

Esquema de Codificação LDPC para Canais de Resposta Parcial Baseado em Códigos RA

Andrei P. Legg e Bartolomeu F. Uchôa Filho

Resumo—Neste artigo, um esquema de codificação LDPC para canais de resposta parcial (PR) baseado na estrutura dos códigos “acumula-repete” (RA, *repeat-accumulate codes*) é proposto. O codificador original RA é modificado a fim de se obter uma relação um-para-um entre a seqüência aqui chamada de \mathcal{D} -palavra-código (que não é a palavra-código transmitida) e a seqüência recebida livre de ruído na saída do canal de resposta parcial. Isto gera a necessidade da definição de um grafo para o decodificador (diferente do grafo do codificador), que considera a \mathcal{D} -palavra-código como palavra-código “verdadeira”. A simplicidade do decodificador, devida à remoção da interferência (pré-codificação), e a complexidade de codificação linear, ao invés de quadrática, tornam a estrutura proposta atrativa para uma aplicação prática. Um código LDPC de taxa $R = 3648/4096 = 0.89$ foi projetado para o canal $1 - D$ (“dicode”). Um ganho de codificação, obtido via simulação computacional, de aproximadamente 5 dB para uma taxa de erro de bit 10^{-5} foi verificado.

Palavras-Chave— Armazenamento de dados, códigos “repete-acumula”, códigos de baixa densidade de verificação de paridade, canais de resposta parcial, precodificação.

Abstract— In this paper, we propose an LDPC coding scheme based on repeat-accumulate (RA) codes for partial response channels. We modify the original RA encoder in such a way that there exists a one-to-one relationship between a sequence called the \mathcal{D} -codeword (which is not the transmitted codeword) and the noiseless received sequence at the output of the partial response channel. This forces us to define a graph (different from the encoder graph) for the decoder, which takes the \mathcal{D} -codeword as the true codeword. The simplicity of the decoder, coming from the interference removal (precoding), and the linear, as opposed to quadratic, complexity of the encoder make the proposed scheme attractive for a practical application. For a code rate $R = 3648/4096 = 0.89$ and for the dicode channel, an LDPC code has been designed and a simulated coding gain of about 5 dB for a bit error rate 10^{-5} was obtained.

Keywords— Data storage, repeat-accumulate codes, low-density parity-check codes, partial response channels, precoding.

I. INTRODUÇÃO

Motivado pelo excelente desempenho dos códigos turbo e dos códigos de verificação de paridade de baixa densidade (LDPC) no canal Gaussiano, pesquisadores tornaram-se interessados em projetar esquemas de codificação, baseados nestes códigos, para os canais de resposta parcial (PR). Canais PR são conhecidos por modelarem os canais de gravação magnética de alta-densidade. Os primeiros trabalhos consideraram a

chamada *equalização-turbo* [2], onde a precodificação faz com que o canal PR (considerado como um código interno) torne-se recursivo, uma necessidade para o bom desempenho de erro em tais sistemas de codificação.

Mostrou-se em [2] que a escolha do pré-codificador afeta o desempenho de erro dos esquemas de equalização-turbo em canais PR. Por outro lado, em um sistema que emprega códigos convolucionais para o canal PR descrito pelo polinômio $g(D)$, o pré-codificador tem função de transferência $1/g(D)$ (modulo 2), e tem como propriedade realizar um mapeamento um-para-um entre a seqüência de entrada bipolar e a seqüência formada na saída do canal PR [6].

Li *et al.* [1] propuseram os chamados códigos produto turbo baseados em códigos de verificação de paridade (TPC/SPC) para os canais PR. Enquanto a complexidade do decodificador MAP (maximum *a posteriori*) para códigos turbo é bastante alta, os códigos TPC/SPC e os códigos LDPC surgem como soluções interessantes, pois suas complexidades da decodificação são muito mais baixas. Em particular, a complexidade de decodificação de códigos LDPC aumenta com $O(N)$, onde N é o comprimento do bloco. Por outro lado, a complexidade de codificação de códigos LDPC é $O(N^2)$. Este fato foi uma das razões pelas quais alguns trabalhos, inclusive [1], não consideram o uso de códigos LDPC para os canais PR.

Muitos pesquisadores desenvolveram maneiras eficientes de codificar códigos LDPC com complexidade mais baixa [3]. Os códigos “acumula-repete” (RA, *repeat-accumulate codes*) [4] são uma das soluções que possuem um algoritmo de codificação linear no tempo. Deve-se notar que os bits de verificação de paridade de um código RA correspondem a uma pré-codificação com a função de transferência $1/(1 \oplus D)$ de uma determinada seqüência de bits no algoritmo de codificação, onde \oplus denota a soma modulo 2.

Neste artigo, propomos um esquema de codificação RA modificado para os canais PR que estende a pré-codificação do codificador RA original aos bits de informação. A idéia é transmitir através do canal de PR uma seqüência (a \mathcal{E} -palavra-código) que corresponde à pré-codificação da chamada \mathcal{D} -palavra-código, a seqüência que, devido ao mapeamento um-para-um, será tomada como palavra-código no decodificador LDPC. A complexidade do codificador proposto é essencialmente a mesma do esquema original do RA, *i.e.*, linear em N , e a complexidade de decodificação é ligeiramente menor do que aquela do decodificador RA original. O sistema é descrito para o canal $1 - D$ (dicode), mas a extensão para os canais PR descritos por $(1 - D)(1 + D)^n$, $n \geq 1$, é indicada. Considerando um código LDPC de taxa igual a

Grupo de Pesquisa em Comunicações (GPqCom), Departamento de Engenharia Elétrica, Universidade Federal de Santa Catarina, Florianópolis, SC, 88040-900. Email: andrei.legg@gmail.com, uchoa@eel.ufsc.br

Este trabalho foi financiado em parte pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), sob os números de processo 140671/2007-2, 484391/2006-2 e 302286/2004-7.

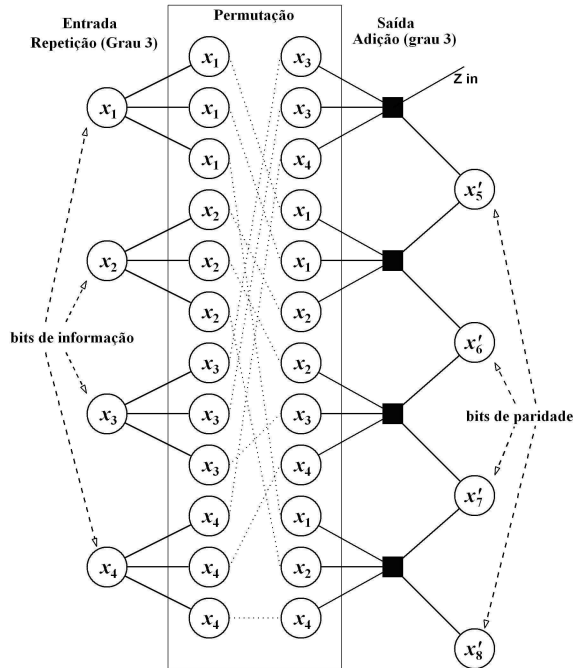


Fig. 1. Grafo de Tanner para o codificador/decodificador de um código RA de taxa 4/8. É apresentada uma permutação arbitrária. Nesta figura, temos $z_{in} \equiv 0$.

0.89 e com um comprimento do bloco de 4 Kbits, uma simulação computacional revela um ganho da codificação de aproximadamente 5 dB a uma probabilidade de erro de bit (BER) 10^{-5} em relação ao canal $1 - D$ não-codificado.

Na próxima seção, o esquema RA será descrito sucintamente. A proposta deste artigo é apresentada na Seção III, onde o codificador é descrito na Subseção III-A, e o decodificador na Subseção III-B. Na Seção IV são apresentados os resultados da simulação. E por fim, a Seção V conclui o artigo.

II. CÓDIGOS ACUMULA-REPETE (RA)

Os códigos RA [4] formam uma sub-classe especial dos códigos LDPC que possuem complexidade de codificação linear em N . Isto representa uma grande vantagem, visto que, em geral, a complexidade de codificação dos LDPCs é quadrática em N . Os códigos RA possuem um codificador e um decodificador que fazem uso das propriedades do grafo que representa o código LDPC. Isso possibilita uma codificação bastante simples e eficiente, como veremos a seguir.

Por questão de simplicidade, vamos considerar nesta e na próxima seções um código curto da taxa 4/8. O codificador para um código RA de taxa 4/8 é representado pelo grafo de Tanner [5] mostrado na Fig. 1. Os nós de variável x_1, x_2, x_3 e x_4 são associados aos bits de informação. Essa informação é triplicada (neste exemplo) gerando uma nova seqüência com 12 “bits de informação”, que sofre uma permutação aleatória. A seqüência resultante desta permutação é somada (três a três) nos nós de função, assim gerando os bits de paridade x'_5, x'_6, x'_7 e x'_8 .

A matriz de verificação de paridade desse código é

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

Pode-se notar que, devido à permutação, alguns bits de informação se ligam a apenas um nó de função. Também, pode ocorrer de um mesmo nó de variável se ligar repetidamente a um mesmo nó de função. Neste caso, deve-se verificar o número de vezes que esse nó de variável se liga a esse nó de função. Se esse número for par, devido à soma módulo 2 que é realizada nos nós de função, considera-se que esse nó de variável não contribui para esse nó de função. Veja, por exemplo, o nó de variável x_3 na Fig. 1, que se liga duas vezes ao primeiro nó de função (de cima pra baixo). Observe a matriz de verificação de paridade H onde a primeira linha representa todas as conexões desse primeiro nó de função aos nós de variável. A conexão com o nó x_3 é representada pelo terceiro elemento dessa linha, e esse elemento na matriz é igual a 0, que significa a ausência de conexão.

Esta arquitetura do codificador possibilita a escolha da taxa desejada com facilidade, possibilitando ainda o uso de várias taxas num mesmo sistema, criando um algoritmo que altere o grau de repetição na entrada, o grau da soma na saída, ou até mesmo os dois, fazendo o codificador variável conforme a taxa desejada.

A decodificação dos códigos RA pode ser realizada pelo algoritmo soma-produto (SPA) [7] aplicado ao grafo de Tanner da Fig. 1, da forma usualmente adotada para LDPCs em geral.

III. ESQUEMA DE CODIFICAÇÃO LDPC PARA O CANAL $1 - D$ BASEADO NO CÓDIGO RA

A. O Codificador

O grafo de Tanner para o codificador é mostrado na Fig. 2. Como é feito usualmente, os nós de variável são denotados por \circ e os nós de função (ou de verificação de paridade) são denotados por \blacksquare . Os nós de variável x_1, x_2, x_3 e x_4 são associados aos bits de informação. O processo de codificação é apresentado a seguir.

O valor do bit x_1 de informação é enviado ao nó de variável x'_1 através do primeiro nó de função (a esquerda, de cima para baixo na Fig. 2). x'_1 é o primeiro bit da seqüência que será transmitida através do canal $1 - D$. Esta seqüência é aqui chamada de \mathcal{E} -palavra-código, onde \mathcal{E} se refere ao “codificador” (*encoder*). O bit x'_1 é somado (módulo 2) ao bit x_2 de informação, assim obtendo x'_2 . Prossegue-se dessa forma até que x'_4 seja obtido. O restante do algoritmo codificador é similar ao algoritmo codificador do RA original. Os bits de informação (neste exemplo) são triplicados para originar uma nova seqüência com 12 “bits de informação”. Estes são permutados por uma permutação arbitrária e são então agrupados em quatro blocos de três bits cada um. O bit x'_4 ($\equiv z_{out} \equiv z_{in}$) e os três bits no primeiro bloco (a direita, de cima para baixo na Fig. 2) são somados (módulo 2) formando o bit x'_5 . De uma maneira similar, $x'_6 \equiv x'_5 \oplus x_1 \oplus x_2 \equiv x'_5 \oplus x_2$. Continua desta forma até que x'_8 seja obtido. A complexidade

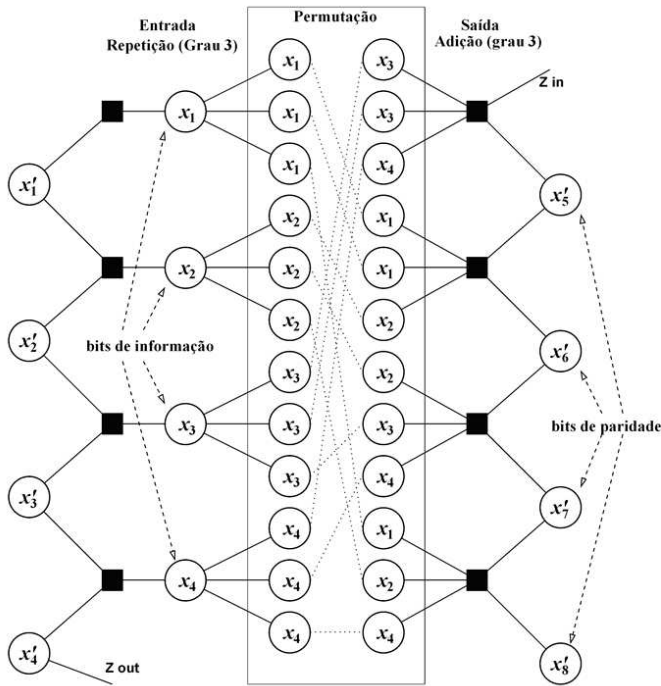


Fig. 2. Grafo de Tanner para o codificador de um código LDPC baseado em códigos RA de taxa 4/8 projetado para o canal $1 - D$. É apresentada uma permutação arbitraria. Nesta figura, $z_{in} \equiv z_{out}$.

deste algoritmo codificador para um comprimento N de bloco é $O(N)$.

A \mathcal{E} -palavra-código, (x'_1, \dots, x'_8) , é formatada para o formato bipolar (± 1) e é então transmitida através do canal $1 - D$. Deve-se notar que a \mathcal{E} -palavra-código é exatamente a seqüência produzida quando a seqüência (x_1, \dots, x_8) , chamada de \mathcal{D} -palavra-código (\mathcal{D} se referindo ao “decodificador”), é passada através do pré-codificador com função de transferência $1/(1 \oplus D)$. Os últimos quatro bits da \mathcal{D} -palavra-código são dados por: $x_5 \equiv x_3 \oplus x_3 \oplus x_4 \equiv x_4$, $x_6 \equiv x_1 \oplus x_1 \oplus x_2 \equiv x_2$, $x_7 \equiv x_2 \oplus x_3 \oplus x_4$, e $x_8 \equiv x_1 \oplus x_2 \oplus x_4$. Isto é, estes bits são obtidos fazendo a soma modulo 2 dos grupos de bits formados após a permutação.

É bem conhecido que a pré-codificação inverte o canal PR “no sentido binário” [6]. Em particular, se $\{x_k\}$ for uma seqüência binária na entrada do pré-codificador, $\{x'_k\}$ for a seqüência binária produzida na saída do pré-codificador, $\{\tilde{x}'_k = 2x'_k - 1\}$ for a seqüência bipolar transmitida através do canal de PR, e $\{y'_k\}$ a seqüência formada na saída do canal de PR, então na ausência do ruído $\{x_k\}$ pode ser recuperado de acordo com

$$x_k \equiv \frac{|y'_k|}{2} \pmod{2} \quad (1)$$

Este fato é levado em consideração no algoritmo de decodificação, descrito a seguir.

B. O Decodificador

Considere a seqüência de símbolos (y'_1, \dots, y'_8) , que denota a seqüência recebida na ausência do ruído na saída do canal $1 - D$, e seja (y_1, \dots, y_8) sua versão ruidosa, onde o ruído é considerado ser o Gaussiano, branco e aditivo (AWGN) com média zero e variância $\sigma^2 = N_0/2$. Devido à memória do

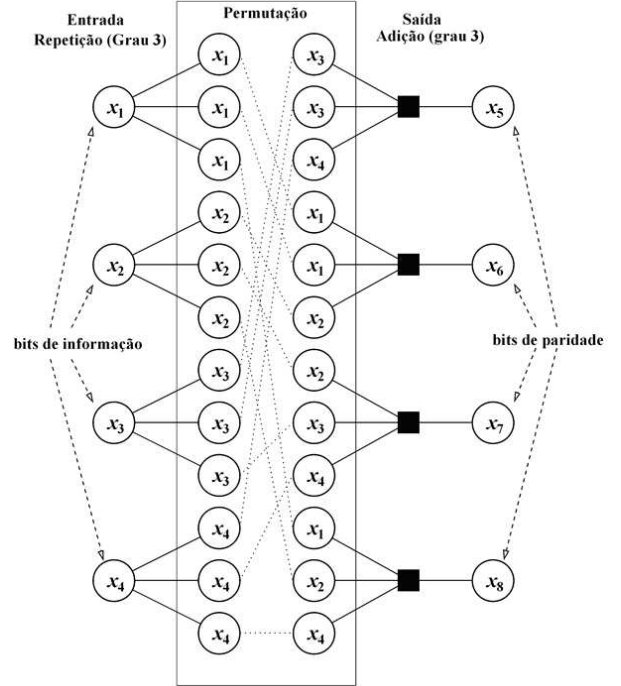


Fig. 3. Grafo de Tanner para o decodificador.

canal $1 - D$, os símbolos $y'_k \in \{0, \pm 2\}$, para $k = 1, \dots, 8$ como anteriormente comentado, possuem uma relação de um-para-um (dada em (1)) entre a \mathcal{D} -palavra-código (x_1, \dots, x_8) e a seqüência recebida sem ruído (y'_1, \dots, y'_8) . Uma vez que o decodificador considera uma outra seqüência como palavra-código, um grafo de Tanner diferente deve ser considerado e uma nova matriz de verificação de paridade definida para o algoritmo de decodificação. O grafo de Tanner para o decodificador é mostrado na Fig. 3.

Deve-se anotar que, devido à remoção da interferência (pré-codificação), o sub-grafo com “zigzag” que apareceu na Fig. 2 foi removido na Fig. 3. Isto faz com que a decodificação seja menos complexa, porque a matriz de verificação de paridade H será mais esparsa. Além disso, H será uma matriz sistemática, embora não seja possível tirar proveito deste fato uma vez que esta matriz não é útil ao codificador. (A \mathcal{E} -palavra-código não é sistemática!)

A matriz de verificação de paridade considerada no algoritmo de decodificação do nosso exemplo ilustrativo é

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

O algoritmo soma-produto [7] é aplicado ao grafo da Fig. 3 para recuperar os bits de dados transmitidos através do canal $1 - D$ ruidoso. O fluxo do algoritmo (envio de mensagem) é o mesmo seguido para todos os demais códigos LDPC, com matriz de verificação de paridade (esparsa) H . Entretanto, como os símbolos transmitidos pertencem a $\{0, \pm 2\}$, e considerando a relação um-para-um apresentada em (1), precisamos obter a probabilidade *a posteriori* (APP) $P_k = \Pr(x_k = 1|y_k)$, que é a probabilidade de o bit x_k da \mathcal{D} -palavra-código ser 1, dado o conhecimento do símbolo recebido y_k , para $k = 1, \dots, 8$.

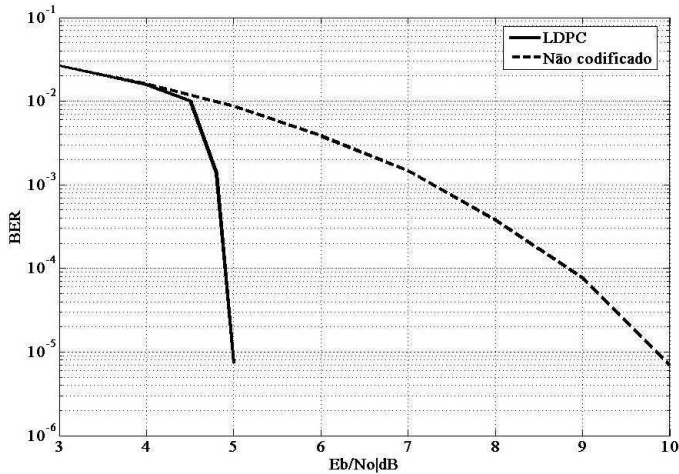


Fig. 4. Resultado de simulação.

Estas APPs são usadas na inicialização do algoritmo SPA.

Para o canal $1 - D$, temos as seguintes densidades de probabilidades condicionadas:

$$p(y_k | x_k = 1, y'_k = -2) \Pr(x_k = 1, y'_k = -2) = \frac{0.25}{\sigma\sqrt{2\pi}} e^{-\frac{(y_k+2)^2}{2\sigma^2}}, \quad (2)$$

$$p(y_k | x_k = 1, y'_k = +2) \Pr(x_k = 1, y'_k = +2) = \frac{0.25}{\sigma\sqrt{2\pi}} e^{-\frac{(y_k-2)^2}{2\sigma^2}}, \quad (3)$$

e

$$p(y_k | x_k = 0, y'_k = 0) \Pr(x_k = 0, y'_k = 0) = \frac{0.5}{\sigma\sqrt{2\pi}} e^{-\frac{y_k^2}{2\sigma^2}}, \quad (4)$$

de onde podemos facilmente obter

$$P_k = \Pr(x_k = 1 | y_k) = 1 - \frac{1}{1 + \exp\left(\frac{-2}{\sigma^2}\right) \cosh\left(\frac{2y_k}{\sigma^2}\right)}. \quad (5)$$

IV. SIMULAÇÃO E DESEMPENHO DE ERRO

Um código LDPC baseado em códigos RA, como descrito na Seção III, foi projetado para o canal $1 - D$. A taxa do código é $R = 3648/4096 = 0.89$, por ser uma prática comum na literatura de códigos baseados em grafos para a gravação magnética [1]. A permutação foi realizada de forma pseudo-aleatória. O número máximo de iterações no SPA foi ajustado para 15. A BER versus E_b/N_0 é apresentada na Fig. 4, de onde se pode observar um ganho de codificação de aproximadamente 5 dB a uma BER = 10^{-5} . Um ganho similar de codificação foi obtido em [1] para o canal PR4 com a mesma taxa de código. Devemos observar que, além de ter um desempenho de erro muito bom, o esquema proposto neste trabalho tem a complexidade de codificação linear com o comprimento de bloco, e a matriz de verificação de paridade adotada em seu decodificador é facilmente obtida, baseada na permutação pseudo-aleatório realizada.

V. CONCLUSÃO

Neste artigo, um esquema de codificação LDPC baseado em códigos repete-acumula foi proposto para canais de resposta parcial. O codificador e o decodificador possuem complexidade linear com o comprimento de bloco, o que torna este esquema atrativo para uma aplicação prática. Foi observado através de simulação por computador que o código possui um bom desempenho para o canal $1 - D$. A extensão da técnica proposta para outros canais PR, como o PR4 e o EPR4 [1], [6], que modelam os canais de gravação magnética de alta densidade, é perfeitamente possível e de fácil implementação. Seria necessário apenas modificar a topologia do “zigzag” do grafo para o codificador, de acordo com a função de transferência de pré-codificação para o canal de resposta parcial correspondente, e encontrar as novas probabilidades *a posteriori* para a inicialização do algoritmo soma-produto, pois os canais PR de ordem mais elevada podem apresentar múltiplos níveis de amplitude de saída. Por outro lado, devido à remoção da interferência (pré-codificação), o grafo para o decodificador para *qualquer* canal PR permanece exatamente o mesmo mostrado na Fig. 3.

REFERÊNCIAS

- [1] J. Li, K. R. Narayanan, E. Kurtas, and C. N. Georghiadis, “On the performance of high-rate TPC/SPC codes and LDPC codes over partial response channels,” *IEEE Trans. on Commun.*, vol. 50, no. 5, pp. 723-734, May 2002.
- [2] K. R. Narayanan, “Effect of precoding on the convergence of turbo equalization for partial response channels,” *IEEE J. Select. Areas Commun.*, vol. 19, no. 4, pp. 686-698, Apr. 2001.
- [3] C. B. Schlegel and L. C. Pérez, *Trellis and Turbo Coding*, IEEE Press and Wiley-Interscience, 2004.
- [4] D. Divsalar, H. Jin, and R. J. McEliece, “Coding theorems for ‘turbo-like’ codes,” in *Proc. 36th Allerton Conf. on Communication, Control, and Computing*, pp. 201-210, (Allerton, Illinois, Sept. 1998).
- [5] R. M. Tanner, “A recursive approach to low complexity codes,” *IEEE Trans. Inf. Theory*, vol. IT-27, no. 5, pp. 533-547, Sept. 1981.
- [6] B. F. Uchôa Filho and M. A. Herro, “Good convolutional codes for the precoded $(1 - D)(1 + D)^n$ partial response channels,” *IEEE Trans. on Inf. Theory*, vol. 43, no. 2, pp. 441-453, Mar. 1997.
- [7] F. R. Kschischang, B. Frey, and H.-A. Loeliger, “Factor graphs and the sum-product algorithm,” *IEEE Trans. on Inf. Theory*, vol. 47, no. 2, pp. 498-519, Feb. 2001.