Universidade Estadual de Campinas
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
DEPARTAMENTO DE SEMICONDUTORES INSTRUMENTOS E FOTÔNICA
UNICAMP - FEEC -DSIF, CAMPINAS - SP, C.P. 6101, CEP. 13083-970

Propostas de Códigos Ortogonais para Sistemas OCDMA

Tese de Doutorado

Autor: Adriano Domingos Neto
Orientador: Prof. Dr. Edson Moschim

Banca Examinadora

Prof. Dr. Edson Moschim (DSIF/FEEC/UNICAMP)

Prof. Dr. Felipe Rudge Barbosa (Fundação CPqD/Campinas)

Prof. Dr. Marcelo L. F. Abbade (PUC/Campinas)

Prof. Dr. Amílcar Careli César (USP/SÃO CARLOS)

Prof. Dr. Vicente I. Becerra Sablón (UNISAL/Campinas)

Prof. Dr. Aldário Chrestani Bordonalli (DMO/FEEC/UNICAMP)

Prof. Dr. Yuzo Iano (DECOM/FEEC/UNICAMP)

Tese apresentada à Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas como parte dos requisitos necessários para a obtenção do título de Doutor em Engenharia Elétrica

Campinas, 26 de Agosto de 2005

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA - BAE - UNICAMP

Domingos Neto, Adriano
D713p Propostas de códigos ortogonais para sistemas OCDMA / Adriano Domingos Neto. --Campinas, SP: [s.n.], 2005.

Orientador: Edson Moschim.
Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Detecção de sinais. 2. Formas quadráticas. 3. Formas binárias. 4. Aproximação diofantina. 5. Telecomunicações. 6. Comunicações óticas. I. Moschim, Edson. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Titulo em Inglês: Construction of optical orthogonal codes for use in cdma fiber-optics systems
Palavras-chave em Inglês: Signal detection, Quadratic forms, Binary forms, Diophantine approximation, Telecommunication e Optical communication
Área de concentração: Telecomunicações e Telemática
Titulação: Doutor em Engenharia Elétrica
Banca examinadora: Felipe Rudge Barbosa, Marcelo Luís Francisco Abbade, Amílcar Careli César, Vicente Idalberto Becerra Sablón, Aldário Chrestani Bordonalli e Yuzo Iano
Data da defesa: 26/08/2005

Agradecimentos

"*Donde, pois, vem a sabedoria? Onde está o lugar do entendimento? ...Eis que o temor do Senhor é a sabedoria, e o apartar-se do mal é o entendimento...Portanto, quer comais quer bebais, ou façais, qualquer outra coisa, fazei tudo para glória de Deus*"(Jó cap.28 v.20-28 e I Coríntios cap.10 v.31)

Meu louvor, de agradecimento, ao Altíssimo Deus para me capacitar a usar, sempre, toda sabedoria que me dá, para aproximar-me cada dia mais Dele. Amém.

Para Teresa J. A. Silva Neto, Makiesse Titina L. Balala, Ijie N. Balala e Kidi D. Balala (em véspera do nascimento) mil beijos de amor em agradecimento ao suporte familiar que me concederam.

Meus cordiais agradecimentos fraternos à Igreja Metodista Central de Campinas.

Aos meus pais, irmãos e irmãs, parentes e familiares, meus abraços de agradecimento porque sempre acreditaram que tudo, com Deus, é possível.

À família João e Zuleika meu grande beijo de agradecimento.

Ao Prof. Dr. Edson Moschim meus sinceros agradecimentos pela orientação do trabalho.

Que fiquem registrados os meus sinceros agradecimentos aos membros da banca examinadora desta tese.

Meus agradecimentos póstumos ao Prof. Dr. Duncan Alexander Reiley e sua família.

Meu agradecimento especial aos Prof. Dr. Reginaldo Palazzo Jr e Prof Daniel Camilo por suas contribuições a este trabalho.

Meus agradecimentos à Elisabeth A. da Silva e Samuel F. Gonçalves.

Meus agradecimentos ao amigos Raulison A. Resende e família, e Rangel Arthur.

Meus agradecimentos aos colegas alunos e alunas pelos mais diferentes apoios, discussões e sugestões.

Às meninas da FEEC (Faculdade de Engenharia Elétrica e Computação) os meus mais sinceros agradecimentos.

As meninas da Biblioteca da Área de Engenharia (BAE) sempre fizeram por merecer os meus mais profundos agradecimentos. Eu, de coração, agradeço.

À todos quanto direta ou indiretamente contribuíram para este trabalho o meu muito obrigado.

Que Deus nos abençoe a todos. " **N'gana a tubane dibeçá**".

Resumo

[1] A. D. Neto, "Propostas de Códigos ortogonais para Sistemas OCDMA", Tese de Doutorado, FEEC-UNICAMP, Agosto, 2005.

Nesta tese, propõe se três novas construções de códigos ortogonais ópticos (OOC), do tipo congruentes, tendo como base a estrutura algébrica do grupo multiplicativo do corpo de Galois GF(p), para aplicação em sistemas de comunicação utilizando a técnica de acesso múltiplo por divisão de códigos ópticos (OCDMA). Os códigos ópticos primos e códigos quadráticos são, pela primeira vez na literatura, gerados a partir de códigos de Slepian (códigos esféricos) e, códigos de resíduos quadráticos, respectivamente. Através do algoritmo da d-cadeia fechada, são obtidos os códigos de primos, como caso particular dos códigos de Slepian. Os códigos quadráticos ópticos são representados por números inteiros quadráticos binários na forma de equações de Diofanto com duas variáveis, de modo que, o reticulado $\mathbb{Z}_2$ ou reticulado $\mathbb{A}_2$ fornecem as palavra do código quadrático. O desempenho dos códigos é avaliado usando o critério da probabilidade de erro para situações em que o receptor óptico incorpora um limitador óptico e um fotodiodo APD. O desempenho do sistema é obtido considerando os efeitos da interferência de acesso múltiplo, o ruído balístico do fotodiodo e o ruído térmico do receptor. O desempenho dos códigos propostos é comparado ao desempenho de códigos amplamente divulgados em literatura técnica. Mostra-se ainda que os códigos propostos apresentam desempenho semelhante aos códigos divulgados, tendo como vantagem uma estrutura algébrica de simples implementação e melhor sincronismo.

Abstract

[2] A. D. Neto, "Construction of optical orthogonal codes for use in cdma fiber-optics systems", PhD Thesis, FEEC-UNICAMP, August, 2005.

This thesis presents a study of optical orthogonal codes (OOC) for application in communication systems using the technique of fiber-optics code division multiple access (OCDMA). The Prime Sequence codes and Quadratic codes are, for the first time in literature, characterized as Slepian group codes (spherical codes) and Quadratic Residues codes, respectively. Through the algorithm of the closed d-chain the Prime Sequence codes are obtained, as a particular case of the Slepian codes. The Quadratic codes are represented by binary quadratic integers in the form of Diophantine equations with two variables, so that, $\mathbb{Z}_2$ lattice or $\mathbb{A}_3$ lattice supplies the codeword of the quadratic code. Furthermore, this thesis presents three new constructions of optical orthogonal codes (OOC), construed via congruences having as base the algebraic structure of the multiplicative group of the Galois Field GF(p). The performance of the codes is evaluated using the criterion of the error probability, for situations where the optic receiver incorporates a fiber-optic limiter and a APD photodiode. The performance of the system is evaluated considering the effect of the interference of multiple access, the ballistic noise of the photodiode and the thermal noise of the receiver. The performance of the considered codes is compared with the performance of other codes found in the technical literature. It is observed that the codes considered in this thesis, in this thesis, present similar performance to the reported codes, having as advantage an algebraic structure of simple implementation and better synchronism.

Lista de Siglas e Símbolos

Sigla ou Símbolo	**Designação**
LAN	Rede Local
WAN	Rede de Grande Porte
MAN	Rede Metropolitana
PON	Rede Óptica Passiva
OLT	Terminal Óptico da Linha
ONU	Unidade de Rede Óptica
ONT	Terminal de Rede Óptica
CDMA	Acesso Múltiplo por Divisão de Código
OCDMA	Acesso Múltiplo por Divisão de Código Óptico
OOC	Código Ortogonal Óptico
MAI	Interferência de Acesso Múltiplo
QRC	Códigos de Resíduos Quadráticos
OOK	Modulação *On-Off Keying*
BER	Taxa de erro bit
MAP	Maximum a posteriori
AWGN	*Additive White Gaussian Noise*
SNR	Relação sinal ruído
fdc	Função de distribuição cumulativa
fdp	Função densidade de probabilidade
PS	Código Primo
EPS	Código Primo Estendido
QC	Código quadrático
EQC	Código Quadrático Estendido
2-D	Bidimensional
3-D	Tridimensional
QoS	Qualidade de serviço
GMPLS	*Generalized Multiprotocol label switching*
SIR	Relação sinal interferência
WMC	Ristribuição Webb, McIntyre e Conradi

Sigla ou Símbolo	Designação
APD	Fotodetector de avalanche
SIK	Conversão bipolar-unipolar
ML	Máxima verossimilhança
$GF(p)$	Corpo de Galois
p	Número primo
F	Comprimento do OOC
K	Peso do OOC
λ_a	Valor da auto-correlação do OOC
λ_c	Valor da correlação cruzada do OOC
Tx	Transmissor óptico
Rx	Receptor óptico
L	Corpo
φ	homomorfismo injetor
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Z}_p$	Corpo com p primo
T_b	Duração do bit de informação
T_c	Duração do chip
$x_k(t)$	Seqüência de informação
$p_{T_b}(t)$	Pulso retangular
$y_k(t)$	Seqüência espalhamento
$\varepsilon_k(t)$	Campo óptico
$E_k(t)$	Amplitude óptica
ν_0	Freqüência óptica
$I_k(t)$	Sinal óptico
$i(t)$	Fotocorrente
$s_{k,j}(t)$	Saída do receptor
$Z_{k,k}(n)$	Função de Auto-Correlação
$Z_{k,j}(n)$	Função de Correlação Cruzada
$\mathbf{t_X}$	Vetor de atrasos relativos
$\mathbf{R_X}$	Arranjo de números inteiros
λ	Valor da função de correlação
$\mathbf{M_{X,\lambda}}$	Conjunto dos vetores $\mathbf{t_X}$
$\mathcal{C}$	Código
$\lvert\mathcal{C}\rvert$	Cardinalidade do código
$\Phi\left(F, K, \lambda\right)$	Valor da cardinalidade do código
Pe	Probabilidade de erro de bit
$\Pr\{S_i \lvert R_i\}$	Probabilidade a posteriori
$\Pr\{S_i\}$	Probabilidade a priori
γ	Razão de verossimilhança

Sigla ou Símbolo	Designação
$\mathrm{erf}(x)$	Função de erro
$\mathrm{erfc}(x)$	Função de erro complementar
$\mathrm{Q}(x)$	Função área de cauda de gaussiana
$\lambda(t)$	Taxa de pares elétron-lacunas por unidade de tempo
R	Responsividade do fotodetector
q	Carga do elétron
$h\nu$	Energia do fóton
$P_r(t)$	Potência recebida
η	Eficiência qüântica
N_j	Quantidade de portadores elétricos
$P(N_j = N)$	Taxa de portadores ópticos
r	Valor médio da taxa de fótons incidentes
$\mathbb{Z}_2$	Reticulado
$\varphi(p)$	Função de Euler
$\mathbb{Z}^n$	Espaço inteiro euclidiano n-dimensional
$\mathbb{R}^n$	Espaço real euclidiano n-dimensional
S	Conjunto em $\mathbb{R}^n$
G	Grupo de transformações
H	Subconjunto de transformações
$Sym(A)$	Grupo de simetrias do subgrupo A
$Stab(a)$	Estabilizador do ponto $a \in S$
$\mathbb{X}^{\mathbb{T}}$	Código sobre um conjunto $\mathbb{X}$
$\sum$	Grupo de transformações
Λ	Subgrupo de transformações
$\mathbb{C}$	Código de grupo
$\mathbf{I}$	Transformação identidade
$\mathcal{I}_{SO_n}$	Grupo de isometrias
$\mathcal{I}_r$	Subgrupo normal de isometrias
c_{ij}	Símbolo binário da palavra-código
s_{ij}	Elemento da palavra-código
$S_k(t)$	Sinal transmitido
$R(t)$	Sinal recebido
τ_k	Atraso relativo uniformemente distribuído
P_s	Potência do chip
$n(t)$	Ruído branco gaussiano
N_0	Densidade espectral de ruído
$Z_i(t)$	variável de decisão
M	Fator de multiplicação média de avalanche
r	Número de elétrons na saída do APD
n	Número de fótons na entrada do APD

Sigla ou Símbolo	Designação
F_e	Fator de emissão espontânea
k_{ef}	Razão de ionização
$\Phi(X)$	Função de distribuição cumulativa gaussiana
γ_{ot}	Limiar ótimo do receptor sem ruído
λ_s	Taxa de fótons absorvidos
λ	Taxa de absorção total de fótons
M_e	Razão de extinção
λ_b	Taxa de absorção por emissão espúria
Th	Valor limiar do limitador
$\mathbf{k}$	Vetor de estado das interferências
I_1	Arranjos do vetor de estado das interferências
$p_{I_1}(I_1)$	Probabilidade de I_1 interferências
F_{I_1}	Vetor de permutações das interferências
$P(\mathbf{k};F_{I_1})$	Probabilidade de erro do vetor das interferências
NDP	Total de distintas permutações
$\Pr(\lvert\mathbf{k}\rvert = m\lvert I_1)$	Probabilidade do vetor $\mathbf{k}$ possuir $m \neq 0$ elementos
σ^2_{th}	Variância do ruído térmico
i_{Me}	Parâmetro do limitador óptico
c	Velocidade da luz no vácuo
η	Eficiência Qüântica
k_{eff}	Razão de ionização efetiva
I_b	Corrente de fuga de volume do APD
I_s	Corrente de fuga de superfície do APD
λ_b	Taxa de fótons
M_e	Razão de extinção
R_b	Taxa de bits
T_r	Temperatura equivalente de ruído
R_L	Resistor de carga

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Acesso Óptico

1.1 Introdução

Nas últimas três décadas a partir das primeiras demonstrações de sistemas de de transmissão por fibras óticas de baixa atenuação, tem havido um rápido desenvolvimento na transmissão de dados devido à grande diversificação de serviços de telecomunicações, mas, houve também uma convergência no sentido de que muitos serviços podem ser assegurados por uma mesma rede. Logo, novas tecnologias de rede de alta capacidade, que possam oferecer vários serviços simultaneamente, se tornam substanciais. As redes de acesso podem ser dividas, quanto ao seu tamanho, nas seguintes categorias: redes locais - LAN, redes de grande porte - WAN, e redes metropolitanas - MAN. Em redes locais (LAN), encontra aplicação a rede de acesso óptico. A rede óptica de acesso é um conjunto de tecnologias fotônicas para oferecer novos tipos de serviços e usada para conectar as LAN à rede maior.

A rede óptica passiva (PON), a forma mais implementada de rede de acesso óptico, é uma tecnologia fotônica de acesso com banda larga que oferece, em potencial, ampla largura de banda à custo compatível com as diferentes tecnologias de rede. A PON não contém componentes ativos (requerem potência entre o transmissor e receptor) sendo composta de: optical line terminals (OLT), optical network units (ONU), splitters passivos e optical network terminals (ONT). As transmissões e recepções em PON são realizadas por meio de três topologias, a saber, anel, barramento e árvore [3]. Em redes PON, uma das técnicas usadas para acesso múltiplo é o CDMA (Code Division Multiple Access) cuja principal vantagem consiste no fato de que vários canais podem ser simultaneamente alocados em um meio óptico, conforme ilustrado na Figura 1.1, sem requerer sincronismo entre eles.

O CDMA (acesso múltiplo por divisão de código) assegura que os diferentes usuários possam compartilhar da capacidade de transmissão do sistema e é baseado no espalhamento espectral em que a modulação usada expande o espectro do sinal codificado sobre uma largura de faixa maior do que a faixa do sinal original, como ilustrada na Figura 1.2.

A técnica CDMA provê o acesso, sem necessidade de sincronização, à rede e o número de potenciais assinantes é maior que o número de usuários simultâneos. Por conta destes fatores, esta técnica em fibra óptica é mais apropriado às redes LAN. Na essência, a técnica

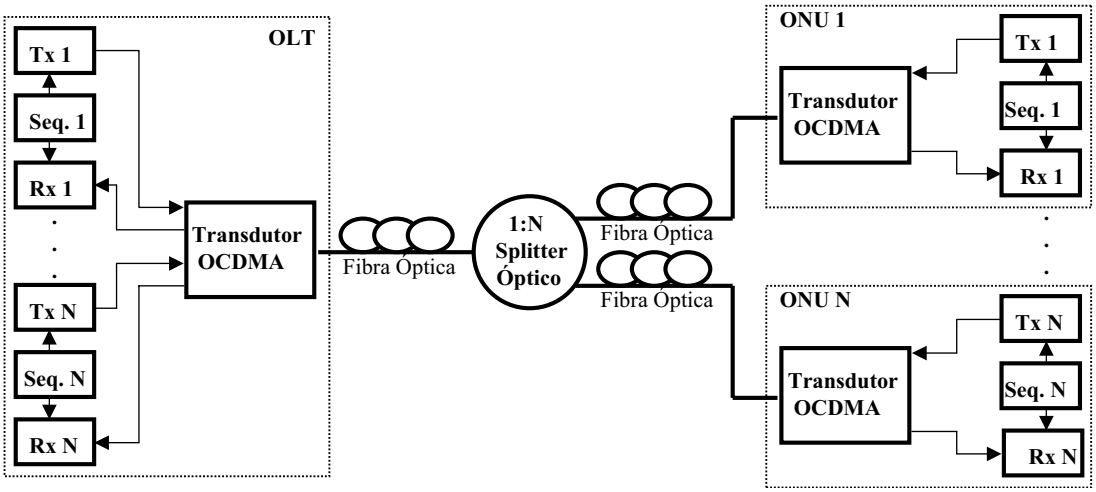


Figura 1.1: Rede PON com OCDMA.

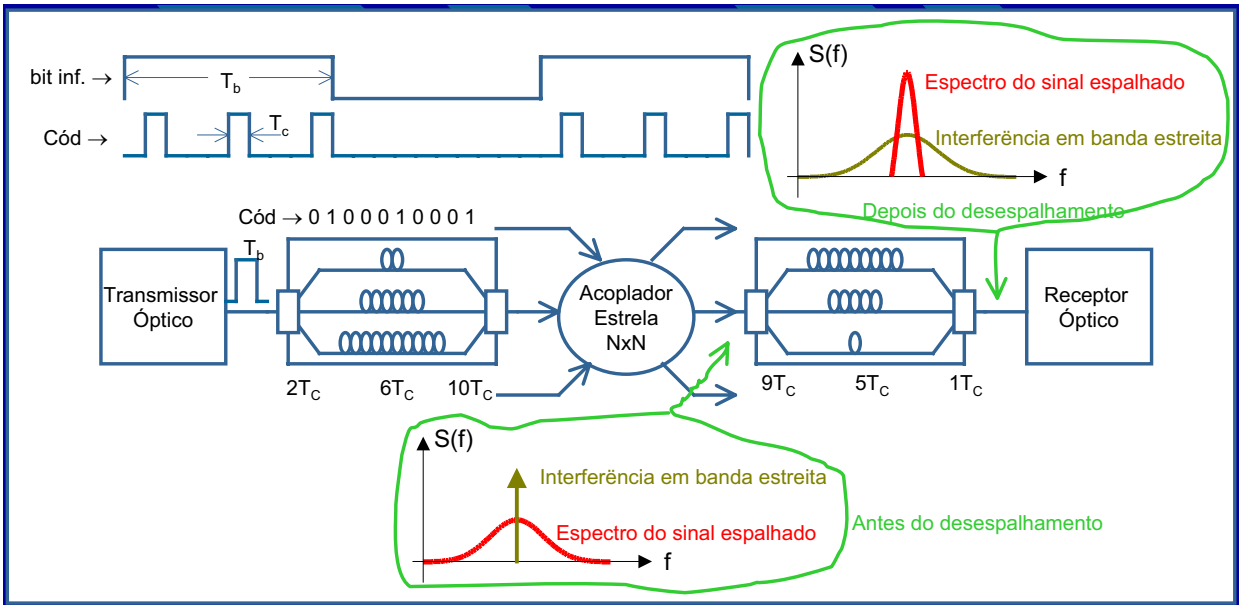


Figura 1.2: Princípio de Operação do Sistema OCDMA

CDMA codifica a informação de forma única para cada usuário. O enlace é estabelecido entre o transmissor e o receptor ajustando ambos a um mesmo código. O transmissor codifica a informação e o receptor reconhece os chips da seqüência desejada, filtrando todas as demais seqüências. Com aumento do número de usuários, a interferência dos canais indesejados aumenta proporcionalmente, degradando o sinal desejado.

Os sistemas OCDMA têm-se tornado populares devido à sua eficiência em usar a largura de faixa oferecida pela fibra óptica e oferecer aos usuários um acesso assíncrono. Os diferentes tipos de sistemas OCDMA estão relacionados a variadas formas de implementar a codificação e a decodificação [4], como ilustrados na Figura 1.3.

Os sistemas OCDMA com espalhamento por seqüência direta são os mais usados e utilizam códigos ortogonais, como os códigos de assinaturas, conseqüentemente, o número de

usuários simultâneos está diretamente relacionado ao comprimento do código. Estes sistemas podem ser classificados em duas sub-categorias: (a) OCDMA coerentes, (b) OCDMA não coerentes.

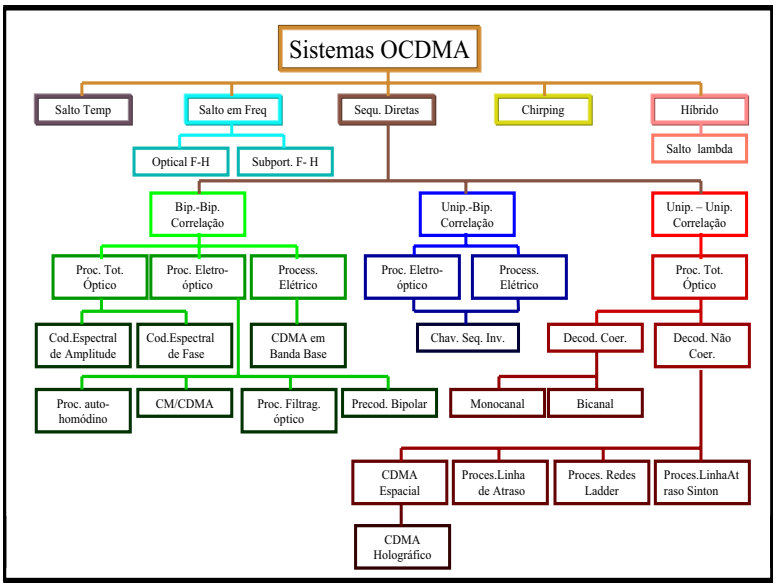


Figura 1.3: Classificação dos sistemas ópticos CDMA.

Nos sistemas ópticos CDMA, cada usuário é rotulado por meio de uma seqüência de um código ortogonal óptico (OOC) para espalhamento da informação. Diferentes métodos são usados na geração das seqüências de espalhamento, todavia, os dois mais aplicados são o de salto em freqüência e seqüência pseudo-aleatória. No salto em freqüência, é gerada uma portadora com freqüência variável "salto" para cada bit. O método de espalhamento, através de seqüência pseudo-aleatória consiste de chips binários com duração menor do bit de informação. Em razão dos bits de informação serem substituídos por chips da seqüência de espalhamento, o espectro do sinal de informação é expandido.

Um código OOC descreve a família de seqüências unipolares (palavras-código) cuja auto-correlação λ_a e correlação cruzada λ_c são menores ou iguais a um, $(\lambda_a = \lambda_c \leq 1)$. Tais códigos minimizam a interferência de múltiplo acesso "MAI - Multiple Access Interference", em sistemas não coerentes, ao mesmo tempo que impõem sérias restrições ao número de seqüências do código, para um dado comprimento [5]. A ortogonalidade, $(\lambda_a = \lambda_c = 0)$, entre as seqüências não pode ser obtida porque os sinais são unipolares, ou seja, dois sinais somados não podem ser iguais a zero, em se tratando de soma de potência. Logo, são necessários códigos de baixa auto-correlação, fora de fase, e baixa correlação cruzada, $(\lambda_a = \lambda_c \leq 1)$.

Logo, esta tese contempla os seguintes objetivos:

• apresentar três novas construções de códigos ortogonais ópticos (OOC), do tipo congruentes, tendo como base a estrutura algébrica do grupo multiplicativo do corpo de Galois $GF(p)$. Avaliar seus desempenhos sob condições de diversos fatores de degradação do sistema OCDMA.

• Mostrar a aplicação da teoria de Gauss como ferramenta matemática para criar novas formas algébricas de códigos ortogonais ópticos, a partir do conjunto de números que formam a representação dos números operação módulo "p".

• Caracterizar os códigos OOC já publicados na literatura, sob o viés da teoria dos códigos. Demonstrar, à luz dos códigos de grupo, que determinadas classes mais abrangentes tornam os códigos OOC casos particulares dos códigos de blocos.

Assim, os objetivos conduziram a organização dos assuntos para estrutura que se segue.

1.2 Estrutura da Tese

O **Capítulo 2** aborda os princípios e conceitos fundamentados nas áreas da teoria dos números, álgebra abstrata, teoria combinatória, e da teoria de transmissão usados em comunicações ópticas para construção de códigos OOC.

O **Capítulo 3** introduz uma técnica de construção de códigos ópticos, visualizando estes no contexto da teoria de códigos. A partir da teoria de Gauss, como ferramenta para criar estruturas algébricas de códigos, o referido capítulo caracteriza os códigos primos e códigos quadráticos como sendo casos particulares dos códigos de Slepian e dos códigos de resíduos quadráticos (QRC), respectivamente.

O **Capítulo 4** apresenta as três novas propostas de códigos ortogonais ópticos, nomeadamente, o código $(F, K, 1, 1) - OOC$, o código $(p(2p-1), p, 1, 2) - OOC$ e o código $((p-1)(2p-1), p-1, 1, 2) - OOC$ que possuem construção algébrica do tipo congruente, tendo como base a estrutura algébrica do grupo multiplicativo do corpo de Galois GF(p). Neste capítulo é ainda realizada a análise das propriedades de correlação e avaliado o desempenho dos códigos propostos, considerando somente a interferência de acesso múltiplo.

O **Capítulo 5** avalia o desempenho de um sistema usando o código $(F, K, 1, 1) - OOC$ proposto, considerando os ruídos balístico, térmico, corrente de escuro do fotodetector (distribuídos de forma gaussiana) e interferência de múltiplo acesso, em um sistema com limitador óptico, devido aos usuários simultâneos como causas de sua degradação.

O **Capítulo 6** apresenta as conclusões e propostas para trabalhos futuros.

O **Apêndice A** apresenta as demonstrações dos teoremas e lemas usados para mostrar e provar, de forma matemática, os conceitos expostos nos respectivos capítulos.

1.2.1 Contribuições da Tese

As contribuições desta tese cobrem as áreas de comunicações ópticas, teoria de códigos e a teoria dos números. A primeira contribuição consiste em apresentar novas famílias de códigos ortogonais ópticos, do tipo congruentes, a partir dos corpos de Galois $GF(p)$. Diversos trabalhos foram publicados sobre códigos ortogonais ópticos (OOC); entretanto, poucos com aplicações de equações diofantinas à teoria de códigos ópticos. Logo, esta tese focaliza aplicações de equações diofantinas parametrizadas na forma algébrica de códigos

ortogonais ópticos para sistemas OCDMA e desperta para o potencial destas equações na construção destes códigos.

A segunda contribuição se presta em uma nova técnica de construção de códigos ópticos enquadrando, de forma eficiente, os códigos ortogonais dentro das classes gerais de códigos, como códigos de permutação e códigos de resíduos quadráticos. Esta contribuição vem da motivação em buscar uma "*estrutura genérica para construção de OOC*", além de apontar para a interconexão entre os códigos OOC e os demais códigos, abrindo nova e interessante direção para futuras pesquisas de OOC.

Uma outra contribuição desta tese consiste na avaliação de desempenho de um sistema OCDMA usando o código $(F, K, 1, 1) - OOC$ proposto e considerando diversos fatores de degradação de desempenho como ruídos e interferência de múltiplo acesso.

Os resultados obtidos nesta tese produziram publicações dentre as quais se os artigos em congressos internacionais e revistas, nomeadamente o LFNM 2002 (IEEE 4th International Workshop on Laser and Fiber-Optical Networks Modeling), o Globecom 2002 e Revista do IEEE América Latina 2005.

Capítulo 2

Definições e Conceitos Preliminares

O capítulo aborda os princípios, conceitos e definições que norteiam e prestam fundamento matemático aos assuntos apresentados nos capítulos subseqüentes da tese. Os conceitos e definições da teoria dos números, da álgebra abstrata, da teoria combinatória e da teoria geral de detecção, e os princípios de detecção óptica são demonstrados para serem utilizados diretamente nos respectivos capítulos.

2.1 Aritmética Modular

Sejam $a,\ b,\ n \neq 0$ números inteiros. Os inteiros a e b são *congruentes módulo* n quando a diferença entre eles, $a - b$, é divisível por n, ou seja,

$$a \equiv b \pmod{n}.$$

Se $a \equiv b \pmod{n}$, então a e b possuem o mesmo resto quando divididos por n, isto é, a e b são *resíduos módulo* n um do outro, logo $(a, n) = (b, n)$. Os elementos a e b pertencem à mesma classe de resíduo quando ambos possuem o mesmo *resíduo módulo* n. Existe em todas classes *módulo* n correspondentes n possíveis valores de resíduo $0, 1, 2, 3, ..., n-1$. Assim, $a \equiv b \pmod{n}$ é a condição necessária e suficiente para que os números inteiros a e b pertençam à mesma classe de resíduo *módulo* n. Qualquer conjunto de n inteiros $\{a_0, a_1, a_2, ..., a_{n-1}\}$ que represente todas as classes de resíduos *módulo* n é chamado *conjunto completo de resíduos módulo* n, cuja forma mais simples é $\mathbb{Z}_n \triangleq \{0, 1, 2, 3, ..., n-1\}$.

As operações de congruência possuem as seguintes propriedades:

1. Para todo módulo n, é válido $a \equiv a \pmod{n}$.

2. Se $a \equiv b \pmod{n}$ então, $b \equiv a \pmod{n}$.

3. Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ então, $a \equiv c \pmod{n}$.

4. Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ então, $a \pm c \equiv b \pm d \pmod{n}$.

5. Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ então, $ac \equiv bd \pmod{n}$.

6. Se $a \equiv b \pmod{n}$ então, $a^m \equiv b^m \pmod{n}$ para todo número inteiro positivo m.

7. Se $a \equiv b \pmod{n}$ e $f(x)$ é um polinômio de coeficientes e expoentes inteiros, então, $f(a) \equiv f(b) \pmod{n}$.

8. Se $a \equiv b \pmod{n}$ e $a \equiv b \pmod{m}$, então $a \equiv b \pmod{s}$, s é o mínimo múltiplo comum entre n m.

9. Se d é divisor de n e $a \equiv b \pmod{n}$ então, $a \equiv b \pmod{d}$.

10. Se $am \equiv bm \pmod{n}$ e $m \neq 0$ tal que $(m, n) = 1$ então, $a \equiv b \pmod{n}$.

11. Se $am \equiv bm \pmod{n}$ e $(m, n) = d$ então, $a \equiv b \pmod{\frac{n}{d}}$.

2.1.1 Corpo de Galois $GF(p)$

Sejam L um corpo e $\neq K \subseteq L$. Então, K é um subcorpo de L se, somente se, para todo $\{a, b\} \in K$, $(a - b) \in K$, $(a.b) \in K$, $a \in K \backslash \{0\}$ e $a^{-1} \in K$.

Se L é um corpo, então K é um subcorpo de L ou L é uma extensão do corpo K. De uma forma mais geral, dizemos que o corpo L é uma extensão do corpo K se L contém um subcorpo isomorfo a K, ou seja, se existe um homomorfismo injetor $\varphi : K \rightarrow L$.

Dizemos que L tem característica zero se o corpo primo de L é isomorfo a $\mathbb{Q}$. L tem característica de um número primo p se o corpo primo de L é isomorfo a $\mathbb{Z}_p$. Como todo corpo de característica zero contém os números irracionais e é portanto infinito, todos os corpos finitos possuem característica p. Se p é um número primo, então os inteiros *módulo p* formam um corpo de p elementos, denotado por $\mathbb{Z}_p$, F_p, ou $GF(p)$. Todos os demais corpos com p elementos são isomorfos a $GF(p)$. Este é chamado de corpo de Galois. Logo, $GF(p)$ é um corpo com número finito de elementos.

Tabela 2.1: Elementos do Corpo de Galois $GF(p)$.

p	GF(p)	x
3	1,2	2
5	1,2,4,3	2
7	1,3,2,6,4,5	3
11	1,2,4,8,5,10,9,7,3,6	2
13	1,2,4,8,3,6,12,11,9,5,10,7	2
17	1,3,9,10,13,5,15,11,16,14,8,7,4,12,2,6	3

Se x é um elemento de $GF(p)$, segundo o teorema de Fermat [6], $x^{p-1} = 1$, onde 1 é a identidade multiplicativa de $GF(p)$. Se r é o menor número inteiro positivo e $x^r = 1$, então r é chamado *grau do elemento x*. O grau do elemento é divisor de $p - 1$. Quando $r = p - 1$, então o elemento x é *elemento primitivo de* $GF(p)$, ou seja, todo corpo de Galois $GF(p)$

possui elemento primitivo, de modo que, se x é o elemento primitivo, então todo elemento diferente de zero pertence a seqüência $x^0 = 1, x^1, x^2, x^3, x^4, ..., x^{p-2}$, denominada *potência cíclica do elemento primitivo* x. A Tabela (2.1) mostra as potências cíclicas de $GF(p)$ para valores de $p = 3, 5, 7, 11, 13, 17$.

2.2 Definições e Propriedades dos Códigos Ópticos

Seja a seqüência de informação dada por:

$$x_k(t) = \sum_{l=-\infty}^{\infty} x_{k,l} \;\; p_{T_b}(t - lT_b) \tag{2.1}$$

onde $x_{k,l} \in \{0, 1\}$ e

$$p_{T_b}(t) = \begin{cases} 1 & 0 \leq t < T_b \\ 0 & fora, \end{cases}$$

e a seqüência espalhamento dada por:

$$y_k(t) = \sum_{n=-\infty}^{\infty} y_{k,n} \;\; p_{T_c}(t - nT_c) \tag{2.2}$$

em que $y_{k,n} \in \{0, 1\}$ e

$$p_{T_c}(t) = \begin{cases} 1 & 0 \leq t < T_c \\ 0 & fora \end{cases}$$

onde $y_{k,n} \neq 0$ determinam as posições dos bits "1".

Se o sinal codificado modular uma fonte óptica usando modulação OOK (On-Off Keying), é criado um campo óptico dado pela expressão:

$$\varepsilon_k(t) = \mathrm{Re}[E_k(t) \exp(j2\pi\nu_0 t)],$$

em que a amplitude óptica é dada pela expressão

$$E_k(t) = \sqrt{2I_k(t)} \;,$$

o sinal óptico é dado pela expressão

$$I_k(t) = \frac{E_0^2[s_k(t)]}{2} \;,$$

em que E_0 é o valor de pico da amplitude,

$$s_k(t) = \sum_{l=-\infty}^{\infty} x_{k,l} \; y_k(t - lT_b)$$

e ν_0 é a freqüência óptica.

No receptor o sinal óptico é dado por:

$$\varepsilon(t) = \sum_{k=-\infty}^{\infty} \varepsilon_k(t)$$

gerando uma fotocorrente da pela expressão

$$i(t) \cong \sum_{k=-\infty}^{\infty} s_k(t) \ .$$

Assim, a natureza quadrática do fotodetector limita os códigos a códigos unipolares para aplicação em sistema OCDMA, por isso chamado de sistema positivo. Os códigos unipolares são construídos para operar em sistema de soma de potência, que é o caso do sistema OCDMA, e não em sistema de soma de amplitude. O sistema não coerente é baseado em soma de potência, por isso apropriado para aplicação dos códigos unipolares. Devido ao processamento óptico do sinal ser equivalente à soma de potência, tais sinais não podem ser manipulados de forma apropriada com códigos bipolares, justificando-se a necessidade de nova classe de códigos para processamento do sinal óptico em sistemas OCDMA. Estes códigos unipolares são chamados de códigos ortogonais ópticos.

O sinal de saída do receptor é dado por:

$$s_{k,j}(t) = \sum_{l=-\infty}^{\infty} x_{k,l} \ Z_{k,j}[t - (l+1)T_b], \tag{2.3}$$

onde k e j correspondem ao transmissor e receptor ópticos de diferentes usuários, respectivamente,

$$Z_{k,j}(t) = \sum_{n=0}^{F-1} Z_{k,j}(n) \ p_{T_c}(t - nT_c) \tag{2.4}$$

Sejam $F,\ K,\ \lambda_a,\ \lambda_c$ números inteiros positivos. Seja F o comprimento e K o peso das seqüências, definidas conforme as expressões (2.1) e (2.2), com exatamente K uns e $F - K$ zeros.

Definição 2.2.1. Um código $(F, K, \lambda_a, \lambda_c)$-OOC, que designamos daqui em diante por $\mathcal{C}$, é uma família de seqüências, formadas por (0,1), designadas por *palavras-código*, de comprimento F, peso K, auto-correlação λ_a, fora de pico (*off-peak autocorrelation*), e máxima correlação cruzada λ_c que satisfaz as seguintes propriedades:

Propriedade 2.2.1. (Auto-Correlação)
Seja a palavra-código $\mathbf{y} = (y_0, y_1, y_2, ..., y_{F-1}) \in \mathcal{C}$, e o número inteiro $n \not\equiv 0 \pmod F$. Então,

$$Z_{k,k}(n) = \sum_{m=0}^{F-1} y_m y_{m+n} \leq \lambda_a \tag{2.5}$$

onde $Z_{k,k}(0) = K$.

Propriedade 2.2.2. (Correlação-Cruzada)
Seja $\mathbf{x} = (x_0, x_1, x_2, ..., x_{F-1}) \in \mathcal{C}$, $\mathbf{x} \neq \mathbf{y}$ e o número inteiro n. Então,

$$Z_{k,j}(n) = \sum_{m=0}^{F-1} y_m x_{m+n} \leq \lambda_c \tag{2.6}$$

O desempenho do sistema OCDMA é determinado pelas propriedades de correlação do código usado. A Propriedade 2.2.1 não é condição necessária e suficiente de desempenho do sistema, e pode ser relaxada se o receptor está sincronizado na desejada posição de pico da amplitude de auto-correlação [7]. Tal sistema é do tipo síncrono. No sistema assíncrono [8], a Propriedade 2.2.1 permite reduzir a probabilidade de falso limiar do receptor causado pelos lóbulos laterais da auto-correlação, como ilustrado na Seção 4.5. Neste sistema, é relaxada a necessidade de rígido sincronismo a custo do número de seqüências do código usado se reduzir por um fator $F-1$, quando comparado ao sistema síncrono [9]. A Propriedade 2.2.2 expressa o quanto a seqüência binária Y_k é diferente de todas as outras seqüências de um dado código.

Um sistema ideal é particularizado pelas seguintes características,

$$\begin{cases} Z_{k,k}(n) = 0 & n \neq 0 \quad (2.7a) \\ Z_{k,j}(n) = 0 & k \neq j, \quad (2.7b) \end{cases}$$

ou seja, as palavras-código $\mathbf{y}$ e $\mathbf{x}$ são *ortogonais*, de modo que o sinal de saída do receptor é dado por

$$s_k(t) = K \sum_{l=-\infty}^{\infty} x_{k,l}\ p_{T_b}[t - (l+1)T_b] \tag{2.8}$$

tal que o sinal de informação é perfeitamente recuperado, com atraso máximo de um símbolo.

Os sistemas OCDMA práticos não alcançam as condições ideais de recuperação perfeita do sinal de informação porque os códigos ópticos não são ortogonais no estrito senso [5], isto é, não asseguram as condições (2.7a) e (2.7b). Porém, os códigos ortogonais ópticos são uma classe de códigos cujas propriedades garantem ao receptor óptico recuperação do sinal de informação próxima do ideal. Por esta razão estes códigos são chamados códigos ortogonais (correlação mínima), nas seguintes condições

$$\begin{cases} Z_{k,k}(n) \leq \lambda_a = 1 & n \neq 0 \quad (2.9a) \\ Z_{k,k}(0) = \lambda_a = K \quad (2.9b) \\ Z_{k,j}(n) \leq \lambda_c = 1 & k \neq j \quad (2.9c) \end{cases}$$

do sinal óptico (unipolar).

Como definido em (2.9), uma palavra-código é ortogonal em relação a seus deslocamentos cíclicos se a sua auto-correlação é mínima, e duas palavras-código são ortogonais se a correlação cruzada é mínima.

2.3 Atraso Relativo Adjacente

Definição 2.3.1. Seja o vetor $\mathbf{X} = [x_0, x_1, x_2, ..., x_{F-1}]$ uma palavra-código de $\mathcal{C}$ com peso K em que os componentes $x_{j0} = x_{j1} = x_{j2} = ... = x_{jF-1} = 1$ e seja $\mathbf{t_X} = [t_0, t_1, t_2, ..., t_{K-1}]$ o vetor de todos atrasos relativos entre chips "1" adjacentes do vetor X. Então, os atrasos relativos adjacentes são definidos por:

$$t_i = \begin{cases} j_{i+1} - j_i & i = 0, 1, 2, ..., K-2 \\ \mathbf{F} + j_0 - j_{K-1} & i = K-1 \end{cases} \tag{2.10}$$

Seja $R_X = [r_X(i,j)]$ o vetor-arranjo, $(K-1)$xK, de números inteiros cujos elementos são dados pela expressão:

$$r_X(i,j) = \sum_{k=0}^{i} t_{j \oplus k} \pmod K \tag{2.11}$$

onde o símbolo "$\oplus$"representa a operação adição módulo F.

Definição 2.3.2. [10]-[11] Seja λ um número inteiro $1 \leq \lambda \leq K-1$. O arranjo $M_{X,\lambda}$ assim definido

$$\mathbf{M_{X,\lambda}} \triangleq \left\{ \sum_{k_0=0}^{i_0} t_{j \oplus k_0}, \quad \sum_{k_1=i_0+1}^{i_1} t_{j \oplus k_1}, \quad \sum_{k_2=i_1+1}^{i_2} t_{j \oplus k_2}, ..., \quad \sum_{k_{\lambda-1}=i_{\lambda-2}+1}^{i_{\lambda-1}} t_{j \oplus k_{\lambda-1}} \right\} \tag{2.12}$$

é um conjunto, cujos elementos são os vetores $\mathbf{t_X}$ de comprimento λ, onde $0 \leq i_0 < i_1 < i_2 < i_3 < ... < i_{\lambda-1} \leq K-2$; $j = 0, 1, 2, ..., K-1$. O total de diferentes vetores $\mathbf{t_X}$ em $\mathbf{M_{X,\lambda}}$ é igual a

$$|\mathbf{M_{X,\lambda}}| = K. \begin{pmatrix} K-1 \\ \lambda \end{pmatrix}. \tag{2.13}$$

Da definição (2.3.2) e equação (2.11) decorrem os seguintes lemas:

Lema 2.3.1. Seja $\mathbf{X}$ um vetor conforme a definição 2.3.1. Então,

$$\sum_{t=0}^{F-1} x_t x_{t \oplus \tau} \leq \lambda \tag{2.14}$$

é válida se, somente se, cada elemento de $\mathbf{R_x}$ aparece $\leq \lambda$ vezes em $\mathbf{R_x}$, para todo $1 \leq \tau \leq F-1$

Lema 2.3.2. Sejam $\mathbf{X}$ um vetor conforme a definição 2.3.1 e $\mathbf{Y} = [y_0, y_1, y_2, ..., y_{F-1}]$ outra palavra-código de $\mathcal{C}$. Então,

$$\sum_{t=0}^{F-1} x_t y_{t \oplus \tau} \leq \lambda \tag{2.15}$$

é válida se, somente se, $\mathbf{M_{X,\lambda}} \cap \mathbf{M_{Y,\lambda}} = \emptyset$, para todo $0 \leq \tau \leq F-1$

Lema 2.3.3. Seja $\mathbf{X}$ um vetor conforme a definição 2.3.1. Então,

$$\sum_{t=0}^{F-1} x_t x_{t\oplus\tau} \leq \lambda \tag{2.16}$$

é válida se, somente se, é válida a equação (2.13) para todo $\tau = 1, 2, ..., F-1$, ou seja, a inequação (2.16) é válida se, somente se, todos os vetores que compõem $\mathbf{M}_{\mathbf{X},\lambda}$ são distintos entre si. Assim, os lemas (2.3.1-2.3.3) expressam o significado de $\mathbf{M}_{\mathbf{X},\lambda}$ e $\mathbf{R}_{\mathbf{x}}$.

2.4 Cardinalidade dos Códigos OOC

Fazendo uso do limitante de Johnson [12]-[13] para códigos corretores de erros, com peso constante, a cardinalidade $|\mathcal{C}|$ do código (F, K, λ)-OOC possui limitante superior dado pela expressão

$$\Phi(F, K, \lambda) \leqslant \left\lfloor \frac{1}{K} \left\lfloor \frac{F-1}{K-1} \left\lfloor \frac{F-2}{K-2} \left\lfloor \ldots \left\lfloor \frac{F-\lambda}{K-\lambda} \right\rfloor \right\rfloor \right\rfloor \right\rfloor \right\rfloor, \tag{2.17}$$

onde o símbolo $\lfloor x \rfloor$ denota a parte inteira do valor real x.

Para os códigos que possuem $\lambda_a \neq \lambda_c$, na inequação (2.17), é usado $\lambda = \max\{\lambda_a, \lambda_c\}$. Considerando $\lambda_a = 1$, $\lambda_c = 2$, a equação (2.17) se reduz a

$$\Phi(F, K, \lambda_a, \lambda_c) \leqslant \frac{(F-1)(F-\lambda_c)}{K(K-1)(K-\lambda_c)}. \tag{2.18}$$

Para $\lambda = \lambda_a = \lambda_c = 1$, esta inequação é expressa por

$$\Phi(F, K, 1) \leqslant \left\lfloor \frac{1}{K} \left\lfloor \frac{F-1}{K-1} \right\rfloor \right\rfloor. \tag{2.19}$$

Quando $\lambda_a = 1$, e $\lambda_c = 2$, a inequação (2.17) se reduz a

$$\Phi(F, K, 1, 2) \leqslant \left\lfloor \frac{1}{K} \left\lfloor \frac{F-1}{K-1} \left\lfloor \frac{F-2}{K-2} \right\rfloor \right\rfloor \right\rfloor. \tag{2.20}$$

Todo código $\mathcal{C}$ com cardinalidade máxima é chamado de *código ótimo*. Logo, os códigos cujo total de palavras-código

$$|\mathcal{C}| = \left\lfloor \frac{1}{K} \left\lfloor \frac{F-1}{K-1} \right\rfloor \right\rfloor, \tag{2.21}$$

para $\lambda_a = \lambda_c = 1$, ou expresso pela seguinte equação:

$$|\mathcal{C}| = \left\lfloor \frac{1}{K} \left\lfloor \frac{F-1}{K-1} \left\lfloor \frac{F-2}{K-2} \right\rfloor \right\rfloor \right\rfloor, \tag{2.22}$$

para $\lambda_a = 1$ e $\lambda_c = 2$, são chamados *códigos ótimos*. O uso de códigos OOC ótimos garante a transmissão da informação de forma eficiente e segura para o maior número de usuários em sistemas assíncronos.

Teorema 2.4.1. O limitante inferior da cardinalidade do código C é dado pela expressão:

$$\Phi\left(F,K,\lambda_a,\lambda_c\right) \geq \frac{\left(\begin{array}{c} F \\ K \end{array}\right) - \Lambda}{\Theta} \tag{2.23}$$

onde

$$\Lambda = \frac{1}{2}\left(F-1\right)\left(\begin{array}{c} K \\ \lambda_a+1 \end{array}\right)\left(\begin{array}{c} F \\ K-\lambda_a-1 \end{array}\right);$$

$$\Theta = F\sum_{i}^{\vartheta}\left(\begin{array}{c} F-K \\ K-i \end{array}\right)\left(\begin{array}{c} K \\ i \end{array}\right);$$

$$\vartheta = \min\{F-K\,,\,K\}; \qquad i = \lambda_c + 1.$$

2.5 Códigos Equivalentes

Definição 2.5.1. Dois códigos são equivalentes quando um dos códigos pode ser obtido a partir do outro usando as seguintes operações: **1)** permutação das posições do código; **2)** permutação dos elementos do código em posições fixas.

Situação 2.5.1. $\{012, 120, 201\} \cong \{000, 111, 222\} \subset \{0,1,2\}^3$ em que o símbolo " $\cong$ " significa "equivalente a".

Situação 2.5.2. $X = \{0,1,2,3\}, M = 4, C = \{00123, 10101, 23103, 33323\}, n = 5, C \subset X^5$ então $C \cong C_{eq1} = \{32100, 10101, 30132, 32333\}$, para a operação (1) e $C \cong C_{eq2} = \{32100, 10101, 30132, 32333\}$, para operação (2) .

Proposição 2.5.1. Se o código C é equivalente ao código C' então a operação $d(C) = d(C')$.

Demonstração da Proposição 2.5.1
Considerando que as operações 1) e 2) da definição (2.5.1) preservam a distância de Hamming entre dois vetores, portanto $d(x,y) = d(\psi(x), \psi(y))$ em que ψ representa a operação 1) ou 2). ■

Lema 2.5.1. Todo código (n, M, d), com os seguintes elementos {0,1,2,...,p-1}, é equivalente ao código (n, M, d) que possui a palavra-código 000....0.

Demonstração do Lema 2.5.1
Sejam $c = (x_1, x_2, ..., x_F) \in C$ e $\sigma_F \in S_p$ a permutação $\sigma_i(x_i) = 0$ para todo $i \in [1, F]$. Portanto F operações do tipo 2) dadas por $\sigma_1, \sigma_2, ..., \sigma_F$, são aplicáveis. ■

2.6 Teoria da detecção

No sistema binário de comunicações, minimizar a probabilidade de erro é equivalente a minimizar o paradigma de Bayes, através da expressão [14]:

$$Pe = \Pr\{S_1|R_i\}\Pr\{R_i\} + \Pr\{S_0|R_i\}\Pr\{R_i\} \tag{2.24}$$

O receptor calcula as probabilidades $\Pr\{S_1|R_i\}$ e $\Pr\{S_0|R_i\}$ e decide que o bit "1" foi transmitido caso $\Pr\{S_1|R_i\} > \Pr\{S_0|R_i\}$ ou decide que o bit "0" foi transmitido caso $\Pr\{S_1|R_i\} < \Pr\{S_0|R_i\}$, ou seja,

$$\Pr\{S_1|R_i\} \gtrless \Pr\{S_0|R_i\} \tag{2.25}$$

onde
$\Pr\{S_i|R_i\}$ é a probabilidade de S_i ser transmitido, dado que R_i foi detetado;
$\Pr\{S_i\}$ é a probabilidade de S_i ser transmitido;
$\Pr\{R_i|S_i\}$ é a probabilidade de R_i ser detetado, dado que S_i foi transmitido;
$\Pr\{R_i\}$ é a probabilidade de R_i ser detetado;
$\Pr\{S_i|R_i\}$ é chamada de *probabilidade a posteriori*, porque determina R_i a partir do conhecimento de que S_i foi transmitido e trafega pelo canal de comunicação;
$\Pr\{S_i\}$ é chamada de *probabilidade a priori*, porque determina S_i a partir do prévio conhecimento de que S_i vai ser transmitido.

Em sistemas de comunicações com M símbolos transmitidos, o detector ótimo é do tipo *maximum a posteriori (MAP)*, ou seja, o detector que possui mínima probabilidade de erro para estimar o símbolo transmitido. O detector MAP demodula R_i, calcula as probabilidades a posteriori $(\Pr\{S_i|R_i\}, \Pr\{R_i|S_i\})$ de cada um dos M possíveis símbolos transmitidos e decide sobre o símbolo $\{0, 1\}$ transmitido com máxima probabilidade a posteriori de ser a detecção correta. O critério MAP de decisão, equação (2.25), pode ser expresso da seguinte forma:

$$\gamma = \frac{\Pr\{R_i|S_1\}}{\Pr\{R_i|S_0\}}\frac{\Pr\{S_1\}}{\Pr\{S_0\}} = \frac{\frac{\Pr\{R_i|S_1\}\Pr\{S_1\}}{\Pr\{R_i\}}}{\frac{\Pr\{R_i|S_0\}\Pr\{S_0\}}{\Pr\{R_i\}}} = \frac{\Pr\{S_1|R_i\}}{\Pr\{S_0|R_i\}} \gtrless 1 \tag{2.26}$$

Assim, no critério MAP o detector decide pelo bit "1" para $\gamma > 1$ ou decide pelo bit "0" para $\gamma < 1$. Quando $\gamma = 1$ o detector decide, de forma aleatória, pelo bit "1" ou pelo bit "0". Quando: $\Pr\{S_i\} = \Pr\{R_i\} = \frac{1}{2}$ a equação (2.26) se reduz à seguinte *razão de verossimilhança*:

$$\gamma = \frac{\Pr\{S_1|R_i\}}{\Pr\{S_0|R_i\}} \gtrless 1 \tag{2.27}$$

O detector, baseado na equação (2.27), para estimar o sinal recebido é chamado de detector de *máxima verossimilhança (ML)*. Este é equivalente ao detector MAP quando os símbolos transmitidos são equivocáveis, ou seja, $\Pr\{0\} = \Pr\{1\} = \frac{1}{2}$. O detector ML representa um detector ótimo, ou seja , que possui a mínima probabilidade de erro. Portanto, *o critério MAP é o critério da mínima probabilidade de erro.* O desempenho dos receptores

é expresso pela probabilidade de erro (BER - *Bit Error Rate*), definida como a probabilidade de detecção incorreta do bit pelo detector.

As probabilidades condicionais são obtidas usando a expansão assintótica das funções erro erf, e erro complementar, (erfc) no cálculo da probabilidade de erro do receptor. Assim,

$$\begin{aligned} P(I=0<\gamma_{ot}|1) &= \int_{-\infty}^{\gamma_{ot}} \frac{1}{\sqrt{2\pi}\sigma_1}\exp\left[-\frac{(I-I_1)^2}{2\sigma_1^2}\right]dI \\ &= \int_{-\infty}^{\frac{\gamma_{ot}-I_1}{\sigma_1}} \frac{1}{\sqrt{2\pi}}\exp(-\frac{y^2}{2})dy \\ &= \left[1-\mathrm{Q}\left(\frac{\gamma_{ot}-I_1}{\sigma_1}\right)\right] \\ &= 1-\frac{1}{2}\left[1-\mathrm{erf}\left(\frac{\gamma_{ot}-I_1}{\sqrt{2}\sigma_1}\right)\right] \\ &= 1-\frac{1}{2}\,\mathrm{erfc}\left(\frac{\gamma_{ot}-I_1}{\sqrt{2}\sigma_1}\right) \end{aligned} \tag{2.28}$$

e de forma análoga:

$$\begin{aligned} P(I=1\geq\gamma_{ot}|0) &= \int_{\gamma}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_0}\exp\left[-\frac{(I-I_0)^2}{2\sigma_0^2}\right]dI \\ &= \int_{\frac{\gamma-I_0}{\sigma_0}}^{\infty} \frac{1}{\sqrt{2\pi}}\exp(-\frac{y^2}{2})dy \\ &= \mathrm{Q}\left(\frac{\gamma_{ot}-I_0}{\sigma_0}\right) = \frac{1}{2}\left[1-\mathrm{erf}\left(\frac{\gamma_{ot}-I_0}{\sqrt{2}\sigma_0}\right)\right] = \frac{1}{2}\,\mathrm{erfc}\left(\frac{\gamma_{ot}-I_0}{\sqrt{2}\sigma_0}\right) \ . \end{aligned} \tag{2.29}$$

Usando a mudança de variáveis $y=\frac{I-I_1}{\sigma_1}$ e $y=\frac{I-I_0}{\sigma_0}$, respectivamente, considerando as relações entre as funções Q, erf, e erfc dadas pelas seguintes expressões:

$$\mathrm{Q}(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty}\exp(-\frac{y^2}{2})dy = \frac{1}{2}\left[1-\mathrm{erf}\left(\frac{x}{\sqrt{2}}\right)\right] = \frac{1}{2}\,\mathrm{erfc}\left(\frac{x}{\sqrt{2}}\right) \tag{2.30}$$

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^{x}\exp(-y^2)dy \tag{2.31}$$

$$\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^{\infty}\exp(-y^2)dy \tag{2.32}$$

sendo válidas as seguintes propriedades:

$$\mathrm{Q}(-x) = 1-\mathrm{Q}(x) \tag{2.33}$$

$$\mathrm{Q}(0) = \frac{1}{2} \tag{2.34}$$

tem-se que a probabilidade de erro (A.2) se torna igual a:

$$\begin{aligned} Pe &= P(I=1\geq\gamma|0)P(0)+P(I=0<\gamma|1)P(1) \\ &= \frac{1}{2}\left\{\mathrm{Q}\left(\frac{\gamma_{ot}-I_0}{\sigma_0}\right)+\left[1-\mathrm{Q}\left(\frac{\gamma_{ot}-I_1}{\sigma_1}\right)\right]\right\} \end{aligned} \tag{2.35}$$

2.6.1 detecção Óptica Ideal

Na detecção óptica, a quantidade de portadores elétricos gerada depende da potência óptica incidente. A taxa de portadores elétricos (pares elétron-lacunas) gerados por unidade de tempo pelo fotodetector é função do tempo dada por:

$$\lambda(t) = \frac{R}{q} P_r(t) \qquad \text{(pares elétron-lacunas por segundo)} \tag{2.36}$$

em que $R = \frac{\eta q}{h\nu}$ é a responsividade do fotodetector, q é a carga do elétron, $h\nu$ é energia do fóton, $P_r(t)$ é a potência recebida em Watts, η é a eficiência qüântica que corresponde a eficiência de conversão de portadores ópticos (fótons) para portadores elétricos. A eficiência qüântica é definida pela relação

$$0 \leq \eta = \frac{\text{número de portadores elétricos gerados}}{\text{número de portadores ópticos incidentes)}} \leq 1 \tag{2.37}$$

A quantidade total de portadores elétricos gerados, durante o período (T) do sinal na $j-$ *ésima* observação, é dada pela expressão:

$$N_j = \int_0^T \lambda_j(\tau) d\tau \tag{2.38}$$

A geração de fótons no transmissor óptico é um processo aleatório [15]. Conseqüentemente, a incidência destes pelo fotodetector pode ser representada pelo processo de contagem de Poisson. A taxa de portadores ópticos que incidem no fotodetector na $j-$ *ésima* observação pode ser representada pela distribuição de Poisson [15] da pela expressão:

$$P(N_j = N) = \frac{\left(\int_0^T \lambda_j(\tau) d\tau \right)^N}{N!} \exp\left[- \int_0^T \lambda_j(\tau) d\tau \right] \tag{2.39}$$

A expressão (2.39) representa um processo de Poisson não-homogêneo condicional (*conditional inhomogeneous Poisson process*) com taxa de portadores elétricos igual a $\lambda(t)$. Este é condicionado ao valor da potência não-homogênea recebida devido a esta potência variar com o tempo. Para potência recebida constante o processo é chamado homogêneo. Para um fotodetector que gera N portadores elétricos no intervalo de tempo T, são válidas as expressões da taxa de portadores e fotocorrente, respectivamente:

$$\lambda(t) = \frac{N}{T} \qquad \text{e} \qquad i(t) = \lambda(t) q = \frac{\eta q}{h\nu} P_r(t) \tag{2.40}$$

Usando a expressão (2.39), a probabilidade de n fótons serem contados, dado que o bit "1" é transmitido, pode ser expressa por:

$$P(n) = \frac{(rT)^n}{n!} \exp(-rT) \tag{2.41}$$

onde $r = \frac{P_{r_1}}{h\nu}$ é o valor médio da taxa de fótons incidente, P_{r_1} é a potência do bit "1", T é o período do bit. A probabilidade do receptor estimar com erro que o bit "1" ou bit "0" tenha sido transmitido é dado pela expressão:

$$Pe = \Pr(0|1)\Pr(1) + \Pr(1|0)\Pr(0) \tag{2.42}$$

onde $\Pr(0) = \Pr(1) = \frac{1}{2}$.

Considerando a modulação OOK (*On-Off Keying*) e o receptor ideal (sem ruído térmico e sem corrente de escuro), a probabilidade de detecção de fótons, dado que o bit "0" foi transmitido, é igual a $\Pr(1|0) = \frac{(0)^n}{n!}\exp(0) = 0$. A probabilidade de detecção de fótons, dado que o bit "1" foi transmitido, é igual a $\Pr(0|1) = \frac{(rT)^0}{0!}\exp(-rT) = \exp(-rT)$. Usando o critério de máxima verossimilhança na decisão, a probabilidade de erro do receptor ótimo é encontrada estabelecendo o limiar de decisão do receptor entre zero e um volt. Então, o receptor decide pelo bit "0", caso a tensão de entrada do detector seja inferior a um volt ou decide pelo bit "1", caso a tensão de entrada do detector seja superior a um volt. Portanto, a probabilidade de detecção de fótons quando o bit "1" é transmitido é dado pela expressão:

$$Pe = \frac{1}{2}\exp(-rT) + \frac{1}{2}(0) = \frac{1}{2}\exp(-\frac{P_{r_1}}{h\nu}T) \tag{2.43}$$

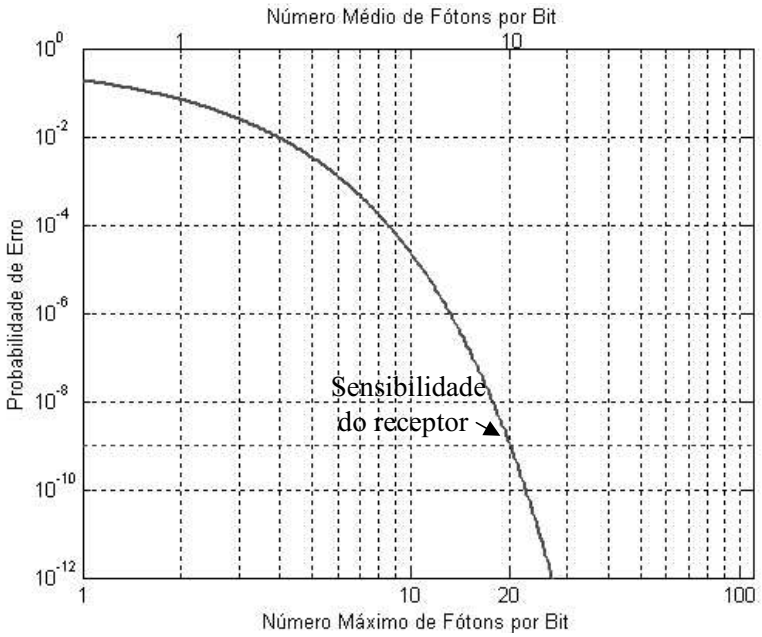


Figura 2.1: Desempenho do receptor óptico ideal versus sinal óptico recebido.

A equação (2.43) representa o limitante fundamental do desempenho do sistema óptico OOK de detecção direta. Para que o desempenho do sistema seja igual a 10^{-9}, são necessários 20 fótons sempre que um bit "1" é transmitido. Considerando equiprováveis os bit "1" e bit "0" e considerando que o bit "0" não requer fótons do transmissor, a sensibilidade do sistema de detecção direta é, em média, igual a 10 fótons por bit. Esta sensibilidade é chamada de *limite qüântico* para sinais do tipo OOK, posto que os efeitos qüânticos associados à fotodetecção são o único fator limitante na especificação da sensibilidade. A Figura (2.1)

apresenta o desempenho do sistema versus amplitude de pico e desempenho vs número médio de fótons por bit. Posto que os lasers emitem radiação eletromagnética, o valor de pico do número de fótons por bit é de particular interesse em sistemas OCDMA. A diferença entre os valores de pico e médio é fator de dois para 50 do decaimento do sinal de saída do sistema OOK. O número de fótons por bit é uma forma particularmente interessante de especificação da sensibilidade porque é independente do comprimento de onda e da taxa de bits de informação. A sensibilidade é freqüentemente especificada no ponto de desempenho igual a 10^{-9} do sistema. Portanto, a sensibilidade qüântica do sistema OOK é de 20 fótons por bit (valor de pico) ou 10 fótons por bit (valor médio).

Capítulo 3

Nova Técnica de construção de Códigos OOC

O objetivo deste capítulo é apresentar a técnica de construção de códigos ópticos que consiste em enquadrar-los como casos particulares de classes mais gerais de códigos.

A contribuição deste capítulo reside em apresentar a nova técnica de construção de códigos ópticos, visualizando-os como casos particulares de códigos mais gerais, mostrando a possibilidade da aplicação da teoria de Gauss como ferramenta para geração de códigos ortogonais e apontando para o potencial desta teoria na construção destes.

Este capítulo está assim ordenado: na Seção 3.1 (Códigos de Bloco Lineares) são estudadas duas classes de códigos cíclicos - os códigos de resíduos quadráticos e os códigos de Slepian; na Seção 3.2 (Códigos de Resíduos Quadráticos), abordam-se o método de análise e a técnica de construção destes últimos códigos; na Seção 3.3 (Códigos de Grupo), é apresentada a teoria de representação de grupos como um isomorfismo da teoria de grupos algébricos com a teoria de álgebra linear, em que um grupo de matrizes de transformações lineares ortogonais representa um grupo algébrico através de um isomorfismo bem definido entre os elementos deste grupo algébrico e o grupo de matrizes de transformações lineares ortogonais; na Seção 3.4 (Casos Particulares dos Códigos de Slepian e Resíduos Quadráticos) é apresentada a estrutura dos códigos Primos e Quadráticos, publicados na literatura, mostrando que ambos são casos particulares dos códigos de Slepian e resíduos quadráticos, respectivamente.

3.1 Códigos de Bloco Lineares

Basicamente os códigos se dividem em dois tipos: *códigos de bloco* e *códigos convolucionais*. Essas classes ainda se subdividem em: ***códigos lineares***, ***códigos cíclicos*** e ***códigos sistemáticos***. Os códigos cíclicos pertencem à classe dos códigos de bloco porque todas as palavras do código possuem o mesmo comprimento. No código cíclico todo deslocamento cíclico da palavra-código resulta em outra palavra-código. Dentre várias classes dos códigos cíclicos são de interesse, para esta tese, os **códigos de resíduos quadráticos** e os

códigos de Slepian ou códigos de permutação.

3.2 Códigos de Resíduos Quadráticos

Os **códigos de resíduos quadráticos** (QRC) são uma classe de códigos cíclicos que possuem comprimento igual a número primo p. O número inteiro α é resíduo quadrático módulo p se a equação (3.6) possui solução, ou seja, se α possui raiz quadrada módulo p. Da teoria dos números, mostra-se que existem $(p-1)/2$ elementos no conjunto dos resíduos quadráticos e $(p-1)/2$ elementos resíduos não quadráticos. A representação dos QRC é feita por meio de reticulados $\mathbb{Z}_2$ ou $\mathbb{A}_2$. Um reticulado é arranjo finito de pontos, que algebricamente formam um grupo sob a adição vetorial, os quais são descritos pelas equações de diofantina. A partir do reticulado, usando os conceitos de reciprocidade quadrática de Gauss e de paridade das palavras-código, são construídos os QRC.

Seja a equação de congruência quadrática

$$ax^2 + bx + c \equiv 0 \pmod{n} \tag{3.1}$$

onde a, b, c são números inteiros, $a \not\equiv 0 \pmod{n}$, $n > 2$, que sujeita às seguintes manipulações matemáticas,

$$\begin{aligned}
&4a(ax^2 + bx + c) \equiv 0 \pmod{4an} \\
&(2ax + b)^2 - b^2 + 4ac \equiv 0 \pmod{4an} \\
&m = 4an; \quad 2ax + b \equiv Y \pmod{m}; \quad b^2 - 4ac \equiv B \pmod{m};
\end{aligned}$$

pode ser expressa na forma

$$Y^2 \equiv B \pmod{m}$$

quando $(B, m) = ke^2 = d$, para e^2 a maior potência quadrada em d considerando $m = 4an = m_0 d$ com $B = db_0$. Logo, ke divide Y então, $Y = kez$, de modo que

$$\begin{aligned}
Y &\equiv kez \pmod{m}; \\
(kez)^2 &\equiv B \pmod{m}; \\
kz^2 &\equiv b_0 \pmod{m_0}
\end{aligned} \tag{3.2}$$

onde z é um número inteiro. Essa equação de congruência possui solução se, somente se, $s|b_0$, para $s = (k, m_0)$. Porém, para (b_0, m_0)=1, a equação (3.2) não possui solução, a menos que $s = 1$.

Seja $s = 1$. Realizando as seguintes manipulações sobre a equação (3.2)

$$\begin{aligned}
(kz)^2 &\equiv kb_0 \pmod{m_0}; \\
y &\equiv kz \pmod{m_0}; \\
y^2 &\equiv kb_0 \pmod{m_0}; \\
kz^2 &\equiv b_0 \pmod{m_0},
\end{aligned} \tag{3.3}$$

esta pode ser apresentada na forma

$$\begin{cases} y^2 \equiv \alpha \pmod{m_0} & \text{(3.4a)} \\ kb_0 \equiv \alpha \pmod{m_0} & \text{(3.4b)} \end{cases}$$

com $(\alpha, m_0) = 1$, para $kb_0 \equiv \alpha \pmod{m_0}$.

Portanto, a busca da solução para a equação de congruência quadrática (3.1) consiste em resolver uma equação de congruência quadrática (3.4a) e outra de congruência linear (3.4b), com incógnita $y \in \mathbb{Z}$; $\{\alpha, m_0\} \in \mathbb{N}$.

Definição 3.2.1. Se $(\alpha, m) = 1$ e a equação (3.5) possui solução, o inteiro α é *resíduo quadrático módulo m (resíduo quadrático de m).* Caso esta não possua solução, o inteiro α é *não-resíduo quadrático módulo m (não-resíduo quadrático de m).*

$$y^2 \equiv \alpha \pmod{m} \tag{3.5}$$

A determinação dos resíduos e não-resíduos quadráticos é equivalente à verificação da possibilidade de solução da equação (3.5). Através da fatoração de m em potências de números primos, reduz-se a equação a uma do tipo $y^2 \equiv \alpha \pmod{p}$ onde p é primo. Para $m = p$ a equação possui ou não solução ([16], lema 8.1, pp. 272). Na busca da solução da equação (3.5), estamos interessados somente na solução que é resíduo quadrático de p.

Caso $p = 2$, todo inteiro ímpar é resíduo quadrático de 2 e os números inteiros pares são excluídos. Porém, para $f(x) = x^2 - a$; $\frac{df(x)}{dx} = 2x$; $d = (\frac{d(2x)}{dx}, 2) = 2$. Portanto, pelo lema 8.1, fica provado que a solução da equação $x^2 \equiv a \pmod{2^{n-1}}$ satisfaz a equação $x^2 \equiv a \pmod{2^n}$ criando, para esta última, duas soluções, ou nenhuma solução pode ser encontrada a partir de x', que é solução da primeira equação. Para a determinação dos resíduos quadráticos para potências de primos pares, precisa-se fazer considerações em contexto separado do contexto dos números primos ímpares, ou seja,

$$y^2 \equiv \alpha \pmod{p} \tag{3.6}$$

Aplicando o critério de Euler para determinar a *condição necessária* da solução para equação (3.6), esta possui solução se, somente se, $\alpha^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Quando $\alpha^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, então α é resíduo quadrático de p e não-resíduo quadrático de p se $\alpha^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Esta condição corresponde ao teste do resíduo quadrático de p se este é um número primo ímpar e α é co-primo de p. Porém, este resultado não garante a *condição suficiente* do resíduo quadrático p. O número de elementos do conjunto de resíduos módulo p é dado pela função de Euler $\varphi(p)$. Se p é um número primo então $\varphi(p) = p-1$. Logo, $\varphi(p)$ representa a cardinalidade do conjunto de resíduos quadráticos módulo p. Por essa razão, é feita, nesta tese, a opção pelo grupo multiplicativo do corpo de Galois ($GF(p) = \mathbb{Z}_p \Rightarrow \varphi(p) = p - 1$) como estrutura algébrica dos códigos propostos no Capítulo 4.

Portanto, fica demonstrado que, através dos teoremas da teoria dos números, podemos encontrar o resíduo quadrático a partir do primo ímpar p. Por outro lado, dado um inteiro

como resíduo quadrático, podemos encontrar o primo ímpar do qual o número inteiro é resíduo quadrático. Se o inteiro dado é ímpar, obviamente é resíduo quadrático do primo 2, de modo que estamos interessados somente nos primos ímpares.

Teorema 3.2.1. ([16] pp. 315) **(Teorema da Reciprocidade Quadrática de Gauss)** Seja $p \neq q$ números primos. Então,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2}\frac{q-1}{2})} \tag{3.7}$$

O Teorema 3.2.1 permite determinar os primos ímpares dos quais um dado inteiro é resíduo ou não-resíduo quadrático. Quando se pretende encontrar os primos dos quais um número composto é resíduo ou não-resíduo quadrático, este composto precisa ser fatorado como produto de primos. Assim, o Teorema 3.2.1 garante a *condição necessária e suficiente*, para que qualquer número inteiro positivo seja resíduo ou não-resíduo quadrático do primo ímpar p.

Usando o lema de Gauss, podemos caracterizar todos os primos que possuem o inteiro 2 por resíduo quadrático. Conseqüentemente, pelo Teorema 9.5 ([16] pp. 305) o inteiro 2 é resíduo quadrático de todos os primos da forma $p \equiv \pm 1 \pmod 8$, e não-resíduo quadrático de todos os primos da forma $p \equiv \pm 3 \pmod 8$.

3.2.1 Teoria dos Reticulados

A geometria dos códigos de resíduos quadráticos pode ser determinada fazendo uso da teoria de reticulados.

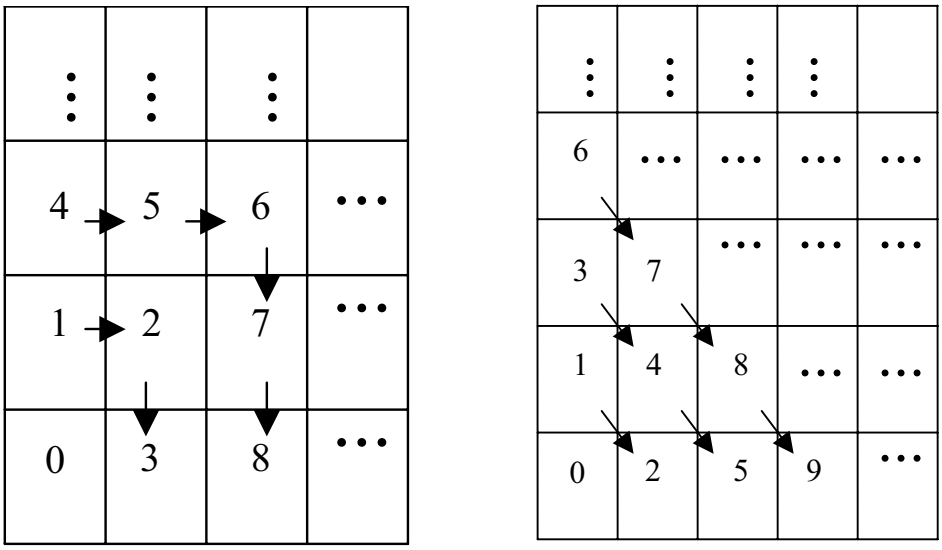
Definição 3.2.2. Um conjunto de pontos cujas coordenadas $(x_0, x_1, x_2, ..., x_{n-1}) \in \mathbb{R}^n$ são números inteiros em $\mathbb{Z}^n$, é um reticulado.

Assim, os conjuntos S pertencem ao espaço real euclidiano n-dimensional $\mathbb{R}^n$ e seus pontos estão em $\mathbb{Z}^n$. Os teoremas de Blichfeldt e Minkowski formam a base da teoria dos reticulados na busca de aproximações aos pontos do reticulado de uma superfície fechada no plano ou espaço.

Teorema 3.2.2. [17] **(Blichfeldt)**
Seja S um conjunto em $\mathbb{R}^n$, com volume $v(S) > 1$. Então, existem dois pontos distintos $\mathbf{s}' \in S$ e $\mathbf{s}'' \in S$ tal que o ponto $\mathbf{s}' - \mathbf{s}''$ do reticulado possui coordenadas inteiras.

Teorema 3.2.3. [18] **(Minkowski)**
Seja A uma matriz não singular n x n, cujos elementos são reais, e $\Lambda = A\mathbb{Z}^n$. Se S, em $\mathbb{R}^n$, é um conjunto simétrico e convexo em torno de $\mathbf{0}$, e se $v(S) > 2^n d(\Lambda)$, então existe um ponto do reticulado $\mathbf{x} \in \Lambda$ tal que $\mathbf{x} \neq 0$ e $\mathbf{x} \in S$.

Os reticulados podem ser enumerados na forma quadrangular ou diagonal, conforme a Figura (3.1).



(a) Quadrangular (b) Diagonal

Figura 3.1: Numeração dos Reticulados.

Situação 3.2.1. As coordenadas (x, y) dos pontos do reticulado são $(0,0)$, $(0,1)$, $(1,1)$, $(1,0)$, $(0,2)$, $(1,2)$, $(2,2)$, $(2,1)$, $(2,0)$ e $(0,0)$, $(0,1)$, $(1,0)$, $(0,2)$, $(0,3)$, ... para numeração quadrangular, Figura (3.1(a)), e numeração diagonal, Figura (3.1(b)), respectivamente.

A busca de um reticulado é equivalente a encontrar as soluções inteiras de uma dada equação. De forma mais geral, somos conduzidos à representação de números inteiros por formas quadráticas binárias, isto é, através de equações de diofantina de duas variáveis.

Definição 3.2.3. A equação polinomial cujas soluções e coeficientes são números inteiros é chamada *equação de diofantina*.

Como o reticulado é descrito por uma equação, estamos particularmente interessados pelas soluções das formas quadráticas da equação de diofantina do tipo:

$$x^2 + y^2 = n \tag{3.8}$$

que conduzem a códigos cíclicos, através da matriz de transformação ortogonal T. As soluções para a equação (3.8) são encontradas através da aplicação dos teoremas (3.2.4 e 3.2.5).

Teorema 3.2.4. [19] **(Genus)** A equação (3.8) de diofantina tem solução para n primo se, somente se, n é um número primo do tipo $4k+1$, exceto para $n = 2$, ou seja, $n \equiv 1 \pmod 4$ ou $n \equiv 2 \pmod 4$.

Teorema 3.2.5. 155 **(Composição)**
Seja $Q(x, y) = x^2 + y^2$. Então,

$$Q(x, y)Q(x', y') = Q(xx' - yy', x'y + xy')$$

onde

$$\begin{aligned}(x^2+y^2)(x'^2+y'^2) &= (xx'-yy')^2+(xy'+x'y)^2\\ &= x^2x'^2+y^2y'^2+x'^2y'^2+x^2y'^2\end{aligned}$$

Assim, a busca pelas soluções da equação (3.8) segue o seguinte procedimento:
1) Fatoração de n em números primos através do teorema (3.2.4) de Genus.
2) Resolver a equação (3.8) para os fatores primos encontrados no item anterior.
3) Determinar todas as soluções possíveis da equação (3.8) através do teorema (3.2.5).
4) Em seguida, a determinação das palavras do código cíclico, associado às soluções encontradas, consiste em encontrar uma matriz de transformação ortogonal, cujas colunas são vetores linearmente independentes, com $det(\mathrm{T}) = n$. Uma das colunas da matriz T precisa ser uma das soluções, (x, y), da equação (3.8), sendo recomendado o inteiro 1 na sua diagonal, para assegurar a diversidade do código, ou seja, no reticulado cada elemento do código precisa formar um quadrado latino.

O ***algoritmo de construção do código de resíduos quadráticos*** possui os seguintes passos:

Passo 1: Mapear em r_1, r_2 e r_3, onde $r_1 = 0$, os elemento da palavra-código do código p-ário.

Passo 2: Efetuar operação adição módulo p para encontrar os elementos da palavra-código do código de resíduos quadráticos.

$$\begin{aligned}s_{i1} &= r_1,\\ s_{i2} &= r_1 + r_2,\\ s_{i3} &= s_{i2} + r_3,\\ s_{i3} &= s_{i1} \oplus s_{i2}\\ &\vdots\\ s_{ij} &= s_{i(j-2)} \oplus s_{i(j-1)}\end{aligned}$$

em que $1 \leq j \leq \frac{p-1}{2}$ e $1 \leq i \leq p$.

Passo 3: Mapear, em suas respectivas imagens, os elementos s_{ij} do Passo 2 com $\frac{p-1}{2}+2 \leq j \leq p$.

Passo 4: Através da paridade zero da palavra-código cujos elementos foram encontrados nos Passo 2 e Passo 3, encontrar o elemento s_{ij}, onde $j = \frac{p-1}{2} + 1$.

Passo 5: Realizar os Passos 1 a 4 do presente algoritmo para todas as palavras do código p-ário.

Passo 6: Completar o código de resíduos quadráticos colocando a palavra-código zero na primeira linha, seguida das outras palavras do código. Nos dois exemplos seguintes, é apresentada a forma sistemática de construção dos códigos de resíduos quadráticos a partir de $\mathbb{Z}_5$ e $\mathbb{Z}_7$.

	0	1	2	3	4
0	00				
1			12		
2					24
3		31			
4				43	

Tabela 3.1: Reticulado $\mathbb{Z}_5$.

0	0	0	0	0
0	1	3	1	0
0	2	1	2	0
0	3	4	3	0
0	4	2	4	0

Tabela 3.2: Código de Resíduos Quadráticos $\mathbb{Z}_5$.

Situação 3.2.2. Para a equação de Diofantina $x^2 + y^2 = 5$, fazendo as soluções $(x, y) = (2, -1)$ e $(x, y) = (1, 2)$ como vetores colunas da matriz $T = \begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix}$ o correspondente código 5-ário será $\{00, 12, 24, 31, 43\}$. Este é gerado iniciando de um ponto arbitrário do reticulado, no caso 00, se movimentando pela coordenada x em dois deslocamentos e pela coordenada y em um deslocamento, ou seja, deslocamentos iguais aos valores dos elementos da primeira linha da matriz T. A numeração é feita de forma quadrangular, como mostrada na Figura (3.1a). O código gerado é cíclico, como pode ser visualizado na Tabela (3.1), cada palavra-código aparece uma somente uma vez no quadrado latino.

Aplicando o ***algoritmo de construção do código de resíduos quadráticos***, para $p = 5$, temos:

Passo 1: Mapear os elementos da palavra-código 12 em $r_1 = 0$, $r_2 = 1$ e $r_3 = 2$.

Passo 2: Encontrar os elementos da palavra-código do código de resíduos quadráticos.

$$s_{21} = r_1 = 0; \qquad s_{22} = r_1 + r_2 = 0 + 1 = 1.$$

Passo 3: Os elementos-imagem são

$$s_{24} = 1; \qquad s_{25} = 0.$$

Passo 4:

$$s_{21} + s_{22} + s_{23} + s_{24} + s_{25} = 0 + 1 + s_{23} + 1 + 0 = 0 \pmod 5.$$

Através da paridade obtemos $s_{23} = 3$, de modo que a palavra-código é: $\{0, 1, 3, 1, 0\}$.

Passo 5: As demais palavras-código do código 5-ário são:

$$s_{31} + s_{32} + s_{33} + s_{34} + s_{35} = 0 + 2 + s_{33} + 2 + 0 = 0 \pmod 5 \Rightarrow s_{33} = 1 \Rightarrow \{0, 2, 1, 2, 0\}.$$

$$s_{41} + s_{42} + s_{43} + s_{44} + s_{45} = 0 + 3 + s_{43} + 3 + 0 = 0 \pmod 5 \Rightarrow s_{43} = 4 \Rightarrow \{0, 3, 4, 3, 0\}.$$

$$s_{51} + s_{52} + s_{53} + s_{44} + s_{55} = 0 + 4 + s_{53} + 4 + 0 = 0 \pmod 5 \Rightarrow s_{53} = 2 \Rightarrow \{0, 4, 2, 4, 0\}.$$

Passo 6: O código de resíduos quadráticos, para p=5, é:

$$\{0, 0, 0, 0, 0\}$$

$$\{0, 1, 3, 1, 0\}$$

$$\{0, 2, 1, 2, 0\}$$

$$\{0, 3, 4, 3, 0\}$$

$$\{0, 4, 2, 4, 0\}$$

O passo 6 do algoritmo satisfaz o lema (2.5.1). A simetria entre as colunas da Tabela (3.2) é assegurada pela lei da reciprocidade quadrática de Gauss.

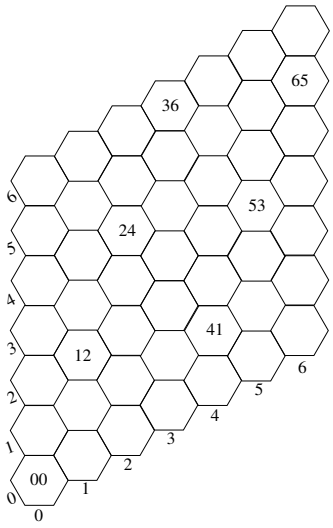


Tabela 3.3: Reticulado $\mathbb{A}_2$.

0	0	0	0	0	0	0
0	1	3	6	3	1	0
0	2	6	5	6	2	0
0	3	2	4	2	3	0
0	4	5	3	5	4	0
0	5	1	2	1	5	0
0	6	4	1	4	6	0

Tabela 3.4: Código de Resíduos Quadráticos $\mathbb{Z}_7$.

Situação 3.2.3. Para a equação de diofantina $x^2 + xy + y^2 = 7$, tornando a solução $(x, y) = (2, 1)$ um dos vetores colunas da matriz $T = \begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix}$, o correspondente código será $\{00, 12, 24, 36, 41, 53, 65\}$. Este código, 7-ário, é gerado iniciando do ponto 00, numerando de forma quadrangular, movimentando-se pelas coordenadas x e y em 2 e 1 deslocamentos, respectivamente. O código gerado é cíclico, como pode ser visualizado na Tabela (3.3), reticulado $\mathbb{A}_2$.

O código de resíduos quadráticos, mostrado na Tabela (3.4), é obtido da seguinte forma: iniciando de um ponto arbitrário do reticulado, no caso 00, movimenta-se pela coordenada x em dois deslocamentos e pela coordenada y em um deslocamento, ou seja, deslocamentos iguais aos valores dos elementos da primeira linha da matriz T. A numeração é feita de forma quadrangular, como mostrada na Figura (3.1). O código gerado é cíclico, como pode ser visualizado na Tabela (3.1); cada símbolo do código aparece uma só vez no quadrado latino.

O ***algoritmo de construção do código de resíduos quadráticos***, para $p = 7$, temos:

Passo 1: Mapear os elementos da palavra-código 12 em $r_1 = 0$, $r_2 = 1$ e $r_3 = 2$.

Passo 2: Encontrar os elementos da palavra-código do código de resíduos quadráticos.

$$\begin{aligned} s_{21} &= r_1 = 0; \\ s_{22} &= r_1 + r_2 = 0 + 1 = 1; \\ s_{23} &= s_{22} + r_3 = 1 + 2 = 3. \end{aligned}$$

Passo 3: Os elementos imagem são

$$s_{25} = 3; \qquad s_{26} = 1; \qquad s_{27} = 0.$$

Passo 4:

$$s_{21} + s_{22} + s_{23} + s_{24} + s_{25} + s_{25} + s_{25} = 0 + 1 + 3 + s_{24} + 3 + 1 + 0 = 0 \pmod 7.$$

Através da paridade obtemos $s_{23} = 6$, de modo que a palavra-código é: $\{0, 1, 3, 6, 3, 1, 0\}$.

Passo 5: As demais palavras-código do código 7-ário são

$$\begin{aligned} s_{31} + s_{32} + s_{33} + s_{34} + s_{35} + s_{36} + s_{37} &= \\ &= 0 + 2 + 6 + s_{34} + 6 + 2 + 0 = 0 \pmod 7; \\ s_{34} &= 5; \\ \{0, 2, 6,&5, 6, 2, 0\}. \\ s_{41} + s_{42} + s_{43} + s_{44} + s_{45} + s_{46} + s_{47} &= \\ &= 0 + 3 + 2 + s_{44} + 2 + 3 + 0 = 0 \pmod 7; \\ s_{44} &= 4; \\ \{0, 3, 2,&4, 2, 3, 0\}. \\ s_{51} + s_{52} + s_{53} + s_{54} + s_{55} + s_{56} + s_{57} &= \\ &= 0 + 4 + 5 + s_{54} + 5 + 4 + 0 = 0 \pmod 7; \\ s_{54} &= 3; \\ \{0, 4, 5,&3, 5, 4, 0\}. \\ s_{61} + s_{62} + s_{63} + s_{64} + s_{65} + s_{66} + s_{67} &= \\ &= 0 + 5 + 1 + s_{64} + 1 + 5 + 0 = 0 \pmod 7; \\ s_{64} &= 2; \\ \{0, 5, 1,&2, 1, 5, 0\}. \\ s_{71} + s_{72} + s_{73} + s_{74} + s_{75} + s_{76} + s_{77} &= \\ &= 0 + 6 + 4 + s_{74} + 4 + 6 + 0 = 0 \pmod 7; \\ s_{74} &= 1; \\ \{0, 6, 4,&1, 4, 6, 0\}. \end{aligned}$$

Passo 6: O código de resíduos quadráticos, para p=7, é

$$\{0,0,0,0,0,0,0\}$$
$$\{0,1,3,6,3,1,0\}$$
$$\{0,2,6,5,6,2,0\}$$
$$\{0,3,2,4,2,3,0\}$$
$$\{0,4,5,3,5,4,0\}$$
$$\{0,5,1,2,1,5,0\}$$
$$\{0,6,4,1,4,6,0\}.$$

3.3 Códigos de Grupo

Seja G um grupo de transformações inversíveis a partir do conjunto S, não vazio, para o conjunto S. O subconjunto de transformações $H < G$ é *transitivo* no subgrupo $A \subseteq S$ se para todo par $\{a, b\} \in A$, existe a transformação $h \in H$, tal que $h(a) = b$. A transformação H é chamado de estritamente transitivo se h é único para cada par a, b, no qual $|H| = |A|$.

Definição 3.3.1. O subgrupo de todas as transformações em G, sob a qual o conjunto A é invariante, é chamado de grupo de simetrias do subconjunto $A \subseteq S$ em relação G, isto é,

$$Sym(A) \cong Sym_G(A) \cong \{g \in G \mid g(a) \in A, \forall a \in A\}$$

Definição 3.3.2. O subgrupo assim definido,

$$Stab(a) \cong Stab_G(a) \cong \{g \in G \mid g(a) = a\}$$

é chamado de estabilizador do ponto $a \in S$. Conseqüentemente [25],

$$Stab(A) = Stab_G(A) = \bigcap_{a \in A} Stab(a)$$

O estabilizador do ponto a coincide com o grupo de simetrias do conjunto singular $\{a\}$, isto é, $Stab(a) = Sym(\{a\})$. O estabilizador do conjunto A é um *subgrupo normal*, $Stab(A)$, do grupo de simetria $Stab(A) \lhd Sym(A)$.

Definição 3.3.3. O subgrupo $H < G$ é um subgrupo normal, ou seja, $H \lhd G$, se $g^{-1}Hg = H, \ \forall g \in G$

Um código sobre um conjunto $\mathbb{X}$, não vazio, é um subconjunto $\mathbb{C} \subseteq \mathbb{X}^{\mathbb{T}}$, indexado pelo conjunto $\mathbb{T}$, o qual está associado ao eixo do tempo,

$$\mathbb{X}^{\mathbb{T}} \cong \{\mathbf{x} \mid \mathbf{x} : \mathbb{T} \longrightarrow \mathbb{X}, \ x_k \in \mathbb{X}, \ \forall k \in \mathbb{T}\}$$

onde o elemento $\mathbf{x} \in \mathbb{C}$ é chamado de palavra-código. O código é chamado finito ou infinito em função da cardinalidade $|\mathbb{C}|$ do conjunto $\mathbb{C}$.

Definição 3.3.4. Seja $\sum$ um grupo de transformações inversíveis do conjunto $\mathbb{X}^{\mathbb{T}}$. Se existem o subgrupo $\Lambda < \sum$ e o ponto $\mathbf{x} \in \mathbb{X}^{\mathbb{T}}$, tal que $\mathbb{C} = \Lambda(\mathbf{x_0})$, então $\mathbb{C}$ é um ***código de grupo***.

Assim, Λ e $\mathbf{x_0}$, para um dado grupo, não são necessariamente únicos. Quando o código possui Λ finito, então $\mathbb{C}$ é código de grupo finito.

Definição 3.3.5. Se o conjunto $\mathbb{X}^{\mathbb{T}}$ é um espaço métrico e o grupo de transformações $\sum$ consiste de isometrias de $\mathbb{X}^{\mathbb{T}}$, ou seja, distância que preserva as transformações $\|\mathbf{x} - \mathbf{y}\| = \|\lambda(\mathbf{x}) - \lambda(\mathbf{y})\|,\ \forall \mathbf{x}, \mathbf{y} \in \mathbb{X}^{\mathbb{T}}$, então o código de grupo $\Lambda(\mathbf{x_0})$ é chamado de *código de grupo de isometria*.

Definição 3.3.6. [20] Sejam $\forall H < G;$ e $\forall \lambda_i \in G$, chamados de *classe lateral à esquerda e classe lateral à direita de* H, respectivamente, no grupo G. Qualquer elemento da classe lateral ("coset") é chamado de *representante da classe lateral*.

O conjunto gerador do código de grupo $\mathbb{C} = \Lambda(\mathbf{x_0})$, em relação a $\mathbf{x_0} \in \mathbb{C}$, é um conjunto minimal de transformações $\Lambda_g \subseteq Sym(\mathbb{C})$, tal que $\Lambda_g(\mathbf{x}) = \Lambda(\mathbf{x_0})$. Quando Λ é um grupo que define o código de grupo $\mathbb{C}$, em relação ao elemento gerador $\mathbf{x}_0$, então o conjunto gerador do código $\mathbb{C}$ pode ser obtido mediante a escolha do representante de cada classe lateral do subgrupo $Stab_{\Lambda}(\mathbf{x_0}) < \Lambda$.

Diferentes representantes da classe lateral e grupos de definição resultam em diferentes conjuntos geradores para um dado código de grupo. Quando o conjunto gerador Λ_g do código de grupo $\mathbb{C}$ é fechado sob a operação do grupo, é chamado de *grupo gerador*. Em outra palavras, o grupo Λ estritamente transitivo $|\Lambda| = |\mathbb{C}|$ é chamado de gerador de grupo do código $\mathbb{C}$. Assim, um código de grupo pode ou não possuir grupo gerador.

Dado um código de grupo $\Lambda(\mathbf{x_0})$, o estabilizador $Stab_{\Lambda}(\mathbf{x_0}) < \Lambda$ é um subgrupo não trivial, isto é, subgrupo não normal em Λ[21]. Freqüentemente se escolhe o sistema de representante da classe lateral à esquerda que formam um grupo, isto é, $\Lambda_g < \Lambda$. O grupo gerador obtido é um subgrupo normal do grupo de definição, ou seja, $\Lambda_g \lhd \Lambda$.

3.3.1 Códigos de Slepian

Os **códigos de Slepian** são conjuntos de pontos sobre uma hiperesfera no espaço euclidiano n-dimensional, equivalente a um código de permutação. Ao código de permutação sobre $\mathbb{Z}_p$ está associado o grupo de automorfismo, o qual define a estrutura do código. Para o código de permutação, o grupo de automorfismo é subgrupo do grupo de permutações S_n. Através do algoritmo da d-cadeia fechada, determina-se a geometria associada ao grupo mediante o estabelecimento de uma cadeia de pontos, o qual é uma homotopia fechada cujo grupo cíclico associado é $\mathbb{Z}_p$.

Os códigos de grupo ou códigos de Slepian (códigos esféricos) foram pela primeira vez apresentados em [22], e depois por Forney [23]. Segundo Slepian, um código de bloco, no espaço euclidiano $n - dimensinal$, $\mathbb{R}^n$, é construído a partir da seguintes condições: 1) existe um vetor $\mathbf{x_0} \in \mathbb{R}^n$; 2) existe um grupo finito Λ de transformações lineares em $\mathbb{R}^n$.

De modo que o código de grupo é o conjunto finito de vetores que definem a superfície de uma hiperesfera limitada pelo grupo finito, ou seja, $\mathbb{C} = \Lambda(\mathbf{x_0})$. Assim, o grupo $\mathbb{G}$ de transformações lineares no espaço euclidiano $\mathbb{R}^n$ e o ponto $\mathbf{x_0} \in \mathbb{R}^n$ definem o código de grupo (código de Slepian) $\mathbb{G}(\mathbf{x_0})$.

O conceito de código de grupo se baseia em considerar a órbita de um ponto $\mathbf{x_0} \in \mathbb{R}^n$ sobre um grupo finito de transformações ortogonais em $\mathbb{R}^n$, ou seja, $\mathbb{C} = \Lambda(\mathbf{x})$.

O código de bloco $\mathbb{C}$ com comprimento n consiste do conjunto de vetores no espaço euclidiano $\mathbb{R}^n$. Para o código de bloco, pode-se tomar o conjunto de índices $\mathbb{T} = \{1, 2, 3, ..., n\}$ e $\mathbb{C} \subset \mathbb{X}^{\mathbb{T}}$. Se o código de bloco $\mathbb{C} \subseteq \mathbb{X}^{\mathbb{T}}$ não se expandir em $\mathbb{R}^n$, então, através de conveniente escolha da base, o código $\mathbb{C}$ pode ser considerado um código de bloco sobre $\mathbb{R}$ com comprimento m. A dimensão da expansão é igual a m, de modo que se pode construir um código de grupo de bloco sobre $\mathbb{R}$, sendo $\sum$ o conjunto de todas as transformações lineares de $\mathbb{R}^n$. Portanto, um código de grupo de bloco $\Lambda(\mathbf{x}_0)$ é especificado pelo grupo finito $\Lambda < \sum$ e o ponto $\mathbf{x}_0 \in \mathbb{R}^n$. Sendo finito o grupo de definição, Λ, toda transformação $\lambda \in \Lambda$ precisa possuir ordem finita, isto é, $\lambda^m = \mathbf{I}$ para alguns números inteiros m e $\mathbf{I}$ é a transformação identidade. Portanto, tornam-se de maior interesse as situações em que $\sum$ consiste das transformações lineares com $\det = \pm 1$

Definição 3.3.7. [24] ***Códigos de grupo ou códigos de Slepian*** são códigos de grupo de bloco com isometria finita sobre $\mathbb{R}$, construídos através da imagem do ponto $\mathbf{x}_0 \in \mathbb{R}^n$ sob o grupo finito Λ de transformações ortogonais em $\mathbb{R}^n$, ou seja, em notação matricial $\mathbf{M}_\lambda^t \mathbf{M}_\lambda = \mathbf{I}$ onde $\{\mathbf{M} \mid \mathbf{M} \in \mathbb{R}^{n \mathrm{x} n}\}$ e $\lambda(\mathbf{x}) = \mathbf{M}_\lambda \mathbf{x}$. Posto que as transformações ortogonais preservam a norma euclidiana dos vetores, o código de Slepian pode ser definido como o conjunto de pontos na superfície de uma n-hiperesfera de raio $\|\mathbf{x}_0\|$ no espaço $\mathbb{R}^n$.

Assim, o código de Slepian é definido pelo grupo de transformações ortogonais Λ e pelo vetor $\mathbf{x}_0$. Freqüentemente, quando o comprimento n do bloco é pequeno o código no espaço euclidiano é considerado um conjunto de sinais ou uma constelação de sinais. Portanto, o código de Slepian é um código de grupo com isometria finita.

3.3.2 Grupo de Isometrias

Definição 3.3.8. Uma isometria λ no espaço euclidiano n-dimensional é uma transformação $\{\lambda : \mathbb{R}^n \to \mathbb{R}^n\}$, que preserva as distâncias euclidianas $\|\mathbf{x} - \mathbf{y}\|^2 = \|\lambda(\mathbf{x}) - \lambda(\mathbf{y})\|^2, \ \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, em que $\lambda(\mathbf{x})$ e $\lambda(\mathbf{y})$ são as imagens de $\mathbf{x}$ e $\mathbf{y}$, respectivamente, sob a transformação λ. Uma das principais aplicações de classe de isometria no espaço euclidiano são as transformações ortogonais do tipo rotação pura, rotação imprópria e reflexão pura.

Assim, toda isometria no espaço euclidiano $\mathbb{R}^n$ é uma transformação $\lambda(\mathbf{x}) = \mathbf{M}_\lambda \mathbf{x} + c_\lambda$, em que $\mathbf{M}_\lambda$ é matriz ortogonal. Uma isometria é chamada de *translação pura*, se $\lambda(\mathbf{x}) = \mathbf{x} + c_\lambda$, onde $\mathbf{M}_\lambda = \mathbf{I}$, e de translação linear, se $\lambda(\mathbf{x}) = \mathbf{M}_\lambda \mathbf{x}$, onde $c_\lambda = 0$. O conjunto de todas isometrias em $\mathbb{R}^n$ forma o ***grupo de isometrias***, denotado por $\mathcal{I}_{SO_n}$.

Definição 3.3.9. O grupo de translação

$$\mathcal{I}_r \cong \{\lambda \in \mathcal{I}_{SO_n} \mid \lambda(\cdot) - \lambda(0) = \mathbf{I}_n\}$$

é um subgrupo normal, $\mathcal{I}_r \lhd \mathcal{I}_{SO_n}$, e o seu grupo quociente, $\frac{\mathcal{I}_{SO_n}}{\mathcal{I}_r}$, é chamado de grupo linear constituinte. O quociente é isomorfo ao grupo de todas as transformações ortogonais em $\mathbb{R}^n$. Dada uma isometria $\lambda(\mathbf{x})$, a sua componente de translação corresponde ao mapeamento $\lambda_T(\mathbf{x}) = \mathbf{x} + \lambda(0)$ e a componente linear corresponde a $\lambda_L(\mathbf{x}) = \lambda(\mathbf{x}) + \lambda(0)$, onde $\lambda(\mathbf{x}) = \lambda_T(\lambda_L(\mathbf{x}))$.

Em [22], somente são considerados os grupos de definição finitos $\Lambda < \mathcal{I}_{SO_n}$ para se assegurar de um código de grupo de isometria finita $\Lambda(\mathbf{x}_0)$, de modo que o grupo de simetria do código de grupo (código de Slepian) tem que possuir um subgrupo de translação trivial Λ_T. Um método alternativo de construção do código de bloco finito sobre $\mathbb{R}$ inicia considerando os subgrupos de translação não triviais, portanto infinitos, associados ao grupo linear constituinte. Este tipo de grupo de definição, Λ, gera um código de grupo de isometria infinita de bloco $\Lambda(\mathbf{x}_0)$. Portanto, o código finito, dado pela expressão, $\Lambda(\mathbf{x}_0)|_{\mathcal{R}} = \mathcal{R} \cap \Lambda(\mathbf{x}_0)$ é um código derivado (subcódigo) do código $\Lambda(\mathbf{x}_0)$ obtido a partir da intersecção com a região limitante de volume finito, $\mathcal{R}$. Quando $\Lambda(\mathbf{x}_0)|_{\mathcal{R}}$ não é um código de grupo, este herda várias propriedades do código de bloco de grupo $\Lambda(\mathbf{x}_0)$ do qual pertence.

3.3.3 Códigos de Permutação

Seja G um grupo de matrizes ortogonais nxn o qual forma a representação fiel de um grupo $\mathcal{G}$ com vetor inicial $\mathbf{x} \in \mathbb{R}^n$. O código de grupo $\mathcal{X}$, como definido na Seção 3.3.1, é a órbita do vetor $\mathbf{x}$ sob $\mathcal{G}$, ou seja, é o conjunto de vetores $\mathbf{xG}$. Inicialmente se considera $\mathcal{G}$ um grupo abstrato e $\mathbf{x}$ um vetor inicial para mostrar que todo código de grupo é equivalente ao código de permutação.

Definição 3.3.10. ***Código de permutação*** é um código de grupo obtido a partir da aplicação ao vetor inicial $\mathbf{x}$ de um grupo G de permutações, ou seja, G é um grupo de matrizes de permutação.

Teorema 3.3.1. [20] Seja $f : G \to G'$ um homomorfismo de G em um grupo G'. Então

$$H = \{x \in G \ : \ f(x) = 1\}$$

é um subgrupo normal de G também chamado de núcleo de f.

Definição 3.3.11. Se G é um grupo, uma ***representação de permutação*** de G é todo homomorfismo de G no grupo de simetrias $Sym(A) \cong Sym_G(A)$, para um conjunto A não vazio, ou a imagem de G sob o homomorfismo. Se o homomorfismo é um isomorfismo, então se diz que a *representação é fiel*.

Teorema 3.3.2. [20] Todo grupo $\mathcal{G}$ de ordem $|\mathcal{G}|$ é isomorfo a subgrupo do grupo de simetria $Sym_G(A)$.

Sejam $\mathcal{H}$ o subgrupo de $\mathcal{G}$ e $\mathcal{R}$ o conjunto de classes laterais à direita de $\mathcal{H}$ em G. Então,

$$\mathcal{G} = \bigcup_{\mathcal{H}r \in \mathcal{R}} \mathcal{H}r$$

é a decomposição do grupo $\mathcal{G}$ em classe lateral de $\mathcal{H}$ à direita. Para todo $g \in \mathcal{G}$ é atribuída a permutação

$$\pi_g : \ \mathcal{R} \to \mathcal{R}$$

em que $\pi_g(\mathcal{H}r) = \mathcal{H}rg$ e $\mathbf{r}$ é o vetor de ruído no receptor. O conjunto $\Gamma = \{\pi_g \mid g \in \mathcal{G}\}$ é o grupo de permutação transitivo de grau $\frac{|\mathcal{G}|}{|\mathcal{H}|}$ e a representação de permutação de $\mathcal{G}$ induzida por $\mathcal{H}$. Esse é o método como toda representação de permutação transitiva de $\mathcal{G}$ pode ser obtida. Quando $\mathcal{H} = \{e\}$, identidade de $\mathcal{G}$, a representação induzida por $\mathcal{H}$ é chamada de representação regular à direita de $\mathcal{G}$. De maneira análoga, define-se a representação regular à esquerda de $\mathcal{G}$.

O mínimo n corresponde a máxima cardinalidade $|\mathcal{H}|$ tal que a representação de Γ é fiel, isto é, tal que o núcleo do homomorfismo de $\mathcal{G}$ em Γ é a identidade. Este núcleo pode ser considerado o subgrupo normal maximal de $\mathcal{G}$ contido em $\mathcal{H}$. Conseqüentemente, se $\mathcal{H}'$ denota o maior subgrupo não normal de $\mathcal{G}$, o qual não inclui subgrupos normais de $\mathcal{G}$, à exceção da identidade, então n é dado pela seguinte razão:

$$n = \frac{|\mathcal{G}|}{|\mathcal{H}'|}.$$

Se $\mathcal{G}$ é abeliano ou p-grupo de Sylow, então todos os seus subgrupos são normais. Quando $|\mathcal{H}'| = 1$, então $n = |\mathcal{G}|$

Teorema 3.3.3. [20] Seja $\mathcal{G}$ um grupo finito que possui os seguintes símbolos reais $\mathcal{X}_1$, $\mathcal{X}_2$, ..., $\mathcal{X}_p$. Seja ρ uma representação fiel $\rho : \ \mathcal{G} \to G$ onde G é um grupo de matrizes ortogonais nxn. Seja $\mathcal{X}_\rho$ o símbolo de ρ e suponha $\mathcal{X}_\rho = \sum_{i=1}^{p} a_i \mathcal{X}_i$. Seja $\mathbf{x} \in \mathbb{R}^n$ e o código de grupo dado por $\mathcal{X} = G\mathbf{x} = \{\rho(g)\mathbf{x} : \ g \in \mathcal{G}\}$. Suponha $\mathcal{H}$ um subgrupo de $\mathcal{G}$ e forma a representação de permutação $\phi : \ \mathcal{G} \to \Gamma = \{\pi_g \mid \ g \in \mathcal{G}\}$ induzida por $\mathcal{H}$. Seja $\mathcal{X}_\phi$ o símbolo de ϕ e suponha ainda $\mathcal{X}_\phi = \sum_{i=1}^{p} b_i \mathcal{X}_i$. *Se ϕ é representação fiel e $b_i \geq a_i \ \forall i$, então Γ gera o código de permutação equivalente ao código $\mathcal{X}$.*

Corolário 3.3.1. Todo código de grupo é equivalente a, no mínimo, um código de permutação.

3.3.4 Algoritmo da d-cadeia Fechada

O algoritmo da *d-cadeia fechada*, proposto em [25], é um complemento do teorema de Slepian [22]. Este algoritmo determina a geometria dos grupos abelianos, ou não abelianos, no espaço euclidiano n - dimensional. Da geometria do grupo que procede do algoritmo, determinam-se novos polígonos regulares em qualquer dimensão $n \neq 2$. Estes polígonos formam os códigos esféricos, ou códigos de Slepian. Deste modo, o algoritmo da *d-cadeia fechada* generaliza a construção dos códigos primos sobre a superfície de hiperesfera n-dimensional,

sendo casos particulares dos códigos de Slepian os códigos primos apresentados em [9], [26] e [27]-[28] e outros.

Teorema 3.3.4. Sejam as palavras de uma d-cadeia iniciando em $X_E, X_{A_1}, X_{A_2}, ..., X_{A_h}$. Então os elementos do grupo, cujas palavras correspondentes distam "d" da palavra X_E formam um conjunto de geradores de H. Se H é um subgrupo próprio de G, então, de qualquer palavra correspondente a um elemento do grupo que não está em H, uma nova d-cadeia pode ser formada e os elementos do grupo correspondentes aos pontos desta nova d-cadeia formam uma classe lateral de H.

Da demonstração do teorema (3.3.4) decorre o algoritmo da *d-cadeia fechada* como instrumento para construção dos códigos de Slepian a partir da tabela de Cayley. O algoritmo é composto dos seguintes passos:

Passo 1: Dado um conjunto e a operação associada, construa a tabela de Cayley.

Passo 2: Para cada linha da tabela de Cayley, determine a permutação correspondente. Quando o conjunto é isomorfo a $\mathbb{Z}_p$, este conjunto de permutação forma um grupo de quadrados latinos.

Passo 3: Forme o conjunto de ciclos para cada permutação.

Passo 4: Do produto de ciclos, colete os pontos antipodais. O conjunto Γ_i consiste na identidade e nos ciclos antipodais. Assinale uma distância d_i para cada conjunto Γ_i.

Passo 5: Dos vários conjuntos Γ_i encontre todos os caminhos Hamiltonianos possíveis iniciando do elemento identidade do grupo. Tal tarefa é acompanhada pela procura das possíveis seqüências de elementos do produto de ciclos pertencentes aos conjuntos Γ_i.

Passo 6: De modo a encontrar grafos associados a cada Γ_i, ou $d_i - cadeia$, encontrados no Passo 5, faça cada caminho Hamiltoniano a primeira coluna de uma tabela cuja 1^a linha são os elementos do conjunto Γ_i correspondentes à $d_i - cadeia$ desejada. Desta linha e coluna, conhecendo a operação de grupo, complete esta tabela.

Situação 3.3.1. Seja GF(5) o corpo de Galois. Sejam representados os elementos de GF(5) como inteiros de $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

Passo 1: Tabela de Cayley

Tabela 3.5: Tabela de Cayley para $p = 5$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Sua composição é conforme se mostra na Tabela 3.5.

Passo 2: Elementos de Permutação

Os elementos de permutação são conforme a Tabela 3.6.

Tabela 3.6: Elementos de Permutação.

Permutações		
$A=\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 \end{bmatrix}$	$B=\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}$	$C=\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \end{bmatrix}$
$D=\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix}$	$E=\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$	

Passo 3: Produtos dos Ciclos

$$A = I = (0)(1)(2)(3)(4) - \text{Identidade}$$
$$B = (0, 1, 2, 3, 4);$$
$$C = (0, 2, 4, 1, 3);$$
$$D = (0, 3, 1, 4, 2);$$
$$E = (0, 4, 3, 2, 1)$$

Passo 4: Formar o Conjunto

$$d_1 = (I, B) = \Gamma_1 = \{B = (0, 1, 2, 3, 4)\}$$
$$d_2 = (I, C) = \Gamma_2 = \{C = (0, 2, 4, 1, 3)\}$$
$$d_3 = (I, D) = \Gamma_3 = \{D = (0, 3, 1, 4, 2)\}$$
$$d_4 = (I, E) = \Gamma_4 = \{E = (0, 4, 3, 2, 1)\}$$

Passo 5: Caminhos Hamiltonianos

$$\Gamma_1 \Rightarrow B = (0, 1, 2, 3, 4) \Rightarrow \begin{cases} 0, 1, 2, 3, 4, 0 \\ 0, 4, 3, 2, 1, 0 \end{cases};$$
$$\Gamma_2 \Rightarrow C = (0, 2, 4, 1, 3) \Rightarrow \begin{cases} 0, 2, 4, 1, 3, 0 \\ 0, 3, 1, 4, 2, 0 \end{cases};$$
$$\Gamma_3 \Rightarrow D = (0, 3, 1, 4, 2) \Rightarrow \begin{cases} 0, 3, 1, 4, 2, 0 \\ 0, 2, 4, 1, 3, 0 \end{cases};$$
$$\Gamma_4 \Rightarrow E = (0, 4, 3, 2, 1) \Rightarrow \begin{cases} 0, 4, 3, 2, 1, 0 \\ 0, 1, 2, 3, 4, 0 \end{cases}.$$

Passo 6: Montagem da Tabela 3.7

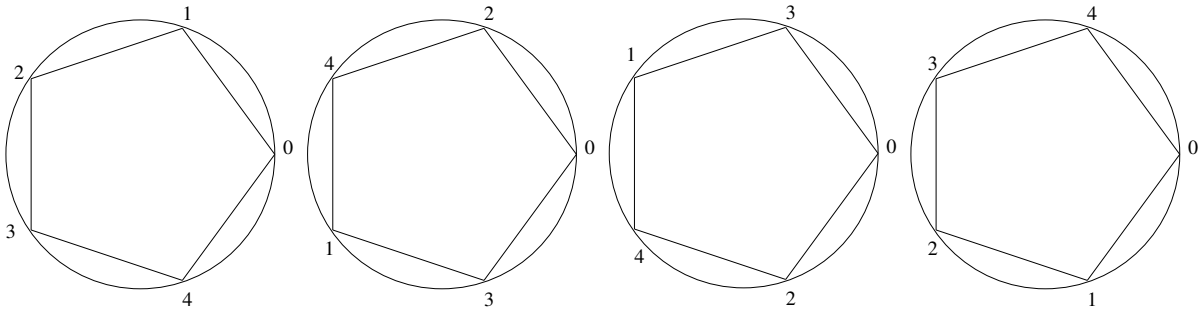
Tabela 3.7: Grafos.

Para Γ_1				
0	1		0	1
1	2		4	0
2	3		3	4
3	4		2	3
4	0		1	2
0	1		0	1

Para Γ_2				
0	2		0	2
2	4		3	0
4	1		1	3
1	3		4	1
3	0		2	4
0	2		0	2

Para Γ_3				
0	3		0	3
3	1		2	0
1	4		4	2
4	2		1	4
2	0		3	1
0	3		0	3

Para Γ_4				
0	4		0	4
4	3		1	0
3	2		2	1
2	1		3	2
1	0		4	3
0	4		0	4



(a) Para Γ_1 (b) Para Γ_2 (c) Para Γ_3 (d) Para Γ_4

Figura 3.2: Grafos de GF(5).

Deste modo, o algoritmo da *d-cadeia fechada* generaliza a forma de determinar a geometria do grupo no espaço euclidiano n-dimensional, a partir das matrizes de permutação, da tabela de Cayley, através de caminhos fechados ou caminhos hamiltonianos. Além da geometria do grupo, que é determinada mediante o estabelecimento predeterminado da distância "*d*" e da ordem do grupo, usando o algoritmo da *d-cadeia fechada* se verifica a simetria e regularidade dos polígonos construídos.

Estes polígonos são iguais entre si, quando gerados a partir de números coprimos. A *d-cadeia fechada* é de fato uma homotopia de caminhos hamiltonianos. O grupo associado à homotopia é um grupo cíclico infinito $\mathbb{Z}$. A figura associada à geometria é uma circunferência em duas dimensões, uma esfera para o caso de três dimensões ou hiperesferas para os casos de $n > 3$ dimensões. Os vértices dos polígonos associados a um grupo estão sobre a superfície da hiperesfera, o que corresponde aos códigos de Slepian ou códigos esféricos, também conhecidos por códigos de permutação. Portanto, o algoritmo da *d-cadeia fechada* determina a geometria.

3.4 Casos Particulares dos Códigos de Slepian e Resíduos Quadráticos

Nesta seção se objetiva mostrar que os códigos primos, apresentados em [9], [26]-[28], e gerados na Subseção 3.4.1 podem ser obtidos pelo método de representação dos códigos de

Slepian.

3.4.1 Slepian: Códigos Primos $(p^2, p, p, 2)$- PS

Esta técnica gera códigos com parâmetros $(p^2, p, p, 2)$ - PS "prime sequences", a partir de um número primo p.

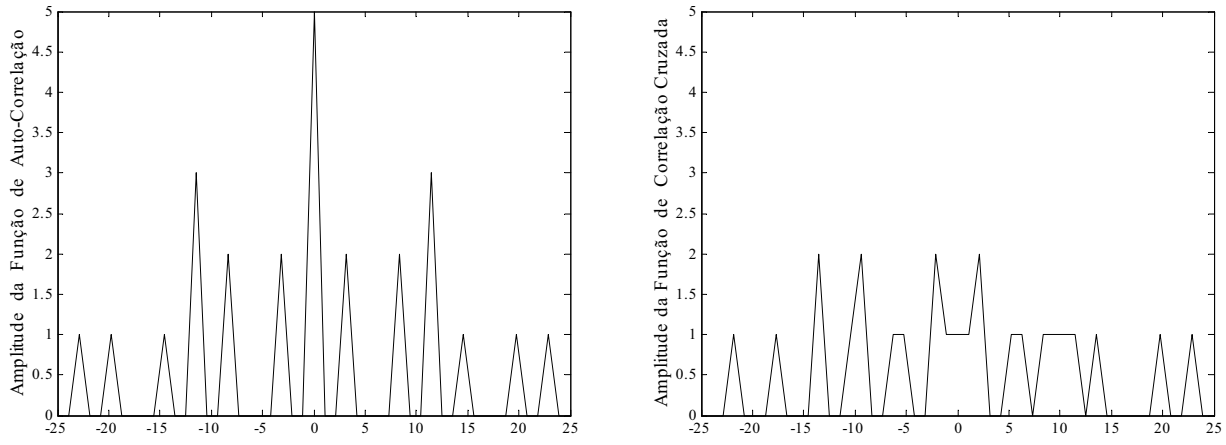
Seja $GF(p) = \{0, 1, 2, 3, ..., j, ..., p-1\}$ um corpo de Galois com p elementos. A seqüência prima $S_i = (s_{i0}, s_{i1}, ..., s_{ip-1})$ é construída a partir da expressão: $s_{ij} = i.j \pmod p$ em $GF(p)$. Cada seqüência de prima é então mapeada em uma seqüência binária consistindo de p blocos, cada com p símbolos binários, isto é, $C_i = (c_{i0}, c_{i1}, ..., c_{ij}, ..., c_{i,(p^2-1)})$ onde

$$c_{ij} = \begin{cases} 1, & j = s_{ik} + kp \quad , k \in \{0, 1, ..., p-1\} \\ 0, & fora \end{cases} . \tag{3.9}$$

Situação 3.4.1. Suponha $p = 5$. A Tabela 3.8 apresenta as palavras-código e as seqüências binárias do código PS para $GF(5)$.

Tabela 3.8: Código primo para $p = 5$.

i	Seqüência S_i	Palavra-código C_i	Seqüência Binária
0	$S_0 = (0, 0, 0, 0, 0)$	C_0	10000 10000 10000 10000 10000
1	$S_1 = (0, 1, 2, 3, 4)$	C_1	10000 01000 00100 00010 00001
2	$S_2 = (0, 2, 4, 1, 3)$	C_2	10000 00100 00001 01000 00010
3	$S_3 = (0, 3, 1, 4, 2)$	C_3	10000 00010 01000 00001 00100
4	$S_4 = (0, 4, 3, 2, 1)$	C_4	10000 00001 00010 00100 01000

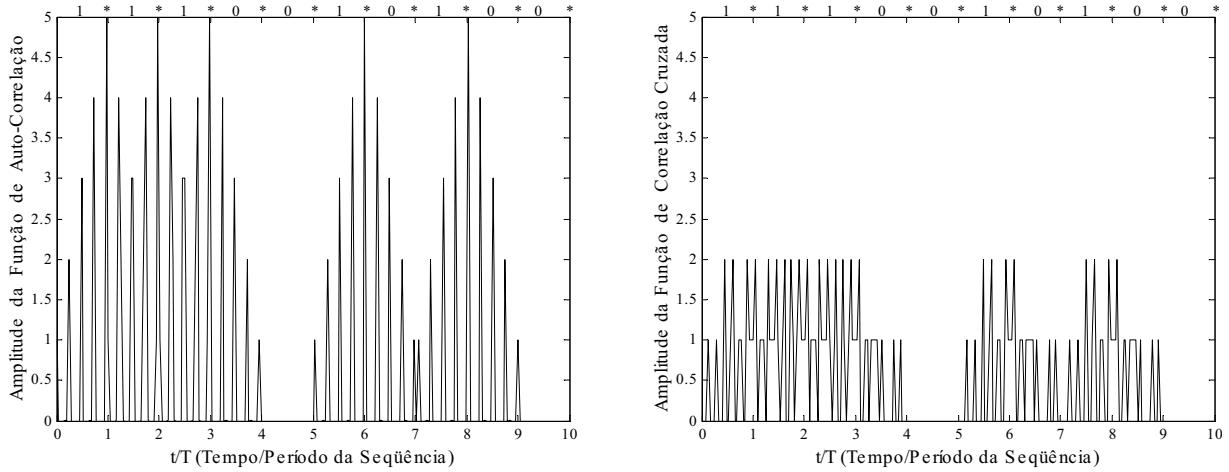


(a) Auto-Correlação de C_3 (b) Correlação Cruzada entre C_3 e C_4

Figura 3.3: Propriedades de Correlação do Código Primo, para $p = 5$.

A Figura 3.3 ilustra as propriedades de correlação do Código Primo, para $p = 5$, quando codifica somente um bit de informação. Como ilustrada na Figura 3.3(a), a auto-correlação da

palavra-código C_3 =10000 00010 01000 00001 00100 possui elevados lóbulos laterais. Devido a estes lóbulos laterais o sincronismo entre o transmissor e receptor pode ser comprometido. Na Figura 3.3(b) é ilustrada a correlação cruzada entre as palavras-código C_3 e C_4. A correlação cruzada não possui valor superior a dois.



(a) Auto-Correlação de C_3

(b) Correlação Cruzada entre C_3 e C_4

Figura 3.4: Propriedades de Correlação do Código Primo como seqüência de decodificação, para $p = 5$.

A Figura 3.4 ilustra as propriedades de correlação do código primo como seqüência de decodificação, para $p = 5$.

O sinal resultante é a auto-correlação da palavra-código C_3 do código primo para $p = 5$, como ilustrado na Figura 3.4(a). Para se obter a correlação cruzada das palavras-código C_2 e C_3, ilustrada na Figura 3.4(b), cada bit "1" da seqüência de informação 1110010100, é espalhado pela seqüência de espalhamento C_3. Os bits "0" da seqüência de informação são transmitidos na forma de seqüência 000000000 000000000 000000000 000000000 000000000. No receptor, a seqüência de informação codificada é comparada com a palavra-código C_3 que corresponde ao código de recuperação da informação do usuário desejado.

Das Figuras 3.4(a) e 3.4(b) se observa que os picos de maior amplitude da auto-correlação e correlação cruzada acontecem durante a transmissão dos bits "1" de informação. Embora estas figuras confirmem o esperado $\lambda_a \leq 5$ e $\lambda_c \leq 2$, conclui-se que os códigos primos são impróprios para sistemas OCDMA de detecção direta devido aos elevados lóbulos laterais da função de auto-correlação.

3.4.2 Slepian: Códigos Primos Estendidos $(p(2p-1), p, p, 1)$ - EPS

A técnica de construção dos códigos primos foi apresentada pela primeira vez em [28] para gerar códigos com parâmetros $(p(2p-1), p, p, 1)$ - EPS "extended prime sequences", a partir de um número primo p.

Seja $GF(p) = \{0, 1, 2, 3, ..., j, ..., p-1\}$ um corpo de Galois com p elementos. A seqüência prima $S_i = (s_{i0}, s_{i1}, ..., s_{ip-1})$ é construída a partir da expressão: $s_{ij} = i.j \pmod p$ $GF(p)$.

Cada seqüência prima é então mapeada em seqüência binária consistindo de p blocos cada com $(2p-1)$ símbolos binários, i.e, $C_i = (c_{i0}, c_{i1}, ..., c_{ij}, ..., c_{i,(p(2p-1))})$ onde

$$c_{ij} = \begin{cases} 1, & j = s_{ik} + k(2p-1) \quad , k \in \{0, 1, ..., p-1\} \\ 0, & fora \end{cases} . \tag{3.10}$$

Assim, os códigos primos estendidos são obtidos a partir dos códigos primos aumentando p-1 zeros em cada série de "chips" do código primo. Os códigos primos estendidos possuem correlação cruzada igual a zero ou um e não são rigorosamente ortogonais, por isso chamados de códigos pseudo-ortogonais.

Situação 3.4.2. Suponha $p = 5$. A Tabela 3.9 apresenta as palavras-código e as seqüências binárias do código EPS para $GF(5)$

Tabela 3.9: Código primo Estendido para $p = 5$.

i	Seqüência S_i	Palavra-código C_i	Seqüência Binária
0	$S_0 = (0,0,0,0,0)$	C_0	100000000 100000000 100000000 100000000 100000000
1	$S_1 = (0,1,2,3,4)$	C_1	100000000 010000000 001000000 000100000 000010000
2	$S_2 = (0,2,4,1,3)$	C_2	100000000 001000000 000010000 010000000 000100000
3	$S_3 = (0,3,1,4,2)$	C_3	100000000 000100000 010000000 000010000 001000000
4	$S_4 = (0,4,3,2,1)$	C_4	100000000 000010000 000100000 001000000 010000000

O passo 1 do algoritmo da d-cadeia fechada é uma representação de $\mathbb{Z}_5$ na tabela de Cayley que corresponde a segunda coluna da Tabela 3.8 do código primo $p = 5$. Os caminhos Hamiltonianos B,C,D,E (Passo 5) completam a superfície da esfera por dois percursos, cada um dos caminhos corresponde a palavra-palavra código da Tabela 3.8, de modo que qualquer permutação da palavras-código na coluna dois da Tabela 3.8 vai ser igual a um dos caminhos hamiltonianos do Passo 5. Portanto, o código primo (código primo estendido) é um caso particular do código de Slepian.

3.4.3 QRC: Códigos Quadráticos $(p^2, p, 2, 4)$ - QC

A técnica de construção dos códigos quadráticos (QC) foi apresentada em [29] para gerar códigos com parâmetros $(p^2, p, p, 2)$ - QC "Quadratic Congruences", a partir de um número primo p. Nesta seção mostramos como obter o código quadrático a partir do código de resíduos quadráticos.

Seja $GF(p) = \{0, 1, 2, 3, ..., j, ..., p-1\}$ um corpo de Galois com p elementos. Os elementos s_{i1} da palavra-código do código quadrático (QC), $S_i = (s_{i0}, s_{i1}, ..., s_{ip-1})$ é construída a partir da expressão: $s_{ij} = i.\frac{j(j+1)}{2} \pmod p$ em $GF(p)$, onde $i \in GF(p)\backslash\{0\}$. Para o QC, cada palavra-código S_i é mapeada em uma seqüência binária consistindo de p blocos cada

com p, isto é, $C_i = (c_{i0}, c_{i1}, ..., c_{ij}, ..., s_{i,(p^2-1)})$ onde

$$c_{ij} = \begin{cases} 1, & j = s_{ik} + kp \quad , k \in \{0, 1, ..., p-1\} \\ 0, & fora \end{cases} \tag{3.11}$$

Situação 3.4.3. Suponha $p = 5$. A Tabela 3.10 apresenta as palavras-código e as seqüências binárias do código QC para $GF(5)$.

Tabela 3.10: Código Quadrático para $p = 5$.

i	Seqüência S_i	Palavra-código C_i	Seqüência Binária
1	$S_0 = (0, 1, 3, 1, 0)$	C_0	10000 01000 00010 01000 10000
2	$S_1 = (0, 2, 1, 2, 0)$	C_1	10000 00100 01000 00100 10000
3	$S_2 = (0, 3, 4, 3, 0)$	C_2	10000 00010 00001 00010 10000
4	$S_3 = (0, 4, 2, 4, 0)$	C_3	10000 00001 00100 00001 10000

3.4.4 QRC: Códigos Quadráticos Estendidos $(p(2p-1), p, 1, 2)$-EQC

A técnica de construção dos códigos quadráticos (QC) foi apresentada em [30] para gerar códigos com parâmetros $(p(2p-1), p, 1, 2)$, para todo número primo p.

Seja $GF(p) = \{0, 1, 2, 3, ..., j, ..., p-1\}$ um corpo de Galois com p elementos. Os elementos s_{i1} da palavra-código do código quadrático (QC) $S_i = (s_{i0}, s_{i1}, ..., s_{ip-1})$ é construída a partir da expressão: $s_{ij} = i.\frac{j(j+1)}{2} \pmod p$ em $GF(p)$, onde $i \in GF(p)\backslash\{0\}$. Para o QC, cada palavra-código S_i é mapeada em seqüência binária consistindo de p blocos cada com $(2p-1)$ símbolos binários, isto é, $C_i = (c_{i0}, c_{i1}, ..., c_{ij}, ..., c_{i,(p(2p-1))})$ onde

$$c_{ij} = \begin{cases} 1, & j = s_{ik} + k(2p-1) \quad , k \in \{0, 1, ..., p-1\} \\ 0, & fora \end{cases} \tag{3.12}$$

Assim, os códigos quadráticos estendidos são obtidos a partir dos códigos quadráticos aumentando $(p-1)$ zeros em cada série de "chips" do código quadrático.

Situação 3.4.4. A Tabela 3.11 apresenta na condição $p = 5$, as palavras-código e as seqüências binárias do código EQC para $GF(5)$.

A equação (9) em [29] quando manipulada, como se segue:

$$\frac{m_2}{2}[k^2 + k(2x+1) + x^2 + x] - \frac{m_1}{2}[k^2 + k] - z \equiv 0 \pmod p; \tag{3.13}$$

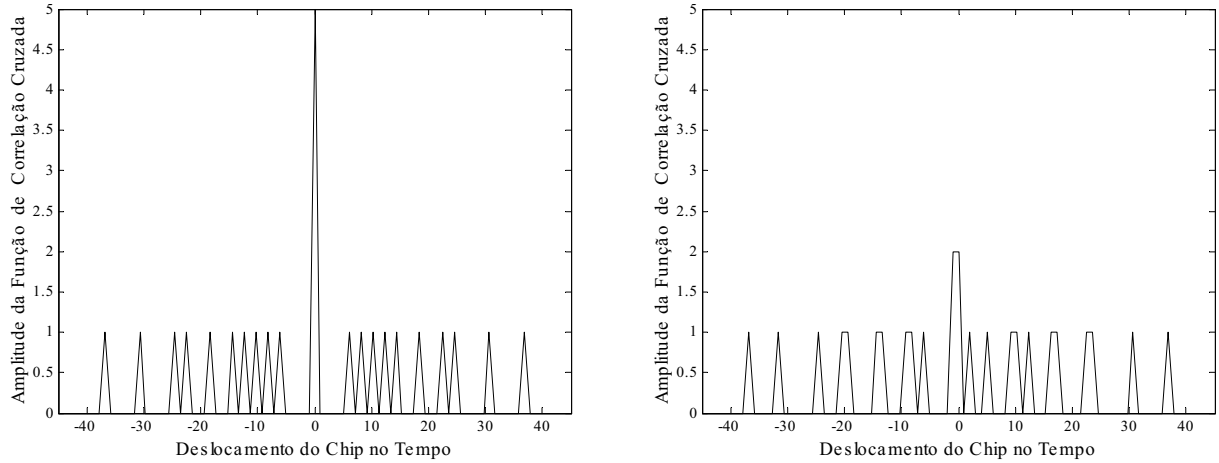
$$k^2[\frac{m_2}{2} - \frac{m_1}{2}] + k[\frac{m_2}{2}(2x+1) - \frac{m_1}{2}] + [\frac{m_2}{2}(x^2 + x) - z] \equiv 0 \pmod p \tag{3.14}$$

pode ser apresentada na forma da equação (3.1), para

$$a = \frac{m_2}{2} - \frac{m_1}{2}; \quad b = \frac{m_2}{2}(2x+1) - \frac{m_1}{2}; \quad c = \frac{m_2}{2}(x^2 + x) - z; \quad m = p. \tag{3.15}$$

Tabela 3.11: Código Quadrático Estendido para $p = 5$.

i	Seqüência S_i	Palavra-código C_i	Seqüência Binária
1	$S_0 = (0, 1, 3, 1, 0)$	C_0	100000000 010000000 000100000 010000000 100000000
2	$S_1 = (0, 2, 1, 2, 0)$	C_1	100000000 001000000 010000000 001000000 100000000
3	$S_2 = (0, 3, 4, 3, 0)$	C_2	100000000 000100000 000010000 000100000 100000000
4	$S_3 = (0, 4, 2, 4, 0)$	C_3	100000000 000010000 001000000 000010000 100000000



(a) Auto-Correlação de C_2

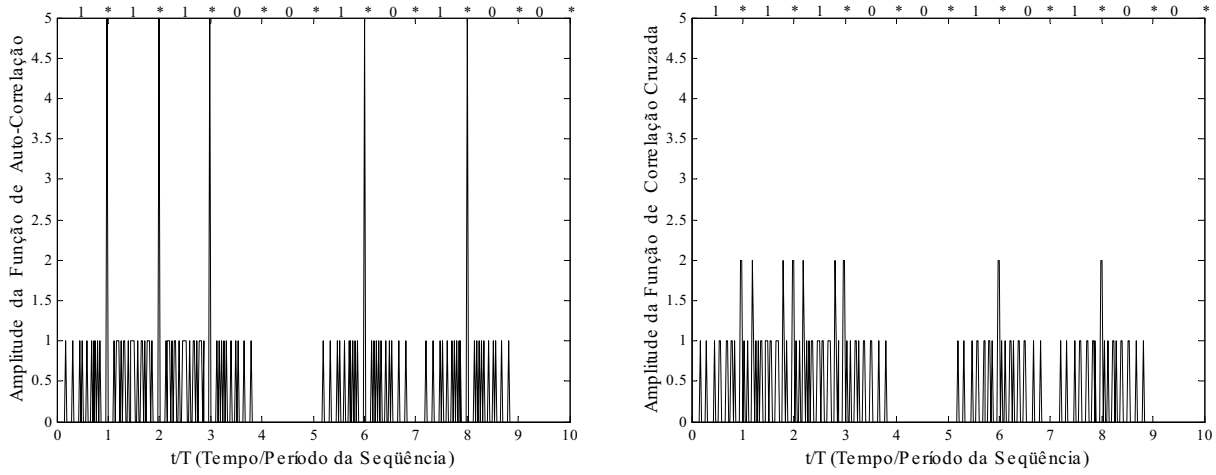
(b) Correlação Cruzada entre C_2 e C_3

Figura 3.5: Propriedades de Correlação do Código EQC, para $p = .5$

A Figura 3.5 ilustra as propriedades de correlação do código EQC, para $p = 5$, quando codifica somente um bit de informação. A fraca propriedade de auto-correlação do código primo trouxe a necessidade de desenvolver códigos com boas propriedades de correlação. Como está ilustrado na Figura 3.5(a), a auto-correlação da palavra-código C_3 =100000000 000010000 001000000 000010000 100000000, diferente da auto-correlação ilustrada na Figura 3.3(a), possui lóbulos laterais não superiores a um. Conseqüentemente, o transmissor e receptor possuem melhor sincronismo. Na Figura 3.5(b) é ilustrada a correlação cruzada das palavras-código C_2 e C_3. A correlação cruzada não possui valor superior a dois.

A Figura 3.6 ilustra as propriedades de correlação do código EQC como seqüência de decodificação, para $p = 5$. Das Figuras 3.6(a) e 3.6(b) se observa que os picos de maior amplitude da auto-correlação e correlação cruzada acontecem durante a transmissão dos bits "1" da seqüência de informação. Estas figuras confirmam o esperado $\lambda_a \leq 5$, no instante de sincronismo, e $\lambda_c \leq 2$, fazendo os códigos EQC próprios para sistemas OCDMA de detecção direta.

Na Figura 3.6(a) está ilustrada a auto-correlação da palavra-código C_3 do código EQC para $p = 5$. Para se obter a correlação cruzada das palavras-código C_2 e C_3, ilustrada na Figura 3.6(b), cada bit "1" da seqüência de informação, é espalhado pela seqüência de espalhamento C_3. No receptor, a seqüência de informação codificada é decodificada através



(a) Auto-Correlação de C_2

(b) Correlação Cruzada entre C_2 e C_3

Figura 3.6: Propriedades de Correlação do Código EQC como seqüência de decodificação, para $p = 5$.

do código de recuperação da informação C_2 =100000000 000100000 000010000 000100000 100000000 que não corresponde ao código do usuário desejado.

Do código de resíduos quadráticos, para $p = 5$, apresentado na Tabela (3.2) retiramos a palavra-código zero. Quando comparada com a Tabela (3.10), fica claro que as palavras do código de resíduos quadráticos correspondem às seqüências S_i do código quadrático e, conseqüentemente, com as seqüências do código quadrático estendido. Realizando o procedimento apresentado na Subseção 3.4.3, isto é, mapear as palavras-código do código de resíduos quadráticos em seqüências binárias unipolares, construímos os códigos quadráticos e quadráticos estendidos.

Assim, os códigos quadráticos e quadráticos estendidos, apresentados nas Subseções 3.4.3 - 3.4.4, podem ser caracterizados como códigos de resíduos quadráticos, do ponto de vista da equação quadrática (3.1), ou seja, são casos particulares dos códigos de resíduos quadráticos para qualquer p primo ímpar.

Capítulo 4

Construção de Códigos OOC

Este capítulo focaliza aplicações de equações diofantinas parametrizadas pelos elementos do corpo de Galois, na forma algébrica de códigos ortogonais ópticos para sistemas ópticos CDMA. Neste caso, as soluções das equações se concentram na representação de números inteiros usando equações quadráticas e quárticas. O capítulo ainda chama a atenção para o potencial das equações diofantinas na construção de códigos ópticos e aponta para as potencialidades da aplicação da teoria de Gauss como ferramenta para geração de códigos ortogonais.

Para os objetivos enunciados, o presente capítulo está assim organizado: na Seção 4.1, é apresentada a trajetória de construção dos códigos ópticos nas últimas três décadas. Essa trajetória é traçada do ponto de vista do código ser ideal $(\lambda_a = \lambda_c = 1)$ ou não ideal $(\lambda_a = 1, \quad \lambda_c \neq 1)$, a fim de se mostrar o processo de evolução dos códigos ópticos e contextualizar nossa proposta de construção de códigos ópticos. Na Seção 4.2, tratamos da representação de números inteiros na forma de equação binária quártica, em duas variáveis, mostrando a complexidade de resolução de tais equações pelo método clássico. Alternativamente, apresentamos a construção algébrica do código $(F, K, 1, 1)$-OOC baseado em solução da equação diofantina quártica parametrizada através de equações de congruência. Apresentamos um exemplo de construção do código proposto para facilitar a compreensão do texto pelo leitor. Os detalhes da demonstração do teorema usado nesta seção são também apresentados. Na Seção 4.3, usamos a representação de números inteiros na forma binária quadrática, em duas variáveis, mostrando a complexidade de resolução de tais equações pelo método clássico. Mas, introduzimos a construção algébrica do código $(F, K, 1, 2) - OOC$ baseado em solução da equação diofantina quadrática parametrizada, através de equações de congruência. Apresentamos um exemplo de construção do código proposto. A demonstração do teorema, usado na seção, é apresentada. Na Seção 4.4, usamos a técnica iterativa para construção do código $(F, K, 1, 2)$-OOC a partir do código proposto na seção anterior. A Seção 4.5 fornece a análise e discussão das propriedades de correlação dos códigos propostos nas Seções 4.2, 4.3 e 4.4. A seção § 4.6 apresenta a análise de desempenho dos códigos propostos, considerando a MAI a única causa de degradação do desempenho do sistema. Os resultados numéricos, as discussões e a comparação dos códigos propostos a outros antes publicados são

apresentados.

4.1 Visão do Estado da Arte de Construção de Códigos OOC

Uma melhoria adicional nas redes ópticas de acesso consiste no uso da técnica de acesso múltiplo por divisão de código (OCDMA) [31]-[40], cuja inerente vantagem reside na baixa necessidade de sincronismo e ausência de conversão eletro-óptica, tornando-se potencial concorrente às demais técnicas de múltiplo acesso pela sua simplicidade e flexibilidade. Como tal, foi inicialmente projetado para LAN [9] e somente depois para redes de acesso [41]-[45].

Segundo o princípio de espalhamento espectral usado, o OCDMA se subdivide nas seguintes subcategorias: seqüências diretas pseudo-ortogonais, tecnicamente conhecidas como códigos ortogonais ópticos (OOC) [46]-[47]; códigos de seqüências diretas bipolares [48]; códigos de freqüência ou fase (*frequency or phase encoding codes*) [49].

Em sistemas OCDMA, cada usuário é rotulado por uma seqüência de um código, conhecida como palavra-código. O código $(F, K, \lambda_a, \lambda_c)$-OOC é uma família de seqüências unipolares, formadas por (0,1), com comprimento F, peso K, auto-correlação λ_a, fora de pico (*off-peak autocorrelation*), e máxima correlação cruzada λ_c. Devido à natureza positiva do sinal óptico, os códigos OOC são unipolares, diferentes das seqüências bipolares (+1,-1) usadas na transmissão e processamento de sinais elétricos.

A autocorrelação e correlação-cruzada são minimizadas para se obter sincronismo e minimização da interferência de múltiplo acesso (MAI - Multiple Access Interference) no sistema. Para isso, os códigos OOC, com $\lambda = \lambda_a = \lambda_c = 1$, são os mais apropriados para seqüências de espalhamento. Como tal, estas precisam possuir determinadas propriedades de correlação. Seqüências de espalhamento (palavras-código) de elevado peso proporcionam melhor detecção do sinal desejado entre a MAI e o ruído. Por outro lado, baixas propriedades de correlação reduzem a MAI no sistema.

Em [13] e [33] foram construídos códigos $(F, k, 1)$-OOC para sistema assíncrono. Porém, sob o requisito de $\lambda_a = \lambda_c = 1$, o número de palavras-código é limitado e o projeto do receptor é complexo para cancelar a MAI do sistema. A cardinalidade destes códigos é bastante esparsa em relação ao seu comprimento. Para aumentá-la, novas famílias de códigos têm sido propostas [32]-[37], com propriedades de correlação $\lambda_a = 1$ e $\lambda_c = 2$.

Em [37], são construídos códigos ótimos, $(p^{2m} - 1, p^m + 1, 2)$-OOC, com cardinalidade igual a $p^m - 2$, em que p é um número primo qualquer. Em [10] são apresentados os códigos $(F, K, 1, 2)$-OOC que possuem limitante superior da cardinalidade, $(2(F-1)/(K^2 - K))$, esta corresponde ao dobro do limitante superior da cardinalidade dos códigos $(F, K, 1)$-OOC. Em [50] foram gerados códigos do tipo $(F, K, 1, 2)$-OOC com cardinalidade K e $(K-1)$ vezes maior a cardinalidade do código $(F, K, 1)$-OOC, para $K < 8$ par e ímpar, respectivamente.

Em [51], os autores propõem códigos $(F, K, 1, 2)$-OOC baseados em planos projetivos para construir *block designs* $(F, \omega, 1)$, com $F = \omega^2 - \omega + 1$, $2 < K < \omega$ onde ω é potência

de número primo mais um [52]. Neste caso, o desempenho dos sistemas OCDMA usando códigos $(F, K, 1, 2)$-OOC como seqüências de espalhamento é similar ao de sistemas com aplicação de códigos $(F, K, 1)$-OOC. Além disso, o limitante superior da cardinalidade dos códigos $(F, K, 1, 2)$-OOC é maior que a cardinalidade dos códigos $(F, K, 1)$-OOC. Porém, com aumento do peso de Hamming dos códigos $(F, K, 1, 2)$-OOC, a sua cardinalidade se reduz. Logo, torna-se impraticável o aumento do peso e cardinalidade do código acima de um dado valor. Uma das técnicas usadas para contornar esta situação consiste em relaxar, ainda mais, as propriedades de correlação do código [53]. Neste trabalho, os autores apresentam códigos $(F, K, 1, \lambda_c)$-OOC baseados em planos projetivos para construir block designs $(F, \omega, 1)$, com tamanho ω para $2 \leq \lambda_c < K < \omega$.

Mais recentemente, têm sido apresentados os códigos multidimensionais (2-D, 3-D) [54]-[57] e os códigos de múltiplos comprimentos, F, ou comprimento de onda (*Multiple-length Multiple-wavelength OOC*) [58]. Espera-se que esse tipo de código venha a encontrar aplicação em sistemas com variedade de serviços, tais como dados, voz e video. Logo, usuários com diferentes requisitos de taxa de bit e qualidade de serviço (QoS) poderão ser simultaneamente alocados, sendo asseguradas, de forma dinâmica, o casamento das diferentes taxas de bits e QoS através dos códigos de diferentes comprimentos [59]-[60]. As pesquisas também se têm dedicado às aplicações OCDMA em redes GMPLS (*Generalized Multiprotocol label switching*)[61]-[63]. Outras pesquisas têm apontado para a aplicação dos OOC na transmissão multimídia em redes ópticas e em sistemas OCDMA que permitem várias taxas de bit [59], [64]-[66].

Portanto, os diversos artigos escritos, sobre códigos ortogonais ópticos, pouco se dedicam às aplicações de equações diofantinas à teoria de códigos ópticos. A equação diofantina é uma equação em que os coeficientes são inteiros e as soluções são restritas aos inteiros. Em geral, as equações diofantinas admitem várias soluções inteiras. Para encontrá-las, não existe somente um algoritmo capaz de determinar se a equação tem ou não solução. Logo, não existe um método comum para resolver todas as equações diofantinas. Cada equação possui sua especificidade, o que justifica, em parte, os mais variados métodos de resolução de tais equações que requerem um conhecimento da teoria dos números.

4.2 Construção de Códigos (F,K,1,1)-OOC

4.2.1 Representação de um inteiro na forma binária quártica

Sejam o polinômio $F(x, y)$ um representante de uma dada forma binária quártica

$$F(x, y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4 \tag{4.1}$$

e a equação quártica

$$F(x, y) = m \tag{4.2}$$

onde m e os coeficientes a, b, c, d, e são números inteiros e diferentes de zero.

Da teoria de Gauss [67], as soluções da equação (4.2) requerem conhecer os invariantes de $F(x, y)$, definidos por

$$g_2 = ae - 4bd + 3c^2; \qquad \text{e} \qquad g_3 = \begin{vmatrix} a & b & c \\ b & c & d \\ c & d & e \end{vmatrix};$$

e os covariantes de $F(x, y)$, assim definidos

$$H = -\frac{1}{144}\begin{vmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y^2} \end{vmatrix}; \quad \text{e} \quad G = -\frac{1}{8}\begin{vmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} \\ \frac{\partial H}{\partial x} & \frac{\partial H}{\partial y} \end{vmatrix}.$$

A relação entre os invariantes e os covariantes de $F(x, y)$ pode ser expressa por meio da equação

$$G^2 = 4H^3 - g_2 H F^2 - g_3 F^3 = 4(H - e_3 F)(H - e_2 F)(H - e_1 F). \tag{4.3}$$

onde e_1, e_2 e e_3 são soluções da equação

$$4t^3 - g_2 t - g_3 = 0 \tag{4.4}$$

A busca da solução (x, y) para a equação diofantina (4.2) de ordem quártica reduz-se a resolver a equação (4.4), com uma incognita t. A classe de equações binárias quárticas para g_2 e g_3 é finita e as condições sob as quais a equação (4.2) deve ser reduzida a uma equação do tipo (4.4) não podem ser expressas em termos simples. Diversos resultados, entretanto, podem ser encontrados de forma mais simples por meio de relações de congruência, mais apropriadas às finalidades computacionais de códigos.

4.2.2 Forma algébrica de códigos $(F, K, 1, 1) - OOC$

Fazendo uso de relações de congruência, nós formulamos as considerações da subseção anterior como segue. Seja α um elemento primitivo de $GF(p)$, onde p é um número primo ímpar, de modo que $K = (p-1)/2$, $F = (\mu+1)K$, $\lambda_a = 1$ e $\lambda_c = 1$. A partir dos elementos β_x não nulos do corpo de Galois, é formado o arranjo $S_x = \{\mu_{x1}, \mu_{x2}, ..., \mu_{xy}\}$ cujos elementos são dados pela seguinte equação paramétrica

$$\mu_{xy} \equiv y^4 + s_{xy} \pmod{p(p-\alpha)^2} \tag{4.5}$$

por meio da equação

$$s_{xy} \equiv \gamma_y + \chi_x \pmod{p}, \tag{4.6}$$

onde $-\beta_x y^2 \equiv \gamma_y \pmod{p}$; $-\beta_x x^2 \equiv \chi_x \pmod{p}$; $\mu = \max\{\mu_{xy}\}$ para $1 \leqslant x \leqslant p-1$, $1 \leqslant y \leqslant (p-1)/2$; e $\beta_x \in GF(p) \setminus \{0\} = \{\beta_1, \beta_2, ..., \beta_x\}$, são os elementos não nulos do corpo de Galois $GF(p)$.

Cada palavra-código do arranjo S_x é mapeada em uma seqüência binária $\mathcal{C}_x = c_{x1}, c_{x2}, ..., c_{xm}, ..., c_{xF})$ através da equação

$$c_{xm} = \begin{cases} 1, & m = \mu_{xy} + (y-1)\mu + 1 \\ 0, & fora \end{cases} \tag{4.7}$$

Teorema 4.2.1. O código gerado através das fórmulas (4.5) e (4.7) é um código $(F, K, 1, 1)$ ortogonal óptico.

4.2.3 Construção dos códigos $(F, K, 1, 1) - OOC$ conforme proposto

Seja $p = 5$, $GF(p)\backslash\{0\} = \{1, 2, 4, 3\}$, e $\alpha = 2$ o elemento primitivo. O arranjo S_x possui os seguintes elementos s_{xy}.

Para S_1:

$$s_{11} = 1^4 + ((-1 \otimes 1^2 \pmod 5) - 1 \otimes 1^2 \pmod 5) \pmod 5) \equiv 4 \pmod{45},$$
$$s_{12} = 2^4 + ((-1 \otimes 1^2 \pmod 5) - 1 \otimes 2^2 \pmod 5) \pmod 5) \equiv 16 \pmod{45}.$$

Para S_2:

$$s_{21} = 1^4 + ((-2 \otimes 2^2 \pmod 5) - 2 \otimes 1^2 \pmod 5) \pmod 5) \equiv 1 \pmod{45},$$
$$s_{22} = 2^4 + ((-2 \otimes 2^2 \pmod 5) - 2 \otimes 2^2 \pmod 5) \pmod 5) \equiv 20 \pmod{45}.$$

Para S_3:

$$s_{31} = 1^4 + ((-4 \otimes 3^2 \pmod 5) - 4 \otimes 1^2 \pmod 5) \pmod 5) \equiv 1 \pmod{45},$$
$$s_{32} = 2^4 + ((-4 \otimes 3^2 \pmod 5) - 4 \otimes 2^2 \pmod 5) \pmod 5) \equiv 19 \pmod{45}.$$

Para S_4:

$$s_{41} = 1^4 + ((-3 \otimes 4^2 \pmod 5) - 3 \otimes 1^2 \pmod 5) \pmod 5) \equiv 5 \pmod{45},$$
$$s_{42} = 2^4 + ((-3 \otimes 4^2 \pmod 5) - 3 \otimes 2^2 \pmod 5) \pmod 5) \equiv 16 \pmod{45}.$$

A Tabela 4.1 apresenta o código gerado através das equações (4.5) e (4.7), para o primo, $p = 5$.

Tabela 4.1: Código (42,2,1,1) - OOC, para $p = 5$.

x	Seqüência S_x	Palavra-Código C_x	Seqüências Binárias
1	$\{4, 16\}$	C_1	000010000000000000000 000000000000000010000
2	$\{1, 20\}$	C_2	010000000000000000000 000000000000000000001
3	$\{1, 19\}$	C_3	010000000000000000000 000000000000000000010
4	$\{5, 16\}$	C_4	000001000000000000000 000000000000000010000

4.3 Construção de Códigos (p(2p-1),p,1,2)- OOC

As pesquisas de códigos ortogonais ópticos se têm dirigido, fundamentalmente, na busca de códigos $(F, K, 1, 1) - OOC$ para sincronismo entre o transmissor e receptor e minimização da interferência. Porém, quando garantidas as propriedades de auto-correlação ideal, equação (2.7a), e correlação cruzada ideal, equação (2.7b), o limitante superior do código é dado pela expressão (2.20). Este limitante é linear em relação ao comprimento do código, conseqüentemente, o tamanho do código é consideravelmente esparso em relação ao seu comprimento. Por outro lado, não existem códigos ópticos estritamente ortogonais. Com propósito de se obter códigos de maior tamanho, são relaxadas as condições impostas pelas equações (2.7b) e (2.7a) para construção de códigos $(F, K, 1, 2) - OOC$, como documentados em [51] e [68], de modo que, sendo o desempenho do sistema limitado basicamente pela interferência de acesso múltiplo, continua existindo um erro assintótico independente da potência recebida também para os códigos $(F, K, 1, 2) - OOC$, mas, com garantia de uma recepção aceitável do sinal espalhado. Portanto, em OCDMA, garantir ortogonalidade do código óptico é assegurar $\lambda_a = \lambda_c \leq 1$ nos códigos "estritamente ortogonais" ou $\lambda_a \leq 1$ e $\lambda_c \leq 2$ nos códigos "estritamente não ortogonais".

A expressão (2.20) é linear em relação ao comprimento F do código, ou seja, a sua cardinalidade é muito menor que o seu comprimento, conseqüentemente, uma baixa razão N/F. O comprimento do código aumenta muito rapidamente com aumento do tamanho N e peso K. A fim de melhorar a razão N/F, duas técnicas podem ser usadas: a) Relaxar as propriedades de correlação para $\lambda_a = 1$ e $\lambda_c = 2$; b) códigos 2D e 3D.

Nossa opção é a de relaxar as propriedades de correlação, preservando o sincronismo através de $\lambda_a = 1$. Fazendo $\lambda_c = 2$ podemos conseguir que o código tenha uma melhor razão $\frac{N}{F}$. O código OOC, cuja $\lambda_a = 1$ e $\lambda_c = 2$, é chamado de "*não ideal*".

4.3.1 Representação de um número inteiro na forma binária quadrática

Sejam o polinômio (4.8) a forma binária quadrática

$$f(x, y) = ax^2 + bxy + cy^2 \tag{4.8}$$

e a equação quadrática

$$f(x, y) = m, \tag{4.9}$$

onde m e os coeficientes a, b, c são números inteiros e diferentes de zero.

A busca da solução (x, y) para a equação diofantina (4.9) consiste em encontrar o discriminante $D = b^2 - 4ac$ e determinar o representante do inteiro m tal que x e y são primos relativos. O polinômio (4.8) representa o número inteiro m caso existam os inteiros, x, y, de modo que $f(x, y) = m$. Formas equivalentes possuem o mesmo discriminante e, para um dado discriminante D, existe um número finito de classes equivalentes. Quaisquer duas formas equivalentes representam um mesmo inteiro. Através do método de solução da equação

(4.9), que consiste em encontrar as formas reduzidas, é tratada a representação de números inteiros pela forma binária quadrática.

Sem perda de generalidade, seja a equação binária quadrática (4.10)

$$f(x,y) = ax^2 + cy^2 = m, \tag{4.10}$$

onde $m > 0$, $(ac, m) = 1$, $(x, y) = 1$ e $(xy, m) = 1$.

A solução da equação (4.10), implica na existência de um número inteiro, k, que satisfaz a equação (4.11)

$$ak^2 + c \equiv 0 \pmod{m} \tag{4.11}$$

sob a condição de que o símbolo de Legendre $(-ac/p) = 1$ para todo número primo p que divide m. Para todo inteiro $M < 2\sqrt{ac}$ existe a solução inteira (x, y), se $x \neq 0$ e $y \neq 0$, tal que

$$f(x,y) = mM, \tag{4.12}$$

onde $a > 0$ e $c > 0$. A solução da equação (4.10) é parte da teoria de Gauss [69], entretanto muitos resultados podem ser encontrados de forma mais simples por meio de relações de congruência.

4.3.2 Forma algébrica de códigos $(F, K, 1, 2) - OOC$

Nesta seção, tratamos da representação de números inteiros por meio da forma binária quadrática através de operações de congruência para gerar códigos ortogonais ópticos. A técnica de construção deste tipo de códigos foi apresentada em [70]-[72]. A partir de relações de congruência, formulamos as considerações da subseção anterior para gerar um código $(F, K, 1, 2)$ ortogonal óptico, como se segue.

Seja α um elemento primitivo de $GF(p)$, onde p é um número primo ímpar, de modo que $F = p\,(2p-1)$, $K = p$, $\lambda_a = 1$ e $\lambda_c = 2$. A partir dos elementos do corpo de Galois β_x, é formado o arranjo S_x, cujos elementos são dados pela equação paramétrica:

$$s_{xy} \equiv \gamma_{xy} + \chi_x \pmod{2p-1}, \tag{4.13}$$

onde $-\beta_x y^2 \equiv \gamma_{xy} \pmod{p}$; $-\beta_x x^2 \equiv \chi_x \pmod{p}$ para $0 \leqslant x \leqslant p-1$, $1 \leqslant y \leqslant p$; e $\beta_x \in GF(p) = \{\beta_1, \beta_2, ..., \beta_x\}$.

Cada palavra-código do arranjo $S_x = \{s_{x1}, s_{x2}, ..., s_{xy}\}$ é mapeada em uma seqüência binária que consiste de p blocos cada com $(2p-1)$ símbolos binários, isto é, $\mathcal{C}_x = (c_{x1}, c_{x2}, ..., c_{xm}, ..., c_{xF})$ através da equação

$$c_{xm} = \begin{cases} 1, & m = s_{xy} + (y-1)(2p-1) + 1 \\ 0, & fora \end{cases} \tag{4.14}$$

Teorema 4.3.1. O código gerado através das fórmulas (4.13) e (4.14) é um código $(p(2p-1), p, 1, 2)$ ortogonal óptico.

4.3.3 Construção do Código $(p(2p-1), p, 1, 2) - OOC$ conforme proposto

Seja $p = 5$, $GF(p) = \{0, 1, 2, 4, 3\}$, e $\alpha = 2$ o elemento primitivo. O arranjo S_x possui os seguintes elementos s_{xy}.

Para S_1:

$s_{11} = (-(1^2 \otimes 1 \pmod 5) - (1^2 \otimes 1 \pmod 5) \equiv 7 \pmod 9)$,
$s_{12} = (-(1^2 \otimes 1 \pmod 5) - (2^2 \otimes 1 \pmod 5) \equiv 4 \pmod 9)$,
$s_{13} = (-(1^2 \otimes 1 \pmod 5) - (3^2 \otimes 1 \pmod 5) \equiv 4 \pmod 9)$,
$s_{14} = (-(1^2 \otimes 1 \pmod 5) - (4^2 \otimes 1 \pmod 5) \equiv 7 \pmod 9)$,
$s_{15} = (-(1^2 \otimes 1 \pmod 5) - (5^2 \otimes 1 \pmod 5) \equiv 8 \pmod 9)$.

Para S_2:

$s_{21} = (-(2^2 \otimes 2 \pmod 5) - (1^2 \otimes 2 \pmod 5) \equiv 4 \pmod 9)$,
$s_{22} = (-(2^2 \otimes 2 \pmod 5) - (2^2 \otimes 2 \pmod 5) \equiv 3 \pmod 9)$,
$s_{23} = (-(2^2 \otimes 2 \pmod 5) - (3^2 \otimes 2 \pmod 5) \equiv 3 \pmod 9)$,
$s_{24} = (-(2^2 \otimes 2 \pmod 5) - (4^2 \otimes 2 \pmod 5) \equiv 4 \pmod 9)$,
$s_{25} = (-(2^2 \otimes 2 \pmod 5) - (5^2 \otimes 2 \pmod 5) \equiv 6 \pmod 9)$.

Para S_3:

$s_{31} = (-(3^2 \otimes 4 \pmod 5) - (1^2 \otimes 4 \pmod 5) \equiv 4 \pmod 9)$,
$s_{32} = (-(3^2 \otimes 4 \pmod 5) - (2^2 \otimes 4 \pmod 5) \equiv 7 \pmod 9)$,
$s_{33} = (-(3^2 \otimes 4 \pmod 5) - (3^2 \otimes 4 \pmod 5) \equiv 7 \pmod 9)$,
$s_{34} = (-(3^2 \otimes 4 \pmod 5) - (4^2 \otimes 4 \pmod 5) \equiv 4 \pmod 9)$,
$s_{35} = (-(3^2 \otimes 4 \pmod 5) - (5^2 \otimes 4 \pmod 5) \equiv 8 \pmod 9)$.

Para S_4:

$s_{41} = (-(4^2 \otimes 3 \pmod 5) - (1^2 \otimes 3 \pmod 5) \equiv 3 \pmod 9)$,
$s_{42} = (-(4^2 \otimes 3 \pmod 5) - (2^2 \otimes 3 \pmod 5) \equiv 4 \pmod 9)$,
$s_{43} = (-(4^2 \otimes 3 \pmod 5) - (3^2 \otimes 3 \pmod 5) \equiv 4 \pmod 9)$,
$s_{44} = (-(4^2 \otimes 3 \pmod 5) - (4^2 \otimes 3 \pmod 5) \equiv 3 \pmod 9)$,
$s_{45} = (-(4^2 \otimes 3 \pmod 5) - (5^2 \otimes 3 \pmod 5) \equiv 6 \pmod 9)$.

A Tabela 4.2 apresenta o código gerado através das equações (4.13) e (4.14), para o primo, $p = 5$.

Tabela 4.2: Código (45,5,1,2) - OOC, para $p = 5$.

x	Seqüência S_x	Palavra-Código C_x	Seqüências Binárias
0	$\{0, 0, 0, 0, 0\}$	C_1	100000000 100000000 100000000 100000000 100000000
1	$\{7, 4, 4, 7, 8\}$	C_2	000000010 000010000 000010000 000000010 000000001
2	$\{4, 3, 3, 4, 6\}$	C_3	000010000 000100000 000100000 000010000 000000100
3	$\{4, 7, 7, 4, 8\}$	C_4	000010000 000000010 000000010 000010000 000000001
4	$\{3, 4, 4, 3, 6\}$	C_4	000100000 000010000 000010000 000100000 000000100

4.4 Construção de Códigos ((p-1)(2p-1),p-1,1,2) - OOC

Diversos métodos e técnicas, tais como geometria projetiva, algoritmo de Greedy [13], construção iterativa (aquela que depende de outra construção que a antecedeu para que seja realizada), teoria algébrica de códigos, técnicas combinatórias e projeto de delineamento em blocos (block design), são usados na construção de códigos ortogonais ópticos.

Para construção destes códigos, restritos a números não primos, pelo mesmo método do "código fonte", teríamos necessidade de usar da estrutura algébrica de anéis, assunto não coberto nesta tese. Para uma construção mais simples, que nos proporciona uma melhora da razão K/F, fazemos opção pela construção iterativa, limitando o peso do código K à $p - 1$.

Fazendo uso da construção iterativa, a partir do código $(p(2p-1), p, 1, 2)$-OOC, vamos construir um novo código cujo peso está limitado à números primos. Este código precisa preservar as propriedades de correlação ($\lambda_a = 1$, $\lambda_c = 2$).

4.4.1 Forma algébrica de códigos $((p-1)(2p-1), p-1, 1, 2)$-OOC

Seja α um elemento primitivo de $GF(p)$, em que p é um número primo ímpar, e que $F = (p-1)(2p-1)$, $K = p-1$. A partir dos elementos não nulos de $GF(p)$ é formado o arranjo S_x cujos elementos são dados pela expressão (4.13), para $1 \leqslant y \leqslant (p-1)$, e cada elemento do arranjo $S_x = \{s_{x1}, ..., s_{xj}\}$ é mapeado em seqüência binária $C_x = (c_{x0}, c_{x1}, ..., c_{xk}, ..., c_{xF})$ através da fórmula (4.14).

Teorema 4.4.1. As seqüências binárias, geradas através das fórmulas (4.13) e (4.14), para $1 \leqslant y \leqslant (p-1)$, formam um código $((p-1)(2p-1), p-1, 1, 2)$ - ortogonal (correlação mínima) óptico (unipolar).

A demonstração do Teorema 4.4.1 segue os mesmos procedimentos matemáticos da demonstração do Teorema 4.3.1.

4.4.2 Exemplo de Construção do Código $((p-1)(2p-1), p-1, 1, 2)$-OOC

A Tabela 4.3 apresenta os arranjos e as seqüências binárias do código $((p-1)(2p-1), p-1, 1, 2) - OOC$ para $GF(5)$.

Tabela 4.3: Código (36,4,1,2)-OOC, para $p = 5$.

x	Seqüência S_x	Palavra-Código C_x	Seqüências Binárias
0	$\{0, 0, 0, 0\}$	C_1	100000000 100000000 100000000 100000000
1	$\{7, 4, 4, 7\}$	C_2	000000010 000010000 000010000 000000010
2	$\{4, 3, 3, 4\}$	C_3	000010000 000100000 000100000 000010000
3	$\{4, 7, 7, 4\}$	C_4	000010000 000000010 000000010 000010000
4	$\{3, 4, 4, 3\}$	C_4	000100000 000010000 000010000 000100000

4.5 Análise das Propriedades de Correlação dos Códigos

Para análise das propriedades de correlação, lançamos mão da técnica usada em [9],[26], [51], [52], [29] e [73], conforme o modelo apresentado na Figura 4.1.

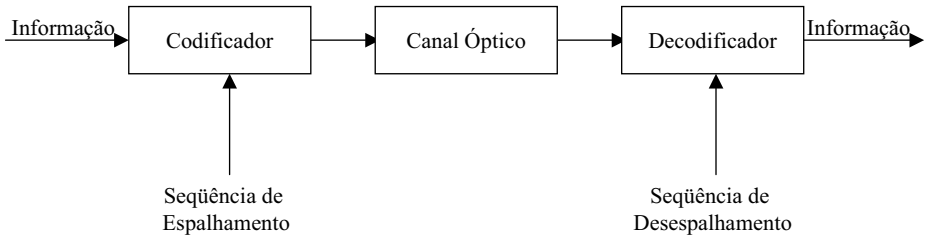
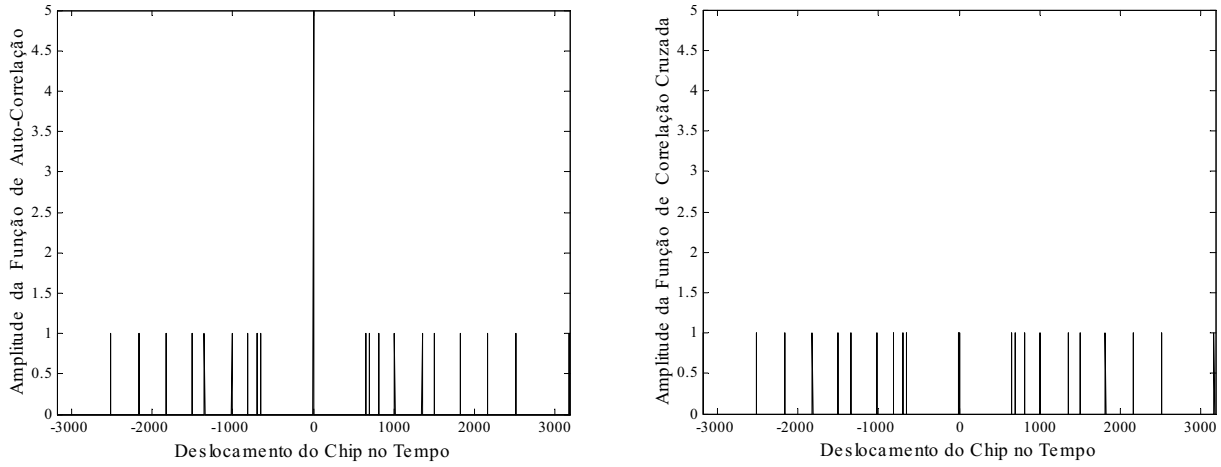


Figura 4.1: Modelo de Transmissão e Recepção OCDMA.

As figuras de auto-correlação e correlação cruzada, descritas abaixo, são obtidas com base no princípio de operação do modelo de transmissão e recepção de um sistema OCDMA, ilustrado na Figura 4.1. Cada bit "1", da seqüência de informação "1110010100", é espalhado pela seqüência de espalhamento C_x. Os bits "0" da mesma seqüência de informação não são codificados, ou seja, para cada bit "0" é transmitida uma seqüência de zeros com comprimento igual ao da seqüência de espalhamento. No receptor, a seqüência de informação codificada é comparada com a seqüência de recuperação da informação C_x, para obtenção da auto-correlação, ou comparada com a seqüência de recuperação da informação C_y, para obtenção da correlação cruzada. No caso da auto-correlação C_x, o processo significa que a seqüência de espalhamento C_x corresponde ao código de recuperação da informação C_x do usuário desejado, ou não corresponde ao código de recuperação da informação C_y do usuário desejado, no caso da correlação cruzada entre C_x e C_y. Para o sistema da Figura 4.1, são apropriados os códigos $(F, K, 1, 1) - OOC$ cujas propriedades de correlação tornam possível o sincronismo entre o transmissor e o receptor, e reduzem a probabilidade de erro.

A Figura 4.2 ilustra as propriedades de correlação do código $(F, K, 1, 1)$, para $p = 11$, quando codifica somente um bit de informação. Como ilustrado na Figura 4.2(a), a auto-correlação da palavra-código C_4 possui lóbulos laterais com amplitude igual um, como esperado. Devido a estes lóbulos laterais, o sincronismo entre o transmissor e receptor pode

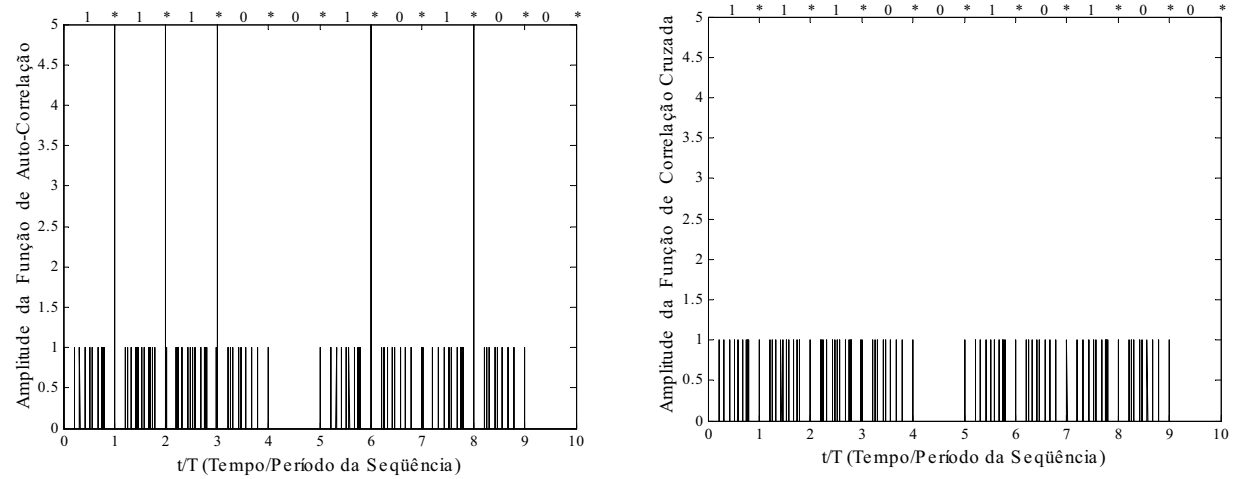
ser facilmente realizado. Esta propriedade torna este tipo de código próprio para sistemas assíncronos.



(a) Auto-Correlação de C_4 (b) Correlação Cruzada entre C_3 e C_4

Figura 4.2: Propriedades de Correlação do Código $(F, K, 1, 1) - OOC$, para $p = 11$.

Na Figura 4.2(b) é ilustrada a correlação cruzada entre as palavras-código C_3 e C_4, cuja amplitude não possui valor superior a um. As Figuras 4.2(b) e 4.2(a) mostram que os lóbulos central e laterais das funções de correlação do código se tornam mais estreitos com aumento da esparsidade (mais zeros do que uns). Essas propriedades, segundo a definição 2.2, provam ainda que o código $(F, K, 1, 1) - OOC$ proposto é ideal.

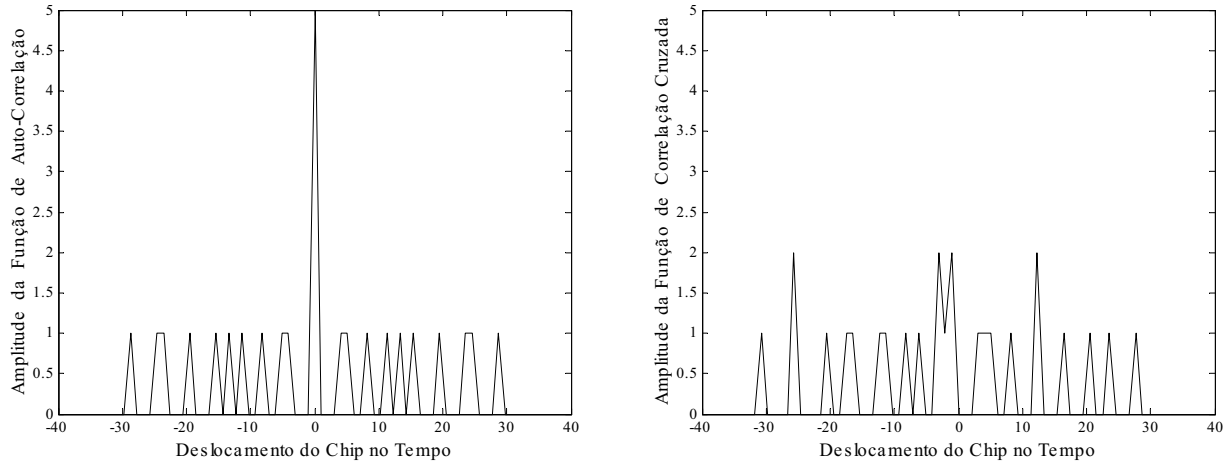


(a) Auto-Correlação de C_4 (b) Correlação Cruzada entre C_3 e C_4

Figura 4.3: Propriedades de Correlação do Código $(F, K, 1, 1)$ como seqüência de decodificação, para $p = 11$.

A Figura 4.3, ilustra as propriedades de correlação do código $(F, K, 1, 1)$, como seqüência de decodificação, para $p = 11$. Cada bit "1" da seqüência de informação 1110010100, é espalhado pela seqüência de espalhamento C_4. O sinal resultante, no receptor, é a auto-correlação da palavra-código C_4 do código $(F, K, 1, 1) - OOC$ proposto para $p = 11$, como

ilustrado na Figura 4.3(a). Para se obter a correlação cruzada das palavras-código C_3 e C_4, ilustrada na Figura 4.3(b), a seqüência de informação codificada é comparada com a seqüência de recuperação da informação C_3 que não corresponde à seqüência de espalhamento do usuário desejado. O símbolo * representa o pico da auto-correlação no instante de tempo em que o sincronismo entre o transmissor e o receptor é aplicado. Das Figuras 4.3(a) e 4.3(b) se observa que os picos de maior amplitude da auto-correlação e correlação cruzada acontecem durante a transmissão dos bits "1" da seqüência de informação. Essas figuras confirmam o esperado $\lambda_a \leq 5$, no instante de sincronismo, e $\lambda_c \leq 1$, e demonstram que os códigos $(F, K, 1, 1) - OOC$ são apropriados para sistemas OCDMA de detecção direta com modulação em intensidade. Pelo fato de este tipo de código possuir propriedade de auto-correlação bem definida, $\lambda_a = 5$ ou $\lambda_a = 0$ no instante de sincronismo, permite, do ponto de vista prático, usar filtros pouco complexos e de fácil implementação.



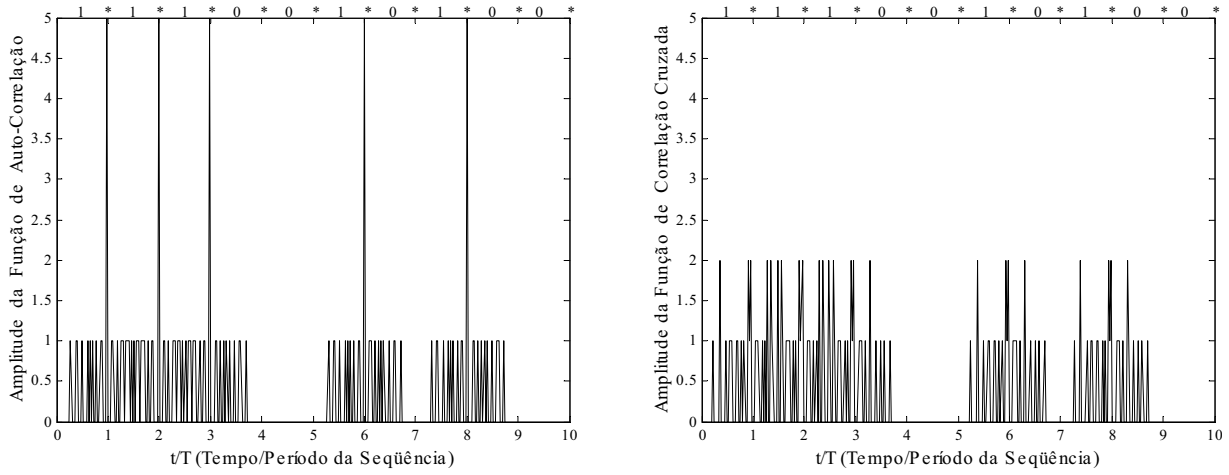
(a) Auto-Correlação de C_3

(b) Correlação Cruzada entre C_3 e C_4

Figura 4.4: Propriedades de Correlação do Código $(p(2p-1), p, 1, 2) - OOC$, para $p = 5$.

A Figura 4.4 ilustra as propriedades de correlação do código $(p(2p-1), p, 1, 2) - OOC$, para $p = 5$, quando codifica somente um bit de informação. Como está ilustrado na Figura 4.4(a), a auto-correlação da palavra-código C_3 não possui lóbulos laterais com amplitude superior a um. Devido a estes lóbulos laterais, o sincronismo entre o transmissor e receptor pode ser realizado sem comprometimento. Esta propriedade torna este tipo de código próprio para sistema assíncrono. Na Figura 4.4(b), é ilustrada a correlação cruzada das palavras-código C_2 e C_3. A correlação cruzada não possui valor superior a dois, como esperado.

A Figura 4.5 ilustra as propriedades de correlação do código $(p(2p-1), p, 1, 2) - OOC$ como seqüência de decodificação, para $p = 5$. O sinal de auto-correlação da palavra-código C_3 está ilustrado na Figura 4.5(a). Para se obter a correlação cruzada das palavras-código C_3 e C_4, ilustrada na Figura 4.5(b), cada bit "1" da seqüência de informação, é espalhado pela seqüência de espalhamento C_4. No receptor, a seqüência de informação codificada é decodificada através da seqüência de recuperação da informação C_4 que não corresponde a palavra-código do usuário desejado. Das Figuras 4.5(a) e 4.5(b) observa-se que os picos de maior amplitude



(a) Auto-Correlação de C_3

(b) Correlação Cruzada entre C_3 e C_4

Figura 4.5: Propriedades de Correlação do Código $(p(2p-1), p, 1, 2) - OOC$, como seqüência de decodificação, para $p = 5$.

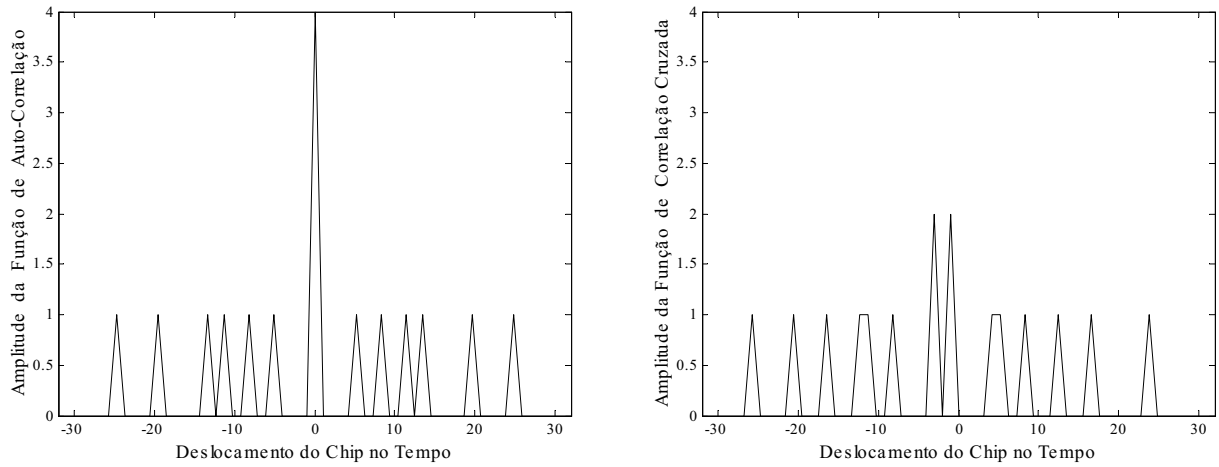
da auto-correlação e correlação cruzada acontecem durante a transmissão dos bits "1" da seqüência de informação.

Essas figuras confirmam o esperado $\lambda_a \leq 5$, no instante de sincronismo, e $\lambda_c \leq 2$, que tornam os códigos $(p(2p-1), p, 1, 2) - OOC$ próprios para sistemas OCDMA de detecção direta com modulação em intensidade. A propriedade de auto-correlação bem definida mostra que cada palavra-código é bastante diferente de todas as outras palavras-código que são sua versão deslocada no tempo (deslocamentos cíclicos).

Na Seção 2.2, um código OOC é definido pelos seguintes parâmetros: o comprimento F; o peso K; a função de auto-correlação λ_a para todos os deslocamentos diferentes de zero; a função de correlação cruzada λ_c para todos os deslocamentos. A partir do código $(p(2p-1), p, 1, 2) - OOC$, e relaxando o parâmetro K, é obtido o código $((p-1)(2p-1), p-1, 1, 2) - OOC$, o qual possui maior relação K/F e, conseqüentemente, ligeira melhoria de desempenho [29].

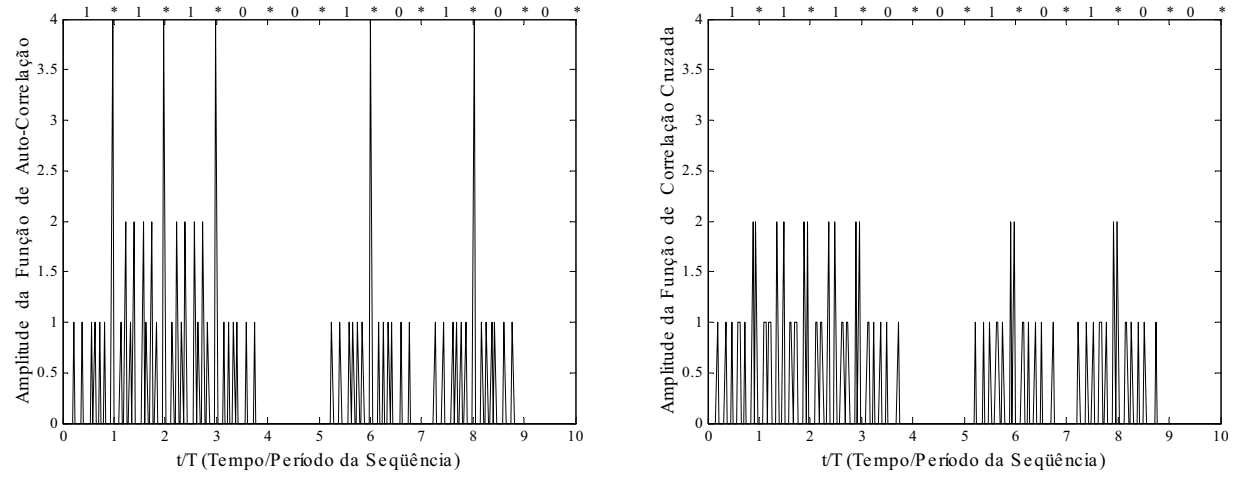
A Figura 4.6 ilustra as propriedades de correlação do código $((p-1)(2p-1), p-1, 1, 2) - OOC$, para $p = 5$, quando codifica somente um bit de informação. Como está ilustrado na Figura 4.6(a), a auto-correlação da palavra-código C_3 não possui lóbulos laterais com amplitude superior a um. Devido a estes lóbulos laterais o sincronismo entre o transmissor e receptor pode ser realizado sem comprometimento. Esta propriedade torna este tipo de código próprio para sistema assíncrono. Na Figura 4.6(b) é ilustrada a correlação cruzada das palavras-código C_2 e C_3. A correlação cruzada não possui valor superior a dois, como esperado.

A Figura 4.7 ilustra as propriedades de correlação do código $((p-1)(2p-1), p-1, 1, 2) - OOC$ como seqüência de decodificação, para $p = 5$. Cada bit "1" da seqüência de informação 1110010100, é espalhado pela seqüência de espalhamento C_3. No receptor, a seqüência de informação codificada é comparada com a palavra-código C_3 que corresponde ao código



(a) Auto-Correlação de C_3 (b) Correlação Cruzada entre C_3 e C_4

Figura 4.6: Propriedades de Correlação do Código $((p-1)(2p-1), p-1, 1, 2) - OOC$, para $p = 5$.



(a) Auto-Correlação de C_3 (b) Correlação Cruzada entre C_3 e C_4

Figura 4.7: Propriedades de Correlação do Código $((p-1)(2p-1), p-1, 1, 2) - OOC$ como seqüência de decodificação, para $p = 5$.

de recuperação da informação do usuário desejado. O sinal resultante é a auto-correlação da palavra-código C_3 do código $((p-1)(2p-1), p-1, 1, 2) - OOC$ para $p = 5$, como ilustrado na Figura 4.7(a). Para se obter a correlação cruzada das palavras-código C_2 e C_3, ilustrada na Figura 4.7(b), cada bit "1" da seqüência de informação, é espalhado pela seqüência de espalhamento C_3. No receptor, a seqüência de informação codificada é decodificada através da seqüência de recuperação da informação C_4 que não corresponde a palavra-código do usuário desejado. Das Figuras 4.7(b) e 4.7(a) se observa que os picos de maior amplitude da auto-correlação e correlação cruzada acontecem durante a transmissão dos bits "1" da seqüência de informação. Estas figuras confirmam o esperado $\lambda_a \leq 4$, no instante de sincronismo (deslocamento zero), e $\lambda_c \leq 2$, que tornam os códigos $((p-1)(2p-$

$1), p-1, 1, 2) - OOC$ próprios para sistemas OCDMA de detecção direta com modulação em intensidade. Pelo fato deste tipo de código possuir propriedade de auto-correlação bem definida, isto é, $\lambda_a = 4$ ou $\lambda_a = 0$ no instante de sincronismo, permite, do ponto de vista prático, a utilização de filtros pouco complexos, perfeitamente casados com o sinal, e de fácil implementação.

À semelhança de outros códigos OOC, os códigos OOC propostos neste capítulo podem ser implementados através de simples codificador óptico de linhas de atraso paralelas [32]-[39], de modo que estes códigos podem ser gerados e decodificadores usando técnicas de processamento óptico para sistemas não coerentes.

4.6 Análise de Desempenho dos Códigos OOC

Considerando o receptor de correlação casado, conforme mostrado na Figura 4.8, a análise de desempenho do sistema é feita em termos da interferência de acesso múltiplo (MAI) como função do número de usuários simultâneos no sistema, N, sem considerar outras causas (ruídos balístico, térmico e corrente de escuro) de degradação do desempenho do sistema. Nesta análise, os efeitos da atenuação, dispersão e espalhamento dos pulsos ópticos que se propagam pela fibra óptica são ignorados, de modo que a MAI, por ser o fator dominante, é considerada a única causa da degradação de desempenho do sistema.

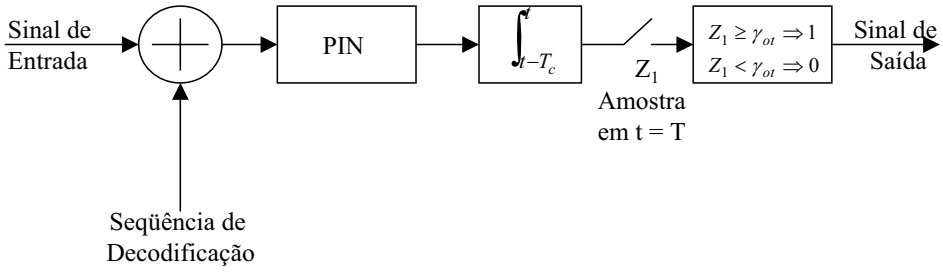


Figura 4.8: Topologia do Receptor Óptico de Correlação.

Os sinais codificados por um código OOC são detetados pelo receptor óptico cuja, variável de decisão na saída é dada por:

$$Y = \begin{cases} K + \eta_1, & \text{quando o bit “1” transmitido} \\ \eta_0, & \text{quando o bit “0” transmitido} \end{cases}$$

em que η_0 e η_1 caracterizam o ruído representado pela MAI, para o bit “0” e o bit “1”, respectivamente.

Na presente análise, são válidas as seguintes condições: **a)** os chips das palavras-código estão perfeitamente sincronizados entre todos os usuários; **b)** os chips não possuem distorção temporal; **c)** a soma do sinal dos usuários é feita de forma não coerente; **d)** a interferência de múltiplo acesso possui distribuição gaussiana e modulação OOK (*On-Off Keying*); **e)** a estatística da variável de decisão é representada pela variância e média da correlação cruzada entre os $N-1$ usuários que interferem no usuário desejado.

Logo, a estatística da variável de decisão, Y, expressa pela média e variância, é dada, respectivamente, por

$$\begin{aligned}
\mu_0 &= \mathbf{E}\{Y|0\} = \mathbf{E}\{\eta_0\} = \mathbf{E}\{\eta_0\} = 0, \\
\mu_1 &= \mathbf{E}\{Y|1\} = \mathbf{E}\{K+\eta_1\} = \mathbf{E}\{K+\eta_1\} = \mathbf{E}\{K\} + \mathbf{E}\{\eta_1\} \\
&= K + 0 = K \\
\sigma_0^2 &= \mathbf{Var}\{Y|0\} = \mathbf{E}\{Y^2|0\} - \mathbf{E}^2\{Y|0\} = \begin{cases} \frac{1}{F^2}\sum_{n=0}^{F-1}\left[Z_{i,j}(n)\right]^2, & i=j \\ 0, & i\neq j \end{cases} \\
\sigma_1^2 &= \mathbf{Var}\{Y|1\} = \mathbf{E}\{Y^2|1\} - \mathbf{E}^2\{Y|1\} \\
&= \frac{1}{2F-1}\sum_{n=0}^{F-1}\left[Z_{i,j}(n) - \frac{1}{F}\sum_{n=0}^{F-1} Z_{i,j}(n)\right]^2 \\
&= \frac{1}{2F-1}\sum_{n=-(F-1)}^{F-1}\left[Z_{i,j}(n) - \overline{Z_{i,j}}\right]^2
\end{aligned}$$

Considerando que as ocorrências do chip "0" ou do chip "1" são variáveis aleatórias independentes com distribuição gaussiana, as suas funções densidade de probabilidade (fdp) são dadas por

$$\begin{aligned}
p(Y|0) &= \frac{1}{\sqrt{2\pi}\sigma_0}\exp\left[-\frac{(Y-\mu_0)^2}{2\sigma_0^2}\right] \\
p(Y|1) &= \frac{1}{\sqrt{2\pi}\sigma_1}\exp\left[-\frac{(Y-\mu_1)^2}{2\sigma_1^2}\right]
\end{aligned} \tag{4.15}$$

Na Figura 4.9 estão ilustras, $p(Z|0)$ e $p(Z|1)$, as fdp do sinal óptico quando o chip "0" e o chip "1", respectivamente, são transmitidos.

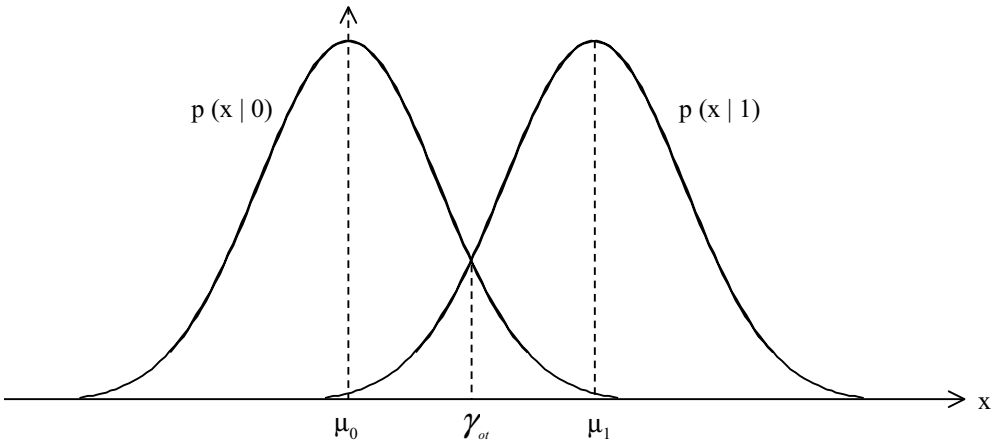


Figura 4.9: Distribuição gaussiana do sinal óptico.

Quando o chip "0" é transmitido, a probabilidade de erro é igual a:

$$Pr(Y \geq \gamma_{ot}|0) = \int_{\gamma_{ot}}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_0}\exp\left[-\frac{(Y-\mu_0)^2}{2\sigma_0^2}\right] dY \tag{4.16}$$

Quando o chip "1" é transmitido, a probabilidade de erro é igual a:

$$Pr(Y < \gamma_{ot}|1) = \int_{-\infty}^{\gamma_{ot}} \frac{1}{\sqrt{2\pi}\sigma_1} \exp\left[-\frac{(Y-\mu_1)^2}{2\sigma_1^2}\right] dY \tag{4.17}$$

Seja considerado que os chips "0" e "1" são transmitidos com igual probabilidade e que todos os usuários contribuem de forma igualitária para a interferência de múltiplo acesso. Logo,

$$\Pr(0) = \Pr(1) = \frac{1}{2} .$$

Conseqüentemente, a probabilidade de erro médio pode ser expressa por:

$$\begin{aligned} Pe &= \Pr(Y \geq \gamma_{ot}|0)\Pr(0) + \Pr(Y < \gamma_{ot}|1)\Pr(1) \\ &= \frac{1}{2}\left\{\int_{\gamma_{ot}}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_1} \exp\left[-\frac{(Y-\mu_0)^2}{2\sigma_0^2}\right] dY + \int_{-\infty}^{\gamma_{ot}} \frac{1}{\sqrt{2\pi}\sigma_1} \exp\left[-\frac{(Z-\mu_1)^2}{2\sigma_1^2}\right] dY\right\} \end{aligned} \tag{4.18}$$

O valor limiar ótimo $\gamma_{ot} = \frac{K}{2}$, que minimiza a probabilidade de erro é determinado da expressão:

$$\frac{\partial Pe}{\partial \gamma_{ot}} = Pr(Z \geq \gamma_{ot}|0)\Pr(0) + Pr(Z < \gamma_{ot}|1)\Pr(1) = 0; \tag{4.19}$$

através do procedimento apresentado na Seção 2.6. Substituindo γ_{ot} na Equação (4.18), obtém-se o valor da probabilidade de erro médio dada pela expressão:

$$Pe = \Phi\left(-\frac{\sqrt{\mathrm{SIR}}}{2}\right) \tag{4.20}$$

em que

$$\Phi(\mathrm{x}) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} \exp(-\frac{y^2}{2})dy \tag{4.21}$$

é a função distribuição cumulativa gaussiana e SIR é a relação sinal interferência, como função da correlação cruzada, dada pela expressão:

$$SIR = \frac{(\mathbf{E}\{y|1\})^2}{\sigma^2} = \frac{(\mathbf{E}\{y|1\})^2}{(N-1)(\sigma_1^2+\sigma_0^2)} = \frac{K^2}{(N-1)\ \overline{\sigma_{i,j}^2}} \tag{4.22}$$

em que N é o número de usuários no sistema, e $\overline{\sigma_{i,j}^2}$ é o valor médio das variâncias da correlação cruzada entre todos os pares de palavras-código $(\mathcal{C}_i, \mathcal{C}_j)$, dada em termos de:

$$\sigma_{i,j}^2(n) = \frac{1}{2F-1} \sum_{n=-(F-1)}^{F-1} \left[Z_{i,j}(n) - \overline{Z_{i,j}}\right]^2 \tag{4.23}$$

em que

$$\overline{Z_{i,j}} = \frac{1}{F} \sum_{n=0}^{F-1} Z_{i,j}(n) \tag{4.24}$$

é a média da correlação cruzada, entre todos os pares de palavras $(\mathcal{C}_i, \mathcal{C}_j)$ do código OOC.

A Figura 4.10 ilustra o desempenho do sistema OCDMA em termos do número de usuários. Nesse tipo de sistema, a principal limitação do desempenho do sistema consiste na

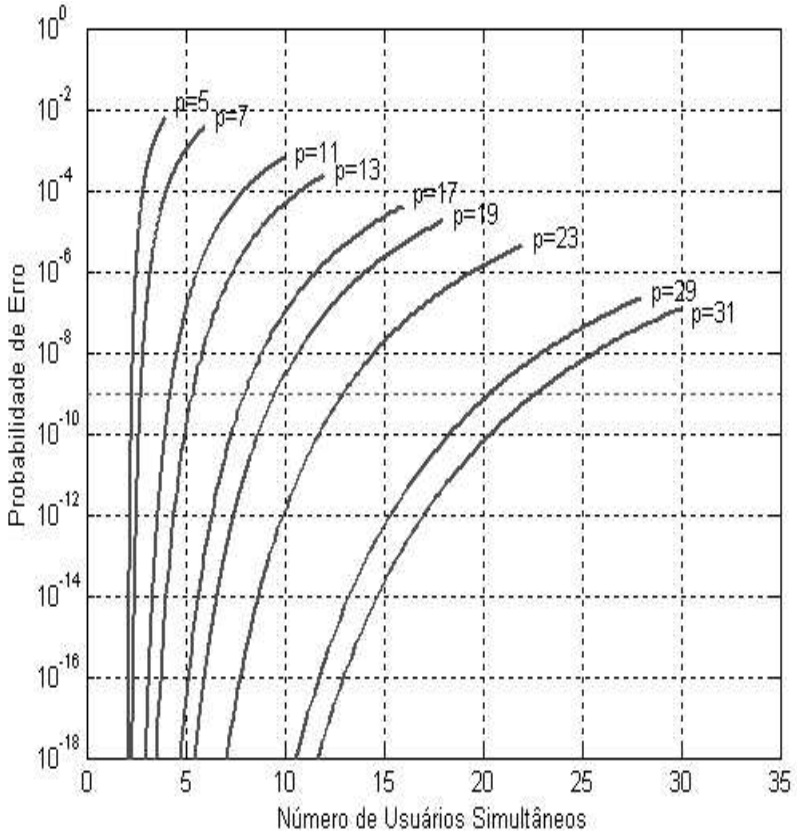


Figura 4.10: Desempenho do Código $(p(2p-1), p, 1, 2) - OOC$.

interferência de acesso múltiplo, gerada a partir dos outros usuários. O efeito dos fatores limitantes (ruído balístico, ruído térmico e corrente de escuro) do sistema, causados pela fotodetecção, é pequeno quando comparado à MAI e, conseqüentemente, pode ser desprezado quando se calcula o desempenho dos sistemas OCDMA assíncronos. Por exemplo, a família de códigos (1012,23,1,2) - OOC pode prover 22 usuários ao sistema (22 palavras-código), permitindo acesso simultâneo a 13 deles, e com taxa de erro de 10^{-9}.

A Figura 4.11 ilustra o desempenho do sistema OCDMA versus o número de usuários simultâneos quando são empregados os códigos $((p-1)(2p-1), (p-1), 1, 2)$ - OOC, para alguns valores de p entre 5 e 31. Devido as boas propriedades do código proposto, o desempenho destes códigos é aproximadamente igual ao desempenho dos códigos primos e EQC, sob as condições do mesmo número de usuários simultâneos. Duas são as formas para aumentar o número de usuários para uma dada BER. A primeira é através do aumento do comprimento do código, conseqüentemente reduzindo a taxa de bit. A segunda forma é aumentando o peso do código e, simultaneamente, reduzindo o comprimento da palavra-código, isto é, a segunda forma equivale a comparar a relação K/F entre os códigos. Para o código proposto, esta relação é igual a $\frac{1}{2p-1}$, o mesmo valor do código EQC, conseqüentemente, apresentando o mesmo desempenho.

A Figura 4.10 ilustra o desempenho do sistema OCDMA em termos do número de usuários. Neste tipo de sistema, a principal limitação do desempenho do sistema consiste na interferência de acesso múltiplo "MAI - Multiple Access Interference", gerada a partir dos outros

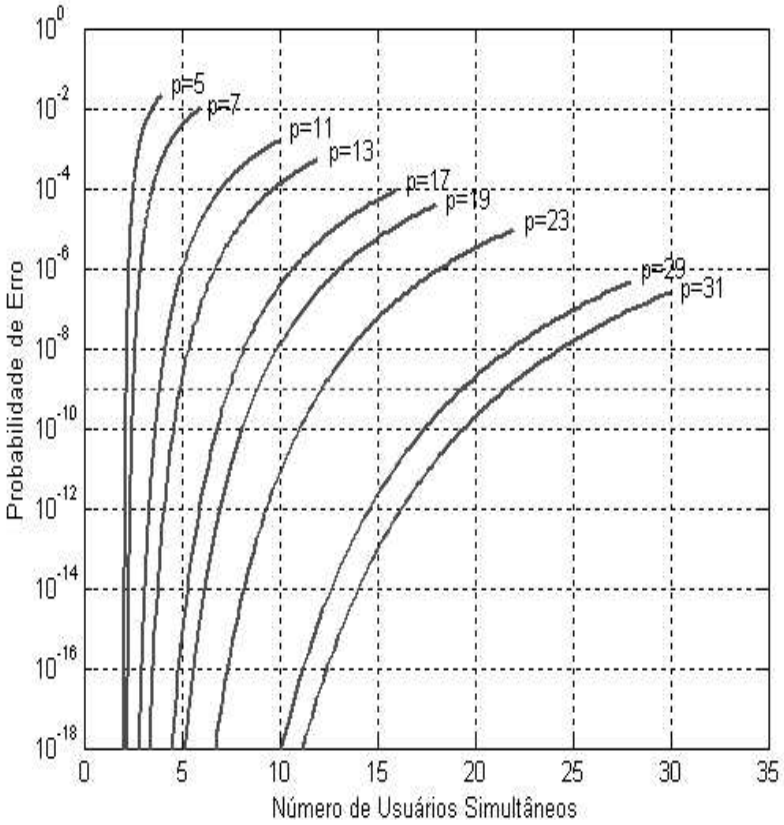


Figura 4.11: Desempenho do Código $((p-1)(2p-1), p-1, 1, 2) - OOC$.

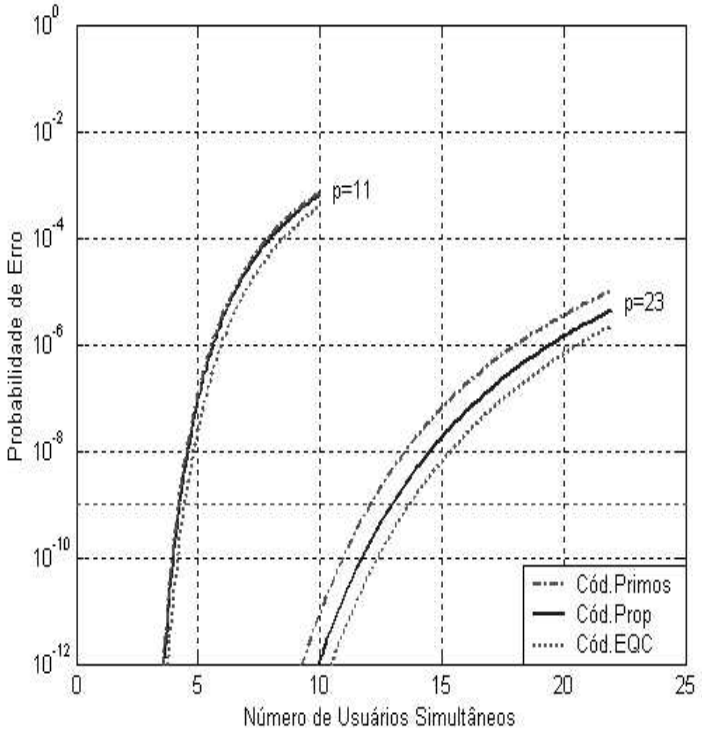


Figura 4.12: Comparação de Desempenho dos Códigos: Prop.,EQC,Primo.

usuários. Por exemplo, o código (1012,23,1,2)- OOC possui 22 palavras-código, garantindo

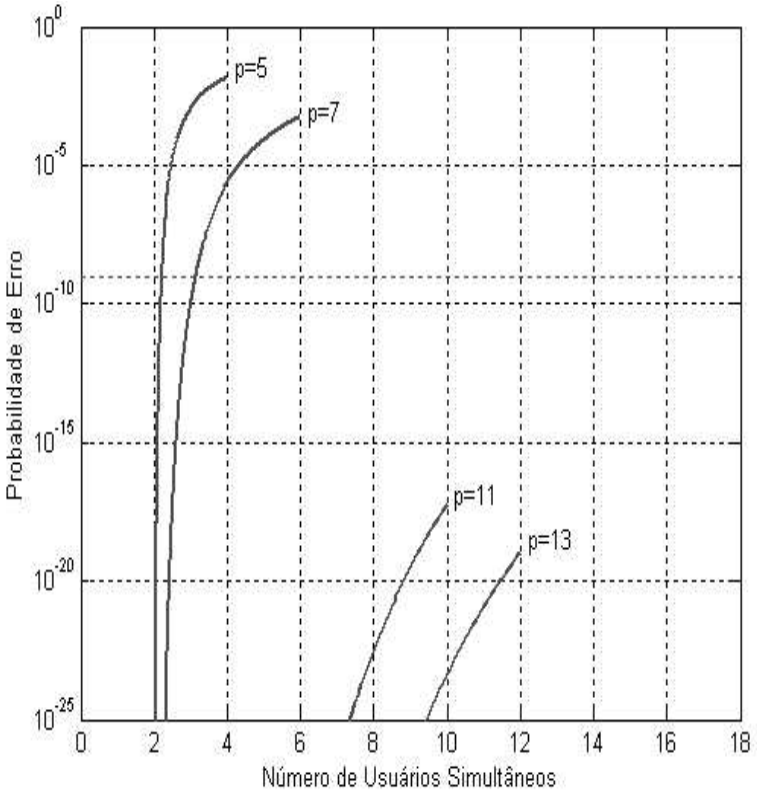


Figura 4.13: Desempenho do Código $(F, K, 1, 1) - OOC$.

acesso simultâneo a 13 usuários, para uma dada BER de 10^{-9}. Para uma taxa de 10 $Gbit/s$ do sistema, cada usuário pode transmitir a uma taxa de $9,8$ $Mbits/s = (10\ Gbits/s)/1012$.

A Figura 4.12 ilustra uma comparação do desempenho entre os códigos primo, os códigos $(p(2p-1), p, 1, 2)$-OOC, e os códigos EQC, tendo como parâmetro o número primo p que gera a respectiva família de códigos. O código $(p(2p-1), p, 1, 2)$-OOC possui desempenho superior ao dos códigos primos e relativamente inferior que o desempenho dos códigos EQC. Assim, para um dado BER de 10^{-9}, o código proposto é superior ao número de usuários assegurados pelo código primo e inferior ao número de usuários assegurados pelo código EQC. O código proposto possui cardinalidade igual a $p - 1$.

A Figura 4.13 apresenta o desempenho do sistema OCDMA não coerente versus o número de usuários simultâneos para as diferentes famílias de códigos $(F, K, 1, 1)$ - OOC propostos. A partir da figura, pode-se concluir [5], [74]: a cardinalidade, isto é, número de usuários simultâneos de uma família OOC ideal, é especificada pela equação (2.20). Esta revela que, independente de sua construção, todo sistema OCDMA está sujeito às seguintes limitações, decorrentes do OOC usado:

Para um dado comprimento F do código, o peso K deste código precisa ser o menor possível para maximizar o número de usuários, isto é, o OOC precisa ser esparso o suficiente em número de "chips" "1", limitando de forma significativa a potência, a menos que sejam usados "chips" de alto valor de potência de pico.

À medida que o número de usuários simultâneos aumenta, a razão F/K precisa ser aumentada para manter o desempenho do sistema OCDMA. Para isso, a largura de chip

precisa ser reduzida a um tamanho que pode se tornar incompatível com a largura de faixa do fotodetector sendo necessário recorrer ao uso de dispositivos ópticos não lineares, portanto aumentando o custo e a complexidade do sistema. Portanto, para que seja alcançado o desempenho ótimo do sistema é necessário um compromisso entre os parâmetros F, K e N do código.

Capítulo 5

Medida de Desempenho de Sistemas OCDMA

A avaliação do desempenho de um sistema OCDMA para diferentes estruturas de códigos é feita fundamentalmente por meio de três métodos principais: **a)** considerando a interferência de múltiplo acesso (MAI) e desprezando os efeitos negativos dos ruídos térmico e balístico do fotodetector [75]-[76]; **b)** modelando o fotodetector através da aproximação de Poisson com base em técnicas de fóton-contagem (photon-counting) para estimar a BER [77]-[84]; **c)** considerando o fotodetector modelado por meio de aproximação Gaussiana, com até dois limitadores ópticos para suprimir a MAI capaz de gerar erro no sistema [85]-[90]. Esta aproximação é aparentemente a mais completa visto que considera vários ruídos e imperfeições no sistema.

O objetivo deste capítulo é avaliar o desempenho de um sistema OCDMA usando o código (F, K, 1, 1)-OOC proposto, considerando os fatores limitantes da detecção óptica, conforme o item c). Ainda neste capítulo, são feitas comparações de desempenho usando código (F, K, 1, 1)-OOC proposto com um código $(F, K, 1, 1) - OOC$ que satisfaz o limitante de Jonhson. Um sistema com conversão bipolar-unipolar é analisado para comparar seu desempenho ao desempenho de um sistema similar que utiliza códigos OOC.

Na Seção 5.2 (distribuição WMC versus Gaussiana), mostramos que a distribuição WMC (*Webb, McIntyre, Conradi*) pode ser substituída por uma gaussiana invertida que conduz a um desempenho aproximadamente igual ao desempenho avaliado através de uma distribuição gaussiana. Logo, esta seção apresenta a justificativa para o uso da distribuição gaussiana na análise de desempenho de um sistema com receptor APD. Na Seção 5.1 (sistema com conversão bipolar-unipolar) é avaliado o desempenho de um sistema que emprega códigos bipolares. Na Seção 5.3 (desempenho de um sistema usando código (F, K, 1, 1)-OOC), são comparados os desempenhos do sistema usando o código $(F, K, 1, 1) - OOC$ proposto no Capítulo 4 e um código $(F, K, 1, 1) - OOC$ ótimo.

5.1 Sistemas com conversão Bipolar - Unipolar

A conversão de código bipolar-unipolar, denotada por "SIK" (*Sequence Inverse Keying*) [91]-[92], é uma técnica que consiste em usar a versão unipolar de um código bipolar para aplicação em sistemas OCDMA.

Considere a topologia do receptor da Figura (5.1) com dois fotodetectores APD balanceados sem limitador óptico (detector de limiar). Uma seqüência bipolar é convertida em unipolar substituindo cada bit "-1" por um bit "0" através do seguinte procedimento. Sejam

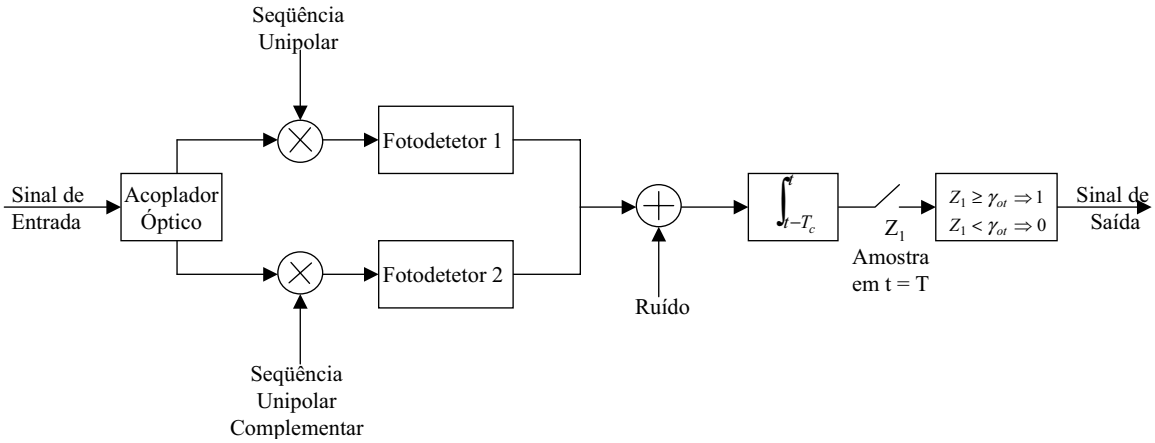


Figura 5.1: Topologia do Receptor Óptico de Correlação Balanceado.

a seqüência de informação definida conforme a expressão (2.1), em que $x_{k,l} \in \{+1, -1\}$, e a seqüência de espalhamento conforme a expressão (2.2), em que $y_{k,l} \in \{+1, -1\}$. Logo, a conversão é efetivada mediante as expressões:

$$\begin{cases} x_k(t) = \left\{b_k(t) - \overline{b}_k(t)\right\} \\ y_k(t) = \left\{a_k(t) - \overline{a}_k(t)\right\} \end{cases} \tag{5.1}$$

em que:

$$b_k(t) = \sum_{l=-\infty}^{\infty} b_{k,l} \;\; p_{T_b}(t - lT_b)$$

é a seqüência unipolar de informação, $b_{k,l} \in \{+1, 0\}$, e $\overline{b}_k(t)$ é a forma complementar de $b_k(t)$;

$$a_k(t) = \sum_{l=-\infty}^{\infty} a_{k,l} \;\; p_{T_c}(t - lT_c)$$

é a seqüência unipolar de espalhamento, $a_{k,l} \in \{+1, 0\}$, e $\overline{a}_k(t)$ é a forma complementar de $a_k(t)$. Assim, as seqüências unipolares e bipolares em um sistema SIK estão relacionadas através das expressões:

$$\begin{cases} b_k(t) = \frac{1-x_k(t)}{2} \\ \overline{b}_k(t) = \frac{1+x_k(t)}{2} \\ a_k(t) = \frac{1-y_k(t)}{2} \\ \overline{a}_k(t) = \frac{1+y_k(t)}{2}, \end{cases} \tag{5.2}$$

logo,

$$b_k(t) \oplus a_k(t) = \frac{1 + x_k(t)y_k(t)}{2},$$

onde o símbolo " $\oplus$ " denota operação de adição módulo 2.

O desempenho do sistema SIK é determinado mediante o seguinte procedimento. Sejam o sinal transmitido pelo $k - ésimo$ usuário, que pode ser representado pela expressão:

$$S_k(t) = P_s b_k(t) \oplus a_k(t),$$

e o sinal recebido, dado pela expressão

$$R(t) = \sum_{k=1}^{N} P_s b_k(t - \tau_k) \oplus a_k(t - \tau_k) + n(t),$$

onde τ_k é o atraso relativo uniformemente distribuído no intervalo $[0, T_b]$, P_s é a potência do chip, $n(t)$ é o ruído branco gaussiano com densidade espectral bilateral de potência igual a $N_0/2$.

A variável de decisão é representada pela expressão:

$$\begin{aligned} Z_i(t) &= \int_0^T R(t)y(t)dt \\ &= \int_0^T \left[\sum_{k=1}^{N} P_s \;\; b_k(t - \tau_k) \oplus a_k(t - \tau_k) + n(t)\right] \{a_i(t) - \overline{a}_i(t)\}\, dt \\ &= \int_0^{T_c} \sum_{k=1}^{N} \sum_{l=0}^{F-1} RGM \frac{2P_s}{F^2} \;\; b_k(lT_c - \tau_k) \oplus a_k(lT_c - \tau_k) \{a_i(lT_c) - \overline{a}_i(lT_c)\}\, dt + \int_0^{T_c} n_o(t)dt; \end{aligned} \tag{5.3}$$

onde R é a responsividade do diodo APD, M é o fator de multiplicação média de avalanche, G é o ganho óptico, $n_o(t)$ é o ruído total do canal.

Sem perda de generalidade, considerando $k = i$ e $\tau_i = 0$, e considerando o receptor sintonizado ao usuário k, a variável de decisão em $t = T_b$ é representada pela expressão:

$$Z_i(T_b) = D + I + \aleph \tag{5.4}$$

$$= \underbrace{T_c RGM \frac{P_s}{N}}_{\text{Sinal Desejado}} + \underbrace{\sum_{k=1 k\neq i}^{K} \sum_{l=0}^{N-1} \int_0^{T_c} RGM \frac{P_s}{N^2} x_k(lT_c - \tau_k) y_k(lT_c - \tau_k) y_i(lT_c) dt}_{\text{MAI}} + \underbrace{\int_0^{T_c} n_o(t)dt}_{\text{Ruído}} \tag{5.5}$$

Com relação ao número de fótons detetados na duração do chip, a estatística da variável

de decisão, expressa pela média e variância, é dada, respectivamente, por

$$\begin{aligned} E_z &= E\left[Z_i(T_b)\right] \\ &= E\left[D\right] + E\left[I\right] + E\left[\aleph\right] \end{aligned}$$

e

$$\begin{aligned} \sigma_z^2 &= Var\left[Z_i(T_b)\right] \\ &= Var\left[D\right] + Var\left[I\right] + Var\left[\aleph\right]. \end{aligned}$$

O termo D na equação (5.4) representa o sinal do usuário desejado k quando a componente DC do sinal é eliminada através do uso de seqüências diretas balanceadas. A média e variância de D, na duração do chip, são dadas, respectivamente, por:

$$E\left[D\right] = \frac{1}{q}\left[T_c RGM \frac{P_s}{F}\right] = \frac{T_c RGM \frac{P_s}{F}}{q}$$

e

$$Var\left[D\right] = 0.$$

O termo I na Equação (5.4) representa a interferência de múltiplo acesso do sistema. Considerando aleatórios o bit de informação e o chip, a média e a variância são dadas, respectivamente, pelas expressões

$$E\left[I\right] = E\left[\sum_{k=1k\neq i}^{N}\sum_{l=0}^{F-1}\int_0^{T_c} RGM\frac{P_s}{qF^2}\;\; x_k(lT_c)\;\; y_k(lT_c)\;\; y_i(lT_c)dt\right] = 0$$

e

$$\begin{aligned} Var\left[I\right] &= E\left[I^2\right] - E^2\left[I\right] = E\left[I^2\right] \\ &= E\left[\left(\sum_{k=1k\neq i}^{N}\sum_{l=0}^{F-1}\int_0^{T_c} RGM\frac{P_s}{qN^2}\;\; x_k(lT_c)\;\; y_k(lT_c)\;\; y_i(lT_c)dt\right)^2\right] \\ &= \left[RGM\frac{P_s}{qF^2}\right]^2 \sum_{k=1k\neq i}^{N} E\left[\left(x_{k,l-1}\;\; R_k(\tau_k) + x_{k,l}\;\; \widehat{R}_k(\tau_k)\right)^2\right]. \end{aligned}$$

Nos intervalos $0 \leq \tau_k \leq T_b$ e $0 \leq lT_c \leq \tau_k \leq (l+1)T_c \leq T_b$, as funções de correlação cruzadas parciais contínuas $R_k(\tau_k)$ e $\widehat{R}_k(\tau_k)$ foram documentadas em [93] como sendo iguais a

$$\sum_{k=1k\neq i}^{N} E\left[\left(x_{k,l-1}R_k(\tau_k) + x_{k,l}\widehat{R}_k(\tau_k)\right)^2\right] = \frac{2\left(N-1\right)}{3F}$$

e

$$\sigma_I^2 = Var\left[I\right] = \left[RGM\frac{P_s}{qF^2}\right]^2 \frac{2(N-1)}{3F}. \tag{5.6}$$

O termo $\aleph$ na Equação (5.4), representa o ruído branco gaussiano aditivo "AWGN - Additive White Gaussian Noise", cuja média e a variância são dados , respectivamente, pelas seguintes expressões:

$$\begin{aligned} E[\aleph] &= E\left[\int_0^{T_b} n(t)\left\{a_i(t)-\overline{a}_i(t)\right\}dt\right] \\ &= \int_0^{T_b}\frac{1}{q}E\left[n(t)\left\{a_i(t)-\overline{a}_i(t)\right\}\right]dt = 0 \end{aligned}$$

e

$$\begin{aligned} \sigma_0^2 = Var(\aleph) &= E\left[\aleph^2\right] - E^2[\aleph] = E\left[\aleph^2\right] \\ &= E\left[\left(\frac{1}{q}\int_0^{T_b}\left[n(t)\ \left\{a_i(t)-\overline{a}_i(t)\right\}\right]dt\right)\left(\frac{1}{q}\int_0^{T_b}\left[n(\xi)\ \left\{a_i(\xi)-\overline{a}_i(\xi)\right\}\right]d\xi\right)\right] \\ &= E\left[\frac{1}{q^2}\int_0^{T_b}\int_0^{T_b}\left[\left\{a_i(t)-\overline{a}_i(t)\right\}\left\{a_i(\xi)\ -\overline{a}_i(\xi)\right\}\right]\left[n(t)n(\xi)\right]dtd\xi\right] \\ &= \frac{T_b}{q^2}\int_0^{T_b}E\left[n(t)n(\xi)\right]dt = \frac{T_b}{q^2}\int_0^{T_b}\frac{N_0}{2}\delta(t-\xi)dt \\ &= \frac{T_c}{q^2}\left(qRGM^{2+x}\frac{NP_s}{F} + 2qM^{2+x}I_{dk} + N_{th}\right) \end{aligned}$$

em que $B = \frac{1}{2T_c}$ e $F = T_b/T_c$.

Considerando que o número de usuários N e o ganho de processamento F são muito maiores que a interferência de múltiplo acesso na entrada do receptor, o sinal de saída pode ser modelado por um processo aleatório gaussiano de média zero. Logo, a relação sinal ruído é dada pela expressão:

$$\begin{aligned} SNR_i &\cong \frac{\left(E\left[Z_i(T_b)\right]\right)^2}{\sigma^2\left[Z_i(T_b)\right]} \\ &= \frac{\left(E[D]\right)^2}{\sigma^2[I]+\sigma_0^2} \\ &= \frac{\left[RGM\frac{P_s}{F}\right]^2}{\left[RGM\frac{P_s}{F}\right]^2\frac{2(N-1)}{3F} + 2qBRGM^{2+x}\frac{NP_s}{F} + 4qBM^{2+x}I_{dk} + 2BN_{th}} \end{aligned} \tag{5.7}$$

Conseqüentemente, seguindo o procedimento apresentado na Seção 2.6 o desempenho do sistema, expresso pela probabilidade de erro é dado por:

$$\begin{aligned} P_e &= P_z(Z<0|1)P(1) + P_z(Z>0|0)P(0) \\ &= \frac{1}{2}P_z(Z<0|1) + \frac{1}{2}P_z(Z>0|0) \\ &= Q\left(\sqrt{SNR_i}\right) \end{aligned} \tag{5.8}$$

A probabilidade de erro do sistema usando a conversão bipolar-unipolar está ilustrada na Figura 5.2, considerando os seguintes parâmetros: $R = 0,8\ AW^{-1}$ (responsividade dos diodos APD), $2B = \frac{1}{T_c} = 140$ Mbit/s (o dobro da largura de banda do receptor), $F = 64$ (ganho de processamento), G (ganho óptico), $F_e = M^x$ (fator de emissão espontânea), $M = 15$ (fator de multiplicação média de avalanche), $x = 0,5$ (parâmetro de ajuste), $I_{dk} = 10$ nA (valor da corrente de escuro), $N_{th} = 1\ pA^2Hz^{-1}$ (densidade de potência do ruído térmico), $\lambda = 1,3\mu m$ (comprimento de onda do sinal óptico em LAN). Para este sistema, sem ganho óptico e com parâmetro N = 1, 3, 5, 8, a sensibilidade é igual a $P_s = -30\ dBm$ para $Pe = 10^{-9}$, como ilustrado na Figura 5.2.

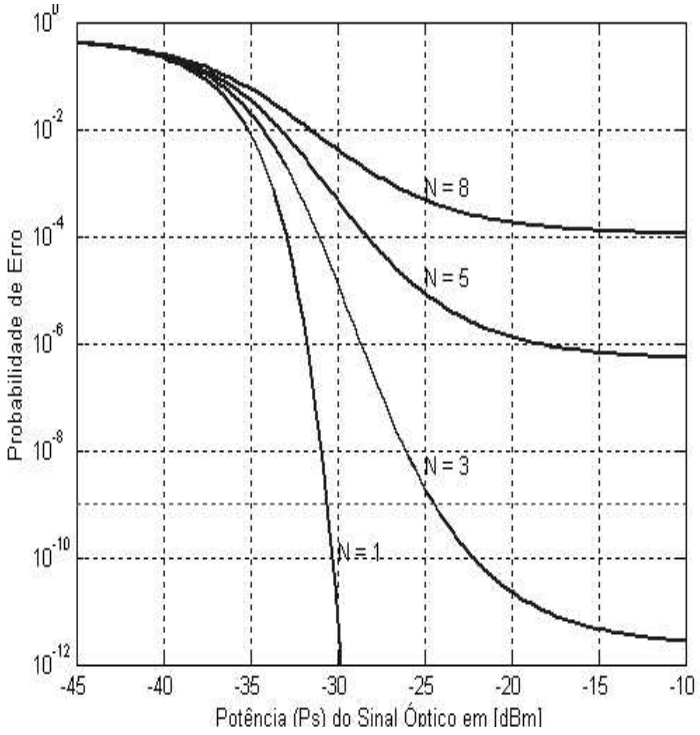


Figura 5.2: Desempenho do Sistema OCDMA com Conversão Bipolar - Unipolar.

Com aumento do número de usuários constata-se uma degradação no desempenho do sistema. A partir de $N = 3$, as curvas tende para um patamar de erro "error floor". Para $N = 3, 5, 8$ os patamares de erro são $Pe = 2,72.10^{-12}$; $Pe = 5,34.10^{-7}$; $Pe = 1,12.10^{-4}$, respectivamente. Para $N = 5$ e 8, a sensibilidade mínima necessária ($Pe = 10^{-9}$) para detecção aceitável do sinal do usuário não é atingida.

O desempenho pode ser melhorado aumentando-se o ganho do sistema (G) através de amplificação óptica [94]-[98]. Usando os parâmetros da Figura 5.2, a probabilidade de erro versus número de usuários no sistema é ilustrada na Figura 5.3.

Os códigos bipolares, aplicados em sistemas ópticos, permitem um número de usuários muito inferior ao seu limitante superior (N+2). Portanto, para este tipo de código, o receptor requer sincronismo com o respectivo transmissor para evitar falsa detecção. Na prática, estas restrições limitam o uso dos códigos bipolares em sistemas OCDMA síncronos.

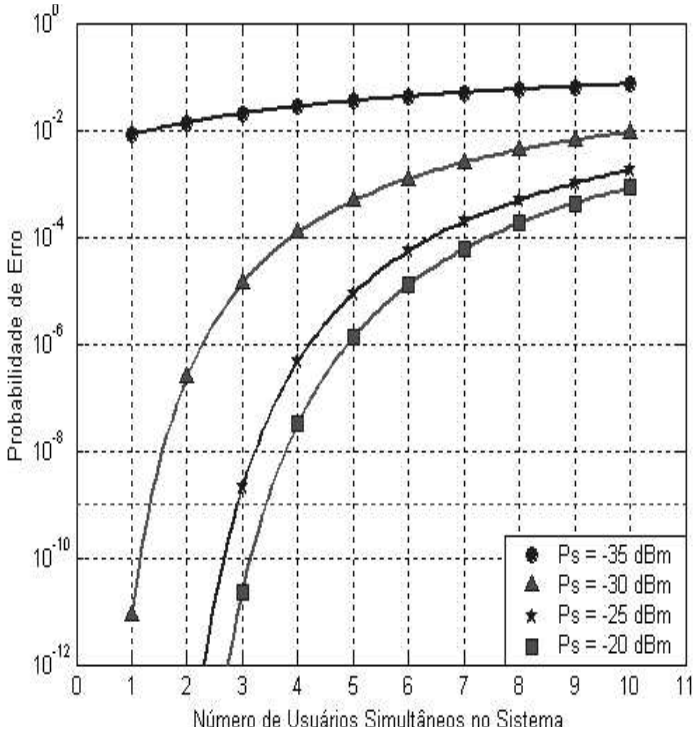


Figura 5.3: Número de Usuários Simultâneos no Sistema.

5.2 Distribuição WMC versus Gaussiana

Seja o receptor APD modelado pela distribuição do tipo Webb, McIntyre, Conradi (WMC) [99]. Devido a sua complexidade, a distribuição WMC é substituída por uma função gaussiana inversa. Esta, equivalente a função WMC, possibilita a geração de variáveis aleatórias distribuídas por meio da distribuição WMC e conduz a uma análise eficiente do detector APD.

O princípio de operação do diodo APD envolve a multiplicação em avalanche, de forma aleatória, entre os portadores ópticos (fótons) na entrada e os portadores elétricos (pares elétron-lacuna) na saída do dispositivo, logo, o sinal de saída precisa ser descrito através de probabilidade de distribuição. Para um dado instante de tempo, a função densidade de probabilidade (fdp) WMC é dada pela expressão:

$$p_r(r|n) = \frac{1}{\sqrt{2\pi}\sigma}\left[1+\frac{r-M}{\Psi\sigma}\right]^{-(3/2)} \exp\left[-\frac{(r-M)^2}{2\sigma^2\left[1+\frac{r-M}{\Psi\sigma}\right]}\right],\ \forall r,\ 0<r<\infty \tag{5.9}$$

em que r é o total de elétrons na saída do APD, n é o número de fótons na entrada do APD, $\overline{n}$ é a média de fótons na entrada do APD, G é o ganho médio do diodo APD, $M = \overline{n}G$ é a média estatística, $\sigma^2 = \overline{n}G^2F_e$ é a variância de r,

$$F_e = k_{ef}G + (1-k_{ef})(2-\frac{1}{G}) \tag{5.10}$$

é o fator de emissão espontânea, k_{ef} é a razão de ionização de elétrons pelas lacunas no APD e a razão $\Psi = \frac{\sqrt{\overline{n}F_e}}{F_e-1}$.

Para um valor médio de fótons na entrada do APD, a WMC descreve o comportamento estatístico do número aleatório de elétrons na saída do APD. Para descrever o sinal de saída do APD, a fdp WMC considera a chegada dos fótons na entrada e que a multiplicação por avalanche dos elétrons no APD possui distribuição de Poisson.

Seja a fdp gaussiana invertida (GI) de uma variável aleatória X, com parâmetros μ e β, dada pela expressão [100]-[101]:

$$p_x(x|\mu,\beta) = \begin{cases} \frac{\beta}{\sqrt{2\pi}}\left[x\right]^{-(3/2)}\exp\left[-\frac{\beta(x-\mu)^2}{2\mu^2 x}\right], & x>0 \\ 0 & fora \end{cases} \tag{5.11}$$

em que $\mu > 0$ e $\beta > 0$. A função de distribuição cumulativa (fdc) da variável X, denotada por $F(x)$, quando expressa em termos da função de distribuição cumulativa gaussiana, $\Phi(X)$, é dada pela expressão [102]:

$$F(X) = \Phi\left[\sqrt{\frac{\beta}{X}}\left(-1+\frac{X}{\mu}\right)\right] + \exp\left(\frac{2\beta}{\mu}\right)\Phi\left[-\sqrt{\frac{\beta}{X}}\left(1+\frac{X}{\mu}\right)\right] \tag{5.12}$$

Seja a variável $x(r)$ definida por

$$x(r) = 1 + \frac{r-M}{\Psi\sigma}, \tag{5.13}$$

então, a derivada de x em relação a r é dada por:

$$\frac{\partial x}{\partial r} = \frac{1}{\Psi\sigma}. \tag{5.14}$$

Por meio de transformação de variáveis aleatórias, determinamos a fdp da variável x

$$\begin{aligned} p_x(x|\mu,\beta)\partial x &= p_r(r|n)\partial r \\ &= \frac{p_r(x(r)|n)}{\left|\frac{\partial x(r)}{\partial r}\right|}; \end{aligned} \tag{5.15}$$

em que $x(r)$ é a correspondente transformação da variável. Logo,

$$\begin{aligned} p_x(x|\mu,\beta) &= \frac{p_r(x(r)|n)}{\left|\frac{\partial x(r)}{\partial r}\right|} \\ &= \frac{\frac{1}{\sqrt{2\pi\sigma}}\left[x(r)\right]^{-(3/2)}\exp\left\{-\frac{\Psi^2[x(r)-1]^2}{2x(r)}\right\}}{\left|\frac{1}{\Psi\sigma}\right|} \\ &= \frac{\Psi}{\sqrt{2\pi}}x^{-(3/2)}\exp\left[-\frac{\Psi^2(x-1)^2}{2x}\right] \end{aligned} \tag{5.16}$$

Assim, a equação (5.16) é igual a equação (5.11) quando $\beta = \Psi^2$ e $\mu = 1$. Substituindo

$$Z = Z(r) = \frac{r}{\Psi\sigma} + (1 - \frac{M}{\Psi\sigma})$$

na equação (5.12) e fazendo uso da função de erro complementar, obtemos a fdc gaussiana dada por:

$$F(r) = \frac{1}{2}\,\mathrm{erfc}(\left[-\frac{\Psi(Z-1)}{\sqrt{2Z}}\right]) + \frac{1}{2}\exp\left(\Psi^2\right)\mathrm{erfc}(\left[\frac{\Psi(Z+1)}{\sqrt{2Z}}\right]) \tag{5.17}$$

A equação (5.17) representa uma solução equivalente à solução da WMC e proporciona a análise de desempenho de sistemas com receptor APD através da função gaussiana, sem complexos métodos numéricos que seriam necessários caso fosse usada diretamente a WMC.

Logo, a probabilidade de erro do sistema com detector APD, usando a aproximação gaussiana, é dada pela expressão:

$$\begin{aligned} Pe &= P(r \geq \gamma|0)P(0) + P(r < \gamma|1)P(1) \\ &= \frac{1}{2}\int_{-\infty}^{\gamma} p_1(r \geq \gamma|0)dr + \frac{1}{2}\int_{\gamma}^{\infty} p_0(r < \gamma|1)dr \\ &= \frac{1}{2}\left\{F_1(\gamma_{ot}) + [1 - F_0(\gamma_{ot})]\right\} \end{aligned} \tag{5.18}$$

onde $F_1(\gamma_{ot})$ e $F_0(\gamma_{ot})$ são as fdc quando o bit "1" e bit "0" são transmitidos, respectivamente, e γ_{ot} é o limiar ótimo do receptor sem ruído.

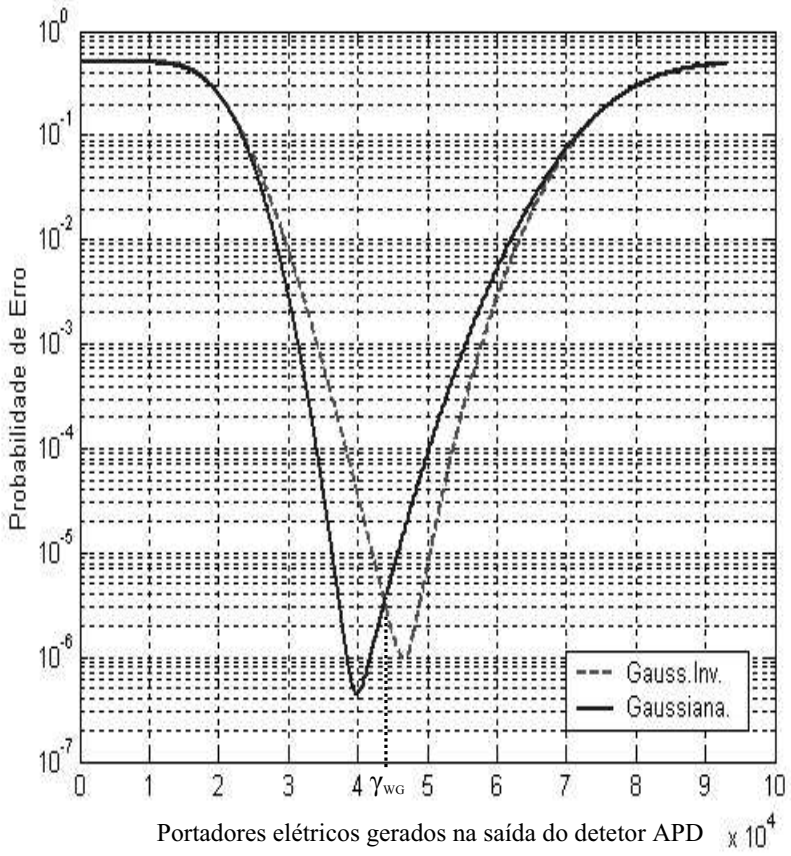


Figura 5.4: Comparação das aproximações GI e gaussiana do detector APD, para $G = 200$ e $k_{ef} = 0,01$.

Considerando que o receptor da Figura 5.5 é sem limitador óptico, sem ruído e possui os seguintes parâmetros $G = 200$ e $k_{ef} = 0,01$, a Figura 5.4 ilustra o desempenho do sistema

para $\overline{n}_1 = 391$ portadores ópticos detetados quando o bit "1" é transmitido e $\overline{n}_0 = 100$ quando o bit "0" é transmitido. O valor limiar ótimo é igual a $\gamma_{ot} = 46625.10^4$ elétrons na saída do receptor para probabilidade de erro $Pe = 10^{-6}$.

No caso da aproximação gaussiana, o número de elétrons é igual a $\gamma_{ot} = 39915.10^4$ para $Pe = 4,48.10^{-7}$. A aproximação gaussiana é exata somente nas proximidades do ponto (γ_{WG}) de máximo da distribuição WMC e menos exata nas caudas da distribuição. Em geral, a aproximação gaussiana sub-avalia a sensibilidade máxima e o valor de limiar ótimo do receptor enquanto super-avalia o ganho ótimo de avalanche. A aproximação gaussiana é amplamente usada na modelagem de sistemas ópticos com detector APD apresentando precisão de resultados aceitável. Pelo fato de sub-avaliar a sensibilidade do receptor (menor que a real sensibilidade do receptor obtida a partir do limitar ótimo) a aproximação gaussiana é considerada uma forma conservativa de estimar o desempenho do receptor.

5.3 Sistema Usando Código (F, K, 1, 1) - OOC

Na análise de desempenho do modelo de receptor da Figura 5.5, consideramos o ruído balístico, o ruído térmico, as correntes de fuga de superfície e de fuga de volume do APD. Os códigos (F, K, 1, 1)-OOC propostos No Capítulo 4 são usados como seqüências de espalhamento do sinal de informação. Para análise, adotamos que os chips estão sincronizados entre os diferentes usuários, posto ser o pior caso e resultar no limitante superior do desempenho [74].

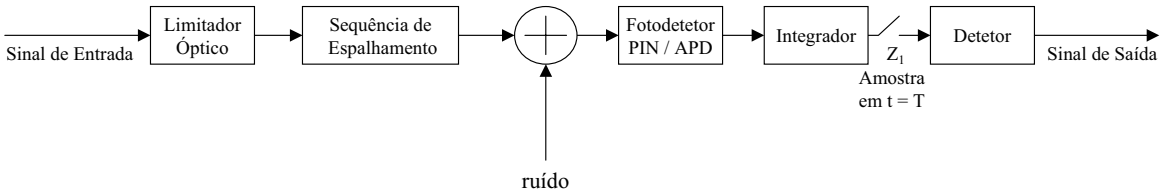


Figura 5.5: Modelo do Receptor Óptico de Correlação usado nos Sistema OCDMA.

A detecção óptica do sinal é um processo estocástico de efeito acumulativo na saída do APD em cada intervalo entre os chips, que pode ser modelado por uma variável aleatória gaussiana [103]. A intensidade do sinal detetado, no intervalo de duração do chip, T_c, pode ser modelado por um processo pontual de Poisson (*Poisson point process*). O número médio de fótons absorvidos, no intervalo de duração do chip, T_c, é igual a $\lambda_s T_c$, e a probabilidade do número médio de fótons que incide no APD é determinada através da distribuição representada pela equação (2.39). Quando um chip "1" da seqüência do usuário desejado é transmitido a taxa de fótons absorvidos é dada por:

$$\lambda_s = \frac{\eta P}{hf} \tag{5.19}$$

onde P é a potência óptica recebida, η é a eficiência do APD f é a freqüência óptica do sinal, $h = 6.626 \times 10^{-34}$ *J.s* é a constante de Planck. No fotodetector APD os pares elétron-lacuna

sujeitos ao processo de avalanche resultam em m elétrons na saída do APD, em resposta à média λT_c de fótons incidentes. A densidade de probabilidade condicional de m elétrons, na saída do APD, dado ter incidida a média λT_c de fótons primários, é caracterizada pela distribuição de Conradi [104]-[105], onde

$$\lambda = \begin{cases} \lambda_s + \lambda_b + I_b/q & \text{para o chip "1"} \\ \lambda_s/M_e + \lambda_b + I_b/q & \text{para o chip "0"} \end{cases} \tag{5.20}$$

é a taxa de absorção total de fótons causada pelos fatores limitantes da fotodetecção (emissão espúria, corrente de fuga de volume "*bulk leakage current*" do APD); λ_b é a taxa de absorção causada pela emissão espúria; $q = 1,602.10^{-19}C$ é a carga elétron; M_e é a razão de extinção e I_b/q representa a contribuição da corrente de fuga de volume do APD.

O limitador óptico é definido pela seguinte função [74]:

$$g(y) = \begin{cases} v_f, & y \geq T_h = K\lambda_s T_c \\ 0, & 0 \leq y \leq T_h = K\lambda_s T_c \end{cases} \tag{5.21}$$

onde y é a taxa de potência óptica na entrada do limitador e Th é o limiar que pode ser fixado em um valor desejado. Se a intensidade do sinal óptico for $y \geq K\lambda_s T_c$, o limitador óptico grampeia o sinal em $K\lambda_s T_c$ e, caso a intensidade óptica seja $y \leq K\lambda_s T_c$, a saída do limitador é zero. Este comportamento não linear do limitador melhora o desempenho do sistema devido ao fato de excluir algumas combinações do vetor de estado das interferências que originariam erros por meio do aumento da variável de decisão, Z_1, a um valor superior ao valor de limiar, γ.

Cada usuário está igualmente sujeito à interferência de qualquer dos K chips do código, independente dos demais usuários. Seja $\mathbf{k}$ o vetor ($\mathbf{k} \equiv k_1, k_2, k_3, ..., k_K$) de estado das interferências dos K chips. Este vetor possui $|\mathbf{k}|$ elementos diferentes de zero. Duas palavras-código OOC se sobrepõem em, no máximo, um pulso. Considerando que cada um dos usuários interfere somente com um pulso, vão ser formados diversos arranjos de interferências. Estes arranjos compõem o vetor de estado das interferências $\mathbf{k}$, dado pela seguinte expressão:

$$I_1 = \sum_{i=1}^{K} k_i(I_1), \qquad \text{onde} \qquad k_1(I_1) \in \{0, 1, 2, ..., I_1\} \tag{5.22}$$

Assim, I_1 é a soma dos k_i chips que interferem sobre cada um dos chips do usuário desejado, k_i representa o números de pulsos detetados no receptor que interferem no sinal desejado e o vetor $\mathbf{k}$ representa as interferências no receptor.

Existem K^2 possibilidades de combinar em pares os K chips que constituem o peso do código, de modo que a probabilidade do pulso de um usuário, que interfere no sinal desejado, sobrepor-se a um pulso do usuário desejado é $p = K^2/2F$, onde $1/2$ representa a probabilidade do usuário transmitir o bit "$b = 1$". O número de usuários que interfere com o desejado possui distribuição binomial, com parâmetros $N - 1$ e p. Logo, a probabilidade de I_1 usuários interferirem, antes do limitador óptico, considerando o sincronismo de chips,

é dada pela expressão:

$$p_{I_1}(I_1) = \sum_{i=0}^{N-1} \left(\begin{array}{c} N-1 \\ i \end{array} \right) p^i (1-p)^{N-1-i} \delta(I_1 - i) \tag{5.23}$$

onde $\delta(x)$ é a função delta de Dirac. Portanto, o desempenho do sistema com limitador óptico, Figura 5.5, depende de $|\mathbf{k}|$ e I_1.

Para um determinado número I_1 de usuários que interferem, existe um conjunto de vetores F_{I_1}, e suas respectivas permutações, que satisfazem a equação (5.22). Este conjunto pode ser representado pela expressão:

$$F_{I_1} = \left\{ \mathbf{k} \ : \ \sum_{i=0}^{K} k_1(I_1) = I_1, \quad k_1(I_1) \in \{0, 1, 2, ..., I_1\} \right\} \tag{5.24}$$

O conjunto F_{I_1} possui cardinalidade dada por

$$|F_{I_1}| = \left(\begin{array}{c} I_1 + K - 1 \\ I_1 \end{array} \right) \tag{5.25}$$

vetores. Como os I_1 usuários que interferem são distintos, podem ser combinados em K^{I_1} arranjos de interferências. Adotando isso, o vetor de estados das interferências, $\mathbf{k}$, pode se apresentar nas distintas permutações, iguais a:

$$\left(\begin{array}{c} I_1 \\ k_1, k_2, k_3, ..., k_K \end{array} \right) = \left(\begin{array}{c} I_1 \\ k_1 \end{array} \right) \left(\begin{array}{c} I_1 - k_1 \\ k_2 \end{array} \right) \left(\begin{array}{c} I_1 - (k_1 + k_2) \\ k_3 \end{array} \right) ... \left(\begin{array}{c} k_K \\ k_K \end{array} \right) = \frac{I_1!}{\prod_{i=1}^{K} k_i!} \tag{5.26}$$

cada uma com probabilidade $Pr(I_1) = 1/K^{I_1}$.

Considerando a probabilidade de erro para um dado vetor de estado das interferências, $P(\mathbf{k};F_{I_1})$, a probabilidade de erro:

$$Pe = \sum_{I_1=0}^{N-1} Pr(I_1) P_E(\mathbf{k};F_{I_1}) \tag{5.27}$$

onde $Pr(I_1)$ é determinado através da expressão (5.23); $P(\mathbf{k};F_{I_1})$ é a probabilidade de que o vetor $\mathbf{k} \in F_{I_1}$.

O vetor $\mathbf{k}$, que pertence ao conjunto F_{I_1}, é um vetor de estados com I_1 usuários, cada um contribuindo com um pulso interferente. Cada usuário possui igual probabilidade de interferir com um pulso, independentemente dos demais usuários. Como decorrência, o vetor $\mathbf{k}$ possui uma distribuição dada pela expressão:

$$P(\mathbf{k};F_{I_1}) = \frac{1}{K^{I_i}} \frac{I_1!}{\prod_{i=1}^{K} (k_i)!} \tag{5.28}$$

Quando o sinal óptico incide sobre o limitador óptico, todos os K pulsos são igualmente prováveis de serem detetados pelo receptor. Este apenas contabiliza as posições ocupadas

pelos pulsos, de modo que quaisquer dois vetores de estados de interferências, que são permutações um do outro, vão possuir a mesma probabilidade, $P_E(\mathbf{k}) = P_E(\beta)$. Assim, o número de vetores que devem ser considerados para determinar a probabilidade de erro pode ser apenas representado por um conjunto de vetores que contenha todas as permutações das interferências, ou seja, pode definir-se esse conjunto de permutações como:

$$G_{I_1} = \left\{ \mathbf{k} \ : \ I_1 = \sum_{i=1}^{K} k_1(I_1), \quad k_1 \geq k_1 \geq k_2 \geq, ..., \geq k_K \geq 0 \right\} \tag{5.29}$$

Logo, a probabilidade do vetor $\mathbf{k}$, considerando as suas permutações contidas no conjunto G_{I_1}, é dada por:

$$P(\mathbf{k};G_{I_1}) = \sum_{\beta \in \prod(\mathbf{k})}^{K} P(\beta;F_{I_1}) = NDP(\mathbf{k})P(\mathbf{k};F_{I_1}) \tag{5.30}$$

onde $\prod(\mathbf{k})$ é o conjunto de todas as permutações do vetor $\mathbf{k}$. Caso todos os elementos de $\mathbf{k}$ sejam distintos, o número de permutações é igual a $K!$, quando algum elemento de $\mathbf{k}$ se repete $R(k_i)$ vezes no vetor, então, toda distinta permutação possui $R(k_i)!$ versões. Logo, o total de distintas permutações do vetor $\mathbf{k}$, no conjunto G_{I_1}, é dado pela expressão

$$NDP(\mathbf{k}) = \frac{K!}{\prod_i R(k_i)!}; \tag{5.31}$$

onde $R(k_i)$ é o número de vezes que o elemento k_i aparece no vetor $\mathbf{k}$ e a produtora $\prod_i$ é feita sobre os índices i para os quais k_i são diferentes.

Vamos adotar que todo usuário é eqüiprovável de ser interferido em um dos K chips pelos demais usuários do sistema. O vetor de estado das interferências $\mathbf{k}$ possui distribuição multinomial [75]-[76]. A probabilidade do vetor $\mathbf{k}$ possuir $|\mathbf{k}| = 0, 1, 2, ..., \min(K, I_1)$ elementos diferentes de zero é dada pela expressão:

$$\Pr(|\mathbf{k}| = m|I_1) = \sum_{\substack{\mathbf{k} \in G_{I_1} \\ |\mathbf{k}|=m}} NDP(\mathbf{k})P(\mathbf{k};F_{I_1}) \tag{5.32}$$

onde F_{I_1} é um arranjo de vetores dos estados de interferências com peso total igual a I_1. O arranjo G_{I_1} inclui todos os vetores de interferências, dispostos em ordem decrescente, que representam os vetores contidos em F_{I_1}.

Quando o bit "1" é transmitido, $K\lambda_s$ fótons incidentes são somados sobre o último chip, porque a potência do sinal é igual ou maior que a potência (P) emitida pelo laser, anulando o efeito do limitador óptico. Além disso, são adicionadas, sobre o último chip, as correntes de fuga de volume e de superfície do APD e o ruído térmico. Assim, a densidade de probabilidade condicional da variável de decisão do usuário 1, considerando I_1, é expressa por:

$$p_{Z_1}(z_1|I_1, b = 1) = \frac{1}{\sqrt{2\pi}\sigma_{b_1}} \exp\left[-\frac{(z_1 - E_{b_1})^2}{2\sigma_{b_1}^2} \right]. \tag{5.33}$$

A média e variância estatísticas de Z_1 são, respectivamente, dadas pelas seguintes expressões:

$$\begin{aligned} E_{b_1} &= \mathbf{E}\{z_1|I_1, b=1\} = GT_cK\lambda_s + GT_cI_b/q + T_cI_s/q = GT_c\left[K\lambda_s + I_b/q\right] + T_cI_s/q \\ \sigma^2_{b_1} &= \mathbf{E}\{z_1^2 - E^2_{b_1}|I_1, b=1\} + \sigma^2_{th} = G^2F_eT_cK\lambda_s + G^2F_eT_cI_b/q + T_cI_s/q + \sigma^2_{th} \\ &= G^2F_eT_c\left[K\lambda_s + I_b/q\right] + T_cI_s/q + \sigma^2_{th} \end{aligned} \tag{5.34}$$

onde $\sigma^2_{th} = \left(2k_BT_rT_c\right)/\left(q^2R_L\right)$ é a variância do ruído térmico do receptor, e F_e dado pela Expressão (5.10), $\frac{I_b}{q}T_c$ é a corrente de fuga de volume (*bulk leakage current*).

Portanto, na saída do receptor, para o usuário desejado, tem-se o efeito acumulativo dos $K\lambda_s$ fótons incidentes sobre o APD, no intervalo de duração do último chip, considerando os fatores limitantes como a corrente de fuga de volume, a corrente de fuga de superfície e o ruído térmico do APD. Logo, seguindo os procedimentos apresentados na Seção 2.6, a probabilidade de erro condicional, dado que o bit "1" foi transmitido, é expressa por:

$$\begin{aligned} Pr(Z_1 \leq \gamma|I_1 = j, b=1) &= \int_{-\infty}^{\gamma} p_{Z_1}(z_1|I_1, b=1)p_{I_1}(I_1)dz_1 \\ &= \int_{-\infty}^{\gamma} \frac{1}{\sqrt{2\pi}\sigma_{b_1}}\exp\left[-\frac{(z_1 - E_{b_1})^2}{2\sigma^2_{b_1}}\right]p_{I_1}(I_1)dz_1 \\ &= \sum_{j=0}^{N-1}\left(1 - Q\left(\frac{\gamma - E_{b_1}}{\sigma_{b_1}}\right)\right)p_{I_1}(j); \end{aligned} \tag{5.35}$$

Quando o bit "0" é transmitido, o limitador óptico grampeia o sinal óptico do receptor. Considerando a razão de extinção (M_e) do laser, os bits "0" dos N usuários contribuem com potência NP/M_e no k^-ésimo chip do sinal do usuário desejado, que pode ser maior que a potência (P) do chip emitido pelo laser, quando $N > M_e$. Neste caso, o limitador grampeia a intensidade do sinal no valor da potência (P) do chip emitido pelo laser. Caso contrário, o limitador grampeia no valor zero. Assim, o comportamento do limitador pode ser descrito pela seguinte função

$$i_{Me} = \begin{cases} 1, & N \geq M_e \\ 0, & N < M_e \end{cases} \tag{5.36}$$

Para $|\mathbf{k}| = 0$, $K.i_{Me}$ chips incidem no APD com taxa de fótons igual a λ_s. Para $|\mathbf{k}| = m > 0$, $(K-m).i_{Me} + m$ chips incidem com taxa de fótons igual a λ_s. Logo, considerando I_1, a densidade de probabilidade condicional da variável de decisão Z_1, é dada pela expressão

$$p_{Z_1}(z_1|I_1, b=0) = \frac{1}{\sqrt{2\pi}\sigma_{b_0}(|\mathbf{k}|)}\exp\left[-\frac{(z_1 - E_{b_0}(|\mathbf{k}|))^2}{2\sigma^2_{b_0}(|\mathbf{k}|)}\right]; \tag{5.37}$$

A média e variância estatísticas são, respectivamente, dadas pelas seguintes expressões

$E_{b_0}(|\mathbf{k}|) = \mathbf{E}\{z_1|I_1, b=0\} = GT_c\left[|\mathbf{k}|\lambda_s + (K - |\mathbf{k}|)i_{Me}\lambda_s + I_b/q\right] + T_cI_s/q,$
$\sigma^2_{b_0}(|\mathbf{k}|) = \mathbf{E}\{z_1^2 - E^2_{b_0}|I_1, b=0\} + \sigma^2_{th} = G^2F_eT_c\left[|\mathbf{k}|\lambda_s + (K - |\mathbf{k}|)i_{Me}\lambda_s + I_b/q\right] + T_cI_s/q + \sigma^2_{th}.$

Assim, a probabilidade de erro condicional, dado que o bit "0" foi transmitido, é expressa por:

$$
\begin{aligned}
Pr(Z_1 > \gamma | I_1 = j,\ |\mathbf{k}| = m,\ b = 0) = \\
&= Pr(Z_1 > \gamma | I_1 = 0,\ |\mathbf{k}| = 0,\ b = 0) p_{I_1}(0) \\
&+ \sum_{j=1}^{N-1} Pr(Z_1 > \gamma | I_1 = j,\ |\mathbf{k}| = m > 0,\ b = 0) pI_1(j) \\
&= \int_{\gamma}^{\infty} p_{Z_1}(z_1 | I_1 = 0,\ |\mathbf{k}| = 0,\ b = 0) p_{I_1}(0) dz_1 \\
&+ \sum_{j=1}^{N-1} \sum_{m=1}^{\min(K,I_1)} \int_{\gamma}^{\infty} p_{Z_1}(z_1 | I_1 = j,\ |\mathbf{k}| = m > 0,\ b = 0) \\
&\qquad p_{I_1}(j) Pr(|\mathbf{k}| = m \,|\, I_1 = j) dz_1 \\
&= \int_{\gamma}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_{b_0}(0)} \exp\left[-\frac{(z_1 - E_{b_0}(0))^2}{2\sigma_{b_0}^2(0)} \right] p_{I_1}(0) dz_1 \\
&+ \sum_{j=1}^{N-1} \sum_{m=1}^{\min(K,I_1)} \int_{\gamma}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_{b_0}(m)} \exp\left[-\frac{(z_1 - E_{b_0}(m))^2}{2\sigma_{b_0}^2(m)} \right] \\
&\qquad p_{I_1}(j) Pr(|\mathbf{k}| = m \,|\, I_1 = j) dz_1 \\
&= Q\left(\frac{\gamma - E_{b_0}(0)}{\sigma_{b_0}(0)} \right) p_{I_1}(0) \\
&+ \sum_{j=1}^{N-1} \sum_{m=1}^{\min(K,I_1)} Q\left(\frac{\gamma - E_{b_0}(m)}{\sigma_{b_0}(m)} \right) p_{I_1}(j) \Pr(|\mathbf{k}| = m \,|\, I_1 = j);
\end{aligned}
\tag{5.38}
$$

obtida de modo similar à equação (5.35), onde a $pI_1(j)$ é a probabilidade dada pela equação (5.23).

Finalmente, a probabilidade de erro do sistema é dada pela expressão:

$$
P_b = \frac{1}{2} Pr(Z_1 > \gamma_{opt} | I_1 = j,\ |\mathbf{k}| = m,\ b = 0) + \frac{1}{2} Pr(Z_1 \leq \gamma_{opt} | I_1 = j,\ b = 1) \tag{5.39}
$$

onde γ_{opt} é o limiar ótimo do receptor, que minimiza a probabilidade de erro total, obtido seguindo o procedimento apresentado na Seção (2.6). Devido ao fato do valor de limiar depender da potência óptica, do peso da palavra-código e do número de usuários simultâneos do sistema, o valor de limiar, determinado pela Equação (A.9) acaba sendo sub-ótimo, posto que é derivada somente em relação a γ. O valor de limiar ótimo é encontrado a partir da mesma Equação (A.9), através de simulação numérica exaustiva, considerando os parâmetros, quais sejam, potência óptica, comprimento e peso do código. Usando os parâmetros da Tabela 5.1, a Figura 5.6 ilustra os valores do limiar ótimo em função da potência óptica (P), com OOC de peso K = 10, comprimento F = 1000 e N = 10 usuários.

A Figura 5.6 ilustra como o limiar ótimo, que minimiza a probabilidade de erro do sistema, aumenta à medida que a potência ($dBW = 10.log_{10}(\frac{\text{Potência em Watts}}{1\text{ Watt}})$) da fonte óptica

Tabela 5.1: Parâmetros de simulação.

Designação	Símbolo	Valor Nominal
Velocidade da luz no vácuo	c	3.10^8 m/s
Eficiência Quântica	η	0,6
Ganho do APD	G	100
Razão de ionização efetiva	k_{eff}	0,02
Corrente de fuga de volume do APD	I_b	0,1 nA
Corrente de fuga de superfície do APD	I_s	10 nA
Taxa de fótons	λ_b	10^9 fótons/s
Razão de extinção	M_e	100
Taxa de bits	R_b	30 Mbit/s
Temperatura equivalente de ruído	T_r	1100 K
Resistor de carga	R_L	1030 Ω

aumenta, devido ao aumento do número médio de fótons recebido. O desempenho do sistema melhora quando o valor de limiar se aproxima do ponto ótimo a partir do limiar de menor valor. Este fenômeno, para altos valores da potência recebida, se deve ao fato do ruído térmico, a emissão óptica espúria e as correntes de fuga do APD serem desprezíveis e conseqüentemente o desempenho torna-se somente sensível ao MAI. Por outro lado, para

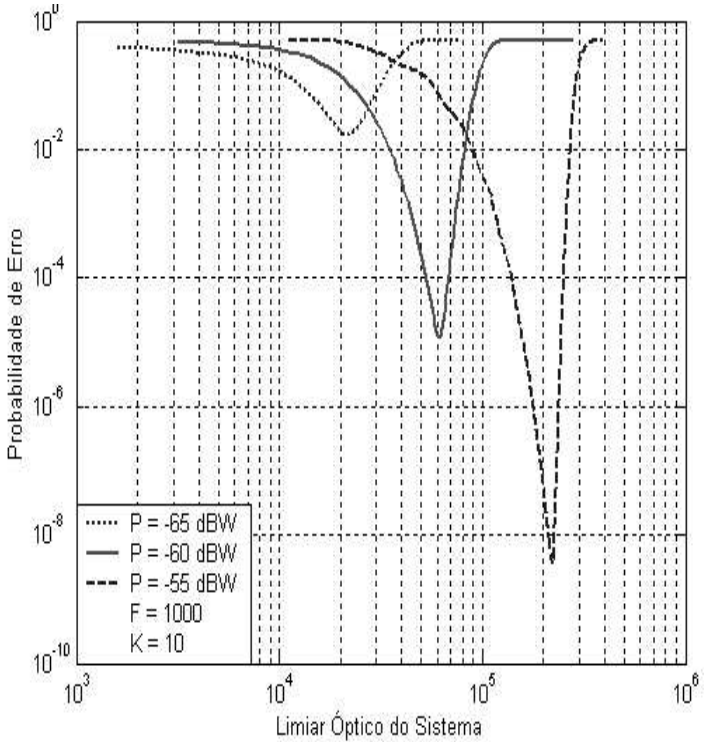


Figura 5.6: Limiar óptico do sistema sem limitador usando um código OOC "genérico."

baixas potências, estes fatores limitantes da fotodetecção não são desprezíveis e afetam a curva de desempenho de forma a torná-la mais suave, à medida que varia o limiar. Finalmente, o desempenho se aproxima do valor $0,5$ depois do ponto de limiar ótimo à medida que este aumenta. Isto, devido ao fato de ocorrer erro quando o bit "1" é transmitido, e não ocorrer quando o bit "0" é transmitido porque o valor de limiar de decisão é alto.

A Figura 5.7 ilustra o desempenho versus a potência óptica recebida, tendo por parâmetro o número de usuários no sistema. Para esta análise, foram usados os mesmos parâmetros do código "genérico" (F=1000, K=10), dados pela Expressão (2.20). A figura ilustra uma piora de desempenho do sistema com aumento do número de usuários, principalmente, devido a redução do peso (K) do código com objetivo de manter a ortogonalidade das seqüências de espalhamento. A potência óptica recebida em cada chip é considerada constante, logo o

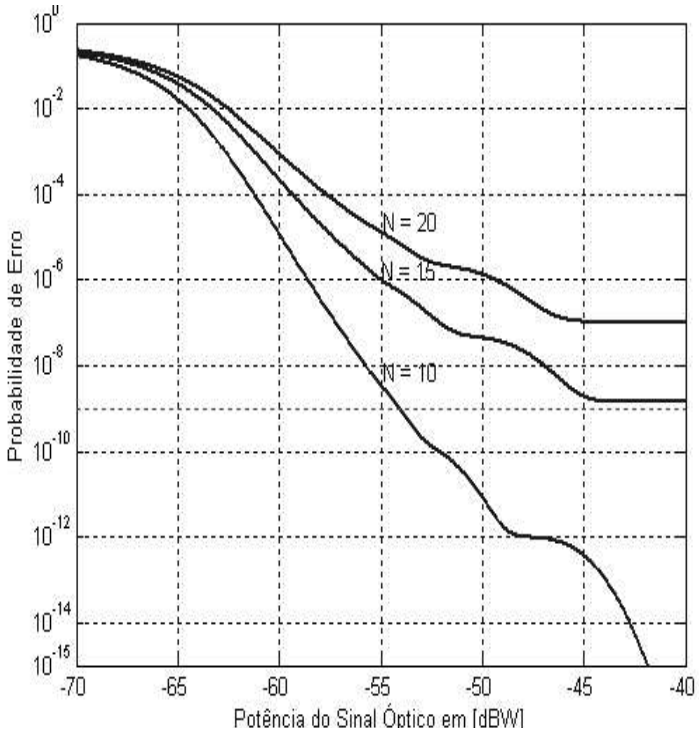


Figura 5.7: Desempenho do sistema sem limitador usando um código "genérico" versus potência do sinal óptico.

total de fótons recebidos (energia óptica recebida) no receptor desejado decresce, causando a degradação de desempenho do sistema com aumento do número de usuários. A outra razão reside no peso total $N.K$ dos códigos aumentar, elevando a contribuição total negativa da interferência nas estatísticas da variável de decisão, quando mais usuários partilham o canal. Uma segunda justificativa é a de que um código de F = 1000 é melhor que um código de F = 2000 quando o número de usuários é menor que 5 e pior para o caso contrário. Em geral, a duração do chip é $T_c = T/F$, e o número médio de fótons recebidos (energia) por chip decresce com aumento de F, para potência constante. Porém, pode-se aumentar o peso do código com aumento de F, sendo necessário um compromisso entre N, K e F para melhor

desempenho do sistema em dada potência da fonte óptica.

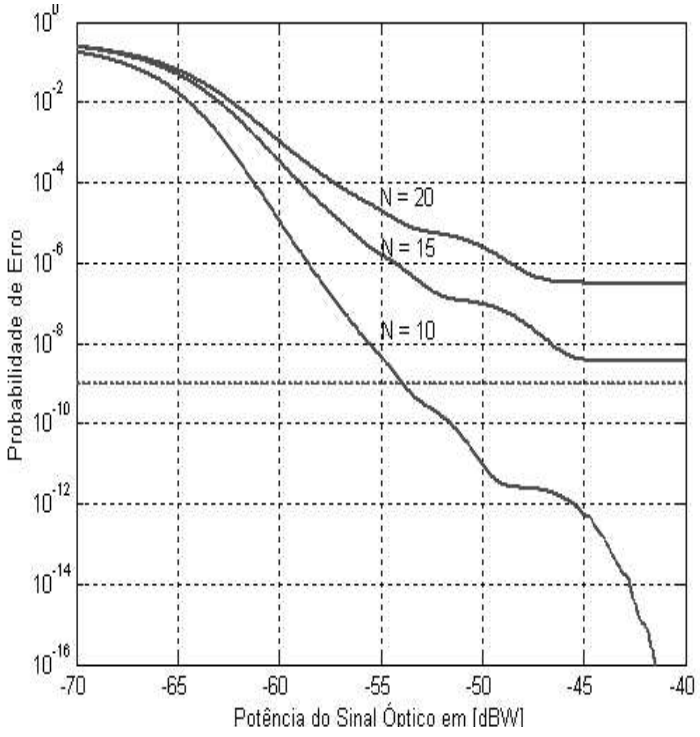


Figura 5.8: Desempenho do Sistema com limitador usando um código "genérico" versus potência do sinal óptico.

A Figura 5.8 ilustra o desempenho do sistema com limitador óptico. Em geral, o desempenho do sistema com limitador óptico pode ser superior a duas vezes o desempenho do sistema sem limitador óptico. Comparando as Figuras 5.7 e 5.8 confirma-se que o desempenho do sistema com limitador óptico, Figura (5.8), é ligeiramente melhor que o desempenho do sistema sem limitador óptico, ilustrado na Figura 5.7.

Em geral, para K máximo do código (com F e N fixos), segundo a Equação (2.20), a melhora de desempenho decorrente da aplicação do limitador óptico, para um enlace óptico não ideal, não é significativa. Eis as razões: o desempenho de ambos sistemas, ideal ou não ideal, não depende da interferência total I_1, ou seja, quando o bit "1" é transmitido o valor final da variável de decisão Z_1, Equação (5.4), é discreto. Quando o bit "0" é transmitido, usando o limiar de decisão entre $K-1$ e K, pode-se eliminar completamente a contribuição da interferência total no período de correlação, exceto para os casos em que todas as durações dos K chips coincidem para os N-1 usuários do sistema ideal.

Porém, no sistema não ideal, o valor da variável de decisão não é discreto e a contribuição total da interferência no período de correlação não é completamente eliminada, mesmo usando o valor limiar ótimo, devido à presença de fatores limitantes da fotodetecção. Uma segunda razão consiste no desempenho do limitador óptico aplicado ao receptor não ideal, poder ser igual a $0,5$, caso o número de usuários $N \geq M_e$ nos bit "1" ou bit "0". A contribuição dos chips "0" dos N usuários para toda $k-$ *ésima* duração de chip "1" do sinal

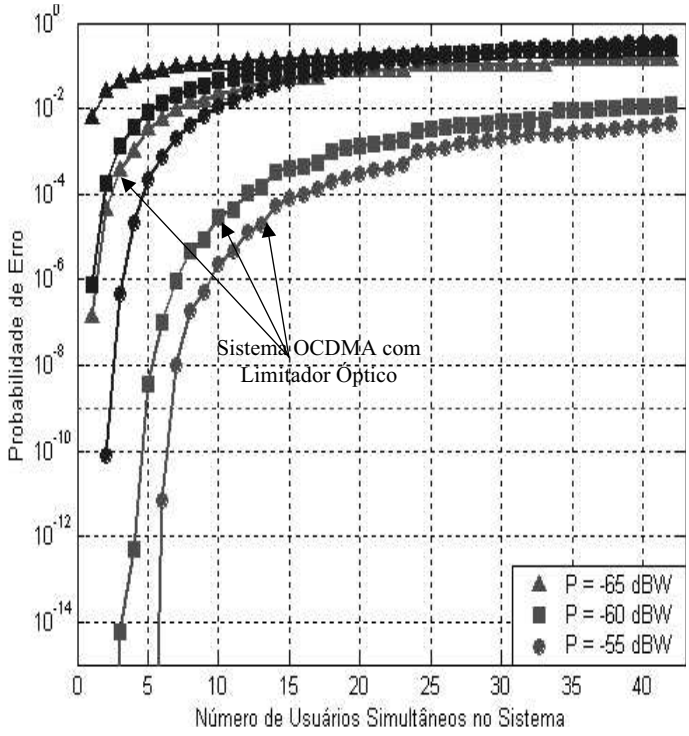


Figura 5.9: Desempenho do sistema com e sem limitador versus número de usuários.

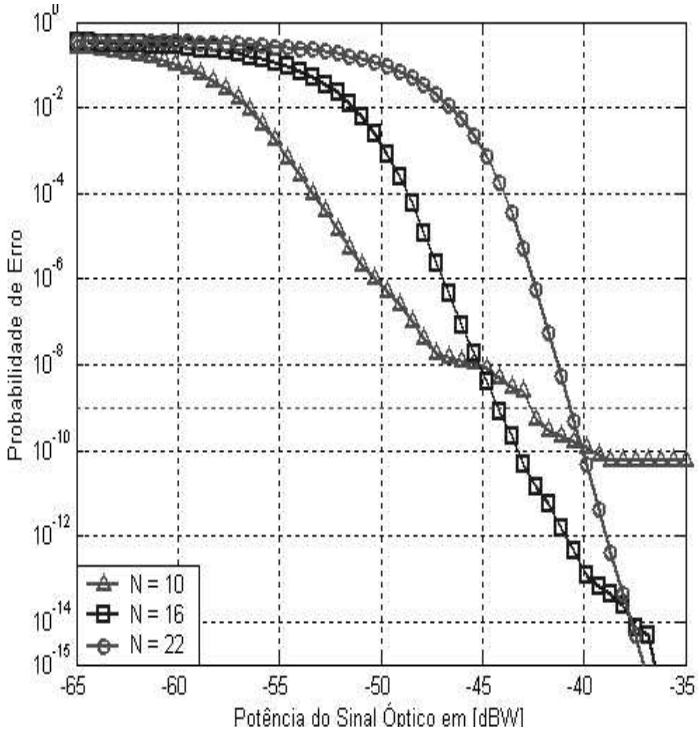


Figura 5.10: Desempenho do sistema com limitador óptico, usando o código (N,F,1,1)proposto, versus potência do sinal óptico.

do usuário desejado é maior ou igual a amplitude unitária da potência da fonte óptica, para $k = 1, 2, 3, ..., K$. Assim, K chips "1" depois do limitador óptico incidem no fotodetector

APD com taxa de fótons incidentes igual a Equação (5.21) quando os bits "1" ou bits "0" são transmitidos, e o valor final da variável de decisão Z_1 não varia.

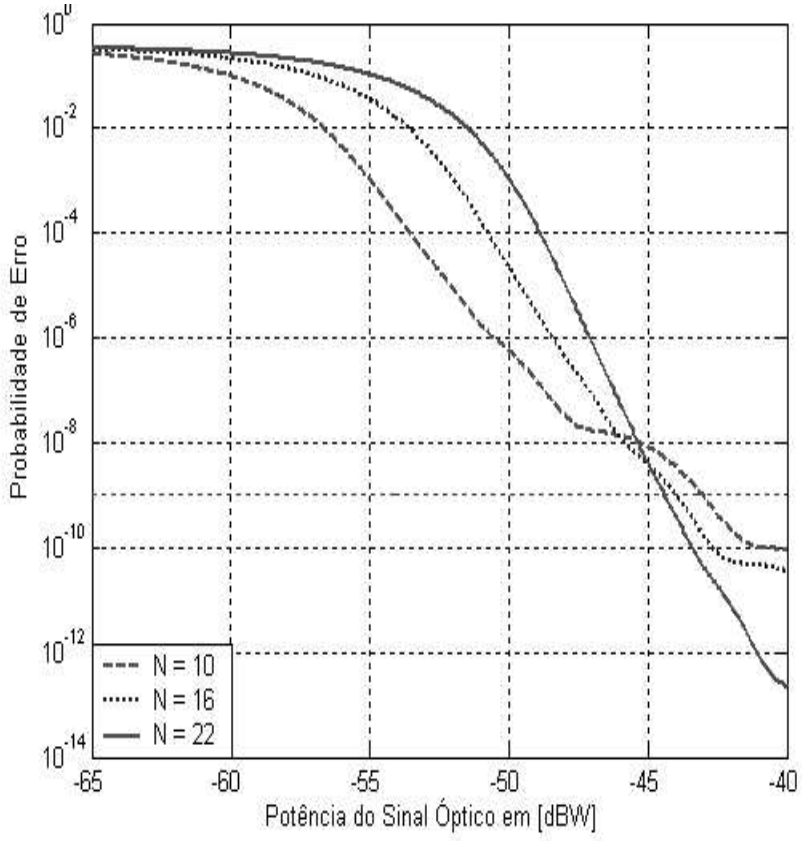


Figura 5.11: Desempenho do sistema sem limitador, usando o código proposto (N,F,1,1), versus potência do sinal óptico.

A Figura 5.9 ilustra a relação entre o desempenho e o número de usuário simultâneos para diferentes potências em sistemas com e sem limitador óptico. Como esperado, para uma dada potência (P), o desempenho dos sistemas se degrada quando o número de usuários simultâneos aumenta. Por outro lado, para um dado número de usuários simultâneos, o desempenho melhora com o aumento da potência. Portanto, existe um compromisso entre o número de usuários simultâneos e a potência óptica recebida. Por exemplo, para um sistema com limitador óptico, é necessária uma potência igual a $-60\ dBW$ para que 5 usuários simultâneos sejam acomodados com desempenho de 10^{-9}. Porém, quando se aumenta o número de usuários simultâneos a 6, para se manter o desempenho do sistema é necessário aumentar a potência para $-55\ dBW$. Portanto, o aumento de um usuário no sistema exige um compromisso de aumento da potência em cerca de 5 dB, pode-se também considerar a seguinte conversão de unidades $dBW = dBm - 30$. A figura confirma ainda, como esperado, para valores fixos de potência e número de usuários simultâneos o sistema com limitador óptico possui melhor desempenho comparado ao sistema sem limitador óptico.

A Figura 5.10 ilustra o desempenho do sistema com limitador óptico versus potência do sinal óptico recebido usando o código $(F, K, 1, 1) - OOC$ proposto no Capítulo 3. Para

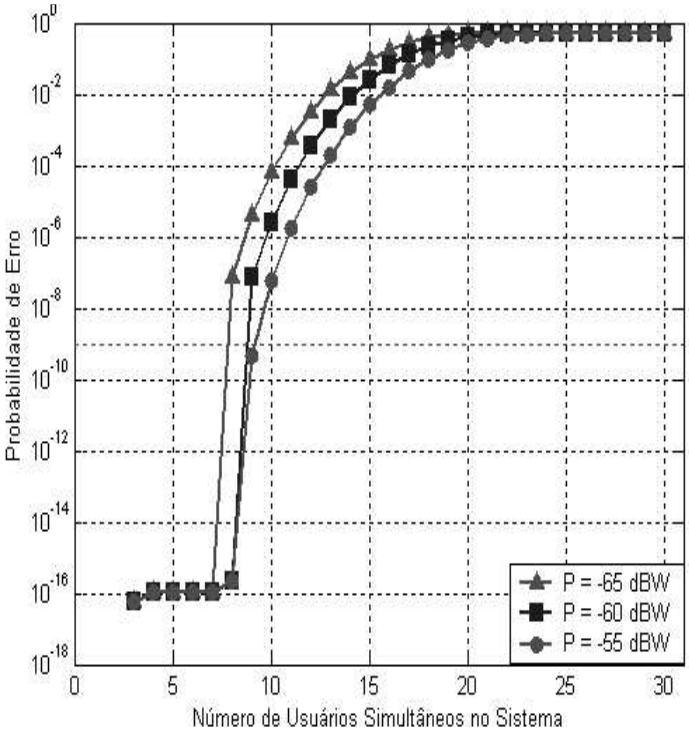


Figura 5.12: Desempenho do sistema sem limitador, usando o código proposto (N,F,1,1), versus número de usuários.

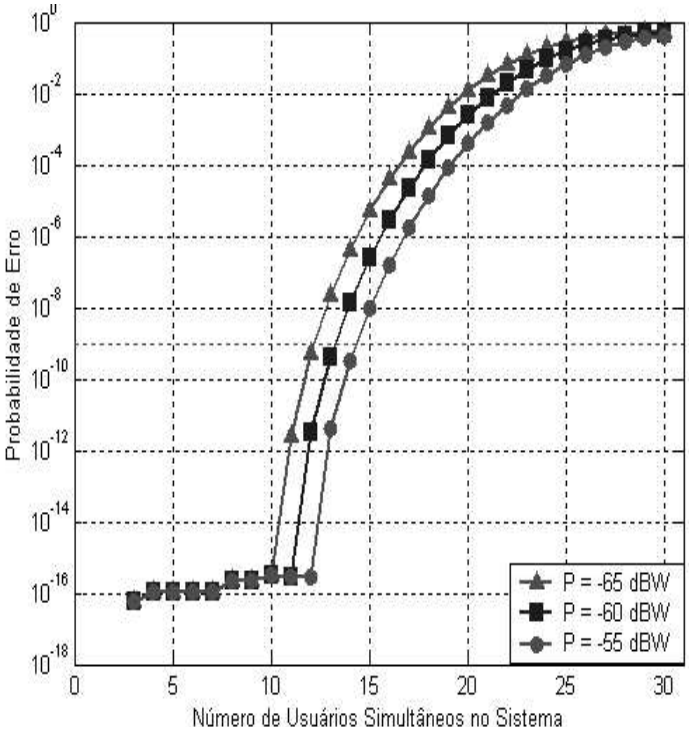


Figura 5.13: Desempenho do sistema com limitador, usando o código proposto (N,F,1,1), versus número de usuários.

avaliação de desempenho foram usados os seguintes parâmetros: N = 10 para $(3180, 5, 1, 1) - OOC$, N = 16 para $(19344, 8, 1, 1) - OOC$ e N = 20 para $(79332, 11, 1, 1) - OOC$ com valores de limiar ótimo obtidos de forma numérica recursiva. As conclusões retiradas da Figura 5.10 são similares às conclusões apresentas para a Figura 5.8.

Comparando ambas figuras, torna-se claro que para número de usuários $N \leq 10$ o desempenho do sistema com o código proposto é inferior ao da Figura 5.8, e esta relação se inverte para $N \geq 10$, sendo melhor o desempenho do sistema usando o código proposto. Este fato deve-se as seguintes causas: da Expressão (2.17) decorre a necessidade do compromisso entre N, K, e F para conseguir o melhor desempenho, para uma dada potência da fonte óptica. Este compromisso ficou salvaguardado na construção do código (F,K,1,1)-OOC proposto no Capítulo 3. Por outro lado, a análise de desempenho ilustrada na Figura 5.8 é feita usando-se um código OOC "genérico" (cujos parâmetros decorrem da Equação (2.20)). A segunda razão decorre do código proposto possuir comprimento maior que o código usado na Figura 5.8. Logo, pelo teorema do limite central, para pequenos valores $N \leq 10$ a aproximação gaussiana é imprecisa, apresentando baixo desempenho do sistema usando o código proposto.

A Figura 5.11 foi obtida nas mesmas condições da Figura 5.10 exceto o fato de que não possui limitador óptico. Quando comparadas, a Figura 5.11 confirma o seu desempenho ser ligeiramente inferior ao sistema com limitador óptico.

No sistema OCDMA, o MAI é o principal fator de degradação de desempenho, gerando um assintótico patamar de erro. A aplicação de um limitador óptico ao sistema é um método efetivo de melhoramento do desempenho, pois o limitador reduz o efeito do MAI gerada da combinação de vários arranjos de interferências, que tornam a variável de decisão Z_1 maior que o limiar ótimo. Portanto, o desempenho do sistema sem limitador óptico, em geral, depende fundamentalmente do arranjo de interferência I_1, e para o caso do sistema com limitador óptico o desempenho depende de I_1 e do número de elementos não zeros no arranjo de interferências $|\mathbf{k}|$.

As conclusões relativas à análise da Figura 5.12 são similares às apresentadas para a Figura 5.13. As considerações a respeito do compromisso entre desempenho, potência e número de usuários simultâneos continuam válidas para este caso. Na Figura 5.13, para o número de usuários inferior a 9, o desempenho em diferentes potências, é praticamente o mesmo. Isto se deve ao fato da aproximação gaussiana, segundo o teorema de limite central para baixos valores de N, apresentar valores pouco exatos.

Capítulo 6

Conclusões e Sugestões para Trabalhos Futuros

6.1 Conclusões

Os códigos OOC já publicados são caracterizados por suas boas propriedades de autocorrelação e correlação cruzada, porém a construção desses códigos através de métodos interativo, geometria projetiva e técnicas combinatórias, é complexa e conseqüentemente a única forma de implementar reside em usar recursos computacionais de alta memória para armazenar esses códigos.

O trabalho de tese apresentado alcança os objetivos a que se propôs. Três *novas famílias de códigos ortogonais ópticos* do tipo congruentes foram apresentadas para aplicação em sistemas assíncronos OCDMA. Estes códigos asseguram $p-1$ diferentes palavras-código correspondentes a p usuários no sistema OCDMA, para todo número primo p. As famílias de códigos foram demonstradas serem do tipo $(p(2p-1),\ p,\ 1,\ 2)-OOC$, $((p-1)(2p-1),\ p-1,\ 1,\ 2)-OOC$ e $(F,\ K,\ 1,\ 1)-OOC$, e, conseqüentemente, possuem propriedades de autocorrelação e correlação cruzada ideal e não ideal, respectivamente. Os códigos propostos possuem estrutura algébrica não complexa e são de simples construção e requerem baixa memória computacional para serem implementados. Devido às propriedades dos códigos propostos, o seu desempenho é melhor comparado ao desempenho de códigos conhecidos na literatura técnica sob as condições do mesmo comprimento do código F, o mesmo peso do código K e o mesmo número de usuários N.

A aplicação de equações diofantinas à construção de códigos ortogonais ópticos sem recorrer a complexos algoritmos para resolver estas equações possibilita que através de relações de congruência possam ser encontradas novas famílias de códigos ópticos a partir de um conhecimento da teoria dos números.

O desempenho dos códigos foi avaliado em termos da probabilidade de erro (BER). Na avaliação, foram consideradas as situações em que o receptor de um limitador óptico com detector APD está sob os efeitos de diversos fatores de degradação do desempenho do receptor, considerando uma transmissão assíncrona do sinal e detecção síncrona dos chips. A análise

de desempenho foi apresentada para os códigos propostos e mostrou que: a probabilidade de erro do sistema OCDMA diminui com aumento do limiar de detecção do receptor; a probabilidade de erro do sistema OCDMA diminui com aumento do peso (K) e comprimento (F) do código.

O desempenho do sistema assíncrono OCDMA é claramente dependente da MAI, do tipo de modulação usado e da topologia do receptor. O código OOC deve ser cuidadosamente selecionado posto que dele podem decorrer problemas de sincronização entre o transmissor e receptor por conta das propriedades de correlação.

Valendo-se do fato de todo grupo ser isomorfo ao grupo de permutação é possível encontrar um código de permutação equivalente. Logo, a proposta de enquadramento dos códigos ortogonais ópticos como casos particulares dos códigos de permutação ou códigos de resíduos quadráticos apresenta como potencial a possibilidade, segundo as características do código óptico que se pretende, de se poder gerar, a partir destes, diversas palavras códigos sem a necessidade de busca de novas estruturas para códigos ópticos. Portanto, a proposta pode ser considerada uma nova técnica de construção de códigos ortogonais ópticos, diferente das técnicas como: relaxamento dos parâmetros do código, iterativa, greedy e geometria projetiva.

Os códigos primos, devido às suas propriedades de correlação mostram-se pouco aplicáveis aos sistemas assíncronos OCDMA. Os códigos EQC possuem os requisitos para sistemas desde que a auto-correlação e a correlação cruzada sejam próximas das propriedades de correlação ideais. O número de usuários é dependente do comprimento e do peso do código mas estes parâmetros devem ser escolhidos de forma cuidadosa pois o desempenho do sistema pode diminuir quando se aumenta alguns desses parâmetros.

A partir dos códigos propostos se poderá construir novas famílias de códigos para sistemas OCDMA síncronos, de modo que os resultados apresentados nesta tese estendem os trabalhos publicados anteriormente em códigos ortogonais ópticos para sistemas OCDMA, pelo fato de introduzirem códigos congruentes de nova estrutura algébrica com razão K/F aceitável, o qual resulta em boas propriedades de sincronismo, sendo portanto, uma contribuição para os sistemas OCDMA e OOC.

6.2 Sugestões para trabalhos futuros

Avaliar o desempenho dos códigos propostos em sistemas OCDMA síncronos.

Desenvolver estruturas algébricas para gerar códigos ortogonais ópticos 2D e 3D.

Considerando-se que uma das particularidades do OOC ideal é ser esparso em termos de “chips” 1, sugere que se crie um modelo de receptor óptico para sistemas OCDMA, cujo princípio de operação seja baseado no algoritmo binário de Berkamp-Massey [106].

Referências Bibliográficas

[1] A. D. Neto, "Propostas de Códigos ortogonais para Sistemas OCDMA", Tese de Doutorado, FEEC-UNICAMP, Agosto, 2005.

[2] A. D. Neto, "Construction of optical orthogonal codes for use in cdma fiber-optics systems", PhD Thesis, FEEC-UNICAMP, August, 2005.

[3] B. Mukherjee, "Optical Communication Networks", McGraw-Hill, New York, 1997

[4] D. J. G. Mestdagh, "Fundamentals of Multiaccess optical Fiber Networks", Boston, Artech House, 1995

[5] J. A. Salehi, "Code division multiple access techniques in optical fiber networks - Part I: Fundamental principles", IEEE Trans. Commun, vol. 37, no. 8, pp. 824-833, Aug., 1989.

[6] A. A. Albert, "Modern Higher Algebra", Chicago, USA, The University of Chicago Press, 1936

[7] P. Prucnal, M. A. Santoro, S. K. Sehgal, "Ultra-fast all-optical synchronous multiple access fiber networks", IEEE J. Select. Areas Commun., vol. 4, no. 9, pp. 1484-1493, 1986

[8] M. A. Santoro, P. Prucnal, "Asynchronous fiber optic local area network using CDMA and optical correlation", IEEE Proc., vol. 75, no. 9, pp. 1336 - 1338, 1987

[9] P. Prucnal, M. Santoro, T. Fan, "Spread Spectrum Fiber Optic Local Area Network Using Optical Processing", IEEE/OSA, J. Lightwave Technol., LT- 4, no. 5, pp. 547-554, May, 1986

[10] G. C. Yang, T. E. Fuja, "Optical orthogonal Codes with Unequal Auto- and Cross-Correlation Constraints", IEEE Trans. Inform. Theory, vol. 41, no. 1, pp. 96-106, Jan., 1995.

[11] G. C. Yang, "Variable-Weight Optical Orthogonal Codes for CDMA Networks with Multiple Performance", IEEE Trans. Commun, vol. 44, no. 1, pp. 47-55, Jan., 1996.

[12] S. M. Johnson, "A new upper bound for error correcting codes", IEEE Trans. Inform. Theory, vol. 8, pp. 203-207, 1962

[13] F. Chung, J. A. Salehi, V. K. Wei, "Optical orthogonal codes: Design, analysis and applications", IEEE Trans. Inform. Theory, vol. 35, no. 3, pp. 595-604, Mar., 1989

[14] H. Van Trees, "Classical Detection and Estimation Theory in Detection Estimation and Modulation Theory - Part I ", John Wiley & Sons, New York, 1968

[15] M.B. Fisher, R.T. McKenzie, "Traveling-wave Photomultiplier", IEEE Jour. Quant. Elect., vol. QE-2, pp. 322-327, 1966

[16] K. H. Rosen, "Elementary Number Theory and its Applictions", Addison Company, 2nd Editon, New York, 1988

[17] H. F. Blichfeldt,"A New Principle in the Geometry of Numbers, with Some Applications", Trans. Amer. Math. Soc. 15, 227-235, 1914

[18] I. N. Stewart, D.O. Tall, "Algebraic Number Theory", 2 ed., CHAPMAN HALL/CRC, 1992

[19] J. H. Conway, N. J. Sloane, "Sphere Packing, Lattices and Groups", Springer-Verlag, New York, 1998

[20] D. S. Dummit, R.M. Foote,"Abstract algebra", Prentice Hall, Inc., 1991.

[21] J. M. Hall, "The Theory of Groups", New York, Chelsea, 1976.

[22] D. Slepian, "Group Codes for the Gaussian Channel", Bell System. Tech. Journal, vol. 47, pp. 575-602, Set., 1968.

[23] G. D. Forney., "Geometrically uniform codes", IEEE Trans. Inform. Theory, vol. 37, no. 9, pp. 1241-1260, Set., 1991

[24] I. Ingemarsson, "Group codes for the Gaussian Channel", in Topics in Coding Theory, no. 128, in Lecture Notes in control and Information Sciences, Berlin, Germany, Springer-Verlag, pp.73-108, 1989

[25] C. E. Câmara, "Construção de códigos esféricos via a d-cadeia e a geometria de grupos", Tese de Doutorado, FEEC-UNICAMP, Agosto, 1995

[26] W. C. Kwong, P. Perrier, P. R. Prucnal, "Performance comparison of asynchronous and synchronous code-division multiple-access techniques for fiber-optic local area networks", IEEE Trans. Commun., vol. 39, no. 11, pp. 1625-1634, Nov., 1991

[27] A. Shaar, P. Davies, "Prime sequences: Quasi-optical sequences for or channel code division multiplexing", Electron. Lett., vol. 19, no. 21, pp. 888 - 890, 1983.

[28] G.-C. Yang, W. C. Kwong, "Performance analysis of optical cdma with prime codes", Electronics Letters, vol. 31, pp. 569-570, Mar. 1995

[29] S. V. Marhic, Z. I. Kostic, E. L. Titlebaum, "A new family of optical code sequences for use in spread spectrum fiber-optic local area networks", IEEE Trans. Commun., vol. 41, no. 8, pp.1217-1221, Aug., 1993

[30] M. E. Marhic, "Coherent CDMA systems", IEEE/OSA J. Lightwave Technol., vol. 11, no. 5/6, pp. 854-864, May-Jun., 1993

[31] G. J. Foschini, G. Vannuci, "Using spread-spectrum in a high-capacity fiber-optic local area network", IEEE/OSA J. Lightwave Technol., vol. 6, no. 3, pp. 370-379, Mar., 1988

[32] P. Prucnal, "VLSI fiber optic local area network", SPIE Proc., vol. 700, pp. 230-232, 1986

[33] Y. Chang, R. Fuji-Hara, Y. Miao, "Combinatorial Constructions of optimal Optical orthogonal codes with weigth 4," *IEEE Trans. Inform. Theory*, vol. 49, no. 5, pp. 1283-1292, May., 2003.

[34] R. Fuji-Hara, Y. Miao, "Optical orthogonal codes: Their bounds and new optimal constructions," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2396-2406, Nov. 2000.

[35] S. Bitan, T. Etzion, "Constructions for optimal constant weight cyclically permutable codes and difference families," *IEEE Trans. Inform. Theory*, vol. 41, pp. 77-87, Jan. 1995.

[36] J.-G. Zhang, "Design of a special family of optical CDMA address codes for fully asynchronous data communications," *IEEE Trans. Commun.*, vol. 47, pp. 967-973, July 1999.

[37] H. Chung, P. V. Kumar, "Optical orthogonal codes - New bounds and an optimal construction," *IEEE Trans. Inform. Theory*, vol. 36, pp. 866-873, July, 1990.

[38] P. Prucnal, "All-optical ultra-fast networks", SPIE Proc., vol. 715-802, 42, 1986

[39] W. Kwong, P. Prucnal, "Synchronous CDMA demonstration for fibre optic networks with optical processing", Electron. Lett. vol. 26. no. 24, pp. 1990-1992, Nov., 1990

[40] A. Holmes, R. R. Syms, "All-optical CDMA using quasi-prime codes", IEEE J. Lightwave Technol., vol. 10, no. 2, pp. 279-286, Fev., 1992

[41] A. S. Holmes, R. R. A. Syms, "Switchable all-optical encoding and decoding using optical fibre lattices", Opt. Commun., vol. 86, no. 1, pp. 25-30, Jan., 1991

[42] T. Pfeiffer, B. Deppisch, M. Witte, R. Heidemann,"Optical CDMA transmission for robust realization of complex and flexible multiple access networks," *in Proc. Optical fiber Commun. Conf. (OFC'99)*, Paper WM51, pp. 344-346.

[43] T. Pfeiffer, B. Deppisch, M. Witte, R. Heidemann,"Optical stability of a spectrally encoded optical CDMA system using inexpensive transmitter without spectral control," *IEEE Photon Technol. Lett.*, vol. 11, pp. 916-918, July 1999.

[44] T. Pfeiffer, J. Kissing, J.-P. Elbers, B. Deppisch, M. Witte, H. Schmuck, E. Voges,"Coarse WDM/CDM/TDM concept for optical packet transmission in metropolitan and access networks supporting 400 channels at 2.5 Gb/s peak rate," *IEEE J. Lightwave Technol.(Special Issue on Optical Networks)*, vol. 8, pp. 1928-1938, Dec., 2000.

[45] A. Stok, E. H. Sargent, "The role of optical CDMA in access networks," *IEEE Commun. Mag.*, pp. 83-87, Sept. 2002.

[46] F. Khansefid, H. Taylor, R. Gagliardi,"Design of (0,1) sequence Sets for Pulsed Coded System," *Univ. Southern California Rep.*, CSI-88-03-03, Mar. 3, 1988.

[47] S. Zahedi, J. A. Salehi, "Analytical comparation of various fiber-optic CDMA receiver structures," *IEEE J. Lightwave Technol.*, vol. 18, pp. 1718-1727, Dec., 2000.

[48] T. O'Farrell, S. Lohmann, "Performance analysis of an optical correlator receiver for SIK DS-CDMA communications systems", Electron. Lett., vol. 30, no. 1, pp. 63-65, Jan., 1994

[49] J. A. Salehi, A. M. Weiner, J. P. Heritage, "Coherent ultrashort lightpulse code-division multiple access communications systems", IEEE/OSA J.Lightwave Technol., vol. 8, no. 3, pp. 478-491, Mar., 1990.

[50] G.-C. Yang, "Some new families of optical orthogonal codes for code-division multiple-access fiber-optic networks", IEEE Trans. Commun., vol. 142, no 6, pp. 363-368, Dec. 1995

[51] C.-S. Weng, J. Wu, "Optical orthogonal codes with nonideal cross correlation", IEEE J. Lightwave , vol. 19, no. 12, pp. 1856-1863, Dec., 2001

[52] C.-S. Weng, J. Wu, "Perfect difference codes for synchronous fiber-optic CDMA communication systems", IEEE J. Lightwave , vol. 19, no. 2, pp. 186-194, Feb., 2001

[53] C.-S. Weng, J. Wu, "Optical orthogonal codes with large cross-correlation and their performance bound for optical asynchronous CDMA systems", IEEE J. Lightwave , vol. 21, no. 3, pp. 735-742, Feb., 2003.

[54] A.J. Mendez, R. M. Gagliardi, V. J. Hernandez, C. V. Bennett, W. J. Lennon, "High-performance optical CDMA system based on 2-D optical orthogonal codes ", *IEEE J. Lightwave*, vol. 22, no. 11, pp. 2409-2419, Nov., 2004.

[55] R. M. H. Kim, L. R. Chen, J. Bajcsy, "Design and performance of 2D codes for wavelength-time optical CDMA," *IEEE Photon Technol. Lett.*, vol. 14, pp. 714 - 716, May, 2002.

[56] G. C. Yang, W. C. Kwong, "Two-dimensional spatial codes signature patterns", *IEEE Trans. Commun.*, vol. 44, pp. 184-191, Feb., 1996.

[57] R. N. Nogueira, P. S. Taluja, A. L. X. Texeira, P. S. B. Andre, J. F. Rocha, J. L. Pinto, "New technique for implementing multiwavelength orthogonal codes for OCDMA using fiber Bragg gratings written i high birefringence fibers", *in Proc. 16th Annu. Meeting IEEE Lasers Electro-Optics Society (LEOS'03)*, vol. 2, Paper WI2, pp. 545-546, Oct., 2003.

[58] W. C. Kwong, G.-C. Yang, "Multiple-length multiple-wavelength optical orthogonal codes for optical CDMA systems supporting multirate services", *IEEE J. Select. Areas Commun.*, vol. 22, no. 9, pp. 1604-1647, Nov., 2004.

[59] W. C. Kwong, G.-C. Yang, "Design of Multilength Optical Orthogonal Codes for Optical CDMA Multimedia Networks", *IEEE Trans. Commun.*, vol. 50, no. 8, pp.1258-1265, Aug., 2002.

[60] G.-C. Yang, S.-Y. Lin, W. C. Kwong, "MFSK/FH-SSMA wireless systems with double-media services over fading channels", *IEEE Trans. Veh. Technol.*, vol. 49, pp. 900-910, May, 2000

[61] K.-I.Kitayama, N. Wada, H. Sotobayashi, "Architectural considerations for photonic IP router based upon optical code correlation," *IEEE J. Lightwave Technol.(Special Issue on Optical Networks)*, vol. 18, pp. 1834-1844, Dec., 2000

[62] N. Wada, H. Harai, F. Kubota,"40 Gb/s interface, optical code based photonic packet switch prototype," *in Proc. Optical fiber Commun. Conf. (OFC'03)*, Paper FS7, pp. 801-802

[63] D. Gurkan, S. Kumar, A. Sahin, A. Willner, K. Parameswaran, M. Feier, D. Starodubov, J. Bannister, P. Kamath, J. Touch,"All optical wavelength and time 2-D code converter for dynamically-reconfigurable O-CDMA networks using a PPLN waveguide," *in Proc. Optical fiber Commun. Conf. (OFC'03)*, Paper FD6, pp. 654-656

[64] S. J. Lee, H. W. Lee, D. K. Sung, "Capacities of single-code and multicode DS-CDMA systems accommodating multiaccess services", *IEEE Trans. Veh. Technol.*, vol. 48, pp. 1323-1326, May, 1999

[65] F. -R. Gu, J. Wu, "Construction and performance analysis of variable-weight optical orthogonal codes for asynchronous optical CDMA systems," *J. Lightwave Technol.*, vol. 23, no. 2, pp. 740-748, Feb., 2005

[66] S. V. Maric, V. K. N. Lau, "Multirate fiber-optic CDMA: System design and performance analysis ", *J. Lightwave Technol.*, vol. 16, pp. 9 - 17, Jan., 1998.

[67] T. Nagell, "Introduction to Number Theory", 2 ed., Chelsea, New York, 1981

[68] S. V. Marhic, "A new family of algebraically designed optical code sequences for use in CDMA fiber-optic networks", Electronic Letters, vol. 26, no. 3, pp. 538-539, Mar., 1993

[69] A. Hurwitz, "Lectures on Number Theory", Springer-Verlag, New York, Chapter 6, pp. 157-264, 1986

[70] A. D. Neto, E. Moschim, "Some Optical Orthogonal Codes for asynchronous CDMA Systems", Proccedings of IEEE GLOBECOM'2002, vol. 3, pp. 2065-2068, Taiwan, Nov., 2002

[71] A. D. Neto, E. Moschim, "Generation of Code Sequences for Asynchronous Optical CDMA Systems", Proccedings of Fourth International Workshop on Laser and Fiber-Optical Networks Modeling, IEEE Laser and Electro-Optics Society, pp. 138-140, Kharkov, Ukraine, June, 2002

[72] A. D. Neto, E. Moschim, "Construção de Novos Códigos Ortogonais Ópticos por meio de Equações Diofantinas", Revista IEEE América Latina, vol. 3, Issue 3, pp. 1-8, Jul., 2005.

[73] S. V. Marhic, M. D. Hahm, E. L. Titlebaum, "Construction and Performance Analysis of a New Family of Optical Orthogonal Codes for CDMA Fiber-Optic Networks", IEEE Trans. Commun., vol. 43, no. 2/3/4, pp.485 - 489, Feb./Mar./Apr., 1995

[74] J. A. Salehi, C. Brackett, "Code division multiple access techniques in optical fiber networks - Part II: Systems performance analysis", IEEE Trans. Commun., vol. 37, no. 8, pp. 834-842, Aug., 1989

[75] M. Azizoglu, J. A. Salehi, Y. Li, "Optical CDMA via temporal codes", IEEE Trans. Commun., vol. 40, no. 7, pp. 1162-1170, July, 1992

[76] M. Azizoglu, J. A. Salehi, Y. Li, "On performance of fiber-optic CDMA systems", IEEE GLOBECOM, San Diego, CA, pp. 1861-1865, Dec., 1990

[77] H. M. H. Shalaby, "A Comparison between the Performance of Number-State and Coherent-State Optical CDMA in Lossy Photon Channels", IEEE J. SAC., vol.13, no. 3, pp. 592-602, April, 1995

[78] H. M. H. Shalaby, "Complexities, error probabilities, and capacities of optical OOK-CDMA communication systems", IEEE Trans. Commun., vol.50, no. 12, pp. 2009-2017, Dec., 2002

[79] H. M. H. Shalaby. "Maximum achievable throughputs for uncoded OPPM and MPPM in optical direct-detection channels", IEEE J. Lightwave Technology, vol. 13, no. 11, pp. 2121-2128, Nov., 1995

[80] H. M. H. Shalaby, "Performance analysis of optical synchronous CDMA communication systems with PPM signaling", IEEE Trans. Commun., vol. 43, no. 2/3/4, pp. 624-634, Feb./Mar./Apr., 1995

[81] H. M. H. Shalaby, "Chip-level detection in optical code division multiple access". IEEE J. Lightwave Technology, vol.16, no.6, pp. 1077-1087, Jun., 1998

[82] H. M. H. Shalaby, "Direct detection optical overlapping PPM-CDMA communication systems with double optical hardlimiters". IEEE J. Lightwave Technology, vol. 17, no. 7, pp. 1158-1165, Jul., 1999

[83] H. M. H. Shalaby, "Synchronous fiber-optic CDMA systems with interference estimators". IEEE J. Lightwave Technology, vol. 17, no. 11, pp. 2268-2275, Nov., 1999

[84] H. M. H. Shalaby, "Effect of thermal noise and apd noise on the performance of OPPM-CDMA receivers". IEEE J. Lightwave Technology, vol. 18, no. 7, pp. 905-914, Jul., 2000

[85] T. Ohtsuki, "Direct-detection optical asynchronous CDMA systems with double optical hard-limiters: APD noise and thermal noise", IEEE GLOBECOM 98, vol. 6, pp. 3233-3238, Nov., 1998

[86] T. Ohtsuki, "Channel Interference Cancellation using Electrooptic Switch and Optical Hard-Limiters for Direct-Detection Optical CDMA Systems", Conf. Rec. ICC, vol. 1, pp. 106-110, 1997

[87] T. Ohtsuki, "Performance Analysis of Direct-Detection Optical Asynchronous CDMA Systems with Double Optical Hard-Limiters", IEEE J. Lightwave Technol., vol. 15, no. 3, pp. 452-457, Mar., 1997

[88] T. Ohtsuki, K. Sato, I. Sasase, S. Mori, "Direct-Detection Optical Synchronous CDMA Systems with Double Optical Hard-Limiters Using Modified Prime Sequence Codes". IEEE J. SAC, vol. 14, no. 9, pp. 1879-1887, Sep., 1996

[89] H. M. Kwon, "Optical Orthogonal Code-Division Multiple-Access System - Part I: APD Noise and Thermal Noise", IEEE Trans. Commun., vol.42, no. 7, pp. 2470-2479, July, 1994

[90] H. M. Kwon, "Optical Orthogonal Code Division Multiple Access System, Part II: Multibits/Sequence-Period OOCDMA", IEEE Trans. Commun., vol. 42, no. 8, pp. 2592-2599, Aug., 1994

[91] T. O'Farrell, M. Beale, "Code division multiple access (CDMA) techniques in optical fibre LANs", in Proceedings of 2nd IEE National Conference on Telecommunications, pp. 111-115, York, UK, 1989

[92] T. O'Farrell, "New signature code sequence design techniques for CDMA systems", Electron. Lett., vol. 27, no. 4, pp. 371-373, Fev., 1991

[93] M. B. Pursley, "Performance evaluation for phase-coded spread spectrum multiple-access communication-Part I", IEEE Trans. Commun., vol. COM-25, no. 8, pp. 85-94, Aug., 1977

[94] A. NETO, A. C. Bordonalli, C. R. Lima, E. Conforti, "Microwave Signal generation by mixing of modulated optical carriers in saturated semiconductor optical amplifier", in Proccedings of 1999 SBMO / IEEE International Microwave and Optoelectronics Conference, Rio Janeiro - Brasil, p.417-420, 1999

[95] S. Grubb, "1.3 μm Raman Fiber Amplifiers", in IEEE 8th Lasers and Electro-Optics Society Annual Meeting Conference Proceedings, vol. 1, pp. 30-31, vol. 2, pp. 69-70, Breckenridge, Colorado, Oct., 1995

[96] T. Durhuus,"High Performance Semiconductor Optical Preamplifier", in Topical Meeting on Optical Amplifiers and Their Applications, Breckenridge, Colorado, Optical Society of America, WB-4, 1994.

[97] J. Crowe, W. Ahearn, "Semiconductor Laser Amplifier", IEEE J. Quant. Elect., vol. QE-2, no 8, pp. 283-289, 1966

[98] E. Desurvire, "Erbium-Doped Fiber Amplifiers: Principles and Applications", New York, John Wiley & Sons, 1994

[99] P. P. Webb, R. J. McIntyre, J. Conradi, "Properties of avalanche photodiodes", RCA Rev., vol. 35, pp. 234 - 278, June, 1974

[100] K. R. Baker, "The Inverse Gaussian distribution and statistical application - A Review", J. R. Statis. Soc. B, vol. 40, no. 3, pp. 263-289, Mar., 1978

[101] M. C. K. Tweedie, "Inverse Statistical Variates", Nature, vol. 155, pp. 453-460, 1945

[102] J. J. Shuster, "On the Inverse Gaussian Distribution Function", J. Amer. Statistical Assn., vol. 63, pp. 1514-1516, Dec., 1968

[103] F. M. Davidson, X. Sun, "Gaussian approximation versus nearly exact performance analysis of optical communication systems with PPM signaling and APD receivers", IEEE Trans. Commun., vol. 36, no. 11, pp. 1185-1192, Nov., 1988

[104] R. J. McIntyre, "The distribution of gains in uniformly multiplying avalanche photodiodes: Theory", IEEE Trans. Electron Devices, vol. ED-19, pp. 703-713, June, 1972

[105] J. Conradi, "The distribution of gains in uniformly multiplying avalanche photodiodes: Experimental", IEEE Trans. Electron Devices, vol. ED-19, pp. 713-718, June, 1972

[106] J. L. Massey, "Shift-register synthesis and BCH decoding", IEEE Trans. Inform. Theory, vol. IT-15, no. 1, pp. 122-127, Jan., 1969

Apêndice A

Demonstrações Complementares

A.1 Atraso Relativo Adjacente

Demonstração do Lema 2.3.1
Os elementos do vetor $\mathbf{R_x}$ são os atrasos relativos entre qualquer par de chips "1" do vetor $\mathbf{X}$, de modo que o vetor $\mathbf{R_x}$ possui $\lambda+1$ elementos repetidos se, somente se, existirem duas seqüências, $\{i_0, i_1, i_2, ..., i_\lambda\}$ e $\{i'_0, i'_1, i'_2, ..., i'_\lambda\}$ tal que $\{x_{i_j} = x_{i'_j} = 1\}$ e $\{i_j - i'_j = \tau' \neq 0\}$, para todo $j = 0, 1, 2, ..., \lambda$. Porém, isto é válido se, somente se, $\sum_{t=0}^{F-1} x_t x_{t\oplus\tau'} \geq \lambda + 1$. ■

Demonstração do Lema 2.3.2
Seja $\mathbf{M}_{\mathbf{X},\lambda}$ o conjunto definido em (2.12) e $\mathbf{m} = [a_0, a_1, a_2, ..., a_{\lambda-1}] \in \mathbf{M}_{\mathbf{X},\lambda}$ se, somente se, existe uma seqüência de $\lambda+1$ distintos números inteiros, ou seja $\{i_0, i_1, i_2, ..., i_\lambda\}$ tal que

$$\begin{cases} x_{i_j} = 1 & j = 0, 1, 2, ..., \lambda \\ i_{j+1} - i_j = a_j & j = 0, 1, 2, ..., \lambda - 1 \end{cases}$$

Portanto, $\mathbf{M}_{\mathbf{X},\lambda} \cap \mathbf{M}_{\mathbf{Y},\lambda} = \emptyset$ se, somente se, possível enfileirar $\lambda+1$ chips "1" no vetor $\mathbf{X}$ e $\lambda+1$ no vetor $\mathbf{Y}$ com seus respectivos deslocamentos cíclicos, ou seja $\mathbf{M}_{\mathbf{X},\lambda} \cap \mathbf{M}_{\mathbf{Y},\lambda} = \emptyset$ se, somente se, é válida a inequação (2.15). ■

Demonstração do Lema 2.3.3

Os vetores de comprimento $\lambda+1$ em $\mathbf{M}_{\mathbf{x},\lambda}$ correspondem a $\lambda+1$ elementos não nulos do vetor $\mathbf{X}$, de modo que os atrasos relativos entre estes elementos são dados pelos vetores de comprimento $\lambda+1$ que compõem $\mathbf{M}_{\mathbf{x},\lambda}$. Se a inequação (2.13) é válida, então existem dois diferentes conjuntos de elementos não nulos relativamente eqüidistantes entre si. Assim, os $\lambda+1$ chips "1" podem ser enfileirados para se obter $\lambda_a \geq \lambda+1$, ou seja, se a inequação (2.13) é válida, então todos os conjuntos de $\lambda+1$ elementos não nulos do vetor $\mathbf{X}$ possuem diferentes atrasos relativos, o que torna impossível obter $\lambda_a \geq \lambda+1$. ■

A.2 Cardinalidade dos Códigos OOC

Demonstração do Limitante Superior

Seja C um código $(F, K, \lambda)-$OOC, cuja cardinalidade $|C| = \Phi(F, K, \lambda)$. Da propriedade de auto-correlação, equação (A.10), decorre que para todo $X \in C$ o conjunto $M_{X,\lambda}$ possui $K.\begin{pmatrix} K-1 \\ \lambda \end{pmatrix}$ distintos vetores de λ números inteiros. Da propriedade de correlação-cruzada, equação (A.15), decorre que para $X,\ Y \in C,\ X \neq Y$, os conjuntos $M_{X,\lambda}$ e $M_{Y,\lambda}$ são disjuntos, conseqüentemente a união de $M_{X,\lambda}$, a medida que X varia sobre todos os $X \in C$, consiste de $\Phi(F, K, \lambda).\ K.\begin{pmatrix} K-1 \\ \lambda \end{pmatrix}$ distintos vetores de λ números inteiros. Por definição, se $[a_0, a_1, a_2, ..., a_{\lambda-1}] \in M_{X,\lambda}$, então $a_0 + a_1 + a_2 + ... = a_{\lambda-1} \leq F-1$, conforme a equação (2.12). Considerando que selecionar os elementos a_i, em quantidade igual a $\lambda \leq F-1$, é igual à combinação de F com $\lambda+1$, isto é, igual a $\begin{pmatrix} F-1 \\ \lambda \end{pmatrix}$. Portanto, $\Phi(F, K, \lambda).\ K.\begin{pmatrix} K-1 \\ \lambda \end{pmatrix} \leq \begin{pmatrix} F-1 \\ \lambda \end{pmatrix}$ em que:

$$\Phi(F, K, \lambda) \leqslant \frac{\begin{pmatrix} F-1 \\ \lambda \end{pmatrix}}{K.\begin{pmatrix} K-1 \\ \lambda \end{pmatrix}} = \frac{(F-1)(F-2).....(F-\lambda)}{K(K-1)(K-2)...(K-\lambda)}$$

■

Demonstração do Teorema 2.4.1

A demonstração consiste em mostrar que, para um dado vetor $\mathbf{X}$:

1) Λ é limitante superior do número de vetores com comprimento F que violam a propriedade de auto-correlação;

2) Θ é limitante superior do número de vetores com comprimento F que violam a propriedade de correlação cruzada.

Demonstração do Limitante Λ

Seja $\mathbf{Y}$ um vetor $F-$*ário* que possui chips "1" nas seguintes posições $S = \{s_1, s_2, ..., s_K\}$. Pretende-se conhecer o número de conjuntos $K-$*ários* que violam a propriedade de auto-correlação. Como mostrado em [13], se $\mathbf{Y}$ viola a propriedade de auto-correlação, então existe um número δ que pode ser representado por $s_i - s_j$ em mais de $\lambda_a + 1$ formas, onde $1 \leq \delta \leq \frac{F-1}{2}$. Assim, existem no total $\frac{F-1}{2}$ escolhas para δ, $\begin{pmatrix} K \\ \lambda_a + 1 \end{pmatrix}$ escolhas para pares de chips "1", e $\begin{pmatrix} F \\ K - \lambda_a - 1 \end{pmatrix}$ escolhas para os demais chips. Portanto,

$\left(\frac{F-1}{2}\right)\begin{pmatrix} K \\ \lambda_a+1 \end{pmatrix}\begin{pmatrix} F \\ K-\lambda_a-1 \end{pmatrix}$ é um limitante superior do número de vetores que violam a propriedade de auto-correlação. □

Demonstração do Limitante Θ
Dado o vetor $\mathbf{X}$, de comprimento F, então existem

$$\Theta = F\sum_{i}^{\vartheta}\begin{pmatrix} F-K \\ K-i \end{pmatrix}\begin{pmatrix} K \\ i \end{pmatrix}$$

vetores $F-$*ário* cujos chips "1" se sobrepõem, aos chips "1" de $\mathbf{X}$ mais do que λ_c vezes. Cada um desses vetores $F-$*ário* possui no máximo F deslocamentos cíclicos que violam a propriedade de correlação cruzada com $\mathbf{X}$. Portanto, estes formam o total de vetores $F-$*ário* que violam a propriedade de correlação cruzada com $\mathbf{X}$. □■

A.3 Teoria da detecção

Para ilustrar o processo de detecção de uma variável com distribuição gaussiana, o desempenho do receptor é dado pela expressão:

$$Pe = P(I = 1 \geq \gamma|0)P(0) + P(I = 0 < \gamma|1)P(1) \tag{A.2}$$

A variável de decisão I, no instante de amostragem, possui densidade de probabilidade gaussiana, dada pela expressão:

$$P(I) = \frac{1}{\sqrt{2\pi}\sigma_1}\exp\left[-\frac{(I-I_1)^2}{2\sigma_1^2}\right] \text{ caso o bit "1" seja detetado} \tag{A.3}$$

onde I_1 e σ_1^2 definem a média e variância, respectivamente. De forma análoga, a variável de decisão I, quando o bit zero é detetado, possui densidade de probabilidade gaussiana, dada pela expressão:

$$P(I) = \frac{1}{\sqrt{2\pi}\sigma_0}\exp\left[-\frac{(I-I_0)^2}{2\sigma_0^2}\right] \text{ caso o bit "0" seja detetado} \tag{A.4}$$

onde I_0 e σ_0^2 definem a média e variância, respectivamente.

Considerando que os bit "1" e bit "0" são transmitidos com probabilidade igual a $Pr(0) = Pr(1) = 1/2$ e que o detector use um valor de limiar γ, a probabilidade de erro do receptor, equação (A.2), é dada pela expressão:

$$Pe = \frac{1}{2}\int_{-\infty}^{\gamma}\frac{1}{\sqrt{2\pi}\sigma_1}\exp\left[-\frac{(I-I_1)^2}{2\sigma_1^2}\right]dI + \frac{1}{2}\int_{\gamma}^{\infty}\frac{1}{\sqrt{2\pi}\sigma_0}\exp\left[-\frac{(I-I_0)^2}{2\sigma_0^2}\right]dI \tag{A.5}$$

O limiar ótimo, γ_{ot}, possui efeito substancial na correta detecção dos bits transmitidos. Seu valor é determinado igualando a equação (A.2) a zero e, em seguida, derivada em relação

ao limiar γ.

$$\frac{\partial Pe}{\partial \gamma} = \Pr(I = 0 < \gamma|1)\Pr(1) - \Pr(I = 1 \geq \gamma|0)\Pr(0) = 0; \tag{A.6}$$

$$\Pr(I = 0 < \gamma|1) = \Pr(I = 1 \geq \gamma|0);$$

$$\frac{1}{\sigma_1}\exp\left[-\frac{(I_1-\gamma)^2}{2\sigma_1^2}\right] = \frac{1}{\sigma_0}\exp\left[-\frac{(\gamma-I_0)^2}{2\sigma_0^2}\right];$$

$$\frac{(\gamma-I_0)^2}{2\sigma_0^2} - \frac{(I_1-\gamma)^2}{2\sigma_1^2} = \ln\left(\frac{\sigma_1}{\sigma_0}\right);$$

que pode ser substituída pela seguinte equação quadrática equivalente:

$$a\gamma^2 + b\gamma + c = 0 \tag{A.7}$$

onde $a = (\sigma_1^2 - \sigma_0^2)$; $b = 2(I_1\sigma_0^2 - I_0\sigma_1^2)$; $c = I_0^2\sigma_1^2 - I_1^2\sigma_0^2 - 2\sigma_1^2\sigma_0^2\ln\left(\frac{\sigma_1}{\sigma_0}\right)$. Resolvendo a equação quadrática em relação a γ se obtém a seguinte expressão:

$$\gamma = \frac{-I_1\sigma_0^2 + I_0\sigma_1^2 + \sqrt{\sigma_1^2\sigma_0^2(I_1-I_0)^2 + 2(\sigma_1^2-\sigma_0^2)\ln\left(\frac{\sigma_1}{\sigma_0}\right)}}{\sigma_1^2-\sigma_0^2} \tag{A.8}$$

Quando o sinal é muito maior que o ruído, se pode considerar:

$$(I_1-I_0)^2 \gg \frac{2(\sigma_1^2-\sigma_0^2)\ln\left(\frac{\sigma_1}{\sigma_0}\right)}{\sigma_1^2\sigma_0^2}.$$

Assim, o limiar ótimo de decisão é igual a

$$\gamma_{ot} = \frac{I_1\sigma_0 + I_0\sigma_1}{\sigma_1 + \sigma_0} \tag{A.9}$$

Para $\sigma_1 = \sigma_0$, o limiar ótimo é dado por $\gamma_{ot} = (I_1 + I_0)/2$.

A.4 Teoria dos Reticulados

Demonstração do Teorema 3.2.3
Seja $S' = A^{-1}S$. Então S' é convexo e simétrico em torno de $\mathbf{0}$. Sendo $det(A^{-1}) = 1/det(A)$, decorre que $\upsilon(S') = \upsilon(S)/|det(A)| = \upsilon(S)/d(\Lambda) > 2^n$. Deste modo, pelo teorema (3.2.2), existe o ponto $\mathbf{c} \in S'$ tal que $\mathbf{c} \neq 0$, $\mathbf{c} \in \mathbb{Z}^n$. Fazendo $\mathbf{x} = A\mathbf{c}$ fica provado o teorema. ■

A.5 Forma algébrica de códigos $(F, K, 1, 1) - OOC$

Demonstração do Teorema 4.2.1

Seja $\mathcal{C}_x = (c_{x0}, c_{x1}, c_{x2}, ..., c_{xm}, ..., c_{x,\mathbf{F}-1}) \in \mathcal{C}$ a x-ésima palavra do código $\mathcal{C}$ cuja função de auto-correlação é definida pela seguinte expressão

$$Z_{x,x} = \sum_{m=0}^{F-1}\sum_{n=0}^{F-1} c_{xm}c_{x,m+n} \tag{A.10}$$

onde $0 \leq m \leq \mathbf{F}-1$, $0 \leq n \leq \mathbf{F}-1$. Seja também

$$c_{xm} = c_{00} f_m$$

o m-ésimo símbolo binário de C_x onde $c_{00} = 1$ e

$$f_m = \begin{cases} 1, & m = \mu_{xy} + (y-1)\mu + 1 \\ 0, & fora \end{cases} \tag{A.11}$$

Para demonstrar a primeira parte do teorema precisamos provar que toda palavra-código $\mathcal{C}_x$ possui $\lambda_a = 1$. Para simplificar a notação a equação (A.10) é reescrita na seguinte forma

$$Z_{x,x} = \sum_{m,n=o}^{F-1} c_m c_{m+n} = c_{00}^2 \sum_{m,n=0}^{F-1} f_m f_{m+n} = \sum_{m,n=0}^{F-1} f_m f_{m+n} \tag{A.12}$$

Se $n = 0$ então $Z_{x,x} = \sum_{m=0}^{F-1} f_m^2$. Como $f_m^2 = f_m$ logo

$$Z_{x,x} = \sum_{m=0}^{F-1} f_m = (p-1)/2$$

Se $n \neq 0$ a operação de somatórias na expressão (A.12) transforma $Z_{x,x}$ em

$$Z_{x,x} = \sum_{m,n\neq 0}^{F-1} f_m f_{m+n} = \left(\sum_{m}^{F-1} f_m \right)^2 - \sum_{m}^{F-1} f_m^2 \tag{A.13}$$

Para uma forma algébrica f que representa um número inteiro $n \in \mathbb{Z}$ existe outra forma algébrica g equivalente a f tal que os coeficientes de g estão em f [67]. Logo, sem perda de generalidade, a expressão (A.13) pode ser representada por uma equação equivalente da forma

$$k^2 - k = r, \tag{A.14}$$

onde $r \in \mathbb{Z}_+$. A equação (A.14) é do segundo grau em k, com determinante $D = 1 + 4r$, cujas raízes são $k_1 = (1 + \sqrt{D})/2$ e $k_2 = (1 - \sqrt{D})/2$. A raiz k_2 perde o seu significado, para o número de soluções da equação (A.13), posto que a auto correlação $0 \leq Z_{x,x} \leq \lambda_a$. Como a equação (A.14) possui somente uma raiz significativa, qualquer palavra-código $\mathcal{C}_x$, para todo deslocamento no tempo, também possui somente uma sobreposição (um chip coincidindo) com a sua própria versão não deslocada no tempo. Assim, a exigência da auto-correlação $\lambda_a = 1$ está provada.

Sejam $\mathcal{C}_\gamma = (c_{\gamma 0}, c_{\gamma 1}, ..., c_{\gamma m}, ..., c_{\gamma,\mathbf{F}-1}) \in \mathcal{C}$ a γ-ésima palavra-código de $\mathcal{C}$, a palavra-código $\mathcal{C}_x$, como antes definida, e $x \neq \gamma$. Seja a correlação cruzada, entre qualquer par de diferentes palavras-código $\mathcal{C}_x$ e $\mathcal{C}_\gamma$, definida pela expressão

$$Z_{x,\gamma} = \sum_{m=0}^{F-1} \sum_{n=0}^{F-1} c_{xm} c_{\gamma,m+n} \tag{A.15}$$

Adotando $c_{\gamma m} = c_{00} g_m$ o m-ésimo símbolo de $\mathcal{C}_\gamma$, onde a função g_m corresponde a seguinte expressão

$$g_m = \begin{cases} 1, & m = \mu_{jy} + (y-1)\mu + 1 \\ 0, & fora \end{cases} \tag{A.16}$$

Nesta parte do teorema, precisamos provar que a correlação cruzada $\lambda_c = 1$, para qualquer par de diferentes palavras-código de $\mathcal{C}$.

Para simplificar a notação, a equação (A.15) é reescrita na seguinte forma

$$Z_{x,\gamma} = c_{00}^2 \sum_{m,n=0}^{F-1} f_m g_{m+n} = \sum_{m,n=0}^{F-1} f_m g_{m+n} \tag{A.17}$$

Fazendo uso da seguinte operação somatória

$$\sum_{i,j}^{M} x_i y_j = \left(\sum_{i}^{M} x_i \right) \left(\sum_{j}^{M} y_j \right), \tag{A.18}$$

válida para qualquer número inteiro M nós obtemos

$$Z_{x,\gamma} = \left(\sum_{m=0}^{F-1} f_m \right) \left(\sum_{n=0}^{F-1} g_{m+n} \right). \tag{A.19}$$

Sem perda de generalidade, a equação (A.19) pode ser representada por uma equação do tipo

$$k^2 = r, \tag{A.20}$$

onde $r \in \mathbb{Z}_+$, de cujas raízes, somente uma, $k_1 = \sqrt{r}$, é significativa para a correlação cruzada $0 \leq Z_{x,\gamma} \leq \lambda_c$. Como a equação (A.20) possui somente uma raiz significativa, logo, qualquer par de diferentes palavras-código $\mathcal{C}_x$ e $\mathcal{C}_\gamma$ possui somente uma sobreposição, para todo deslocamento no tempo. Assim, a exigência da correlação cruzada $\lambda_c = 1$ está encontrada. Logo, o teorema fica provado. ■

A.6 Forma algébrica de códigos $(F, K, 1, 2) - OOC$

Demonstração do Teorema 4.3.1

A demonstração do teorema 4.3.1 está baseada no conceito de atraso cíclico relativo entre chips "1" adjacentes da palavra-código e usa os lema "1" para auto correlação e lema "2" para correlação cruzada apresentados em [50].

Seja $t_{\mathbf{C_x}} = [t_{x1}, t_{x2}, ..., t_{xy}]$ o arranjo que contém os atrasos relativos entre todos os chips "1" adjacentes de $\mathcal{C}_x$. Cada elemento de $t_{\mathcal{C}_\S}$ é definido pela equação seguinte

$$t_{xy} = \begin{cases} (2p-1) + s_{xy+1} - s_{xy} & 1 \leq y \leq p-1 \\ (2p-1) + s_{x1} - s_{xy} & y = p \end{cases} \tag{A.21}$$

Seja definida a matriz $\mathbf{R}_{C_x} = [r_{qy}]$, com *(K-1)* linhas e K colunas cujos elementos r_{qy} são definidos conforme a seguinte equação

$$r_{qy} = \sum_{k_0=0}^{q-1} t_{y \oplus k_0} = q(2p-1) + s_{xq \oplus y} - s_{xy}, \tag{A.22}$$

onde $1 \leqslant q \leqslant K-1$ o símbolo " $\oplus$ " denota a operação de adição módulo k.

Na primeira parte da demonstração, precisamos provar que qualquer elemento da matriz $\mathbf{R}_{C_x}$ aparece nela somente uma vez. Qualquer elemento em uma mesma linha "q" da matriz $\mathbf{R}_{C_x}$ é diferente de todos os outros e possui o fator $q(2p-1)$, conforme a equação (A.22). Logo, qualquer elemento em linhas diferentes da matriz $\mathbf{R}_{C_x}$ é diferente de todos os outros e, conseqüentemente, aparece somente uma vez. Sendo os arranjos $\left\{t_{\mathcal{C}_\S} : 0 \leqslant x \leqslant p-1\right\}$ todos distintos, então todas as matrizes $\mathbf{R}_{C_x}$ também são diferentes e, assim, a auto-correlação $\lambda_a = 1$ para todas as palavras-código $\mathcal{C}_x$.

Sejam $\mathcal{C}_x$ e $\mathcal{C}_{x'}$ duas palavras-código diferentes. Seja $\mathbf{M}_{C_x,2}$ o arranjo de inteiros definido pela seguinte equação

$$\mathbf{M}_{C_x,2} = \left\{ \left[\sum_{j_0=0}^{q_0} t_{y \oplus j_0}, \sum_{j_1=q_0+1}^{q_1} t_{y \oplus j_1} \right] \right\} \tag{A.23}$$

onde $0 \leqslant q_0 < q_1 \leqslant k-1$, e $y = 1, 2, ..., k$.

Para demonstrar que $\lambda_c = 2$, mostramos que não existe $\mathbf{m} = \mathbf{m}'$ tal que $\mathbf{m} \in \mathbf{M}_{C_x,2}$ e $\mathbf{m}' \in \mathbf{M}_{C_x,2}$ para um par de diferentes palavras-código $\mathcal{C}_x$ e $\mathcal{C}_{x'}$, ou seja, $\mathbf{M}_{C_x,2} \cap \mathbf{M}_{C_{x'},2} = \emptyset$.

Reescrevendo $\mathbf{M}_{C_x,2}$ na forma de matriz com $\begin{pmatrix} K-1 \\ 2 \end{pmatrix}$ linhas e K colunas, cada um de seus elementos $\mathbf{m}_{jy} = [a_0, a_1]$ possui componentes definidos pelas seguintes equações

$$\begin{aligned} a_0 &= d_0(2p-1) + s_{xb_0} - s_{xc_0} \\ a_1 &= d_1(2p-1) + s_{xb_1} - s_{xb_0} \end{aligned} \tag{A.24}$$

onde

$$d_0 = \begin{cases} p + b_0 - c_0 & b_0 < c_0 \\ b_0 - c_0 & b_0 \geq c_0 \end{cases}$$

$$d_1 = \begin{cases} p + b_1 - b_0 & b_1 < b_0 \\ b_1 - b_0 & b_1 \geq b_0 \end{cases}$$

e $1 \leqslant j \leqslant \begin{pmatrix} K-1 \\ 2 \end{pmatrix}$.

Para simplificar a notação, usaremos as letras $\mathbf{m}$ e $\mathbf{m}'$ para, respectivamente, designarem $\mathbf{m}_{jy}$ e $\mathbf{m}'_{jy}$. Conforme a equação (A.24), cada elemento $\mathbf{m}$ possui somente um inteiro s_{xy} comum aos componentes a_0 e a_1. Sem perda de generalidade, vamos adotar que este inteiro seja s_{xb_0}. Para que $\mathbf{m} = \mathbf{m}'$ seja válido, são requeridas as seguintes condições:

a) Os elementos $\mathbf{m}$ e $\mathbf{m}'$ devem estar na mesma linha da matriz $\mathbf{M}_{C_x,2}$, ou seja q_0 e q_1 são

comuns aos elementos $\mathbf{m}$ e $\mathbf{m}'$;
b) O sistema de equações

$$\begin{cases} s_{xb_0} - s_{xc_0} = s'_{xb_0} - s'_{xc_0} \\ s_{xb_1} - s_{xb_0} = s'_{xb_1} - s'_{xb_0} \end{cases}$$

deve ser válido.

Este sistema de equações será válido somente quando $s_{xc_0} - s'_{xc_0} = s_{xb_1} - s'_{xb_1}$, para todos os $\mathbf{m}$ e $\mathbf{m}'$ na mesma linha de $\mathbf{M}_{C_x,2}$ o que significa as palavras-código $\mathcal{C}_x$ e $\mathcal{C}_{x'}$ serem iguais violando assim a condição inicial de que $\mathcal{C}_x$ e $\mathcal{C}_{x'}$ são diferentes. Portanto, $\mathbf{m} \neq \mathbf{m}'$ para todas as linhas e assim $\mathbf{M}_{C_x,2} \cap \mathbf{M}_{C_{x'},2} = \emptyset$. Logo a exigência da correlação cruzada $\lambda_c = 2$ está provada concluindo a demonstração do teorema. ■