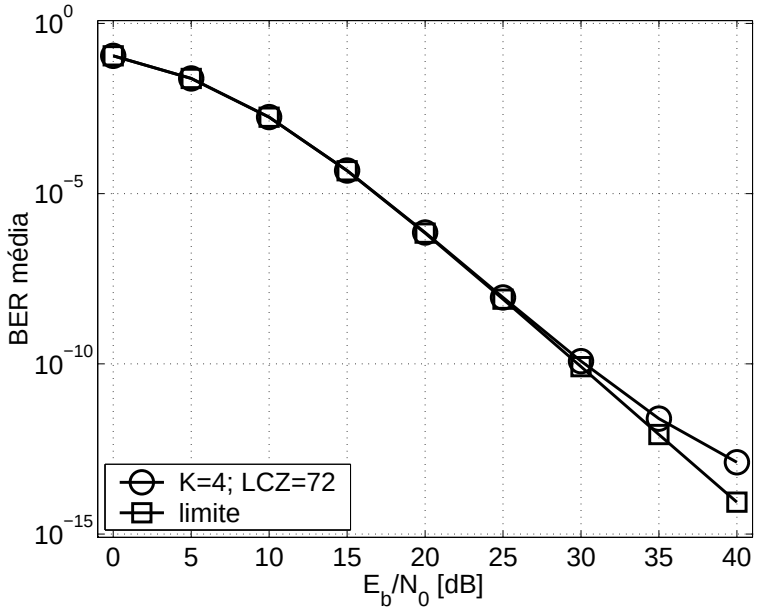

Figura 2.40: $\overline{BER} \times \frac{E}{N_0}$ para a família de seqüências LCZ-GMW binária com $N = 511$ obtidas com $1 + x^4 + x^9$, $1 + x + x^3$, $1 + x^2 + x^3$ e $\tau_{\max} = 4T_c$.

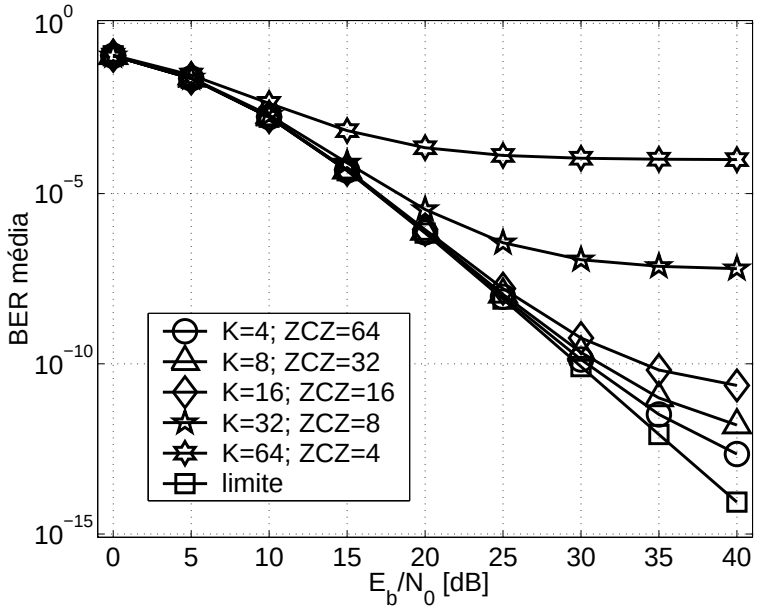

Figura 2.41: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências ZCZ com $N = 512$ e $\tau_{\max} = 4T_c$.

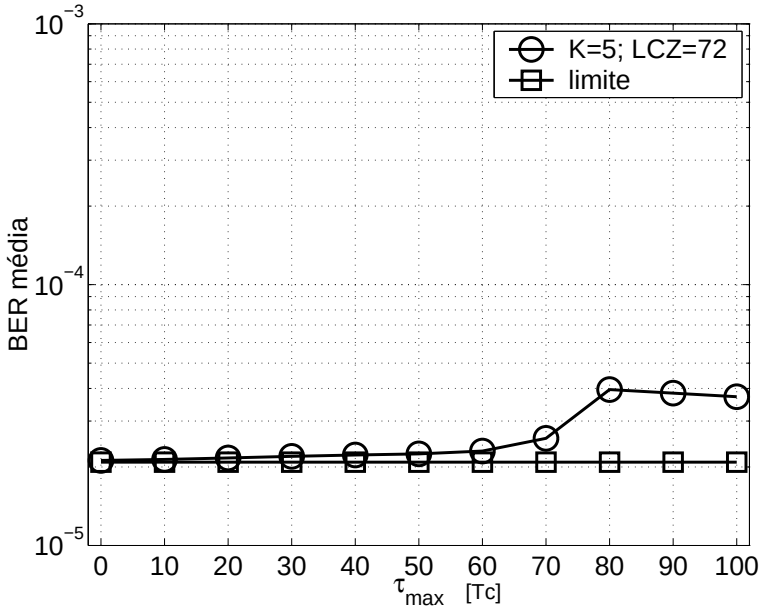

Figura 2.42: $\overline{BER} \times \tau_{\max}$ para a família de seqüências Lin-Chang com $N = 511$ obtidas com $1 + x^4 + x^9$, $m = 3$ e $\frac{E_b}{N_0} = 16dB$.

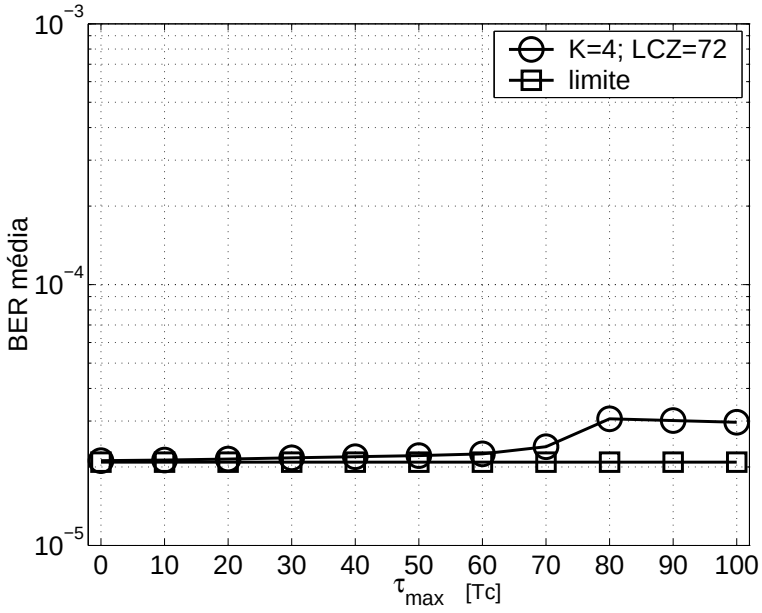

Figura 2.43: $\overline{BER} \times \tau_{\max}$ para a família de seqüências LCZ-GMW binária com $N = 511$ obtidas com $1 + x^4 + x^9$, $1 + x + x^3$, $1 + x^2 + x^3$ e $\frac{E_b}{N_0} = 16dB$.

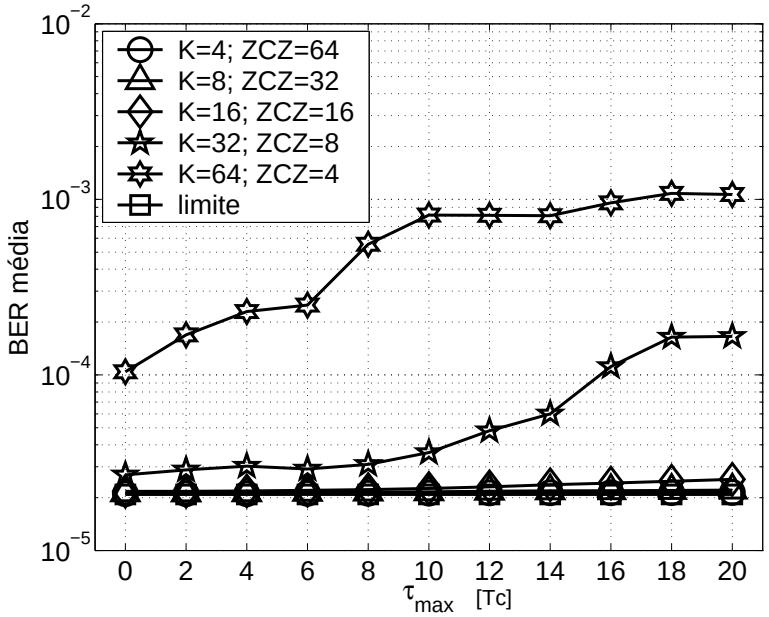

Figura 2.44: $\overline{BER} \times \tau_{\max}$ para a família de seqüências ZCZ binária com $N = 512$ e $\frac{E_b}{N_0} = 16dB$.

3 Esquemas multitaxa

Os sistemas de comunicação móvel exigem taxa de dados variáveis para integrar serviços variados como o de voz, de comunicação de dados e de multimídia. Basicamente, existem quatro esquemas de implementação de taxas de dados variáveis em sistemas CDMA, além de variações e combinações dessas (OTTOSSON, 1997) (JOHANSSON, 1998). Considerando todos os usuários com a mesma taxa de chip e, portanto, a mesma largura de banda (*bandwidth*, BW), os principais esquemas são: variação do nível de modulação, conhecido por esquema *multi-modulation* (MM), utilização de múltiplos códigos de espalhamento, conhecido por esquema *multi-code* (MC), e múltiplos do ganhos de processamento, conhecido por esquema *multi-processing gain* (MPG). O esquema *variable chip rate* (VCR), ao contrário do MPG, mantém o ganho de processamento fixo e varia a taxa de chip e, portanto, a BW alocada.

O ganho de processamento representa uma medida de quanto a interferência externa é suprimida pelo sistema. Se for desejado que todos os usuários, independente da taxa de dados, suprimam igualmente a interferência externa, o ganho de processamento deve ser constante para todos os usuários (SIMON et al., 1994) (ZIEMER; PETERSON, 1985).

3.1 Esquemas MM, MC, MPG e VCR

O esquema MM utiliza topologias que suportam altas ordens de modulação como o MPSK (*M-ary phase-shift keying*) e o MQAM (*M-ary quadrature amplitude modulation*). Quanto maior a taxa, maior deve ser a ordem de modulação utilizada. Os sinais resultantes de modulações de alta ordem necessitam de amplificadores lineares, os quais são menos eficientes em potência do que os amplificadores utilizados nos esquemas de modulação binária. Além disso, o detector para um esquema MQAM necessita estimar a amplitude para a recuperação da informação. Outro inconveniente

desse esquema é a disparidade de potência entre os usuários que transmitem baixas taxas, portanto, baixas potências, e os usuários que transmitem em altas taxas, portanto, potências elevadas. Esse efeito, similar ao efeito *near-far*, também contribui para a degradação de desempenho de um sistema com detecção convencional.

No esquema MC, os usuários de alta taxa transmitem seus dados através de canais paralelos independentes, os quais utilizam seqüências de espalhamento distintas. Mesmo utilizando modulação binária BPSK, o sinal resultante, que será a soma de vários sinais BPSK independentes, terá variação de amplitude, além da variação de fase. Essa característica representa um problema principalmente para o canal reverso, onde a eficiência em potência dos amplificadores dos terminais móveis é importante. Adicionalmente, há uma maior complexidade do receptor do terminal móvel devido à necessidade de um correlacionador (ou receptor Rake, no caso de canal multipercurso) para cada canal paralelo. Quanto maior for a taxa dos usuários, maior será o número de canais utilizados e, consequentemente, maior será a quantidade de interferência MAI produzida entre os canais, considerando que as seqüências designadas a cada um dos canais não mantém a ortogonalidade em um canal multipercurso e/ou assíncrono, ou ainda, quase síncrono.

O esquema MPG assume a mesma modulação para todos os usuários e transmite taxas de dados variáveis alterando o ganho de processamento. Verifica-se que quanto maior a taxa de dados, maior é a amplitude do sinal transmitido a fim de manter a energia de símbolo constante para todas as taxas. Essa inconveniente disparidade de potência entre sinais dos usuários, assim como no esquema MM, contribuirá para a degradação de desempenho de um sistema com detecção convencional. Outra desvantagem desse esquema é o nível de supressão de interferência não constante para os usuários devido ao ganho de processamento variável.

No esquema VCR, o ganho de processamento é constante para todos os usuários, independentemente da taxa. A taxa de chip varia, sendo maior para as altas taxas e menor para as baixas taxas. Assim, os usuários de altas taxas utilizarão uma BW maior que os usuários de baixas taxas. Há a possibilidade de separar espectralmente as portadoras dos usuários de taxas distintas, reduzindo a interferência mútua entre esses usuários. Porém, os receptores necessitam de filtros para cada BW e portadora utilizada, o que na prática limitaria a quantidade de taxas distintas disponíveis. Além disso, os sistemas de banda larga alcançam melhores desempenhos do que os de banda

estreita devido a possibilidade de utilização da diversidade Rake em canais seletivos.

Um conjunto de seqüências adequado para um sistema de taxa única será também adequado para um sistema multitaxa que utiliza o esquema MM. Em ambos os sistemas, a forma de espalhar o sinal é a mesma para qualquer taxa de dados. Taxas de dados mais elevadas são obtidas utilizando modulação de maior ordem, mantendo as taxas de símbolo e chip e o ganho de processamento constantes.

No caso de se utilizar o esquema MC, o conjunto de seqüências deve estar preparado para ter mais seqüências que o número de usuários ativos, pois quanto maior a taxa dos usuários, mais canais (mais seqüências) serão utilizados. Similarmente ao sistema QS-CDMA modelado anteriormente, em um sistema que utiliza o esquema MC, as seqüências utilizadas em canais de usuários distintos devem possuir um intervalo $|d| \leq \left\lceil \frac{\tau_{\max}+\Delta_L}{T_c} \right\rceil$ em que as funções de correlação cruzada periódica são reduzidas. As seqüências utilizadas nos canais de um mesmo usuário devem possuir essa propriedade de correlação cruzada apenas com as seqüências dos canais dos demais usuários. Para as seqüências dos canais de um mesmo usuário, é suficiente que elas resultem em valores reduzidos para as funções de correlação cruzada periódica apenas para $|d| \leq \left\lceil \frac{\Delta_L}{T_c} \right\rceil$. Isso porque as seqüências de um mesmo usuário serão transmitidas sempre em fase, pois são geradas dessa forma no transmissor.

No esquema MPG, o correlacionador de um dado usuário fará a integração no período de símbolo que representará apenas um segmento da seqüência utilizada por um usuário de menor taxa e mais de um período da seqüência utilizada por um usuário de maior taxa. Assim, um conjunto adequado para o esquema MPG deve resultar em reduzidos valores de correlação cruzada entre segmentos de seqüências.

Existem poucas publicações sobre seleção de seqüências para sistemas QS-CDMA multitaxa. Destacam-se o trabalho da referência (SAITO et al., 2001), onde é apresentada uma metodologia para seleção de seqüências de Gold para sistemas multitaxa MC e o trabalho da referência (LEE; JOO; TCHAH, 2001), onde é apresentada uma metodologia para seleção de seqüências para sistemas MPG.

Seções subseqüentes descreverão os esquemas MC e MPG com maiores detalhes. Devido às restrições de implementação do esquema VCR mencionadas, não serão analisados conjuntos de seqüências adequados para sistemas multitaxa que utilizam tal esquema.

3.2 Desempenho de sistemas de taxa de dados variável do tipo MC

3.2.1 Modelagem do sistema QS-CDMA com esquema MC

Considera-se um sistema multitaxa do tipo MC oferecendo n taxas de dados distintas (ou n serviços distintos). A taxa básica R é oferecida por meio de apenas um canal disponibilizado para cada usuário do serviço. Taxas mais elevadas são alcançadas utilizando mais de um canal para cada usuário do serviço (figura 3.1).

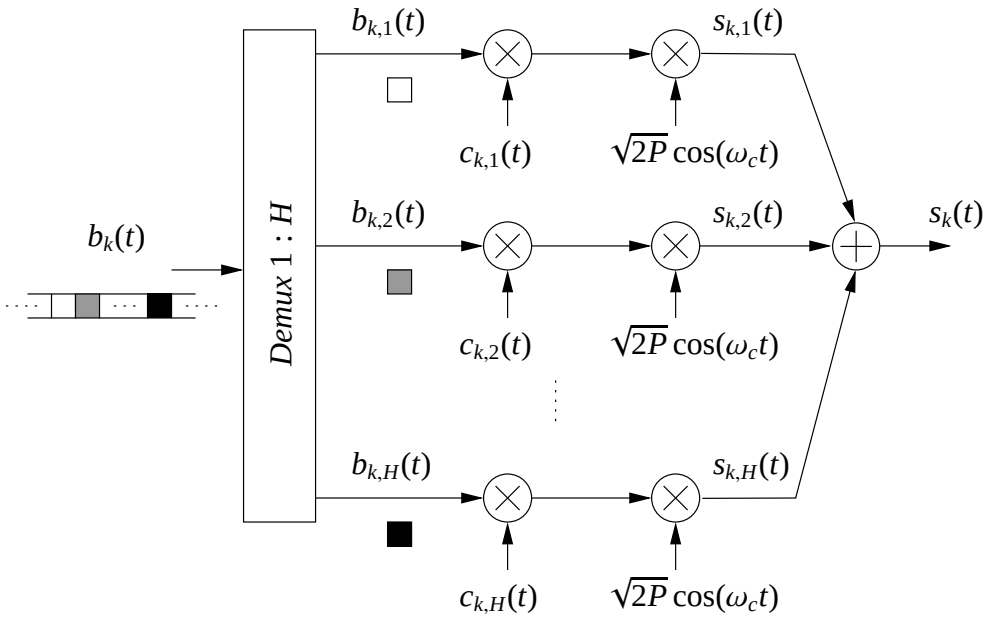

Figura 3.1: Transmissor com esquema MC.

O sinal transmitido pelo h-ésimo canal utilizado pelo k-ésimo usuário será:

$$s_{k,h}(t) = \sqrt{2P} b_{k,h}(t) c_{k,h}(t) cos(\omega_c t) \tag{3.1}$$

onde P é a potência do sinal transmitido, a qual será considerada igual para todos os usuários; $b_{k,h}(t)$ é o sinal de informação modulada em BPSK transmitida pelo h-ésimo canal utilizado pelo k-ésimo usuário e $c_{k,h}(t)$ o sinal relativo à seqüência de espalhamento, dado por:

$$c_{k,h}(t) = \sum_{m=-\infty}^{\infty} p(t - mT_c) \underline{c}_{k,h,m} \tag{3.2}$$

onde $\underline{c}_{k,h,m} = c_{k,h,m(\text{mod } N)}$ é o m-ésimo chip da seqüência de espalhamento de comprimento N utilizada pelo h-ésimo canal do k-ésimo usuário; $p(t)$ é a formatação de pulso retangular de amplitude unitária no intervalo $[0; T_c)$ e zero fora.

O sinal recebido na estação rádio base será:

$$r(t) = \sum_{u=1}^{U} \sum_{h=1}^{H} \sum_{\mathcal{L}=1}^{L} \alpha_{\mathcal{L}}(t) s_{u,h}(t - \tau_{u,\mathcal{L}}) + n(t) \tag{3.3}$$

onde U é o número de usuários ativos no sistema; $\alpha_{\mathcal{L}}(t)$ representa o ganho do canal para o componente multipercurso $\mathcal{L}$ e $\tau_{u,\mathcal{L}}$ o atraso absoluto do $\mathcal{L}$-ésimo componente multipercurso do u-ésimo usuário.

Fazendo o desenvolvimento análogo à modelagem do sistema de taxa única (seção 1.1) a saída do ℓ-ésimo correlacionador do h-ésimo canal do k-ésimo usuário analisada apenas em um período de símbolo de informação T (sem perda de generalidade considera-se o intervalo $0 \leq t \leq T$), será:

$$\begin{aligned} z_{k,h,\ell} &= \int_0^T r(t) c_{k,h}^*(t) cos(\omega_c t - \phi_{k,\ell}) dt \\ &= \sqrt{\frac{P}{2}} \alpha_\ell T b_{k,h}^{(0)} + I_{k,h,\ell} + S I_{k,h,\ell} + n_{k,h,\ell}(t) \end{aligned} \tag{3.4}$$

onde o primeiro termo representa o sinal de interesse, o segundo a MAI, o terceiro a SI e o último o ruído aditivo branco Gaussiano (AWGN) processado; $\phi_{k,\ell} = \omega_c \tau_{k,\ell}$ é o deslocamento de fase devido ao atraso $\tau_{k,\ell}$. Foi considerado o ganho de canal $\alpha_{\mathcal{L}}(t)$ constante no intervalo de integração T (ou periodo do símbolo de informação). Assim, $\alpha_{\mathcal{L}}(t) = \alpha_{\mathcal{L}}$.

Considerando recepção Rake com D correlacionadores (*fingers*) e combinador de razão máxima (*maximum ratio combiner*, MRC), tem-se na saída do combinador:

$$\begin{aligned} y_{k,h} &= \sum_{\ell=1}^{D} \Re\{z_{k,h,\ell} \hat{\alpha}_\ell\} \\ \hat{b}_{k,h}^{(0)} &= \text{sign}(y_{k,h}) \end{aligned} \tag{3.5}$$

onde $\hat{\alpha}_\ell$ é a estimativa do ganho de canal, a qual foi considerada perfeita, e $\hat{b}_{k,h}^{(0)}$ é a informação de interesse estimada.

A MAI sobre o ℓ-ésimo correlacionador do h-ésimo canal do k-ésimo usuário será:

$$
\begin{aligned}
I_{k,h,\ell} &= \sum_{u=1}^{U} \sum_{(g=1,\ g\neq h \ para \ u=k)}^{H} \sum_{\mathcal{L}=1}^{L} \sqrt{2P}\cdot \\
&\cdot \int_0^T \alpha_{\mathcal{L}}(t) b_{u,g}(t-\tau_{u,\mathcal{L}}) c_{u,g}(t-\tau_{u,\mathcal{L}}) c^*_{k,h}(t) cos(\omega_c t - \phi_{u,\mathcal{L}}) cos(\omega_c t - \phi_{k,\ell}) dt \\
&= \sum_{u=1}^{U} \sum_{(g=1,\ g\neq h \ para \ u=k)}^{H} \sum_{\mathcal{L}=1}^{L} \sqrt{\frac{P}{2}} \alpha_{\mathcal{L}} \int_0^T b_{u,g}(t-\tau_{u,\mathcal{L}}) c_{u,g}(t-\tau_{u,\mathcal{L}}) c^*_{k,h}(t) dt \ cos(\varphi_{u,\mathcal{L}})
\end{aligned}
\tag{3.6}
$$

onde $\tau_{u,\mathcal{L}} = \tau_{u,\mathcal{L}} - \tau_{k,\ell}$ é o atraso relativo entre o sinal de interesse (sinal do ℓ-ésimo componente multipercurso do h-ésimo canal do k-ésimo usuário) e o sinal interferente (sinal do $\mathcal{L}$-ésimo componente multipercurso do g-ésimo canal do u-ésimo usuário); $\varphi_{u,\mathcal{L}} = \phi_{u,\mathcal{L}} - \phi_{k,\ell}$ é a fase relativa das portadoras do sinal de interesse e do sinal interferente. Os termos que correspondem ao atraso relativo e à fase relativa não possuem os índices do sinal de interesse para simplificar a notação.

As *pdf*s de $\varphi_{u,\mathcal{L}}$, de $\tau_{u,\mathcal{L}}$ e dos símbolos de informação são consideradas como na modelagem do sistema de taxa única (seção 1.1).

A SI sobre o ℓ-ésimo correlacionador do h-ésimo canal do k-ésimo usuário será:

$$
SI_{k,h,\ell} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \sqrt{\frac{P}{2}} \alpha_{\mathcal{L}} \int_0^T b_{k,h}(t-\tau_{k,\mathcal{L}}) c_{k,h}(t-\tau_{k,\mathcal{L}}) c^*_{k,h}(t) dt \ cos(\varphi_{k,\mathcal{L}}) \tag{3.7}
$$

O AWGN processado para o ℓ-ésimo correlacionador do h-ésimo canal do k-ésimo usuário é dado por:

$$
\begin{aligned}
n_{k,h,\ell}(t) &= \int_0^T n(t) c^*_{k,h}(t) cos(\omega_c t) dt \\
&= \sum_{m=0}^{N-1} \underline{c}^*_{k,h,m} \int_{mT_c}^{(m+1)T_c} n(t) cos(\omega_c t) dt
\end{aligned}
\tag{3.8}
$$

Será calculada a relação sinal-ruído-interferência (SNIR) na saída do ℓ-ésimo correlacionador do k-ésimo usuário:

$$SNIR_{k,h,\ell} = \frac{\text{potência do sinal de interesse}}{\text{potência da MAI, da SI e do AWGN processado}} \tag{3.9}$$

onde a potência do sinal de interesse será:

$$\mathbb{E}_{\alpha}\left\{\left(\sqrt{\frac{P}{2}}\alpha_{\ell}Tb_{k,h}^{(0)}\right)^2\right\} = \frac{P}{2}T^2\mathbb{E}_{\alpha}\{\alpha_{\ell}^2\} \tag{3.10}$$

Analogamente ao caso de taxa única (seção 1.1), a potência do AWGN processado será:

$$\mathbb{E}\left\{(n_{k,h,\ell}(t))^2\right\} = \frac{N_0\,T}{4} \tag{3.11}$$

Como φ, b, τ e α são variáveis aleatórias independentes, a potência da MAI e da SI sobre o ℓ-ésimo correlacionador do k-ésimo usuário serão:

$$\begin{aligned}
\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,h,\ell})^2\right\} &= \mathbb{E}_{\alpha}\left\{\mathbb{E}_{\tau}\left\{\mathbb{E}_{b}\left\{\mathbb{E}_{\varphi}\left\{(I_{k,h,\ell})^2\right\}\right\}\right\}\right\} \\
\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(SI_{k,h,\ell})^2\right\} &= \mathbb{E}_{\alpha}\left\{\mathbb{E}_{\tau}\left\{\mathbb{E}_{b}\left\{\mathbb{E}_{\varphi}\left\{(SI_{k,h,\ell})^2\right\}\right\}\right\}\right\}
\end{aligned} \tag{3.12}$$

Inicialmente, calcula-se a potência da MAI. Realizando a média na variável $\varphi_{u,g,\mathcal{L}}$:

$$\begin{aligned}
\mathbb{E}_{\varphi}\left\{(I_{k,h,\ell})^2\right\} = &\sum_{(u=1,\ u\neq k)}^{U}\sum_{g=1}^{H}\sum_{\mathcal{L}=1}^{L}\frac{P}{4}\alpha_{\mathcal{L}}^2J_{u,g,\mathcal{L}}^2 \ + \\
&+ \sum_{(g=1,\ g\neq h)}^{H}\frac{P}{4}\alpha_{\ell}^2b_{k,g}^{(0)}T_c\theta(\mathbf{c}_{k,g},\mathbf{c}_{k,h},0) \ + \\
&+ \sum_{(g=1,\ g\neq h)}^{H}\sum_{(\mathcal{L}=1,\ \mathcal{L}\neq\ell)}^{L}\frac{P}{4}\alpha_{\mathcal{L}}^2J_{k,g,\mathcal{L}}^2
\end{aligned} \tag{3.13}$$

onde $\theta(\mathbf{c}_{k,g},\mathbf{c}_{k,h},d)$ é a função de correlação cruzada periódica par entre as seqüências utilizadas pelo g-ésimo canal do u-ésimo usuário e pelo h-ésimo canal do k-ésimo usuário; $J_{u,g,\mathcal{L}}$ será:

$$\begin{aligned} J_{u,g,\mathcal{L}} &= \int_0^T b_{u,g}(t-\tau_{u,\mathcal{L}})c_{u,g}(t-\tau_{u,\mathcal{L}})c^*_{k,h}(t)dt \\ &= \begin{cases} \left(b^{(-1)}_{u,g}\mathcal{R}_{u,g,k,h}(\tau_{u,\mathcal{L}}) + b^{(0)}_{u,g}\tilde{\mathcal{R}}_{u,g,k,h}(\tau_{u,\mathcal{L}})\right), & \tau_{u,\mathcal{L}} \geq 0 \\ \left(b^{(0)}_{u,g}\mathcal{R}_{u,g,k,h}(\tau_{u,\mathcal{L}}) + b^{(1)}_{u,g}\tilde{\mathcal{R}}_{u,g,k,h}(\tau_{u,\mathcal{L}})\right), & \tau_{u,\mathcal{L}} < 0 \end{cases} \end{aligned} \tag{3.14}$$

onde $b^{(-1)}_{u,g}$, $b^{(0)}_{u,g}$ e $b^{(1)}_{u,g}$ são as informações do usuário interferente que participam da integração e as funções $\mathcal{R}_{u,g,k,h}(\tau_{u,\mathcal{L}})$ e $\tilde{\mathcal{R}}_{u,g,k,h}(\tau_{u,\mathcal{L}})$ são chamadas de funções de correlação cruzada parciais par e ímpar, respectivamente, definidas como:

$$\begin{aligned} \mathcal{R}_{u,g,k,h}(\tau) &= \int_0^{\underline{\tau}} c_{u,g}(t-\underline{\tau})c^*_{k,h}(t)\,dt \\ \tilde{\mathcal{R}}_{u,g,k,h}(\tau) &= \int_{\underline{\tau}}^T c_{u,g}(t-\underline{\tau})c^*_{k,h}(t)\,dt, \quad \text{com } \underline{\tau} = \tau \text{ para } \tau \geq 0 \text{ e } \underline{\tau} = T+\tau \text{ para } \tau < 0 \end{aligned} \tag{3.15}$$

Observa-se que, para $\tau < 0$, $\mathcal{R}_{u,g,k,h}(\tau)$ e $\tilde{\mathcal{R}}_{u,g,k,h}(\tau)$ são equivalentes a $\mathcal{R}_{u,g,k,h}(T+\tau)$ e $\tilde{\mathcal{R}}_{u,g,k,h}(T+\tau)$, respectivamente.

A potência da MAI sobre o ℓ-ésimo correlacionador do h-ésimo canal do k-ésimo usuário será:

$$\begin{aligned} \mathbb{E}_{\alpha,\varphi,b,\tau}\left\{(I_{k,h,\ell})^2\right\} &= \sum_{(u=1,\ u\neq k)}^{U}\sum_{g=1}^{H}\sum_{\mathcal{L}=1}^{L}\frac{P}{8\tau_{max}}\mathbb{E}_\alpha\{\alpha^2_{\mathcal{L}}\}\sum_{m=\upsilon_1}^{\upsilon_2-1}\rho_{u,g,k,h}(m \bmod N) \ + \\ &+ \sum_{(g=1,\ g\neq h)}^{H}\frac{P}{4}\mathbb{E}_\alpha\{\alpha^2_\ell\}T_c\theta(\mathbf{c}_{k,g},\mathbf{c}_{k,h},0) \ + \\ &+ \sum_{(g=1,\ g\neq h)}^{H}\sum_{(\mathcal{L}=1,\ \mathcal{L}\neq\ell)}^{L}\frac{P}{8\tau_{max}}\mathbb{E}_\alpha\{\alpha^2_{\mathcal{L}}\}\sum_{m=\upsilon_1}^{\upsilon_2-1}\rho_{k,g,k,h}(m \bmod N) \end{aligned} \tag{3.16}$$

onde:

$$\begin{aligned} \rho_{u,g,k,h}(m) &= \frac{T_c^3}{3}\Big(C_{u,g,k,h}(m-N+1)C_{u,g,k,h}(m-N) + C_{u,g,k,h}(m+1)C_{u,g,k,h}(m) + \\ &+ C^2_{u,g,k,h}(m-N) + C^2_{u,g,k,h}(m) + C^2_{u,g,k,h}(m-N+1) + C^2_{u,g,k,h}(m+1)\Big) \end{aligned} \tag{3.17}$$

e

$$C_{u,g,k,h}(d) = \begin{cases} \sum_{v=0}^{N-d-1} c_{u,g,v} c^*_{k,h,v+d} & 0 \leq d \leq N-1 \\ \sum_{v=0}^{N+d-1} c_{u,g,v-d} c^*_{k,h,v} & 1-N \leq d < 0 \\ 0 & |d| \geq N \end{cases} \tag{3.18}$$

onde $\mathbf{c}_{k,h} = \{c_{k,h,1}, c_{k,h,2}, ..., c_{k,h,N}\}$ e $\mathbf{c}_{u,g} = \{c_{u,g,1}, c_{u,g,2}, ..., c_{u,g,N}\}$.

Analogamente ao caso de taxa única (seção 1.1), a potência da SI será:

$$\mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,h,\ell})^2\right\} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \frac{P}{4}\mathbb{E}_{\alpha}\left\{\alpha^2_{\mathcal{L}}(t)\right\}\left(\left(T_c C_{k,h,k,h}(\frac{\tau_{k,\mathcal{L}}}{T_c} - N)\right)^2 + \left(T_c C_{k,h,k,h}(\frac{\tau_{k,\mathcal{L}}}{T_c})\right)^2\right) \tag{3.19}$$

Então, a relação sinal-ruído-interferência (SNIR) na saída do ℓ-ésimo correlacionador do h-ésimo canal k-ésimo usuário, será:

$$SNIR_{k,h,\ell} = \frac{\frac{P}{2}T^2\mathbb{E}_{\alpha}\{\alpha^2_{\ell}\}}{\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,h,\ell})^2\right\} + \mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,h,\ell})^2\right\} + \frac{N_0 T}{4}} \tag{3.20}$$

onde $\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,h,\ell})^2\right\}$ é dado pela equação (3.16) e $\mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,h,\ell})^2\right\}$ é dado pela equação (3.19).

Como as energias de símbolo $E_b = P \cdot T$ são iguais para todos os usuários:

$$SNIR_{k,h,\ell} = \frac{E_b\ \mathbb{E}_{\alpha}\{\alpha^2_{\ell}\}}{\frac{2}{T}\left\{\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,h,\ell})^2\right\} + \mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,h,\ell})^2\right\}\right\} + \frac{N_0}{2}} \tag{3.21}$$

Serão apresentados resultados em termos de taxa de erro de bit (BER) de sistemas QS-CDMA com esquema MC, utilizando diferentes conjuntos de seqüências. Será considerado recepção Rake MRC e canal com desvanecimento multipercurso Rayleigh.

Assim como observado no caso de taxa única, se nas equações (3.6) e (3.7) os somatórios $\sum_g$, $\sum_u$ e $\sum_{\mathcal{L}}$ compreenderem um grande número de termos, de (YAO, 1977), pode-se afirmar que a *pdf* resultante para a MAI adicionada à SI tenderá a uma

Gaussiana. Fazendo-se essa aproximação, obtém-se uma expressão analítica para o desempenho aproximado do *k*-ésimo usuário em termos de taxa de erro de bit (BER) por meio de (PROAKIS, 1995):

$$BER_{k,h} = \frac{1}{2}\sum_{\ell=1}^{D} \Upsilon_\ell \left[1 - \sqrt{\frac{SNIR_{k,h,\ell}}{2 + SNIR_{k,h,\ell}}}\right] \tag{3.22}$$

$$\Upsilon_\ell = \prod_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{D} \frac{SNIR_{k,h,\ell}}{SNIR_{k,h,\ell} - SNIR_{k,h,\mathcal{L}}} \tag{3.23}$$

A avaliação de desempenho será realizada observando a BER média dos usuários de cada serviço ($\overline{BER_i}$) dada pela média aritmética das BER de todos os canais de todos os usuários de cada serviço.

3.2.2 Resultados numéricos

As figuras 3.2 e 3.3 apresentam resultados de $\overline{BER} \times \frac{E}{N_0}$ para um sistema QS-CDMA com características descritas na tabela 3.1, considerando seqüências QS com $N = 127$ e ZCZ com $N = 128$, respectivamente. A família QS com $N = 127$, $K = 32$ e $L_{CZ} = 1$ foi obtida de $Gold(207, 277)$ com $r = 3$, tabela 2.13. A família ZCZ com $N = 128$, $K = 32$ e $Z_{CZ} = 2$ foi obtida com $n = 4$, $m = 1$ e $= 3$, tabela 2.17.

Para a família ZCZ, as seqüências são atribuídas aos usuários de forma ordenada. Os usuários de taxa básica utilizam as primeiras seqüências ZCZ da família (primeiras linhas da matriz F^n, seção 2.2.3). O usuário de taxa mais elevada utiliza as últimas seqüências ZCZ da família (últimas linhas da matriz F^n, seção 2.2.3). A atribuição das seqüências QS para os usuários do sistema 1 é descrita pela tabela 3.2.

O perfil atraso-potência adotado foi o mesmo adotado na seção 2.3.1 dado pela tabela 2.11. Observa-se que o desempenho obtido com a família ZCZ é superior ao obtido com a família QS. Isso pode ser explicado pela maior zona de correlação reduzida/nula da família ZCZ.

Alterando-se a taxa oferecida pelo serviço 3 para $R_3 = 20 \times R$ e o número de usuários do serviço 3 para 1 mantendo-se os 32 canais utilizados, obtém-se os resultados apresentados pelas figuras 3.4 e 3.5. Há um aumento de desempenho para o serviço 3 para as duas famílias. A família ZCZ se mantém com melhor desempenho que a família QS.

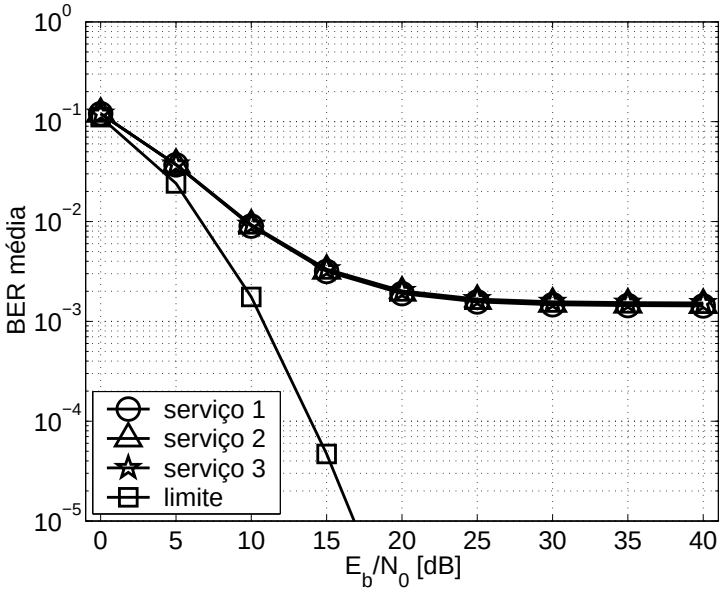

Figura 3.2: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências QS com $N = 127$, $LCZ = 1$, $\tau_{\max} = 2T_c$ e $D = 4$; 2 usuários utilizam o serviço 1 com $R_1 = 30,236kb/s$, 2 usuários utilizam o serviço 2 com $R_2 = 151,181kb/s$ e 2 usuários utilizam o serviço 3 com $R_3 = 302,362kb/s$.

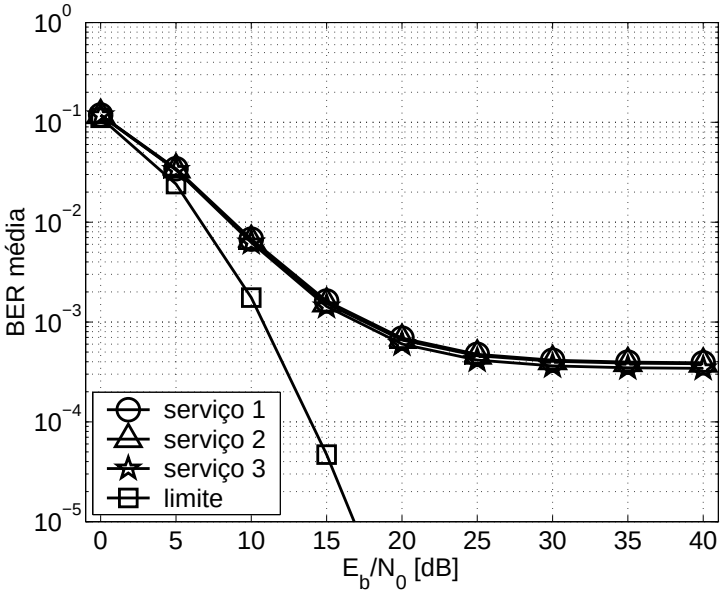

Figura 3.3: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências ZCZ com $N = 128$, $ZCZ = 2$, $\tau_{\max} = 2T_c$ e $D = 4$; 2 usuários utilizam o serviço 1 com $R_1 = 30kb/s$, 2 usuários utilizam o serviço 2 com $R_2 = 150kb/s$ e 2 usuários utilizam o serviço 3 com $R_3 = 300kb/s$.

Considere agora o sistema QS-CDMA com os parâmetros da tabela 3.3. Os de-

Tabela 3.1: Parâmetros de configuração do sistema 1.

$\tau_{\max}$	$2T_c$	
D	4	
n	3	
U_1	2	
U_2	2	
U_3	2	
N	127	128
R	$30,236kb/s$	$30kb/s$
R_1	$1 \times R = 30,236kb/s$	$1 \times R = 30kb/s$
R_2	$5 \times R = 151,181kb/s$	$5 \times R = 150kb/s$
R_3	$10 \times R = 302,362kb/s$	$10 \times R = 300kb/s$

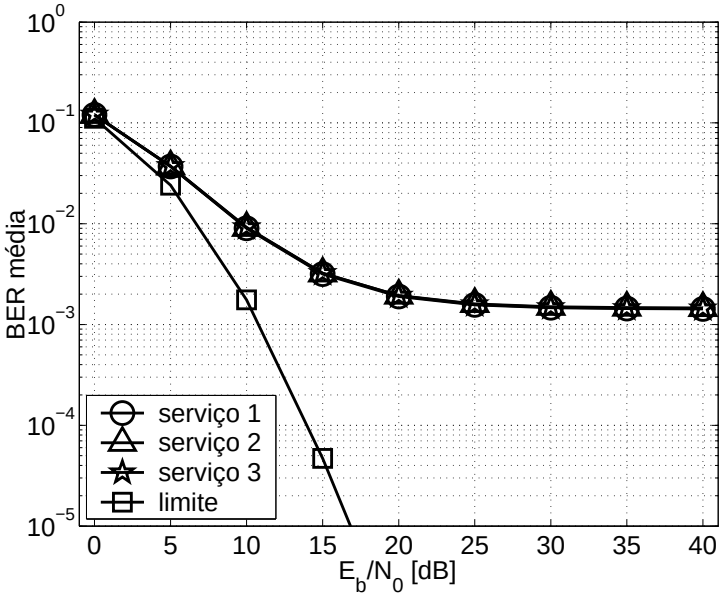

Figura 3.4: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências QS com $N = 127$, $LCZ = 1$ e $\tau_{\max} = 2T_c$; 2 usuários utilizam o serviço 1 com $R_1 = 30,236kb/s$, 2 usuários utilizam o serviço 2 com $R_2 = 151,181kb/s$ e 1 usuário utiliza o serviço 3 com $R_3 = 604,724kb/s$.

sempenhos obtidos com as famílias ZCZ de $N = 256$ e $N = 512$ são apresentados pelas figuras 3.6 e 3.7. A família ZCZ com $N = 256$ foi obtida com os parâmetros $n = 5$, $m = 1$ e $t = 4$ e a família ZCZ com $N = 512$ foi obtida com os parâmetros $n = 5$, $m = 1$ e $t = 3$.

Para sistemas que utilizam esquema MC são necessárias famílias que compreendem um grande número de seqüências para acomodar taxas de dados elevadas, conforme já mencionado na seção 3. Assim, não é viável utilizar seqüências de com-

Tabela 3.2: Atribuição de seqüências QS para os usuários do sistema 1.

serviço i	usuário k	seqüência do conjunto $Gold(207, 277)$
1	1	$\mathbf{g_1}$
	2	$\mathbf{g_8}$
2	1	$\mathbf{g_{16}}$
		$\mathbf{g_{18}}$
		$\mathbf{g_{21}}$
		$\mathbf{g_{26}}$
		$\mathbf{g_{28}}$
	2	$\mathbf{g_{34}}$
		$\mathbf{g_{38}}$
		$\mathbf{g_{41}}$
		$\mathbf{g_{44}}$
		$\mathbf{g_{52}}$
3	1	$\mathbf{g_{55}}$
		$\mathbf{g_{58}}$
		$\mathbf{g_{62}}$
		$\mathbf{g_{66}}$
		$\mathbf{g_{70}}$
		$\mathbf{g_{73}}$
		$\mathbf{g_{75}}$
		$\mathbf{g_{79}}$
		$\mathbf{g_{84}}$
		$\mathbf{g_{88}}$
	2	$\mathbf{g_{90}}$
		$\mathbf{g_{95}}$
		$\mathbf{g_{97}}$
		$\mathbf{g_{100}}$
		$\mathbf{g_{102}}$
		$\mathbf{g_{104}}$
		$\mathbf{g_{106}}$
		$\mathbf{g_{112}}$
		$\mathbf{g_{118}}$
		$\mathbf{g_{127}}$

primento reduzido, pois na maioria dos casos, para uma determinada família, quanto menor o comprimento das seqüências, menor é a família.

Não foram obtidas figuras de desempenho para as famílias QS de comprimento $N = 512$ devido à complexidade de obtenção do conjunto já explicada na seção 2.3.1. Devido a esse mesmo motivo não foram obtidas figuras de desempenho para a família OQS. As famílias LCZ-GMW e as famílias Lin-Chang com $N = 63$ e $N = 511$ apresentam poucas seqüências (tabelas 2.8 e 2.7, respectivamente) e, por isso, não foram

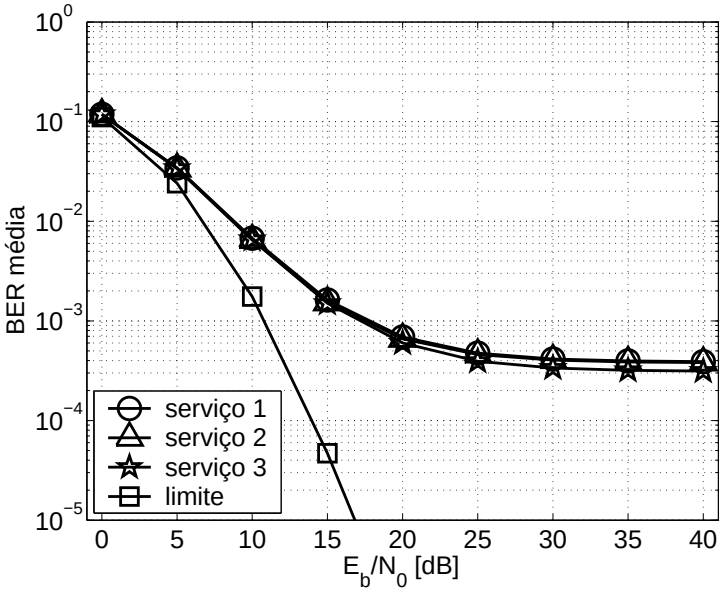

Figura 3.5: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências ZCZ com $N = 128$, $LCZ = 2$ e $\tau_{\max} = 2T_c$; 2 usuários utilizam o serviço 1 com $R_1 = 30b/s$, 2 usuários utilizam o serviço 2 com $R_2 = 150kb/s$ e 1 usuário utiliza o serviço 3 com $R_3 = 600kb/s$.

Tabela 3.3: Parâmetros de configuração do sistema 2.

$\tau_{\max}$	$2T_c$	
D	4	
n	3	
U_1	9	
U_2	3	
U_3	1	
N	256	512
R	$15kb/s$	$7,5kb/s$
R_1	$1 \times R = 15kb/s$	$1 \times R = 7,5kb/s$
R_2	$10 \times R = 150kb/s$	$10 \times R = 75kb/s$
R_3	$25 \times R = 375kb/s$	$25 \times R = 187,5kb/s$

consideradas na análise de sistemas com esquema MC. As famílias Lin-Chang com $N = 255$ e $N = 1023$ possuem muitas seqüências, porém, não existe um método sistemático para a seleção das sementes, conforme já mencionado na seção 2.3.1.

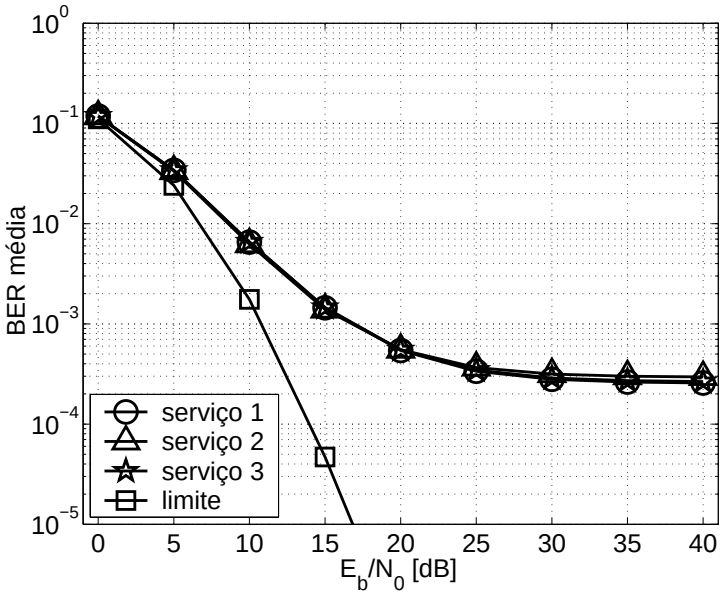

Figura 3.6: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências ZCZ com $N = 256$, $ZCZ = 2$ e $\tau_{\max} = 2T_c$; 9 usuários utilizam o serviço 1 com $R_1 = 15kb/s$, 3 usuários utilizam o serviço 2 com $R_2 = 150kb/s$ e 1 usuário utiliza o serviço 3 com $R_3 = 375kb/s$.

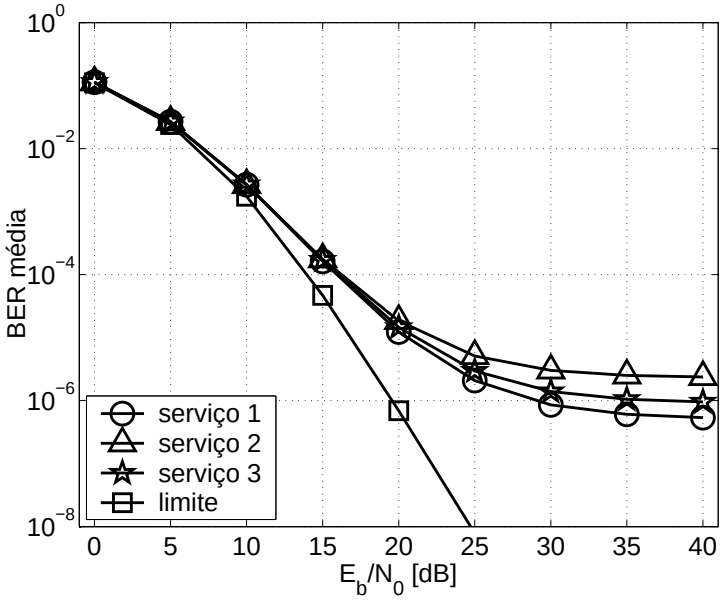

Figura 3.7: $\overline{BER} \times \frac{E}{N_0}$ para famílias de seqüências ZCZ com $N = 512$, $ZCZ = 4$ e $\tau_{\max} = 2T_c$; 9 usuários utilizam o serviço 1 com $R_1 = 7,5kb/s$, 3 usuários utilizam o serviço 2 com $R_2 = 75kb/s$ e 1 usuário utiliza o serviço 3 com $R_3 = 187,5kb/s$.

3.3 Seqüências para sistemas de taxa de dados variável do tipo MPG

Existem diversos trabalhos que sugerem seqüências que resultam em reduzidos valores de autocorrelação e correlação cruzada para pequenos deslocamentos. As seções an-

teriores apresentaram alguns desses. Na maioria dos trabalhos são estudadas funções de correlação entre seqüências de mesmo comprimento. Em sistemas que utilizam esquemas multitaxa do tipo MPG, as correlações envolvidas no processo de detecção e recuperação da informação transmitida são realizadas entre:

1. seqüências de mesmo comprimento, caso o usuário interferente utilize a mesma taxa de dados do usuário de interesse;

2. uma seqüência e um trecho de outra seqüência de comprimento maior, caso o usuário interferente utilize taxa de dados menos elevada que o usuário de interesse;

3. uma seqüência e alguns períodos de outra seqüência de comprimento menor, caso o usuário interferente utilize taxa de dados mais elevada que o usuário de interesse;

Em relação aos dois últimos casos, as propriedades de correlação na maioria das vezes não são conhecidas totalmente, mesmo na condição de pequenos deslocamentos entre seqüências (caso dos sistemas QS-CDMA). Para otimizar um sistema multitaxa do tipo MPG em termos de desempenho, todos os três casos apontados acima devem ser considerados. Existem poucos trabalhos sobre otimização de seqüências de espalhamento para MPG, sendo que a maioria discute o problema para o caso síncrono (canal direto). Especificamente para sistemas que permitem um reduzido nível de assincronismo (canal reverso de um sistema QS-CDMA) encontra-se apenas a referência (LEE; JOO; TCHAH, 2001). Nessa referência, a modelagem do sistema considera um único componente multipercurso de cada usuário e canal sem desvanecimento. Dessa forma, não há SI e, conseqüentemente, as autocorrelações entre as seqüências de espalhamento não são consideradas. O método utilizado em (LEE; JOO; TCHAH, 2001) consiste em minimizar o parâmetro chamado interferência média multitaxa (*average multi-rate interference parameter*, AMIP), o qual está relacionado com a soma da MAI observada no receptor convencional de cada um dos usuários do sistema. O AMIP é minimizado através do ajuste das fases iniciais das seqüências de espalhamento do conjunto.

O método de otimização de seqüências para MPG apresentado aqui consiste na procura por seqüências que resultam na maximização do parâmetro relação sinal-

ruído-interferência (*signal-to-noise-to-interference* ratio, SNIR), o qual está intimamente relacionado com o desempenho do sistema. Considera-se a SI, ou seja, canal multipercurso e, adicionalmente, diversidade Rake no receptor. Em canal com desvanecimento multipercurso, não é razoável minimizar simplesmente a interferência na saída do correlacionador, como em (LEE; JOO; TCHAH, 2001), pois os componentes multipercurso sofrem atenuações distintas e, portanto, as interferências MAI e SI podem ser mais significativas na saída de um correlacionador do Rake do que em outro. Maximizando-se a SNIR, indiretamente a MAI e a SI são minimizadas diferentemente para cada componente multipercurso, ou seja, componentes multipercurso mais atenuados tenderão a ter MAI e SI menos elevadas e componentes multipercurso menos atenuados tenderão a ter MAI e SI mais elevadas, de forma que a SNIR é maximizada para ambos. Dessa forma, além da minimização da MAI e da SI, há também um melhor aproveitamento da diversidade Rake.

A seguir será apresentada a família de seqüências OVSF, a qual é adequada para sistemas síncronos multitaxa do tipo MPG. Esse conjunto é composto por seqüências Walsh-Hadamard organizadas de tal forma a viabilizar a implementação de sistemas síncronos multitaxa do tipo MPG. No final deste capítulo, serão realizadas comparações entre utilizar o conjunto OVSF em sistemas QS-CDMA e utilizar um conjunto de seqüências selecionadas conforme o método que será proposto aqui. Na seqüência, será apresentada a modelagem de um sistema QS-CDMA que utiliza o esquema MPG e caracterizadas a MAI e a SI. Serão também calculadas as potências da MAI e da SI na saída de um correlacionador do Rake e, então, apresentada uma expressão para a SNIR do sistema modelado.

3.3.1 Família OVSF

Em (ADACHI; SAWAHASHI; OKAWA, 1997) foi proposto um conjunto de seqüências adequado para sistemas síncronos multitaxa do tipo MPG. Essas seqüências são chamdas de OVSF (*orthogonal variable spreading factor sequences*).

Um conjunto OVSF composto de N seqüências de comprimento N é obtido das linhas da matriz C_N:

$$C_N = \begin{bmatrix} \mathbf{c}_N^{(1)} \\ \mathbf{c}_N^{(2)} \\ \mathbf{c}_N^{(3)} \\ \mathbf{c}_N^{(4)} \\ \vdots \\ \mathbf{c}_N^{(1)} \end{bmatrix} = \begin{bmatrix} \mathbf{c}_{N/2}^{(1)} \mathbf{c}_{N/2}^{(1)} \\ \mathbf{c}_{N/2}^{(1)} \left[-\mathbf{c}_{N/2}^{(1)} \right] \\ \mathbf{c}_{N/2}^{(2)} \mathbf{c}_{N/2}^{(2)} \\ \mathbf{c}_{N/2}^{(2)} \left[-\mathbf{c}_{N/2}^{(2)} \right] \\ \vdots \\ \mathbf{c}_{N/2}^{(N/2)} \mathbf{c}_{N/2}^{(N/2)} \\ \mathbf{c}_{N/2}^{(N/2)} \left[-\mathbf{c}_{N/2}^{(N/2)} \right] \end{bmatrix} \tag{3.24}$$

onde $\mathbf{c}_1^{(1)} = \{1\}$.

Observa-se que um conjunto OVSF de comprimento N é composto pelas mesmas seqüências do conjunto Walsh-Hadamard de comprimento N, ou seja, as linhas de (3.24) são encontradas em ordem diferente em (2.157), para $N = 2^n$.

Uma família OVSF é composta de seqüências selecionadas do conjunto OVSF de forma a se obter a função de correlação periódica par:

$$\theta(\mathbf{c}_{N^q}^{(k)}, \mathbf{c}_{N/s}^{(u)}, 0) = \begin{cases} 0, & \text{para } k \neq u \text{ e } s \geq 1 \\ N, & \text{para } k = u \text{ e } s = 1 \end{cases} \tag{3.25}$$

onde $q = 0, 1, ..., s-1$ e $\mathbf{c}_N^{(k)} = \{c_{N^0}^{(k)} c_{N^1}^{(k)} ... \mathbf{c}_{N^q}^{(k)} ... c_{N^{s-1}}^{(k)}\}$.

Para (3.25) ocorrer, a seqüência $\mathbf{c}_{N/s}^{(u)}$ não pode ser "seqüência-mãe" da seqüência $\mathbf{c}_N^{(k)}$, ou seja, $\mathbf{c}_N^{(k)}$ não pode ter sido construída a partir de $\mathbf{c}_{N/s}^{(u)}$. A figura 3.8 ilustra a construção de seqüências OVSF. Observa-se na figura que $\mathbf{c}_1^{(1)}$ é "seqüência-mãe" de todas as outras e $\mathbf{c}_2^{(1)}$ é "seqüência mãe" de $\mathbf{c}_4^{(1)}$, $\mathbf{c}_4^{(2)}$, $\mathbf{c}_8^{(1)}$, $\mathbf{c}_8^{(2)}$, $\mathbf{c}_8^{(3)}$ e $\mathbf{c}_8^{(4)}$.

Assim como as seqüências Walsh-Hadamard, a função de correlação periódica par para seqüências OVSF $\theta(\mathbf{c}_{N^q}^{(k)}, \mathbf{c}_{N/s}^{(u)}, d)$ para $d \neq 0$ pode assumir valores elevados. O motivo é o mesmo para seqüências Walsh-Hadamard: o conjunto possui seqüências ciclicamente equivalentes e seqüências com período menor que $N = 2^n$. Observe na figura 3.8 que $\mathbf{c}_4^{(4)}$ é uma versão deslocada de $\mathbf{c}_4^{(2)}$ e $\mathbf{c}_4^{(3)}$ tem período 2. Essa característica é devida ao método de construção, onde cada seqüência de comprimento N do conjunto é uma concatenação de seqüências de comprimento $N/2$.

O número de seqüências OVSF de uma família, ou seja, o número de seqüências que satisfaz (3.25) depende das taxas de dados exigidas pelo sistema ou, equivalentemente, depende dos comprimentos das seqüências que o sistema necessita.

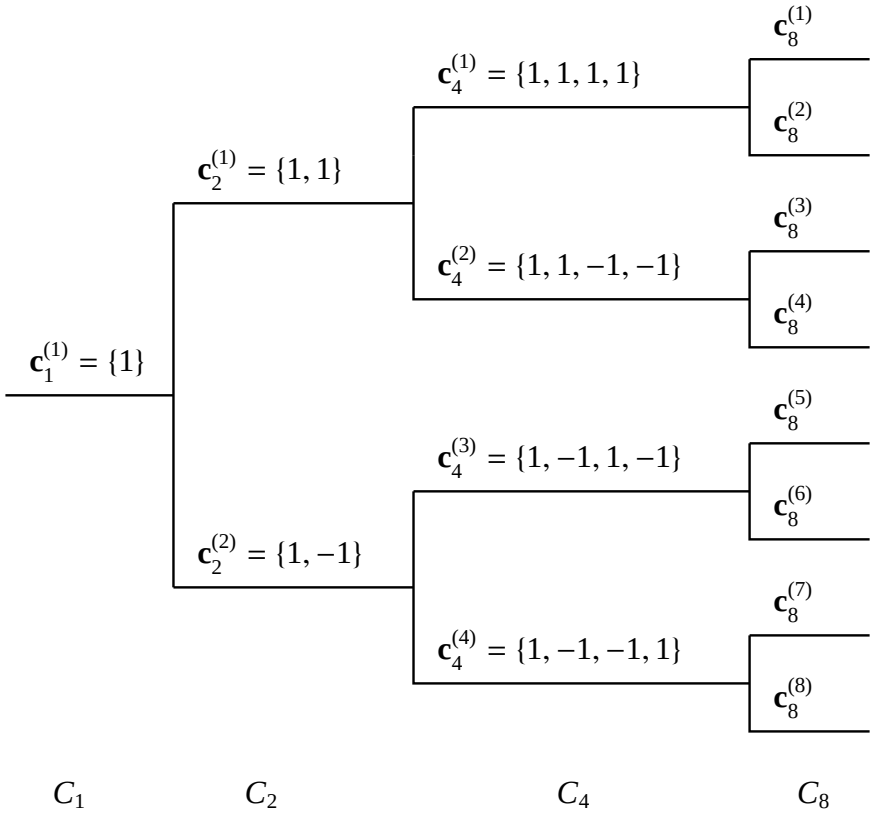

Figura 3.8: Construção de seqüências OVSF.

3.3.2 Modelagem do sistema QS-CDMA com esquema MPG

Considera-se um sistema multitaxa do tipo MPG que oferece n taxas de dados distintas. Cada taxa de dados R_i é oferecida por meio de um serviço i. Em cada serviço i existem U_i usuários ativos.

O sinal transmitido pelo k-ésimo usuário do serviço i, figura 3.9, é dado por:

$$s_{k,i}(t) = \sqrt{2P_i} b_{k,i}(t) c_{k,i}(t) cos(\omega_c t) \tag{3.26}$$

onde P_i é a potência dos sinais transmitidos pelos usuários do serviço i; $b_{k,i}(t)$ é o sinal de informação modulada em BPSK e $c_{k,i}(t)$ o sinal relativo à seqüência de espalhamento, dado por:

$$c_{k,i}(t) = \sum_{m=-\infty}^{\infty} p(t - mT_c) \underline{c}_{k,i,m} \tag{3.27}$$

onde $\underline{c}_{k,i,m} = c_{k,i,m(\text{mod } N_i)} \in \{-1; 1\}$ é o m-ésimo chip da seqüência de comprimento N_i

utilizada pelo *k*-ésimo usuário do serviço *i*; T_c é o período de chip; $p(t)$ é a formatação de pulso retangular de amplitude unitária no intervalo $[0; T_c)$ e zero fora.

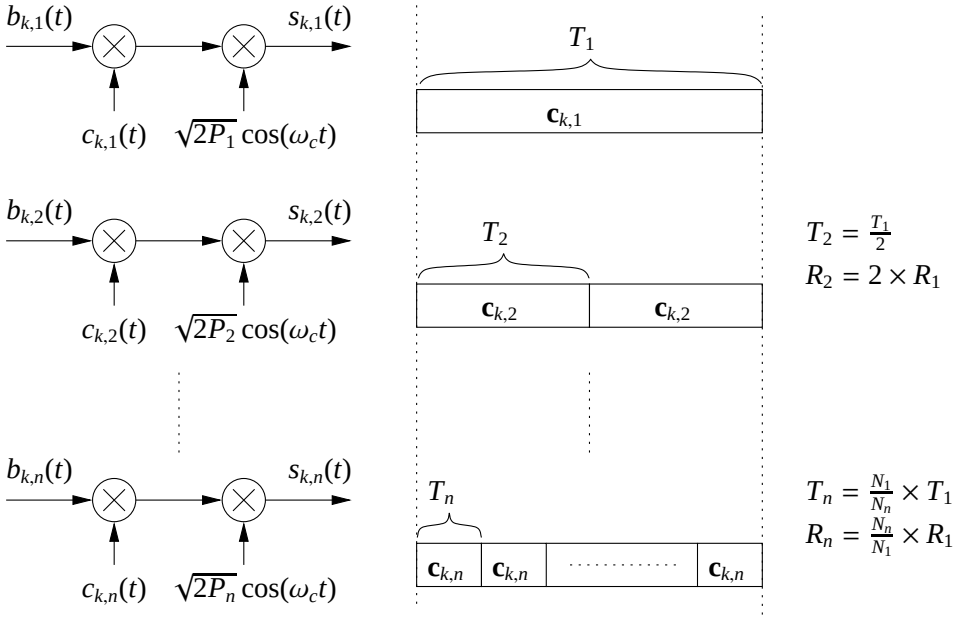

Figura 3.9: Transmissor com esquema MPG.

O sinal recebido na estação rádio base será:

$$r(t) = \sum_{j=1}^{n} \sum_{u=1}^{U_j} \sum_{\mathcal{L}=1}^{L} \alpha_{\mathcal{L}}(t) s_{u,j}(t - \tau_{u,j,\mathcal{L}}) + n(t) \tag{3.28}$$

onde $\alpha_{\mathcal{L}}(t)$ representa o ganho do canal para o componente multipercurso $\mathcal{L}$; $\tau_{u,j,\mathcal{L}}$ o atraso absoluto do $\mathcal{L}$-ésimo componente multipercurso do *u*-ésimo usuário do serviço *j* e $n(t)$ o AWGN.

A saída do ℓ-ésimo correlacionador do *k*-ésimo usuário do serviço *i*, analisada apenas em um período de símbolo de informação T_i (sem perda de generalidade considera-se o intervalo $0 \leq t < T_i$, onde $T_i = N_i T_c$) será:

$$\begin{aligned} z_{k,i,\ell} &= \int_0^{T_i} r(t) c^*(t) cos(\omega_c t - \phi_{k,i,\ell}) dt \\ &= \sqrt{2P_i} \int_0^{T_i} \alpha_\ell(t) b_{k,i}(t) c_{k,i}(t) c^*_{k,i}(t) cos^2(\omega_c t - \phi_{k,i,\ell}) dt + I_{k,i,\ell} + S I_{k,i,\ell} + n_{k,i,\ell}(t) \end{aligned} \tag{3.29}$$

onde o primeiro termo representa o sinal de interesse, o segundo a MAI, o terceiro a SI e o último o AWGN processado; $\phi_{k,i,\ell} = \omega_c \tau_{k,i,\ell}$ é o deslocamento de fase devido ao atraso $\tau_{k,i,\ell}$. Será considerado o ganho de canal $\alpha_{\mathcal{L}}(t)$ constante no intervalo de integração T_i (ou periodo do símbolo de informação). Assim, $\alpha_{\mathcal{L}}(t) = \alpha_{\mathcal{L}}$. Rearranjando a equação anterior, tem-se:

$$z_{k,i,\ell} = \sqrt{\frac{P_i}{2}} \alpha_\ell T_i b_{k,i}^{(0)} + I_{k,i,\ell} + S\,I_{k,i,\ell} + n_{k,i,\ell}(t) \tag{3.30}$$

onde $b_{k,i}^{(0)} \in \{-1; 1\}$ é a informação de interesse.

Considerando recepção Rake com D correlacionadores (*fingers*) e combinador de razão máxima (*maximum ratio combiner*, MRC), tem-se na saída do combinador:

$$\begin{aligned} y_{k,i} &= \sum_{\ell=1}^{D} \Re\{z_{k,i,\ell} \hat{\alpha}_\ell\} \\ \hat{b}_{k,i}^{(0)} &= \text{sign}(y_{k,i}) \end{aligned} \tag{3.31}$$

onde $\hat{\alpha}_\ell$ é a estimativa do ganho de canal, a qual foi considerada perfeita, e $\hat{b}_{k,i}^{(0)}$ é a informação de interesse estimada.

A MAI sobre o ℓ-ésimo correlacionador do k-ésimo usuário do serviço i será:

$$\begin{aligned} I_{k,i,\ell} &= \sum_{j=1}^{n} \sum_{(u=1,\ u\neq k \ para \ j=i)}^{U_j} \sum_{\mathcal{L}=1}^{L} \sqrt{2P_j} \cdot \\ &\cdot \int_0^{T_i} \alpha_{\mathcal{L}}(t) b_{u,j}(t - \tau_{u,j,\mathcal{L}}) c_{u,j}(t - \tau_{u,j,\mathcal{L}}) c_{k,i}^*(t) cos(\omega_c t - \phi_{u,j,\mathcal{L}}) cos(\omega_c t - \phi_{k,i,\ell}) dt \\ &= \sum_{j=1}^{n} \sum_{(u=1,\ u\neq k \ para \ j=i)}^{U_j} \sum_{\mathcal{L}=1}^{L} \sqrt{2P_j} \alpha_{\mathcal{L}} \cdot \\ &\cdot \int_0^{T_i} b_{u,j}(t - \tau_{u,j,\mathcal{L}}) c_{u,j}(t - \tau_{u,j,\mathcal{L}}) c_{k,i}^*(t) \frac{1}{2} \left(cos(\varphi_{u,j,\mathcal{L}}) + cos(2\omega_c t - (\phi_{u,j,\mathcal{L}} - \phi_{k,i,\ell})) \right) dt \\ &= \sum_{j=1}^{n} \sum_{(u=1,\ u\neq k \ para \ j=i)}^{U_j} \sum_{\mathcal{L}=1}^{L} \sqrt{\frac{P_j}{2}} \alpha_{\mathcal{L}} \int_0^{T_i} b_{u,j}(t - \tau_{u,j,\mathcal{L}}) c_{u,j}(t - \tau_{u,j,\mathcal{L}}) c_{k,i}^*(t) dt \; cos(\varphi_{u,j,\mathcal{L}}) \end{aligned} \tag{3.32}$$

onde $\tau_{u,j,\mathcal{L}} = \tau_{u,j,\mathcal{L}} - \tau_{k,i,\ell}$ é o atraso relativo entre o sinal de interesse (sinal do ℓ-ésimo componente multipercurso do k-ésimo usuário do serviço i) e o sinal interferente

(sinal do $\mathcal{L}$-ésimo componente multipercurso do u-ésimo usuário do serviço j); $\varphi_{u,j,\mathcal{L}} = \phi_{u,j,\mathcal{L}} - \phi_{k,i,\ell}$ é a fase relativa das portadoras do sinal de interesse e do sinal interferente. Os termos que correspondem ao atraso relativo e à fase relativa não possuem os índices do sinal de interesse para simplificar a notação.

Será considerada a fase relativa $\varphi_{u,j,\mathcal{L}}$ com *pdf* uniforme definida no intervalo $[0; 2\pi)$ e o atraso relativo $\tau_{u,j,\mathcal{L}}$ com *pdf* uniforme definida no intervalo $[-\tau_{\max} + \gamma_{\mathcal{L}}; \tau_{\max} + \gamma_{\mathcal{L}}]$, onde $\gamma_{\mathcal{L}} = \Delta_{\mathcal{L}} - \Delta_{\ell}$. As variáveis Δ_{ℓ} assumem apenas valores positivos e múltiplos de T_c e representam os atrasos dos componentes multipercurso dado um perfil atraso-potência determinístico. Observe que $\gamma_{\mathcal{L}}$ também não possui o índice do componente multipercurso de interesse para simplificar a notação. Considera-se também, os símbolos de informação $b = -1$ e $b = 1$ equiprováveis.

Analogamente à MAI, a SI sobre o ℓ-ésimo correlacionador do k-ésimo usuário do serviço i será:

$$SI_{k,i,\ell} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \sqrt{\frac{P_i}{2}}\alpha_{\mathcal{L}} \int_0^{T_i} b_{k,i}(t - \tau_{k,i,\mathcal{L}})c_{k,i}(t - \tau_{k,i,\mathcal{L}})c^*_{k,i}(t)dt\ cos(\varphi_{k,i,\mathcal{L}}) \qquad (3.33)$$

O AWGN processado para o ℓ-ésimo correlacionador do k-ésimo usuário do serviço i é dado por:

$$\begin{aligned} n_{k,i,\ell}(t) &= \int_0^{T_i} n(t)c^*_{k,i}(t)cos(\omega_c t)dt \\ &= \sum_{m=0}^{N_i-1} \underline{c}^*_{k,m} \int_{mT_c}^{(m+1)T_c} n(t)cos(\omega_c t)dt \end{aligned} \qquad (3.34)$$

Será calculada a relação sinal-ruído-interferência (SNIR) na saída do ℓ-ésimo correlacionador do k-ésimo usuário do serviço i:

$$SNIR_{k,i,\ell} = \frac{\text{potência do sinal de interesse}}{\text{potência da MAI, da SI e do AWGN processado}} \qquad (3.35)$$

onde a potência do sinal de interesse será:

$$\mathbb{E}_{\alpha}\left\{\left(\sqrt{\frac{P_i}{2}}\alpha_{\ell}T_i b_{k,i}^{(0)}\right)^2\right\} = \frac{P_i}{2}T_i^2\mathbb{E}_{\alpha}\{\alpha_{\ell}^2\} \tag{3.36}$$

A potência do AWGN processado será:

$$\begin{aligned}
\mathbb{E}\left\{(n_{k,i,\ell}(t))^2\right\} &= \mathbb{E}\left\{\left(\sum_{m=0}^{N_i-1}\underline{c}_{k,m}^{*}\int_{mT_c}^{(m+1)T_c} n(t)cos(\omega_c t)dt\right)^2\right\} \\
&= \mathbb{E}\left\{\sum_{m=0}^{N_i-1}\left(|\underline{c}_{k,m}|^2\int_{mT_c}^{(m+1)T_c}\int_{mT_c}^{(m+1)T_c} n(t)n(u)cos(\omega_c t)cos(\omega_c u)\,dt\,du + \right.\right. \\
&\quad \left.\left. + \sum_{p=0}^{N_i-1}\underline{c}_{k,m}^{*}\underline{c}_{k,p}^{*}\int_{mT_c}^{(m+1)T_c}\int_{pT_c}^{(p+1)T_c} n(t)n(u)cos(\omega_c t)cos(\omega_c u)\,dt\,du\right)\right\} \\
&= \sum_{m=0}^{N_i-1}\left(\int_{mT_c}^{(m+1)T_c}\int_{mT_c}^{(m+1)T_c}\frac{N_0}{2}\delta(t-u)cos(\omega_c t)cos(\omega_c u)\,dt\,du\right) \\
&= \sum_{m=0}^{N_i-1}\frac{N_0\,T_c}{4} \\
&= \frac{N_0\,T_i}{4}
\end{aligned} \tag{3.37}$$

Como φ, b, τ e α são variáveis aleatórias independentes, a potência da MAI e da SI sobre o ℓ-ésimo correlacionador do k-ésimo usuário do serviço i serão:

$$\begin{aligned}
\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,i,\ell})^2\right\} &= \mathbb{E}_{\alpha}\left\{\mathbb{E}_{\tau}\left\{\mathbb{E}_{b}\left\{\mathbb{E}_{\varphi}\left\{(I_{k,i,\ell})^2\right\}\right\}\right\}\right\} \\
\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(S\,I_{k,i,\ell})^2\right\} &= \mathbb{E}_{\alpha}\left\{\mathbb{E}_{\tau}\left\{\mathbb{E}_{b}\left\{\mathbb{E}_{\varphi}\left\{(S\,I_{k,i,\ell})^2\right\}\right\}\right\}\right\}
\end{aligned} \tag{3.38}$$

A potência da MAI será:

$$\mathbb{E}_{\varphi}\left\{(I_{k,i,\ell})^2\right\} = \mathbb{E}_{\varphi}\left\{\left(\sum_{j=1}^{n}\sum_{(u=1,\ u\neq k\ para\ \ j=i)}^{U_j}\sum_{\mathcal{L}=1}^{L}\sqrt{\frac{P_j}{2}}\alpha_{\mathcal{L}}(t)J_{u,j,\mathcal{L}}\,cos(\varphi_{u,j,\mathcal{L}})\right)^2\right\} \tag{3.39}$$

onde $J_{u,j,\mathcal{L}} = \int_0^{T_i} b_{u,j}(t-\tau_{u,j,\mathcal{L}})c_{u,j}(t-\tau_{u,j,\mathcal{L}})c_{k,i}^{*}(t)dt$. Realizando a média na variável $\varphi_{u,j,\mathcal{L}}$, tem-se:

$$\begin{aligned}\mathbb{E}_{\varphi}\left\{(I_{k,i,\ell})^2\right\} &= \sum_{j=1}^{n}\sum_{(u=1,\ u\neq k\ para\ j=i)}^{U_j}\sum_{\mathcal{L}=1}^{L}\frac{P_j}{2}\alpha_{\mathcal{L}}^2(t)J_{u,j,\mathcal{L}}^2\int_0^{2\pi}cos^2(\varphi_{u,j,\mathcal{L}})\frac{1}{2\pi}\,d\varphi_{u,j,\mathcal{L}} \\ &= \sum_{j=1}^{n}\sum_{(u=1,\ u\neq k\ para\ j=i)}^{U_j}\sum_{\mathcal{L}=1}^{L}\frac{P_j}{4}\alpha_{\mathcal{L}}^2(t)J_{u,j,\mathcal{L}}^2 \qquad (3.40)\end{aligned}$$

Realizando a média na variável $b_{u,j}$, tem-se:

$$\mathbb{E}_b\left\{\mathbb{E}_{\varphi}\left\{(I_{k,i,\ell})^2\right\}\right\} = \sum_{j=1}^{n}\sum_{(u=1,\ u\neq k\ para\ j=i)}^{U_j}\sum_{\mathcal{L}=1}^{L}\frac{P_j}{4}\alpha_{\mathcal{L}}^2(t)\mathbb{E}_b\left\{J_{u,j,\mathcal{L}}^2\right\} \qquad (3.41)$$

Para os próximos passos do desenvolvimento, devem-se considerar 3 casos:

1. $T_i > T_j$: o período do símbolo de informação do usuário de interesse do serviço i, T_i, é maior que o período de informação dos usuários interferentes do serviço j, T_j (de outra forma, a taxa dos usuários interferentes é maior que a taxa do usuário de interesse);

2. $T_i < T_j$: caso contrário do anterior. O período de símbolo de informação do usuário de interesse do serviço i, T_i, é menor que o período de informação dos usuários interferentes do serviço j, T_j (de outra forma, a taxa dos usuários interferentes é menor que a taxa do usuário de interesse);

3. $T_i = T_j$: os usuários interferentes estão utilizando o mesmo serviço do usuário de interesse, assim $i = j$ e $T_i = T_j$.

Considerando $T_i > T_j$, primeiro caso, calcula-se $\mathbb{E}_b\left\{J_{u,j,\mathcal{L}}^2\right\}$:

$$\mathbb{E}_b\left\{J_{u,j,\mathcal{L}}^2\right\} = \mathbb{E}_b\left\{\left(\sum_{q=0}^{M-1}\int_{q\frac{T_j}{M}}^{(q+1)\frac{T_j}{M}} b_{u,j}(t-\tau_{u,j,\mathcal{L}})c_{u,j}(t-\tau_{u,j,\mathcal{L}})c_{k,i}^*(t)\,dt\right)^2\right\} \qquad (3.42)$$

onde $M = \frac{T_i}{T_j}$. Reescrevendo $J_{u,j,\mathcal{L}}$:

$$J_{u,j,\mathcal{L}} = \sum_{q=0}^{M-1}\int_{q\frac{T_j}{M}}^{(q+1)\frac{T_j}{M}} b_{u,j}(t-\tau_{u,j,\mathcal{L}})c_{u,j}(t-\tau_{u,j,\mathcal{L}})c_{k,i}^*(t)dt$$

$$= \sum_{q=0}^{M-1} \begin{cases} \left(b_{u,j}^{(-1)} \mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}}) + b_{u,j}^{(0)} \tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right), & \tau_{u,j,\mathcal{L}} \geq 0 \\ \left(b_{u,j}^{(0)} \mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}}) + b_{u,j}^{(1)} \tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right), & \tau_{u,j,\mathcal{L}} < 0 \end{cases} \quad (3.43)$$

onde $b_{u,j}^{(-1)}$, $b_{u,j}^{(0)}$ e $b_{u,j}^{(1)}$ são as informações do usuário interferente que participam da integração e as funções $\mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})$ e $\tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})$ são definidas como[1]:

$$\begin{aligned} \mathcal{R}_{u,k^{(q)}}(\tau) &= \int_{q\frac{T_j}{M}}^{q\frac{T_j}{M}+\underline{\tau}} c_{u,j}(t-\underline{\tau}) c^*_{k^{(q)},i}(t)\, dt \\ \tilde{\mathcal{R}}_{u,k^{(q)}}(\tau) &= \int_{q\frac{T_j}{M}+\underline{\tau}}^{(q+1)\frac{T_j}{M}} c_{u,j}(t-\underline{\tau}) c^*_{k^{(q)},i}(t)\, dt, \\ &\quad \text{com } \underline{\tau} = \tau \text{ para } \tau \geq 0 \text{ e } \underline{\tau} = T + \tau \text{ para } \tau < 0 \end{aligned} \quad (3.44)$$

onde $c_{k^{(q)},i}(t)$ é o sinal relativo ao trecho $\mathbf{c}_{k^{(q)}} = \left\{c_{k,q\frac{N_i}{M}}\ c_{k,q\frac{N_i}{M}+1}\ \ldots\ c_{k,(q+1)\frac{N_i}{M}-1}\right\}$ da seqüência de espalhamento $\mathbf{c}_k$ utilizada pelo usuário k do serviço i definida da seguinte forma:

$$\mathbf{c}_k = \{\mathbf{c}_{k^{(0)}}\ \mathbf{c}_{k^{(1)}}\ \ldots\ \mathbf{c}_{k^{(q)}}\ \ldots\ \mathbf{c}_{k^{(M-1)}}\} \quad (3.45)$$

Assim, tem-se:

$$\begin{aligned} \mathbb{E}_b\left\{J_{u,j,\mathcal{L}}^2\right\} &= \mathbb{E}_b\left\{\left(\sum_{q=0}^{M-1} b_{u,j}^{(-1)} \mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}}) + b_{u,j}^{(0)} \tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2\right\}, \tau_{u,j,\mathcal{L}} \geq 0 \\ &= \sum_{q=0}^{M-1} \begin{cases} \mathbb{E}_b\left\{\left(b_{u,j}^{(-1)} \mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}}) + b_{u,j}^{(0)} \tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2\right\}, & \tau_{u,j,\mathcal{L}} \geq 0 \\ \mathbb{E}_b\left\{\left(b_{u,j}^{(0)} \mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}}) + b_{u,j}^{(1)} \tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2\right\}, & \tau_{u,j,\mathcal{L}} < 0 \end{cases} \\ &= \sum_{q=0}^{M-1} \frac{1}{2}\left\{\left(\mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}}) + \tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2 + \right. \\ &+ \left.\left(\mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}}) - \tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2\right\} \\ &= \sum_{q=0}^{M-1} \left\{\left(\mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2 + \left(\tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2\right\} \end{aligned} \quad (3.46)$$

O próximo passo é realizar a média na variável $\tau_{u,j,\mathcal{L}}$:

[1]Observa-se que, para $\tau < 0$, $\mathcal{R}_{u,k^{(q)}}(\tau)$ e $\tilde{\mathcal{R}}_{u,k^{(q)}}(\tau)$ são equivalentes a $\mathcal{R}_{u,k^{(q)}}(T+\tau)$ e $\tilde{\mathcal{R}}_{u,k^{(q)}}(T+\tau)$, respectivamente.

$$\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{\mathbb{E}_\varphi\left\{(I_{k,i,\ell})^2\right\}\right\}\right\} = \sum_{j=1}^{n} \sum_{(u=1,\ u\neq k \ para \ \ j=i)}^{U_j} \sum_{\mathcal{L}=1}^{L} \frac{P_j}{4}\alpha_{\mathcal{L}}^2 \mathbb{E}_\tau\left\{\mathbb{E}_b\left\{J_{u,j,\mathcal{L}}^2\right\}\right\} \tag{3.47}$$

onde:

$$\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{J_{u,j,\mathcal{L}}^2\right\}\right\} = \sum_{q=0}^{M-1} \frac{1}{2\tau_{\max}} \int_{-\tau_{\max}+\gamma_{\mathcal{L}}}^{\tau_{\max}+\gamma_{\mathcal{L}}} \left[\left(\mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2 + \left(\tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2\right] d\tau_{u,j,\mathcal{L}} \tag{3.48}$$

Fazendo $-\tau_{\max}+\gamma_{\mathcal{L}}$ e $\tau_{\max}+\gamma_{\mathcal{L}}$ múltiplos de T_c, tem-se $\frac{-\tau_{\max}+\gamma_{\mathcal{L}}}{T_c} = \upsilon_1$ e $\frac{\tau_{\max}+\gamma_{\mathcal{L}}}{T_c} = \upsilon_2$ números inteiros. Como os sinais $c_{u,j}(t)$ são periódicos com período $N_j T_c$, tem-se (1.25).

Assim, pode-se reescrever (3.48) como:

$$\begin{aligned}\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{J_{u,j,\mathcal{L}}^2\right\}\right\} = & \sum_{q=0}^{M-1} \frac{1}{2\tau_{\max}} \sum_{m=\upsilon_1}^{\upsilon_2-1} \cdot \\ & \cdot \int_{(m \bmod N)T_c}^{((m \bmod N)+1)\ T_c} \left[\left(\mathcal{R}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2 + \left(\tilde{\mathcal{R}}_{u,k^{(q)}}(\tau_{u,j,\mathcal{L}})\right)^2\right] d\tau_{u,j,\mathcal{L}}\end{aligned} \tag{3.49}$$

com N igual ao comprimento das seqüências $\mathbf{c}_{k^{(q)}}$ e $\mathbf{c}_u$.

O desenvolvimento da integral da expressão acima é apresentado no anexo A.1. Com esse resultado, tem-se:

$$\mathbb{E}_\tau\left\{\mathbb{E}_b\left\{J_{u,j,\mathcal{L}}^2\right\}\right\} = \sum_{q=0}^{M-1} \frac{1}{2\tau_{\max}} \sum_{m=\upsilon_1}^{\upsilon_2-1} \rho_{u,k^{(q)}}(m \bmod N) \tag{3.50}$$

onde:

$$\begin{aligned}\rho_{u,k^{(q)}}(m) = & \frac{T_c^3}{3}\left(C_{u,k^{(q)}}(m-N+1)C_{u,k^{(q)}}(m-N) + C_{u,k^{(q)}}(m+1)C_{u,k^{(q)}}(m) + \right. \\ & + \left. C_{u,k^{(q)}}^2(m-N) + C_{u,k^{(q)}}^2(m) + C_{u,k^{(q)}}^2(m-N+1) + C_{u,k^{(q)}}^2(m+1)\right)\end{aligned} \tag{3.51}$$

e

$$C_{u,k^{(q)}}(d) = \begin{cases} \sum_{v=0}^{N-d-1} c_{u,v} c^*_{k^{(q)},v+d} & 0 \leq d \leq N-1 \\ \sum_{v=0}^{N+d-1} c_{u,v-d} c^*_{k^{(q)},v} & 1-N \leq d < 0 \\ 0 & |d| \geq N \end{cases} \tag{3.52}$$

Finalmente, realiza-se a média na variável $\alpha_{\mathcal{L}}$:

$$\begin{aligned} \mathbb{E}_{\alpha}\left\{\mathbb{E}_{\tau}\left\{\mathbb{E}_{b}\left\{\mathbb{E}_{\varphi}\left\{(I_{k,i,\ell})^2\right\}\right\}\right\}\right\} &= \sum_{j=1}^{n} \sum_{(u=1,\ u\neq k \ para \ j=i)}^{U_j} \sum_{\mathcal{L}=1}^{L} \frac{P_j}{8\tau_{max}} \mathbb{E}_{\alpha}\{\alpha^2_{\mathcal{L}}\} \sum_{q=0}^{M-1} \cdot \\ &\quad \cdot \sum_{m=\upsilon_1}^{\upsilon_2-1} \rho_{u,k^{(q)}}(m \bmod N) \end{aligned} \tag{3.53}$$

Portanto, a potência da MAI sobre o ℓ-ésimo correlacionador do k-ésimo usuário do serviço i para $T_i > T_j$ será:

$$\mathbb{E}_{\alpha,\varphi,b,\tau}\left\{(I_{k,i,\ell})^2\right\} = \sum_{j=1}^{n} \sum_{(u=1,\ u\neq k \ para \ j=i)}^{U_j} \sum_{\mathcal{L}=1}^{L} \frac{P_j}{8\tau_{max}} \mathbb{E}_{\alpha}\{\alpha^2_{\mathcal{L}}(t)\} \sum_{q=0}^{M-1} \sum_{m=\upsilon_1}^{\upsilon_2-1} \rho_{u,k^{(q)}}(m \bmod N) \tag{3.54}$$

Seja agora considerado o segundo caso, $T_i < T_j$. O valor médio quadrático da interferência causada por um usuário de baixa taxa sobre o de alta taxa é igual ao o valor médio quadrático da interferência causada pelo usuário de alta taxa sobre o de baixa taxa, dividido pela relação entre as potências e pelo número de símbolos de informação do usuário de alta taxa compreendidos no período de símbolo do usuário de baixa taxa. Considerando um sistema com apenas 2 usuários ativos, um usuário k utilizando o serviço i e o outro usuário u utilizando o serviço j, sendo que $T_i < T_j$, adicionalmente apenas um multipercurso ℓ, tem-se:

$$\begin{aligned} \mathbb{E}_{\alpha,\varphi,b,\tau}\left\{(I_{k,i,\ell})^2\right\} &= \mathbb{E}_{\alpha,\varphi,b,\tau}\left\{\left(I_{u,j,\ell}\right)^2\right\} \cdot \frac{1}{P_i/P_j} \cdot M \\ &= \frac{P_i}{8\tau_{max}} \mathbb{E}_{\alpha}\{\alpha^2_{\mathcal{L}}\} \sum_{q=0}^{1/M-1} \sum_{m=\upsilon_1}^{\upsilon_2-1} \rho_{u^{(q)},k}(m \bmod N) \cdot \frac{1}{P_i/P_j} \cdot M \end{aligned}$$

$$= \frac{P_j M}{8\tau_{max}} \mathbb{E}_\alpha\{\alpha_{\mathcal{L}}^2\} \sum_{q=0}^{1/M-1} \sum_{m=\upsilon_1}^{\upsilon_2-1} \rho_{u^{(q)},k}(m \bmod N) \tag{3.55}$$

com $M = \frac{T_i}{T_j}$ e N igual ao comprimento das seqüências $\mathbf{c}_{u^{(q)}}$ e $\mathbf{c}_k$.

Genericamente, em um sistema com vários usuários e vários multipercursos, a potência da MAI sobre o ℓ-ésimo correlacionador do k-ésimo usuário do serviço i para o segundo caso, $T_i < T_j$, será:

$$\mathbb{E}_{\alpha,\varphi,b,\tau}\left\{(I_{k,i,\ell})^2\right\} = \sum_{j=1}^{n} \sum_{(u=1,\ u\neq k \ para \ j=i)}^{U_j} \sum_{\mathcal{L}}^{L} \frac{P_j M}{8\tau_{max}} \mathbb{E}_\alpha\{\alpha_{\mathcal{L}}^2\} \sum_{q=0}^{1/M-1} \sum_{m=\upsilon_1}^{\upsilon_2-1} \rho_{u^{(q)},k}(m \bmod N) \tag{3.56}$$

Finalmente, para o último caso, $T_i = T_j$, ou seja, $i = j$:

$$\mathbb{E}_{\alpha,\varphi,b,\tau}\left\{(I_{k,i,\ell})^2\right\} = \sum_{u=1,\ u\neq k}^{U_j} \sum_{\mathcal{L}}^{L} \frac{P_j}{8\tau_{max}} \mathbb{E}_\alpha\{\alpha_{\mathcal{L}}^2\} \sum_{m=\upsilon_1}^{\upsilon_2-1} \rho_{u,k}(m \bmod N) \tag{3.57}$$

A potência da SI sobre o ℓ-ésimo correlacionador do k-ésimo usuário do serviço i é semelhante à potência da MAI do último caso considerado, pois o período do símbolo do usuário de interesse é igual ao período de símbolo de seus multipercursos (interferentes). Será calculada a potência da SI como em (3.38). Inicialmente, calcula-se $\mathbb{E}_\varphi\left\{(SI_{k,i,\ell})^2\right\}$, onde $SI_{k,i,\ell}$ é dado por (3.33):

$$\mathbb{E}_\varphi\left\{(SI_{k,i,\ell})^2\right\} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \frac{P_i}{4} \alpha_{\mathcal{L}}^2 J_{k,i,\mathcal{L}}^2 \tag{3.58}$$

onde $J_{k,i,\mathcal{L}}$ é dado por:

$$\begin{aligned} J_{k,i,\mathcal{L}} &= \int_0^{T_i} b_{k,i}(t-\tau_{k,i,\mathcal{L}}) c_{k,i}(t-\tau_{k,i,\mathcal{L}}) c_{k,i}(t)^* dt \\ &= b_{k,i}^{(-1)} \mathcal{R}_{k,k}(\tau_{k,i,\mathcal{L}}) + b_{k,i}^{(0)} \tilde{\mathcal{R}}_{k,k}(\tau_{k,i,\mathcal{L}}) \end{aligned} \tag{3.59}$$

onde:

$$\mathcal{R}_{k,k}(\tau) = \int_0^{\tau} c_{k,i}(t-\tau) c_{k,i}^*(t)\, dt$$

$$\tilde{\mathcal{R}}_{k,k}(\tau) = \int_{\tau}^{T_i} c_{k,i}(t-\tau)c_{k,i}^{*}(t)\,dt \tag{3.60}$$

Realizando a média para o símbolo de informação $b_{k,i}$:

$$\mathbb{E}_b\left\{\mathbb{E}_\varphi\left\{(SI_{k,i,\ell})^2\right\}\right\} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \frac{P_i}{4}\alpha_{\mathcal{L}}^2(t)\mathbb{E}_b\left\{J_{k,i,\mathcal{L}}^2\right\} \tag{3.61}$$

onde $\mathbb{E}_b\left\{J_{k,i,\mathcal{L}}^2\right\}$ é dado por:

$$\mathbb{E}_b\left\{J_{k,i,\mathcal{L}}^2\right\} = \left(\mathcal{R}_{k,k}(\tau_{k,i,\mathcal{L}})\right)^2 + \left(\tilde{\mathcal{R}}_{k,k}(\tau_{k,i,\mathcal{L}})\right)^2 \tag{3.62}$$

O perfil atraso-potência considerado é determinístico e, portanto, $\tau_{k,i,\mathcal{L}} = \tau_{k,i,\ell} - \tau_{k,i,\mathcal{L}} = \Delta_\ell - \Delta_{\mathcal{L}}$ é uma constante e não uma variável aleatória. Adicionalmente, $\tau_{k,i,\mathcal{L}}$ assume apenas valores múltiplos de T_c, imposto pelo perfil atraso-potência do canal. Assim, do apêndice A.2, pode-se reescrever:

$$\begin{aligned}\mathcal{R}_{k,k}(\tau_{k,i,\mathcal{L}}) &= T_c C_{k,k}\left(\frac{\tau_{k,i,\mathcal{L}}}{T_c} - N\right)\\ \tilde{\mathcal{R}}_{k,k}(\tau_{k,i,\mathcal{L}}) &= T_c C_{k,k}\left(\frac{\tau_{k,i,\mathcal{L}}}{T_c}\right)\end{aligned} \tag{3.63}$$

com N igual ao comprimento da seqüência $\mathbf{c}_k$.

Realizando a média na variável $\alpha_{\mathcal{L}}$:

$$\mathbb{E}_\alpha\left\{\mathbb{E}_b\left\{\mathbb{E}_\varphi\left\{(SI_{k,i,\ell})^2\right\}\right\}\right\} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \frac{P_i}{4}\mathbb{E}_\alpha\left\{\alpha_{\mathcal{L}}^2\right\}\left(\left(T_c C_{k,k}\left(\frac{\tau_{k,i,\mathcal{L}}}{T_c} - N\right)\right)^2 + \left(T_c C_{k,k}\left(\frac{\tau_{k,i,\mathcal{L}}}{T_c}\right)\right)^2\right) \tag{3.64}$$

A potência da SI é, portanto, dada por:

$$\mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,i,\ell})^2\right\} = \sum_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{L} \frac{P_i}{4}\mathbb{E}_\alpha\left\{\alpha_{\mathcal{L}}^2(t)\right\}\left(\left(T_c C_{k,k}\left(\frac{\tau_{k,i,\mathcal{L}}}{T_c} - N\right)\right)^2 + \left(T_c C_{k,k}\left(\frac{\tau_{k,i,\mathcal{L}}}{T_c}\right)\right)^2\right) \tag{3.65}$$

Então, obtém-se a relação sinal-ruído-interferência (SNIR) na saída do ℓ-ésimo

correlacionador do *k*-ésimo usuário do serviço *i*:

$$SNIR_{k,i,\ell} = \frac{\frac{P_i}{2} T_i^2 \mathbb{E}_\alpha\{\alpha_\ell^2\}}{\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,i,\ell})^2\right\} + \mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,i,\ell})^2\right\} + \frac{N_0 T_i}{4}} \tag{3.66}$$

onde $\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,i,\ell})^2\right\}$ é dado pela equação (3.54) para $T_i > T_j$, pela equação (3.56) para $T_i < T_j$, pela equação (3.57) para $T_i = T_j$ e $\mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,i,\ell})^2\right\}$ é dado pela equação (3.65).

Considerando energias de símbolo $E_b = P_i \cdot T_i$ iguais para todos os usuários:

$$SNIR_{k,i,\ell} = \frac{E_b\, \mathbb{E}_\alpha\{\alpha_\ell^2\}}{\frac{2}{T_i}\left\{\mathbb{E}_{\varphi,b,\tau,\alpha}\left\{(I_{k,i,\ell})^2\right\} + \mathbb{E}_{\varphi,b,\alpha}\left\{(SI_{k,i,\ell})^2\right\}\right\} + \frac{N_0}{2}} \tag{3.67}$$

Conforme mencionado na seção anterior, para maximizar o desempenho do sistema para todos os usuário, deve-se maximizar a SNIR na saída de todos os correlacionadores, de todos os usuários e de todos os serviços. Na seção seguinte, será apresentado um parâmetro que deve ser minimizado a fim de maximizar a SNIR. A minimização desse parâmetro será o critério de seleção das seqüências de espalhamento utilizadas pelo sistema.

3.3.3 Critério para a seleção de seqüências

Um critério para a seleção de seqüências para sistemas QS-CDMA que utilizam o esquema MPG pode ser obtido da maximização do parâmetro SNIR na saída de todos os correlacionadores, de todos os usuários e de todos os serviços:

$$\max_{\mathbf{c}_k} \{SNIR_{k,i,\ell}\}, \quad \text{para todo } k, i \text{ e } \ell \tag{3.68}$$

onde $\mathbf{c}_k$ é a seqüência de espalhamento do *k*-ésimo usuário dado por (3.45) e $SNIR_{k,i,\ell}$ é dado pela equação (3.67).

Observe que a maximização da SNIR é um problema combinatório. O espaço, no qual a SNIR é definida, é composto por todas as combinações de todas as seqüências de comprimento N_i, onde *i* representa a classe de serviço oferecido. Esse espaço em problemas práticos pode ser muito grande. Por exemplo, considere um sistema CDMA com taxa de chip $R_c = 3,84 Mchips/s$, conforme a especificação W-CDMA (ZENG;

ANNAMALAI; BHARGAVA, 2000). Esse sistema fornece um serviço 1 de taxa de dados de $60kb/s$ para 4 usuários e um serviço 2 de taxa de dados de $120kb/s$ para 2 usuários. Isso resulta em seqüências de comprimento $N = 64$ para o serviço 1 e $N = 32$ para o serviço 2, admitindo-se códigos curtos como na modelagem da seção anterior. Existem 2^{64} seqüências para o serviço 1 e 2^{32} seqüências para o serviço 2. O número de combinações possíveis de todas essas seqüências para compor um conjunto e servir os 6 usuários será $\binom{2^{64}}{4} \times \binom{2^{32}}{2} \approx 10^{96}$. Para verificar qual das combinações resulta em um melhor desempenho, deve-se testar $\frac{\binom{2^{64}}{4} \times \binom{2^{32}}{2}}{64} \cong 4,45 \times 10^{94}$ conjuntos de seqüências. Esse espaço de aproximadamente $4,45 \times 10^{94}$ opções é muito grande para ser todo testado.

Uma solução para esse problema é obtida por meio da definição de uma função que deve ser minimizada para atingir o objetivo (maximizar o desempenho). Essa função é chamada de função objetivo. Para a minimização da função objetivo existem diversos métodos de minimização de funções propostos na literatura (PRESS et al., 1992).

Será definido um objetivo para a maximização da SNIR. Esse objetivo é dado pela relação sinal-ruído-interferência desejada, chamada de SNIR alvo (*signal-to-noise plus interference ratio target*, SNIRT), para a saída de cada correlacionador de cada usuário. É também desejável que as SNIR das saídas de todos os correlacionadores de um determinado usuário resultem em valores aproximadamente iguais, para melhor aproveitar a diversidade Rake (PROAKIS, 1995). Dessa forma, o critério de seleção de seqüências passa a ser:

$$\min_{\mathbf{c}_k} \left\{ \frac{SNIRT_{k,i}}{SNIR_{k,i,\ell}} \right\}, \quad \text{para todo } k, i \text{ e } \ell \tag{3.69}$$

onde $SNIRT_{k,i}$ é a chamada SNIR alvo (SNIRT) para a $SNIR_{k,i,\ell}$ (3.67), ou seja, é o valor que se deseja obter para a SNIR de todos os correlacionadores do k-ésimo usuário que utiliza o i-ésimo serviço.

De (3.69), verifica-se que a relação $\frac{SNIRT_{k,i}}{SNIR_{k,i,\ell}}$ deve ser menor ou igual a 1 para atender à SNIRT. Então, a minimização de (3.69) deve ser realizada de modo a resultar em $\frac{SNIRT_{k,i}}{SNIR_{k,i,\ell}} \leq 1$ para todo k, i e ℓ.

Para obter uma função objetivo, mapeia-se $\frac{SNIRT_{k,i}}{SNIR_{k,i,\ell}}$ em uma função côncava. Considere a função do tipo $f(x) = \left(\frac{x}{a}\right)^{\lambda}$, onde λ assume qualquer valor inteiro maior que zero e a é um número real. A figura 3.10 apresenta o esboço dessa função.

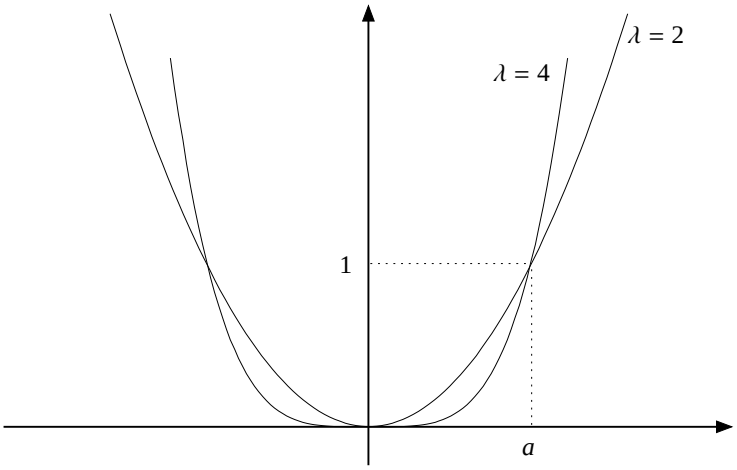

Figura 3.10: Esboço da função $f(x) = \left(\frac{x}{a}\right)^{\lambda}$.

O objetivo é garantir que $\frac{SNIRT_{k,i}}{SNIR_{k,i,\ell}} \leq 1$, então, adota-se $a = 1$ e, agora, deve-se garantir $f(\frac{SNIRT_{k,i}}{SNIR_{k,i,\ell}}) \leq 1$, pois para $0 < x \leq 1$ tem-se $f(x) \leq 1$. Para o problema da minimização conjunta das relações $\frac{SNIRT_{k,i}}{SNIR_{k,i,\ell}}$ de todos os correlacionadores de todos usuários pode-se considerar uma função côncava como descrita anteriormente porém, agora, para múltiplas variáveis $f(x_1, x_2, ..., x_V) = \left(\frac{x_1}{a_1}\right)^{\lambda} + \left(\frac{x_2}{a_2}\right)^{\lambda} + ... + \left(\frac{x_V}{a_V}\right)^{\lambda}$. As figuras 3.11, 3.12 e 3.13 apresentam funções côncavas para duas variáveis, $f(x_1, x_2) = \left(\frac{x_1}{a_1}\right)^{\lambda} + \left(\frac{x_2}{a_2}\right)^{\lambda}$, com $a_1 = a_2 = 1$ e $\lambda = 2$, $\lambda = 4$ e $\lambda = 10$, respectivamente.

As curvas de nível na condição de $f(x_1, x_2) = 1$ para $\lambda = 2$, $\lambda = 4$ e $\lambda = 10$ são apresentadas na figura 3.14.

Todos os pontos (x_1, x_2) definidos internamente e sobre a curva de nível resultam em $f(x_1, x_2) \leq 1$. Assim, $f(x_1, x_2) \leq 1$ significa que $|x_1| \leq 1$ e $|x_2| \leq 1$. No caso limite, $\lambda \to \infty$, tem-se todo ponto (x_1, x_2), com $|x_1| \leq 1$ e $|x_2| \leq 1$, resultando em $f(x_1, x_2) \leq 1$.

Quando λ não for um número par, a função $f(x_1, x_2)$ será como mostrada na figura 3.15, para $\lambda = 7$ e $a_1 = a_2 = 1$. Para $x_1 \geq 0$ e $x_2 \geq 0$, as funções $f(x_1, x_2)$ para λ par ou ímpar tem o mesmo comportamento. Como $\frac{SNIRT_{k,i}}{SNIR_{k,i,\ell}} > 0$, pode-se considerar λ par ou ímpar.

Com as observações sobre a função côncava do tipo $f(x_1, x_2, ..., x_V) = \left(\frac{x_1}{a_1}\right)^{\lambda} + \left(\frac{x_2}{a_2}\right)^{\lambda} + ... + \left(\frac{x_V}{a_V}\right)^{\lambda}$, obtém-se a função objetivo para o problema da maximização da SNIR de todos os correlacionadores de todos os usuários:

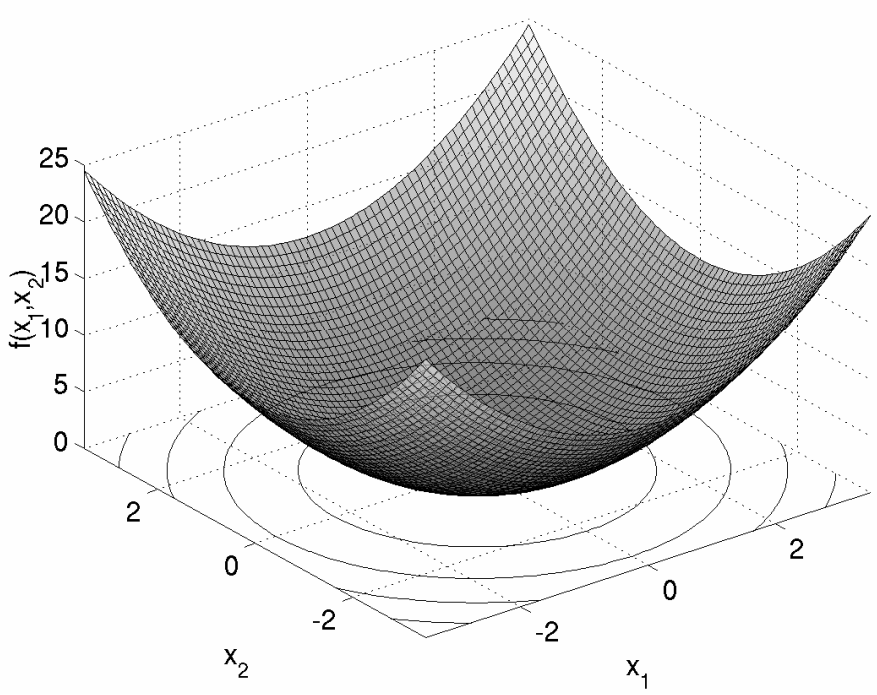

Figura 3.11: Função $f(x_1, x_2) = \left(\frac{x_1}{a_1}\right)^{\lambda} + \left(\frac{x_2}{a_2}\right)^{\lambda}$, com $a_1 = a_2 = 1$ e $\lambda = 2$.

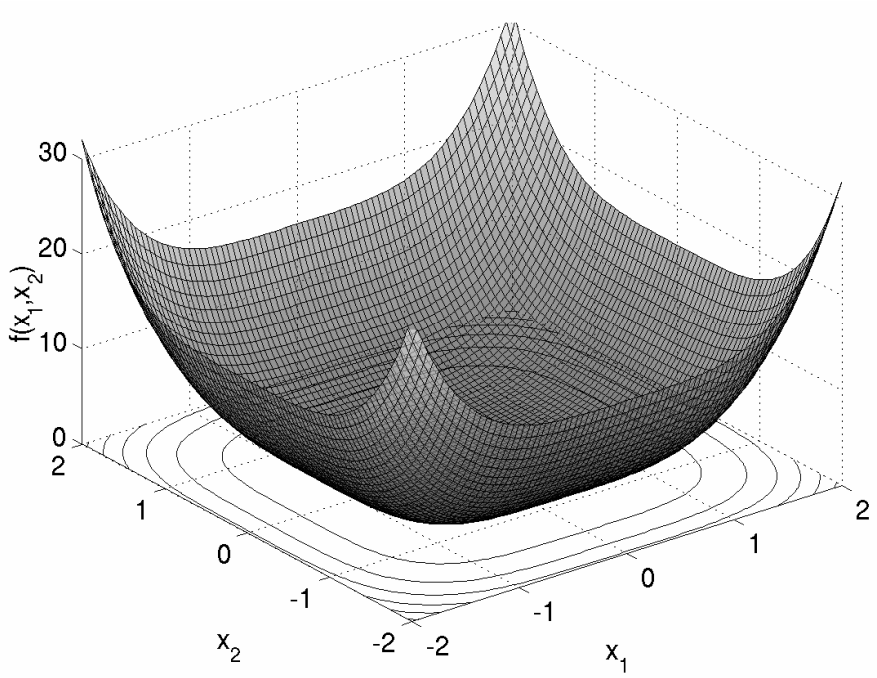

Figura 3.12: Função $f(x_1, x_2) = \left(\frac{x_1}{a_1}\right)^{\lambda} + \left(\frac{x_2}{a_2}\right)^{\lambda}$, com $a_1 = a_2 = 1$ e $\lambda = 4$.

$$f_O(A) = \sum_{i=1}^{n} \sum_{k=1}^{U_i} \sum_{\ell}^{L} \left(\frac{SNIRT_{k,i}}{SNIR_{k,i,\ell}} \right)^{\lambda} \tag{3.70}$$

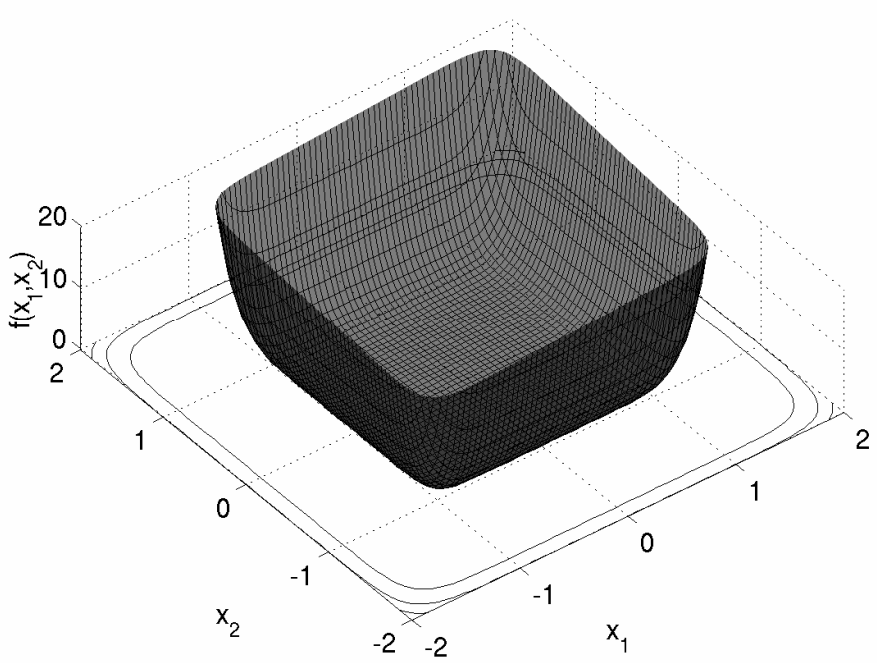

Figura 3.13: Função $f(x_1, x_2) = \left(\frac{x_1}{a_1}\right)^{\lambda} + \left(\frac{x_2}{a_2}\right)^{\lambda}$, com $a_1 = a_2 = 1$ e $\lambda = 10$.

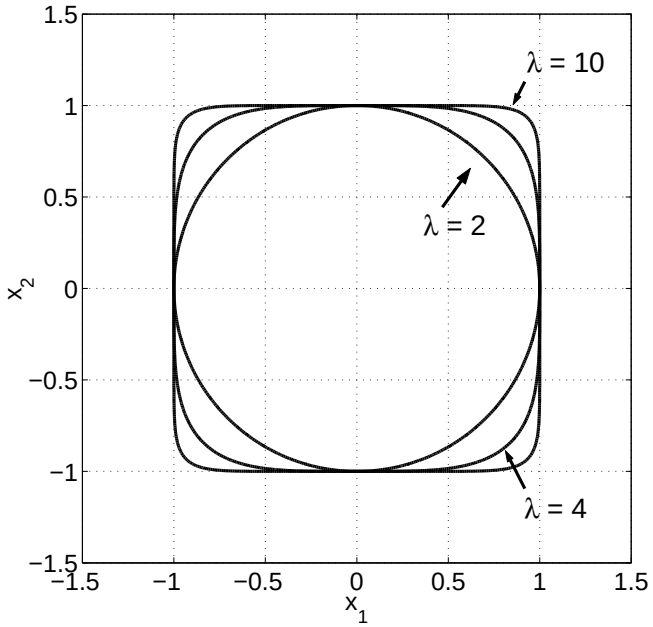

Figura 3.14: Curvas de nível para a função $f(x_1, x_2) = \left(\frac{x_1}{a_1}\right)^{\lambda} + \left(\frac{x_2}{a_2}\right)^{\lambda} = 1$, com $a_1 = a_2 = 1$ e $\lambda = 2, 4$ e 10.

onde A é o conjunto de seqüências, $SNIRT_{k,i}$ é a SNIR alvo (SNIRT) para as SNIR de todos os correlacionadores do receptor do k-ésimo usuário que utiliza o i-ésimo serviço, $SNIR_{k,i,\ell}$ (3.67), e λ é a ordem da função objetivo.

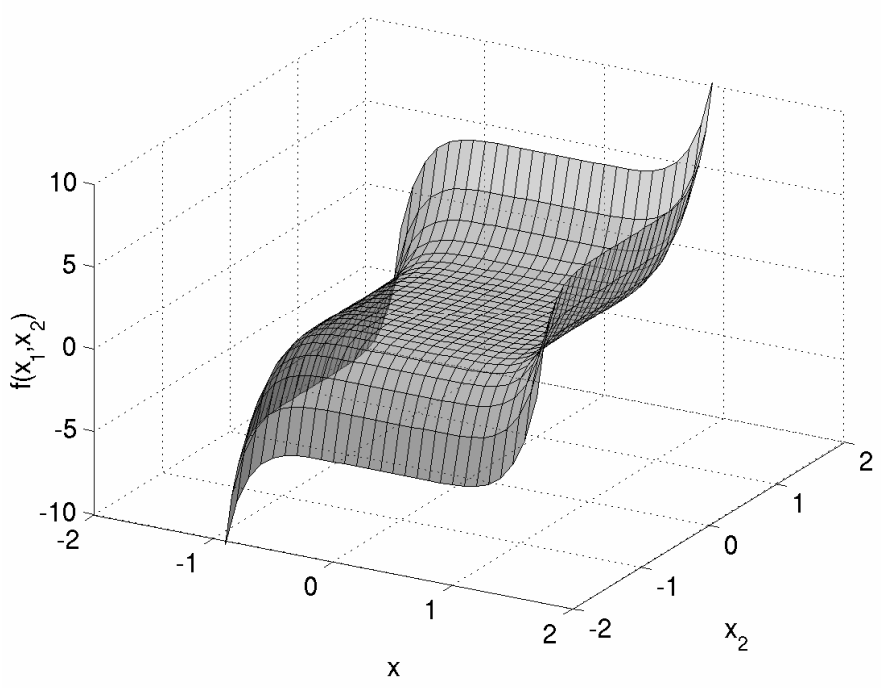

Figura 3.15: Função $f(x_1, x_2) = \left(\frac{x_1}{a_1}\right)^{\lambda} + \left(\frac{x_2}{a_2}\right)^{\lambda}$, com $a_1 = a_2 = 1$ e $\lambda = 7$.

O desempenho do sistema não é função apenas da SNIR. Esse depende também da *pdf* da MAI e da SI. Porém, se nas equações (3.32) e (3.33) os somatórios $\sum_j$, $\sum_u$ e $\sum_{\mathcal{L}}$ compreenderem um grande número de termos, do teorema central do limite (PAPOULIS, 1991), pode-se afirmar que a *pdf* resultante para a MAI adicionada à SI tenderá à uma Gaussiana. Essas somadas ao AWGN, o qual também é Gaussiano, resulta em uma interferência mais ruído com *pdf* tendendo à uma Gaussiana. Adicionalmente, se a potência do AWGN for predominante às potências da MAI e da SI, tem-se também um ruído mais interferência aproximadamente Gaussiano. Assim, o desempenho aproximado do sistema pode ser obtido por uma função da SNIR.

O método de otimização que será utilizado para obter o conjunto de seqüências A que resulta em $f_O(A) \leq 1$ dados os valores de SNIRT, será o método chamado de recozimento simulado (*Simulated Annealing*, SA). Este trabalho não tem como objetivo o estudo de métodos de otimização. Portanto, o método SA será aplicado à função objetivo obtida (3.70) para exemplificar o problema de seleção de seqüências de espalhamento para sistemas QS-CDMA com taxa de dados variáveis do tipo MPG.

A seção seguinte apresenta um breve comentário sobre o método SA.

3.3.4 O método *Simulated Annealing*

Annealing (recozimento, em português) é o nome dado ao processo de aquecimento e resfriamento de um material com o objetivo de alterar sua estrutura física. A mecânica estatística, uma importante disciplina da física da matéria condensada, estuda um conjunto de métodos para analisar propriedades de um grande número de átomos que podem ser encontrados em amostras de sólidos e líquidos. Devido ao grande número de átomos por centímetro cúbico de matéria, apenas o comportamento mais provável do sistema em equilíbrio térmico em uma dada temperatura é observado. De outra forma, existem pequenas flutuações na configuração dos átomos em torno do comportamento médio do sistema. Cada configuração, definida pelas posições dos átomos, é ponderada pelo seu fator de probabilidade de Boltzmann dada por $\exp\left(\frac{-E}{kT_{sa}}\right)$, onde E é a energia da configuração, T_{sa} é a temperatura do sistema e k é a constante de Boltzmann. Observa-se que quanto menor a temperatura, menor é a probabilidade de se obter uma configuração de átomos que resulta em energia elevada. Uma questão fundamental da mecânica estatística é o que acontece com um sistema no limite de baixa temperatura. Se os átomos solidificam-se, em que situação eles formam um sólido cristalino, ou seja, em que situação os átomos assumem uma configuração de baixa energia? Estruturas cristalinas são extremamente raras em corpos macroscópicos. Em um contexto prático, somente abaixar a temperatura não é suficiente para obter estados de baixa energia da matéria. Por exemplo, para o crescimento de cristais a partir de um material fundido, a temperatura deve ser reduzida lentamente e se manter por um longo tempo em temperaturas próximas da temperatura de solidificação. Se isso não for feito, a substância pode sair do equilíbrio e resultar em um cristal com inúmeros defeitos (KIRKPATRICK; GELLAT; VECCHI, 1983). Encontrar estados de baixa energia de um sistema conhecendo-se a forma de calcular sua energia é um problema de otimização similar ao problema de otimização combinatória. As variáveis do problema combinatório estão sujeitas às modificações como os átomos em um sistema físico. A função que se deseja minimizar representa uma medida da energia do sistema. Imitando-se, assim, o processo físico de *annealing*, pesquisadores têm tentado solucionar diversos tipos de problemas de minimização de funções (GAMAL et al., 1987). O método de minimização de funções que imita o *annealing* é conhecido como *simulated annealing* (SA).

O método SA (KIRKPATRICK; GELLAT; VECCHI, 1983) é utilizado em problemas

de otimização de larga escala, especialmente aqueles em que o extremo global está "escondido" entre diversos extremos locais. Como exemplos: o problema clássico do caixeiro viajante (*traveling salesman problem*, TSP) (PEPPER; WASIL, 2002) e de projeto de circuitos integrados complexos (PRESS et al., 1992). Vale ressaltar que o SA é um algoritmo heurístico, o que significa que não existe uma garantia formal de seu desempenho (PAPADIMITRIOU; STEIGLITZ, 1998).

O problema TSP pertence à classe de problemas chamados de *NP*-completo. Em resumo, um problema *P* é um problema cujo algoritmo de solução requer um número de passos que cresce polinomialmente com a dimensão da entrada, ou seja, requer um número de passos limitado por uma função polinomial da entrada. É dito que o tempo de processamento para obter a solução do problema é polinomial. Por exemplo, o tempo de processamento para obter a solução do problema TSP é uma função polinomial do número de localidades que o caixeiro viajante deve visitar. Um problema *NP* é, de modo geral, um problema *P* cuja relação polinomial para o tempo de processamento é não determinística. O *NP*-completo é um problema cujo algoritmo que o soluciona pode ser traduzido para obter soluções para qualquer outro problema da mesma classe (PAPADIMITRIOU; STEIGLITZ, 1998).

O algoritmo *SA* tem-se apresentado eficaz para resolver problemas combinatórios de sistemas de comunicação como a construção de códigos de fonte, códigos corretores de erros e códigos esféricos (GAMAL et al., 1987), e, recentemente, a seleção de seqüências para sistemas de múltiplo acesso do tipo salto no tempo (*time hopping*, TH) e seqüência direta (*direct sequence*, DS) (CANADEO et al., 2003). Para a minimização da função objetivo dada por (3.70), a rigor, deve-se caracterizar o problema, ou seja, determinar a qual classe de problemas este pertence: programação convexa, programação linear, *NP*-completo, etc (PAPADIMITRIOU; STEIGLITZ, 1998). Porém, como o SA tem-se apresentado eficaz na obtenção de soluções razoáveis para os problemas combinatórios citados e para problemas extremamente complexos como os da classe *NP*-completo (por exemplo o TSP), intuitivamente, esse método será aplicado para a minimização da função objetivo dada por (3.70). Nesse caso, a função objetivo $f_O(A)$ será uma medida da energia do sistema e o conjunto de seqüências A estará sujeito às modificações como os átomos do sistema físico.

A seguir é apresentado um algoritmo que modela o processo de *annealing*. As variáveis do processo de *annealing* são parâmetros do sistema QS-CDMA com taxa

de dados variáveis do tipo MPG. Com esse algoritmo, procura-se obter o mínimo da função objetivo anterior dada por (3.70).

```
Escolha um conjunto inicial A de seqüências e a temperatura inicial Tsa;
FAÇA
     {
     FAÇA
          {
          aplique uma perturbação em A resultando no conjunto A';
          DeltaE = Energia(A') - Energia(A);
          se DeltaE < 0, então A = A';
          senão, com probabilidade p = exp( -DeltaE/(Tsa) ), A = A';
          }
     Até vários "sucessos" ou até muitas iterações;
     Reduz a temperatura;
     }
Até obter uma "configuração estável";
```

O conjunto inicial é um conjunto de seqüências escolhidas aleatoriamente do conjunto de todas as seqüências binárias existentes. Aplicar uma perturbação no conjunto de seqüências significa escolher aleatoriamente uma seqüência e alterar um ou dois chips, escolhidos também aleatóriamente (GAMAL et al., 1987). A energia do sistema, dada por `Energia(A)` é o valor de $f_O(A)$. O termo `"sucessos"` está representando uma perturbação que resulta em `DeltaE < 0`. O termo `"configuração estável"` representa a situação na qual $f_O(A) < 1$, ou seja, situação na qual o objetivo já foi alcançado. O valor de T_{sa} inicialmente deve ser consideravelmente maior que o valor de `DeltaE` de maior ocorrência nas primeiras iterações do algoritmo. Para obter esse valor, são necessários alguns testes (PRESS et al., 1992). A redução de temperatura adotada foi de 10% da temperatura atual do sistema. O algoritmo permanece em uma mesma temperatura por $5 \times N_i$, onde N_i é o comprimento das seqüências utilizadas pelos usuários do serviço de taxa de dados mais elevada, ou até ocorrerem $2 \times N_i$ `"sucessos"`. Esse ajuste dos parâmetros do SA foi baseado em (PRESS et al., 1992) e (GAMAL et al., 1987).

Não é necessário escolher um conjunto de seqüências inicial, pois inicialmente a temperatura T_{sa} é elevada e p é aproximadamente 1 para qualquer valor de ΔE. Portanto, qualquer conjunto inicial rapidamente se tornará um conjunto de seqüências aleatórias (GAMAL et al., 1987).

Tabela 3.4: Parâmetros de configuração dos sistemas 1 e 2.

Parâmetros de configuração	**Sistema 1**	**Sistema 2**
$\tau_{\max}$	$1T_c$	$2T_c$
D	2	3
n	2	3
R_1	$60kb/s$	$60kb/s$
R_2	$120kb/s$	$120kb/s$
R_3	-	$240kb/s$
U_1	4	5
U_2	2	3
U_3	-	2
$SNRIT_{k,1}$	$15dB$	$8dB$
$SNRIT_{k,2}$	$15dB$	$8dB$
$SNRIT_{k,3}$	-	$8dB$

Tabela 3.5: Perfil atraso-potência dos canais utilizados nos sistemas 1 e 2.

	Sistema 1		**Sistema 2**	
ℓ	Δ_ℓ	$E\{\alpha_\ell^2\}$	Δ_ℓ	$E\{\alpha_\ell^2\}$
1	$0T_c$	$0,7$	$0T_c$	$0,210$
2	$1T_c$	$0,25$	$1T_c$	$0,420$
3	$2T_c$	$0,05$	$2T_c$	$0,265$
4	-	-	$6T_c$	$0,105$

A seguir são apresentados alguns resultados de minimização de $f_O(A)$ utilizando o método *SA*.

3.3.5 Resultados numéricos

Os resultados que serão apresentados consideram dois sistemas modelados como na seção 3.3.2. Foi adotada taxa de chip do sistema W-CDMA, $3,84Mchip/s$. Os parâmetros máximo erro de sincronismo ($\tau_{\max}$), diversidade Rake (D), número de serviços oferecidos (n), a taxa de dados R_i para cada serviço i, o número U_i de usuários em cada serviço i e o valor da SNIRT dos usuários de cada serviço ($SNRIT_{k,i}$) são apresentados na tabela 3.4 para os sistemas denominados 1 e 2. O perfis atraso-potência dos canais utilizado para os sistemas 1 e 2 são apresentados na tabela 3.5. Para o sistema 2 o perfil atraso-potência foi baseado no modelo COST207 urbano (STUBER, 2001). Para reduzir o esforço computacional foram utilizados apenas os 4 componentes multipercurso mais significativos. Foi considerado $\frac{E_b}{N_0} \to \infty$, situação em que a SNIR não depende do AWGN.

As figuras 3.16 e 3.17 apresentam a minimização de $f_O(A)$ em função das iterações para os sistemas 1 e 2, respectivamente.

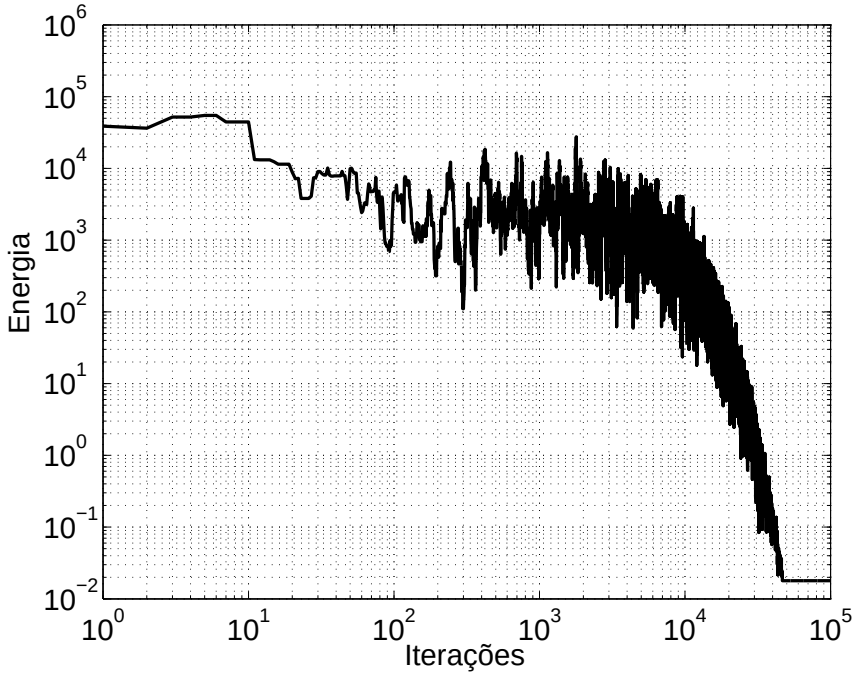

Figura 3.16: Resultado da minimização da energia, $f_O(A)$, para o sistema 1.

Além de resultados em termos de SNIR, os quais são exatos, serão também apresentados resultados aproximados em termos de taxa de erro de bit (BER) do sistema considerando desvanecimento Rayleigh. Esses resultados permitirão avaliar comparativamente o desempenho do sistema com as seqüências selecionadas. Como nas equações (3.32) e (3.33) os somatórios $\sum_j$, $\sum_u$ e $\sum_{\mathcal{L}}$ compreendem um grande número de termos (17 para o sistema 1 e 39 para o sistema 2) de (YAO, 1977) pode-se afirmar que a *pdf* resultante para a MAI adicionada à SI tenderá a uma Gaussiana. Fazendo-se essa aproximação, obtém-se o desempenho aproximado do *k*-ésimo usuário que utiliza o serviço *i* em termos de taxa de erro de bit (BER) por meio de (PROAKIS, 1995):

$$BER_{k,i} = \frac{1}{2}\sum_{\ell=1}^{D} \Upsilon_\ell \left[1 - \sqrt{\frac{SNIR_{k,i,\ell}}{2 + SNIR_{k,i,\ell}}}\right] \tag{3.71}$$

$$\Upsilon_\ell = \prod_{\mathcal{L}=1,\ \mathcal{L}\neq\ell}^{D} \frac{SNIR_{k,i,\ell}}{SNIR_{k,i,\ell} - SNIR_{k,i,\mathcal{L}}} \tag{3.72}$$

A avaliação de desempenho será realizada observando a BER média do serviço

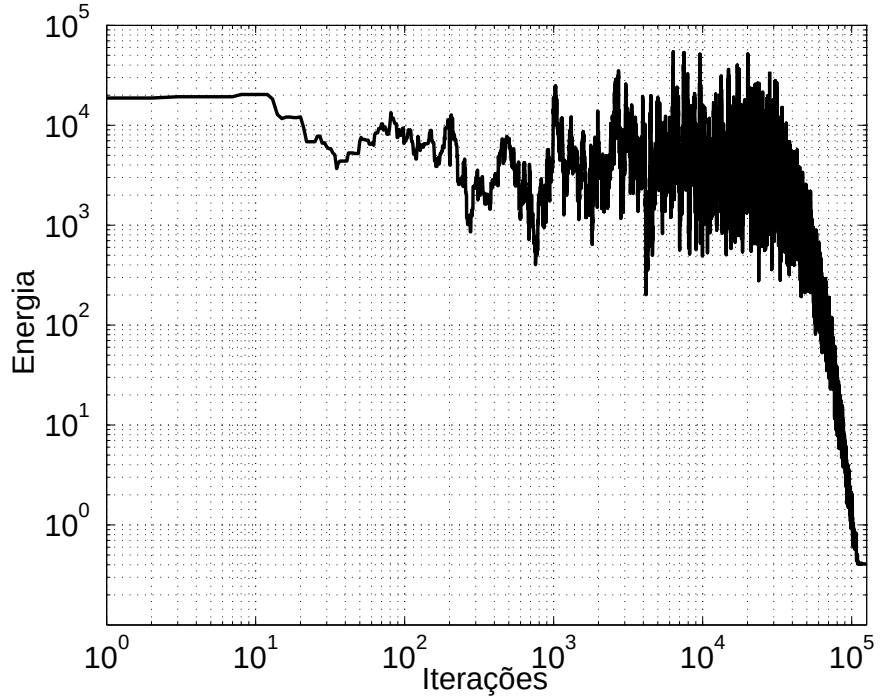

Figura 3.17: Resultado da minimização da energia, $f_O(A)$, para o sistema 2.

i ($\overline{BER}_i$) dada pela média aritmética das BER de todos os usuários do serviço i. As figuras 3.18 e 3.19 apresentam a minimização da BER média em função das iterações do algoritmo SA para os sistemas 1 e 2, respectivamente.

Para o sistema 1, a execução do algoritmo SA foi interrompida imediatamente após 10^5 iterações. O critério de $f_O(A) \leq 1$ foi satisfeito na iteração 24197. Os valores mínimos atingidos de BER média foram: $\overline{BER}_1 = 2,45 \times 10^{-6}$ e $\overline{BER}_2 = 1,21 \times 10^{-5}$. O valor mínimo atingido de energia foi $0,0179$. Com apenas 10^5 iterações o que representa uma quantidade de testes muito menor que o número de conjuntos de seqüências binárias existentes, $\frac{\binom{2^{64}}{4}\times\binom{2^{32}}{2}}{64} \cong 4,45\times10^{94}$, foi atingido o objetivo e obtido um elevado ganho de desempenho. Os valores atingidos de SNIR na saída de cada correlacionador de cada usuário com o método SA são apresentados na tabela 3.6.

Para o sistema 2, a execução do algoritmo SA foi interrompida imediatamente depois de 126000 iterações. O critério de $f_O(A) \leq 1$ foi satisfeito na iteração 99159 Os valores mínimos atingidos de BER média foram: $\overline{BER}_1 = 9,49 \times 10^{-7}$, $\overline{BER}_2 = 5,96 \times 10^{-6}$ e $\overline{BER}_3 = 2,70 \times 10^{-5}$. O valor mínimo atingido de energia foi $0,40743$. Com apenas 126×10^3 iterações o que representa uma quantidade de testes muito menor que o número de conjuntos de seqüências binárias existentes $\frac{\binom{2^{64}}{5}\times\binom{2^{32}}{3}\times\binom{2^{16}}{2}}{64} \cong 5\times10^{131}$,

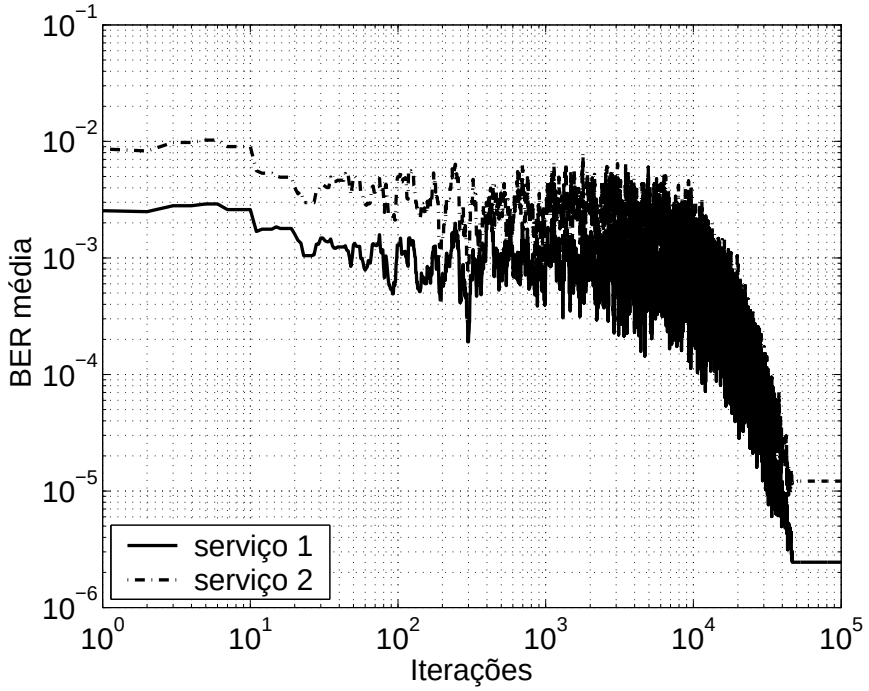

Figura 3.18: Resultado da minimização da BER média para o sistema 1.

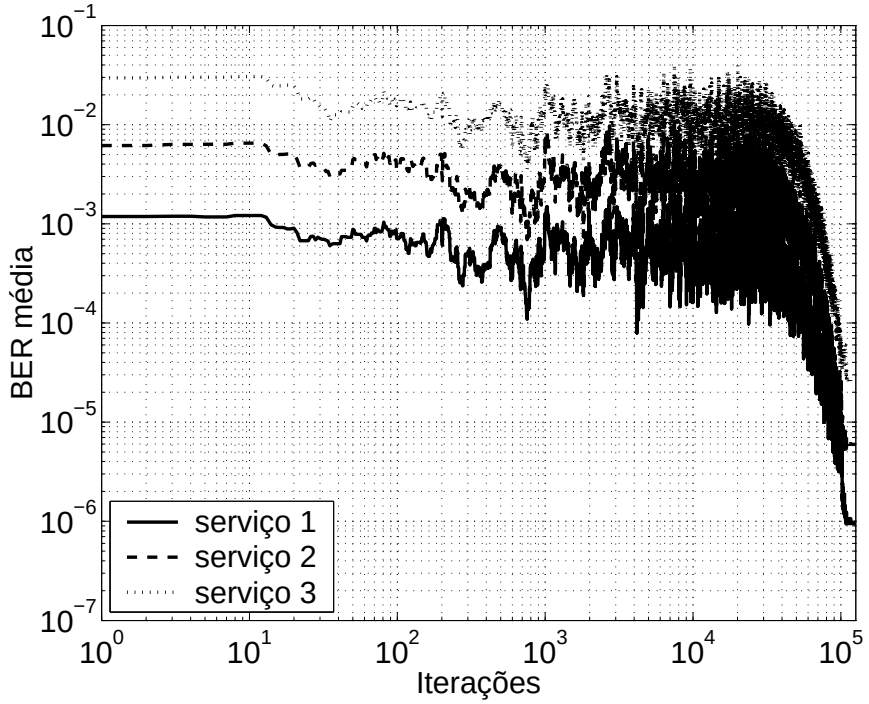

Figura 3.19: Resultado da minimização da BER média para o sistema 2.

Tabela 3.6: Valores de SNIR atingidos com o método SA aplicado ao sistema 1.

serviço i	usuário k	correlacionador d	$SNIR_{i,k,d}$ $[dB]$
1	1	1	29,0216
		2	24,2578
	2	1	28,9615
		2	25,5672
	3	1	32,0017
		2	26,4387
	4	1	30,2743
		2	24,2956
2	1	1	26,0113
		2	21,2475
	2	1	25,9512
		2	22,5569

foi atingido o objetivo e obtido um elevado ganho de desempenho. Os valores atingidos de SNIR na saída de cada correlacionador de cada usuário com o método SA são apresentados na tabela 3.7.

Observe que os valores de SNIR para correlacionadores de um mesmo usuário estão próximos. Dessa modo, obtém-se um melhor aproveitamento da diversidade Rake e o desempenho do sistema é maximizado.

Como não existem trabalhos sobre seqüências adequadas para sistemas QS-CDMA multitaxa do tipo MPG em canal multipercurso, a comparação dos resultados será feita com as seqüências conhecidas como *orthogonal variable spreading factor* (OVSF) (ADACHI; SAWAHASHI; OKAWA, 1997), as quais foram propostas para sistemas síncronos multitaxa do tipo MPG. As figuras 3.20 e 3.21 apresentam a BER média versus $\frac{E_b}{N_0}$ para os sistemas utilizando as seqüências selecionadas e também para os sistemas utilizando as seqüências OVSF selecionadas ao acaso, porém respeitando o critério de ortogonalidade de (ADACHI; SAWAHASHI; OKAWA, 1997). Adicionalmente, essas figuras apresentam o limite de BER, o qual é dado por (3.71) com $SNIR_{k,i,\ell} = \frac{2E_b\mathbb{E}\{\alpha_{k,i,\ell}\}}{N_0}$. Para o sistema 1, as seqüências OVSF escolhidas foram: $\mathbf{c}_{64}^{(26)}$, $\mathbf{c}_{64}^{(28)}$, $\mathbf{c}_{64}^{(55)}$, $\mathbf{c}_{64}^{(60)}$, $\mathbf{c}_{32}^{(15)}$ e $\mathbf{c}_{32}^{(24)}$, geradas conforme mostra a seção 3.3.1 e (ADACHI; SAWAHASHI; OKAWA, 1997). Para o sistema 2, as seqüências OVSF escolhidas foram: $\mathbf{c}_{64}^{(3)}$, $\mathbf{c}_{64}^{(25)}$, $\mathbf{c}_{64}^{(55)}$, $\mathbf{c}_{64}^{(65)}$, $\mathbf{c}_{64}^{(61)}$, $\mathbf{c}_{32}^{(5)}$, $\mathbf{c}_{32}^{(12)}$, $\mathbf{c}_{32}^{(21)}$, $\mathbf{c}_{16}^{(13)}$ e $\mathbf{c}_{16}^{(15)}$, também geradas conforme mostra a seção 3.3.1 e (ADACHI; SAWAHASHI; OKAWA, 1997).

Observa-se que utilizando o método de seleção de seqüências proposto aqui, há

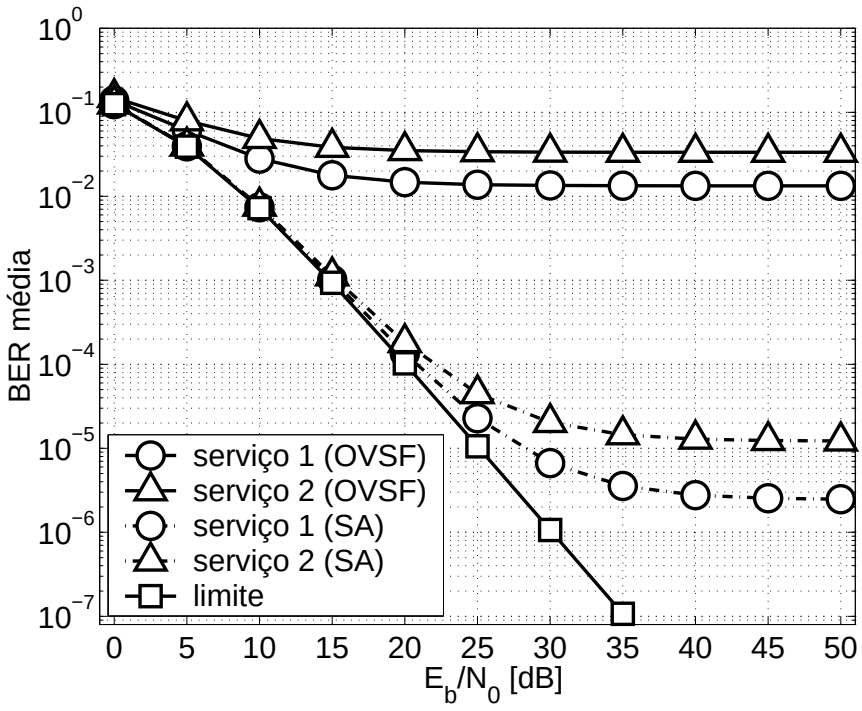

Figura 3.20: Comparação da BER média para o sistema 1 com seqüências OVSF e com seqüências selecionadas pelo método SA.

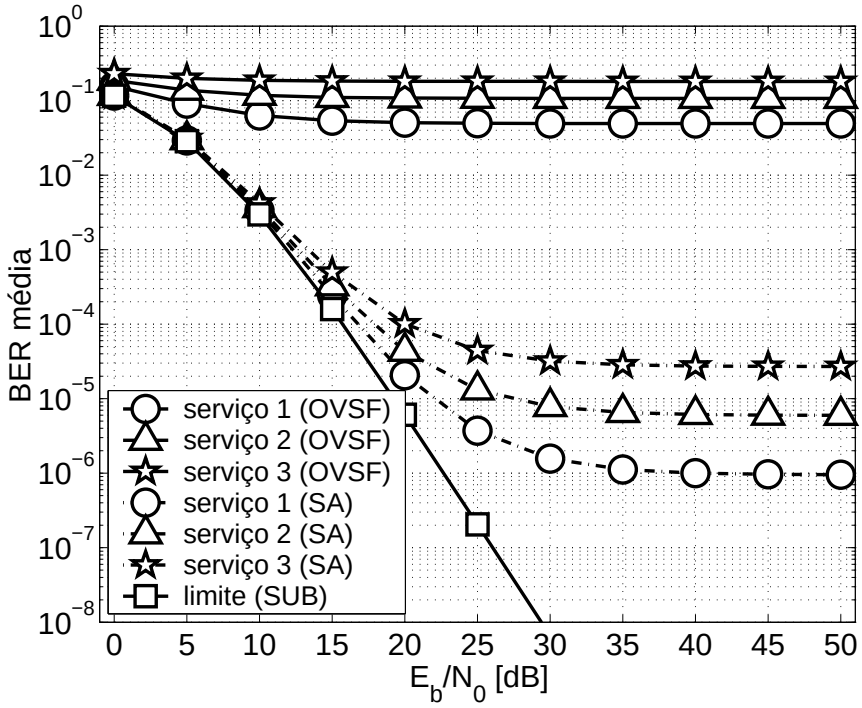

Figura 3.21: Comparação da BER média para o sistema 2 com seqüências OVSF e com seqüências selecionadas pelo método SA.

um elevado ganho de desempenho. Com um número de iterações extremamente reduzido, quando comparado ao tamanho do universo de seqüências binárias, é possível maximizar o desempenho do sistema.

3.3.6 Extensão do método de seleção de seqüências

O método de seleção de seqüências proposto para sistemas QS-CDMA com taxa de dados variáveis do tipo MPG pode ser utilizado para selecionar seqüências para sistemas de taxa única. Para tanto, basta considerar apenas um serviço na modelagem apresentada na seção 3.3.2. Esse método também pode ser aplicado para selecionar seqüências para sistemas de taxa de dados variáveis do tipo MC. Nesse caso, na função objetivo (3.70) a SNIR será dada por (3.21).

A seleção de seqüências por meio da minimização de um parâmetro como a função objetivo dada por (3.70) é um método eficaz, conforme mostrado na seção anterior. Porém, no caso de sistemas de taxa única ou taxa de dados variáveis do tipo MC, bons desempenhos podem ser obtidos com diversos conjuntos de seqüências construídos por métodos sistemáticos. Seções anteriores apresentaram alguns desses métodos que, basicamente, consistem em utilizar propriedades da álgebra de corpos finitos ou propriedades de seqüências complementares para obter seqüências adequadas para sistemas QS-CDMA de taxa única ou variável do tipo MC.

Devido a um grande número de usuários ativos ou usuários com necessidade de elevadas taxas de dados, um sistema de taxa única ou variável do tipo MC pode necessitar de um número de seqüências maior do que o disponível em um conjunto construído sistematicamente. Nesse caso, aplicar o método apresentado neste capítulo para seleção de seqüências para sistemas de taxa única ou variável do tipo MC é uma solução razoável.

Tabela 3.7: Valores de SNIR atingidos com o método SA aplicado ao sistema 2.

serviço i	usuário k	correlacionador d	$SNIR_{i,k,d}$ $[dB]$
1	1	1	19,2052
		2	23,8300
		3	22,2056
	2	1	18,7832
		2	23,3891
		3	20,8626
	3	1	17,4235
		2	21,8898
		3	19,9360
	4	1	18,0344
		2	22,2187
		3	20,1122
	5	1	17,5807
		2	21,7498
		3	20,2404
2	1	1	16,1949
		2	20,8197
		3	19,1953
	2	1	15,7729
		2	20,3788
		3	17,8523
	3	1	14,4132
		2	18,8795
		3	16,9257
3	1	1	13,1846
		2	17,8094
		3	16,1850
	2	1	12,7626
		2	17,3685
		3	14,8420

4 Conclusões

O desempenho de um sistema CDMA é limitado principalmente pela interferência de múltiplo acesso (MAI) e pela auto-interferência (SI). Na seção 1.1 foi mostrado que a MAI e a SI podem ser escritas em termos das funções de correlação periódica das seqüências de espalhamento utilizadas no sistema. As funções de correlação periódica utilizadas para o cálculo da MAI e da SI consideram apenas deslocamentos dentro de um intervalo que representa o intervalo de tempo em que os diversos multipercursos são recebidos. Utilizando-se seqüências de espalhamento que resultam em reduzidos valores de correlação periódica para tal intervalo pode-se minimizar os efeitos da MAI e da SI.

Em um sistema QS-CDMA, os usuários transmitem sincronizadamente resultando na condição de todos os multipercursos dos sinais transmitidos chegando ao receptor da estação rádio base com diferenças de atrasos confinadas em um intervalo de tempo definido. Assim, a utilização de seqüências ortogonais ou quase ortogonais generalizadas minimizam os efeitos da MAI e da SI. Conforme mostrado na seção 1.2, quanto menor a zona de correlação reduzida ou nula, maior será o universo de pares de seqüências que apresentam valores reduzidos de correlação. Essa característica confere aos sistemas QS-CDMA melhor desempenho e capacidade comparado aos sistemas CDMA assíncronos convencionais.

As famílias de seqüências binárias adequadas para sistemas QS-CDMA apresentadas neste trabalho incluem: QS, Lin-Chang, LCZ-GMW, OQS e ZCZ. Para essas famílias foram apresentadas as metodologias de construção, funções de correlação, características como o número de seqüências em uma família, os comprimentos de seqüências existentes, o compromisso entre a zona de correlação reduzida ou nula e o número de seqüências no conjunto etc. Para fundamentar a análise das famílias de seqüências adequadas para sistemas QS-CDMA, foram também estudadas as seqüências de máximo comprimento (SMC), Gold e GMW, pois são bases para a construção das

famílias quase ortogonais generalizadas QS, Lin-Chang e LCZ-GMW. Essa relação foi apresentada na seção 2.1.8.

As famílias de seqüências binárias para QS-CDMA foram comparadas em termos de suas características e desempenhos (BER) proporcionados em um sistema com recepção convencional em canal Rayleigh multipercurso. A família ZCZ apresentou-se com o melhor conjunto de características e desempenho. Essa família de seqüências confere ao sistema uma boa resistência ao erro de sincronismo. O método de construção da família ZCZ é bastante flexível. Para um comprimento de seqüências fixo, pode-se variar a zona de correlação aumentando ou diminuindo-se o número de seqüências no conjunto.

Ao contrário da família ZCZ, as famílais Lin-Chang e LCZ-GMW não são flexíveis. Para comprimentos de seqüências menores ou iguais a 1023 não é possível variar a zona de correlação alterando-se o tamanho do conjunto (seção 2.3). Adicionalmente, a família Lin-Chang possui o inconveniente de não garantir o valor nulo de correlação cruzada periódica par para seqüências em fase. Para obter tal resultado com algumas seqüências do conjunto é necessário ajustar as fases das sementes. Isso exige uma procura exaustiva, já que não existe um método sistemático. Para a família LCZ-GMW, é garantido o valor nulo para a função de correlação cruzada periódica para seqüências em fase, porém ainda não foi obtida um expressão genérica para o número de seqüência em um conjunto. Pode-se obter esse número construindo-se o conjunto ou ainda obter uma boa aproximação a partir do limite de Tang-Fan, seção 2.1.6.2. A família LCZ-GMW é composta de seqüências selecionadas da família Lin-Chang. Assim, o desempenho obtido com a família LCZ-GMW é superior ao obtido com a família Lin-Chang.

As famílias de seqüências QS e OQS são derivadas da família Gold. O método de construção da família QS considera a busca exaustiva por seqüências Gold que apresentam a característica de zona de correlação reduzida. O método de construção da família OQS também considera a busca exaustiva, porém buscam-se seqüências ortogonais generalizadas em um conjunto Gold ortogonal. O método de busca exaustiva pode exigir considerável processamento computacional dependendo do tamanho do universo de busca. Isso foi exemplificado na seção 2.3. Para um dado valor de zona de correlação nula, a relação $\frac{\max\{K\}}{N}$ é menor para os conjuntos OQS e QS do que para o conjunto ZCZ. Essa característica impede que os desempenhos obtidos com as famílias

QS e OQS sejam superiores que os obtidos com a família ZCZ.

Neste trabalho, também foram abordados os esquemas de taxa de dados variável do tipo múltiplos códigos de espalhamento (MC) e múltiplos ganhos de processamento (MPG). O esquema MC exige famílias que compreendem um grande número de seqüências para acomodar taxas de dados elevadas. Das família abordadas neste trabalho, as que se apresentaram adequadas para o esquema MC foram: ZCZ, QS e OQS. O desempenho do QS-CDMA com esquema MC obtido com a família ZCZ foi superior ao obtido com a família QS, seção 3.2.2.

Foi proposta uma metodologia de seleção de seqüências para sistemas QS-CDMA com taxa de dados variável do tipo MPG. A metodologia consiste em obter uma expressão para a relação sinal ruído mais interferência (SNIR) e, por meio de um método de otimização combinatória, maximizá-la atingindo um nível predefinido como aceitável para prover determinada qualidade de serviço. Essa metodologia foi exemplificada utilizando o método de otimização combinatória chamado de recozimento simulado (*simulated annealing*, SA). O conjunto de seqüências resultante foi comparado em termos taxa de erro de bit de um sistema QS-CDMA MPG com o conjunto de seqüências OVSF. Verificou-se o elevado ganho de desempenho com a utilização do método proposto, seção 3.3.5. Esse mesmo método pode ser aplicado à seleção de seqüências para sistemas de taxa única ou MC utilizando as expressões de SNIR derivadas nesse trabalho. Porém, para tais sistemas, bons desempenhos podem ser obtidos por meio de métodos de menor complexidade computacional como os analisados nesse trabalho.

Este trabalho também apresentou um breve estudo sobre as seqüências polifásicas adequadas para sistemas QS-CDMA: LCZ-GMW polifásica, ZCZ quadrifásica, PS e SP, apêndice C. O método de construção das famílias LCZ-GMW polifásica e ZCZ quadrifásica são semelhantes aos das famílias LCZ-GMW binária e ZCZ binária, respectivamente. A função de correlação cruzada periódica par para as famílias PS e SP apresenta valor nulo para qualquer seqüência do conjunto e qualquer deslocamento. Porém, a função de correlação cruzada periódica ímpar apresenta diversos picos. Para a família PS, a ocorrência desses picos pode ser controlada reduzindo-se o número de seqüências no conjunto.

O sitema LAS-CDMA, recentemente proposto na literatura também é abordado neste trabalho, apêndice D. Esse sistema utiliza uma família de seqüências ternárias que possui zona de correlação aperiódica nula também chamada de janela livre de

interferência (IFW). Dessa forma, se os multipercursos de todos os sinais transmitidos estiverem confinados em um intervalo de tempo que não provoque um deslocamento entre seqüências maior que a IFW, a MAI e a SI resultante será nula.

Um breve estudo sobre a utilização de detecção multiusuário em sistemas QS-CDMA complementa o trabalho, apêndice E. Com esse estudo verifica-se que um único estágio PIC-HD em um sistema QS-CDMA utilizando seqüências adequadas é suficiente para uma significativa melhoria de desempenho. Adicionalmente, a utilização do PIC-HD minimiza as diferenças de desempenho obtidas com as famílias QS, Lin-Chang, LCZ-GMW e ZCZ.

4.1 Trabalhos futuros e publicações resultantes deste trabalho

Como proposta futura de trabalho sugere-se:

- Estudos adicionais de seqüências ternárias;
- Análise estocástica do método SA aplicado à metodologia de seleção de seqüências proposta nesse trabalho.
- Aplicação de outros métodos de otimização combinatória à metodologia de seleção de seqüências proposta nesse trabalho.

Este trabalho originou até essa data as seguintes publicações em conferências nacionais:

- (KURAMOTO; ABRÃO; JESZENSKY, 2003) André S. R. Kuramoto, Taufik Abrão e Paul Jean E. Jeszensky: "Conjuntos de Seqüências para Sistemas QS-CDMA com Detecção Multiusuário Sujeitos a Desvanecimento Multipercurso", *Anais do XX Simpósio Brasileiro de Telecomunicações, SBT'03, 2003, p. 426–431*
- (KURAMOTO; ABRÃO; JESZENSKY, 2004a) André S. R. Kuramoto, Taufik Abrão e Paul Jean E. Jeszensky: "Projetos de Seqüências para Sistemas QS-CDMA Multitaxa MPG", *XXI Simpósio Brasileiro de Telecomunicações, SBT'04, 2004*

as seguintes publicações em conferências internacionais:

- (KURAMOTO; ABRÃO; JESZENSKY, 2004c) André S. R. Kuramoto, Taufik Abrão and Paul Jean E. Jeszensky: "Spreading Sequence Comparison for QS-CDMA Systems", *IEEE International Symposium on Spread Spectrum Techniques and Applications, 2004, p. 350–354*

- (KURAMOTO; ABRÃO; JESZENSKY, 2004b) André S. R. Kuramoto, Taufik Abrão and Paul Jean E. Jeszensky: "Set of Sequences for QS-CDMA Systems with Interference Cancellation over Multipath-Fading Channels", *IEEE International Symposium on Spread Spectrum Techniques and Applications, 2004, p. 694–698*

e o seguinte artigo a ser publicado em revista internacional:

- (KURAMOTO; ABRÃO; JESZENSKY,) André S. R. Kuramoto, Taufik Abrão and Paul Jean E. Jeszensky: "Set of Sequences for QS-CDMA Systems with Multi-User Detection and Multipath-Fanding Channels", *Wireless Personal Communication, Kluwer Academic Publisher, in press.*

Apêndice A – Algumas derivações matemáticas

A.1 Solução da Integral:

$$\int_{m\ T_c}^{(m+1)\ T_c} \mathcal{R}_{u,k}^2(\tau) + \tilde{\mathcal{R}}_{u,k}^2(\tau)\ d\tau \tag{A.1}$$

onde $R_{u,k}(\tau)$ e $\tilde{\mathcal{R}}_{u,k}(\tau)$ foram definidos em (1.21).

A função de correlação parcial para $\tau = mT_c$, com m um número inteiro, pode ser escrita como:

$$\mathcal{R}_{u,k}(mT_c) = T_c C_{u,k}(m-N) \tag{A.2}$$

onde $C_{i,j}(d)$ foi definido (1.29).

Como foi assumido formatação de pulso retangular para as seqüências de espalhamento, a função $\mathcal{R}_{u,k}(\tau)$ tem comportamento linear para $mT_c \leq \tau < (m+1)T_c$, com $0 \leq m < N-1$ (apêndice A.2). Assim:

$$\begin{aligned} \mathcal{R}_{u,k}(mT_c) &= T_c C_{u,k}(m-N) + \left[C_{u,k}(m-N+1) - C_{u,k}(m-N)\right](\tau - mT_c) \\ &= A_1 + A_2\tau \end{aligned} \tag{A.3}$$

onde $A_1 = (m+1)T_c C_{u,k}(m-N) - mT_c C_{u,k}(m-N+1)$ e $A_2 = C_{u,k}(m-N+1) - C_{u,k}(m-N)$.

Analogamente:

$$\tilde{\mathcal{R}}_{u,k}(mT_c) = T_c C_{u,k}(m) \tag{A.4}$$

e

$$\begin{aligned}\tilde{\mathcal{R}}_{u,k}(mT_c) &= T_c C_{u,k}(m) + \left[C_{u,k}(m+1) - C_{u,k}(m)\right](\tau - mT_c) \\ &= B_1 + B_2\tau \end{aligned} \tag{A.5}$$

onde $B_1 = (m+1)T_c C_{u,k}(m-N) - mT_c C_{u,k}(m-N+1)$ e $B_2 = C_{u,k}(m-N+1) - C_{u,k}(m-N)$.

Assim:

$$\int_{m\ T_c}^{(m+1)\ T_c} \mathcal{R}^2_{u,k}(\tau) + \tilde{\mathcal{R}}^2_{u,k}(\tau)\, d\tau = \int_{m\ T_c}^{(m+1)\ T_c} (A_1 + A_2\tau)^2\, d\tau + \int_{m\ T_c}^{(m+1)\ T_c} (B_1 + B_2\tau)^2\, d\tau$$

$$= (A_1^2 + B_1^2)T_c + (A_1A_2 + B_1B_2)(2m+1)T_c^2 + \frac{A_2^2 + B_2^2}{3}(3m^2 + 3m + 1)T_c^3 \tag{A.6}$$

Substituindo A_1, A_2, B_1 e B_2:

$$\begin{aligned}&\int_{m\ T_c}^{(m+1)\ T_c} \mathcal{R}^2_{u,k}(\tau) + \tilde{\mathcal{R}}^2_{u,k}(\tau)\, d\tau = \\ &\frac{T^3}{3}\Big(C_{u,k}(m-N+1)C_{u,k}(m-N) + C_{u,k}(m+1)C_{u,k}(m) + C^2_{u,k}(m-N) + \\ &C^2_{u,k}(m) + C^2_{u,k}(m-N+1) + C^2_{u,k}(m+1)\Big)\end{aligned} \tag{A.7}$$

O conteúdo deste apêndice é baseado em (JESZENSKY, 2001).

A.2 Relações entre as funções de correlação

$$\mathcal{R}_{u,k}(\tau) = \int_0^{\tau} c_u(t-\tau)c_k^*(t)\, dt \tag{A.8}$$

Fazendo $\tau = rT_c$:

$$\begin{aligned}\mathcal{R}_{u,k}(rT_c) &= \int_0^{rT_c} c_u(t - rT_c)c_k^*(t)\, dt \\ &= \int_0^{rT_c} \sum_{m=-\infty}^{\infty} p(t - rT_c - mT_c)\underline{c}_{u,m} \sum_{n=-\infty}^{\infty} p(t - nT_c)\underline{c}^*_{k,n}\, dt\end{aligned} \tag{A.9}$$

Fazendo $r + m = q$:

$$\begin{aligned}\mathcal{R}_{u,k}(rT_c) &= \int_0^{rT_c} \sum_{q-r=-\infty}^{\infty} p(t-qT_c)\underline{c}_{u,(q-r)} \sum_{n=-\infty}^{\infty} p(t-nT_c)\underline{c}_{k,n}^{*}\, dt \\ &= \int_0^{rT_c} \sum_{n=0}^{r-1} p(t-nT_c)\underline{c}_{u,(q-r)}\underline{c}_{k,n}^{*} \end{aligned} \tag{A.10}$$

Fazendo $r-1 = N+d-1$

$$\begin{aligned}\mathcal{R}_{u,k}(rT_c) &= T_c \sum_{n=0}^{N-d-1} \underline{c}_{u,(n-N-d)}\underline{c}_{k,n}^{*} \\ &= T_c \sum_{n=0}^{N-d-1} \underline{c}_{u,(n-d)}\underline{c}_{k,n}^{*} \\ &= T_c C_{u,k}(d) \\ &= T_c C_{u,k}(r-N) \end{aligned} \tag{A.11}$$

Para $\tau = (r+1)T_c$:

$$\mathcal{R}_{u,k}((r+1)T_c) = T_c C_{u,k}(r-N+1) \tag{A.12}$$

Como $\mathcal{R}_{u,k}(\tau)$ é linear para $rT_c \leq \tau \leq (r+1)T_c$:

$$\mathcal{R}_{u,k}(\tau) = T_c C_{u,k}(r-N) + \left[C_{u,k}(r-N+1) - C_{u,k}(r-N)\right](\tau - rT_c) \tag{A.13}$$

Analogamente, obtém-se:

$$\tilde{\mathcal{R}}_{u,k}(\tau) = T_c C_{u,k}(r) + \left[C_{u,k}(r+1) - C_{u,k}(r)\right](\tau - rT_c) \tag{A.14}$$

O conteúdo deste apêndice é baseado em (JESZENSKY, 2001).

Apêndice B – Álgebra

B.1 Teoria básica de corpos finitos

Nesta seção será apresentada uma teoria básica para o estudo e análise de seqüências construídas algebricamente, ou seqüências sobre $GF(q)$, como são comumente chamadas. As referências bibliográficas para esta seção são (MCELIECE, 1987), (GOLOMB, 1982) e (LIDL; NIEDERREITER, 1997).

B.1.1 Corpos finitos

Em (MCELIECE, 1987) define-se, informalmente, corpo como um "lugar" onde se pode somar, subtrair, multiplicar e dividir. Formalmente, é um conjunto F no qual realizam-se duas operações binárias "+" e "·", soma e multiplicação, respectivamente. Operação binária em um conjunto A não vazio é um mapeamento $f : A \times A \rightarrow A$ tal que f é definido para todo elemento de A e a imagem de A sobre f é única. A imagem de A sobre f é o conjunto de todos os valores que f pode assumir à medida que seu argumento A varia.

Para o corpo, como foi definido, valem os axiomas:

- F é um grupo[1] Abeliano [2] sobre "+", com elemento identidade 0, ou seja, $0+a = a+0$, $a \in F$;
- Os elementos não nulos de F formam um grupo Abeliano sobre "·";
- A lei distributiva $a.(b+c) = a.b + a.c$ é aplicável.

[1] grupo é um conjunto finito ou infinito de elementos e uma operação binária os quais conjuntamente satisfazem as quatro propriedades fundamentais: fechamento, associativa, identidade e inversabilidade.
[2] grupo Abeliano é um grupo no qual seus elementos comutam.

Um corpo pode ser finito ou infinito, de acordo com o conjunto (finito ou infinito) em que é definido. Alguns exemplos de corpo infinito incluem números reais, números racionais e números complexos. Um corpo finito é um corpo com número de elementos (também chamado de ordem do corpo, seção B.1.4) finito.

Pode-se definir o corpo finito da seguinte forma:

$$F_p = \{0, 1, ..., p-1\}, \text{ aritmética mod } p. \tag{B.1}$$

Por exemplo, o conjunto $Z_2 = \{0, 1\}$ é um corpo finito. Em contrapartida, o conjunto $Z_4 = \{0, 1, 2, 3\}$ não é um corpo, pois não há nenhum elemento x tal que $2x \equiv 1$, onde $\equiv$ denota equivalência (a relação de equivalência será tratada a seguir), ou seja, a propriedade de inversabilidade não é verificada. Ainda nesta seção, será mostrado que p deve ser primo para Z_p ser um corpo finito.

B.1.2 Domínio Euclidiano

Um domínio integral é um conjunto D, acrescido de duas operações binárias, + e $\cdot$, tais que:

1. Os elementos de D formam um grupo Abeliano sobre +, no qual a identidade de adição é denotado pelo elemento 0;
2. A multiplicação é associativa e comutativa. Adicionalmente, tem como elemento identidade o elemento denotado por 1;
3. A lei de cancelamento é aplicável. Isto é, se $ab = ac$ e $a \neq 0$, então $b = c$;
4. A lei distributiva é aplicável. Isto é, se a, b e c pertencem a D, então $a(b + c) = ab + ac$.

O domínio Euclidiano é um domínio integral com uma característica adicional: a noção de "tamanho" entre os elementos. O "tamanho" do elemento a, com $a \neq 0$, denotado por $g(a)$, é um inteiro não negativo tal que:

$$g(a) \leq g(ab) \text{ se } b \neq 0 \tag{B.2}$$

e ainda, para todo $a, b \neq 0$, existem q e r ("quociente" e "resto") tais que $a = qb + r$, com $r = 0$ ou $g(r) < g(b)$.

Alguns exemplos de domínios Euclidianos são: o conjunto dos números inteiros com $g(n) = |n|$ e polinômios sobre um corpo, com $g(f(x)) = \text{grau}(f)$.

B.1.3 Construção de um corpo finito

Nesta seção será mostrado um teorema muito importante da álgebra de corpos e fundamental para o estudo de seqüências.

Teorema B.1.1 *Se p for primo, D* mod *p é um corpo.*

Considere um elemento $m \in D$ não necessariamente primo. Define-se uma relação de equivalência "≡" como $a \equiv b \,(\text{mod}\, m)$ se e somente se $m|(a - b)$, ou seja, se a for congruente com b módulo m. Verifica-se que a relação definida é realmente uma relação de equivalência, pois são verificadas as três propriedades de equivalência completamente independentes:

1. Reflexividade: $a \equiv a$;
2. Simetria: $a \equiv b$ implica em $b \equiv a$;
3. Transitividade: $a \equiv b$ e $b \equiv c$ implica em $a \equiv c$.

onde essas três propriedades são completamente independentes.

Essa relação de equivalência, como qualquer outra relação de equivalência, divide o conjunto fundamental, nesse caso D, em subconjuntos disjuntos chamados classes[3] equivalentes. Se $a \in D$, denota-se $\overline{a}$ a única classe equivalente que contém a.

Exemplo B.1.1 *Seja D o conjunto dos inteiros e m* = 6*. Conforme a relação de*

[3] dá-se o nome classe a um grupo de objetos com alguma propriedade comum.

equivalência descrita anteriormente, existem seis classes equivalentes:

$$\begin{aligned}
\overline{0} &= \{0, \pm 6, \pm 12, \pm 18, ...\} \\
\overline{1} &= \{..., -17, -11, -5, 1, 7, 13, 19, ...\} \\
\overline{2} &= \{..., -16, -10, -4, 2, 8, 14, 20, ...\} \\
\overline{3} &= \{..., -15, -9, -3, 3, 9, 15, 21, ...\} \\
\overline{4} &= \{..., -14, -8, -2, 4, 10, 16, 22, ...\} \\
\overline{5} &= \{..., -13, -7, -1, 5, 11, 17, 23, ...\}
\end{aligned} \tag{B.3}$$

Note que a classe equivalente $\overline{1}$ poderia ser chamada de $\overline{7}$, $\overline{13}$, $\overline{-5}$, etc. Entretanto, costuma-se representar uma classe equivalente particular pelo seu menor elemento não-negativo. De fato, a notação $a \bmod m$ é comumente utilizada para representar o menor elemento não-negativo de $\overline{a}$.

Define-se adição de classe equivalente. como:

$$\overline{a} + \overline{b} = \overline{a + b} \tag{B.4}$$

e multiplicação, como:

$$\overline{a} \cdot \overline{b} = \overline{(a \cdot b)} \tag{B.5}$$

Para ilustrar, observe no exemplo que $\overline{1} + \overline{2} = \overline{3}$ e também $\overline{1} + \overline{2} = \overline{-5} + \overline{20} = \overline{15}$, pois $\overline{3} = \overline{15}$. Observa-se que o conjunto de classes equivalentes formam um anel. O anel, no contexto matemático, é definido como um conjunto S com duas operações binárias (comumente a adição e multiplicação) que satisfazem as condições:

1. Associativa para a adição: para todo a, b e $c \in S$, $(a + b) + c = a + (b + c)$;
2. Comutativa para a adição: para todo a e $b \in S$, $a + b = b + a$;
3. Identidade para a adição: existe um elemento $0 \in S$ tal que para todo $a \in S$, $a + 0 = 0 + a = a$;
4. Inversibilidade para a adição: para todo $a \in S$, existe um elemento $-a \in S$ tal que, $a + (-a) = (-a) + a = 0$;
5. Associativa para a multiplicação: para todo a, b e $c \in S$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

6. Distributiva: para todo a, b e $c \in S$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ e $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

A identidade para a adição é dada por:

$$\overline{0} = \{x \in D : x \equiv 0 \,(\mathrm{mod}\, m)\} \tag{B.6}$$

e a identidade para a multiplicação por:

$$\overline{1} = \{x \in D : x \equiv 1 \,(\mathrm{mod}\, m)\} \tag{B.7}$$

onde 0 e 1 são as identidades da adição e multiplicação no domínio Euclidiano, respectivamente. Nesse caso, o anel é representado por $D \bmod m$. O exemplo B.1.1 mostrou que $Z \bmod 6$, sendo Z o conjunto dos números inteiros, é um anel com 6 elementos. Para $D \bmod m$ ser um corpo, deve existir, para qualquer $\overline{a} \neq \overline{0}$, um $\overline{b}$ tal que:

$$\overline{a} \cdot \overline{b} = \overline{1} \tag{B.8}$$

No exemplo B.1.1 não se verifica essa condição, portanto, não se pode ter um corpo. Porém, se m for um número primo p, $\overline{a} \neq 0$ significa que $p \nmid a$ (p não é fator de a). Se $p \in D$ é primo e $p \nmid a$, então p e a são primos relativos[4]. Isso é facilmente verificado. Seja d um divisor comum de p e a. Como p é primo, d deve ser a unidade ou um associado[5] de p. Como $p \nmid a$, nenhum associado de p pode dividir a, então d é a unidade. Conclui-se, portanto, que $\mathrm{mdc}(p, a) = 1$ e então existem elementos b e t em D tais que $ab + pt = 1$. Portanto, com $ab \equiv 1 \,(\mathrm{mod})\, p$ satisfazendo (B.8) e conforme o Teorema B.1.1, tem-se que $D \bmod p$ é um corpo.

A seguir, é apresentado um exemplo de corpo finito com $D = Z$, ou seja, o domínio Euclidiano será o conjunto dos números inteiros.

Exemplo B.1.2 *Seja $D = Z$ e $p = 5$. Tem-se $D \bmod p$ com 4 elementos (a partir de agora, chamar-se-á de elementos as classes equivalentes por questão de simplicidade*

[4] dois inteiros são primos relativos se não existe nenhum fator positivo comum exceto o 1.

[5] nas circunstâncias de p primo e $p \nmid a$, o associado de um elemento $x \in \{1, 2, 3, ..., p - 1\}$, denotado por x', é tal que $xx' \equiv a \,(\mathrm{mod}\, p)$.

de redação), os quais serão denotados por $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ *e* $\overline{5}$.

$$\begin{aligned}
\overline{0} &= \{0, \pm 5, \pm 10, \pm 15, ...\} \\
\overline{1} &= \{..., -14, -9, -4, 1, 6, 11, 16, ...\} \\
\overline{2} &= \{..., -13, -8, -3, 2, 7, 12, 17, ...\} \\
\overline{3} &= \{..., -12, -7, -2, 3, 8, 13, 18, ...\} \\
\overline{4} &= \{..., -13, -6, -1, 4, 9, 14, 19, ...\}
\end{aligned} \tag{B.9}$$

A aritmética sobre o corpo é da forma:

$$\overline{4} + \overline{3} = \overline{2},\ \overline{2} \cdot \overline{3} = \overline{1},\ etc. \tag{B.10}$$

Para encontrar o inverso de um elemento basta aplicar o algoritmo de Euclides (MCELIECE, 1987). O algoritmo de Euclides é utilizado para obter o mdc(a, b) e combinações lineares de a e b que resultam em um outro elemento específico.

Em sua versão estendida, o algoritmo compreende as equações de recorrência:

$$\begin{aligned}
r_{i-2} &= q_i r_{i-1} + r_i \\
s_i &= s_{i-2} - q_i s_{i-1} \\
t_i &= t_{i-2} - q_i t_{i-1}
\end{aligned} \tag{B.11}$$

onde q_i é o quociente da divisão de r_{i-2} por r_{i-1} e r_i o resto. O algoritmo é realizado até $r_{n+1} = 0$ e, nesse ponto, tem-se $r_n = \text{mdc}(a, b)$. As outras variáveis s_i e t_i relacionam-se com a e b através da equação:

$$s_i a + t_i b = r_i \tag{B.12}$$

As condições iniciais para o algoritmo são:

$$\begin{aligned}
s_{i-1} &= 1,\ s_0 = 0 \\
t_{i-1} &= 0,\ t_0 = 1
\end{aligned} \tag{B.13}$$

Para aplicar o algoritmo na determinação do inverso de $\overline{3}$ do Exemplo B.1.2, faz-se $a = p = 5$ e $b = 3$. Assim:

i	s_i	t_i	r_i	q_i
-1	1	0	5	-
0	0	1	3	-
1	1	-1	2	1
2	-1	2	1	1
3	2	-3	1	1
4	-3	5	0	1

(B.14)

Tem-se o ponto de parada do algoritmo em $i = 4$, pois $r_4 = 0$, assim, $r_3 = 1 = \text{mdc}(5, 3)$. Da linha $i = 2$ obtém-se a expressão $2 \cdot 3 - 1 \cdot 5 = 1$. Então, $\overline{2} \cdot \overline{3} = \overline{1}$, ou seja, $(\overline{3})^{-1} = \overline{2}$. Observe que $\overline{3} \cdot \overline{2} = \overline{6} = \overline{1}$, conforme (B.9), e, portanto, o inverso de $\overline{3}$ é realmente $\overline{2}$.

O algoritmo de Euclides é um método sistemático para a obtenção do máximo divisor comum entre dois elementos e também para a obtenção de combinações lineares para determinar, por exemplo, o inverso de um elemento. No exemplo B.1.2 o corpo é reduzido, então, não se faz necessário utilizar o algoritmo de Euclides para determinar o inverso de elementos. Como um corpo do tipo $Z \bmod p$ possui p elementos, onde p é primo e existem infinitos números primos, a determinação do inverso de um elemento pode ser uma tarefa exaustiva, caso não seja utilizado um método sistemático.

O corpo finito $D \bmod p$ com p elementos anteriormente denotado por F_p é também comumente denotado por $GF(p)$.

O exemplo a seguir irá introduzir a construção de corpos finitos $D \bmod p$ quando D é o conjunto de polinômios no indeterminado x com coeficientes no corpo finito $F_p = Z \bmod p$. Esse tipo de construção é fundamental para o entendimento de corpos finitos, pois todo corpo finito pode ser construído dessa forma.

Exemplo B.1.3 *Seja $D = F_2[x]$ e $p(x) = x^3 + x + 1$. Construir-se-á um corpo F composto por polinômios sobre F_p. Observe que $p(x)$ é irredutível. Inicialmente, calcula-se potências de x módulo $p(x) = x^3 + x + 1$:*

$$\begin{aligned}
x^0 &\equiv 1 && \bmod x^3 + x + 1 \\
x^1 &\equiv x && \bmod x^3 + x + 1 \\
x^2 &\equiv x^2 && \bmod x^3 + x + 1 \\
x^3 &\equiv x + 1 && \bmod x^3 + x + 1 \\
x^4 &\equiv x^2 + x && \bmod x^3 + x + 1 \\
x^5 &\equiv x^3 + x^2 \equiv x^2 + x + 1 && \bmod x^3 + x + 1 \\
x^6 &\equiv x^3 + x^2 + x \equiv x^2 + 1 && \bmod x^3 + x + 1 \\
x^7 &\equiv x^3 + x \equiv 1 && \bmod x^3 + x + 1
\end{aligned} \tag{B.15}$$

Por questões de simplicidade de notação, representa-se as classes equivalentes (elementos) do corpo $\overline{x}$ *por* α*. Assim, tem-se os elementos do corpo:*

$$\begin{aligned}
\alpha^0 &= 1 \\
\alpha^1 &= x \\
\alpha^2 &= x^2 \\
\alpha^3 &= x + 1 \\
\alpha^4 &= x^2 + x \\
\alpha^5 &= x^2 + x + 1 \\
\alpha^6 &= x^2 + 1 \\
\alpha^7 &= 1
\end{aligned} \tag{B.16}$$

Observe que as 7 *primeiras potências de* α *são distintas em* $GF(8)$*. Como existem* 7 *elementos não nulos em* $GF(8)$*, conforme (B.1), tem-se que todos os elementos não nulos de* $GF(8)$ *são potências de* α*. Verifica-se que o Teorema B.1.1 "transforma" o espaço vetorial tridimensional sobre* F_2 *em um corpo finito, podendo-se representar* $\alpha = [010]$*, onde* $\alpha^k = a\alpha^2 + b\alpha + 1 = [abc]$*.*

As operações $+$ *e* $\cdot$ *são realizadas da forma convencional:*

$$\begin{aligned}
\alpha^3 \cdot \alpha^6 &= \alpha^{3+6} = \alpha^9 = \alpha^2 = [100] \\
\alpha^3 + \alpha^6 &= \alpha + 1 + \alpha^2 + 1 = \alpha^2 + \alpha = \alpha^4 = [110]
\end{aligned} \tag{B.17}$$

A seguir, serão definidos alguns conceitos básicos relacionados à corpos importantes para o estudo de seqüências. Tais conceitos são: raiz primitiva, polinômio mínimo, polinômio primitivo, recorrência linear e polinômio característico.

B.1.4 Raiz primitiva

Um gerador de um grupo cíclico[6] $F^* = F - \{0\}$, é chamado uma raiz primitiva do corpo F.

Exemplo B.1.4 *Considere o corpo do Exemplo B.1.2,* $F_5 = Z \bmod 5$*, cujos elementos são* $\{0, 1, 2, 3, 4\}$*. Verifica-se que o elemento* 2 *é uma raiz primitiva de* F_5*, pois* $2^0 = 1$*,* $2^1 = 2$*,* $2^2 = 4$ *e* $2^3 = 3$*, ou seja, as potências* 0*,* 1*,* 2 *e* 3 *do elemento gerador* 2 *formam um grupo cíclico. O elemento* 3 *também é raiz primitiva de* F_5*, pois* $3^0 = 1$*,* $3^1 = 3$*,* $3^2 = 4$ *e* $3^3 = 2$*. Por outro lado, o elemento* 4 *não é raiz primitiva de* F_5*, pois* $4^0 = 1$*,* $4^1 = 4$*,* $4^2 = 1$ *e* $4^3 = 4$*, ou seja, as n potências de* 4 *não formam um grupo cíclico.*

A ordem de um grupo representa o número de elementos que esse compreende. A ordem de um elemento α, ord(α), é dado por t tal que $(\alpha^0, \alpha^1, \alpha^2, ..., \alpha^{t-1})$ são todos distintos.

Do Exemplo B.1.4 tem-se que a ordem dos elementos geradores do grupo cíclico α é ord(2) = ord(3) = 5.

Um Lema bastante útil no estudo de seqüências é enunciado a seguir:

Lema B.1.1 *Se a ordem do elemento* α *é* $\text{ord}(\alpha) = t$*, então* $\text{ord}(\alpha^i) = t/\text{mdc}(i, t)$.

Segue a prova. Um resultado direto do Exemplo B.1.3 é que para qualquer $\beta \neq 0$ vale:

$$\beta^s = 1 \quad \text{se e somente se ord}(\beta)|s \tag{B.18}$$

O desenvolvimento da prova será separado em itens para facilitar o entendimento:

1. No Lema B.1.1, seja $\text{mdc}(i, t) = d$;
2. Observe que $(\alpha^i)^{(t/d)} = (\alpha^t)^{(i/d)}$ e, de (B.18), $(\alpha^t)^{(i/d)} = 1$. Diretamente de (B.18), tem-se que $\text{ord}(\alpha^i)|(t/d)$;

[6] dá-se o nome de grupo cíclico de ordem n ao grupo formado por seu gerador e suas n potências, tal que o gerador elevado à potência n é o objeto identidade.

3. Seja agora, do item anterior, $\text{ord}(\alpha^i) = s$, então, $\alpha^{is} = 1$ e, de (B.18), $\text{ord}(\alpha)|is$. Assim, do Lema B.1.1, tem-se $t|is$.

4. No item 1 foi assumido $d = \text{mdc}(i,t)$. Isso significa que $ia + tb = d$ para algum inteiro a e b. Multiplicando essa equação por s tem-se $isa + tsb = ds$. Como, do item anterior, $t|is$, segue-se que $t|ds$ também.

5. De outra forma do item anterior, $(t/d)|s$ e, do item 3, $(t/d)|\text{ord}(\alpha^i)$;

Assim, foi provado que tanto $\text{ord}(\alpha^i)|(t/d)$ como $(t/d)|\text{ord}(\alpha^i)$. Então, $\text{ord}(\alpha^i) = t/d$, como afirmado pelo Lema.

B.1.5 Polinômio mínimo e polinômio primitivo

Seja F um corpo finito com p^m elementos, onde p é um número primo. O corpo F pode ser visto como um espaço vetorial m-dimensional sobre o subcorpo F_p. Seja α um elemento arbitrário de F. Como F tem dimensão m sobre F_p, segue-se que os $m+1$ elementos, $\alpha^0, \alpha^1, \alpha^2, ..., \alpha^m$, devem ser linearmente dependentes sobre F_p. Então, devem existir $m+1$ elementos $A_0, A_1, ..., A_m$ de F_p, tais que:

$$A_0 + A_1\alpha + ... + A_m\alpha^m = 0 \tag{B.19}$$

Ou seja, se o polinômio $A(x) = A_0 + A_1x + ... + A_mx^m$, α é raiz da equação polinomial $A(x) = 0$. É claro que α pode satisfazer outras equações polinomiais de outros polinômios. Define-se $S(\alpha)$ como o conjunto de tais polinômios:

$$S(\alpha) = \{f(x) \in F_p(x) : f(\alpha) = 0\} \tag{B.20}$$

Seja $p(x)$ um polinômio não nulo de menor grau (denota-se grau(p)) de $S(\alpha)$ e $f(x)$ qualquer polinômio de $S(\alpha)$. Através da divisão polinomial, tem-se:

$$f(x) = q(x)p(x) + r(x), \quad \text{grau}(r) < \text{grau}(p) \tag{B.21}$$

Como $f(\alpha) = 0$, tem-se que $p(\alpha) = 0$ e $r(\alpha) = 0$. Então, se $r(x) \equiv 0$, conclui-se que grau(p) é mínimo, ou seja, o menor grau dos polinômios não nulos de $S(\alpha)$. Adicionalmente, verifica-se que $p(x)|f(x)$ para todo $f(x) \in S(\alpha)$. Chama-se, assim, $p(x)$

polinômio mínimo de α em relação ao corpo F. Se for definido que o coeficiente do monômio de maior grau de $p(x)$ deva ser 1 (ou seja, se $p(x)$ for um *monic polynomial*), tem-se que $p(x)$ de α é irredutível. Essa afirmação é clara, pois se for possível fatorar $p(x) = a(x)b(x)$, necessariamente $a(\alpha) = 0$ ou $b(\alpha) = 0$ e isso contradiz o grau mínimo de $p(x)$.

Dá-se o nome de polinômio primitivo ao polinômio mínimo $p(x)$ de α, sendo α uma raiz primitiva de F.

Para obter sistematicamente o polinômio mínimo de um elemento qualquer α, introduzir-se-á o conceito de conjugados de α em relação a um corpo F.

Seja F um corpo sobre o subcorpo com q elementos, F_p, onde p é primo. Os elementos de F são dados em potências de α. Nesse corpo estão contidos subcorpos K, assim como o F_p. Note-se que esses subcorpos podem ser muito maiores que F_p e menores que F.

Dá-se o nome de conjugados de α em relação ao subcorpo K aos elementos:

$$\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, ..., \alpha^{q^d} \tag{B.22}$$

onde d, chamado de grau de α e denotado por grau(α), é tal que $\alpha^{q^d} = \alpha$. Assim, tem-se que:

$$q^d \equiv 1 \bmod t \tag{B.23}$$

onde $t = \text{ord}(\alpha)$.

Se α é raiz de uma equação polinomial $p(x) = 0$, com $p(x) = p_0 + p_1 x + p_2 x^2 + ... + p_d x^d$, tem-se que:

$$\sum_{k=0}^{d} p_k \alpha^k = 0 \tag{B.24}$$

Fazendo $p(\alpha^q)$, tem-se:

$$0 = \left(\sum_{k=0}^{d} p_k \alpha^k \right)^q$$

$$\begin{aligned} &= \sum_{k=0}^{d} p_k^q \alpha^{qk} \\ &= \sum_{k=0}^{d} p_k (\alpha^q)^k \\ &= p(\alpha^q) \end{aligned} \tag{B.25}$$

ou seja, todos os conjugados de α são também raizes de $p(x)$, pois:

$$\begin{aligned} 0 &= \left(\sum_{k=0}^{d} p_k \alpha^k \right)^{q^j} \\ &= p(\alpha^{q^j}) \end{aligned} \tag{B.26}$$

Na equação (B.25) foi utilizada a propriedade:

$$(\alpha_1 + \alpha_2)^{p^k} = \alpha_1^{p^k} + \alpha_2^{p^k} \tag{B.27}$$

onde $k = 1, 2, 3, ...$

Essa é facilmente verificada para $k = 1$:

$$(\alpha_1 + \alpha_2)^p = \alpha_1^p + \binom{p}{1}\alpha_1^{p-1}\alpha_2 + ... + \binom{p}{p-1}\alpha_1\alpha_2^{p-1} + \alpha_2^p \tag{B.28}$$

onde, por definição:

$$\binom{p}{k} = \frac{p(p-1)...(p-k+1)}{k(k-1)...1} \tag{B.29}$$

Em (B.29), pode-se observar que o numerador é divisível por p, assim, em um corpo com característica p, todos os coeficientes de (B.27) serão equivalentes a zero. Assim, verifica-se a propriedade de (B.27) para $k = 1$. Para verificar a propriedade com $k > 1$, basta escrever $(\alpha_1 + \alpha_2)^{p^k}$ em produtos de $(\alpha_1 + \alpha_2)^p$ e utilizar o mesmo argumento de coeficientes equivalentes a zero.

Sabendo que todos os conjugados de α em relação ao subcorpo K são também raízes da mesma equação polinomial da qual α é raiz, tem-se que o polinômio mínimo de α em relação ao subcorpo K é dado por:

$$f_\alpha(x) = (x-\alpha)(x-\alpha^q)...(x-\alpha^{q^{d-1}}) \tag{B.30}$$

onde d é o grau de α, grau(α), em relação ao subcorpo K.

O exemplo a seguir mostra a construção de um corpo finito $GF(2^4)$. A construção será $D \bmod p$, onde $D = F_2[x]$ e $p(x) = x^4 + x + 1$. Isso significa que o domínio Euclidiano em questão é o conjunto de polinômios no indeterminado x, com coeficientes no corpo finito $F_2 = Z \bmod 2$, onde Z é o conjunto dos números inteiros.

Exemplo B.1.5 *Sejam $D = F_2[x]$ e $p(x) = x^4 + x + 1$. Para obter o corpo $D \bmod p$, denotado por $GF(2^4)$, primeiramente calcula-se as* 15 *primeiras potências de x módulo $p(x) = x^4 + x + 1$:*

$$\begin{aligned}
x^0 &\equiv 1 && \bmod x^4 + x + 1\\
x^1 &\equiv x && \bmod x^4 + x + 1\\
x^2 &\equiv x^2 && \bmod x^4 + x + 1\\
x^3 &\equiv x^3 && \bmod x^4 + x + 1\\
x^4 &\equiv x + 1 && \bmod x^4 + x + 1\\
x^5 &\equiv x^2 + x && \bmod x^4 + x + 1\\
x^6 &\equiv x^3 + x^2 && \bmod x^4 + x + 1\\
x^7 &\equiv x^4 + x^3 \equiv x^3 + x + 1 && \bmod x^4 + x + 1\\
x^8 &\equiv x^4 + x^2 + x \equiv x^2 + 1 && \bmod x^4 + x + 1\\
x^9 &\equiv x^3 + x && \bmod x^4 + x + 1\\
x^{10} &\equiv x^4 + x^2 \equiv x^2 + x + 1 && \bmod x^4 + x + 1\\
x^{11} &\equiv x^3 + x^2 + x && \bmod x^4 + x + 1\\
x^{12} &\equiv x^4 + x^3 + x^2 \equiv x^3 + x^2 + x + 1 && \bmod x^4 + x + 1\\
x^{13} &\equiv x^4 + x^3 + x^2 + x \equiv x^3 + x^2 + 1 && \bmod x^4 + x + 1\\
x^{14} &\equiv x^4 + x^3 + x \equiv x^3 + 1 && \bmod x^4 + x + 1\\
x^{15} &\equiv x^4 + x \equiv 1 && \bmod x^4 + x + 1
\end{aligned} \tag{B.31}$$

Voltando ao corpo $GF(2^4)$, representam-se as classes equivalente $\bar{x}$ por α. Então, da tabela de potências de x, obtém-se a tabela de potências de α e vetores de dimensão 4 *sobre $GF(2)$:*

$$
\begin{array}{ll}
\alpha^0 = 1 & 0001 \\
\alpha^1 = \alpha & 0010 \\
\alpha^2 = \alpha^2 & 0100 \\
\alpha^3 = \alpha^3 & 0011 \\
\alpha^4 = \alpha + 1 & 0110 \\
\alpha^5 = \alpha^2 + \alpha & 1100 \\
\alpha^6 = \alpha^3 + \alpha^2 & 1011 \\
\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1 & 0101 \\
\alpha^8 = \alpha^4 + \alpha^2 + \alpha = \alpha^2 + 1 & 1010 \\
\alpha^9 = \alpha^3 + \alpha & 0111 \\
\alpha^{10} = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1 & 1110 \\
\alpha^{11} = \alpha^3 + \alpha^2 + \alpha & 1111 \\
\alpha^{12} = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1 & 1101 \\
\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1 & 1101 \\
\alpha^{14} = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + 1 & 1001 \\
\alpha^{15} = \alpha^4 + \alpha = 1 & 0001
\end{array}
\tag{B.32}
$$

Observe que $\alpha^{15} = \alpha^0$ *(o grupo é cíclico), então* $\{\alpha^0, \alpha^1, ..., \alpha^{14}\}$ *são os* 15 *elementos não nulos de* $GF(2^4)$*.*

Agora, verificar-se-á se α^5 *é raiz primitiva de* $GF(2^4)$*, ou seja, se* α^5 *é um gerador do grupo cíclico* $GF(2^4)^* = GF(2^4) - \{0\}$*. Tomam-se as potências de* α^5*:*

i	$(\alpha^5)^i$
0	$\alpha^0 = 1$
1	α^5
2	α^{10}
3	$\alpha^{15} = \alpha^0$
4	$\alpha^{20} = \alpha^5$
5	$\alpha^{25} = \alpha^{10}$

(B.33)

Verifica-se que potências de α^5 *não geram o grupo cíclico* $GF(2^4)^*$*.*

De (B.33) tem-se que $(\alpha^5)^0$*,* $(\alpha^5)^1$ *e* $(\alpha^5)^2$ *são distintos e portanto a ordem de* α^5 *é* $\text{ord}(\alpha^5) = 3$*. Então,* α^5 *pertence ao subcorpo* $GF(2^2)$*, o qual contém* 3 *elementos não nulos. Além disso,* α^5 *é uma raiz primitiva do subcorpo* $GF(2^2)$*.*

Calcula-se, agora, o polinômio mínimo de α^5 *em* $GF(2^2)$. *Para tanto, deve-se obter o número de conjugados de* α^5. *O número de conjugados de* α, *ou o grau de* α, grau(α), *é facilmente obtido de (B.23):*

$$\begin{aligned} 2^d &\equiv 1 \bmod \text{ord}(\alpha^5) \\ 2^d &\equiv 1 \bmod 3 \\ d &= 2 \end{aligned} \tag{B.34}$$

Assim, tem-se que o grau de α^5 *é* grau(α^5) = d = 2. *Os conjugados de* α^5 *são:* α^5 *e* $(\alpha^5)^2$. *O elemento* $(\alpha^5)^{2^2} = (\alpha^5)^4 = \alpha^{20} = \alpha^5$ *não é contabilizado como conjugado de* α^5 *pois é um elemento equivalente à* α^5. *Esse resultado pode ser verificado em (B.33).*

O polinômio mínimo de α^5 *no subcorpo* $GF(2^2)$ *é dado por:*

$$\begin{aligned} f_{\alpha^5}(x) &= (x - \alpha^5)(x - (\alpha^5)^2) \\ f_{\alpha^5}(x) &= x^2 + x + 1 \end{aligned} \tag{B.35}$$

Esse polinômio é um polinômio mínimo de uma raiz primitiva do subcorpo $GF(2^2)$, *portanto, é um polinômo primitivo em* $GF(2^2)$.

Agora, será obtido o polinômio mínimo de α^4. *A ordem de* α^4 *é* 15, *pois* $(\alpha^4)^0$, $(\alpha^4)^1$, ..., $(\alpha^4)^{14}$, *são distintos:*

i	$(\alpha^4)^i$
0	$(\alpha^4)^0 = 1$
1	$(\alpha^4)^1 = \alpha^4$
2	$(\alpha^4)^2 = \alpha^8$
3	$(\alpha^4)^3 = \alpha^{12}$
4	$(\alpha^4)^4 = \alpha^1$
5	$(\alpha^4)^5 = \alpha^5$
6	$(\alpha^4)^6 = \alpha^9$
7	$(\alpha^4)^7 = \alpha^{13}$
8	$(\alpha^4)^8 = \alpha^2$
9	$(\alpha^4)^9 = \alpha^6$
10	$(\alpha^4)^{10} = \alpha^{10}$
11	$(\alpha^4)^{11} = \alpha^{14}$
12	$(\alpha^4)^{12} = \alpha^3$
13	$(\alpha^4)^{13} = \alpha^7$
14	$(\alpha^4)^{14} = \alpha^{11}$

(B.36)

Como a ordem de α^4 *é* $\text{ord}(\alpha) = 15$*, tem-se que* α^4 *é gerador do grupo cíclico de 15 elementos,* $GF(2^4)^*$.

O grau de α^4*,* $\text{grau}(\alpha)$*, é dado por (B.23):*

$$\begin{aligned} 2^d &\equiv 1 \bmod \text{ord}(\alpha^4) \\ 2^d &\equiv 1 \bmod 15 \\ d &= 4 \end{aligned} \tag{B.37}$$

Assim, tem-se que o grau de α^4 *é* $\text{grau}(\alpha^4) = d = 4$ *e seus* 4 *conjugados são:* $(\alpha^4)^{2^0} = \alpha^4$, $(\alpha^4)^{2^1} = (\alpha^4)^2$, $(\alpha^4)^{2^2} = (\alpha^4)^4$ *e* $(\alpha^4)^{2^3} = (\alpha^4)^8$.

O polinômio mínimo de α^4 *no subcorpo* $GF(2^4)$ *é dado por:*

$$\begin{aligned} f_{\alpha^4}(x) &= (x - \alpha^4)(x - (\alpha^4)^2)(x - (\alpha^4)^4)(x - (\alpha^4)^8) \\ f_{\alpha^4}(x) &= x^4 + x + 1 \end{aligned} \tag{B.38}$$

O polinômio obtido é um polinômio mínimo da raiz primitiva do corpo $GF(2^4)$, $D \bmod p$, *com* $D = F_2[x]$ *e* $p(x) = x^4 + x + 1$, *portanto, é um polinômo primitivo em* $GF(2^4)$.

Com a mesma metodologia, obtém-se o polinômio mínimo de α^8. *A ordem de* α^8 *é* $\text{ord}(\alpha^8) = 15$ *e o grau* $\text{grau}(\alpha^8) = 4$. *O polinômio mínimo:*

$$f_{\alpha^4}(x) = x^4 + x^3 + 1 \tag{B.39}$$

Novamente, o polinômio obtido é um polinômio mínimo da raiz primitiva do corpo $GF(2^4)$. *Porém, agora, o corpo* $GF(2^4)$ *é construído de* $D \bmod p$, *com* $D = F_2[x]$ *e* $p(x) = x^4 + x^3 + 1$. *Portanto,* $f_{\alpha^4}(x)$ *é um polinômo primitivo desse corpo* $GF(2^4)$.

B.1.6 Coconjuntos ciclotômicos

O conjunto dos números inteiros de 1 a p, $\{1, 2, 3, 4, ..., p\}$, primos relativos a p formam um grupo sob a multiplicação módulo p. A função de Euler $\phi(p)$ denota o número de primos relativos a p pertencentes ao conjunto $\{1, 2, ..., p\}$. Se p é impar, é claro que $\{1, 2, 4, 8, ...\}$ forma um subgrupo daquele grupo. No caso de $p = 2^m - 1$, o subgrupo é composto de m elementos:

$$\{1, 2, 4, 8, ..., 2^{m-1}\} \tag{B.40}$$

Um coconjunto é obtido multiplicando (módulo p) todos os elementos do subgrupo por qualquer elemento do conjunto dos números inteiros de 1 a p. Por exemplo, para $p = 15$, o subgrupo (B.40) é $\{1, 2, 4, 8\}$. Os coconjuntos desse subgrupo são:

$$\begin{array}{lllll} C_0: & 0 & & & \\ C_1: & 1 & 2 & 4 & 8 \\ C_2: & 3 & 6 & 12 & 9 \\ C_3: & 5 & 10 & & \\ C_4: & 7 & 14 & 13 & 11 \end{array} \tag{B.41}$$

Dos coconjuntos de um subgrupo, pelo menos um é impróprio e $\frac{\phi(p)}{m}$ são próprios. Coconjuntos impróprios são obtidos da multiplicação de cada um dos elementos do

subgrupo por um número que não é primo relativo a p. No exemplo, os coconjuntos C_0, C_2 e C_3 são impróprios e os demais são próprios. O conjunto de todos os coconjuntos (próprios e impróprios) de um subgrupo compõem os coconjuntos ciclotômicos.

Para o polinômio mínimo de um elemento $\alpha \in GF(2^m)$ ser de grau m e primitivo, deve-se ter $\text{ord}(\alpha) = 2^m - 1$, pois, nesse caso, de (B.23):

$$\begin{aligned} 2^d &\equiv 1 \bmod \text{ord}(\alpha) \equiv 1 \bmod (2^m - 1) \\ d &= m \end{aligned} \tag{B.42}$$

e, portanto, $\text{grau}(\alpha) = m$.

Do lema B.1.1, a ordem de $\beta = \alpha^r$ será $\text{ord}(\beta) = \text{ord}(\alpha^r) = \frac{\text{ord}(\alpha)}{\text{mdc}(r,\text{ord}(\alpha))}$. Assim, para o polinômio mínimo de α^r ser primitivo e de grau m, deve-se ter r e $2^m - 1$ primos relativos.

Então, o polinômio mínimo de α^r com $r \in C$, onde C é um coconjunto próprio, é primitivo e de grau m.

Observe que:

$$\begin{aligned} f_\alpha(x) &= (x-\alpha)(x-\alpha^2)...(x-\alpha^{2^{m-1}}) \\ &= (x-\alpha^2)(x-\alpha^2.2)...(x-\alpha^{2^{m-2}2})(x-\alpha^{2^{m-1}2}) \\ &= (x-\alpha^2)(x-\alpha^4)...(x-\alpha^{2^{m-1}})(x-\alpha) \\ &= f_\alpha(x) \end{aligned} \tag{B.43}$$

Como os elementos c_i de um coconjunto são do tipo $c_i = 2^i c_0$, tem-se que para $r, s \in C$, o polinômio mínimo de α^r é igual ao polinômio mínimo de α^s.

Com as observações anteriores, tem-se que o número de polinômios primitivos de grau m é dado pelo número de coconjuntos próprios do subgrupo $\{1, 2, 4, 8, ..., 2^{m-1}\}$. Logo, o número de polinômios primitivos de grau m é dado por $\frac{\phi(p)}{m} = \frac{\phi(2^m-1)}{m}$.

B.1.7 Elemento primitivo

O elemento primitivo de um corpo distingue-se da raiz primitiva por não estar situado em um subcorpo. Ou seja, o elemento primitivo do corpo F forma uma base para o corpo F. No Exemplo B.1.5 foi visto que α^4 pertence ao corpo $GF(2^4)$ e é raiz primitiva do corpo $GF(2^2)$. Assim, α^4 não é elemento primitivo de $GF(2^4)$, em outras palavras, não forma uma base para $GF(2^4)$.

B.1.8 Função traço

A função traço, ou simplesmente traço, é uma ferramenta muito útil na álgebra de corpos finitos. Seja $F = GF(q^m)$ e $K = GF(q^n)$, F é um subcorpo de K. Se α é um elemento de K, seu traço em relação ao subcorpo F é definido como:

$$Tr_m^n(\alpha) = \sum_{i=0}^{\frac{n}{m}-1} \alpha^{q^{mi}} \tag{B.44}$$

É também utilizada algumas vezes, por conveniência, a notação $Tr_F^K(\alpha)$.

As principais propriedades do traço são:

1. $Tr_m^n(\alpha) \in GF(2^m)$. Para verificar a propriedade, mostrar-se-á que $Tr_m^n(\alpha)$ pertence à um grupo cíclico de ordem q^m, ou seja, $Tr_m^n(\alpha)^{q^m} = Tr_m^n(\alpha)$. Então, $Tr_m^n(\alpha)^{q^m} = (\alpha + \alpha^{q^m} + \alpha^{q^{2m}} + ... + \alpha^{q^{n-m}})^{q^m} = \alpha^{q^m} + \alpha^{q^{2m}} + ... + \alpha^{q^{n-m}} + \alpha^{q^n}$, porém, $\alpha^{q^n} = \alpha$, pois α é elemento de $GF(2^n)$. Assim, $Tr_m^n(\alpha)^{q^m} = Tr_m^n(\alpha)$.

2. $Tr(\alpha+\beta) = Tr(\alpha)+Tr(\beta)$. Essa propriedade é diretamente verificada por (B.27).

3. $Tr_m^n(\lambda\alpha) = \lambda Tr_m^n(\alpha)$ com $\lambda \in GF(2^m)$. Verificação:

$$\begin{aligned} Tr_m^n(\lambda\alpha) &= \sum_{i=0}^{\frac{n}{m}-1} (\lambda\alpha)^{q^m i} \\ &= \lambda\alpha + \lambda^{q^m}\alpha^{q^m} + \lambda^{q^2m}\alpha^{q^2m} + ... + \lambda^{q^{(\frac{n}{m}-1)m}}\alpha^{q^{(\frac{n}{m}-1)m}} \\ &= \lambda\alpha + \lambda\alpha^{q^m} + \lambda\alpha^{q^2m} + ... + \lambda\alpha^{q^{(\frac{n}{m}-1)m}} \\ &= \lambda(\alpha + \alpha^{q^m} + \alpha^{q^2m} + ... + \alpha^{q^{(\frac{n}{m}-1)m}}) \\ &= \lambda Tr_m^n(\alpha) \end{aligned} \tag{B.45}$$

4. $Tr_m^n(\alpha^q) = Tr_m^n(\alpha)$. Observe que $\alpha^{q^n} = \alpha$. Como α é raiz primitiva de $GF(2^n)$, o grau de α é n. Então:

$$\begin{aligned} Tr_m^n(\alpha^q) &= \alpha^q + \alpha^{q^2} + ... + \alpha^{q^{n-1}} + \alpha^{q^n} \\ &= \alpha^q + \alpha^{q^2} + ... + \alpha^{q^{n-1}} + \alpha \\ &= Tr_m^n(\alpha) \end{aligned} \tag{B.46}$$

Para simplificar a notação, será utilizado $Tr(\alpha)$, com $\alpha \in GF(2^n)$, para representar $Tr_1^n(\alpha)$.

B.1.9 Recorrência linear e polinômio característico

Chama-se de recorrência linear de ordem m a equação de recorrência da forma:

$$s_t = a_1 s_{t-1} + a_2 s_{t-2} + ... + a_m s_{t-m} \tag{B.47}$$

onde, por exemplo, $(s_0, s_1, s_2, ...)$ pode ser a seqüência dos números reais e $a_1, a_2, ..., a_m$ constantes reais quaisquer. Porém, será dada atenção ao caso em que (s_t) é uma seqüência de elementos de um corpo finito F e $a_1, a_2, ..., a_m$ elementos fixos também de F.

O polinômio característico da recorrência de (B.47) é definido como:

$$f(x) = x^m - a_1 x^{m-1} - a_2 x^{m-2} - ... - a_m \tag{B.48}$$

Um importante teorema para a obtenção de seqüências é enunciado a seguir:

Teorema B.1.2 *Se o polinômio característico (B.48) é irredutível e seus coeficientes estão em $GF(q)$, então para qualquer $\theta \in GF(q^m)$, a seqüência definida por:*

$$s_t = Tr_1^m(\theta \alpha^t) \tag{B.49}$$

satisfaz (B.47).

A prova do Teorema é imediata. Se α é uma raiz da equação polinomial $f(x) = 0$, onde $f(x)$ é o polinômio característico (B.48) com coeficientes em $GF(q)$, tem-se:

$$\alpha^m = \sum_{i=0}^{m} a_i \alpha^{m-i} \tag{B.50}$$

Utilizando essa expressão em (B.49), tem-se:

$$\begin{aligned} s_t &= Tr_m^n(\theta\alpha^{t-m}\alpha^m) \\ &= Tr_m^n(\theta\alpha^{t-m} \cdot \sum_{i=1}^{m} a_i\alpha^{m-i}) \\ &= \sum_{i=1}^{m} Tr_m^n(a_i\theta\alpha^{t-i}) \\ &= \sum_{i=1}^{m} a_i Tr_m^n(\theta\alpha^{t-i}) \\ &= \sum_{i=1}^{m} a_i s_{t-i} \end{aligned} \tag{B.51}$$

Então (B.47) é satisfeita. Isso mostra que seqüências podem ser geradas com o auxílio do traço de um elemento.

A recorrência linear (B.47) com (s_t) uma seqüência de elementos de $GF(2^m)$ com coeficientes $a_1, a_2, ..., a_m$ sobre $GF(2)$ pode ser implementada em circuito pelo registrador de deslocamento apresentado na figura B.1.

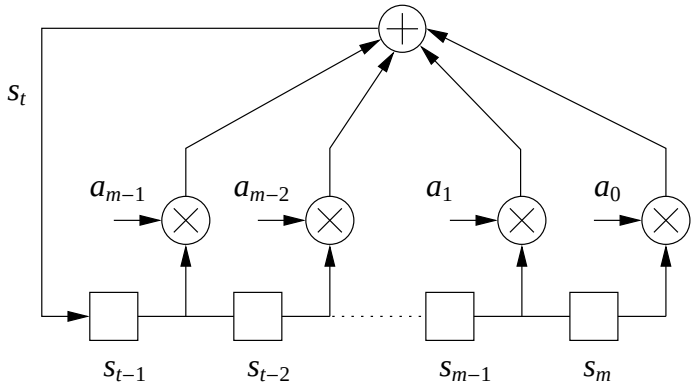

Figura B.1: Circuito que implementa a recorrência linear

Uma seqüência (s_t) tem período N, se:

$$s_{t+N} = s_t, \text{ para todo } t \geq 0 \tag{B.52}$$

onde N é o menor inteiro que satisfaz (B.52).

Se (s_t) é uma solução de (B.47) e o polinômio característico é irredutível, do Teorema B.1.2, $s_t = Tr_1^m(\theta\alpha^t)$ para algum $\theta \in GF(q^m)$. Se o período da seqüência for N:

$$\begin{aligned} Tr_1^m(\theta\alpha^{t+N}) &= Tr_1^m(\theta\alpha^t), \quad t \geq 0 \\ Tr_1^m(\theta\alpha^t(\alpha^N - 1)) &= 0, \quad t \geq 0 \end{aligned} \tag{B.53}$$

Isso ocorre somente se $\theta = 0$ ou $\alpha^N = 0$. No primeiro caso, tem-se $s_t = 0$ para todo t. No segundo caso tem-se (s_t) periódica com período N se e somente se a ordem de α dividir N. O menor N para o qual $s_{t+N} = s_t$ é $N = \text{ord}(\alpha)$. Então, no caso em que $f(x)$ é irredutível, o período da seqüência definida por (s_t), $s_t = Tr_1^m(\theta\alpha^t)$, é dado por $N = \text{ord}(\alpha)$. Esse é um importante Teorema:

Teorema B.1.3 *Se $f(x)$ é irredutível, então toda solução não nula de (B.47) tem período N, onde $N = \text{ord}(\alpha)$. De forma equivalente, N é o menor inteiro tal que $x^N \equiv 1 \pmod{f(x)}$.*

B.2 mdc$(2^e + 1, 2^m - 1)$

Para $1 \leq e \leq m$:

$$\text{mdc}(2^e + 1, 2^m - 1) = 1, \quad \text{se mdc}(2e, m) = \text{mdc}(e, m) \tag{B.54}$$

Segue a prova. Como $(2^e + 1)(2^e - 1) = 2^{2e} - 1$, tem-se que mdc$(2^e + 1, 2^m - 1)$ é fator de mdc$(2^{2e} - 1, 2^m - 1)$. Como mdc$(t^n - 1, t^m - 1) = t^{\text{mdc}(n,m)} - 1$, (MCELIECE, 1987), tem-se que mdc$(2^{2e} - 1, 2^m - 1) = 2^{\text{mdc}(2e,m)} - 1$ e, portanto:

$$\text{mdc}(2^e + 1, 2^m - 1) \mid 2^{\text{mdc}(2e,m)} - 1 \tag{B.55}$$

Considerando o caso de (B.54), mdc$(2e, m) =$ mdc(e, m), tem-se que:

$$\begin{aligned} \text{mdc}(2^e+1, 2^m-1) \mid 2^{\text{mdc}(2e,m)}-1 &= 2^{\text{mdc}(e,m)}-1 = \\ &= \text{mdc}(2^e-1, 2^m-1) \mid 2^e-1 \end{aligned} \quad \text{(B.56)}$$

Observe que 2^e+1 e 2^e-1 são números ímpares que diferem de duas unidades. Sejam $a = 2^e-1$ e $b = 2^e+1 = a+2$. Um divisor c de a maior que 1 deve ser ímpar, pois a é ímpar. Assim, um divisor de a não será um divisor de b, pois:

$$\begin{aligned} \frac{a}{c} &\in \mathbb{Z} \\ \frac{b}{c} &= \frac{a}{c} + \frac{2}{c} \end{aligned} \quad \text{(B.57)}$$

onde $\frac{2}{c} \notin \mathbb{Z}$, conseqüentemente, $\frac{b}{c} \notin \mathbb{Z}$. Então:

$$\text{mdc}(2^e+1, 2^e-1) = 1. \quad \text{(B.58)}$$

De (B.56) tem-se que $\text{mdc}(2^e+1, 2^m-1) \mid 2^e-1$. Como $\text{mdc}(2^e+1, 2^e-1) = 1$ (eq (B.57)), tem-se $\text{mdc}(2^e+1, 2^m-1) = 1$ quando $\text{mdc}(2e, m) = \text{mdc}(e, m)$.

O conteúdo deste apêndice encontra-se resumido em (MCELIECE, 1987).

B.3 Formas quadráticas sobre um corpo finito

Este apêndice descreve de forma detalhada alguns teoremas sobre formas quadráticas sobre um corpo finito apresentados em (MCELIECE, 1987).

Seja um corpo arbitrário F e $x_1, x_2, ..., x_{m-1}$ indeterminados sobre F. Uma forma quadrática sobre F é uma função de m variáveis $x_1, x_2, ..., x_m$ dada por:

$$Q(x_1, x_2, ..., x_m) = \sum_{i,j=1, i\leq j}^{m} a_{ij} x_i x_j \quad \text{(B.59)}$$

Uma forma quadrática é dita não singular se não puder ser transformada por uma mudança não singular de variáveis em uma forma com menos de m variáveis. Uma forma quadrática $Q(x_1, x_2, ..., x_m)$ representa zero se existe $(\xi_1, \xi_2, ..., \xi_m) \neq (0, 0, ..., 0)$

tal que $Q(\xi_1, \xi_2, ..., \xi_m) = 0$.

Considere uma forma quadrática que representa zero. Considere também qualquer transformação linear não singular da forma:

$$x_i \leftarrow \xi_i x_1 + ..., \quad i = 1, 2, ..., m \tag{B.60}$$

Aplicando essa transformação linear em (B.59):

$$\begin{aligned} Q(x_1, x_2, ..., x_m) &= \sum_{i,j=1,i\leq j}^{m} a_{ij} x_i x_j \\ &= a_{11}x_1^2 + a_{12}x_1x_2 + a_{23}x_2x_3 + ... + a_{mm}x_m^2 \\ &= a_{11}\xi_1\xi_1 x_1^2 + ... + a_{12}\xi_1\xi_2 x_1^2 + ... \\ &+ a_{23}\xi_2\xi_3 x_1^2 + ... + a_{mm}\xi_m\xi_m x_1^2 + ... \end{aligned} \tag{B.61}$$

ou seja, em cada termo da soma de (B.59), $\sum_{i,j=1,i\leq j}^{m} a_{ij}x_ix_j$, existe um termo do tipo $a_{ij}\xi_i\xi_j x_1^2$. Claramente, o coeficiente de x_1^2 será $\sum_{i,j=1,i\leq j}^{m} a_{ij}\xi_i\xi_j$. Como foi considerado que a forma quadrática representa zero:

$$Q(\xi_1, \xi_2, ..., \xi_m) = \sum_{i,j=1,i\leq j}^{m} a_{ij}\xi_i\xi_j = 0 \tag{B.62}$$

tem-se que o coeficiente de x_1^2 será zero e, portanto, Q é transformado na forma:

$$\begin{aligned} Q &= a'_{12}x_1x_2 + a'_{13}x_1x_3 + a'_{14}x_1x_4 + ... \\ &+ a'_{22}x_2^2 + a'_{23}x_2x_3 + a'_{24}x_2x_4 + ... \\ &+ a'_{33}x_3^2 + a'_{34}x_3x_4 + ... \end{aligned} \tag{B.63}$$

Observe que nem todos os a'_{1j} podem ser zero, ou Q seria uma função de somente $m - 1$ variáveis $x_2, x_3, ..., x_m$.

Então, aplicando-se as transformações lineares:

$$\begin{aligned} x_2 &\leftarrow \frac{1}{a'_{12}}(x_2 - a'_{13}x_3 - a'_{14}x_4 - ...) \\ x_i &\leftarrow x_i \qquad (i \neq 2) \end{aligned} \tag{B.64}$$

Q fica na forma:

$$\begin{aligned} Q &= x_1x_2 + a''_{22}x_2^2 + a''_{23}x_2x_3 + ... \\ &+ a'_{33}x_3^2 + ... \end{aligned} \tag{B.65}$$

Finalmente, aplicando-se as transformações lineares:

$$\begin{aligned} x_1 &\leftarrow x_1 - a''_{22}x_2 - a''_{23}x_3 - ... \\ x_i &\leftarrow x_i \qquad (i \neq 1) \end{aligned} \tag{B.66}$$

é obtido:

$$\begin{aligned} Q &= x_1x_2 + a'_{33}x_3^2 + ... \\ &= x_1x_2 + Q'(x_3, ..., x_m) \end{aligned} \tag{B.67}$$

É claro que Q' é não singular, pois, se fosse singular, poderia ser escrita como função de menos de $m-2$ variáveis. Assim, $Q = x_1x_2 + Q'$ implicaria que Q seria uma função de menos de m variáveis.

Com essa análise, foi provado um importante Teorema sobre formas quadráticas:

Teorema B.3.1 *Se Q é uma forma quadrática não singular como definido em (B.59) e representa zero, então, com uma transformação linear adequada, Q pode ser colocado na forma:*

$$Q = x_1x_2 + Q'(x_3, x_4, ..., x_m) \tag{B.68}$$

onde Q' é uma forma quadrática não singular em $x_3, x_4, ..., x_m$.

Continuando a realizar as transformações lineares como foram feitas até aqui,

pode-se estender o Teorema anterior para o Corolário:

Corolário B.3.1 *Com uma transformação linear adequada, qualquer forma quadrática não singular de m variáveis pode ser colocada na forma:*

$$Q = x_1x_2 + x_3x_4 + ... + x_{2s-1}x_2 2s + Q'(x_{2s+1}, ..., x_m) \tag{B.69}$$

onde Q' é uma forma não singular em $m - 2s$ *variáveis que não representa zero.*

Para a afirmação desse Corolário ser aplicável, deve-se obter em quais condições uma forma quadrática não representa zero. Em seguida, será enunciado o Teorema de Chevalley-Warning. Com esse Teorema, pode-se mostrar que, em um corpo finito, qualquer polinômio quadrático em 3 ou mais variáveis representam zero. Com isso, será possível identificar parte das condições para qual uma forma quadrática não representa zero.

Algumas definições formais de polinômios em várias variáveis sobre um corpo F seguem abaixo:

- Define-se monômio nos indeterminados $x_1, x_2, ..., x_m$ como a expressão da forma $\lambda x_1^{e_1} x_2^{e_2} ... x_m^{e_m}$, onde $\lambda \in F$ e os e_i são inteiros não negativos. O grau do monômio é dado pela soma dos e_i.
- Define-se polinômio nos indeterminados $x_1, x_2, ..., x_m$ como a soma de monômios. O grau do polinômio é dado pelo maior grau de seus monômios.

O Teorema de Chevalley-Warning é enunciado abaixo:

Teorema B.3.2 *Se* $F = GF(q)$*, onde q é uma potência do número primo p, e se* $f(x_1, x_2, ..., x_m)$ *é um polinômio de grau* $d < m$*, então o número de soluções* $N(f)$ *para:*

$$f(x_1, x_2, ..., x_m) = 0 \tag{B.70}$$

com $x_1, x_2, ..., x_m \in F$*, é divisível por p.*

Para cada m-upla $\mathbf{x} \in F^m$, tem-se:

$$1 - f(\mathbf{x})^{q-1} = \begin{cases} 1, & \text{se } f(\mathbf{x}) = 0 \\ 0, & \text{caso contrário.} \end{cases} \tag{B.71}$$

pois o corpo F possui q elementos, sendo assim, para qualquer elemento não nulo $x \in F$, tem-se $x^{q-1} = 0$. Somando todos $1 - f(\mathbf{x})^{q-1}$ sobre todos $\mathbf{x} \in F^m$, obtém-se o número de soluções $N(f)$:

$$\begin{aligned} \sum_{\mathbf{x}} (1 - f(\mathbf{x})^{q-1}) &= q^m - \sum_{\mathbf{x}} f(\mathbf{x})^{q-1} \\ &= -\sum_{\mathbf{x}} f(\mathbf{x})^{q-1} \bmod p \\ &= N(f) \bmod p \end{aligned} \tag{B.72}$$

Então, para provar o Teorema de Chevalley-Warning, basta provar que para qualquer polinômio de grau $< m$, tem-se:

$$\sum_{\mathbf{x} \in F^m} f(\mathbf{x})^{q-1} = 0 \tag{B.73}$$

O polinômio $f(\mathbf{x})^{q-1}$ possui grau $d(q-1)$, lembrando que d é o grau de $f(\mathbf{x})$, Teorema B.3.2. Assim, o polinômio $f(\mathbf{x})^{q-1}$ é uma combinação linear de monômios com graus menores ou iguais a $d(q-1)$. Se $m(\mathbf{x}) = x_1^{e_1} ... x_m^{e_m}$ for um desses monômios:

$$\sum_{\mathbf{x}} m(\mathbf{x}) = \prod_{i=1}^{m} \sum_{x \in F} x^{e_i} \tag{B.74}$$

Se houver algum $e_j = 0$:

$$\begin{aligned} \prod_{i=1}^{m} \sum_{x \in F} x^{e_i} &= \left(\prod_{i=1, i \neq j}^{m} \sum_{x \in F} x^{e_i} \right) \underbrace{(1 + 1 + ... + 1)}_{\text{soma de } q \text{ uns}} \\ &= 0 \end{aligned} \tag{B.75}$$

pois a soma de q uns resulta $(1 + 1 + ... + 1) = 0 \bmod p$.

Por outro lado, se nenhum $e_i = 0$, pelo menos um dos e_i estará na faixa $1 \leq e_i < q - 1$, pois $e_1 + ... + e_m \leq d(q-1) < m(q-1)$. Fazendo $x = \alpha$, uma raiz primitiva em

F, a soma $\sum_{x\in F} x^{e_i}$ será:

$$\sum_{j=0}^{q-2} \alpha^{je_i} = 1 + \alpha^{e_i} + \alpha^{2e_i} + ... + \alpha^{(q-2)e_i} \tag{B.76}$$

que é uma série geométrica. Desse modo:

$$\begin{aligned} \sum_{j=0}^{q-2} \alpha^{je_i} &= \frac{\alpha^{e_i(q-1)} - 1}{\alpha^{e_i} - 1} \\ &= \frac{1-1}{\alpha^{e_i} - 1} \\ &= 0 \end{aligned} \tag{B.77}$$

Portanto, em todos os casos a soma $\sum_{x\in F} x^{e_i}$ será zero, conseqüentemente, $f(\mathbf{x})^{q-1} = 0$. Então, $N(f) \bmod p = -\sum_{\mathbf{X}} f(\mathbf{x})^{q-1} = 0$, ou seja, o número de soluções $N(f)$ de $f(x_1, x_2, ..., x_m) = 0$ é divisivel por p, o que prova o Teorema B.3.2 de Chevalley-Warning.

Para qualquer forma quadrática $Q = \sum a_{ij}x_ix_j$ tem-se $Q(0, 0, ..., 0) = 0$. Uma forma quadrática é um caso particular de polinômio quadrático f. Então, com o Teorema B.3.2 de Chevalley-Warning, pode-se afirmar que $Q(\xi_1, \xi_2, ..., \xi_m) = 0$, com $m > 2$, para $N(f)$ casos diferentes de $(\xi_1, \xi_2, ..., \xi_m)$, com $N(f)$ divisível por p, onde p é a característica do corpo F. Então, existem pelo menos $p - 1$ vetores $(\xi_1, \xi_2, ..., \xi_m)$ para os quais $Q(\xi_1, \xi_2, ..., \xi_m) = 0$, além do $(0, 0, ..., 0)$. Com isso, segue o Corolário:

Corolário B.3.2 *Em qualquer corpo finito, uma forma quadrática com $m \geq 3$ variáveis representa zero.*

Com essa afirmação, a forma quadrática Q' do Corolário B.3.1, a qual não representa zero, deve ser de $m \leq 2$ variáveis.

Considerando apenas o corpo binário $GF(2)$, a forma quadrática $Q = \sum a_{ij}x_ix_j$, como definida anteriormente, terá $a_{ij} = 0$ ou 1. Assim, a única forma quadrática com $m = 1$ variável é:

$$Q_1(x) = x^2 \tag{B.78}$$

Pode-se observar que no corpo binário $GF(2)$ não faz sentido um elemento com expoente, x^2, pois, $1 \times 1 = 1$ e $0 \times 0 = 0$. Assim:

$$Q_1(x) = x \tag{B.79}$$

Claramente, $Q_1(x)$ não representa zero, pois $Q_1(x) = 0$ apenas para $x = 0$.

As formas quadráticas com $m = 2$ variáveis são:

$$\begin{aligned} Q_2(x) &= x^2 + xy = x + xy \\ Q_2'(x) &= x^2 + y^2 = x + y \\ Q_2''(x) &= xy + y^2 = xy + y \\ Q_2'''(x) &= x^2 + xy + y^2 = x + xy + y \end{aligned} \tag{B.80}$$

A forma quadrática $Q_2(x)$ representa zero, pois se $x = 1$ e $y = 1$, $Q_2(1,1) = 0$. A mesma observação vale para Q' e Q'', ou seja, $Q_2'(1,1) = 0$ e $Q_2''(1,1) = 0$. Somente $Q_2'''(x)$ é uma forma quadrática em $GF(2)$ que não representa zero.

Então, considerando o corpo binário $GF(2)$, tem-se do Corolário B.3.1, do Corolário B.3.2 e das observações anteriores que:

$$Q = x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + Q'(x_{2s+1}, ..., x_m) \tag{B.81}$$

onde Q' poderá ser:

- De 1 váriável para m ímpar, resultando em $Q' = Q_1(x) = x_m$ e $s = \frac{m-1}{2}$;
- De 2 variáveis para m par, resultando em $Q' = Q_2(x) = x_{m-1} + x_{m-1}x_m + x_m$ e $s = \frac{m-2}{2}$;
- Ou ainda para m par, $Q' = 0$ e $s = \frac{m}{2}$.

Com essa análise pode-se enunciar o Teorema:

Teorema B.3.3 *Toda forma quadrática não singular em m variáveis sobre* $GF(2)$ *pode*

ser escrita, com transformação linear das variáveis, como:

$$x_1x_2 + x_3x_4 + ... + x_{m-2}x_{m-1} + x_m \tag{B.82}$$

para m ímpar. Para m par, pode ser escrita como:

$$x_1x_2 + x_3x_4 + ... + x_{m-1}x_m \tag{B.83}$$

ou

$$x_1x_2 + x_3x_4 + ... + x_{m-1}x_m + x_{m-1} + x_m \tag{B.84}$$

Define-se *rank* de Q, dado por r, como o menor número de variáveis no qual Q pode ser expresso, através de transformações lineares não singulares de variáveis. Ou seja, $Q(x_1, x_2, ..., x_m) = Q'(x'_1, x'_2, ..., x'_r)$. Se Q for uma forma quadrática, é claro que Q' será também uma forma quadrática. Com essa definição e com o Teorema B.3.3, pode-se afirmar:

Corolário B.3.3 *Toda forma quadrática em m variáveis (singular ou não) sobre* $GF(2)$ *é equivalente a alguma das formas abaixo:*

$$\begin{aligned} x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + x_{2s+1} &\quad \text{(caso de } rank\, r = 2s+1\text{)} \\ x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} &\quad \text{(caso de } rank\, r = 2s\text{)} \\ x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + x_{2s-1} + x_{2s} &\quad \text{(caso de } rank\, r = 2s\text{)} \end{aligned} \tag{B.85}$$

onde $s = \lfloor r/2 \rfloor$.

Considere o caso:

$$Q(a_1 + b_1, a_2 + b_2, ..., a_m + b_m) = Q(a_1, a_2, ..., a_m) \tag{B.86}$$

Se o *rank* de Q for ímpar, conforme o Corolário B.3.3, Q pode ser transformado em $x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + x_{2s+1}$. Assim, (B.86) pode ser reescrito como:

$$\begin{aligned} &(a_1 + b_1)(a_2 + b_2) + (a_3 + b_3)(a_4 + b_4) + ... \\ &... + (a_{2s-1} + b_{2s-1})(a_{2s} + b_{2s}) + (a_{2s+1} + b_{2s+1}) = \\ &= a_1a_2 + a_2a_3 + ... + a_{2s-1}a_{2s} + a_{2s+1} \end{aligned}$$

$$(a_1b_2 + a_2b_1 + b_1b_2) + ...$$
$$... + (a_{2s-1}b_{2s} + a_{2s}b_{2s-1} + b_{2s-1}b_{2s}) + b_{2s+1} = 0 \quad \text{(B.87)}$$

para todo $(a_1, a_2, ..., a_m)$. Na condição particular de $(a_1, a_2, ..., a_m) = (0, 0, ..., 0)$, para que (B.87) seja verdade, tem-se necessariamente que:

$$b_1b_2 + ... + b_{2s-1}b_{2s} + b_{2s+1} = 0 \quad \text{(B.88)}$$

Combinando (B.88) e (B.87):

$$(a_1b_2 + a_2b_1) + ... + (a_{2s-1}b_{2s} + a_{2s}b_{2s-1}) = 0 \quad \text{(B.89)}$$

para todo $(a_1, a_2, ..., a_m)$. Isso ocorrerá se e somente se $b_1 = b_2 = ... = b_{2s} = 0$, que combinado com (B.88), resulta em $b_{2s+1} = 0$. Ou seja, o caso (B.86) só ocorre para todos $(a_1, a_2, ..., a_m)$ se e somente se $b_1 = b_2 = ... = b_{2s} = b_{2s+1} = 0$.

Existem exatamente 2^{m-2s-1} vetores $(0, 0, ..., 0, b_{2s+2}, b_{2s+3}, ..., b_m)$, com o *rank* de Q é igual a $r = 2s + 1$ (r um inteiro ímpar), tais que satisfazem a condição $b_1 = b_2 = ... = b_2s = b_{2s+1} = 0$ para que (B.86) ocorra.

Com a análise de (B.86) provou-se o Corolário:

Corolário B.3.4 *Se $Q(x_1, x_2, ..., x_m)$ é uma forma quadrática em $GF(2)$ com rank r, então o número de vetores $(b_1, b_2, ..., b_m)$ tais que:*

$$Q(a_1 + b_1, a_2 + b_2, ..., a_m + b_m) = Q(a_1, a_2, ..., a_m) \quad \text{(B.90)}$$

para todos os 2^m vetores $(a_1, a_2, ..., a_m)$ é 2^{m-r}.

Observa-se que para r par o Corolário não está provado, porém a metodologia é análoga à apresentada para r ímpar. Se r é par, Q pode ser transformado em $x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s}$ ou $x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + x_{2s-1} + x_{2s}$. Considerando o primeiro caso, Q de (B.86) torna-se:

$$(a_1 + b_1)(a_2 + b_2) + (a_3 + b_3)(a_4 + b_4) + ...$$

$$... + (a_{2s-1} + b_{2s-1})(a_{2s} + b_{2s}) =$$
$$= a_1a_2 + a_3a_4 + a_5a_6 + ... + a_{2s-1}a_{2s}$$

$$(a_1b_2 + a_2b_1 + b_1b_2) + ... + (a_{2s-1}b_{2s} + a_{2s}b_{2s-1} + b_{2s-1}b_{2s}) = 0 \quad \text{(B.91)}$$

para todo $(a_1, a_2, ..., a_m)$. Se $(a_1, a_2, ..., a_m) = (0, 0, ..., 0)$, de (B.91) tem-se:

$$b_1b_2 + b_3b_4 + ... + b_{2s-1}b_{2s} = 0 \quad \text{(B.92)}$$

Da expressão acima e (B.91) conclui-se, como anteriormente, que:

$$(a_1b_2 + a_2b_1) + ... + (a_{2s-1}b_{2s} + a_{2s}b_{2s-1}) = 0 \quad \text{(B.93)}$$

para todo $(a_1, a_2, ..., a_m)$. Ou seja, o caso (B.91), analogamente ao anterior, só ocorre para todos $(a_1, a_2, ..., a_m)$ se e somente se $b_1 = b_2 = ... = b_{2s} = 0$.

Analogamente ao caso de r ímpar, existem exatamente 2^{m-2s} vetores $(0, 0, ..., 0, b_{2s+1}, b_{2s+2}, ..., b_m)$, com o *rank* de Q igual a $r = 2s$ (r um inteiro par), tais que satisfazem a condição $b_1 = b_2 = ... = b_{2s} = 0$ para que (B.91) ocorra, o que está de acordo com o Corolário B.3.4.

Finalmente, para terminar a prova do Corolário B.3.4 deve-se ainda considerar o caso de r par e Q transformado em $x_1x_2 + x_3x_4 + ... + x_{2s-1}x_{2s} + x_{2s-1} + x_{2s}$. Considerando esse caso em (B.86), tem-se:

$$(a_1 + b_1)(a_2 + b_2) + (a_3 + b_3)(a_4 + b_4) + ...$$
$$... + (a_{2s-1} + b_{2s-1})(a_{2s} + b_{2s}) + (a_{2s-1} + b_{2s-1}) + (a_{2s} + b_{2s}) =$$
$$= a_1a_2 + a_3a_4 + a_5a_6 + ... + a_{2s-1}a_{2s}$$

$$(a_1b_2 + a_2b_1 + b_1b_2) + ... + (a_{2s-1}b_{2s} + a_{2s}b_{2s-1} + b_{2s-1}b_{2s}) + b_{2s-1} + b_{2s} = 0 \quad \text{(B.94)}$$

Analogamente aos casos anteriores (r ímpar e r par) a condição de $(a_1, a_2, ..., a_m) = (0, 0, ..., 0)$ implica em $b_1 = b_2 = ... = b_{2s} = 0$. E dessa, conclui-se que:

$$(a_1b_2 + a_2b_1) + ... + (a_{2s-1}b_{2s} + a_{2s}b_{2s-1}) = 0 \tag{B.95}$$

para todo $(a_1, a_2, ..., a_m)$. Novamente, o caso (B.94), igualmente ao anterior, só ocorre para todos $(a_1, a_2, ..., a_m)$ se e somente se $b_1 = b_2 = ... = b_{2s} = 0$.

Então, existem exatamente 2^{m-2s} vetores $(0, 0, ..., 0, b_{2s+1}, b_{2s+2}, ..., b_m)$, com o *rank* de Q igual a $r = 2s$ (r um inteiro par), tais quais satisfazem a condição $b_1 = b_2 = ... = b_2s = 0$ para que (B.94) ocorra. Assim, está provado o Corolário B.3.4.

Apêndice C – Seqüências polifásicas

C.1 Família LCZ-GMW polifásica

As seqüências LCZ-GMW polifásicas foram propostas em (TANG; FAN, 2001b). O algoritmo de construção dessas seqüências é semelhante aos apresentados na seção 2.1.6. A diferença resume-se em utilizar SMC sobre $GF(p)$ com $p \neq 2$ dada genericamente por $\{s_t\} = \{Tr_1^n(\alpha^t)\}$, onde α é elemento primitivo de $GF(p^n)$. Vale lembrar que p deve ser primo (seção B.1.3). As características de SMC sobre $GF(p)$ com $p \neq 2$, bem como as características de uma família LCZ-GMW polifásica não serão demonstradas aqui.

A função de correlação periódica par para seqüências $\mathbf{x} = \{x_0, x_1, ..., x_{N-1}\}$ e $\mathbf{y} = \{y_0, y_1, ..., y_{N-1}\}$, com x_i e $y_i \in GF(p)$, de uma família LCZ-GMW polifásica será:

$$\theta(\mathbf{x}, \mathbf{y}, \tau) = \begin{cases} N & \text{se } \tau = 0 \text{ e } \mathbf{x} = \mathbf{y} \\ p^{n-m} - 1 + p^{n-m}\theta(\mathbf{u}, \mathbf{v}, d) & \text{se } \tau = 0 \bmod \mathcal{T} \text{ e } \tau \neq 0 \\ -1 & \text{caso contrário} \end{cases} \tag{C.1}$$

onde $N = p^n - 1$ é comprimento das seqüências $\mathbf{x}$ e $\mathbf{y}$; $\mathbf{u}$ e $\mathbf{v}$ são formadas por SMC de comprimento $p^m - 1$; $\mathcal{T} = \frac{p^n-1}{p^m-1}$.

De (C.1) verifica-se que a zona de correlação reduzida será $L_{CZ} = \mathcal{T} - 1 = \frac{p^n-1}{p^m-1} - 1$.

Assim como para as seqüências LCZ-GMW binárias, não existe uma expressão para o número de seqüências em um conjunto LCZ-GMW, porém, o limite de Tang-Fan (1.98) é uma medida razoável:

$$K \leq \frac{N^2 - 1}{(L_{CZ} + 1)(N - 1)} \tag{C.2}$$

Em (TANG; FAN, 2001b) foi mostrado que, para $p = 3$, $m = 3$ e $n = 6$, têm-se $N = 728$, $L_{CZ} = 27$ e $K = 18$. A desigualdade (C.2) fornece $K < 26,0357$.

C.2 Família ZCZ quadrifásica

Seqüências ZCZ quadrifásicas[1], são obtidas com o mesmo método apresentado na seção 2.2.3 utilizando como sementes pares complementares quadrifásicos (FAN; HAO, 2000). A seguir são apresentados alguns exemplos (FAN; HAO, 2000):

$$\begin{aligned}
[X_0, Y_0] &= [0\ \ 3] \\
[X_0, Y_0] &= [010\ \ 002] \\
[X_0, Y_0] &= [010\ \ 002] \\
[X_0, Y_0] &= [01321\ \ 00013] \\
[X_0, Y_0] &= [0313210121\ \ 0301230303] \\
[X_0, Y_0] &= [0001200302031\ \ 0122212003203] \\
[X_0, Y_0] &= [012121232101032103030323 01\ \ 012121232101230321212101 23]
\end{aligned} \tag{C.3}$$

onde agora $-F = (F + 2) \bmod 4$.

As seqüências obtidas são $\mathbf{a}_i = \left\{\exp\left(\frac{\sqrt{-1}\pi a_{ij}}{2}\right)\right\} = \left\{W_4^{a_{ij}}\right\}$, onde a_{ij} são elementos da i-ésima linha e j-ésima coluna de F^n e $W_p = \exp\left(\frac{\sqrt{-1}2\pi}{p}\right)$. O conjunto de seqüências ZCZ quadrifásicas possui $N = 2^{2n+m-t+1}N_0$, onde N_0 é o comprimento de X_0 e Y_0, $K = 2^{n+1}$ e $Z_{CZ} \leq 2^{n+m-t-1}$.

C.3 Família PS

Foram propostos vários métodos de construção de conjuntos de seqüências polifásicas ortogonais generalizadas utilizando a matriz de transformada discreta de Fourier (*discrete Fourier transform*, DFT) (SUEHIRO; HATORI, 1988) (SUEHIRO, 1994) (SUEHIRO, 1996). Em (PARK et al., 2000) foi proposto também um conjunto de seqüências

[1] os chips pertencem ao conjunto $\{0, 1, 2, 3\}$

ortogonais denominado *Park-Park-Song-Suehiro (PS) sequence*. A função de autocorrelação periódica par fora da origem para essas seqüências assume valor zero, exceto em intervalos periódicos, e a função de correlação cruzada periódica par assume valor zero para qualquer atraso. Neste trabalho, não são derivadas as funções de correlação para esse conjunto. Será apenas apresentado o método de geração e algumas características.

C.3.1 Construção de uma família PS

A matriz DFT $N_F \times N_F$ com índice m é definida como:

$$F^{(N_F,m)} = \left[W_{N_F}^{-klm}\right] \tag{C.4}$$

onde m é um número natural; $k, l = 0, 1, .., N-1$ e $W_{N_F} = e^{\frac{2\pi j}{N_F}}$,com $j = \sqrt{-1}$.

A matriz diagonal $D(\{x_l\})$ da seqüência $\{x_l\}$ é definida como:

$$D(\{x_l\}) = diag(\{x_l\}) \tag{C.5}$$

As funções quociente *quo* e resíduo *res* são definidas como:

$$\begin{aligned} quo(\varsigma, \kappa) &= q \\ res(\varsigma, \kappa) &= r \end{aligned} \tag{C.6}$$

onde ς e q são inteiros, κ é um número natural, e $\varsigma = q\kappa + r$ com $r = 0, 1, ..., \kappa - 1$.

Definem-se os símbolos básicos como N_b símbolos κ_i, $i = 0, 1, ..., N_b - 1$, todos com mesma magnitude (sem perda de generalidade, pode-se assumir κ_i localizados no círculo unitário do plano complexo). Primeiramente uma seqüência é gerada a partir dos κ_i's. Para um conjunto $\{\kappa_i\}$, e $1 \leq m \leq N_b - 1$, define-se a matriz de seqüência básica ortogonal G de dimensão $N_b \times N_b$ como:

$$G = F^{(N_b,-m)} D(\{\kappa_i\}) \tag{C.7}$$

Genericamente, uma seqüência básica ortogonal $\{g_p\}$ de comprimento N_b^2 é defi-

nida como:

$$\begin{aligned} g_p &= G_{Q(p,N_b),R(p,N_b)} \\ &= \beta_{R(p,N_b)} W_{N_b}^{Q(p,N_b)R(p,N_b)m} \end{aligned} \tag{C.8}$$

onde $p = 0, 1, ..., N_b^2 - 1$ e $G_{a,b}$ denota o elemento da a-ésima linha e b-ésima coluna. Utilizando a seqüência básica ortogonal $\{g_p\}$, obtém-se a matriz H de dimensão $N \times K$:

$$\begin{aligned} H &= [h_{i,k}] \\ h_{i,k} &= \sum_{p=0}^{N_b^2-1} g_p \delta(i - k - pK) \end{aligned} \tag{C.9}$$

onde $N = KN_b^2$, K é um número natural e δ função delta de Kronecker. A primeira coluna de H é composta de g_0 seguido por $K - 1$ zeros, g_1 seguido por $K - 1$ zeros, até $g_{N_b^2-1}$ seguido por $K - 1$ "0"s. As outras colunas de H possuem o vetor da primeira coluna deslocado.

Finalmente, a matriz de seqüência PS, PS, de dimensão $N \times K$ é definida como:

$$PS = [c_{l,k}] = \frac{1}{N_b} F^{(N,-1)} H \tag{C.10}$$

A seqüência $\{c_{l,k}\}$, com $l = 0, 1, ..., N - 1$, a qual é uma coluna de PS, é chamada de seqüência PS.

C.3.2 Características da família PS

O método de construção de seqüências PS apresentado aqui (método I de (PARK et al., 2000)) garante que a função de correlação cruzada periódica par será zero, independente do deslocamento e demais parâmetros utilizados na construção. O comprimento das seqüências será $N = KN_b^2$, onde N_b é um número inteiro maior que 1, o qual representa o número de símbolos básicos utilizados na construção, e K é igual ao número de seqüências disponíveis no conjunto PS. Diferentemente da função de correlação cruzada periódica par, a função de correlação cruzada periódica ímpar apresenta valores não-nulos, como ilustrado na figura C.1.

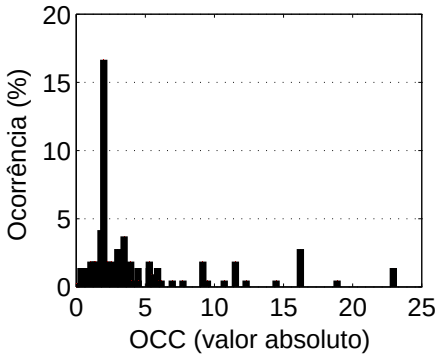

Figura C.1: Histograma da função de correlação cruzada ímpar no intervalo $|d| < N$ para o conjunto PS com $K = 4$ e $N_b = 3$. $N = 64$.

A relação entre o máximo número de seqüências e N será $\frac{\max\{K\}}{N} = \max\left\{\frac{1}{N_b^2}\right\} = \frac{1}{4}$ quando o número de símbolos básicos for mínimo, $N_b = 2$.

Em um conjunto de seqüências PS, a função de autocorrelação periódica par apresentará picos de magnitude N quando $\tau = iN_b^2$, $i = 0, 1, 2, ..., K-1$. Para os demais valores de τ, a função de autocorrelação periódica par assume valor zero. A característica indesejável dos picos de EAC, quando $\tau = iN_b^2$, com $i = 1, 2, ..., K-1$, pode ser amenizada, controlando-se o intervalo entre picos. Para tanto, deve-se obter um compromisso entre a distância entre os picos da função de EAC e $\frac{\max\{K\}}{N}$.

C.4 Família SP

Em (PARK et al., 2002), foi proposto um conjunto generalizado de seqüências polifásicas ortogonais denominado PS. A função de correlação cruzada periódica par assume valor zero, para qualquer argumento e a função de correlação cruzada periódica ímpar assume valor máximo de $\frac{N}{\pi}$, aproximadamente. No entanto, a função de autocorrelação periódica par $\theta(\mathbf{c}, \mathbf{c}, d)$ assume valor máximo para vários valores de d.

C.4.1 Construção de uma família SP

O conjunto SP $C = \{\mathbf{c}_k\}$, composto de K seqüências $\mathbf{c}_k$ de comprimento N, é definido como:

$$c_{k,l} = (-1)^l W_{K+1}^{lk} \tag{C.11}$$

onde $N = 2(K+1)$; $l = 0, 1, ..., N-1$; $W_K^l = W_K^{nK+l} = e^{j\frac{2\pi l}{K}}$ com n inteiro; K é um inteiro par.

Com algumas manipulações matemáticas, tem-se (PARK et al., 2002):

$$c_{k,l} = W_N^{p(l,k)} \tag{C.12}$$

onde $p(l,k) = 2lk + (K+1) \cdot \delta(R(l,2) - 1)$ sendo δ a função delta de Kronecker.

C.4.2 Características da família SP

O número de seqüências disponíveis em um conjunto SP é dado por $\frac{N-2}{2}$, conseqüentemente tem-se $\frac{\max\{K\}}{N} = \frac{\frac{N-2}{2}}{N} = \frac{1}{2} - \frac{1}{N}$, tendendo a $\frac{1}{2}$ à medida que o comprimento da seqüência aumenta.

A função de correlação cruzada periódica par para as seqüências PS é dada por (PARK et al., 2002):

$$\theta_{i,j}(\tau) = (-1)^\tau W_{K+1}^{-\tau i} \sum_{l=0}^{N-1} W_{K+1}^{l(i-j)}, \quad i \neq j \tag{C.13}$$

Observa-se que quando $i \neq j$ o somatório da equação (C.13) será zero se $(i-j) \in \{1, 2, ..., K-1\}$. Dessa forma, a função de correlação cruzada periódica par assume valor zero independente do valor de τ.

O máximo valor absoluto assumido pela função correlação cruzada periódica ímpar com $(i-j) = cte$ é dado por (PARK et al., 2002):

$$\begin{aligned} \Theta_{i,j} &= \max_\tau \left|\Theta_{i,j}(\tau)\right| \\ \left|\Theta_{i,j}(\tau)\right| &\leq 2 \left| \sum_{l=0}^{\tau_0 - 1} W_{K+1}^{l(i-j)} \right| \end{aligned} \tag{C.14}$$

onde $\tau_0 = \left\lfloor \frac{K}{2(j-i)} \right\rfloor + 1$; $\lfloor x \rfloor$ denota o maior inteiro igual ou menor que x. O maior

valor assumido pela função de correlação cruzada periódica ímpar para um conjunto SP, $\Theta_{máx} = \max_{i,j} \Theta_{i,j}$, ocorre quando $(i - j) = 1$ e nesse caso $\Theta_{máx} = \max_{\tau} \Theta_{i,j}(\tau) \cong \frac{N}{\pi}$ (PARK et al., 2002).

A função de autocorrelação periódica par para as seqüências SP é:

$$\theta_{i,i}(\tau) = N \times c_{(K-i+1),\tau}, \ 0 \leq \tau \leq N-1 \tag{C.15}$$

Esse resultado pode ser rapidamente verificado fazendo $i = j$ na equação (C.13):

$$\begin{aligned} \theta_{i,i}(\tau) &= (-1)^{\tau} W_{K+1}^{-\tau i} \sum_{l=0}^{N-1} W_{K+1}^{l(i-i)} = (-1)^{\tau} W_{K+1}^{-\tau i} N \\ &= (-1)^{\tau} W_{K+1}^{\tau(K+1-i)} N \end{aligned} \tag{C.16}$$

Comparando as equações (C.11) e (C.16) obtém-se (C.15).

De (C.15), tem-se $|\theta_{i,i}(\tau)| = N$, para qualquer valor de τ. Isso é um inconveniente para sistemas que operam em canal com multipercurso, pois a auto-interferência não será combatida.

A função de autocorrelação periódica ímpar das seqüências SP é dada por (PARK et al., 2002):

$$\Theta_{i,i}(\tau) = \frac{(N-2\tau)}{N} \theta_{i,i}(\tau), \ 0 \leq \tau \leq N-1 \tag{C.17}$$

De (C.15), tem-se $|\theta_{i,i}(\tau)| = N$ para qualquer valor de τ. Isso é um inconveniente para sistemas que operam em canal com multipercurso, pois a auto-interferência não será combatida quando símbolos de informação consecutivos forem iguais. Quando símbolos consecutivos forem diferentes, de (C.17) tem-se $|\Theta_{i,i}(\tau)| = |N - 2\tau|$, o qual também pode assumir valores elevados dependendo de τ.

Apêndice D – O sistema LAS-CDMA e as seqüências ternárias

O sistema LAS-CDMA (*large area synchronized-code division multiple access*) foi desenvolvido pela empresa LinkAir (LINKAIR, 2003) com o objetivo de aprimorar o desempenho do padrão de telefonia móvel celular cdma2000 (ZENG; ANNAMALAI; BHARGAVA, 2000). Existem perspectivas de adaptar esse novo sistema ao cdma2000 posicionando-o assim na geração 3,5 (3.5G) e quarta geração (4G) de telefonia móvel celular. Como o LAS-CDMA foi projetado para ser compatível com o IS-95 e com o cdma2000, a taxa de chip do LAS-CDMA é de $1,2288 Mchip/s$ e a banda ocupada para a transmissão é de $1,25 MHz$. O LAS-CDMA explora a característica de ortogonalidade das seqüências de espalhamento para minimizar as interferências MAI e SI e aumentar a capacidade do sistema CDMA. As famílias de seqüências utilizadas possuem uma zona de correlação aperiódica nula também chamada de janela livre de interferência (*interference free window*, IFW) (LI, 2003):

$$IFW = \\ = \max\{\mathcal{Z} : |C(\mathbf{u}, \mathbf{v}, d)| = 0, \text{ onde } (|d| \leq \mathcal{Z} \text{ e } \mathbf{u} \neq \mathbf{v}) \text{ ou } (0 < |d| \leq \mathcal{Z} \text{ e } \mathbf{u} = \mathbf{v})\} \tag{D.1}$$

onde **u** e **v** são as seqüências consideradas.

Observe que o conceito de IFW é diferente da ZCZ. A IFW refere-se à correlação aperiódica e a ZCZ refere-se à correlação periódica.

Uma família de seqüências, denominada LA, possui a função de reduzir a interferência entre células adjacentes. Outra família de seqüências, chamada de LS, é usada para o espalhamento, ou seja, para multiplexar os sinais dos usuários. A combinação

adequada das famílias LA e LS produz a família LAS, a qual é utilizada no sistema LAS-CDMA

O canal direto é síncrono por natureza e, portanto, a IFW será responsável por minimizar a auto-interferência. O canal reverso mantém quase sincronizados os sinais dos usuários. Assim, a IFW será responsável por minimizar a interferência de múltiplo acesso (MAI) e a auto-interferência (SI).

Se os atrasos entre os sinais dos usuários estiverem confinados em um intervalo que represente um deslocamento entre seqüências menor que a IFW, pode-se afirmar que as interferências MAI e SI serão totalmente eliminadas. Para que isso ocorra é necessário, além do sincronismo do canal reverso, ter um canal com espalhamento máximo multipercurso limitado.

As seções seguintes apresentarão as famílias LS, LA e LAS.

D.1 Família LS

A família LS é construída, assim como a família ZCZ (seção 2.2.3), a partir de seqüências complementares. Porém, as seqüências complementares utilizadas, nesse caso, são ternárias. Seqüências ternárias são compostas por três elementos: 0, -1 e 1. Para obter uma família LS são necessários dois pares ortogonais de seqüências complementares.

Seja $\{\mathbf{c}, \mathbf{s}\}$ um par de seqüências complementares. Em (GAVISH; LEMPEL, 1994) foram apresentados pares de seqüências ternárias complementares que possuem o mínimo de elementos 0. Esses resultados são apresentados na tabela D.1.

Sejam dois pares ortogonais de seqüências complementares $\{\mathbf{c}_1, \mathbf{s}_1\}$ e $\{\mathbf{c}_2, \mathbf{s}_2\}$ compostos por seqüências de comprimento N_1. Em (TSENG; LIU, 1972) foi mostrado que $\{\overline{\mathbf{s}}, -\overline{\mathbf{c}}\}$, onde $\overline{\mathbf{s}}$ representa a seqüência reversa de $\mathbf{s}$ (eq. (2.162)), será um par de seqüências complementares ortogonal ao par $\{\mathbf{c}, \mathbf{s}\}$. Então, adota-se $\{\mathbf{c}_2 = \overline{\mathbf{s}_1}, \mathbf{s}_2 = -\overline{\mathbf{c}_1}\}$. Seja também uma matriz $N_2 \times N_2$ ortogonal $H_{N_2 \times N_2}$. A tabela D.2 apresenta algumas matrizes ortogonais ternárias obtidas de (XU; LI, 2003). Obtém-se um conjunto de seqüências de comprimento $N_1 \cdot N_2$ a partir das linhas da matriz (XU; LI, 2003):

Tabela D.1: Pares complementares ótimos.

Comprimento das seqüências N_1	Número de zeros	Par complementar $\{\mathbf{c}, \mathbf{s}\}$
2	0	$\{++, +-\}$
3	1	$\{++-, -+0-\}$
4	0	$\{+++-, ++-+\}$
5	2	$\{++0+-, ++0-+\}$
6	2	$\{++-+0+, ++0-+\}$
7	4	$\{--+0-0-, --+0+0++-\}$
8	0	$\{------++-, --+++-+-+\}$
9	2	$\{+++-0++-+, +++-0--+-\}$
10	0	$\{+--+-+---+, +--------++-\}$
11	6	$\{+-+-000++-+, +-+-000--+-\}$
12	4	$\{+++-++00--+-, +++-00-++++-+\}$
13	≥ 4	$\{\}$
14	2	$\{++++-++--+-+0+, +++--+++-+--0-\}$

$$\begin{bmatrix} H_{N_2 \times N_2} \otimes \mathbf{c}_1 & H_{N_2 \times N_2} \otimes \mathbf{s}_1 \\ H_{N_2 \times N_2} \otimes \mathbf{c}_2 & H_{N_2 \times N_2} \otimes \mathbf{s}_2 \end{bmatrix} \tag{D.2}$$

onde $\otimes$ denota a operação produto de Kronecker (MEYER, 2000).

O conjunto obtido é composto por $K = 2N_2$ seqüências de comprimento $N = N_1 N_2$. Prova-se que esse conjunto obtido possui $IFW = N_1 - 1$.

Conforme (D.2) a seqüência referente à linha $i = (k_1 - 1)N_2 + \ell_1 - 1$, com $0 \leq k_1 \leq 1$ e $0 \leq \ell_1 \leq N_2 - 1$, será:

$$\begin{aligned} \{([c_{k_1,0}, c_{k_1,1}, ..., c_{k_1,N_1-1}] \cdot h_{\ell_1,0}, [c_{k_1,0}, c_{k_1,1}, ..., c_{k_1,N_1-1}] \cdot h_{\ell_1,1}, ... \\ ... [c_{k_1,0}, c_{k_1,1}, ..., c_{k_1,N_1-1}] \cdot h_{\ell_1,N_2-1}) \\ ([s_{k_1,0}, s_{k_1,1}, ..., s_{k_1,N_1-1}] \cdot h_{\ell_1,0}, [s_{k_1,0}, s_{k_1,1}, ..., s_{k_1,N_1-1}] \cdot h_{\ell_1,1}, ... \\ ... [s_{k_1,0}, s_{k_1,1}, ..., s_{k_1,N_1-1}] \cdot h_{\ell_1,N_2-1})\} \end{aligned} \tag{D.3}$$

e a seqüência referente à linha $j = (k_2 - 1)N_2 + \ell_2 - 1$, com $0 \leq k_2 \leq 1$ e $0 \leq \ell_2 \leq N_2 - 1$, será:

$$\begin{aligned} \{([c_{k_2,0}, c_{k_2,1}, ..., c_{k_2,N_1-1}] \cdot h_{\ell_2,0}, [c_{k_2,0}, c_{k_2,1}, ..., c_{k_2,N_1-1}] \cdot h_{\ell_2,1}, ... \\ ... [c_{k_2,0}, c_{k_2,1}, ..., c_{k_2,N_1-1}] \cdot h_{\ell_2,N_2-1}) \\ ([s_{k_2,0}, s_{k_2,1}, ..., s_{k_2,N_1-1}] \cdot h_{\ell_2,0}, [s_{k_2,0}, s_{k_2,1}, ..., s_{k_2,N_1-1}] \cdot h_{\ell_2,1}, ... \end{aligned}$$

$$... \left[s_{k_2,0}, s_{k_2,1}, ..., s_{k_2,N_1-1}\right] \cdot h_{\ell_2,N_2-1})\} \tag{D.4}$$

Por conveniência da análise, divide-se cada seqüência LS em duas partes: uma parte C, derivada das seqüências $\mathbf{c}_1$ e $\mathbf{c}_2$, e outra parte S, derivada das seqüências $\mathbf{s}_1$ e $\mathbf{s}_2$.

Define-se função de correlação aperiódica entre as seqüências LS $\{\mathbf{c}_i\mathbf{s}_i\}$ e $\{\mathbf{c}_j\mathbf{s}_j\}$ como:

$$C_{i,j}(\tau) = C(\mathbf{c}_i, \mathbf{c}_j, \tau) + C(\mathbf{s}_i, \mathbf{s}_j, \tau) \tag{D.5}$$

Assim, a função de correlação aperiódica $C_{i,j}(\tau)$, com $0 < \tau < N_1$, entre as seqüências LS definidas em (D.3) e (D.4), será:

$$\begin{aligned} C_{i,j}(\tau) &= \sum_{m=0}^{N_2-1} h_{\ell_1,m}h^*_{\ell_2,m} \sum_{n=0}^{N_1-\tau-1} c_{k_1,n}c^*_{k_2,n+\tau} + \sum_{m=0}^{N_2-2} h_{\ell_1,m}h^*_{\ell_2,m+1} \sum_{n=N_1-\tau}^{N_1-1} c_{k_1,n}c^*_{k_2,n+\tau-N_1} + \\ &+ \sum_{m=0}^{N_2-1} h_{\ell_1,m}h^*_{\ell_2,m} \sum_{n=0}^{N_1-\tau-1} s_{k_1,n}s^*_{k_2,n+\tau} + \sum_{m=0}^{N_2-2} h_{\ell_1,m}h^*_{\ell_2,m+1} \sum_{n=N_1-\tau}^{N_1-1} s_{k_1,n}s^*_{k_2,n+\tau-N_1} \\ &= C_{k_1,k_2}(\tau) \sum_{m=0}^{N_2-1} h_{\ell_1,m}h^*_{\ell_2,m} + C_{k_1,k_2}(-N_1+\tau) \sum_{m=0}^{N_2-2} h_{\ell_1,m}h^*_{\ell_2,m+1} \end{aligned} \tag{D.6}$$

Observe que $C_{k_1,k_2}(\tau) = 0$ e $C_{k_1,k_2}(-N_1 + \tau) = 0$, pois $\{\mathbf{c}_1, \mathbf{s}_1\}$ e $\{\mathbf{c}_2, \mathbf{s}_2\}$ foram escolhidos ortogonais, então, $C_{i,j}(\tau) = 0$.

Quando $\tau = 0$, tem-se:

$$C_{i,j}(0) = C_{k_1,k_2}(0) \sum_{m=0}^{N_2-1} h_{\ell_1,m}h^*_{\ell_2,m} \tag{D.7}$$

Se $k_1 \neq k_2$, tem-se $C_{k_1,k_2}(0) = 0$, pois, novamente, $\{\mathbf{c}_1, \mathbf{s}_1\}$ e $\{\mathbf{c}_2, \mathbf{s}_2\}$ escolhidos são ortogonais. Assim, tem-se $C_{i,j}(0) = 0$.

Se $\ell_1 \neq \ell_2$, tem-se $\sum_{m=0}^{N_2-1} h_{\ell_1,m}h^*_{\ell_2,m} = 0$, pois a matriz $H_{N_2\times N_2}$ é ortogonal. Então, $C_{i,j}(0) = 0$.

Quando $i = j$, tem-se $k_1 = k_2$ e $\ell_1 = \ell_2 = \ell$. Assim, $C_{i,i}(\tau) = C_{k,k}(0)|\mathbf{h}_\ell|^2$, onde $\mathbf{h}_\ell = \{h_{\ell,0}, h_{\ell,1}, ..., h_{\ell,N_2-1}\}$ com $0 \leq \ell \leq N_2 - 1$ é a ℓ-ésima linha da matriz ortogonal

$H_{N_2 \times N_2}$.

Como $C_{i,j}(-\tau) = C^*_{j,i}(\tau)$ (equação (1.45)), tem-se que $C_{i,j}(\tau)$, para $-N_1 < \tau < 0$, é igual a $C^*_{j,i}(\tau)$, para $0 < \tau < N_1$. Então, para verificar que $C_{i,j}(\tau) = 0$, para $-N_1 < \tau < 0$, basta seguir o procedimento anterior calculando $C^*_{j,i}(\tau)$, para $0 < \tau < N_1$.

Assim, verifica-se que $C_{i,j}(\tau) = 0$ para $0 < |\tau| < N_1$ exceto quando $i = j$. Nesse caso, $C_{i,i}(\tau) = C_{k,k}(0)|\mathbf{h}_\ell|^2$, onde $\mathbf{h}_\ell$ é a ℓ-ésima linha da matriz ortogonal $H_{N_2 \times N_2}$. Então o conjunto LS possui $IFW = N_1 - 1$.

O conjunto LS é comumente especificado por $(K, N, IFW) = (2N_2, N_1N_2, N_1 - 1)$.

Uma seqüência resultante da concatenação das partes C e S das seqüências LS não apresentará uma função de correlação dada por (D.5). Para que (D.5) ocorra, deve-se inserir zeros, também chamados de *gaps*, antes ou após as partes C e S, de forma que $C_{i,j}(\tau) = C(\mathbf{c}_i, \mathbf{c}_j, \tau) + C(\mathbf{s}_i, \mathbf{s}_j, \tau)$ para alguma faixa de valores de τ. Essa é a idéia da construção das seqüências LAS. Uma seqüência LA especifica como cada uma das partes C e S das seqüências LS e seus *gaps* devem estar posicionados para formar uma família LAS.

D.2 Famílias LA e LAS

As estações rádio base são distinguidas pelas seqüências LA. O LAS-CDMA utiliza um conjunto de 16 seqüências LA (BROOKS, 2002). Uma seqüência LA e uma família LS dão origem a uma família LAS utilizada para multiplexar os usuários em uma célula.

Uma seqüência LAS é obtida da concatenação de 17 pares C e S de uma seqüência LS juntamente com *gaps*, organizados conforme os intervalos definidos pela seqüência LA (ZHOU; LU, 2002). As outras seqüências LAS da mesma família são obtidas alterando-se a seqüência LS. Famílias diferentes de seqüências LAS são obtidas alterando-se as as seqüências LA (CONTI; GUNAWARDANA, 2003). Como existem 16 seqüências LA, obtém-se 16 famílias de seqüências LAS.

Cada seqüência LA pode ser entendida como um conjunto de intervalos de comprimentos distintos. Esses intervalos especificam como devem estar posicionadas as partes C e S das seqüências LS juntamente com os *gaps* para formar uma seqüência LAS. A figura D.1 exemplifica como são inseridos os *gaps* nas partes C e S das seqüências

LS. A figura D.2 mostra como é construída uma seqüência LAS.

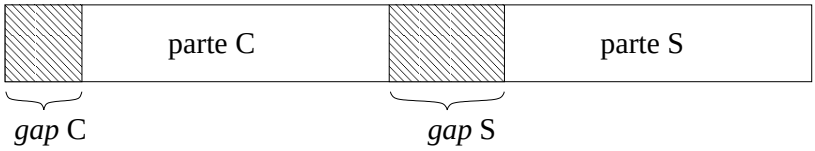

Figura D.1: Inserção de *gaps* nas partes C e S das seqüências LS

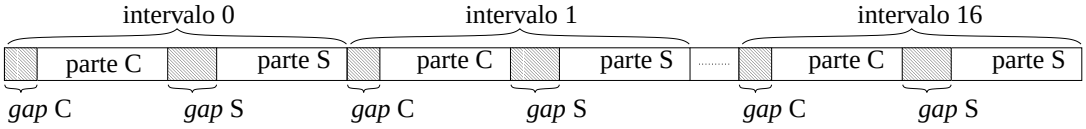

Figura D.2: Seqüência LAS

A tabela D.3 apresenta o tamanho de cada intervalo, dado em chips (ou elementos), para uma seqüência LA (ZHOU; LU, 2002). Essa seqüência foi obtida por meio de uma busca computacional exaustiva (BROOKS, 2002). Somando-se todos os intervalos da seqüência LA tem-se um total de 24576 chips. As outras 15 seqüências LA são geradas permutando-se os intervalos definidos para a seqüência LA da tabela D.3. A tabela D.4 apresenta através dos índices a permutação dos intervalos para formar as 16 seqüências LA (CONTI; GUNAWARDANA, 2003).

O sistema LAS-CDMA utiliza uma família de seqüências LS de 128 *chips*, sendo 64 na parte C e 64 na parte S. Essa família LS pode ser gerada conforme a seção D.1, com $N_1 = 4$ e $N_2 = 32$, resultando em uma família composta por $K = 64$ seqüências de comprimentos $N = 128$ e $IFW = 3$. Para formar uma seqüência LAS, cada intervalo da seqüência LA é preenchido com os 128 chips de uma seqüência LS restando chips zero (*gaps*). As outras seqüências LAS da família são obtidas utilizando-se as demais seqüências LS. Cada série de 128 *chips* das seqüências LS modulam um símbolo de informação.

A tabela D.5 especifica o tamanho do *gap* C e do *gap* S, ou seja, o número de zeros inseridos antes da parte C e antes da parte S, respectivamente, para cada um dos 17 pares C e S (ou intervalos da seqüência LA) (BROOKS, 2002). O menor *gap* é composto por 4 zeros, o qual, aliado à $IFW = 3$ das seqüências LS, garante-se para as seqüências LAS $IFW = 3$. Assim, a função de correlação aperiódica $C_{i,j}(\tau)$ entre seqüências LAS $\mathbf{c}_i$ e $\mathbf{c}_j$ de uma mesma família resultará zero para $|\tau| < 4$ e $i \neq j$ ou

$0 < |\tau| < 4$ e $i = j$. Devido a essa característica das seqüências LAS, o sistema LAS-CDMA elimina completamente a MAI e SI que seriam provocadas por sinais com atrasos menores ou iguais a 3 *chips*, em magnitude, em relação ao sinal de interesse.

Tabela D.2: Matrizes ortogonais ternárias.

N_2	Matrizes ortogonais $H_{N_2 \times N_2}$
1	$\begin{bmatrix} + \end{bmatrix}$
2	$\begin{bmatrix} + & + \\ + & - \end{bmatrix}$
3	$\begin{bmatrix} + & + & 0 \\ + & - & 0 \\ 0 & 0 & + \end{bmatrix}$
4	$\begin{bmatrix} + & + & + & - \\ + & - & + & + \\ + & + & - & + \\ + & - & - & - \end{bmatrix}$
5	$\begin{bmatrix} + & + & + & - & 0 \\ + & - & + & + & 0 \\ + & + & - & + & 0 \\ + & - & - & - & 0 \\ 0 & 0 & 0 & 0 & + \end{bmatrix}$
6	$\begin{bmatrix} + & + & + & - & 0 & 0 \\ + & - & + & + & 0 & 0 \\ + & + & - & + & 0 & 0 \\ + & - & - & - & 0 & 0 \\ 0 & 0 & 0 & 0 & + & + \\ 0 & 0 & 0 & 0 & + & - \end{bmatrix}$
7	$\begin{bmatrix} + & + & + & - & 0 & 0 & 0 \\ + & - & + & + & 0 & 0 & 0 \\ + & + & - & + & 0 & 0 & 0 \\ + & - & - & - & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & + & + & 0 \\ 0 & 0 & 0 & 0 & + & - & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & + \end{bmatrix}$
8	$\begin{bmatrix} + & + & + & - & + & - & + & + \\ + & + & - & + & + & - & - & - \\ + & - & + & + & + & + & + & - \\ + & - & - & - & + & + & + & - \\ + & + & + & - & - & + & - & - \\ + & + & - & + & - & + & + & + \\ + & - & + & + & - & - & - & + \\ + & - & - & - & - & - & + & - \end{bmatrix}$

Tabela D.3: Especificação de uma seqüência LA.

índice do intervalo	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
tamanho	136	138	140	142	144	146	148	150	152	154	156	158	160	162	164	172	137

Tabela D.4: Conjuntos de seqüências LA.

Seq. LA	índice do intervalo																
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	0	2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	0	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	0	4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	0	6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	0	7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	0	8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	0	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	0	10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	0	11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	0	12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	0	13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	0	14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	0	15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	0	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Tabela D.5: *Gaps* inseridos antes das 17 partes C e S das seqüências LS que compõem as seqüências LAS.

índice do intervalo	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
gap C	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	22	4
gap S	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	22	5

Apêndice E – Sistemas QS-CDMA com detecção multiusuário

Em canais com desvanecimento multipercurso, a interferência presente na saída de um correlacionador do detector Rake é composta pela MAI e pela auto-interferência (*self-interference*, SI). A SI, por sua vez, é composta de auto-interferência intersimbólica (*self intersymbol interference*, SII), provocada por componentes multipercurso correspondentes ao símbolo anterior, e auto-interferência de um mesmo símbolo (*self current-symbol interference*, SCI), provocada por componentes correspondentes ao símbolo corrente (WENG et al., 1999). O detector multiusuário (*multi-user-detector*, MuD), utiliza informações dos demais usuários ativos, além de outras estimativas, para cancelar a MAI e a SII presentes no sinal recebido. A SCI pode ser utilizada beneficamente na etapa combinação e decisão do símbolo. Dessa forma, há um aumento na capacidade dos sistemas de comunicação comparado à detecção convencional. Porém, a complexidade de implementação é maior.

O MuD do tipo cancelador de interferência paralelo (*paralell interference canceller*, PIC) (VARANASI; AAZHANG, 1990) (ABRÃO, 2001) (WENG et al., 1999) estima e subtrai a interferência simultânea e paralelamente para todos os usuários. Em um MuD PIC, o primeiro estágio é um banco de correlacionadores como o do detector Rake, os quais geram estimativas para os sinais de todos os usuários. No segundo estágio, a MAI e a SII são reconstruídas a partir das estimativas obtidas no estágio anterior e subtraídas do sinal recebido, produzindo o sinal do usuário de interesse adicionado à interferência residual, devido ao cancelamento imperfeito e ruído térmico. Esse processo pode ser repetido em múltiplos estágios, passando o sinal do usuário de interesse, mais a interferência residual, por um segundo banco de correlacionadores, e posterior cancelamento paralelo.

O cancelador de interferência com decisão abrupta (*paralell interference canceller*

with hard decision, PIC-HD) multiestágio descrito aqui remove a interferência a partir das estimativas da auto-interferência intersimbólica (SII) e da MAI em S estágios, figura E.1. No primeiro estágio, $s = 1$, as estimativas são obtidas das saídas dos correlacionadores, estágio $s = 0$. Considerando a modelagem da seção 1.1, a SII sobre o ℓ-ésimo componente multipercurso do k-ésimo usuário é obtida de (1.11) e (1.33) com $b^{(0)} = 0$:

$$SII_{k,\mathcal{L}} = \begin{cases} \sum_{\mathcal{L}=1}^{L} \sqrt{\frac{P}{2}} \alpha_{\mathcal{L}} b_k^{(-1)} \mathcal{R}_{k,k}(\tau_{k,\mathcal{L}}) cos(\phi_{k,\mathcal{L}}), & \text{para } \tau_{k,\mathcal{L}} \geq 0 \\ \sum_{\mathcal{L}=1}^{L} \sqrt{\frac{P}{2}} \alpha_{\mathcal{L}} b_k^{(1)} \tilde{\mathcal{R}}_{k,k}(\tau_{k,\mathcal{L}}) cos(\phi_{k,\mathcal{L}}), & \text{para } \tau_{k,\mathcal{L}} < 0 \end{cases} \tag{E.1}$$

A estimativa para a $SII_{k,\mathcal{L}}$, obtida no s-ésimo estágio de cancelamento, pode ser escrita como:

$$\widehat{SII}_{k,\mathcal{L}}(s) = \begin{cases} \sum_{\mathcal{L}=1}^{D} \sqrt{\frac{\hat{P}}{2}} \hat{\alpha}_{\mathcal{L}} \hat{b}_k^{(-1)}(s-1) \hat{\mathcal{R}}_{k,k}(\hat{\tau}_{k,\mathcal{L}}) cos(\hat{\phi}_{k,\mathcal{L}}), & \text{para } \hat{\tau}_{k,\mathcal{L}} \geq 0 \\ \sum_{\mathcal{L}=1}^{D} \sqrt{\frac{\hat{P}}{2}} \hat{\alpha}_{\mathcal{L}} \hat{b}_k^{(1)}(s-1) \hat{\tilde{\mathcal{R}}}_{k,k}(\hat{\tau}_{k,\mathcal{L}}) cos(\hat{\phi}_{k,\mathcal{L}}), & \text{para } \hat{\tau}_{k,\mathcal{L}} < 0 \end{cases} \tag{E.2}$$

onde D representa o número de correlacionadores do receptor para cada usuário, também chamado de diversidade Rake e cujos parâmetros a serem estimados para todos os usuários em um sistema real incluem: coeficiente de canal, $\hat{\alpha}$, potência, $\hat{P}$, atrasos, $\hat{\tau}$, (e portanto correlações, $\widehat{\mathcal{R}}$), fase, $\hat{\varphi}$, e os bits obtidos no estágio de cancelamento anterior, $\hat{b}^{(\cdot)}(s-1)$.

A estimativa para a MAI, $\hat{I}_{\ell,k}^{(i)}(s)$, obtidas no s-ésimo estágio de cancelamento pode ser escrita como:

$$\hat{I}_{k,\ell}(s) = \sum_{(u=1,\ u\neq k)}^{U} \sum_{\mathcal{L}=1}^{D} \sqrt{\frac{\hat{P}}{2}} \hat{\alpha}_{\mathcal{L}} \hat{J}_{u,\mathcal{L}}(s) cos(\hat{\phi}_{u,\mathcal{L}}) \tag{E.3}$$

onde:

$$\hat{J}_{u,\mathcal{L}}(s) = \begin{cases} \hat{b}_u^{(-1)}(s-1) \hat{\mathcal{R}}_{u,k}(\hat{\tau}_{u,\mathcal{L}}) + \hat{b}_u^{(0)}(s-1) \hat{\tilde{\mathcal{R}}}_{u,k}(\hat{\tau}_{u,\mathcal{L}}), & \text{para } \hat{\tau}_{u,\mathcal{L}} \geq 0 \\ \hat{b}_u^{(0)}(s-1) \hat{\mathcal{R}}_{u,k}(\hat{\tau}_{u,\mathcal{L}}) + \hat{b}_u^{(1)}(s-1) \hat{\tilde{\mathcal{R}}}_{u,k}(\hat{\tau}_{u,\mathcal{L}}), & \text{para } \hat{\tau}_{u,\mathcal{L}} < 0 \end{cases} \tag{E.4}$$

A saída do s-ésimo estágio PIC, considerando o ℓ-ésimo componente multipercurso do k-ésimo usuário para o bit de interesse, figura E.1, resulta:

$$\begin{aligned}\hat{z}_{k,\ell}(s) &= \hat{z}_{k,\ell}(0) - \widehat{SII}_{k,\ell}(s) - \hat{I}_{k,\ell}(s) \\ &= \sqrt{\tfrac{P}{2}}\alpha_\ell T b_k^{(0)} + SI_{k,\ell} - \widehat{SII}_{k,\ell}(s) + \\ &+ I_{k,\ell} - \hat{I}_{k,\ell}(s) + n_{k,\ell}\end{aligned} \tag{E.5}$$

Finalmente, realiza-se a combinação de razão máxima (MRC) para os sinais dos D correlacionadores, seguida da decisão abrupta:

$$\hat{y}_k(s) = \sum_{\ell=1}^{D} \Re\left\{\hat{z}_{k,\ell}(s)\hat{\alpha}_\ell\right\} \tag{E.6}$$

$$\hat{b}_k^{(0)}(s) = \operatorname{sign}\left(\hat{y}_k(s)\right) \tag{E.7}$$

A seguir são apresentadas algumas simulações de sistemas QS-CDMA de taxa única utilizando as seqüências binárias descritas anteriormente (WH, QS, Lin-Chang, LCZ e ZCZ).

E.1 Resultados Numéricos

Objetivando uma adequada comparação de desempenho entre os vários sistemas QS-CDMA, os conjuntos de seqüências utilizados nas simulações Monte-Carlo foram escolhidos de forma a resultar em carregamentos os mais similares possíveis. Para o conjunto Lin-Chang, foi adotado $m = 3$ e $n = 2m$. O polinômio primitivo utilizado para a construção do corpo $GF(2^6)$ foi $x^6 + x^5 + x^2 + x + 1$. No cálculo de desempenho, a cada iteração sorteiam-se quatro seqüências dentre as cinco disponíveis. No conjunto LCZ-GMW, adotou-se $p = 2$, $n = 6$, $m = 3$ e o polinômio primitivo $x^6 + x^5 + x^2 + x + 1$ para a construção do corpo $GF(2^6)$. Para o conjunto ZCZ foi adotado $m = 4$, $n = 1$ e $t = 1$, resultando em um conjunto de 4 seqüências de comprimento $N = 64$ e $Z_{CZ} = 9$. O conjunto de seqüências QS escolhido é derivado do conjunto $Gold(203, 277)$. Desse conjunto de Gold, obtém-se 4 subconjuntos compostos de 8 seqüências QS de comprimento $N = 127$ com propriedade $QOQS(5)$. Arbitrariamente escolheu-se o subconjunto Q_1, uma vez que todos os 4 subconjuntos apresentam propriedades de correlação similares. Para o WH foi adotado $N = 64$ sendo que no cálculo

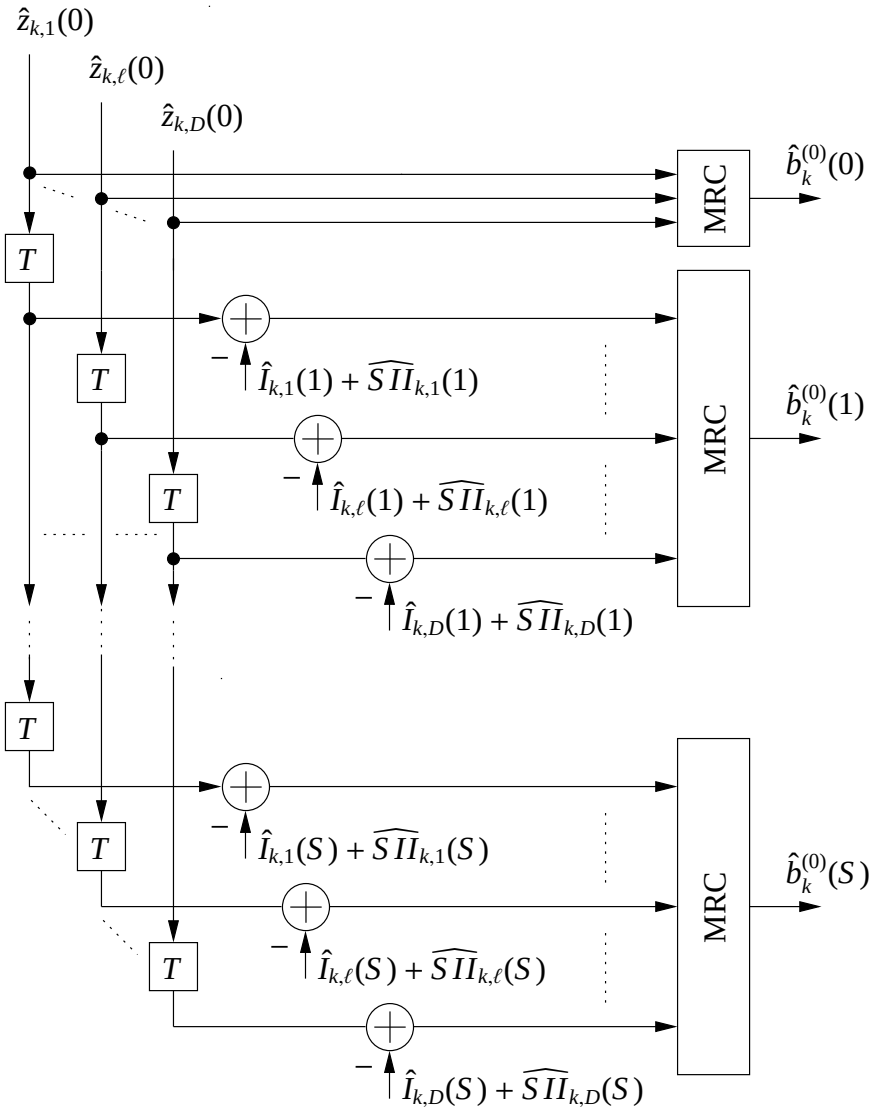

Figura E.1: Detector multiusuário PIC-HD pós-detecção.

de desempenho sorteiam-se 4 seqüências dentre as disponíveis em cada iteração.

A tabela E.1 sintetiza os principais parâmetros dos conjuntos de seqüências previamente escolhidos: o ganho de processamento N, o número de usuários ativos U no sistema, os valores máximos de $\theta_{i,j}(d)$ e $\Theta_{i,j}(d)$ com $0 \leq d < N$, o intervalo em que a função ECC é mantida mínima e o máximo erro de sincronismo, $\tau_{\max}$, sem ocorrer problemas de sincronismo.

A tabela E.2 mostra o perfil atraso-potência adotado para análise de desempenho em canal com desvanecimento Rayleigh multipercurso. Esse perfil, para ambiente urbano típico, foi baseado no estudo COST207 (STUBER, 2001) e possui um número

Tabela E.1: Características dos conjuntos de seqüências de espalhamento analisados.

Conjunto	N	U	$Load \simeq$	$\max\|\theta_{i,j}(d)\|$	$\max\|\Theta_{i,j}(d)\|$	$d\|\min\|\theta_{i,j}(d)\|$	$\tau_{\max}\ [T_c]$
WH	64	4	$0,0625$	64	32	0	< 1
Seqüência QS	127	8	$0,063$	17	45	$\|d\| \in [0;2]$	< 127
Lin-Chang	63	4	$0,063$	33	33	$\|d\| \in [1;8]$	< 63
LCZ-GMW	63	4	$0,063$	33	29	$\|d\| \in [0;8]$	< 63
ZCZ	64	4	$0,0625$	32	32	$\|d\| \in [0;8]$	< 64

reduzido de componentes multipercurso, visando amenizar a complexidade e o tempo de processamento computacional das simulações.

Tabela E.2: Perfil atraso-potência baseado no modelo COST207.

ℓ	**Atraso (Δ_ℓ)**	$\mathbb{E}\left\{\alpha_\ell^2\right\}$
3	$0T_c = 0s$	$0,189$
1	$1T_c = 0,260\mu s$	$0,379$
2	$2T_c = 0,520\mu s$	$0,239$
4	$6T_c = 1,562\mu s$	$0,095$
5	$9T_c = 2,343\mu s$	$0,061$
6	$19T_c = 4,947\mu s$	$0,037$

Nas simulações, foi considerado controle perfeito de potência. Foi considerada estimativa perfeita de fase, potência, atraso e coeficiente de canal para todos os sinais que chegam ao receptor. Considerou-se freqüência da portadora $f_c = 2GHz$, velocidade do móvel $v = 110\,km/h$, resultando numa freqüência Doppler máxima de $f_m = \frac{v}{\lambda_c} = 203,7Hz$, e diversidade Rake $D = 4$, pois com 4 *fingers* é possível capturar mais de 90% da energia total do sinal recebido. Os resultados de desempenho foram obtidos em termos de taxa de erro de bit (*bit error rate*, BER) média ($\overline{BER}$).

As figuras E.2 a E.6 apresentam os resultados de desempenho $\overline{BER} \times \frac{E_b}{N_0}$, onde $E_b = P \cdot T$, obtidos por simulação Monte-Carlo. Para as seqüências de comprimento $N = 63$ e $N = 64$, considerou-se $\tau_{\max} = 2T_c$ e, para a seqüência de comprimento $N = 127$, considerou-se $\tau_{\max} = 4T_c$, resultando em atrasos máximos relativos praticamente iguais para todas as simulações. O atraso máximo relativo é definido em função do comprimento das seqüências: $\tau_{\max\,\%} = \frac{\tau_{\max}}{N} \times 100$ [%], e permite comparar o efeito do assincronismo de sistemas com seqüências de espalhamento de comprimento N distintos.

Para efeito de comparação, foi incluído nos gráficos o mesmo limite para *BER*, utilizado nos resultados da seção 2.3.1.

Os sistemas QS-CDMA com detecção multiusuário PIC-HD apresentam consi-

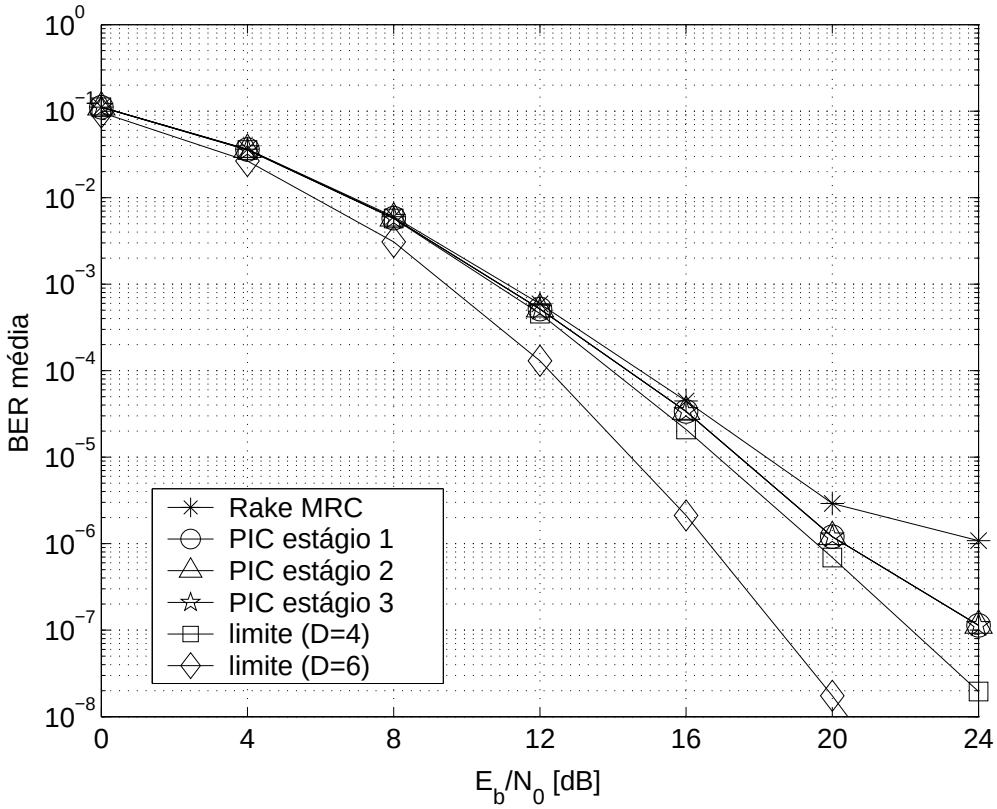

Figura E.2: Desempenho $\overline{BER} \times \frac{E_b}{N_0}$ do receptor Rake MRC e receptor Rake associado ao PIC-HD multiestágio utilizando o conjunto de seqüências ZCZ; $\tau_{\max} = 2T_c$.

derável melhoria de desempenho em relação à detecção convencional (conjunto de correlacionadores seguidos de combinador MRC).

Nos sistemas QS-CDMA com detector Rake MRC aqui analisados, o melhor desempenho é obtido com o conjunto ZCZ, figura E.2, seguido pelos desempenhos obtidos com o conjunto LCZ-GMW, figura E.3 e com o conjunto de seqüências QS, figura E.4. Já com o conjunto Lin-Chang, figura E.5, o desempenho do Rake é insatisfatório e próximo ao desempenho obtido com o conjunto WH, figura E.6.

O melhor desempenho do detector PIC-HD é obtido com o conjunto ZCZ, seguido pelo desempenho obtido com o conjunto LCZ-GMW. Observa-se ainda os desempenhos semelhantes para o PIC-HD obtidos com os conjuntos Lin-Chang e de seqüências QS. Isso indica que o incremento na complexidade do algoritmo de detecção do MuD PIC-HD, operando em canal com desvanecimento multipercurso, reduz ou mesmo elimina pequenas diferenças de desempenho observadas com o Rake MRC associado a esses dois conjuntos de seqüências. Finalmente, verifica-se que mesmo com a

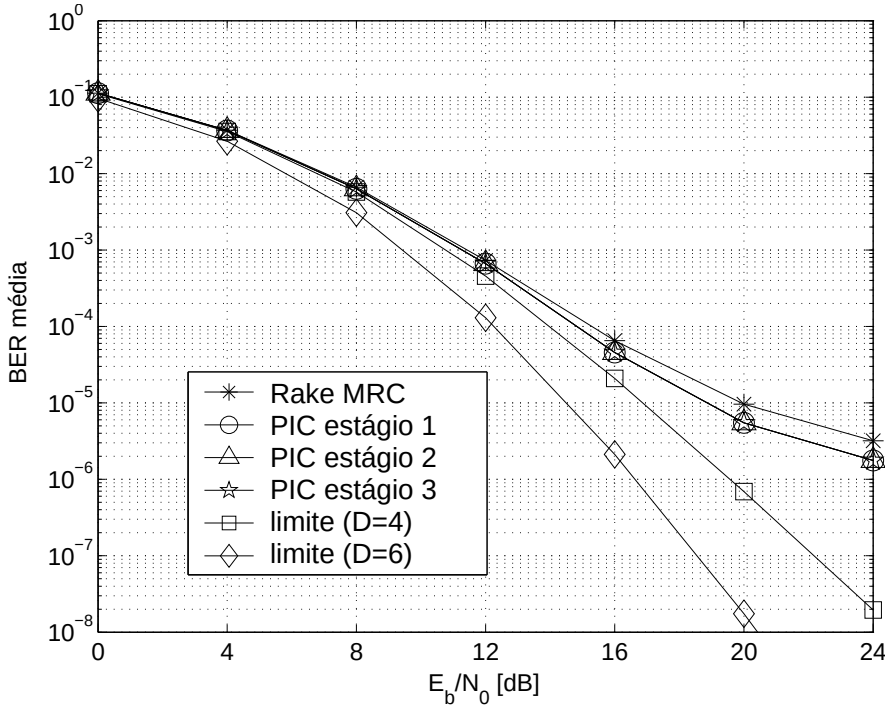

Figura E.3: Desempenho $\overline{BER} \times \frac{E_b}{N_0}$ do receptor Rake MRC e receptor Rake associado ao PIC-HD multiestágio utilizando o conjunto de seqüências LCZ-GMW; $\tau_{\max} = 2T_c$.

utilização do detector PIC-HD, o desempenho obtido com o conjunto WH é insatisfatório (figura E.6).

Devido ao baixo carregamento utilizado nas simulações, limitado pelo conjunto LCZ-GMW, um único estágio PIC-HD é suficiente para a obtenção de uma significativa melhoria de desempenho em relação ao receptor Rake MRC. Nessa condição de baixo carregamento, verifica-se que não há ganho de desempenho com o aumento do número de estágios PIC-HD.

A figura E.7 apresenta o desempenho médio em função do nível de assincronismo dos usuários em um receptor Rake MRC considerando os cinco conjuntos de seqüências com carregamentos similares (tabela E.1). O conjunto ZCZ resultou em melhor desempenho relativo. Praticamente para todo intervalo de atrasos analisado, o desempenho médio manteve-se muito próximo ao desempenho *limite*($D = 4$), indicando uma relativa robustez do sistema contra erros de sincronismo (pelo menos até 16%), mesmo em canal com grande número de multipercursos.

Degradações progressivas no desempenho do receptor Rake MRC são verifica-

das com a utilização dos conjuntos LCZ-GMW e QS, tanto em relação ao conjunto ZCZ quanto ao aumento do erro de sincronismo. O conjunto WH resulta no pior desempenho relativo, mantendo-se praticamente constante com o aumento do erro de sincronismo.

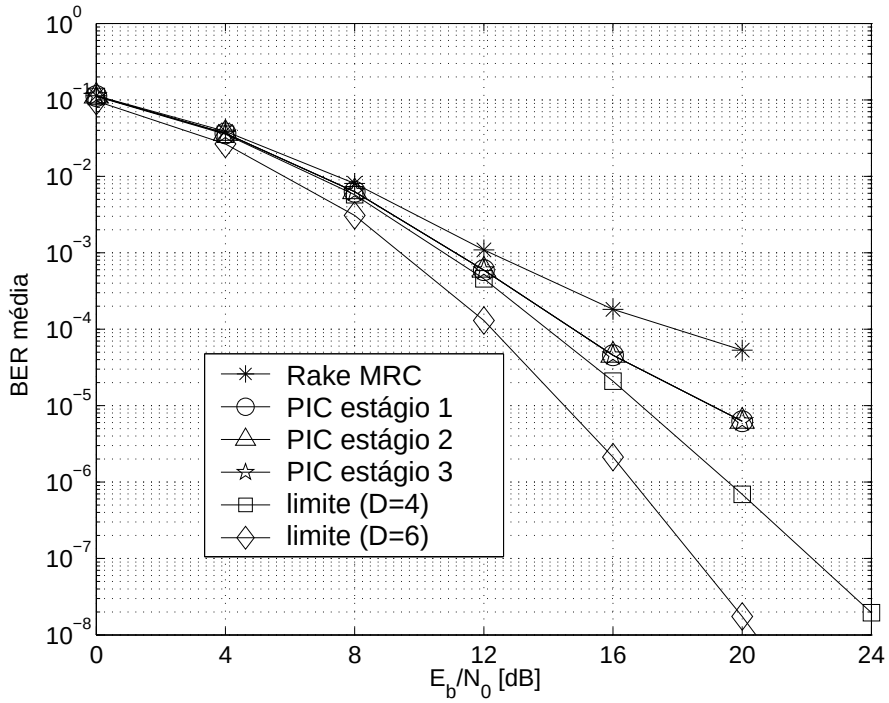

Figura E.4: Desempenho $\overline{BER} \times \frac{E_b}{N_0}$ do receptor Rake MRC e receptor Rake associado ao PIC-HD multiestágio utilizando o conjunto de seqüências QS; $\tau_{\max} = 4T_c$.

Ao contrário do comportamento dos demais conjuntos, o Lin-Chang apresenta melhoria de desempenho médio com o aumento do $\tau_{\max\,\%}$, tendendo ao desempenho obtido com o conjunto QS. Isso é devido à característica não-ótima para a correlação cruzada do conjunto Lin-Chang em torno da origem ($|\tau| < 1$) (LIN; CHANG, 1997).

Ao contrário do observado em canal de percurso único, a figura E.7 indica um desempenho médio não-ótimo para o receptor Rake MRC com o conjunto WH na condição de perfeito sincronismo, $\tau_{\max\,\%} = 0$, pois a característica do canal multipercurso impossibilita a manutenção da ortogonalidade entre os sinais recebidos. Problema similar ocorre com a utilização do conjunto de seqüências QS. Por exemplo, a boa característica de ECC mínima, quando $|\tau| \leq 2T_c$, para o conjunto com propriedade *QOQS* (5), utilizado nas simulações, são evidenciadas nos resultados de desempenho em canal de percurso único (KURAMOTO; ABRÃO; JESZENSKY, 2002). No entanto,

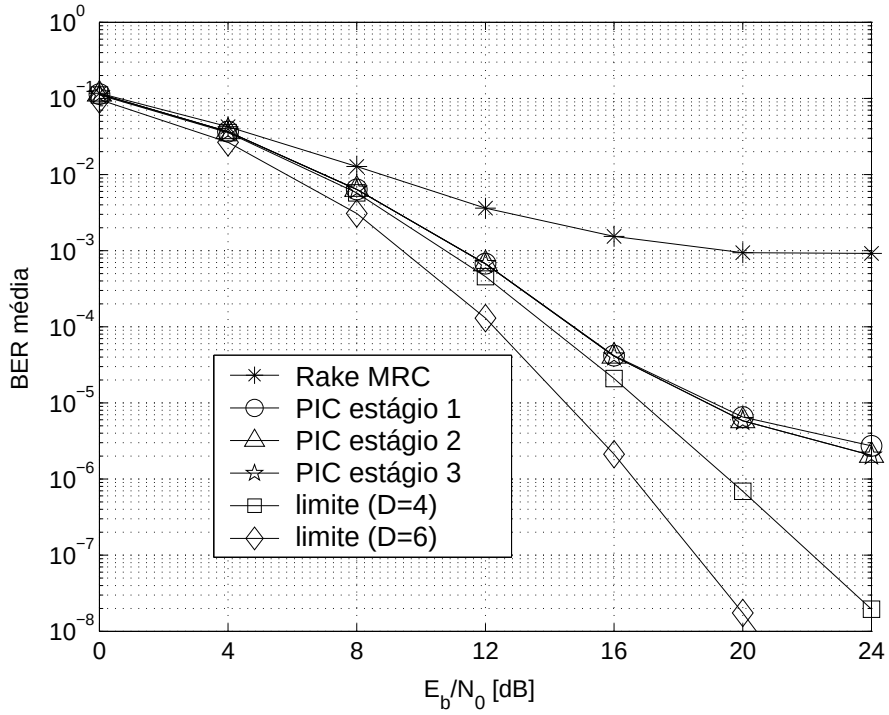

Figura E.5: Desempenho $\overline{BER} \times \frac{E_b}{N_0}$ do receptor Rake MRC e receptor Rake associado ao PIC-HD multiestágio utilizando o conjunto de seqüências Lin-Chang; $\tau_{\max} = 2T_c$.

nos resultados em canal com desvanecimento multipercurso, essa boa característica é insuficiente devido aos diversos componentes multipercurso com atrasos elevados.

Finalmente, a figura E.8 apresenta os resultados de desempenho para os cinco conjuntos de seqüências associado ao detector PIC-HD com 1 estágio de cancelamento em função do erro de sincronismo percentual. Verifica-se que, para a mesma diversidade Rake, $D = 4$, as diferenças de desempenhos com o MuD são minimizadas e, adicionalmente, as respectivas $\overline{BER}$ resultam mais próximas do limite com diversidade $D = 4$. Nota-se que mesmo com o aumento do erro de sincronismo percentual, não houve degradação do desempenho.

Com a escolha adequada do conjunto de seqüências para sistemas QS-CDMA, um único estágio PIC-HD é suficiente para uma significativa melhoria de desempenho em relação ao obtido com o receptor Rake MRC. Tal ganho de desempenho, acompanhado de um pequeno incremento na complexidade do receptor e da disponibilidade de um relativo controle de potência dos sinais recebidos, viabiliza a implementação do MuD subtrativo do tipo PIC-HD na estação base do sistema QS-CDMA.

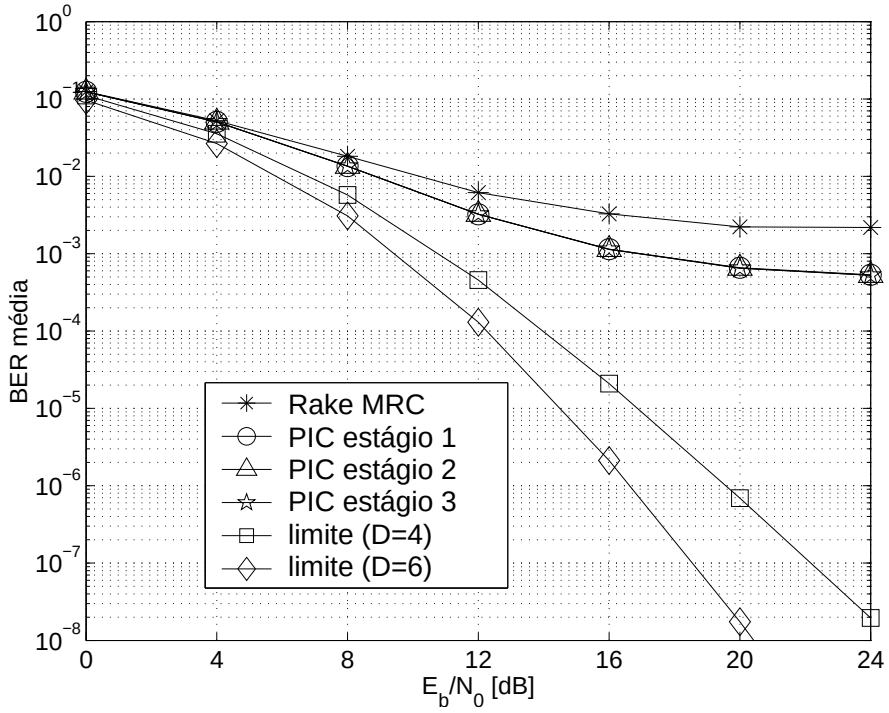

Figura E.6: Desempenho $\overline{BER} \times \frac{E_b}{N_0}$ do receptor Rake MRC e receptor Rake associado ao PIC-HD multiestágio utilizando o conjunto de seqüências WH; $\tau_{\max} = 2T_c$.

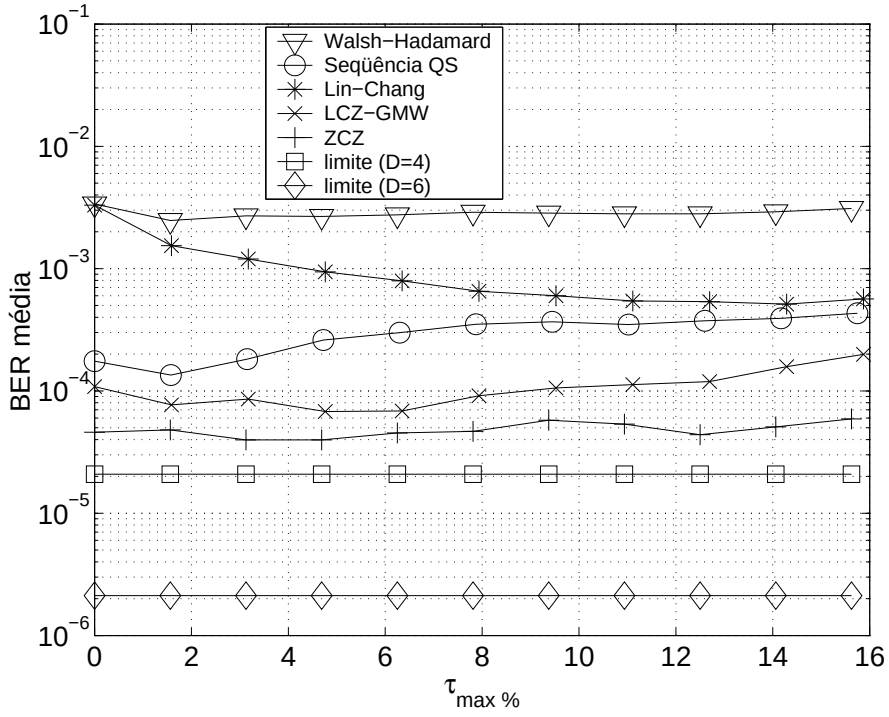

Figura E.7: Desempenho $\overline{BER} \times \tau_{\max_{\%}}$ para o receptor Rake MRC; $\frac{E_b}{N_0} = 16dB$ e diversas seqüências de espalhamento.

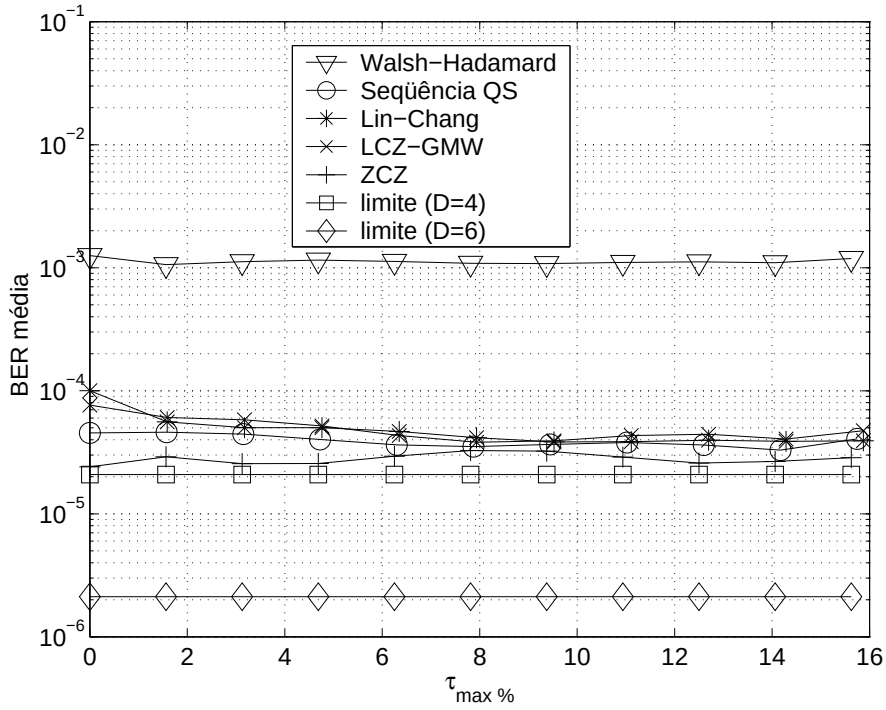

Figura E.8: Desempenho $\overline{BER} \times \tau_{\max_{\%}}$ para o receptor MuD PIC-HD com 1 estágio; $\frac{E_b}{N_0} = 16dB$ e diversas seqüências de espalhamento.

Apêndice F – Procedimento de simulação Monte-Carlo

O método numérico Monte-Carlo foi utilizado neste trabalho para o cálculo da $\overline{BER}$. Cada simulação Monte-Carlo emula basicamente um transmissor DS/CDMA, um canal de comunicação e finalmente um receptor, conforme os modelos de sistemas adotados. A seqüência de bits de informação, os atrasos, fases, amplitudes e demais parâmetros envolvidos no sistema são escolhidos aleatoriamente conforme a distribuição adotada na modelagem do sistema. Nas simulações, foi considerado taxa de amostragem do sinal igual a $\frac{5}{T_c}$. Dessa forma, o menor atraso entre os diversos multipercursos dos usuários ativos é de $\frac{T_c}{5}$.

A $\overline{BER}$ é obtida da relação entre o número de bits detectados com erro (N_e) e o número de bits transmitidos (N_t):

$$\overline{BER} = \frac{N_e}{N_t} \tag{F.1}$$

O resultado mais confiável para a $\overline{BER}$ é obtido quando o número de bits transmitidos tender ao infinito. Nesse caso, tem-se a $\overline{BER}$ estimada pelo método Monte-Carlo igual à $\overline{BER}$ verdadeira ($\overline{BER}_{verd}$).

Em (JERUCHIM; BALABAN; SHANMUGAN, 1992), para o método de Monte-Carlo de cálculo de $\overline{BER}$, foi apresentada uma aproximação para o intervalo de confiança normalizado:

$$\begin{aligned} P\left[y_+ \leq \overline{BER} \leq y_-\right] &= 1-\alpha \\ y_\pm &= 10^{-\nu}\left\{1+\left(\frac{d_\alpha^2}{2\eta}\right)\left[1 \pm \left(\frac{4\eta}{d_\alpha^2}+1\right)^{\frac{1}{2}}\right]\right\} \end{aligned} \tag{F.2}$$

onde $N_t = \eta 10^{\nu}$ e d_α é escolhido de forma a satisfazer:

$$\frac{1}{\sqrt{2\pi}} \int_{-d_\alpha}^{d_\alpha} e^{\frac{-t^2}{2}}\, dt \;=\; 1 - \alpha \tag{F.3}$$

A figura F.1 apresenta as curvas para intervalos de confiança de 90%, 95% e 99%.

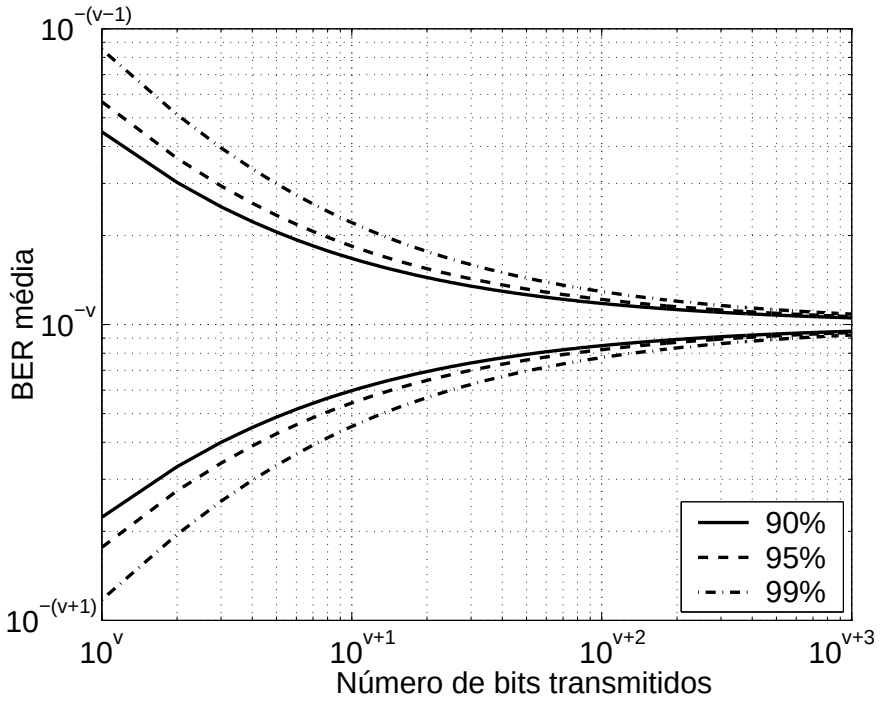

Figura F.1: Intervalos de confiança.

Considera-se razoável, para estimativa de $\overline{BER}$, um intervalo de 95% de confiança (JERUCHIM; BALABAN; SHANMUGAN, 1992):

$$\frac{1}{2}\overline{BER} \leq \overline{BER}_{verd} \leq 2\overline{BER} \tag{F.4}$$

O intervalo $0,55\overline{BER} \leq \overline{BER}_{verd} \leq 1,8\overline{BER}$ de 95% de confiança é obtido com $N_t = \frac{10}{\overline{BER}}$, conforme a figura F.1. Nos resultados de simulação Monte-Carlo deste trabalho, considerou-se esse intervalo de confiança. Logo, nas simulações Monte-Carlo, adotou-se $N_t \geq \frac{10}{\overline{BER}}$.

Apêndice G – Simulador de canal

Neste trabalho foi adotado um simulador de canal proposto em (SILVA; ABRãO; JESZENSKY, 2004). Esse modelo produz múltiplas envoltórias Rayleigh com estatísticas corretas e com menor esforço computacional quando comparado ao modelo de Jakes modificado (ZHENG; XIAO, 2003) e ao modelo de Smith modificado (YOUNG; BEAULIEU, 2000).

Um canal típico de rádio móvel pode ser representado por coeficientes de canal (ou coeficientes de transmissão), os quais representam a fase e amplitude do sinal recebido quando transmite-se um sinal contínuo de amplitude unitária. Um processo aleatório Gaussiano estacionário no sentido amplo pode ser usado para caracterizar os coeficientes de transmissão:

$$c(t) = c_R(t) + jc_I(t) \tag{G.1}$$

onde $c_R(t)$ e $c_I(t)$ para qualquer t são variáveis aleatórias Gaussianas independentes.

As propriedades de (G.1) são (GANS, 1972):

$$\mathbb{E}\{c(t)\} = \mathbb{E}\{c_R(t)\} = \mathbb{E}\{c_I(t)\} = 0 \tag{G.2}$$

$$\mathbb{E}\{|c(t)|^2\} = 2\mathbb{E}\left\{(c_R(t))^2\right\} = 2\mathbb{E}\left\{(c_I(t))^2\right\} = 2\sigma^2 \tag{G.3}$$

$$g(\tau) = \mathbb{E}\{c_R(t)c_R(t+\tau)\} = \mathbb{E}\{c_I(t)c_I(t+\tau)\} = \sigma^2 J_0(\omega_m \tau) \tag{G.4}$$

$$h(\tau) = \mathbb{E}\{c_R(t)c_I(t+\tau)\} = -\mathbb{E}\{c_I(t)c_R(t+\tau)\} = 0 \tag{G.5}$$

$$R_c\tau = \mathbb{E}\{c(t)c^*(t+\tau)\} = 2\sigma^2 J_0(\omega_m \tau) \tag{G.6}$$

$$C_{c_i,c_j}(\tau) = \mathbb{E}\{c_i(t)c_j^*(t+\tau)\} - \mathbb{E}\{c_i(t)\}\mathbb{E}\{c_j^*(t)\} = 0, \;\; i \neq j \tag{G.7}$$

onde $J_0(.)$ é a função de Bessel de primeira espécie e primeira ordem; $\omega_m = 2\pi f_m = \frac{v}{\lambda}$ é o máximo deslocamento Doppler; v é a velocidade do móvel; λ é o comprimento de

onda da portadora.

As propriedades (G.2), (G.4) e (G.6) mostram que $c(t)$ é estacionário no sentido amplo. A propriedade (G.5) mostra que as partes reais e imaginárias de $c(t)$ são independentes. Utilizando as propriedades (G.2), (G.3) e (G.2), mostra-se que o processo $c(t)$ possui fase $\angle c(t)$ com distribuição uniforme no intervalo $[0; 2\pi)$ e módulo $|c(t)|$ com *pdf* Rayleigh.

De (G.7) verifica-se que duas funções amostras são não correlacionadas. Esta propriedade é necessária para a simulação de canais multipercurso, os quais foram considerados neste trabalho.

Utilizando a seqüência $c[n]$ com comprimento N para representar $c(t)$ em tempo discreto com período de amostragem $T_s = \frac{1}{f_s}$, em (SILVA; ABRãO; JESZENSKY, 2004) foi apresentado o modelo:

$$\begin{aligned} c[n] &= IDFT\left\{|S_T[k]|e^{j\varphi_k}\right\} \\ &= \frac{1}{N}\sum_{k=0}^{N-1}|S_T[k]|e^{j\varphi_k}e^{\frac{j2\pi kn}{N}} \quad n = 0, 1, ..., N-1 \end{aligned} \tag{G.8}$$

onde $\varphi[k] = \{\varphi_0, \varphi_1, ..., \varphi_k, ..., \varphi_{N-1}\}$ é a seqüência de variáveis aleatórias independentes uniformemente distribuídas de 0 a 2π e $S_T[k] = |DFT\{c[n]\}|$:

$$|S_T[k]| = \begin{cases} 0, & k = 0 \\ \sqrt{\left(\frac{2\sigma^2 N}{T_s}\right)\frac{1}{\pi f_m\sqrt{1-\left(\frac{kT_f}{f_m}\right)^2}}}, & 1 \le k \le K_m - 1 \\ \sqrt{\left(\frac{2\sigma^2 N}{T_f T_s}\right)\left(\frac{1}{2} - \frac{1}{\pi}\arcsin\left(\frac{(K_m-1)T_f}{f_m}\right)\right)}, & k = K_m \\ 0, & K_m + 1 \le k \le N - 1 - K_m \\ |S_T[N-k]|, & N - K_m \le k \le N - 1 \end{cases} \tag{G.9}$$

onde $K_m = \left\lfloor \frac{f_m}{f_s} N \right\rfloor$; $T_f = \frac{1}{T}$ é o intervalo de freqüência entre duas amostras de $S_T[k]$ e $T = NT_s$.

A soma de variáveis aleatórias independentes em (G.8) permite afirmar que, para valores elevados de N, $c[n]$ é um processo aleatório Gaussiano. Em (SILVA; ABRãO; JESZENSKY, 2004), foi mostrado que as propriedades (G.2) a (G.7) são satisfeitas,

sendo que as estatísticas temporais, realizadas em uma função amostra, são iguais às estatísticas de conjunto, o que significa que o modelo é ergódico na média e autocorrelação.

Referências

ABRÃO, T. *Cancelladores de Interferência Multiusuário Aplicados a Sistemas DS/CDMA de Múltipla Taxa*. Tese (Doutorado) — Escola Politécnica da Universidade de São Paulo, Março 2001.

ADACHI, F.; SAWAHASHI, M.; OKAWA, K. Tree-structured generation of orthogonal spreading codes with different length for forward link of ds-cdma mobile radio. *Electronics Letters*, v. 33, n. 1, p. 27–28, 1997.

BROOKS, S. A. *Analysis of Large Area Synchronous Code-Division Multiple Access (LAS-CDMA)*. Dissertação (Mestrado) — Naval Postgraduate School, Monterey, California, June 2002.

CANADEO, C. M.; TEMPLE, M. A.; BALDWIN, R. O.; RAINES, R. A. Code selection for enhancing uwb multiple access communication performance using th-ppm and ds-bpsk modulations. *IEEE Transactions on Information Theory*, IT-33, n. 1, p. 116–123, 2003.

CONTI, P. G.; GUNAWARDANA, U. The use of permutations on LA codes. *Australian Telecommunications, Networks and Application Conference (ATNAC)*, December 2003.

DENG, X.; FAN, P. Spreading sequence set with zero correlation zone. *Electronics Letters*, v. 36, n. 11, p. 993–994, May 2000.

FAN, P.; HAO, L. Generalized orthogonal sequences and their applications in synchronous cdma systems. *IEICE Transactions on Fundamentals*, E83, n. 11, p. 2054–2069, November 2000.

FAN, P. Z.; KUROYANAGI, N. S. N.; DENG, X. M. Class of binary sequences with zero correlation zone. *Electronics Letters*, v. 35, n. 10, p. 777–779, May 1999.

GAMAL, A. A. E.; HEMACHANDRA, L. A.; SHPERLING, I.; WEI, V. K. Using simulated annealing to design good codes. *IEEE Transactions on Information Theory*, IT-33, n. 1, p. 116–123, 1987.

GAMES, R. A. Crosscorrelation of m-sequences and gmw-sequences with the same primitive polynomial. *Discrete Applied Mathematics*, n. 12, p. 139–146, 1984.

GANS, M. J. A power-spectral theory os propagation in mobile-radio environment. *IEEE Transactions on Vehicular Technology*, VT-21, n. 1, p. 27–38, February 1972.

GAUDENZI, R. de; ELIA, C.; VIOLA, R. Bandlimited quasi-synchronous CDMA: A novel satellite access technique for mobile and personal communication systems. *IEEE Journal on Selected Areas in Communications*, v. 10, n. 2, p. 328 – 343, February 1992.

GAVISH, A.; LEMPEL, A. On ternary complementary sequences. *IEEE Transactions on Information Theory*, v. 40, n. 2, p. 522–526, March 1994.

GOLAY, M. J. E. Complementary series. *IEEE Transaction on Information Theory*, v. 7, p. 82–87, 1961.

GOLD, R. Optimal binary sequences for spread spectrum multiplexing. *IEEE Transactions on Information Theory*, p. 619–621, October 1967.

GOLOMB, S. W. *Shift Register Sequences*. Revised. Laguna Hills, California: Aegean Park Press, 1982.

GORDON, B.; MILLS, W. H.; WELCH, L. R. Some new differences sets. *Canadian Journal of Mathematics*, v. 14, p. 614–625, 1962.

HARADA, H.; PRASAD, R. *Simulation and Software Radio for Mobile Communications*. [S.l.]: Artech House, 2002.

ILTIS, R. A. Demodulation and code acquisition using decorrelator detectors for QS-CDMA. *IEEE Transactions on Communications*, v. 44, n. 11, p. 1553–1560, November 1996.

ILTIS, R. A.; MAILAENDER, L. Multiuser detection of quasisynchronous CDMA signals using linear decorrelators. *IEEE Transactions on Communications*, v. 44, n. 11, p. 1561–1570, November 1996.

JERUCHIM, M. C.; BALABAN, P.; SHANMUGAN, K. S. *Simulation of Commuication Systems*. New York: Pleum Press, 1992.

JESZENSKY, P. J. E. *CDMA (Code Division Multiple Access), DS/SS (Direct Sequence Spread Spectrum) and Related Topics*. September 2001. Notas de aula.

JOHANSSON, A.-L. *Successive Interference Cancellation in DS-CDMA Systems*. Tese (Doutorado) — School of Electrical and Computer Engineering, Chalmers University of Technology, Göteborg, Sweden, October 1998.

KAJIWARA, A.; NAKAGAWA, M. Microcellular CDMA system with a linear multiuser interference canceler. *IEEE Journal on Selected Areas in Communications*, v. 12, n. 4, p. 605–611, May 1994.

KASAMI, T. Some lower bounds on the minimum weight of cyclic codes of composite length. *IEEE Transactions on Information Theory*, v. 14, n. 6, p. 814–818, November 1968.

KIRKPATRICK, S.; GELLAT, C. D.; VECCHI, M. P. Optimization by simulated annealing. *Science*, v. 220, n. 4598, p. 671–681, May 1983.

KUNO, S.; YAMAZATO, T. T.; KATAYAMA, M.; OGAWA, A. A study on quasisynchronous CDMA based on selected PN signature sequences. *IEEE International Symposium of Spread Spectrum Techniques and Applications*, p. 479 – 483, September 1994.

KURAMOTO, A. S. R.; ABRÃO, T.; JESZENSKY, P. J. E. Set of sequences for qs-cdma systems with multi-user detection and multipath-fanding channels. *Wireless Personal Communication, Kluwer Academic Publisher, in press*.

KURAMOTO, A. S. R.; ABRÃO, T.; JESZENSKY, P. J. E. Comparação de seqüências de espalhamento aplicáveis a sistemas QS-CDMA. *Revista Semina, UEL Londrina/PR*, v. 23, n. 1, p. 27–40, dezembro 2002.

KURAMOTO, A. S. R.; ABRÃO, T.; JESZENSKY, P. J. E. Conjuntos de seqüências para sistemas qs-cdma com detecção multiusuário sujeitos a desvanecimento multipercurso. *Anais do XX Simpósio Brasileiro de Telecomunicações, SBT'03, Rio de Janeiro-RJ*, p. 426–431, Outubro 2003.

KURAMOTO, A. S. R.; ABRÃO, T.; JESZENSKY, P. J. E. Projetos de seqüências para sistemas qs-cdma multitaxa mpg. *XXI Simpósio Brasileiro de Telecomunicações, SBT'04, Belém-PA*, Setembro 2004.

KURAMOTO, A. S. R.; ABRÃO, T.; JESZENSKY, P. J. E. Set of sequences for qs-cdma systems with interference cancellation over multipath-fading channels. *IEEE International Symposium on Spread Spectrum Techniques and Applications*, p. 694–698, September 2004.

KURAMOTO, A. S. R.; ABRÃO, T.; JESZENSKY, P. J. E. Spreading sequence comparison for QS-CDMA systems. *IEEE International Symposium on Spread Spectrum Techniques and Applications*, p. 350–354, September 2004.

LEE, Y.; JOO, Y. I.; TCHAH, K. H. Optimal sequences for a quasi-synchronous multi-rate VPG DS/CDMA system. *Telecommunications Review*, v. 11, n. 1, p. 144–160, 2001.

LI, D. The perspectives of large area synchronous cdma technology for the fourth-generation mobile radio. *IEEE Communications Magazine*, v. 41, n. 3, p. 114–118, March 2003.

LIDL, R.; NIEDERREITER, H. *Encyclopedia of Mathematics and its Applications: Finite fields*. 2nd. ed. The Edinburgh Building, Cambridge: Cambridge University Press, 1997.

LIMA, J. A. de. *Análise de Um Sistema de Comunicação Por Pacotes Para Uso Em Telefonia Móvel Microcelular*. Dissertação (Mestrado) — Escola Politécnica - Universidade de São Paulo - Departamento de Engenharia Eletrônica área de Sistemas Eletrônicos, Dezembro 1996.

LIN, X. D.; CHANG, K. H. Optimal PN sequence design for quasisynchronous CDMA communication systems. *IEEE Transactions on Communications*, v. 45, n. 2, p. 221–226, February 1997.

LINKAIR. *LinkAir*. 2003. Site www.linkair.com.

LONG, B. Q.; ZHANG, P. The analysis of a generalized QS-CDMA system over a multipath rayleigh fading channel. *IEEE Wireless Communication System Symposium*, p. 137–141, November 1995.

MASSEY, J. L. On welch's bound for the correlation of a sequence set. *Proceedings of IEEE International Symposium on Information Theory*, p. 385, November 1991.

MASSEY, J. L.; MITTELHOLZER, T. Final report: Technical assistence for the CDMA communication system analysis. *ESTEC Contract No. 8696/89/NL/US Institute for Signal and Information Processing CII-8092 ETII - Zürich*, v. 1 February 1990 - 31 July 1990, p. 1–40, February 1991.

MCELIECE, R. J. *Finite Field for Computer Scientists and Engineers*. [S.l.]: Kluwer Academic Publishers, 1987.

MEYER, C. *Matrix Analysis and Applied Linear Algebra*. University City Science Center, Philadelphia: Society for Industrial and Applied Mathematics, 2000.

NO, J.-S.; KUMAR, P. V. A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span. *Canadian Journal of Mathematics*, v. 35, p. 371–379, 1989.

OTTOSSON, T. *Coding, Modulation and Multiuser Decoding for DS-CDMA Systems*. Tese (Doutorado) — School of Electrical and Computer Engineering, Chalmers University of Technology, Göteborg, Sweden, November 1997.

PAPADIMITRIOU, C. H.; STEIGLITZ, K. *Combinatorial Optimization: Algorithms and Complexity*. [S.l.]: Dover Publications, 1998.

PAPOULIS, A. *Probability, Random Variables, and Stocastic Processes*. 3rd. ed. [S.l.]: Mc Graw-Hill, 1991. (Electrical engineering. Communications ans signal processing).

PARK, S. I.; PARK, S. R.; SONG, I.; SUEHIRO, N. Multiple-access interference reduction for QS-CDMA systems with a novel class of polyphase sequences. *IEEE Transactions on Information Theory*, v. 46, n. 4, p. 1448–1458, July 2000.

PARK, S. R.; SONG, I.; YOON, S.; LEE, J. A new poliphase sequence with perfect even and good odd cross-correlation functions for ds/cdma systems. *IEEE Transactions on Vehicular Technology*, v. 51, n. 5, p. 855–866, September 2002.

PENG, D.; FAN, P. Generalised sarwate bounds on periodic autocorrelations and cross-correlations of binary sequences. *Electronics Letters*, v. 38, n. 4, p. 1521–1523, November 2002.

PENG, D.; FAN, P. Bounds on aperiodic auto- and cross-correlations of binary sequences with low or zero correlation zone. *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003*, v. 38, p. 882–886, November 2003.

PENG, D.; FAN, P. Generalized sarwate bounds on the periodic correlation of complex roots of unity sequences. *IEEE Proceedings on 14th Personal, Indoor and Mobile Radio Communications, 2003*, v. 1, p. 449–452, September 2003.

PEPPER, J. W.; WASIL, B. L. G. ans E. A. Solving the traveling salesman problem with annealing-based heuristics: A computational study. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, v. 32, n. 1, p. 72–77, January 2002.

PICKHOLTZ, R. L.; MILSTEIN, L. B.; SCHILLING, D. L. Spread spectrum for mobile communications. *IEEE Transactions on Vehicular Technology*, v. 40, n. 2, p. 313–322, May 1991.

PRESS, W. H.; TEUKOLSKY, S. A.; VETTERLING, W. T.; FLANNERY, B. P. *Numerical Recipes in C: The Art of Scientifc Computing*. [S.l.]: Cambridge University Press, 1992.

PROAKIS, J. G. *Digital Communications*. 3th. ed. [S.l.]: McGraw-Hill, 1995. (Electrical and Computer Engineering. Communications and Signal Processing).

SAITO, M.; YAMAZATO, T.; OKADA, H.; KATAYAMA, M.; OGAWA, A. New quasi-synchronous sequences for CDMA slotted ALOHA systems. *IEICE Transactions on Fundamentals*, E81-A, n. 11, p. 2274–2280, November 1998.

SAITO, M.; YAMAZATO, T.; OKADA, H.; KATAYAMA, M.; OGAWA, A. Generation of sets of sequences suitable for multicode transmission in quasi-synchronous CDMA systems. *IEICE Transactions on Communications*, E84-B, n. 3, p. 576–580, March 2001.

SARWATE, D. V. Bounds on crosscorrelation and autocorrelation of sequences. *IEEE Transactions on Information Theory*, IT-25, n. 6, p. 720–724, November 1979.

SCHOLTZ, R. A.; WELCH, L. R. GMW sequences. *IEEE Transaction on Information Theory*, IT-30, n. 3, p. 548–553, 1984.

SILVA, V.; ABRãO, T.; JESZENSKY, P. J. E. Statistically correct simulation models for the generation of multiple uncorrelated rayleigh fading waveforms. *IEEE International Symposium on Spread Spectrum Techniques and Applications*, p. 472–476, September 2004.

SIMON, M. K.; OMURA, J. K.; SCHOLTZ, R. A.; LEVITT, B. K. *Spread Spectrum Communications Handbook*. Revised edition. [S.l.]: McGraw-Hill, 1994.

SINGER, J. A theorem in finite projective geometry and some applications to number theory. *Transaction of American Mathematics Society*, v. 43, p. 377–385, 1938.

STUBER, G. L. *Principles of Mobile Communication*. 2nd. ed. Norwell, Massachusetts: Kluwer Academic Publisher, 2001.

SUEHIRO, N. A signal design without co-channel interference for approximately synchronized CDMA systems. *IEEE Journal on Selected Areas in Communications*, v. 12, n. 5, p. 837–841, June 1994.

SUEHIRO, N. Binary or quadriphase signal design for approximately synchronized CDMA systems without detection sidelobe nor co-channel interference. *Proceedings IEEE 4th International Symposium of Spread Spectrum Techniques and Applications*, p. 650–656, September 1996.

SUEHIRO, N.; HATORI, M. Modulatable orthogonal sequences and their application to SSMA systems. *IEEE Transactions on Information Theory*, v. 34, n. 1, p. 93–100, January 1988.

TANG, X. H.; FAN, P. Z. Bounds on aperiodic and odd correlations of spreading sequences with low and zero correlation zone. *Electronics Letters*, v. 37, n. 19, p. 1201–1203, September 2001.

TANG, X. H.; FAN, P. Z. A class of pseudonoise sequences over GF(P) with low correlation zone. *IEEE Transactions on Information Theory*, v. 47, n. 4, p. 1644–1649, May 2001.

TANG, X. H.; FAN, P. Z.; MATSUFUJI, S. Lower bounds on correlation of spreading sequences set with low or zero correlation zone. *Electronics Letters*, v. 36, n. 6, p. 551–552, March 2000.

TSENG, C. C.; LIU, C. L. Complementary sets of sequences. *IEEE Transaction on Information Theory*, v. 18, p. 644–652, 1972.

VARANASI, M. K.; AAZHANG, B. Multistage detection in asynchronous code-division multiple-access communications. *IEEE Transactions on Communications*, v. 38, n. 4, p. 509–519, April 1990.

WELCH, L. R. Lower bounds on the maximum cross correlation of signals. *IEEE Transactions on Information Theory*, IT-20, n. 3, p. 397–399, May 1974.

WENG, J.; XUE, G.; LE-NGOC, T.; TAHAR, S. Multistage interference cancellation with diversity reception for asynchronous QPSK DS/CDMA systems over multipath channels. *IEEE Journal on Selected Areas in Communications*, v. 17, n. 12, p. 2162–2180, December 1999.

WHALEN, P. On the road to third generation wireless. *Hill Associates Magazine*, 2002.

XU, S.; LI, D. Ternary complementary orthogonal sequences with zero correlation window. *IEEE Proceedings on 14th Personal, Indoor and Mobile Radio Communications*, v. 2, p. 1669–1672, September 2003.

YAO, K. Error probability of asynchronous spread spectrum multiple access communication systems. *IEEE Transactions on Communications*, COM-25, n. 8, p. 803–809, August 1977.

YOUNG, D. J.; BEAULIEU, N. C. The generation of correlated rayleigh random variates by inverse discrete fourier transform. *IEEE Transactions on Communications*, v. 48, n. 7, p. 1114–1127, July 2000.

ZENG, M.; ANNAMALAI, A.; BHARGAVA, V. K. Harmonization of global third-generation mobile systems. *IEEE Communications Magazine*, v. 38, n. 12, p. 94–98, December 2000.

ZHENG, Y.; XIAO, C. Simulation models with correct statistical properties for rayleigh fading channels. *IEEE Transactions on Communications*, v. 51, n. 6, p. 920–928, June 2003.

ZHOU, X.; LU, W. Performance analysis of LA codes in LAS-CDMA. *IEEE Proceedings on ICSP'02*, 2002.

ZIEMER, R. E.; PETERSON, R. L. *Digital Communications and Spread Spectrum Systems*. [S.l.]: Macmillan, 1985.