Esdras Nicoletto da Cunha

Análise de Desempenho de um Sistema de Codificação LDPC Cooperativa

Campinas
2013

Universidade Estadual de Campinas
Faculdade de Engenharia Elétrica e de Computação

Esdras Nicoletto da Cunha

Analise de Desempenho de um Sistema de Codificação LDPC Cooperativa

Tese de mestrado apresentada ao Programa de Pós Graduação em Engenharia Elétrica da Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas para a obtenção do título de Mestre em Engenharia Elétrica. Área de concentração: Telecomunicações e Telemática.

Orientador: Prof. Dr. Renato Baldini Filho

Este exemplar corresponde à versão final da tese defendida pelo aluno Esdras Nicoletto da Cunha, e orientada pelo Prof. Dr. Renato Baldini Filho

---

Campinas
2013

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Área de Engenharia e Arquitetura
Rose Meire da Silva - CRB 8/5974

C914a

Cunha, Esdras Nicoletto, 1987-
Análise de desempenho de um sistema de codificação LDPC cooperativa / Esdras Nicoletto da Cunha. - Campinas, SP : [s.n.], 2013.

Orientador: Renato Baldini Filho.
Dissertação (mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Comunicação móvel. 2. Comunicação digital. 3. Codificação. 4. Teoria da codificação. 5. Códigos de controle de erro (Teoria da informção) . I. Filho, Renato Baldini. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Performance analysis of a cooperative LDPC coding system
Palavras-chave em inglês:
Mobile communication Digital
communication
Coding
Coding theory
Error-correcting codes (Information theory)
Área de concentração: Telecomunicações e Telemática
Titulação: Mestre em Engenharia Elétrica
Banca examinadora:
Renato Baldini Filho [Orientador]
José Cândido Silveira Santos Filho
Carlos Eduardo Camara
Data de defesa: 30-08-2013
Programa de Pós-Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE MESTRADO

Candidato: Esdras Nicoletto da Cunha

Data da Defesa: 30 de agosto de 2013

Título da Tese: "Análise de Desempenho de um Sistema de Codificação LDPC Cooperativa"

Prof. Dr. Renato Baldini Filho (Presidente): _____

Prof. Dr. Carlos Eduardo Camara: _____

Prof. Dr. José Cândido Silveira Santos Filho: _____

Aos meus pais.

Agradecimentos

Agradeço,

a Deus pelo dom da vida.

ao meu orientador Prof. Renato Baldini Filho, pela oportunidade concedida, pelo incentivo e ideias contribuídas, pela grande disposição de ajuda durante todo o trabalho.

agradeço aos meus pais, Sebastião e Lori, pela educação e incentivo ao trabalho durante toda a vida. Aos irmãos Estêvão, Lucas e familiares pela amizade e apoio. À minha namorada Letícia, pela ajuda e carinho.

aos professores José Cândido e Carlos Eduardo Câmara por participarem da banca.

aos Profs. Gustavo e Cândido pelas aulas ministradas e pela oportunidade de monitoria. Aos demais Professores da FEEC pelo ensino nas disciplinas por mim cursadas.

aos funcionários da FEEC pela paciência e atenção.

aos colegas de departamento: Rodolpho, Pâmela, Lucas, Juan, Carol, Ana Carolina, Christian e Adailton, Edgar e Diana, pela amizade, companhia durante os estudos.

Agradeço a CAPES pelo apoio financeiro.

à FEEC/UNICAMP pela boa estrutura que oferece aos estudantes e pesquisadores.

A maravilhosa disposição e harmonia do universo só pode ter tido origem segundo o plano de um Ser que tudo sabe e tudo pode. Isto fica sendo a minha última e mais elevada descoberta.

Isaac Newton

Resumo

Comunicação cooperativa faz uso da natureza de radiodifusão das comunicações sem fio, utilizando nós intermediários como retransmissores para produzir diversidade em um enlace de comunicação ponto a ponto. Esta diversidade permite que se aumente a capacidade, a velocidade (taxa) e o desempenho do sistema de comunicação. O processo de codificação de canal, que explora de forma inteligente a diversidade produzida pela comunicação cooperativa, é denominado de cooperação codificada. Para a obtenção de sistemas mais eficientes de comunicação entre dois pontos, a cooperação codificada pode utilizar ou adaptar várias técnicas conhecidas de codificação de canal, tais como: codificação convolucional, turbo, LDPC, RS (*Reed-Solomon*), etc. O objetivo deste trabalho é explorar as características da comunicação cooperativa associadas à técnica de codificação LDPC (*Low Density Parity Check*), com alfabeto binário, de forma a obter sistemas mais simples, confiáveis e eficientes.

Palavras-chave: Comunicaçães Cooperativas, Codificação cooperativa, cooperação codificada, códigos LDPC.

Abstract

Cooperative communications make use of the nature of wireless communications broadcasting, by using intermediate nodes as relays to introduce diversity into a communication link. This diversity allows an increase in capacity, speed and performance of the system. The process of channel coding, named cooperative coding, explores wisely the diversity of cooperative communications. The cooperative coding can use or adapt many known techniques of coding channel as convolutional coding, turbo, LDPC, RS, etc., to reach more efficiency between two nodes. The goal of this work is to exploit the characteristics of cooperative communicationsassociated to LDPC (*Low Density Parity Check*) coding technique, with binary alphabet, to obtain simpler, reliable and efficient systems.

Key-words: Cooperative Communications, Cooperative coding, Coded Cooperation, LDPC.

Lista de Figuras

2.1 Modelo de comunicação cooperativa. 5
2.2 O canal Relay. 6
2.3 Exemplo de Cooperação Codificada. 8
2.4 Quatro tipos de cooperação entre usuários. 8

3.1 Grafo de Tanner para um código de bloco (8,4) 13
3.2 Girth do código de bloco (8,4) 14
3.3 O cálculo de a) r_{ji} e b) q_{ij} (Bernhard M.J, 2009) 18
3.4 Representação do Grafo de Tanner 20
3.5 Representação do Grafo de Tanner 21
3.6 Calculo dos coeficientes Q_{12}^0 e Q_{12}^1 24

4.1 Modelo do sistema de cooperação codificada 27
4.2 Função densidade de probabilidade gaussiana dos símbolos ± 1 29
4.3 Canal equivalente (AWGN + Desvanecimento Rayleigh) 29
4.4 Partição das palavras-códigos nos três canais 31
4.5 Cooperação codificada do código 1 com o mesmo nível de desvanecimento nos três canais 33
4.6 Cooperação codificada do código 1 com desvanecimento plano 3dB mais severo no canal fonte-relay 34
4.7 Cooperação codificada do código 1 com desvanecimento plano 3dB mais severo no canal direto 34
4.8 Exemplo de apagamento nos três canais em uma sequência de 4 bits das palavras-códigos, nas mesmas posições 35
4.9 Exemplo de apagamento nos canais, direto e fonte-destino em uma sequência de 4 bits das palavras-códigos, em posições diferentes 35
4.10 Apagamento de 10 bits nos três canais – mesma posição 36
4.11 Apagamento de 50 bits nos três canais – mesma posição 37
4.12 Apagamento de 100 bits nos três canais – mesma posição 37
4.13 Apagamento de 50 bits nos canais direto e fonte-relay(mesmas posições) 38
4.14 Apagamento de 50 bits nos canais direto e fonte-relay(posições diferentes) 38

Lista de Tabelas

3.1 Vetor recebido correspondente aos fatores f 19
3.2 Valores de R_{ij}^0, primeira iteração 22
3.3 Valores de R_{ij}^1, primeira iteração 22
3.4 Valores de Q_{ij}^0, segunda iteração 24
3.5 Valores de Q_{ij}^1, segunda iteração 24
3.6 Valores de R_{ij}^0, segunda iteração 25
3.7 Valores de R_{ij}^1, segunda iteração 25
3.8 Estimação na segunda iteração 25
3.9 Valores de Q_{ij}^0, terceira iteração 26
3.10 Valores de Q_{ij}^1, terceira iteração 26
3.11 Valores de R_{ij}^0, terceira iteração 26
3.12 Valores de R_{ij}^1, terceira iteração 26
3.13 Estimação na terceira iteração 26

4.1 Representação do esquema de Cooperação total 32

Lista de Acrônimos e Notação

BER	Bit Error Rate (taxa de erro de bit)
MIMO	Multiple–Input and Multiple–Output (multiplas entradas e multiplas saídas)
LDPC	Low-Density Parity-Check (verificação de paridade de baixa densidade)
ERB	Estação Rádio Base
TDMA	Time Division Multiple Access (múltiplo acesso por divisão de tempo)
FDMA	Low-Density Parity-Check (múltiplo acesso por divisão de frequência)
CDMA	Low-Density Parity-Check (múltiplo acesso por divisão de código)
CRC	Cyclic Redundancy Check (código de redundância cíclica)
GF	Galois field (campo de galois)
AWGN	Additive White Gaussian Noise (ruído branco gaussiano aditivo)
SNR	Signal-to-Noise Ratio (razão sinal ruído)

R	indica a taxa do código
k	indica número de bits de informação
u	indica a informação transmitida
n	indica o tamanho da palavra-código
G	indica a matriz geradora
H	indica a matriz de verificação de paridade
I	indica a matriz identidade
c	indica palavra-código transmitida
r	indica palavra-código recebida
w_r	indica o peso de linha de uma matriz
w_c	indica o peso de coluna de uma matriz
η	representa o ruído AWGN (variável aleatória gaussiana)
σ	representa o desvio padrão do ruído AWGN
γ	representa os coeficientes de desvanecimento do canal (variável aleatória Rayleigh)

Sumário

1 Introdução **1**
1.1 Organização da Dissertação 3

2 Comunicações Cooperativas **4**
2.1 Introdução 4
2.2 Comunicações Cooperativas 4
2.3 Cooperação Codificada 6
2.4 Codificação LDPC Cooperativa 9

3 Códigos de Verificação de Paridade de Baixa Densidade **10**
3.1 Introdução 10
3.2 Códigos de Bloco Corretores de Erro 10
3.3 Códigos LDPC 11
3.3.1 Descrição do Código LDPC 12
3.3.2 Representação dos códigos LDPC 13
3.3.3 Construção de Códigos LDPC 14
3.3.4 Códigos LDPC Quase-Cíclicos 15
3.4 Taxa de Erro 15
3.5 Decodificação dos códigos LDPC 16

4 Análise de Desempenho e Resultados **27**
4.1 Modelo do Sistema de Cooperação Codificada 27
4.1.1 Canal AWGN 28
4.1.2 Canal com Desvanecimento 28
4.2 Parâmetros de Simulação 30
4.2.1 Código 1 30
4.2.2 Código 2 30
4.3 Resultados 31
4.3.1 Cenário 1 32
4.3.2 Cenário 2 33
4.3.3 Cenário 3 33

4.3.4 Cenário 4 35

5 Conclusões e Perspectivas **39**

Bibliografia **41**

Capítulo 1

Introdução

Nos últimos anos, vem acontecendo uma grande evolução nas comunicações móveis. Um grande avanço nas transições das gerações das comunicações móveis (1G, 2G, 3G, 4G,...) pode ser visto no mercado consumidor (dispositivos móveis, aparelhos celulares, etc.) e na prestação de serviços de telefonia móvel, que passaram de somente a tradicional transmissão de voz para serviços de mensagem de texto, áudio, imagens e vídeos com alta definição.

Nesse contexto, surge a necessidade de exploração e descoberta de novas tecnologias capazes de fornecer estes serviços de forma eficiente e eficaz no uso do espectro e sob a restrição de energia (potência), e que apresente viabilidade de implementação (bom custo-benefício). A transmissão de conteúdos deve obedecer à limitação da largura de banda disponível e de probabilidade de erro de bit (BER - *Bit Error Rate*), para que o serviço atenda aos critérios de qualidade necessários de modo a garantir um serviço confiável e com bom desempenho. (Mataveli 2008)

Para poder atender às demandas por altas taxas de transmissão das comunicações multimídia, os sistemas celulares devem empregar algoritmos e técnicas avançadas que, além de aumentar a taxa de dados, garantam uma qualidade de serviço desejável ou aceitável para os diversos tipos de mídia. Nesse contexto, pesquisadores estão desenvolvendo novas arquiteturas de rede sem fio que se diferenciam da tradicional, baseada em comunicação ponto-a-ponto tendo o controle central realizado por uma estação base. Por exemplo, nas redes ad-hoc e nas redes de sensores, permite-se que qualquer nó da rede possa auxiliar na transmissão da informação proveniente de outros nós, estabelecendo assim a comunicação. (Hunter n.d.).

As técnicas que atualmente estão sendo pesquisadas para alcançar esse objetivo incluem processamento digital de sinais avançado, componentes do sistema (tais como codificação de fonte e canal, modulação e detecção) específicos para o ambiente sem fio, e várias formas de utilização da diversidade inerente ao sistema. A exploração dessa diversidade acaba sendo fundamental, devido à natureza do ambiente sem fio descentralizado (Blázovics, Varga, Bamford, Zanaty & Fitzek 2011),(Fitzek 2006),(Fitzek & Katz 2007), (Kristensen 2007), (Perrucci, Fitzek, Zhang & Katz 2009).

O canal de comunicação móvel no qual o sinal sem fio se propaga sofre desvanecimento por múltiplos percursos, o que implica que, na duração de uma determinada transmissão, o sinal do usuário móvel passa por variações repentinas e intensas nos valores de sua amplitude e fase. Uma maneira de amenizar o desvanecimento por múltiplos percursos é através de uma transmissão

de cópias do sinal. A diversidade torna-se, então, um método que combate diretamente os efeitos do desvanecimento(Hunter n.d.), (Hunter & Nosratinia 2006), (Nosratinia, Hunter & Hedayat 2004), (Sendonaris, Erkip & Aazhang 2003).

Diversidade espacial é conseguida fazendo-se um sinal ser transmitido por uma ou mais antenas e/ou recebido no destino por uma ou mais antenas; que estão em locais geograficamente espaçados, com desvanecimentos independentes. A composição das várias réplicas desse sinal, provenientes de diferentes canais independentes, permite a obtenção de um ganho de diversidade na recepção. Entretanto, o uso de várias antenas em um dispositivo móvel pode se tornar impraticável devido à sua dimensão reduzida.

Por outro lado, a diversidade espacial pode também ser construída de modo a permitir que dispositivos móveis usem a capacidade ociosa de outros dispositivos em estado de espera (não transmitindo ou recebendo dados) para a transmissão de seus dados de forma redundante. Nesse caso, o ganho de diversidade é obtido por meio da cooperação entre usuários pertencentes a uma dada célula.

Nos últimos anos, diversidade por cooperação tem surgido como um novo paradigma que explora a natureza de radiodifusão de sistemas de comunicação sem fio, com o intuito de simular um sistema de múltiplas antenas. Através da transmissão/processamento distribuído da informação, os benefícios obtidos até então com o uso de múltiplas antenas vêm sendo usufruídos por dispositivos com apenas uma única antena. Dessa maneira, comunicações cooperativas podem ser vistas como um sistema MIMO (*multiple-input and multiple-output*), onde as múltiplas antenas são emuladas através dos vários dispositivos com uma única antena que compõem o sistema sem fio.

Independentemente de outras formas de diversidade serem empregadas, o uso de muitas antenas transmissoras é desejável, pois provê diversidade espacial. Infelizmente, isso se torna impraticável no caso do uplink do sistema celular das redes sem fio, considerando o tamanho dos equipamentos das unidades móveis. Desse modo, torna-se necessário e essencial um estudo para implementação de novas técnicas de transmissão e processamento de sinais entre os nós terminais de uma rede sem fio. Para poder superar essa limitação, e ainda obter diversidade na transmissão da antena, utilizamos uma outra forma de gerar diversidade espacial, e o ganho de diversidade é obtido por meio da cooperação de usuários na célula. Em cada célula, cada usuário tem um "parceiro" e é responsável pela transmissão dele e do parceiro.

Assim, a comunicação cooperativa, utiliza nós intermediários como retransmissores para produzir diversidade em um enlace de comunicação ponto a ponto. Essa diversidade permite que se aumente a capacidade, a velocidade (taxa) e o desempenho do sistema de comunicação. O processo de codificação de canal que explora de forma inteligente a diversidade produzida pela comunicação cooperativa é denominado de cooperação codificada.

Para a obtenção de sistemas mais eficientes de comunicação entre dois pontos, a cooperação codificada pode utilizar ou adaptar várias técnicas conhecidas de codificação de canal, tais como a codificação convolucional, turbo, LDPC e Reed-Solomon.

O objetivo deste trabalho de pesquisa é explorar as características da comunicação cooperativa associada a códigos de verificação de paridade de baixa densidade (LDPC – *Low Density Parity Check*) com alfabeto binário, de forma a obter sistemas mais simples, confiáveis e efici-

entes. A escolha da codificação LDPC se deve a seu ótimo desempenho na correção de erro e a certa flexibilidade para o seu truncamento e decodificação. A classe de códigos LDPC permite um processo de decodificação iterativo, que faz com que o desempenho desses códigos chegue muito próximo do limite de capacidade de Shannon para canais com ruído aditivo gaussiano. A fácil implementação do codificador e do decodificador para esses códigos também aumenta o interesse pelo estudo e aplicação dos mesmos.

Pesquisadores já exploraram esta técnica de utilizar códigos LDPC em cooperação (Karkooti & Cavallaro 2008),(Duyck, Boutros & Moeneclaey 2011), (Zhao & Li 2009), (Zhao & Li 2008). Uma novidade deste trabalho é a forma que as palavras-códigos são organizadas antes do processo de decodificação, e se encontra no Capítulo 4 desta dissertação.

1.1 Organização da Dissertação

Esta dissertação é composta por cinco capítulos e está organizada da seguinte maneira:

No capítulo 2, são apresentados os conceitos de comunicações cooperativas, definições e exemplos de métodos utilizados, os benefícios da utilização em canais com desvanecimento e a cooperação usando codificação de canal.

No capítulo 3, é apresentada uma introdução aos códigos LDPC, composta da definição desses códigos, expondo-se sua estrutura, representação, construção e, por fim, a decodificação iterativa.

No capítulo 4, são apresentados os resultados obtidos da simulação do esquema de codificação LDPC utilizado, para diferentes situações de transmissão pelos canais.

Finalmente, no capítulo 5, apresentamos uma breve discussão e conclusão dos resultados obtidos e algumas sugestões para trabalhos futuros.

Capítulo 2

Comunicações Cooperativas

2.1 Introdução

Este capítulo traz uma abordagem geral das técnicas de comunicações cooperativas. A ênfase, porém, é para comunicação cooperativa com o uso de codificação de canal ou codificação cooperativa. Apesar de existirem outros esquemas e diversos ambientes cuja comunicação cooperativa pode ser empregada, por exemplo, redes de sensores, redes ad-hoc, etc., o modelo que será considerado neste trabalho, é o de um sistema de comunicações móveis, constituídos por terminais de usuários móveis e uma estação rádio base – ERB.

A ideia básica por traz desta comunicação está no fato de que o sinal enviado pelo transmissor pode ser recebido tanto pelo retransmissor quanto pelo destino (broadcast), e cada um recebe uma cópia deste sinal contaminado por ruído que diferem estatisticamente de um canal para o outro, ou seja, são independentes. A partir disso, o retransmissor, através do uso de alguma técnica de detecção, estima o sinal recebido, para minimizar a influência do ruído que foi adicionado ao sinal, ao se propagar pelo canal entre os terminais, e retransmite a estimativa do sinal recebido para o destino.(Ferro 2011)

2.2 Comunicações Cooperativas

A ideia básica da comunicação cooperativa é permitir que dispositivos móveis com uma única antena compartilhem suas antenas de modo a criar um sistema de múltiplas entradas e múltiplas saídas (MIMO). Esses transmissores interagem entre si para, em conjunto, transmitirem suas informações.

O canal de comunicações sem fio sofre desvanecimento, isto é, o sinal pode ser atenuado de forma significativa e variada no curso de uma dada transmissão. A transmissão de cópias do mesmo sinal produz diversidade, fazendo com que os efeitos do desvanecimento possam ser minorados. Em particular, a comunicação cooperativa gera diversidade espacial, fazendo uso da transmissão de sinais de diferentes localizações, obtendo-se assim no receptor diferentes versões desvanecidas de forma independente do sinal. No sistema móvel, há limitações em termos de consumo de potência e do tamanho das unidades transmissoras, o que impossibilita o uso de diversas antenas transmissoras num único equipamento. Nesses casos, os terminais móveis

podem se beneficiar do uso de cooperação, compartilhando suas antenas com outros terminais a fim de alcançar ganho em diversidade, aumento da taxa de transmissão ou da duração da bateria (Khatir 2007).

A Figura 2.1 mostra um esquema de comunicação cooperativa que utiliza dois usuários e um destinatário. Nesse sistema, cada usuário transmite seus dados e também atua como retransmissor gerando assim diversidade espacial.

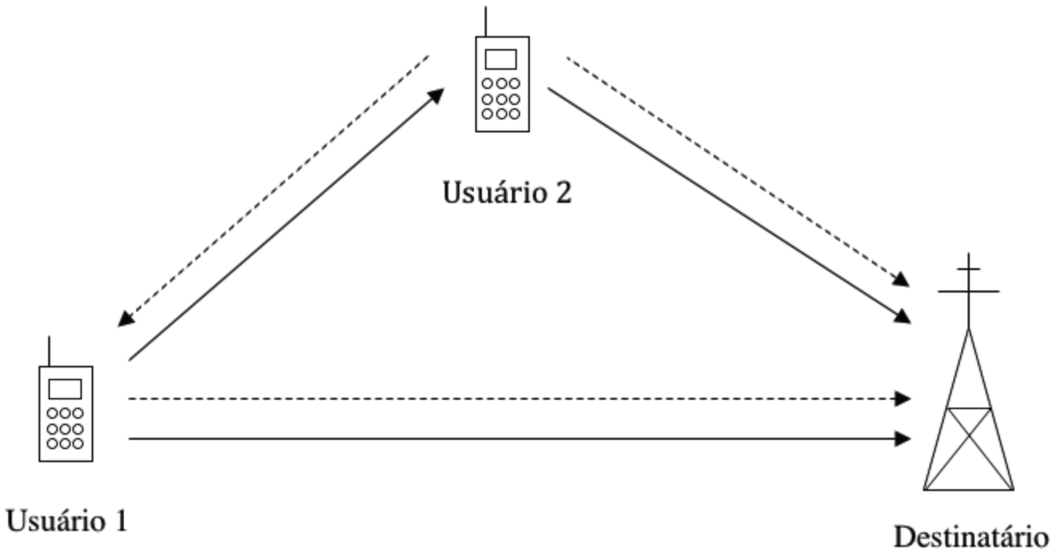

Figura 2.1: Modelo de comunicação cooperativa.

A cooperação entre os usuários faz com que a eficiência espectral do sistema aumente porque, devido à diversidade, a taxa de codificação do canal pode ser aumentada. Além disso, a potência transmitida de cada usuário é reduzida pelo mesmo motivo.

Na comunicação cooperativa, caminhos independentes entre o usuário e a estação base são formados através de um canal relay, Figura 2.2. Nesse modelo, o transmissor F envia um sinal S, que é corrompido por ruído, e uma versão atenuada é recebida pelo destino D e pelo relay R. O relay então transmite um outro sinal S_1 para o destino, de acordo com o que ele recebeu da fonte. Esse modelo pode ser decomposto em um canal broadcast (F transmite, R e D recebem), e um canal de múltiplo acesso (F e R transmitem, D recebe), que pode ser por divisão em slots de tempo (TDMA - *Time Division Multiple Access*), frequência (FDMA - *Frequency Division Multiple Access*) ou por código (CDMA - *Code Division Multiple Access*). Cover e El Gamal (Cover & Gamal 1979) calcularam a capacidade de informação desse canal relay e descobriram que é o mínimo das taxas de transmissões dos canais broadcast e múltiplo acesso. A capacidade do modelo de canal relay é melhor que a capacidade individual dos canais entre F e D.

O canal relay pode ser visto como um canal auxiliar do canal direto entre a fonte e o destino. Um aspecto chave do processo de comunicação cooperativa é o processamento do sinal recebido da fonte e do relay. O processamento no relay se difere de acordo com o protocolo

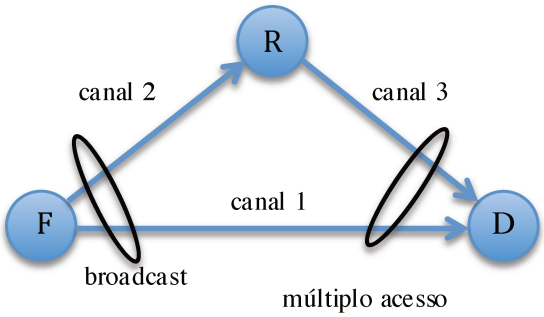

Figura 2.2: O canal Relay.

utilizado. Alguns métodos de cooperação entre usuários são método de detecção e retransmissão, método de amplificação-e-retransmissão e método de cooperação codificada. (Gupta, Kramer & Wijngaarden 2004)

O método de detecção e retransmissão, o relay recebe o sinal da fonte, detecta-o, tenta remover o ruído e as interferências reenviando-o para o destinatário. O destinatário então combina o sinal recebido direto da fonte com o sinal retransmitido pelo relay e faz a detecção da informação transmitida.

No método de amplificação e retransmissão o relay recebe uma versão ruidosa do sinal enviado pela fonte, que é então amplificado e retransmitido para o destinatário, sem nenhum tipo de tratamento adicional. O destinatário, por sua vez, combina o sinal recebido direto da fonte com o sinal retransmitido pelo relay e faz a detecção da informação transmitida.

O método de cooperação codificada integra a cooperação com a codificação de canal. Na cooperação codificada, porções diferentes da palavra-código de cada usuário são enviadas via canais distintos com desvanecimento. A ideia básica desse método é cada usuário transmitir redundância que serão combinadas no destinatário para realização da decodificação da informação transmitida, ou seja, no destino, ambas as palavras códigos são usadas a fim de obter a melhor estimativa da informação original transmitida pela fonte (Karkooti & Cavallaro 2008), (Liu, Sadek, Su & Kwasinski 2009), (Laneman, Tse & Wornell 2004), (Zimmermann, Herhold & Fettweis 2005). E essa redudância pode ser utilizada na detecção e correção de erros introduzidos pelo canal, melhorando o desempenho do sistema. Esse método é o foco dos estudos deste trabalho.

2.3 Cooperação Codificada

Nesta seção introduziremos a cooperação codificada, que é cooperação integrada com codificação de canal. A ideia fundamental por trás da cooperação codificada é que cada usuário tenta transmitir redundância incremental para seu parceiro. Sempre que não é possível, os usuários automaticamente retornam ao modo de não cooperação. Isso é administrado automaticamente pelo código, de maneira eficiente, sem a necessidade de realimentação entre os usuários. Podemos ressaltar duas características. A primeira é que cooperação ocorre, particionando-se a palavra código do usuário de modo que parte é transmitida pelo próprio usuário e o restante é

transmitido pelo parceiro. E a segunda é que o parceiro realiza detecção e correção de erros para evitar a propagação dos mesmos. A propagação de erros diminui o desempenho, especialmente quando o canal entre os usuários é ruim.

Essas características são possíveis de implementar de maneira natural e simples, por um método que usa códigos corretores de erro. Além disso, a incorporação de cooperação com codificação de canal permite certos graus de flexibilidade. De acordo com a taxa do código, a integração entre os usuários cooperantes pode ser controlada e adaptada às condições de canal.

A Figura 2.3 apresenta um modelo de codificação cooperativa, onde temos dois usuários parceiros na cooperação e uma estação rádio base receptora. A cooperação codificada envia diferentes porções da palavra-código de cada usuário por canais independentes com desvanecimento. Ao bloco de informação produzido por cada usuário é adicionado um código de redundância cíclica (CRC). Então, esse bloco é codificado através de um codificador de canal projetado para este fim. Os usuários então dividem suas palavras-códigos formadas em dois segmentos, com N_1 e N_2 bits. Assim, a palavra-código original possui $N_1 + N_2$ bis. Note que cada usuário dispõe de dois quadros para acomodar uma palavra código.

No primeiro quadro, cada usuário transmite uma fração de N_1 bits de sua palavra código. Cada usuário também tenta decodificar a transmissão de seu parceiro. Se a tentativa tiver sucesso, o segundo quadro é preenchido com os N_2 bits do seu parceiro, obtido através de uma recodificação dos bits de informação decodificados. Note que o sucesso acima mencionado é determinado pela verificação usando o código CRC. Caso a tentativa seja frustrada, o usuário transmite sua própria porção de N_2 bits. (Chakrabarti, Erkip, Sabharwal & Aazhang 2007) (Ferro 2011)

Assim, cada usuário sempre transmite um total de $N = N_1 + N_2$ bits em dois quadros. O nível de cooperação é definido como sendo a razão N_2/N. Note que os usuários atuam de forma independente para o preenchimento do segundo quadro, sem conhecimento se o conteúdo do primeiro quadro foi corretamente decodificado.

Existem assim 4 tipos de cooperação entre usuários (ilustrados na Figura 2.4):

a) ambos usuários cooperam,

b) nenhum usuário coopera,

c) usuário 1 coopera mas o usuário 2 não,

d) usuário 2 coopera mas o usuário 1 não.

No primeiro caso, ambos os usuários decodificam com sucesso a informação um do outro, de modo que usam o segundo quadro para transmitir a informação do parceiro. No segundo caso, nenhum do usuários conseguem decodificar a informação do parceiro e o sistema passa ao modo de não cooperação. No terceiro, o U1 (usuário 1) decodifica corretamente a informação do U2 (usuário 2), mas o U1 não o faz. Consequentemente, nenhum usuário transmite a informação de U1, ambos os quadros ficam disponíveis para os dados de U2. Os dois sinais independentes são combinados antes do processo de decodificação. E o último caso é similar ao terceiro, mas invertido, em que somente os bits de U1 são transmitidos [8].

Vários tipos de codificação de canal podem ser utilizados na cooperação codificada: codificação de bloco, codificação convolucional, codificação LDPC, codificação turbo, etc. Note que

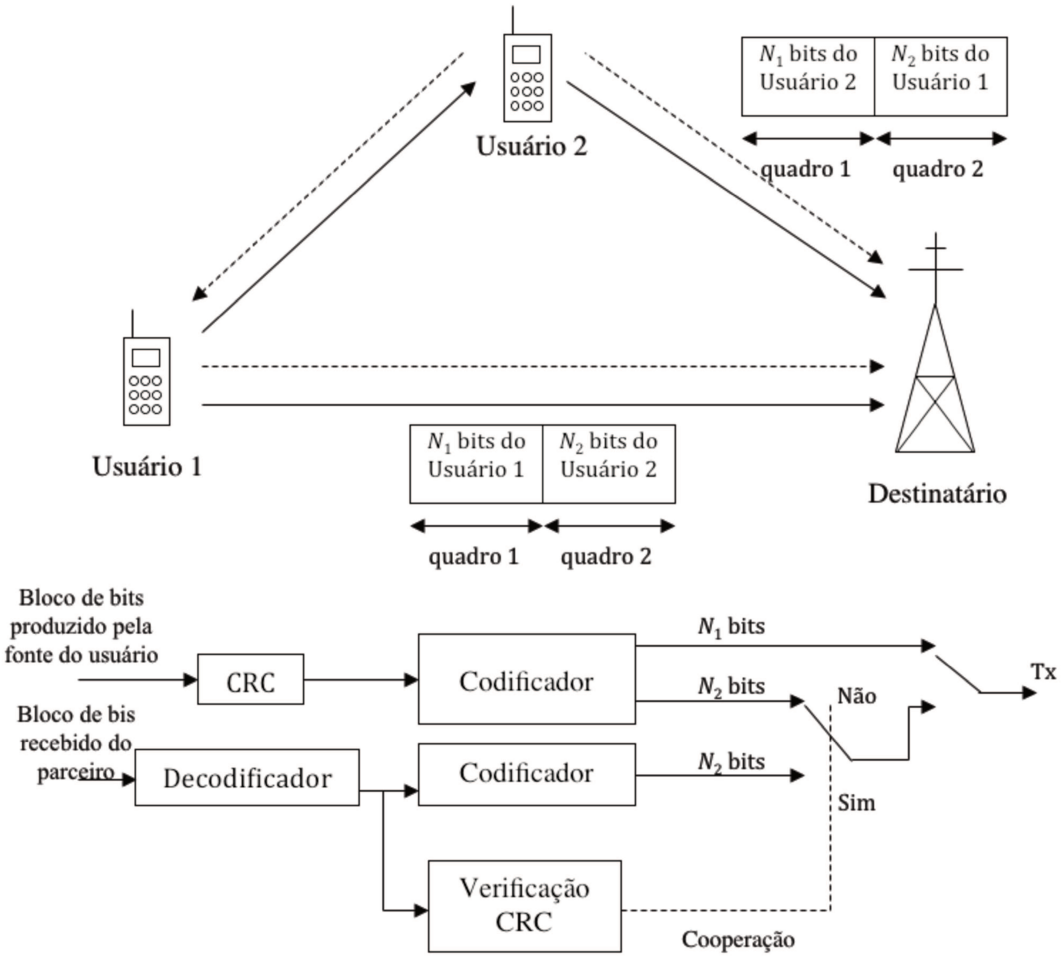

Figura 2.3: Exemplo de Cooperação Codificada.

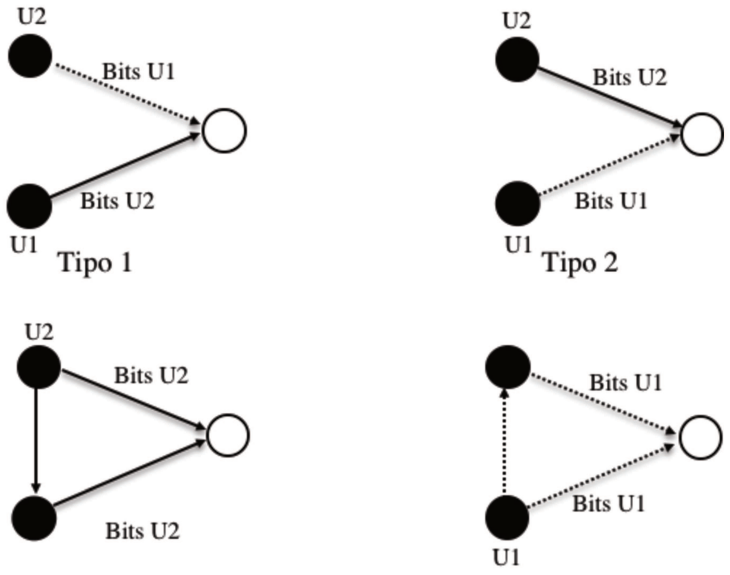

Figura 2.4: Quatro tipos de cooperação entre usuários.

é possível tirar proveito da independência (ou descorrelação) entre os canais utilizados (direto e com retransmissão) para simplificar o esquema de codificação. Além disso, diversas variações desse esquema de codificação podem ser propostas e analisadas.

2.4 Codificação LDPC Cooperativa

Códigos de verificação de paridade de baixa densidade, ou simplesmente códigos LDPC (*Low Density Parity Check*), podem ser construídos de tal forma que se permita uma partição de suas palavras-códigos em blocos decodificáveis que podem ser utilizados em sistemas de cooperação codificada. (Duyck et al. 2011) Os códigos LDPC geralmente são especificados por sua matriz H de verificação de paridade esparsa. Assim, técnicas algébricas de construção dessas matrizes permitem que se obtenham códigos apropriados para serem utilizados em comunicação cooperativa. Por exemplo, códigos LDPC construídos a partir de quadrados latinos (definição e conceito podem ser encontrados em: (Alegri 2006)) são uma classe de códigos candidata a essa aplicação. No próximo capítulo, introduzimos a classe de códigos LDPC binários.

Note, entretanto, que a cooperação codificada baseada em códigos LDPC pode também utilizar códigos não binários, tais como os códigos definidos sobre anéis ou campos finitos de inteiros. Em (Zhao & Li 2009), (Zhao & Li 2008), temos exemplos de codificação cooperativa usando códigos LDPC. Neste trabalho, analisaremos esquemas de codificação LDPC cooperativa que sejam simples e eficientes, fazendo uso das características peculiares da comunicação cooperativa baseada em um sistema com apenas um retransmissor, ou seja, em um sistema com dois canais distintos e independentes. Visamos, portanto, a utilização de códigos LDPC que permitam sua partição em dois blocos, com a preservação de parte da capacidade de correção de erro na decodificação com a palavra-código reduzida, além de permitir a decodificação da palavra-código reconstruída na recepção.

Capítulo 3

Códigos de Verificação de Paridade de Baixa Densidade

3.1 Introdução

Neste capítulo introduziremos os códigos de verificação de paridade de baixa densidade (LDPC - *Low Density Parity Check*), que possuem matriz de verificação de paridade esparsa. A descrição desta classe de códigos será feita em termos de sua construção, codificação e decodificação utilizando algoritmos iterativos.

3.2 Códigos de Bloco Corretores de Erro

Códigos de bloco corretores de erros inserem bits de redundância (ou símbolos) na informação digital transmitida. Esses bits de redundância são usados para detectar e/ou corrigir possíveis erros ocorridos durante a transmissão por um canal ruidoso. Na codificação, a informação é dividida em blocos de comprimento fixos de k bits. O codificador então transforma os blocos de k bits em uma entrada em blocos de n bits de comprimento, sendo $n > k$ para garantir a presença de redundância necessária para detecção e/ou correção dos erros. A taxa de codificação é expressa por $R = k/n$. A mensagem de entrada contendo k bits, fará com que existam 2^k possibilidades de mensagens. Os blocos de n bits é denominado de uma palavra-código.

Um código de bloco de comprimento n e 2^k palavras-código é denominado de um código linear (n, k) se e somente se suas 2^k palavras-código formarem um subespaço do espaço vetorial de todas as n-uplas sobre o campo GF(2). Em outras palavras, um código de bloco é linear se, e somente se, a soma de duas palavras-código for também uma palavra-código. Esta propriedade permite representar um código de bloco linear através de uma matriz geradora G de dimensão igual a k linhas por n colunas, formada por vetores linha linearmente independentes. (Gomes 2003)

O codificador gera uma palavra-código c multiplicando o vetor de informação u em sua entrada pela matriz geradora G, ou seja, fazendo $c = uG$. Para qualquer matriz geradora G de dimensão $k \times n$, existe uma matriz H de dimensão $(n-k) \times n$, tal que, qualquer vetor gerado por G é ortogonal às linhas de H. Quando o decodificador recebe um vetor $\mathbf{r} = \mathbf{c} + \mathbf{n}$, onde $\mathbf{n}$ é o vetor erro produzido pelo canal, ele verifica, se o vetor recebido é uma palavra-código,

utilizando a matriz H. Este produto gera um vetor denominado de síndrome $\mathbf{s}$, se $\mathbf{s} = 0$ então $\mathbf{r}$ é uma palavra-código, isto é, não ocorreu erro ou ocorreu um erro não detectável em $\mathbf{r}$. Se $\mathbf{s} \neq 0$ então $\mathbf{r}$ não é uma palavra-código, isto é, ocorreu erro detectável em $\mathbf{r}$.

Para se obter a matriz H a partir da matriz geradora G, colocamos G na forma sistemática através de combinações lineares entre suas linhas obtendo:

$$G = [P_{k\times(n-k)} \quad I_k] = \begin{bmatrix} p_{11} & p_{12} & \dots & p_{1n-k} & 1 & 0 & \dots & 0 \\ p_{21} & p_{12} & \dots & p_{1n-k} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{k1} & p_{k2} & \dots & p_{kn-k} & 0 & 0 & \dots & 1 \end{bmatrix}_{k\times n} \tag{3.1}$$

Assim, a forma da matriz H é obtida fazendo:

$$H = [P_{k\times(n-k)} \quad I_k] = \begin{bmatrix} 1 & 0 & \dots & 0 & p_{11} & p_{21} & \dots & p_{k1} \\ 0 & 1 & \dots & 0 & p_{21} & p_{22} & \dots & p_{k1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & p_{1n-k} & p_{2n-k} & \dots & p_{kn-k} \end{bmatrix}_{(n-k)\times n} \tag{3.2}$$

O peso de Hamming $w(\mathbf{v})$ de um vetor $\mathbf{v}$ é definido como o número de componentes diferentes de zero de $\mathbf{c}$. Enquanto que a distância de Hamming $d(\mathbf{v},\mathbf{x})$ entre dois vetores $\mathbf{v}$ e $\mathbf{x}$ é definida como o número de posições em que estes vetores diferem.

Se C é um código de bloco linear, então, a distância mínima de C é definida por $d_{min} = min\{d(v,x) : v, x \in C, v \neq x\}$. Como $v + x = z$ também é uma palavra-código do código linear C, então $d_{min} = min\{w(z) : z \in C, z \neq 0\} = w_{min}$, ou seja, a distância mínima de um código de bloco linear é igual ao peso mínimo de suas palavras-código não nulas. (Lin & Costello 2004)

Se C é um código linear de bloco com matriz de verificação de paridade H, então se nenhuma $d-1$ ou menos colunas de H somam-se zero, o código possui peso (distância) mínimo pelo menos igual a d. Por outro lado, o peso (distância) mínimo de C é igual ao menor número de colunas de H que somam-se zero. A capacidade de detecção e correção de erro de um código C está diretamente ligada a distância mínima d_{min}. Note que para um código de bloco C, nenhum padrão de erro com $d_{min} - 1$ ou menos erros mudará uma palavra-código em outra. Portanto, um código de bloco C com distância mínima d_{min} é capaz de detectar todos os padrões de erro com $d_{min} - 1$ ou menos erros. Observe ainda que um código de bloco com distância mínima d_{min} corrige todos os padrões de erro de $t = [(d_{min} - 1)/2]$ ou menos erros.

3.3 Códigos LDPC

Os códigos corretores de erro permitem que a comunicação ponto-a-ponto possa ser realizada virtualmente livre de erro em um canal ruidoso. Além disso, estes códigos melhoram a capacidade de um sistema de comunicações permitindo a transmissão de dados a altas taxas

de transmissão com uma alta eficiência de potência de transmissão. Em 1948, Claude Shannon mostrou que era possível otimizar a energia e o tempo de transmissão de dados em um canal de comunicação através de um esquema de codificação correto. Desde então, o desafio tem sido desenvolver sistemas de codificação que possuam desempenho próximo da capacidade de canal, sem limitar a vazão de dados ou adicionar grandes atrasos na transmissão.

Até o início da década de 1990, os melhores sistemas práticos de codificação tinham desempenho entre 3 e 5 dB abaixo da capacidade de canal. Entretanto, em 1993, Claude Berrou e Alain Glavieux apresentaram os códigos turbo, que forneciam 3 dB de ganho sobre os melhores esquemas de codificação conhecidos na época. (Moreira & Farrell 2006) Em outras palavras, os códigos turbo foram os primeiros códigos a terem um desempenho muito perto do limitante de Shannon para a capacidade de canal.

As pesquisas em codificação então voltaram-se para a área de decodificadores iterativos por decisão suave e para a busca de códigos de baixa complexidade. Estes esforços levaram à redescoberta dos códigos de verificação de paridade de baixa densidade - LDPC, proposto por Robert Gallager em sua tese de doutorado em 1960, mas esquecidos e ignorados por longo tempo devido a alta complexidade computacional necessária para implementação. Robert Tanner, em 1981, generalizou os códigos LDPC e desenvolveu um método gráfico de representação destes códigos, que ficaram conhecidos como grafos de Tanner ou grafos bipartites. Apesar destas iniciativas, somente em meados de 1990, com David MacKay, Michael Luby e outros aconteceu o ressurgimento definitivo dos códigos LDPC. (*LDPC Coded Modulation – Ceragon* 2009)

A decodificação dos códigos LDPC também segue um processo iterativo como nos códigos turbo, mas apresenta algumas vantagens sobre estes tais como o paralelismo na decodificação e operações computacionais de baixa complexidade. O código LDPC é construído tomando por base a matriz de verificação de paridade H com uma quantidade pequena e esparsa de elementos 1's em suas linhas e colunas. A codificação é feita usando equações obtidas da matriz H para gerar os bits de verificação de paridade. A decodificação é feita usando entradas suaves e essas mesmas equações para gerar novas estimativas dos valores enviados. Este processo é repetido de modo iterativo resultando em um decodificador poderoso. Códigos LDPC só alcançam desempenho próximo à capacidade de canal de Shannon quando o comprimento destes códigos é muito grande (n da ordem de milhares de símbolos). Por outro lado, a complexidade dos códigos LDPC é proporcional a n^2.

3.3.1 Descrição do Código LDPC

Os códigos LDPC são uma classe de códigos de bloco lineares definida por uma matriz de verificação de paridade H onde suas linhas e colunas caracterizam-se por uma quantidade pequena de '1' quando comparada com '0'. A quantidade w_r de 1's em uma linha da matriz H é denominada de peso da linha, enquanto que a quantidade w_c de 1's em uma coluna é denominada de peso da coluna, onde $w_r \ll n$ e $w_r \ll n - k$.

Um código (n, k, w_c) LDPC é regular se os pesos de todas as linhas e todas as colunas são constantes, onde $w_r = w_c n/(n-k)$. Quando o código não obedece essas condições ele é irregular. Os códigos irregulares apresentam desempenho superior aos regulares. A taxa de codificação é definida por

$$r_c = \frac{k}{n} = \frac{w_r - w_c}{w_r} = 1 - \frac{w_c}{w_r} \tag{3.3}$$

3.3.2 Representação dos códigos LDPC

Os códigos LDPC podem ser representados pela suas respectivas matrizes de verificação de paridade H esparsas. Entretanto, eles também podem ser representados por um grafo bipartido, também conhecido como grafo de Tanner. (Bernhard M.J. Leiner 2009)

Um grafo bipartido é um grafo composto de dois conjuntos de nós, denominados de nós de verificação (*check nodes*) e nós de variável (*variable nodes*), representando as linhas e as colunas da matriz H, respectivamente. O grafo possui $n - k$ nós de verificação e n nós de variável. Um nó de verificação f_i é conectado a um nó de variável v_j se o elemento h_{ij} da matriz H for 1. A Figura 3.1 mostra o grafo de Tanner correspondente a uma matriz de paridade H para um código (8,4) de bloco linear,

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Os nós de verificação f_0, f_1, f_2 e f_3 representam as quatro linhas da matriz, e os nós de variável

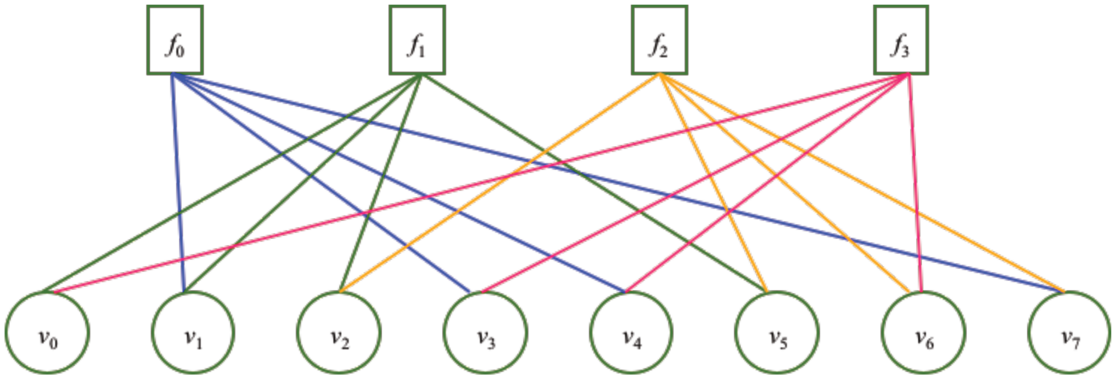

Figura 3.1: Grafo de Tanner para um código de bloco (8,4)

$v_0, v_1, v_2, v_3, v_4, v_5, v_6$ e v_7 a suas oito colunas. O número de arestas em cada nó de verificação é igual ao peso de linha w_r e o número de arestas que partem dos nós de variável equivale ao peso de coluna w_r da matriz de verificação de paridade.

Um ciclo (girth) de um código LDPC é formado em um grafo de Tanner pelo menor caminho iniciando em um nó e terminando no mesmo nó. (Malema 2007) O comprimento do ciclo é dado pelo número de arestas deste caminho. A Figura 3.2 mostra um ciclo formado no código de bloco (8, 4). Dessa forma, na Figura acima, temos que o código de bloco (8, 4) possui ciclo máximo de tamanho igual a 6 e um ciclo mínimo (*girth*) de tamanho igual a 4. Na prática, ao se projetar um código LDPC, busca-se evitar a existência de ciclos curtos de forma a melhorar o desempenho do algoritmo de decodificação denominado de *Belief Propagation*.

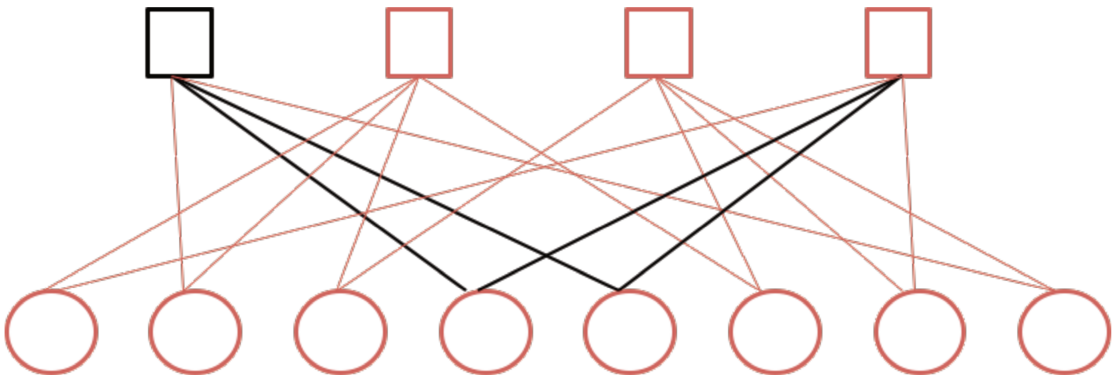

Figura 3.2: Girth do código de bloco (8,4)

3.3.3 Construção de Códigos LDPC

Existem vários algoritmos diferentes para a construção de códigos LDPC. A construção de um bom código LDPC não é um problema difícil, uma vez que matrizes H construídas de forma completamente aleatória produzem bons códigos com alta probabilidade de corrigirem erros. Entretanto, tais códigos geralmente possuem um processo de codificação bastante complexo.

A forma mais simples de projetar um código LDPC (n, k) consiste na construção da matriz de verificação de paridade que cumpra um conjunto requisitos pretendido, como por exemplo, definir um código regular ou irregular, ou ainda, garantir um dado ciclo mínimo.(Shokrollahi 2003) Obviamente, para qualquer conjunto de especificações existe um conjunto de códigos LDPC que as cumprem. A construção da matriz H é feita seguindo algumas regras que tentam maximizar a probabilidade do código obtido possuir um bom desempenho. No entanto, com essas regras não temos qualquer garantia de que isso de fato aconteça.

Makay e Neal(MacKay 1999), (MacKay & Neal 1997), (Johnson 0000) apresentaram um algoritmo para gerar matrizes H esparsas de forma semi-aleatória de códigos LDPC. Os modos para geração da matriz H são as seguintes:

1. A matriz H é gerada partindo de uma matriz toda nula de dimensões $(n - k) \times n$ e invertendo-se (0 para 1) w_c bits em cada coluna de modo aleatório (o código assim gerado é irregular);

2. A matriz H é gerada criando aleatoriamente colunas de peso de Hamming w_c;

3. A matriz H é gerada criando aleatoriamente colunas de peso de Hamming w_c e procurando uniformizar ao máximo o peso de Hamming w_r de cada linha;

4. A matriz H é gerada com colunas de peso de Hamming w_c, linhas de peso de Hamming w_r, e não possuindo quaisquer duas colunas com mais de um 1 em posição comum;

5. A matriz H é gerada de acordo com o procedimento anterior, mas tendo como objetivo a maximização do ciclo mínimo (*girth*) do código;

6. A matriz H é gerada de acordo com o procedimento referido em (4) procurando obter uma matriz H de característica máxima, de preferência na forma $H = [H_1|H_2]$ com H_1 ou H_2 invertível.

Note, entretanto, o processo de construção de um bom código LDPC não se resume a se

obter uma matriz H, mas sim de se obter um codificador e um decodificador eficientes e de simples implementação.

Sendo os códigos LDPC códigos de bloco lineares, podemos obter uma matriz geradora como foi feito na Seção 3.2 deste trabalho ($v = uG$). Entretanto, os métodos utilizados na construção de códigos LDPC firmam-se na obtenção da sua matriz de verificação de paridade H. Na maioria das vezes, a matriz H obtida não é sistemática nem de posto completo. A matriz H pode ser colocada na forma sistemática utilizando o método de Gauss, tornando a obtenção da matriz G muito simples e direta.

3.3.4 Códigos LDPC Quase-Cíclicos

Códigos LDPC quase-cíclicos (QC) são formados por uma matriz H onde as linhas ou colunas em uma sub-matriz componente possui conexões similares e cíclicas. Por causa da estrutura quase cíclica, os códigos podem ser codificados de modo eficiente através de registradores de deslocamentos; e a arquitetura do decodificador requer simplesmente mecanismos de geração de endereços, usando menos memória e acesso de memoria localizada (Malema 2007). Um código QC pode ser formado concatenando sub-matrizes formadas por deslocamentos circulares com ou sem matrizes de zeros. Assim, a estrutura da matriz H é dada por:

$$H = [A_1, A_2, \ldots, A_k] \tag{3.4}$$

onde A_i é uma submatriz circulante, isto é, uma submatriz onde suas linhas são obtidas através de i deslocamentos circulares de uma dada sequência binária.

A matriz H pode então ser formada por submatrizes I_x identidades de dimensão p identidade deslocadas ciclicamente, enquanto que O é uma submatriz nula, também de dimensão p, sendo p um número inteiro primo.

$$H = \begin{bmatrix} I_{11} & 0 & 0 & 0 & I_{12} & I_{13} & 0 & I_{14} \\ 0 & I_{21} & I_{22} & I_{23} & 0 & 0 & I_{24} & 0 \\ I_{31} & I_{32} & 0 & I_{33} & 0 & 0 & 0 & I_{34} \\ 0 & I_{41} & I_{42} & 0 & I_{43} & I_{44} & 0 & 0 \\ 0 & 0 & I_{51} & 0 & 0 & I_{52} & I_{53} & I_{54} \\ I_{61} & 0 & 0 & I_{62} & I_{63} & 0 & I_{64} & 0 \end{bmatrix} \tag{3.5}$$

3.4 Taxa de Erro

Embora parâmetros como *girth* possam ser usados como medida do desempenho de decodificação, eles não mostram quantos erros o código pode corrigir. Também um código com um *girth* melhor não garante melhor performance que um com um *girth* menor. Os códigos LDPC são avaliados usando desempenho de taxa de erro de bit (BER) sobre um dado canal com um tipo de modulação.

Os canais são descritos por modelos matemáticos tornando fácil o projeto de esquemas aceitáveis de codificação e modulação. O canal AWGN é um dos modelos mais simples. A quantidade de ruído em qualquer instante de tempo pode ser descrita como uma variável aleatória n de

modo que os símbolos no canal são representados por $y_i = u_i + n_i$, onde u_i é o $i-$ésimo símbolo transmitido. O ruído Gaussiano tem densidade espectral de potência unilateral N_0 que depende da variância σ^2, através da expressão $N_0 = 2\sigma^2$.

3.5 Decodificação dos códigos LDPC

O algoritmo usado para a decodificação de códigos LDPC foi descoberto de forma independente por diversos pesquisadores (Moreira & Farrell 2006) e, por isso, possui vários nomes diferentes, tais como, *belief propagation*, *message passing*, *soma-produto*, etc. O algoritmo soma-produto (SPA - *Sum-Product Algorithm*) é uma poderosa ferramenta para a decodificação de códigos LDPC, sendo baseado no cálculo das razões de verossimilhança associadas com cada bit de informação a partir de informações fornecidas pelas equações de verificação de paridade disjuntas.(Abrantes 2005) Em outras palavras, este algoritmo estima a probabilidade a *posteriori* de cada bit em função da palavra-código recebida e das equações de paridade obtidas a partir da matriz H. O algoritmo produzirá de forma exata as probabilidades a posteriori de todos os bits se o grafo bipartido de Tanner (Abrantes 2005) construído a partir da matriz H, não contiver ciclos.

Os M nós de verificação correspondem à paridade enquanto que os N nós variáveis representam os bits da palavra-código. O algoritmo estima a palavra-código atualizando iterativamente as informações trocadas pelos nós do grafo de Tanner. Os nós de verificação estimam a probabilidade de uma equação de verificação de paridade ser satisfeita dada a mensagem, ou seja, os nós de verificação calculam a confiabilidade do bit utilizando estimações dos nós de variáveis adjacentes. Os nós de variáveis estimam a probabilidade de um dado bit ser 0 ou 1 com base no bit recebido e a partir de um valor de probabilidade inicial.

O algoritmo de decodificação é normalmente implementado no domínio logarítmo para simplificar as operações aritméticas. Assim, as operações de multiplicação e divisão são substituídas por adição e subtração respectivamente.

Considerando a decodificação por decisão suave (*soft decision algorithm*), temos que o objetivo do algoritmo SPA é maximizar a probabilidade a *posteriori* de um bit c_n, da palavra-código c, ser 1 ou 0, dado que a palavra recebida foi y, ou seja, pretendemos calcular:

$$P_r[c_n = 0|y] \tag{3.6}$$

$$P_r[c_n = 1|y] \tag{3.7}$$

Antes de apresentarmos o algorítmo, vamos apresentar algumas notações:

- $p_n = P_r[c_n = 0|y_n]$ com y_n sendo o n-ésimo símbolo da palavra recebida y;
- $c_{kj} \rightarrow k$-ésimo bit da j-ésima equação de teste de paridade envolvendo c_n;
- q_{ij} é a mensagem enviada pelo nó de variavel c_i ao nó de verificação f_j. Cada mensagem contém o par $q_{ij}(0)$ e $q_{ij}(1)$ que indica a confiabilidade de y_i ser "0" ou "1".

- $r_j i$ é a mensagem enviada pelo nó de verificação f_j para o nó de variável c_i. O par $r_{ji}(0)$ e $r_{ji}(1)$ indica a atual confiabilidade de y_i ser 0 ou 1, respectivamente.

O algoritmo é iniciado com os valores de Q_{ij}^x que são a probabilidade a priori dos símbolos denotados por f_j^x, que é a probabilidade de que o j-ésimo símbolo seja igual a x. Esta informação depende do canal empregado no modelo. Para o caso do canal Gaussiano esta probabilidade se estima com a função de distribuição gaussiana de probabilidade.

O processo de decodificação por decisão suave do algoritmo SPA pode ser dividido nos seguintes passos (Gallager 1963):

Passo 1: Todos os nós de variável enviam suas mensagens q_{ij} para os nós de verificação. Como estas informações ainda não podem ser calculadas faz-se $q_{ij}(1) = p_n$ e $q_{ij}(0) = 1 - p_n$.
Passo 2: Os nós de verificação calculam suas mensagens respostas r_{ji} a partir das mensagens q_{ij} recebidas:

$$r_{ji}(0) = \frac{1}{2} + \frac{1}{2} \prod_{i' \in V_i \setminus i} (1 - 2q_{i'j}(1)) \tag{3.8}$$

e

$$r_{ji}(1) = 1 - r_{ji}(0) \tag{3.9}$$

A equação para $r_{ji}(0)$ usa o seguinte resultado de Gallager (Bernhard M.J. Leiner 2009):
Para uma sequência de M dígitos binários independentes a_i com uma probabilidade p_i para $a_i = 1$, a probabilidade de toda a sequência conter um número par de 1's é:

$$P_{par} = \frac{1}{2} + \frac{1}{2} \prod_{i=1}^{M} (1 - 2p_i) \tag{3.10}$$

Então, os nós de verificação calculam a probabilidade de existir um número par de 1 's entre os nós de variável com exceção de c_i (significado de $V_{j\setminus i}$). Esta probabilidade é igual a probabilidade $r_{ji}(0)$ de c_i ser um 0.

Este passo e a informação utilizada para o calculo da resposta está ilustrado na Figura 3.3 a seguir.
Passo 3: Os nós de variável atualizam suas mensagens respostas para os nós de verificação, segundo:

$$q_{ij}(0) = K_{ij}(1 - P_i) \prod_{j' \in C_i \setminus j} r_{j'i}(0)) \tag{3.11}$$

e

$$q_{ij}(1) = K_{ij} P_i \prod_{j' \in C_i \setminus j} r_{j'i}(1)) \tag{3.12}$$

onde K_{ij} são escolhidos de forma a $q_{ij}(0) + q_{ij}(1) = 1$, $C_{i\setminus j}$, são todos os nós de verificação exceto f_j. Este passo também está ilustrado na Figura 3.3.

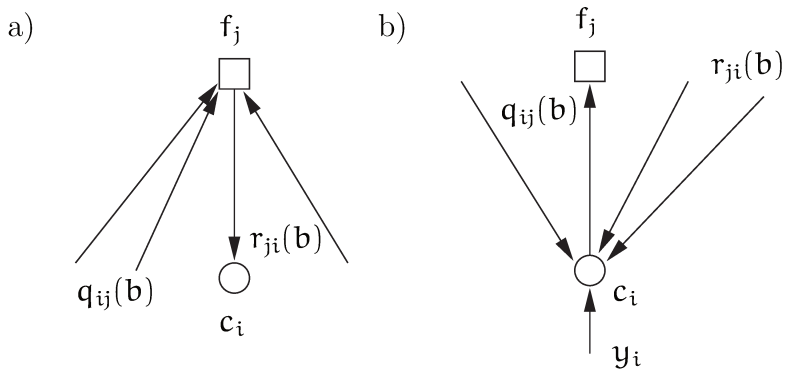

Figura 3.3: O cálculo de a) r_{ji} e b) q_{ij} (Bernhard M.J, 2009)

Os nós de verificação também atualizam suas estimativas $\hat{c}_i$ atuais de suas variáveis c_i fazendo o cálculo das probabilidades para 0 e 1 e votando na maior, isto é, calculando

$$Q_{ij}(0) = K_{ij}(1 - P_i) \prod_{j' \in C_i \setminus j} r_{j'i}(0)) \tag{3.13}$$

e

$$Q_{ij}(1) = K_{ij} P_i \prod_{j' \in C_i \setminus j} r_{j'i}(1)) \tag{3.14}$$

onde a informação de cada nó de verificação utilizada é:

$$\hat{c}_i = \begin{cases} 1, & \text{se} \quad x \leq 0, \\ 0, & c.c \end{cases} \tag{3.15}$$

Se as estimativas da palavra-código satisfazem as equações de verificação de paridade, o algoritmo termina. Caso contrário, o término é forçado pela definição do número máximo de iterações.
Retorna ao passo 2.

A estabilidade numérica deste algoritmo pode ficar comprometida devido às várias multiplicações de probabilidades. Isto é, os resultados das multiplicações podem se aproximar muito de zero para valores grandes do comprimento do bloco.

A seguir, um exemplo de decodificação retirado de (Moreira & Farrell 2006):
Suponha que temos uma matriz de paridade H de dimensão 8×12 que caracteriza um código de blocos linear C_b (12,4), de taxa R_c=1/3, cuja matriz geradora G está na forma sistemática:

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{8\times 12} \tag{3.16}$$

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}_{4\times 12} \tag{3.17}$$

O procedimento para geração das palavras-código é dada pela equação $c = mG$, onde m é o vetor informação e c a palavra-código. A palavra-código deve satisfazer a equação da síndrome $cH^T = 0$. O vetor informação transmitido é m =(1 0 0 0) que resulta na palavra-código c =(1 1 1 1 1 0 0 0 1 0 0 0). A palavra-código é convertida para sua representação polar z =(1 1 1 1 1 -1 -1 -1 1 -1 -1 -1) para a transmissão pelo canal. Com o resultado da presença do ruído gaussiano de média nula e variância $\sigma^2 = 0.8$, obtemos a mensagem recebida pelo decodificador r = (1.3129 2.6584 0.7413 2.1745 0.5981 -0.8323 -0.3962 -1.7586 1.4905 0.4084 -0.9290 1.0765)

Se realizarmos uma uma decisão abrupta na recepção r se torna a sequência (1 1 1 1 1 0 0 1 1 0 1), com erro nas posições 10 e 12. Dado que a transmissão foi num canal gaussiano, obtemos os fatores $f_j^{\times}$ que resultam do vetor recebido, aplicando a expressão da função de distribuição de probabilidade gaussiana temos:

$$f_j^0 = \frac{1}{\sqrt{2\pi}\sigma} e^{-(r_j+1)^2/2\sigma^2}$$
$$f_j^1 = \frac{1}{\sqrt{2\pi}\sigma} e^{-(r_j-1)^2/2\sigma^2}$$

Calculando os coeficientes obtemos os seguintes resultados mostrados na Tabela 3.1.

j	1	2	3	4	5	6	7	8	9	10	11	12
r	1.3129	2.6584	0.7413	2.1745	0.5981	-0.8323	-0.3962	-1.7586	1.4905	0.4084	-0.9290	1.0765
t	1	1	1	1	1	-1	-1	-1	1	-1	-1	-1
f_j^0	0.0076	0.000	0.0467	0.0002	0.0678	0.487	0.3751	0.3181	0.0039	0.1059	0.4967	0.0172
f_j^1	0.4619	0.0582	0.473	0.1697	0.4369	0.0362	0.1088	0.0013	0.4132	0.3794	0.0272	0.4964

Tabela 3.1: Vetor recebido correspondente aos fatores f

A informação proveniente do canal é determinada pelos fatores f. Os coeficientes da iteração são calculados pelo grafo bipartido, que se obtém diretamente das equações de paridade. Portanto podemos escrever as equações de paridade como sendo:

$c_2 \bigoplus c_4 \bigoplus c_6 \bigoplus c_7 \bigoplus_8 \bigoplus_{12} = 0$ $\quad c_1 \bigoplus c_3 \bigoplus c_4 \bigoplus c_9 = 0$ $\quad c_2 \bigoplus c_5 \bigoplus c_7 \bigoplus c_{12} = 0$
$c_2 \bigoplus c_6 \bigoplus c_8 \bigoplus c_9 \bigoplus c_{10} = 0$ $\quad c_3 \bigoplus c_5 \bigoplus c_6 \bigoplus c_10 = 0$ $\quad c_1 \bigoplus c_4 \bigoplus c_{10} \bigoplus c_{11} = 0$

$c_1 \bigoplus c_3 \bigoplus c_7 \bigoplus c_8 \bigoplus c_{11} = 0 \qquad c_5 \bigoplus c_9 \bigoplus c_{11} \bigoplus c_{12} = 0$

Representado graficamente na Figura 3.4:
Cada linha da matriz H corresponde a um nó de paridade e cada bit da mensagem representa um nó de variável.

A inicialização do algoritmo soma-produto é feita ajustando os coeficientes de informação do nó de variável ao nó de paridade Q^0_{ij} e Q^1_{ij} como nenhuma outra informação está disponível, as mensagens enviadas são os próprios valores obtidos das probabilidades de transição do canal

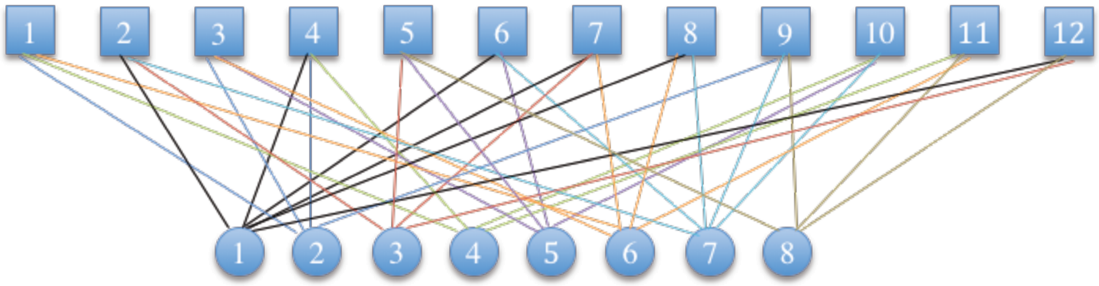

Figura 3.4: Representação do Grafo de Tanner

f^0_j e f^1_j. $Q^0_{ij} = f^0_j$ e $Q^1_{ij} = f^1_j$. Dessa maneira temos:

$Q^0_{12} = 0.0000 \quad Q^0_{12} = 0.0582 \quad Q^0_{14} = 0.0002 \quad Q^0_{14} = 0.1697$
$Q^0_{16} = 0.4878 \quad Q^0_{16} = 0.0362 \quad Q^0_{17} = 0.3751 \quad Q^0_{17} = 0.1088$
$Q^0_{18} = 0.3181 \quad Q^1_{18} = 0.0013 \quad Q^0_{1,12} = 0.0172 \quad Q^1_{1,12} = 0.4964$

$Q^0_{21} = 0.0076 \quad Q^1_{21} = 0.4619 \quad Q^0_{23} = 0.0467 \quad Q^1_{23} = 0.4733$
$Q^0_{24} = 0.0002 \quad Q^1_{24} = 0.1697 \quad Q^0_{29} = 0.0039 \quad Q^1_{29} = 0.4132$

$Q^0_{32} = 0.0000 \quad Q_32^1 = 0.0582 \quad Q^0_{35} = 0.0678 \quad Q^1_{35} = 0.4369$
$Q^0_{37} = 0.3751 \quad Q^1_{37} = 0.1088 \quad Q^0_{3,12} = 0.0172 \quad Q^1_{3,12} = 0.4964$

$Q^0_{41} = 0.0076 \quad Q^1_{41} = 0.4619 \quad Q^0_{44} = 0.0002 \quad Q^1_{44} = 0.1697$
$Q^0_{4,10} = 0.1059 \quad Q^1_{4,10} = 0.3794 \quad Q^0_{4,11} = 0.4967 \quad Q^1_{4,11} = 0.0272$

$Q^0_{53} = 0.0467 \quad Q^1_{53} = 0.4733 \quad Q^0_{55} = 0.0678 \quad Q^1_{55} = 0.4396$
$Q^0_{56} = 0.4878 \quad Q^1_{56} = 0.0362 \quad Q^0_{5,10} = 0.1059 \quad Q^1_{5,10} = 0.3794$

$Q^0_{61} = 0.0076 \quad Q^1_{61} = 0.4619 \quad Q^0_{63} = 0.0467 \quad Q^1_{63} = 0.4733$
$Q^0_{67} = 0.3751 \quad Q^1_{67} = 0.1088 \quad Q^0_{68} = 0.3181 \quad Q^1_{68} = 0.0013$
$Q^0_{6,11} = 0.4967 \quad Q^1_{6,11} = 0.0272$

$Q^0_{72} = 0.0000 \quad Q^1_{72} = 0.0582 \quad Q^0_{76} = 0.4878 \quad Q^1_{76} = 0.0362$
$Q^0_{78} = 0.3181 \quad Q^1_{78} = 0.0013 \quad Q^0_{79} = 0.0039 \quad Q^1_{79} = 0.4132$
$Q^0_{7,10} = 0.1059 \quad Q^1_{7,10} = 0.3794$

$Q^0_{85} = 0.0678 \quad Q^1_{85} = 0.4396 \quad Q^0_{89} = 0.0039 \quad Q^1_{89} = 0.4132$
$Q^0_{8,11} = 0.4967 \quad Q^1_{8,11} = 0.0272 \quad Q^0_{8,12} = 0.0172 \quad Q^1_{8,12} = 0.4964$

Com esses valores de inicialização, obtém-se então os coeficientes R^0_{ij} e R^1_{ij} que são os valores correspondentes a estimação de paridade comunica ao nó de variável 2. Por exemplo, o elemento R^0_{12} é a informação que o nó de paridade 1 leva ao nó de variável 2, levando em conta que a equação de paridade que o corresponde $c_2 \oplus c_4 \oplus c_6 \oplus c_7 \oplus c_8 \oplus c_{12} = 0$, e satisfaz com o bit ou símbolo 2 no estado $c_2 = 0$, resultando em 16 combinações dos símbolos c_4, c_6, c_7, c_8 e c_{12}. Assim temos,

$$
\begin{aligned}
R^0_{12} = {} & Q^0_{14}Q^0_{16}Q^0_{17}Q^0_{18}Q^0_{1,12} + Q^0_{14}Q^0_{16}Q^0_{17}Q^1_{18}Q^1_{1,12} + Q^0_{14}Q^0_{16}Q^1_{17}Q^0_{18}Q^1_{1,12} + Q^0_{14}Q^0_{16}Q^1_{17}Q^1_{18}Q^0_{1,12} \\
& + Q^0_{14}Q^1_{16}Q^0_{17}Q^0_{18}Q^1_{1,12} + Q^0_{14}Q^1_{16}Q^0_{17}Q^1_{18}Q^0_{1,12} + Q^0_{14}Q^1_{16}Q^1_{17}Q^0_{18}Q^0_{1,12} + Q^0_{14}Q^1_{16}Q^1_{17}Q^1_{18}Q^1_{1,12} \\
& + Q^1_{14}Q^0_{16}Q^0_{17}Q^0_{18}Q^1_{1,12} + Q^1_{14}Q^0_{16}Q^0_{17}Q^1_{18}Q^0_{1,12} + Q^1_{14}Q^0_{16}Q^1_{17}Q^0_{18}Q^0_{1,12} + Q^1_{14}Q^0_{16}Q^1_{17}Q^1_{18}Q^1_{1,12} \\
& + Q^1_{14}Q^1_{16}Q^0_{17}Q^0_{18}Q^0_{1,12} + Q^1_{14}Q^1_{16}Q^0_{17}Q^1_{18}Q^1_{1,12} + Q^1_{14}Q^1_{16}Q^1_{17}Q^0_{18}Q^1_{1,12} + Q^1_{14}Q^1_{16}Q^1_{17}Q^1_{18}Q^0_{1,12} = 0.0051
\end{aligned}
$$

Da mesma forma o elemento R^1_{12} é a informação que o nó de paridade 1 envia ao nó de variável 2, que obtém da equação de paridade $c_2 \oplus c_4 \oplus c_6 \oplus c_7 \oplus c_8 \oplus c_{12} = 0$ e se satisfaz com o bit ou símbolo $c_2 = 1$.

$$
\begin{aligned}
R^1_{12} = {} & Q^0_{14}Q^0_{16}Q^0_{17}Q^0_{18}Q^1_{1,12} + Q^0_{14}Q^0_{16}Q^0_{17}Q^1_{18}Q^0_{1,12} + Q^0_{14}Q^0_{16}Q^1_{17}Q^0_{18}Q^0_{1,12} + Q^0_{14}Q^0_{16}Q^0_{17}Q^1_{18}Q^1_{1,12} \\
& + Q^0_{14}Q^1_{16}Q^0_{17}Q^0_{18}Q^+_{1,12}Q^0_{14}Q^1_{16}Q^0_{17}Q^1_{18}Q^1_{1,12} + Q^0_{14}Q^1_{16}Q^1_{17}Q^0_{18}Q^1_{1,12} + Q^0_{14}Q^1_{16}Q^1_{17}Q^1_{18}Q^0_{1,12} \\
& + Q^1_{14}Q^0_{16}Q^0_{17}Q^0_{18}Q^0_{1,12} + Q^1_{14}Q_16^0Q^0_{17}Q^1_{18}Q^1_{1,12} + Q^1_{14}Q^0_{16}Q^1_{17}Q^0_{18}Q^1_{1,12} + Q^1_{14}Q^0_{16}Q^1_{17}Q^1_{18}Q^0_{1,12} \\
& + Q^1_{14}Q^1_{16}Q^0_{17}Q^0_{18}Q^1_{1,12} + Q^1_{14}Q^1_{16}Q^0_{17}Q^1_{18}Q^0_{1,12} + Q^1_{14}Q^1_{16}Q^1_{17}Q^0_{18}Q^0_{1,12} + Q^1_{14}Q^1_{16}Q^1_{17}Q^1_{18}Q^1_{1,12} = 0.0051
\end{aligned}
$$

O fluxo de informação pode ser visto na Figura 3.5. O nó que comunica a estimação, não tem participação no valor calculado. Evidentemente quanto maior o número de '1's por linha da matriz de paridade maior possibilidades de combinação no calculo dos coeficientes R^0_{ij} e R^1_{ij}. As Tabelas 3.2 e 3.3 apresentam os valores calculados destes coeficientes, na forma de uma ma-

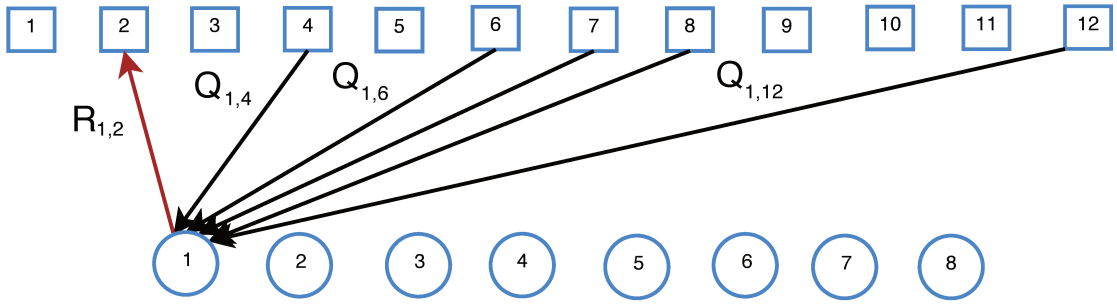

Figura 3.5: Representação do Grafo de Tanner

triz, onde as linhas correspondem ao índice i, e as colunas ao índice j. A Tabela 3.2 representa os coeficientes R^0_{ij}, ou seja, as estimativas para o valor do bit ou símbolo $x = 0$, e a Tabela 3.3 os coeficientes R^1_{ij}, as estimativas para o valor do bit ou símbolo $x = 1$.

	1	2	3	4	5	6	7	8	9	10	11	12
1		0.0051		0.0017		0.0002	0.0001	0.0004				0.0006
2	0.0036		0.0009	0.0113					0.0043			
3		0.0868			0.0109		0.0024					0.01
4	0.0325			0.0889						0.039	0.0088	
5			0.0875		0.0925	0.0423				0.1049		
6	0.0126		0.01				0.0348	0.0431			0.027	
7		0.025				0.0008		0.0016	0.0035	0.0037		
8					0.1022				0.1101		0.0179	0.0912

Tabela 3.2: Valores de R^0_{ij}, primeira iteração

	1	2	3	4	5	6	7	8	9	10	11	12
1		0.002		0.0007		0.0006	0.0008	0.0009				0.0002
2	0.0332		0.0324	0.0906					0.0372			
3		0.0393			0.0035		0.0128					0.0043
4	0.0107			0.0305						0.028	0.0299	
5			0.0416		0.0398	0.0857				0.0333		
6	0.0295		0.028				0.006	0.0188			0.0107	
7		0.0089				0.0029		0.0046	0.0012	0.0003		
8					0.0101				0.0264		0.0908	0.0197

Tabela 3.3: Valores de R^1_{ij}, primeira iteração

O elemento $R_4, 10^0 = 0.039$ se refere a $i = 4$ e $j = 10$. Uma vez calculados os coeficientes R^0_{ij} e R^1_{ij}, é possível estabelecer uma primeira estimação dos bits decodificados, empregando a expressão:

$$\hat{d} = \arg\max_x f^x_j \prod_{k \in M(j)} R^x_{kj}$$

Assim,

$$\hat{d_1} = \begin{cases} \hat{0} \rightarrow f^0_1 \times R^0_{21} \times R^0_{41} \times R^0_{61} = 1.13 \times 10^{-8} \\ \hat{1} \rightarrow f^1_1 \times R^1_{21} \times R^1_{41} \times R^1_{61} = 4.85 \times 10^{-6} \end{cases} \Rightarrow 1$$

$$\hat{d_2} = \begin{cases} \hat{0} \rightarrow f^0_2 \times R^0_{12} \times R^0_{32} \times R^0_{72} = 1.58 \times 10^{-10} \\ \hat{1} \rightarrow f^1_2 \times R^1_{12} \times R^1_{32} \times R^1_{72} = 4.06 \times 10^{-8} \end{cases} \Rightarrow 1$$

$$\hat{d_3} = \begin{cases} \hat{0} \rightarrow f^0_3 \times R^0_{23} \times R^0_{53} \times R^0_{63} = 3.59 \times 10^{-8} \\ \hat{1} \rightarrow f^1_3 \times R^1_{23} \times R^1_{53} \times R^1_{63} = 1.78 \times 10^{-5} \end{cases} \Rightarrow 1$$

$$\hat{d_4} = \begin{cases} \hat{0} \rightarrow f^0_4 \times R^0_{14} \times R^0_{24} \times R^0_{44} = 3.31 \times 10^{-10} \\ \hat{1} \rightarrow f^1_4 \times R^1_{14} \times R^1_{24} \times R^1_{44} = 3.19 \times 10^{-7} \end{cases} \Rightarrow 1$$

$$\hat{d}_5 = \begin{cases} \hat{0} \rightarrow f_5^0 \times R_{35}^0 \times R_{55}^0 \times R_{85}^0 = 7.01 \times 10^{-6} \\ \hat{1} \rightarrow f_5^1 \times R_{35}^1 \times R_{55}^1 \times R_{85}^1 = 6.20 \times 10^{-7} \end{cases} \Rightarrow 0$$

$$\hat{d}_6 = \begin{cases} \hat{0} \rightarrow f_6^0 \times R_{16}^0 \times R_{56}^0 \times R_{76}^0 = 3.39 \times 10^{-9} \\ \hat{1} \rightarrow f_6^1 \times R_{16}^1 \times R_{56}^1 \times R_{76}^1 = 5.34 \times 10^{-9} \end{cases} \Rightarrow 1$$

$$\hat{d}_7 = \begin{cases} \hat{0} \rightarrow f_7^0 \times R_{17}^0 \times R_{37}^0 \times R_{67}^0 = 2.73 \times 10^{-9} \\ \hat{1} \rightarrow f_7^1 \times R_{17}^1 \times R_{37}^1 \times R_{67}^1 = 6.37 \times 10^{-9} \end{cases} \Rightarrow 1$$

$$\hat{d}_8 = \begin{cases} \hat{0} \rightarrow f_8^0 \times R_{18}^0 \times R_{68}^0 \times R_{78}^0 = 7.96 \times 10^{-9} \\ \hat{1} \rightarrow f_8^1 \times R_{18}^1 \times R_{68}^1 \times R_{78}^1 = 1.03 \times 10^{-10} \end{cases} \Rightarrow 0$$

$$\hat{d}_9 = \begin{cases} \hat{0} \rightarrow f_9^0 \times R_{29}^0 \times R_{79}^0 \times R_{89}^0 = 6.52 \times 10^{-9} \\ \hat{1} \rightarrow f_9^1 \times R_{29}^1 \times R_{79}^1 \times R_{89}^1 = 4.98 \times 10^{-7} \end{cases} \Rightarrow 1$$

$$\hat{d}_{10} = \begin{cases} \hat{0} \rightarrow f_{10}^0 \times R_{4,10}^0 \times R_{5,10}^0 \times R_{7,10}^0 = 1.62 \times 10^{-6} \\ \hat{1} \rightarrow f_{10}^1 \times R_{4,10}^1 \times R_{5,10}^1 \times R_{7,10}^1 = 1.17 \times 10^{-8} \end{cases} \Rightarrow 0$$

$$\hat{d}_{11} = \begin{cases} \hat{0} \rightarrow f_{11}^0 \times R_{4,11}^0 \times R_{6,11}^0 \times R_{8,11}^0 = 2.12 \times 10^{-6} \\ \hat{1} \rightarrow f_{11}^1 \times R_{4,11}^1 \times R_{6,11}^1 \times R_{8,11}^1 = 7.91 \times 10^{-7} \end{cases} \Rightarrow 0$$

$$\hat{d}_{12} = \begin{cases} \hat{0} \rightarrow f_{12}^0 \times R_{1,12}^0 \times R_{3,12}^0 \times R_{8,12}^0 = 9.23 \times 10^{-9} \\ \hat{1} \rightarrow f_{12}^1 \times R_{1,12}^1 \times R_{3,12}^1 \times R_{8,12}^1 = 8.87 \times 10^{-9} \end{cases} \Rightarrow 0$$

A primeira estimação da palavra decodificada é $d =$(1 1 1 1 0 1 1 0 1 0 0 0) que contem 3 erros em relação a palavra transmitida $c = (1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0)$. A iteração continua visto que a síndrome para o vetor decodificado d é diferente de zero. Para realizar a próxima iteração é necessário calcular os coeficientes Q_{ij}^0 e Q_{ij}^1. Estes coeficientes são obtidos pela expressão:

$$Q_{ij}^x = \alpha ij f_j^x \prod_{k \in M(j) \setminus i} R_{kj}^{\alpha},$$

de onde α_{ij} é uma constante de normalização para a qual os fatores cumprem a condição, $Q_{ij}^0 + Q_{ij}^1 = 1$. Assim o elemento Q_{12}^0 é a probabilidade que o nó de paridade 1 recebe do nó de variável 2, e a obtém levando em conta as conexões do grafo que chegam ao nó de variável 2 através do produto dos elementos do tipo R_{k2}^0; o mesmo ocorre para o elemento Q_{12}^1. O cálculo dos coeficientes Q_{12}^0 e Q_{12}^1 para o caso particular deste exemplo é feito da seguinte forma:

$$Q_{12}^0 = \alpha 12 f_2^0 R_{32}^0 R_{72}^0 \qquad Q_{12}^1 = \alpha 12 f_2^1 R_{32}^1 R_{72}^1$$

onde,

$$\alpha_{12} = \frac{1}{f_2^0 R_{32}^0 R_{72}^0 + f_2^1 R_{32}^1 R_{72}^1}$$

A forma como o cálculo é feito, pode ser vista na Figura 3.6. As Tabelas 3.4 e 3.5 apresentam

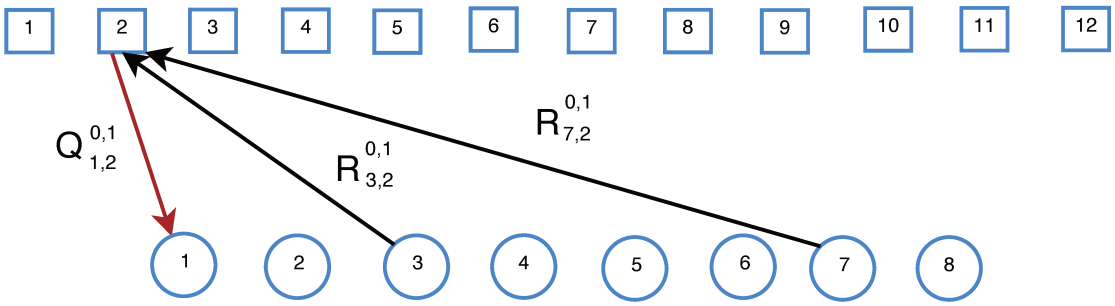

Figura 3.6: Calculo dos coeficientes Q_{12}^0 e Q_{12}^1

os valores calculados dos coeficientes Q_{12}^0 e Q_{12}^1, respectivamente. Com os valores atualizados

	1	2	3	4	5	6	7	8	9	10	11	12
1		0.0015		0.0004		0.6601	0.7898	0.9950				0.2731
2	0.0209		0.691	0.0083					0.1014			
3		0.0018			0.7843		0.6946					0.3068
4	0.0008			0.0004						0.9091	0.9008	
5			0.001		0.8294	0.562				0.9777		
6	0.0054		0.0056				0.0688	0.971			0.5147	
7		0.0014				0.6847		0.9954	0.0046	0.9239		
8					0.5273				0.0031		0.9316	0.1838

Tabela 3.4: Valores de Q_{ij}^0, segunda iteração

	1	2	3	4	5	6	7	8	9	10	11	12
1		0.9985		0.9996		0.3399	0.2102	0.005				0.7269
2	0.9791		0.9309	0.9917					0.8986			
3		0.9982			0.2157		0.3054					0.6932
4	0.9992			0.9996						0.0909	0.0992	
5			0.999		0.1706	0.438				0.0223‘		
6	0.9956		0.9944				0.9312	0.029			0.4853	
7		0.9986				0.3153		0.0046	0.9954	0.0761		
8					0.4727				0.9969		0.0684	0.8162

Tabela 3.5: Valores de Q_{ij}^1, segunda iteração

das probabilidades Q_{ij}^0 e Q_{ij}^1, pode-se agora calcular os novos valores dos coeficientes R_{ij}^0 e R_{ij}^1. Esses valores atualizados permitem realizar outra estimação dos bits, definindo um novo valor do vetor decodificado d, sobre o qual se faz o calculo da síndrome. Se a síndrome encontrada for igual a zero, o processo finaliza, senão continua realizando a próxima iteração. O número de iterações para em em um valor pré-fixado ou quando encontra uma solução.

Neste exemplo foram necessárias três iterações para encontrar a palavra-código correta. O processo iterativo fez a correção dos dois erros. As Tabelas 3.6 e 3.7 mostram os valores dos coeficientes. E a segunda estimação resulta como mostra a Tabela 3.8.

	1	2	3	4	5	6	7	8	9	10	11	12
1		0.5416		0.5415		0.3704	0.4284	0.4581				0.5915
2	0.1622		0.1244	0.1709					0.094			
3		0.4572			0.575		0.6095					0.3897
4	0.1723			0.1726						0.8999	0.9081	
5			0.539		0.4409	0.1859				0.4593		
6	0.5118		0.5118				0.5135	0.4876			0.1027	
7		0.3463				0.915		0.6547	0.3453	0.6808		
8					0.7713				0.4851		0.5172	0.4766

Tabela 3.6: Valores de R_{ij}^0, segunda iteração

	1	2	3	4	5	6	7	8	9	10	11	12
1		0.4584		0.4585		0.0296	0.5716	0.5419				0.4085
2	0.8378		0.8756	0.8291					0.906			
3		0.5428			0.425		0.3905					0.6103
4	0.8277			0.8274						0.1001	0.0919	
5			0.461		0.5591	0.8141				0.5407		
6	0.4882		0.4882				0.4805	0.5124			0.0893	
7		0.6537				0.085		0.0046	0.6547	0.3192		
8					0.2287				0.5149		0.4828	0.5234

Tabela 3.7: Valores de R_{ij}^1, segunda iteração

j	1	2	3	4	5	6	7	8	9	10	11	12
r	1.3129	2.6584	0.7413	2.1745	0.5981	-0.8323	-0.3962	-1.7586	1.4905	0.4084	-0.929	1.0765
t	1	1	1	1	1	-1	-1	-1	1	-1	-1	-1
d_j^0	0.0001	0.0000	0.0016	0.0000	0.0133	0.0307	0.0503	0.0465	0.0001	0.0298	0.0024	0.0019
d_j^1	0.1564	0.0095	0.0933	0.0534	0.0239	0.0016	0.0118	0.0001	0.1262	0.0066	0.0011	0.0648

Tabela 3.8: Estimação na segunda iteração

De acordo com essas estimações, o vetor decodificado é d =(1 1 1 1 1 0 0 0 1 0 0 1), e é a palavra transmitida com um único erro no último bit. Esta palavra gera uma síndrome diferente de zero, portanto o cálculo prossegue na próxima iteração. Para isso atualiza-se os coeficientes Q_{ij}^0 e Q_{ij}^1 apresentados nas Tabelas 3.9 e 3.10.

E então, um novo cálculo é feito para os coeficientes R_{ij}^0 e R_{ij}^1. Os valores são mostrados nas Tabelas 3.11 e 3.12. Esses valores são utilizados para uma nova estimação da palavra-código. Os valores podem ser vistos na Tabela 3.13.

Por essas estimações, o vetor decodificado resulta ser o mesmo transmitido $d = c$ =(1 1 1 1 1 0 0 0 1 0 0 0), e a síndrome calculada é enfim igual a zero. A mensagem decodificada é então: m =(1 0 0 0). A decodificação iterativa pode neste exemplo corrigir dois erros em uma palavra de 12 bits. A distância de Hamming deste código é $d_{min} = 4$. Desta forma pode-se dizer que este código corrige todos padrões de um erro, e pode corrigir alguns erros de outros padrões.

	1	2	3	4	5	6	7	8	9	10	11	12
1		0.0001		0.000		0.9707	0.8503	0.9977				0.0197
2	0.0036		0.1078	0.0003					0.0047			
3		0.0002			0.2909		0.7318					0.0436
4	0.0033			0.0003						0.3358	0.691	
5			0.0145		0.413	0.9884				0.8426		
6	0.0007		0.0161				0.8013	0.9974			0.9948	
7		0.0002				0.0642		0.9949	0.0009	0.6807		
8					0.1413				0.0005		0.9538	0.031

Tabela 3.9: Valores de Q_{ij}^0, terceira iteração

	1	2	3	4	5	6	7	8	9	10	11	12
1		0.9999		0.100		0.0293	0.1497	0.0023				0.9803
2	0.9964		0.8922	0.9997					0.9953			
3		0.9998			0.7091		0.2682					0.9564
4	0.9967			0.9997						0.6642	0.309	
5			0.9855		0.587	0.0116				0.1574		
6	0.9993		0.9839				0.1987	0.0026			0.0052	
7		0.9998				0.3558		0.0051	0.9991	0.3193		
8					0.8587				0.9995		0.0462	0.969

Tabela 3.10: Valores de Q_{ij}^1, terceira iteração

	1	2	3	4	5	6	7	8	9	10	11	12
1		0.8153		0.8153		0.1651	0.0501	0.1833				0.8282
2	0.1117		0.0085	0.1143					0.1109			
3		0.5885			0.7115		0.039205					0.5969
4	0.0527			0.5623						0.6896	0.337	
5			0.4418		0.175	0.5579				0.5825		
6	0.2129		0.2037				0.9758	0.7882			0.7897	
7		0.4485				0.6784		0.552	0.4485	0.6424		
8					0.9252				0.8053		0.1639	0.8252

Tabela 3.11: Valores de R_{ij}^0, terceira iteração

	1	2	3	4	5	6	7	8	9	10	11	12
1		0.1847		0.1847		0.8349	0.9499	0.8167				0.1718
2	0.8883		0.9915	0.8857					0.8891			
3		0.4115			0.2885		0.6908					0.4031
4	0.4373			0.4377						0.3104	0.663	
5			0.5582		0.825	0.4421				0.4175		
6	0.7871		0.7963				0.0242	0.2128			0.2103	
7		0.5515				0.3216		0.448	0.5515	0.3576		
8					0.0748				0.1947		0.8361	0.1748

Tabela 3.12: Valores de R_{ij}^1, terceira iteração

j	1	2	3	4	5	6	7	8	9	10	11	12
r	1.3129	2.6584	0.7413	2.1745	0.5981	-0.8323	-0.3962	-1.7586	1.4905	0.4084	-0.929	1.0765
t	1	1	1	1	1	-1	-1	-1	1	-1	-1	-1
d_j^0	0.0001	0.000	0.000	0.000	0.0077	0.0305	0.0057	0.0254	0.0002	0.0273	0.0217	0.007
d_j^1	0.1412	0.0024	0.2086	0.0122	0.0078	0.0043	0.0017	0.0001	0.0394	0.0176	0.0032	0.006

Tabela 3.13: Estimação na terceira iteração

Capítulo 4

Análise de Desempenho e Resultados

Este capítulo apresenta uma análise do desempenho de um sistema de cooperação codificada. As curvas de desempenho são apresentadas na forma de taxa de erro de bit *versus* energia por bit sobre densidade espectral de potência unilateral do ruído (E_b/N_0).

4.1 Modelo do Sistema de Cooperação Codificada

A Figura 4.1 apresenta o diagrama de bloco do sistema de codificação LDPC cooperativa analisado.

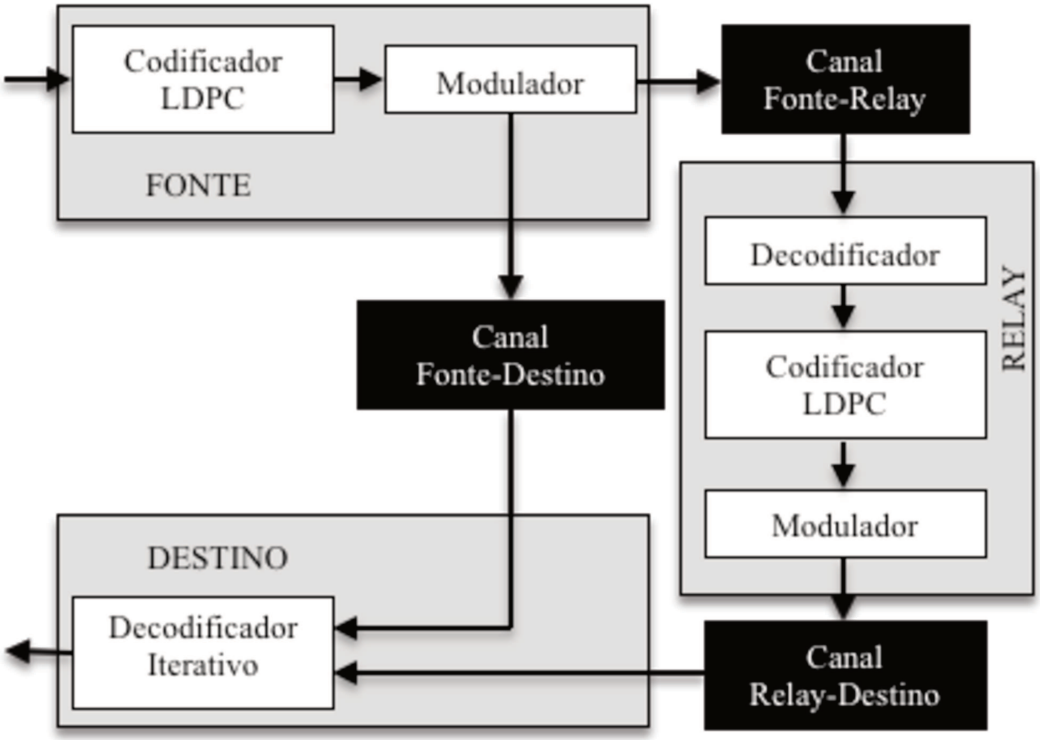

Figura 4.1: Modelo do sistema de cooperação codificada

Note que dois usuários (fonte e relay) estão transmitindo para um único destino. Os canais entre os usuários e os canais entre cada usuário e o destino são considerados mutuamente independentes e estão sujeitos a ruído aditivo gaussiano branco (AWGN) e desvanecimento Rayleigh. Para efeito de análise da diversidade espacial o desvanecimento é feito plano durante toda a duração do quadro de transmissão.

Em nossa análise e simulação, consideramos, sem perda de generalidade, o esquema de modulação BPSK, em que os sinais que chegam aos receptores são dados por

$$r_{fd} = \gamma_{sd}c + \eta_{fd} \tag{4.1}$$

$$r_{fr} = \gamma_{sr}c + \eta_{fr} \tag{4.2}$$

$$r_{rd} = \gamma_{rd}c + \eta_{rd} \tag{4.3}$$

sendo γ_{fd}, γ_{fr} e γ_{rd} o desvanecimento no canal fonte-destino, no canal fonte-relay e no canal relay-destino, respectivamente; c a palavra-código transmitida pela fonte e c' a palavra-código gerada e transmitida pelo relay, ambas representadas na forma antipodal, e η_{xy} o ruído AWGN introduzido por um dado canal.

4.1.1 Canal AWGN

O ruído AWGN é modelado pela função densidade de probabilidade gaussiana de média nula e variância σ^2 , ou seja,

$$f(\eta) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(\eta-m)^2/2\sigma^2}, \tag{4.4}$$

em que o desvio padrão é dado (Gonçalves 2010):

$$\sigma = \frac{1}{\sqrt{2.R.SNR}}, \tag{4.5}$$

sendo R a taxa de codificação e SNR a razão da energia do sinal transmitido pela densidade espectral de potência unilateral do ruído.

A sequência de bits proveniente do codificador é convertida pelo modulador na sequência representada por símbolos antipodais $+1$ e -1. Assim, com ruído gaussiano adicionado a estes valores temos na saída de cada canal duas funções densidade de probabilidade gaussianas com variâncias σ^2 e médias $+1$ e -1, respectivamente, como mostrado na Figura. 4.2.

4.1.2 Canal com Desvanecimento

O sinal que chega ao receptor geralmente é representado pela soma de várias réplicas com diferentes amplitudes e fases do sinal transmitido, causando o desvanecimento no sinal. Isso ocorre devido a reflexções e refrações sofridas pelo sinal transmitido por conta de objetos presentes em sua trajetória, tais como construções, árvores, montanhas, etc. A distribuição de Rayleigh é um bom modelo estatístico para representar a envoltória do sinal recebido resultante desta propagação por multi-percurso, quando a visada direta entre transmissor e receptor

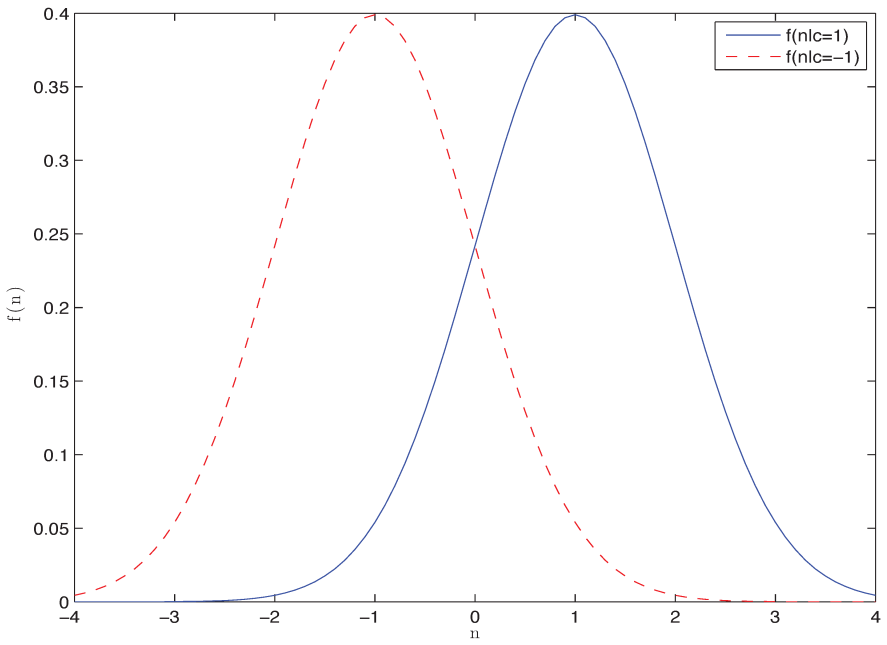

Figura 4.2: Função densidade de probabilidade gaussiana dos símbolos ± 1

não está presente. A função densidade de probabilidade da distribuição Rayleigh com potência média $2\beta^2$ é dada por (Yacoub 1993)

$$p(\gamma) = \frac{1}{\beta^2} e^{-\gamma^2/2\beta^2} \tag{4.6}$$

Assim, o canal equivalente considerando o ruído AWGN e o desvanecimento Rayleigh, pode ser visto na Figura 4.3, em que c_k é o sinal transmitido, r_k é o sinal recebido, η_k é o ruído AWGN e γ_k é o desvanecimento Rayleigh. Os coeficientes de desvanecimento utilizados na simulação são amostras independentes da distribuição Rayleigh obtidas através da função raylrnd do MatLab©.

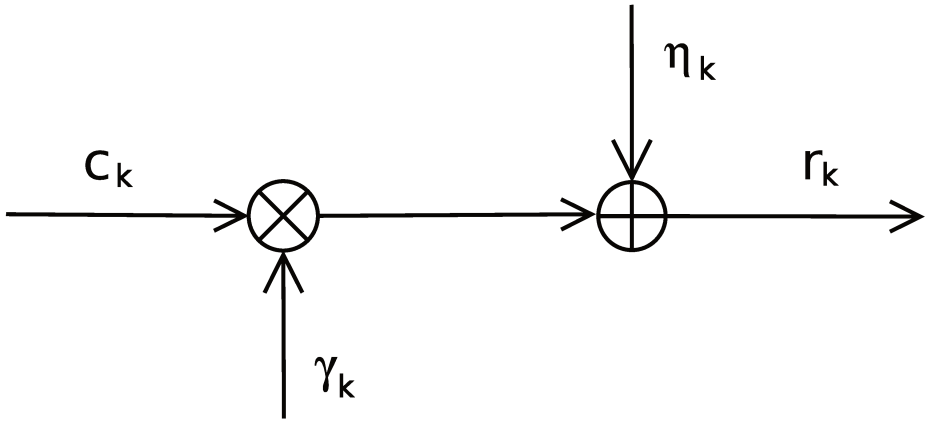

Figura 4.3: Canal equivalente (AWGN + Desvanecimento Rayleigh)

4.2 Parâmetros de Simulação

Nesta seção apresentamos a implementação dos codificadores LDPC utilizados na análise de desempenho do sistema de cooperação codificada descrita neste trabalho.

4.2.1 Código 1

Código LDPC (4512, 2256) irregular, criado por (Xiao 2010), (Xiao 2009),(Kong & Xiao 2008),(Xiao & Lee 2006) e com os seguintes parâmetros:

- Comprimento do código, $n = 4512$;
- Comprimento da sequência de informação, $k = 2256$;
- Taxa de codificação, $R = 1/2$;
- Peso da linha, $w_r = 6$, e peso da coluna, $w_c = 3$;

4.2.2 Código 2

Código quasi-cíclico proposto por Yang Xiao (Xiao 2009), (Kong & Xiao 2008), (Xiao & Lee 2006), com os seguintes parâmetros:

- Comprimento do código, $n = 1270$;
- Comprimento da sequência de informação, $k = 635$;
- Taxa de codificação, $R = 1/2$;
- Peso de coluna e de linha, respectivamente, $w_c = 5$ e $w_r = 10$.

A matriz de verificação de paridade do código quase-cíclico é construída da seguinte forma (Xiao & Kim 2008),(Zhang, Huang, Lin, Abdel-Ghaffar & Blake 2010):

$$H = \begin{bmatrix} I & I & 0 & 0 & 0 & I_{a^5} & I_{a^6} & I_{a^7} & I_{a^8} & I_{a^9} \\ 0 & I & I & 0 & 0 & I_{ba^5} & I_{ba^6} & I_{ba^7} & I_{ba^8} & I_{ba^9} \\ I & 0 & I & I & 0 & I_{b^2a^5} & I_{b^2a^6} & I_{b^2a^7} & I_{b^2a^8} & I_{b^2a^9} \\ 0 & 0 & 0 & I & I & I_{b^3a^5} & I_{b^3a^6} & I_{b^3a^7} & I_{b^3a^8} & I_{b^3a^9} \\ I & 0 & 0 & 0 & I & I_{b^4a^5} & I_{b^4a^6} & I_{b^4a^7} & I_{b^4a^8} & I_{b^4a^9} \end{bmatrix}_{(n-k)\times n} \tag{4.7}$$

em que I_s é a matriz identidade com suas linhas ciclicamente deslocadas para a esquerda, de s posições; O é uma matriz de zeros. A maneira como foi feita a construção da matriz H, o deslocamento e os valores escolhidos para a e b são explicados com mais detalhes em [41, 42].

Colocando-se a matriz H na forma de duas submatrizes, tem-se:

$$H = [A_{(n-k)\times(n-k)} | B_{(n-k)\times(n-k)}] \tag{4.8}$$

Portanto, a matriz de paridade é dada por (Lin & Costello 2004)

$$P = [A^{-1}B] \tag{4.9}$$

Por fim, obtemos a matriz geradora do código LDPC quasi-cíclico como sendo (Lin & Costello 2004)

$$G = [P|I] \tag{4.10}$$

4.3 Resultados

Esta seção apresenta os resultados de simulação para o sistema proposto, com sinais BPSK transmitidos por um canal AWGN sob desvanecimento plano, e com códigos descritos na seção anterior.

O método de simulação computacional utilizado para a obtenção da probabilidade de erro de bit foi o de Monte Carlo. O número de erros foi limitado inferiormente em 200 bits. Assumimos ainda um sincronismo perfeito de relógio de bit e de quadro.

A transmissão de dados da fonte e do relay é baseada em quadros de comprimento n bits. Cada quadro é dividido em dois sub-quadros de comprimento n_1 e n_2 bits, respectivamente (Figura 4.4). Se um usuário (relay) cooperar, permite-se que o outro usuário (fonte) utilize de seu subquadro ou todo quadro. Isso dependerá da estratégia de cooperação adotada pelo sistema. Assim, a cooperação codificada é muito flexível e pode ser utilizada em qualquer cenário de codificação de canal.

Figura 4.4: Partição das palavras-códigos nos três canais

Neste trabalho, assumimos que a fonte transmite k bits de informação na palavra-código c de comprimento n bits, sendo então a taxa do código de $R = k/n$. Dessa maneira, a fonte não coopera no sistema. A palavra-código chega em ambos destino e relay por diferentes caminhos. No relay, a palavra-código corrompida por ruído é detectada, decodificada e recodificada na palavra-código c_1 de comprimento n bits e então é transmitida ao destino. O comprimento n' de

c_1 está relacionado ao nível de cooperação provido pelo relay. Se o relay não está transmitindo dados, então todo seu quadro está disponível para cooperar com a fonte. Em outras palavras, $n' = n$.

O processo de codificação no relay não necessariamente precisa ser o mesmo da fonte, mas neste trabalho o consideramos o mesmo. O destino recebe a versão corrompida por ruído de ambas as palavras-códigos c e c_1, e faz uso delas para melhor estimar os k bits de informação enviados pela fonte.

Consideramos os canais fonte-destino, relay-destino e fonte-relay independentes. O relay decodifica a sequência recebida de modo iterativo para estimar os k bits de informação e recodifica essa estimação usando o mesmo código LDPC da fonte.

Duas situações são analisadas: cooperação completa, com o relay processando e enviando a palavra-código total ($n' = n$) para o destino, que verifica bit a bit as palavras-códigos recebidas da fonte e do relay, respectivamente; e cooperação parcial, em que o relay usa apenas um subquadro, enviando portanto apenas metade da palavra-código ($n' = n_2 = n/2$). A representação da cooperação total está exemplificada na Tabela 4.1. Os valores de r_{sd} é a informação que chega pelo canal fonte-destino, enquanto que r_{rd} é a informação vinda do canal relay-destino. No receptor, r_d, apenas os sinais mais próximos de ± 1 são mantidos, segundo o critério de mínima distância mínima.

r_{sd}	1.733	-1.073	1.716	1.115	2.132	-1.156	0.159	2.824	-1.157	2.177
r_{rd}	0.751	-0.744	1.578	1.924	1.035	-0.293	-0.889	0.952	-0.799	0.839
r_d	0.751	-1.073	1.578	1.115	1.035	-1.156	-0.889	0.952	-1.157	0.839

Tabela 4.1: Representação do esquema de Cooperação total

O destino recebe as sequências corrompidas por ruído r_{sd} e r_{rd} , relativas às palavras-códigos c e c_1, respectivamente. Os símbolos recebidos de r_{sd} e r_{rd} são primeiramente comparados um a um em cada posição que eles ocupam, onde então apenas os símbolos mais confiáveis são mantidos em cada posição, formando uma única sequência recebida (r_d). Essa sequência final é então enviada ao decodificador iterativo do destino, para se obter a melhor estimativa da sequência de informação transmitida pela fonte. O decodificador iterativo utiliza o algoritmo soma-produto.

O desempenho do sistema é analisado considerando-se quatro cenários diferentes.

4.3.1 Cenário 1

O desvanecimento plano tem a mesma potência nos três canais, fonte-destino, fonte-relay e relay-destino.

A Figura 4.5 mostra o desempenho, em termos de taxa de erro de bit (BER) *versus* a razão energia por bit por densidade espectral unilateral de ruído (E_b/N_0), do esquema de cooperação codificada que utiliza o código 1. Nesse caso, nenhum dos canais possui desvanecimento. Note que, para uma $BER = 10^5$, a cooperação codificada produz um ganho de 2dB e 0.4 dB para o caso onde a palavra-código inteira e sua metade é transmitida pelo relay, respectivamente. A

curva que mostra o desempenho da transmissão codificada fonte-destino é também desenhada para efeito de comparação.

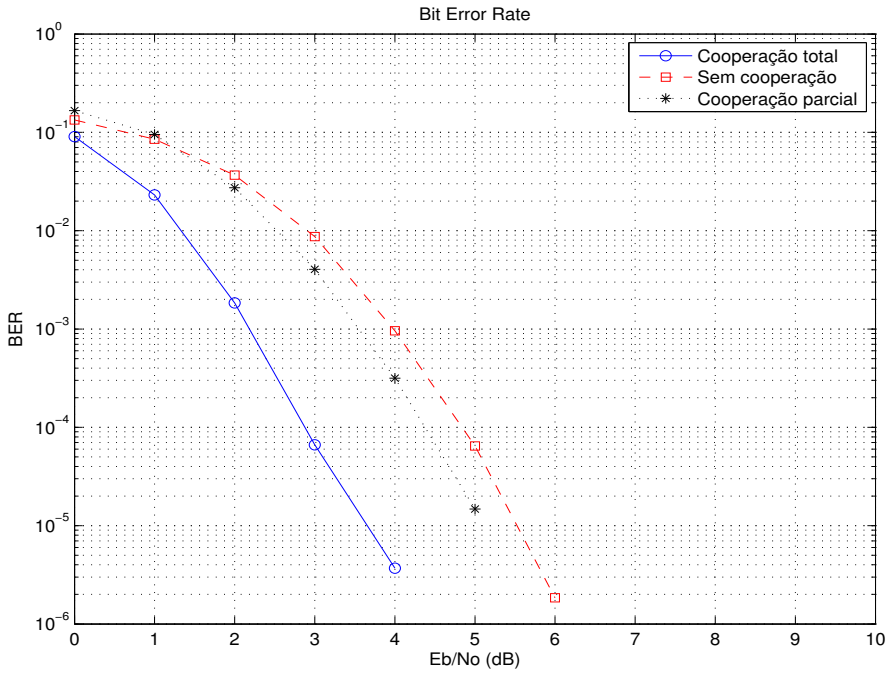

Figura 4.5: Cooperação codificada do código 1 com o mesmo nível de desvanecimento nos três canais

4.3.2 Cenário 2

O desvanecimento plano é 3 dB mais intenso no canal fonte-relay em relação ao outros dois canais. Utilizamos o código 1.

A Figura 4.6 mostra a curva do desempenho BER versus E_b/N_0, para o caso em que o desvanecimento plano no canal fonte-relay é mantido 3 dB pior que nos outros dois canais. Note que ambos os esquemas de cooperação codificada produzem uma perda em relação à transmissão direta entre fonte e destino sem cooperação. Isso se deve ao fato de que a estimativa obtida pelo relay da sequência de informação contém erros que, ao ser transmitida ao destino, causará mais erros. Portanto, não há vantagem em se cooperar quando o canal fonte-relay apresenta desvanecimento mais severo que o fonte-destino.

4.3.3 Cenário 3

O desvanecimento plano é 3 dB mais intenso no canal fonte-destino que nos outros dois canais. Utilizamos também o código 1. A Figura 4.7 mostra o desempenho BER *versus* E_b/N_0 para o caso em que o canal fonte-destino apresenta desvanecimento plano maior que o percurso via relay. Note que a codificação cooperativa produziu um ganho de 3.5 dB e 1.3 dB, para

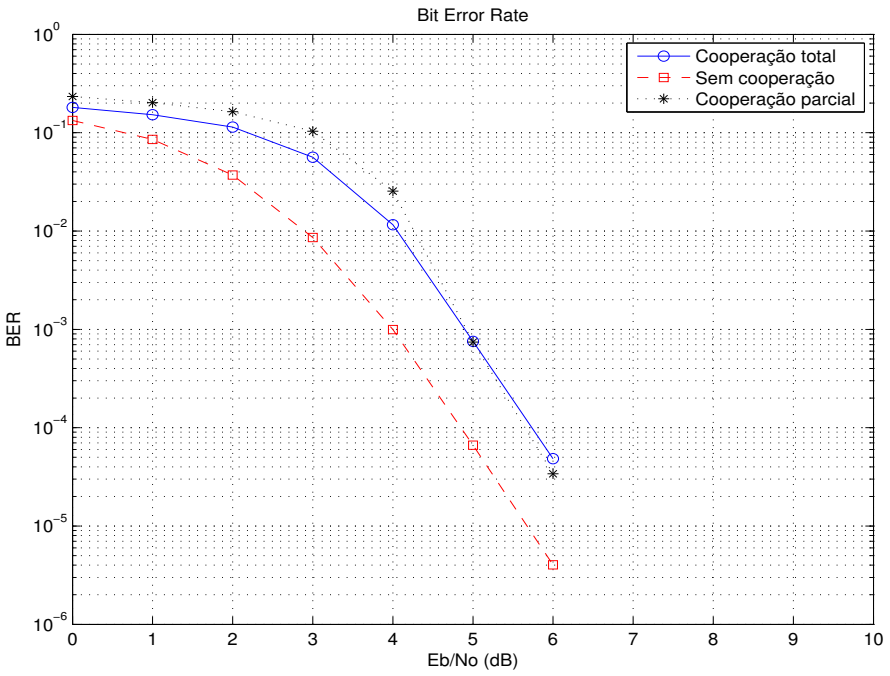

Figura 4.6: Cooperação codificada do código 1 com desvanecimento plano 3dB mais severo no canal fonte-relay

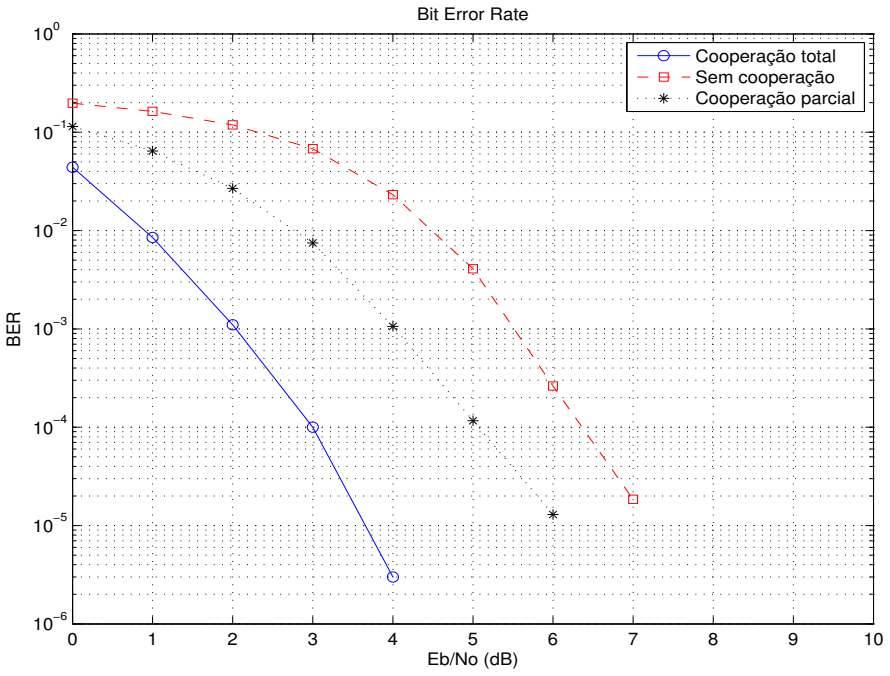

Figura 4.7: Cooperação codificada do código 1 com desvanecimento plano 3dB mais severo no canal direto

$BER = 10^{-4}$, para cooperação total, na qual o destino recebe integralmente as duas palavras-códigos, e parcial, na qual apenas a paridade da palavra código é enviada pelo relay ao destino, respectivamente.

Quando o canal fonte-destino fica sujeito a um maior nível de desvanecimento, a cooperação codificada tem o melhor desempenho. Mesmo para o caso em que os canais possuem o mesmo nível de desvanecimento, o esquema de cooperação total mostrou ser superior ao parcial e ambos ao esquema de não cooperação.

4.3.4 Cenário 4

Consideramos canais com apagamento simulando uma rajada de erros (*burst error*), em uma sequência de 10, 50 e 100 bits consecutivos, nos três canais e a seguir, nos canais, direto e fonte-destino. Utilizamos o código 2.

O modo como foi feito o apagamento está exemplificado nas Figuras. 4.8 e 4.9. Os quadrados preenchidos em cinza representam os bits "apagados"(zerados).

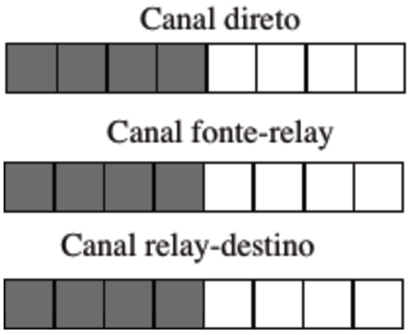

Figura 4.8: Exemplo de apagamento nos três canais em uma sequência de 4 bits das palavras-códigos, nas mesmas posições

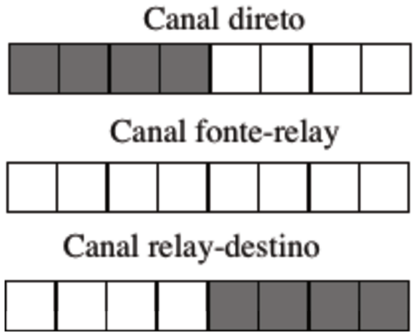

Figura 4.9: Exemplo de apagamento nos canais, direto e fonte-destino em uma sequência de 4 bits das palavras-códigos, em posições diferentes

A Figura 4.10 mostra o desempenho para uma sequência de 10 bits que foram "apagados" das palavras-códigos nos três canais. Obteve-se um ganho com o uso de cooperação de 2.7 dB, para uma BER de 10^{-5}, em comparação com a transmissão direta.

A Figura 4.11 corresponde ao sistema com apagamento em 50 bits, sendo esses presentes nos três canais, direto, fonte-relay e relay-destino. Obteve-se um ganho de 1.8 dB, para uma BER

de 10^{-5}, utilizando cooperação.

A Figura 4.12 corresponde ao sistema com apagamento em 100 bits, da mesma forma nos casos anteriores. Obteve-se um ganho na cooperação de 1.7 dB, para uma BER de 10^{-5}. O ganho observado nas Figuras 4.11 e 4.12 foi praticamente o mesmo, com uma diferença de 0.1 dB. Conforme o aumento do número de bits que sofrem apagamento, nota-se que o ganho tende a diminuir, o que é de se esperar, já que a quantidade erros aumenta.

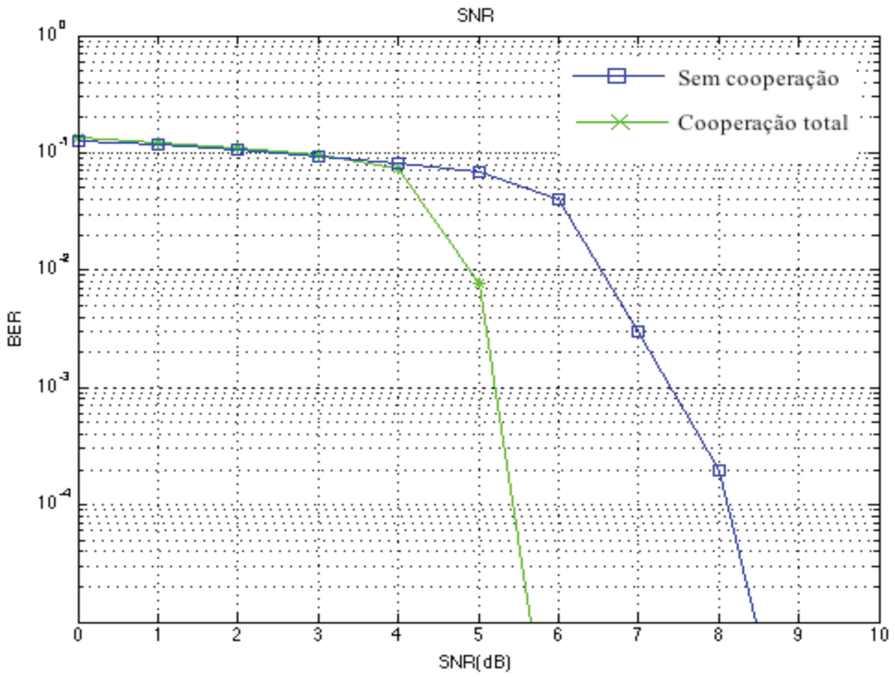

Figura 4.10: Apagamento de 10 bits nos três canais – mesma posição

Comparando as Figuras 4.10, 4.11 e 4.12, observa-se que nas mesmas condições de transmissão, o caso com menor quantidade de bits "apagados" obteve o maior ganho (uso de cooperação em relação à transmissão direta). Quanto maior o número de bits "apagados", mais erros são introduzidos e consequentemente, menor o desempenho.

Já na Figura 4.13 apresenta o desempenho do sistema com apagamento nos 50 primeiros bits nos canais direto e fonte-relay. Obteve-se um ganho de 2.8 dB, para uma BER de 10^{-5}.

E por fim, na Figura 4.14 apresenta o desempenho do sistema com apagamento nos 50 primeiros bits da palavra-código no canal direto e nos 50 últimos bits da palavra-código recebida pelo canal fonte-destino (os bits "apagados" em posições diferentes). Obteve-se um ganho de aproximadamente 5 dB, para uma BER de 10^{-5}.

O ganho foi maior para o caso dos bits apagados que se encontram posições diferentes. Isso pode ser explicado pelo fato de que quando eles estão em posições diferentes, o destino pode considerar a sequência de bits vinda do canal que não sofreu apagamento, e, portanto, desconsiderar os bits menos confiáveis. Em contrapartida, quando o apagamento ocorreu nas mesmas posições das palavras-códigos, o receptor não tem outra alternativa senão considerar o apagamento.

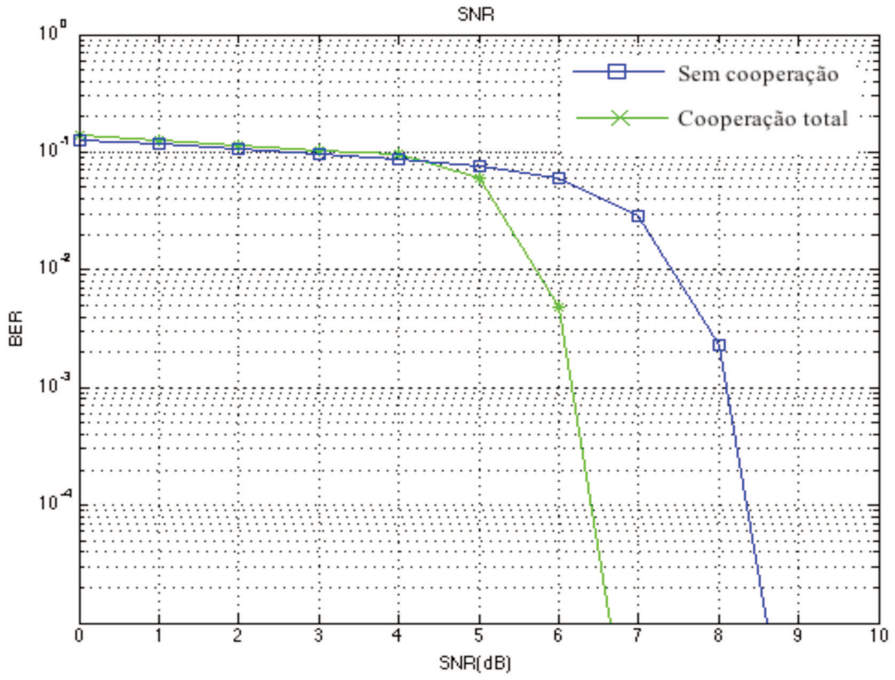

Figura 4.11: Apagamento de 50 bits nos três canais – mesma posição

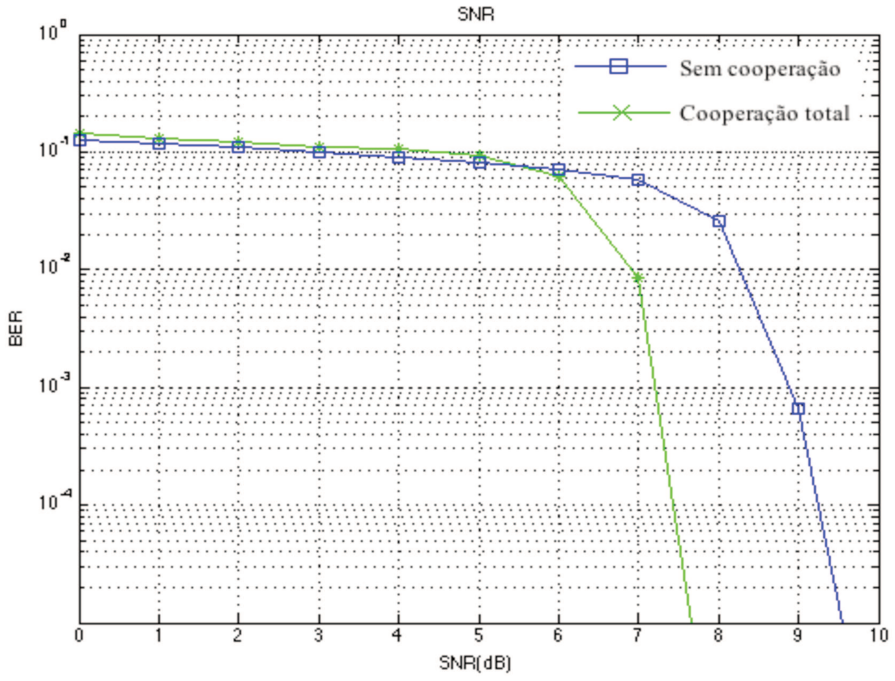

Figura 4.12: Apagamento de 100 bits nos três canais – mesma posição

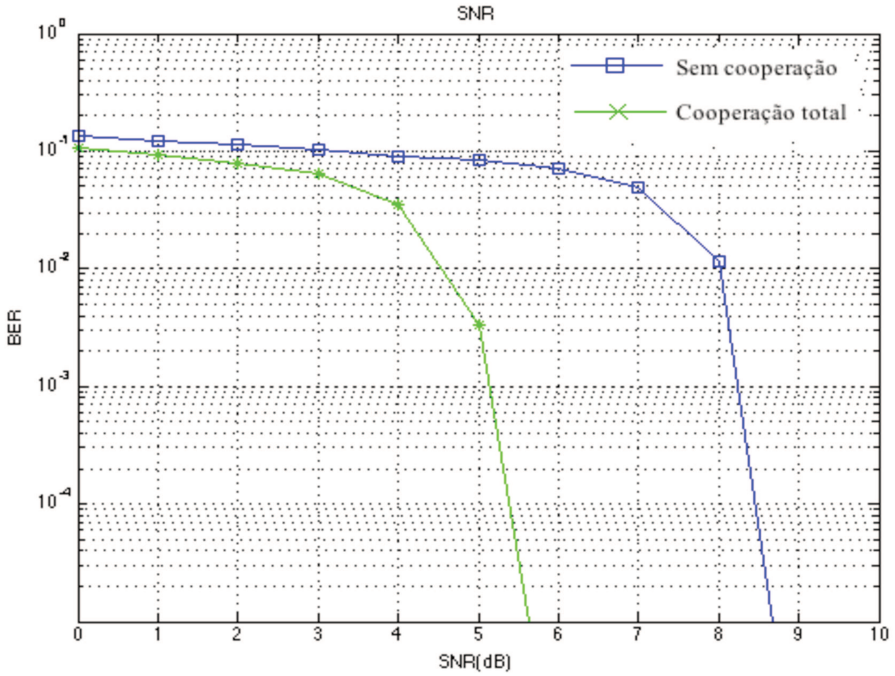

Figura 4.13: Apagamento de 50 bits nos canais direto e fonte-relay(mesmas posições)

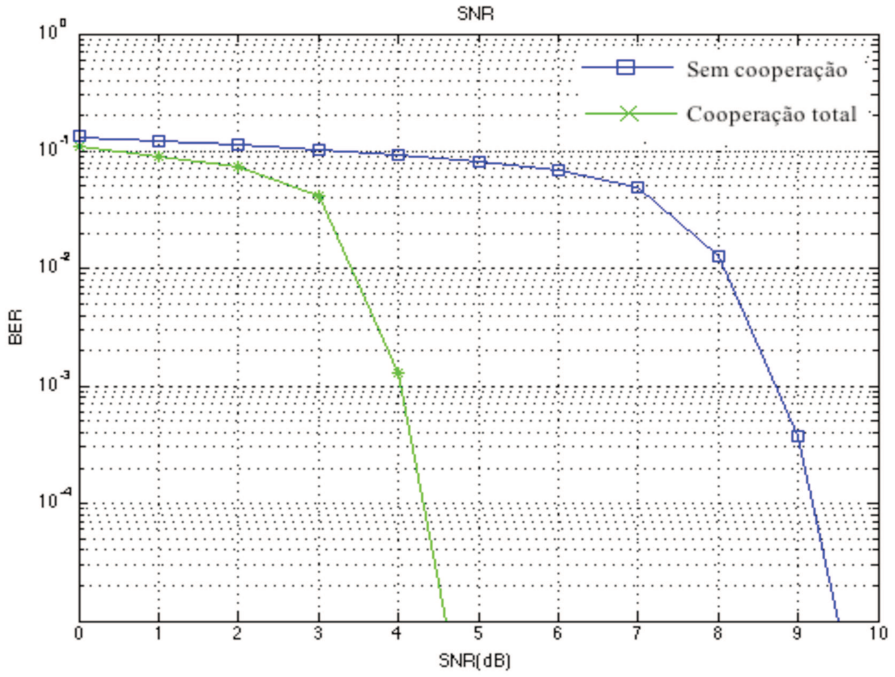

Figura 4.14: Apagamento de 50 bits nos canais direto e fonte-relay(posições diferentes)

Capítulo 5

Conclusões e Perspectivas

Comentários e Conclusões

Nesta dissertação de mestrado consideramos um sistema de comunicação onde a cooperação está integrada à codificação de canal através do uso de códigos LDPC binários. O desempenho deste sistema de cooperação codificada foi obtido para dois tipos de códigos LDPC. A associação das palavras códigos que chegam no destino via canal fonte-destino e relay-destino foi feita utilizando a confiabilidade de seus símbolos equivalentes, sendo escolhido para compor a palavra código decodificada aqueles símbolos de maior confiabilidade. A confiabilidade dos símbolos foi medida com base na distância euclidiana entre os símbolos provenientes de cada canal e os possíveis símbolos transmitidos. Assim, o protocolo de cooperação utilizado foi aquele baseado na decodificação, recodificação e retransmissão (*decode-re-encode and-forward*) para um canal com um único relay com ruído AWGN e desvanecimento plano.

A probabilidade de erro de bit do sistema foi obtida por métodos computacionais (Monte Carlo), com o fim de se analisar o desempenho do sistema de cooperação codificada proposto. Foi mostrado que a utilização de um canal alternativo (relay) pode ser vantajoso, principalmente quando o canal direto (fonte-destino) se encontra mais degradado que o percurso via relay. Os benefícios em se utilizar cooperação codificada podem ser vistos mais claramente nas curvas de desempenho traçadas no capítulo anterior. Os resultados indicaram que diversidade espacial obtida pela utilização de um retransmissor (relay) associada a codificação LDPC são uma forma eficiente de se combater os efeitos do desvanecimento no canal direto.

A contribuição deste trabalho se deu na proposta de um sistema simples de seleção dos dados codificados que chegam por canais distintos e na avaliação do seu desempenho utilizando-se códigos LDPC binários conhecidos. Desta forma, pode-se concluir que mesmo utilizando uma maneira simples de combinar as palavras código semelhantes que chegam ao destino é possível alcançar melhoras significativas na taxa de erro de bit. Geralmente, o projeto de cooperação faz uso de esquemas de múltiplos acessos (CDMA, OFDMA, TDMA) para transmissão de dados entre os usuários e a estação radio-base. Por conveniência e simplicidade, mas sem perda da generalidade, foi considerada a modulação PSK binária para transportar os dados pelos canais.

Trabalhos Futuros

Os resultados apresentados neste trabalho mostraram que há inúmeras possibilidades para se explorar e melhorar o desempenho da comunicações por cooperação codificada. Entre elas podemos citar:

• Estender este simples caso para outros esquemas de transmissão e de múltiplos acessos com outros tipos de desvanecimento.

• Considerar o caso com mais de um retransmissor (relay) e escolhendo aquele que tem melhor desempenho. ainda utilizando códigos LDPC.

• Busca de códigos LDPC quasi-cíclicos mais adequados para a realização de sua partição, como por exemplo códigos cuja construção se baseia em quadrados latinos (latim square).

• Procurar outras formas de realizar a associação dos dados codificados que chegam ao destino via diferentes canais.

• Utilização de códigos LDPC não binários nos esquemas de cooperação codificada.

• Utilização de outros tipos de codificação distintos da LDPC.

Publicações

CUNHA, E. N. ; BALDINI FILHO R . A Simple Cooperative LDPC Coding Scheme. In: V International Workshop on Telecommunications - ITW 2013, 2013, Santa Rita do Sapucaí. Proceedings - International Workshop on Telecommunicatios. Santa RIta do Sapucaí: INATEL, 2013. v. 1.

Bibliografia

Abrantes, S. A. (2005). *Descodificação iterativa de códigos LDPC por transferência de mensagens em grafos de factores.*

Alegri, M. (2006). *Quadrados latinos e aplicações.*

Bernhard M.J. Leiner, S. (2009). LDPC codes–a brief tutorial, *Information Theory, IEEE Transactions on* .

Blázovics, L., Varga, C., Bamford, W., Zanaty, P. & Fitzek, F. (2011). Future cooperative communication systems driven by social mobile networks, *Wireless Personal Communications* **57**(3): 377–391.
URL: *http://dx.doi.org/10.1007/s11277–010-0075–8*

Chakrabarti, A., Erkip, E., Sabharwal, A. & Aazhang, B. (2007). Code designs for cooperative communication, *Signal Processing Magazine, IEEE* **24**(5): 16–26.

Cover, T. & Gamal, A. (1979). Capacity theorems for the relay channel, *Information Theory, IEEE Transactions on* **25**(5): 572–584.

Duyck, D., Boutros, J. & Moeneclaey, M. (2011). Low–density graph codes for coded cooperation on slow fading relay channels, *Information Theory, IEEE Transactions on* **57**(7): 4202–4218.

Ferro, V. L. D. (2011). *Comparação Entre Algorítmos de Decisão em Sistemas de Comunicação com Codificação Cooperativa.*

Fitzek, F. H. P., K. M. (2006). *Cooperation in wireless networks: Principles and applications–real egoistic behavior is to cooperate.*, Springer Publishing Company.

Fitzek, F. H. P. & Katz, M. D. (2007). *Cognitive Wireless Networks: Concepts, Methodologies and Visions Inspiring the Age of Enlightenment of Wireless Communications*, 1st edn, Springer Publishing Company, Incorporated.

Gallager, R. G. (1963). *Low–Density Parity–Check Codes.*

Gomes, M. A. (2003). *Códigos binários definidos por matrizes de teste de paridade esparsas algoritmos de decodificação*, Tese de Mestrado em Engenharia Electrotécnica e de Computadores - Departamento de Engenharia Electrotécnica e de Computadores da Fac. de Ciências e Tecnologia de Coimbra. Coimbra.

Gonçalves, M. L. (2010). *Códigos LDPC Quaternários Aplicados à Técnica de Transmissão OFDM.*

Gupta, P., Kramer, G. & Wijngaarden, A. J. V. (2004). *Advances In Network Information Theory: Dimacs Workshop Network Information Theory, March 17–19, 2003, Piscataway, New Jersey (Dimacs Series in Discrete Mathematics and Theoretical Computer Science)*, American Mathematical Society, Boston, MA, USA.

Hunter, T. E. (n.d.). *Coded Cooperation: A New Framework For User Cooperation In Wireless Networks*, Doctor of Philosophy in Electrical Engineering, The University of Texas at Dallas.

Hunter, T. & Nosratinia, A. (2006). Diversity through coded cooperation, *Wireless Communications, IEEE Transactions on* **5**(2): 283–289.

Johnson, S. J. (0000). Introducing low–density parity–check codes, *Technical report*, Department of Electrical and Computer Engineering, University of Newcastle, Australia.

Karkooti, M. & Cavallaro, J. (2008). Cooperative communications using scalable, medium block–length ldpc codes, *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pp. 88–93.

Khatir, K. (2007). *Coded Cooperative Communications*, Electrical Engineering Blekinge, Instituto de Tecnologia Karlskrona.

Kong, L. & Xiao, Y. (2008). Construction of good quasi–cyclic ldpc codes based on the row vectors of generator matrix, *Wireless, Mobile and Multimedia Networks (ICWMMN 2008), IET 2nd International Conference on*, pp. 215–218.

Kristensen, J. M., F. F. H. P. (2007). *Cognitive wireless networks: Cognitive wireless networks–cellular controlled P2P communication using software defined radio*, Springer.

Laneman, J., Tse, D. & Wornell, G. W. (2004). Cooperative diversity in wireless networks: Efficient protocols and outage behavior, *Information Theory, IEEE Transactions on* **50**(12): 3062–3080.

LDPC Coded Modulation – Ceragon (2009).

Lin, S. & Costello, D. (2004). *Error Control Coding: Fundamentals and Applications*, Pearson–Prentice Hall.
URL: *http://books.google.com.br/books?id=0nVfQgAACAAJ*

Liu, K. J. R., Sadek, A. K., Su, W. & Kwasinski, A. (2009). *Cooperative Communications and Networking*, Cambridge University Press, New York, NY, USA.

MacKay, D. J. C. (1999). Good error–correcting codes based on very sparse matrices, *Information Theory, IEEE Transactions on* **45**(2): 399–431.

MacKay, D. J. C. & Neal, R. M. (1997). Near shannon limit performance of low density parity check codes, *Electronics Letters* **33**(6): 457–458.

Malema, G. A. (2007). Low–density parity–check codes: Construction and implementation, *Technical report*, Doutorado em Filosofia na Faculdade de Engenharia Elétrica–Universidade de Adelaide, Australia.

Mataveli, L. O. (2008). *Avaliação do Algorítmo de Busca de Sequências de Espalhamento em Canais com Desvanecimento Seletivo em Frequência com códigos Corretores de Erros*, Tese mestrado FEEC–DECOM.

Moreira, J. & Farrell, P. (2006). *Essentials of Error–Control Coding*, Wiley.
URL: *http://books.google.com.br/books?id=QmZQ–A76FusC*

Nosratinia, A., Hunter, T. & Hedayat, A. (2004). Cooperative communication in wireless networks, *Communications Magazine, IEEE* **42**(10): 74–80.

Perrucci, G. P., Fitzek, F. H. P., Zhang, Q. & Katz, M. D. (2009). Cooperative mobile web browsing, *EURASIP J. Wirel. Commun. Netw.* **2009**: 7:1–7:9.
URL: *http://dx.doi.org/10.1155/2009/543054*

Sendonaris, A., Erkip, E. & Aazhang, B. (2003). User cooperation diversity–part (i) and part (ii), **51**(11): 1927–1948.

Shokrollahi, A. (2003). LDPC codes: An introduction, *Digital Fountain, Inc., Tech. Rep* p. 2.

Xiao, Y. (2009). *MIMO Multiple Antenna Wireless Communication Systems.*

Xiao, Y. (2010). *Turbo and LDPC Codecs and their Applications.*

Xiao, Y. & Kim, K. (2008). Good encodable irregular quasi–cyclic ldpc codes, *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on*, pp. 1291–1296.

Xiao, Y. & Lee, M. H. (2006). Construction of good quasi–cyclic ldpc codes, *Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on*, pp. 1–4.

Yacoub, M. D. (1993). *Foundations of Mobile Radio Engineering*, 1st edn, CRC Press, Inc., Boca Raton, FL, USA.

Zhang, L., Huang, Q., Lin, S., Abdel-Ghaffar, K. & Blake, I. (2010). Quasi–cyclic ldpc codes: An algebraic construction, rank analysis, and codes on latin squares, *Communications, IEEE Transactions on* **58**(11): 3126–3139.

Zhao, D. & Li, D. (2008). Two types of ldpc decoding methods for coded cooperation, *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on*, pp. 1–4.

Zhao, D. & Li, D. (2009). Coded cooperation using LDPC codes, *Global Mobile Congress 2009*, pp. 1–4.

Zimmermann, E., Herhold, P. & Fettweis, G. (2005). On the performance of cooperative relaying protocols in wireless networks, *Eur. Trans. Telecomm* **16**: 5–16.