

Design of Nonbinary LDPC Codes over GF(q) for Multiple-Antenna Transmission

Rong-Hui Peng and Rong-Rong Chen

Dept. of Electrical and Computer Engineering, University of Utah, Salt Lake City, UT 84112

Email: {peng, rchen}@eng.utah.edu

Abstract—In this paper, we investigate the application of nonbinary low density parity check (LDPC) codes over Galois field GF(q) for multiple-input multiple-output (MIMO) fading channels. Depending on the size of the Galois field GF(q), we study both iterative systems which employ joint MIMO detection and channel decoding, and non-iterative systems which employ separate MIMO detection and channel decoding. Based on the concept of coset LDPC code and coset MIMO detector, we develop extrinsic information transfer chart (EXIT) approaches for the design of nonbinary LDPC codes for MIMO channels. Simulation results show that the proposed systems employing the designed nonbinary LDPC codes achieve a superior performance than that of the best optimized binary LDPC codes at a reduced complexity.

I. INTRODUCTION

In recent years, multiple antenna transmission has been identified as one of the most practical methods to combat fading and increase the capacity of wireless channels. There has been much research on designing good channel codes such as turbo codes and low density parity check (LDPC) codes to realize the capacity gain promised by the multiple antenna channel. In particular, LDPC codes, originally devised by Gallager in 1963 [1][2] have attracted substantial interest due to their capacity approaching performance and great flexibility in code design and practical implementation. It has been shown that well designed irregular LDPC codes can achieve within a fraction of a dB of the Shannon limit for a wide class of channels [3]. In [4], the design of binary irregular LDPC codes is investigated for multiple-input multiple-output (MIMO) channels. The optimized binary LDPC codes demonstrate excellent capacity-approaching performances for MIMO channels. Most research [4], [5], however, focuses on the design and construction of binary LDPC codes.

Nonbinary LDPC codes were first investigated by Davey and Mackay in 1998 [6]. It is shown that nonbinary LDPC codes constructed over higher order Galois fields may obtain superior performance than the binary codes. Recently, irregular nonbinary LDPC codes over GF(q) are constructed by Hu *et al.* using the progressive edge growth (PEG) algorithm [7]. The performance of these codes improves as the size of the Galois field q increases. Furthermore, it is shown that the best nonbinary codes become almost regular for large values of q [7]. In recent work, nonbinary LDPC codes are applied to the nonbinary AWGN channel [8] and MIMO channels [9]. These codes demonstrate better performance than that of

the binary LDPC codes when concatenated with multilevel codes (MLC) [5] or used in conjunction with bit-interleaved coded modulation with iterative decoding (BICM-ID) [10][11]. However, these works do not address the code design issue of the nonbinary LDPC codes.

In previous work [8], EXIT chart is used to design nonbinary LDPC codes for AWGN channels and discrete memoryless channels. In this paper, we first extend the EXIT chart approach to the MIMO channel and consider a nonbinary iterative system employing joint MIMO detection and channel decoding. We propose two general methods based on open-loop simulation to compute the EXIT curves. Compared to the method in [8], we relax the Gaussian assumption on the density of the logarithmic likelihood ratios (LLR) to obtain more accurate design of nonbinary LDPC codes and better prediction of the convergence threshold. We also introduce the concept of MIMO coset detector which makes it feasible to compute the EXIT curves for the MIMO detector. To the best of our knowledge, this is the first work to study the design of nonbinary LDPC codes for MIMO channels. Simulation results demonstrate that the nonbinary LDPC codes designed by the proposed methods outperform the best optimized binary LDPC codes in both performance and complexity. In addition to the iterative system, we also propose a non-iterative system employing LDPC codes over large Galois field. The non-iterative system leads to excellent performance at the cost of an increased decoding complexity.

This paper is organized as follows. In Section II, we introduce the channel model. In Section III, we propose an iterative system where a symbol-wise MIMO detector is concatenated with the nonbinary LDPC codes. Nonbinary LDPC design using EXIT chart is discussed in Section IV. In Section V, we consider an alternative non-iterative system where a nonbinary LDPC over a large Galois field GF(q) is employed. Simulation results and performance comparisons are presented in Section VI. Complexity analysis is given in Section VII. Finally, we conclude in Section VIII.

II. CHANNEL MODEL

Consider a MIMO channel with N_t transmit antennas and N_r receive antennas. The channel model can be described as

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{n} \quad (1)$$

where $\mathbf{s} \in \mathbb{C}^{N_t}$, $\mathbf{y} \in \mathbb{C}^{N_r}$, and $\mathbf{n} \in \mathbb{C}^{N_r}$ are complex column vectors that represent the transmitted signal, received signal,

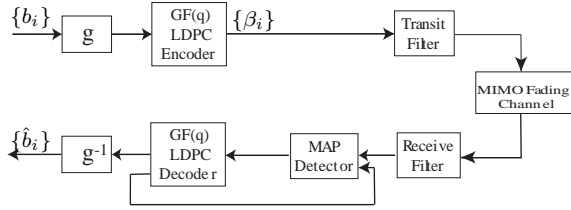


Fig. 1. A schematic block diagram of the iterative system.

and channel noise respectively; \mathbf{H} is the N_r by N_t channel fading matrix with independent and identical distributed (i.i.d.) Rayleigh fading entries; the noise vector \mathbf{n} has i.i.d. complex Gaussian entries with zero mean and variance σ^2 .

Throughout this paper, we assume that the fading matrix \mathbf{H} is perfectly known at the receiver, but not at the transmitter. We also assume that each entry of the transmitted signal vector \mathbf{s} is chosen independently from a finite constellation set such as the quadrature amplitude modulation (QAM).

In the next section, we will first investigate an iterative system that employs nonbinary LDPC codes over $\text{GF}(q)$ and performs joint MIMO detection and channel decoding.

III. ITERATIVE SYSTEM WITH JOINT DETECTION AND CHANNEL DECODING

Fig. 1 presents the block diagram of the proposed iterative system using nonbinary LDPC codes. At the transmitter side, a sequence of information bits $\{b_i\}$ is mapped to a sequence of nonbinary symbols in $\text{GF}(q)$, where $q = 2^p$ (every p bits are mapped to a single nonbinary symbol), through a bit-to-symbol mapper g , before passing to the nonbinary LDPC encoder. For the iterative system considered here, we assume that the constellation size is the same as the size of the Galois field q . For instance, if the nonbinary LDPC code is over $\text{GF}(16)$, then we may choose to use the 16 QAM constellation. At the output of the LDPC encoder, each coded nonbinary symbol $\beta \in \text{GF}(q)$ is mapped to a constellation symbol. The sequence of constellation symbols are then passed to the transmit filter and sent through the MIMO fading channel.

For simplification of notations, we let $\{0, 1, \dots, q-1\}$ denote the elements in $\text{GF}(q)$. Given a nonbinary system over $\text{GF}(q)$, the log-likelihood-ratio-vector (LLRV) is given by

$$\mathbf{z} = \{z_0, z_1, \dots, z_{q-1}\} \quad (2)$$

where

$$z_i = \ln \frac{P(\beta = 0)}{P(\beta = i)}. \quad (3)$$

Here $P(\beta = i)$ denotes the probability that the transmitted $\text{GF}(q)$ symbol β equals i . At the output of the maximum a posteriori (MAP) detector, the i -th component of the LLRV corresponding to the signal transmitted from the j -th antenna, denoted by $z_i(j)$, equals

$$z_i(j) = \log \frac{\sum_{\mathbf{s}: s_j=0} \exp\{-\frac{(\mathbf{y} - \mathbf{H}\mathbf{s})^2}{2\sigma^2}\} \prod_{\substack{k=1 \\ k \neq j}}^{N_t} p(s_k)}{\sum_{\mathbf{s}: s_j=i} \exp\{-\frac{(\mathbf{y} - \mathbf{H}\mathbf{s})^2}{2\sigma^2}\} \prod_{\substack{k=1 \\ k \neq j}}^{N_t} p(s_k)} \quad (4)$$

where $p(s_k)$ denotes the prior probability that the k -th antenna transmits symbol s_k .

IV. DESIGN OF NONBINARY LDPC CODES BASED ON EXIT CHART

In this section, we take the EXIT chart approach to design nonbinary LDPC codes for the iterative system considered in Section III.

For a binary LDPC coded system, density evolution and EXIT chart are the two most successful approaches for code design. Direct extension of these approaches to the nonbinary system, however, is non-trivial. In a nonbinary system, since the probability messages are $q-1$ dimensional vectors, in order to perform density evolution, it is necessary to track $q-1$ message densities. This becomes computationally infeasible for higher order nonbinary codes. Based on Gaussian approximation, Li *et al.* [12] prove that the distribution of message vectors can be characterized by $q-1$ parameters. Moreover, Bennatan *et al.* [8] show the distributions may be characterized by a single parameter, which simplifies the analysis significantly. In this paper, we follow some of the basic assumptions in [8] which are summarized as follows:

- 1) *The labels of the nonzero entries in the parity check matrix are uniformly distributed. Hence, the message vectors flowing in nonbinary LDPC decoder are permutation-invariant. This means that a LLRV $\tilde{\mathbf{W}} \triangleq \mathbf{W}^{\times h}$ is identically distributed to \mathbf{W} , where $\mathbf{W}^{\times h}$ is defined as the LLRV whose components are given by $w_j^{\times h} = w_{j \times h}$, $j = 1, \dots, q-1$. Here the product $j \times h$ is over $\text{GF}(q)$.*
- 2) *Using the symmetry assumption, the permutation-invariant property, and the all-zero codeword transmission, the distribution of the LLRV message in the nonbinary LDPC decoder can be approximated by a joint $(q-1) \times 1$ Gaussian vector with mean \mathbf{m} and covariance matrix Σ where*

$$\mathbf{m} = \begin{bmatrix} \sigma^2/2 \\ \sigma^2/2 \\ \vdots \\ \sigma^2/2 \end{bmatrix} \quad \Sigma = \begin{bmatrix} \sigma^2 & & & \sigma^2/2 \\ & \sigma^2 & & \\ & & \ddots & \\ \sigma^2/2 & & & \sigma^2 \end{bmatrix} \quad (5)$$

Based on these assumptions, efficient code design methods for nonbinary LDPC codes are developed in [8] for AWGN channels. Our new contributions here include (1) Generalize the code design method in [8] for AWGN channel to MIMO channel and introduce the MIMO coset detector. (2) Propose two methods based on an open-loop system to produce accurate EXIT curves and find optimal nonbinary LDPC codes for MIMO channels.

Consider a LDPC code with code length n and rate $R = k/n$. The LDPC code may be visualized as bipartite graph with n variable nodes corresponding to n coded symbols and $n-k$ check nodes corresponding to $n-k$ check equations. The variable nodes and check nodes are connected by edges. The operations of iterative decoding at variable nodes are similar to the decoding of repetition codes and are referred to as the

variable node decoder (VND); and the operations at check nodes are similar to the decoding of single parity check codes and are referred to as the check node decoder (CND).

Following the notations of [4], we let I_A denote the average mutual information between the transmitted symbol and its corresponding input prior LLRV at the decoder or the detector. Similarly, we let I_E denote the average mutual information between the transmitted symbol and its corresponding output extrinsic LLRV at the decoder or the detector. An EXIT curve $I_E(I_A)$ characterizes how I_E changes as a function of I_A . In the remainder of this section, we proceed by showing how to compute the EXIT curve for the combined variable node decoder/ detector (VND/DET) and the EXIT curve for check node decoder (CND). Similar to [8], we use a coset LDPC

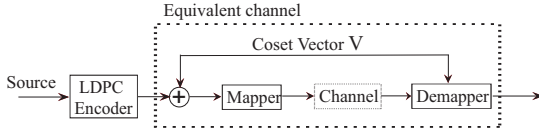


Fig. 2. Coset LDPC codes

ensemble [13] to resolve the asymmetry of the channel. A coset code is obtained by adding a fixed vector called the coset vector to each codeword. With the random coset LDPC setting, the coset vector is generated randomly but is known at the receiver as shown in Fig. 2. With coset LDPC codes, the equivalent channel output is shown to be symmetric. The probability of decoding error is averaged over all channel realizations and is independent of the codeword transmitted. In [14], it is proved that a coset LDPC code achieves similar performance as a standard LDPC with the same degree distribution. This enables us to use the random coset LDPC code with the all-zero codeword transmission assumption to find the optimal degree sequence for the standard LDPC code.

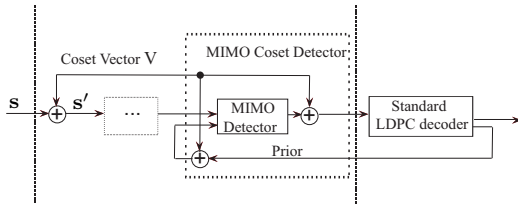


Fig. 3. The MIMO Coset detector

1) *MIMO coset detector*: Corresponding to the coset LDPC code, we introduce a MIMO coset detector to deal with the coset vector \mathbf{v} such that the operations between the two dash lines in Fig. 3 are transparent to LDPC decoder. The LLRV message in the MIMO detector shows the probabilities of $\mathbf{s}' = \mathbf{s} + \mathbf{v}$ because a standard MIMO detector does not know the existence of the coset vector. A standard MIMO detector performs the MAP detection as if \mathbf{s}' were transmitted, whereas the LLRV messages in the LDPC decoder represent the probabilities of \mathbf{s} . Therefore, if we denote the output extrinsic message of the MIMO detector by $\mathbf{R}'^{(0)}$ and the LLRV message sent to the LDPC decoder by $\mathbf{R}^{(0)}$, then $\mathbf{R}^{(0)}$ is simply a shifted version of $\mathbf{R}'^{(0)}$. Hence, the j -th component

of $\mathbf{R}^{(0)}$ is represented by

$$\mathbf{R}_j^{(0)} = \mathbf{R}'_{j+v_i} - \mathbf{R}'_{v_i},$$

where the addition is performed over $\text{GF}(q)$. Similarly, the prior information fed back by the LDPC decoder is also shifted by v_i before sending to the MIMO detector

$$\mathbf{Q}'_j = \mathbf{Q}_{j+v_i} - \mathbf{Q}_{v_i}.$$

Here \mathbf{Q}_j denotes the j -th component of the LLRV message fed back from the LDPC decoder and \mathbf{Q}' denotes the input prior message of the MIMO detector.

2) *Open-loop system for generating EXIT curves*: For binary LDPC codes, the Gaussian assumption has been shown to be quite accurate in approximating the densities of the LLR messages. This approximation, however, becomes less accurate for nonbinary LDPC codes even for AWGN channels [8]. In [8], the CND messages are assumed to be Gaussian distributed. The VND messages are modeled as the summation of two random vectors. One vector is the summation of the CND messages and the other is the initial channel messages (not necessarily Gaussian) computed from the empirical distribution of the AWGN channel.

Due to multi-dimensional integration, it is non-trivial to find a close-form EXIT function for the nonbinary codes even under the Gaussian assumption. Therefore, we propose an open-loop system to generate random samples to evaluate the EXIT functions empirically. Fig. 4 shows the block diagram of the proposed system. The open-loop system works as follows.

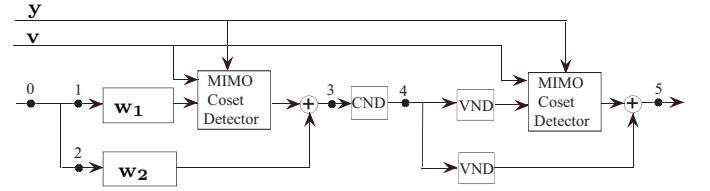


Fig. 4. Open-loop system to evaluate EXIT function.

With a specified pair of (d_v, d_c) , where d_v denotes the degree of variable nodes and d_c denotes the degree of check nodes, and the channel signal-to-noise ratio (SNR), we initiate the open-loop system by generating two sets of LLRV samples each with a joint Gaussian distribution given in (5). The first set of samples \mathbf{w}_1 has a parameter $\sigma^2 = \sigma_n^2$ which is used to model the summation of d_v CND messages as the input prior information of the MIMO coset detector. Here σ_n is a value along a fine grid in the range of $[0, \dots, 12]$. The second set of samples \mathbf{w}_2 has a parameter $\sigma^2 = \sigma_n^2 \frac{d_v-1}{d_v}$ which is used to model the summation of $d_v - 1$ CND messages as the input message of VND. These samples combined with the received vector \mathbf{y} first perform a combined VND/DET. The output of which is sent to the CND. Consequently, with the output samples of CND as input, another combined VND/DET is performed. Since we assume that the all-zero codeword is transmitted, the output samples between point 0 and point 5 can be used to produce the EXIT curves.

Next, we describe the details of computing the EXIT curves for the nonbinary LDPC codes based on the proposed open-loop system.

3) *The combined VND/DET EXIT curve:* Consider an arbitrary variable node i of degree d_v . Let $\mathbf{l}^{(n)}$ denote the CND message coming from its n -th neighboring check node. Also, let $\mathbf{R}_k^{(j)}$ denote the k -th component of output extrinsic LLRV message from variable node i to its j -th neighboring check node after one iteration of combined VND/DET. We compute $\mathbf{R}_k^{(j)}$ as follows:

$$\begin{aligned} \mathbf{Q}_k &= \sum_{n=1}^{d_v} \mathbf{l}_k^{(n)} \\ \mathbf{Q}'_k &= \mathbf{Q}_{k+v_i} - \mathbf{Q}_{v_i} \\ \mathbf{R}_k^{(0)} &= [\mathcal{MAP}(\mathbf{Q}', \mathbf{y})]_k \\ \mathbf{R}_k^{(0)} &= \mathbf{R}'_{k+v_i} - \mathbf{R}'_{v_i} \\ \mathbf{R}_k^{(j)} &= \sum_{n=1, n \neq j}^{d_v} \mathbf{l}_k^{(n)} + \mathbf{R}_k^{(0)} \end{aligned}$$

where $[\mathcal{MAP}(\mathbf{Q}', \mathbf{y})]_k$ denotes the k -th component of the extrinsic output of the MIMO MAP detector with input prior message \mathbf{Q}' and received vector \mathbf{y} .

The combined VND/DET EXIT curve is determined by the variable node degree d_v and the channel SNR. For each d_v , we denote the combined VND/DET curve by $I_{E,VND/DET}(I_{A,VND/DET}; d_v, \text{SNR})$ where $I_{A,VND/DET}$ denotes the mutual information of the input CND message.

Based on the open-loop system shown in Fig.4, we propose two approaches for computing the combined VND/DET EXIT curve. In the first approach, we obtain $I_{A,VND/DET}$ and $I_{E,VND/DET}$ by measuring the mutual information based on random samples collected at point 0 and point 3 respectively. Details of computing the mutual information based on random samples are briefly discussed towards the end of this section. We find that the first approach is less accurate due to the Gaussian assumption at the input of the MIMO coset detector. In fact, the input to the MIMO coset detector comes from the CND and the density of the CND messages resembles a ‘‘spike’’ distribution rather than a Gaussian distribution. Therefore, in the second approach, we relax the Gaussian assumption at the input of the MIMO coset detector and use actual output of the CND to drive the MIMO detector. In this approach, we obtain $I_{A,VND/DET}$ and $I_{E,VND/DET}$ by measuring the mutual information based on random samples collected at point 4 and point 5 respectively.

In Fig. 5, we plot the combined VND/DET EXIT curves using the two approaches described above. While the two set of EXIT curves are relatively close to each other, it is noted that the EXIT curves obtained by the first approach based on the Gaussian assumption are always higher than those obtained by the second approach. This result is in agreement with the claim in [15] that EXIT charts based on the Gaussian assumption lead to a predicted convergence threshold that is lower than the actual threshold. Simulation results in Section VI also justify the effectiveness of the second approach by showing that the gap between the actual convergence threshold and the predicted threshold of the designed LDPC code is smaller if the second approach is adopted.

4) *The CND EXIT curve:* Consider an arbitrary check node j of degree d_c . Let $\mathbf{R}^{(n)}$ denote the VND message from its n -th neighboring variable node, and let h_n denote the label

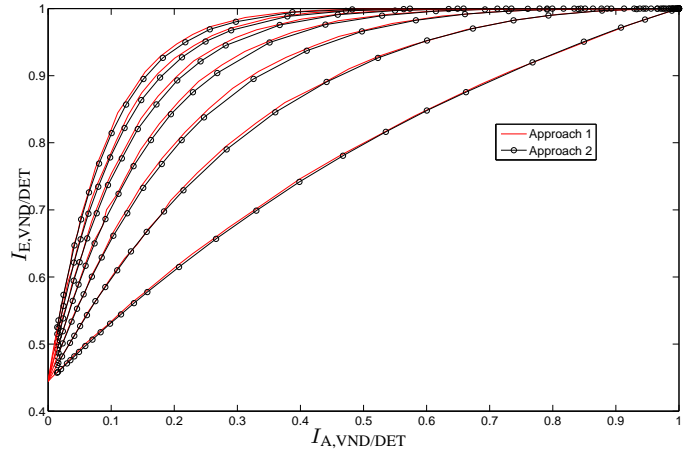


Fig. 5. Comparisons of the combined VND/DET curves for $d_v = 2, \dots, 8$ (from the bottom to the top) using the two proposed approaches.

of the edge connecting these two nodes. We compute the k -th component of the output extrinsic LLRV message $\mathbf{l}_k^{(i)}$ of the CND sending from check node j to its i -th neighboring variable node by

$$\begin{aligned} \mathbf{l}'_k^{(n)} &= \{\mathcal{F}[\mathcal{P}_n(\mathbf{R}^{(n)})]\}_k \\ \mathbf{l}''_k^{(i)}(s) &= \prod_{n=1, n \neq i}^{d_c} \mathbf{l}'_k^{(n)}(s) \\ \mathbf{l}''_k^{(i)}(m) &= \sum_{n=1, n \neq i}^{d_c} \mathbf{l}'_k^{(n)}(m) \\ \mathbf{l}_k^{(i)} &= \{\mathcal{P}_i^{-1}[\mathcal{F}^{-1}(\mathbf{l}''^{(i)})]\}_k. \end{aligned}$$

Here \mathcal{F} denotes the Fourier transform in the logarithmic domain over $\text{GF}(q)$ [16] [17]; $\mathcal{P}_n(\mathbf{R}^{(n)})$ denotes the permutation of $\mathbf{R}^{(n)}$ by h_n ; $\mathbf{l}(s)$ and $\mathbf{l}(m)$ denote the sign and magnitude of the message \mathbf{l} respectively.

Through simulation we observe that the CND EXIT curve is independent of the channel SNR and the degree of the VND connecting to the CND. Therefore, we let $I_{E,CND}(I_{A,CND}; d_c)$ denote the CND EXIT curve for each check node degree d_c , where $I_{A,CND}$ represents the mutual information of the input message to the CND. We then proceed to obtain the EXIT curve by measuring $I_{A,CND}$ and $I_{E,CND}$ based on the random samples collected at point 3 and point 4 (shown in Fig.4) respectively.

5) *Calculation of mutual information:* When computing the EXIT curves based on the open-loop system, we make measurements at different points and compute mutual information using the collected random LLRV samples. In general, the calculation of the mutual information of vector samples requires multi-dimensional integration. For nonbinary codes over $\text{GF}(q)$, this requires $q-1$ dimensional integration which makes it computationally intensive for large values of q . Assuming that a coset LDPC code is used to ensure that the symmetry condition of the channel holds, the computation of the mutual information per bit can be simplified [8] as

$$I_b(C; \mathbf{W}) = 1 - E \left[\log_q \left(1 + \sum_{i=0}^{q-1} e^{-W_i} \right) | C = 0 \right], \quad (6)$$

where C denotes the transmitted symbol, and \mathbf{W} denotes the corresponding LLRV message. In our paper, we follow (6) to compute the mutual information used for generating the EXIT curves.

6) *Code design via linear programming*: Once we obtain the VND/DET and CND EXIT curves, we can proceed with the code optimization via linear programming. For simplicity, we limit ourselves to consider check-regular codes only. For a given variable node degree distribution λ , the mixed combined VND/DET curve is $I_{E,VND/DET}(I_{A,VND/DET}, \text{SNR}) = \sum_{d_v} \lambda_{d_v} I_{E,VND/DET}(I_{A,VND/DET}, d_v, \text{SNR})$. Therefore the code optimization problem can be solved by linear programming:

$$\begin{aligned} & \text{Fix} && d_c \\ & \text{maximize} && \text{code rate } R \\ & \text{subject to} && \sum_{d_v} \lambda_{d_v} = 1, \\ & && R = 1 - \frac{1/d_c}{\sum_{d_v} \lambda_{d_v}/d_v} \\ & && I_{E,VND/DET}(I_A, \text{SNR}) > I_{E,CND}^{-1}(I_A, d_c) \end{aligned}$$

V. NON-ITERATIVE SYSTEM

In this section, we study a non-iterative system using non-binary LDPC codes over a large Galois field. As opposed to the iterative system considered in Section III, here we employ separate MIMO detection and channel decoding. Performance comparisons between the iterative system and non-iterative system are included in Section VI.

Fig. 6 describes the proposed non-iterative system. Assume that the LDPC code is defined over $\text{GF}(q)$, where $q = 2^p$. In this system, we assume a higher order modulation scheme with a constellation size of $M = 2^m$ is used. At the output of the LDPC encoder, each coded nonbinary symbol $\beta \in \text{GF}(q)$ is mapped to a group of n_c constellation symbols through the mapping ϕ . Here we have $p = n_c \cdot m$. The sequence of constellation symbols are then passed to the transmit filter and sent through the fading channel. At the receiver side, based on the output of the receive filter, symbol-wise maximum likelihood (ML) detection is performed to compute the prior probabilities for each group of n_c transmitted constellation symbols. These prior probabilities will then be passed (after the mapping ϕ^{-1}) to the LDPC decoder for iterative decoding. After a finite number of decoding iterations, hard decisions on the nonbinary symbols will be made at the output of LDPC decoder, which will be demapped to the sequence of estimated information bits.

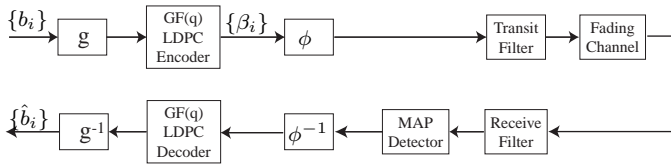


Fig. 6. A schematic block diagram of the proposed non-iterative system.

The proposed system in Fig. 6 is applicable to both the single-input single-output (SISO) channel and the MIMO channel. In Fig. 7 we show the MIMO system that employs a nonbinary LDPC code over $\text{GF}(256)$. We use two transmit

and receive antennas ($N_t = N_r = 2$) and 16QAM modulation. Each coded $\text{GF}(256)$ symbol β is mapped to two 16QAM symbols ($n_c = 2$) and are transmitted simultaneously through two different transmit antennas. Next, we explain how the ML

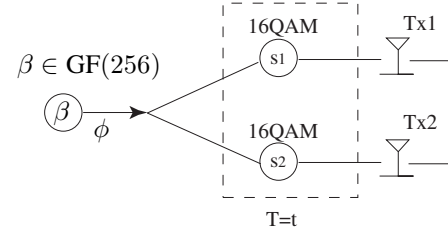


Fig. 7. $N_t = N_r = 2$, each $\text{GF}(256)$ symbol is mapped to two 16QAM symbols

detector shown in Fig. 6 works. For each received vector \mathbf{y} , the ML detector computes channel LLRV as follows

$$z_i = \left\{ \frac{1}{2\sigma^2} \|\mathbf{y} - \mathbf{H}\mathbf{s}^i\|^2 - \frac{1}{2\sigma^2} \|\mathbf{y} - \mathbf{H}\mathbf{s}^0\|^2 \right\} \quad (7)$$

where $\|\cdot\|^2$ denotes the norm square of a vector, $\mathbf{s}^i = \phi(i)$ denotes transmitted vector corresponding to the field element i . Subsequently, these LLRV values will be passed to the LDPC decoder for iterative decoding.

It is important to note that the proposed system in Fig. 6 does not require any iterative processing between the ML detector and the LDPC decoder. This is because the ML detector produces the prior probabilities for each $\text{GF}(q)$ symbol which can be used directly for nonbinary LDPC decoding over $\text{GF}(q)$. This is in contrast with the iterative system where iterative processing between the MAP detector and the LDPC decoder is required for optimal performance [4]. In the iterative system, the MAP detector generates LLRV values to be used for LDPC decoding. Note that these LLRV values are dependent for those bits either belonging to the same constellation symbol or transmitted simultaneously through different transmit antennas. Hence, it is necessary to pass soft information about the dependent bits from the LDPC decoder back to the MAP detector to produce updated LLRV. These updated LLRV will be passed to the LDPC decoder for the next decoding iteration to achieve better performance.

VI. DESIGN EXAMPLES AND PERFORMANCE COMPARISON

In this section, we present simulation results for the proposed iterative and non-iterative systems employing nonbinary LDPC codes. Performance comparisons with the binary LDPC coded system are also provided.

We consider a MIMO channel with two transmit and receive antennas ($N_t = N_r = 2$) and use 16QAM modulation in all simulations. Fig. 8 shows the EXIT curves of MIMO detectors over Galois fields of different sizes. Each curve in the figure describes the functional relation between the mutual information of input prior information (sum of the feedback CND messages) and the mutual information of output extrinsic message of MIMO detector. As shown in Fig. 8, the left endpoint (at $I_{A,DET} = 0$) of each curve increases with the field size q . This is because the symbol-wise ML detector (when no

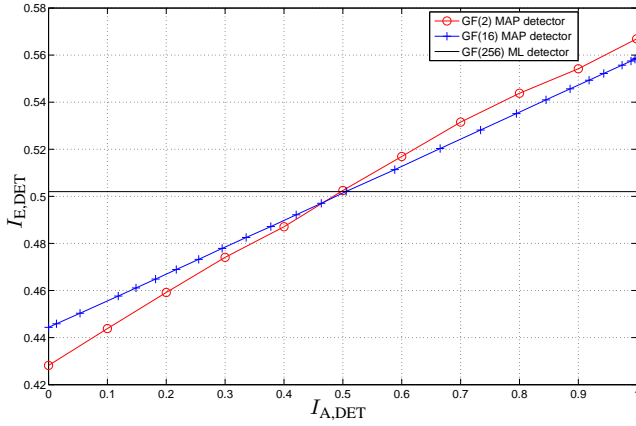


Fig. 8. EXIT curve for MIMO detectors at 4.1dB and $R = 1/2$.

prior information available) is optimized for minimizing the error probability of symbols while the bit-wise ML detector is optimized for minimizing the error probability of bits. In contrast, at $I_{A,DET} = 1$, the right end-point of each curve decreases with the field size. This is because more prior information feedback are available to the MIMO detector employing smaller Galois field.

Our code design choices for the iterative and non-iterative systems are as follows: For the binary iterative system, we apply the code design method of [4] to find the optimal binary LDPC code matched to the MIMO detector. For the nonbinary iterative system, we design two codes over GF(16) using code design methods discussed in Section IV. The two nonbinary LDPC codes: code 1 and code 2 are obtained by using the first and second approach of computing the combined VND/DET EXIT curve, respectively. For non-iterative system, instead of searching the optimal irregular codes, we simply use a regular LDPC code over GF(256) with $d_v = 2$ and $d_c = 4$. This code has been shown to demonstrate excellent performance for AWGN channels [18]. The degree distributions of the optimized codes are shown in Table I. In Fig. 9, we compare

TABLE I
DEGREE DISTRIBUTIONS OF THE OPTIMIZED LDPC CODES

Binary	$d_v = [2, 3, 7, 8, 23, 24], d_c = [7]$ $u_v = [0.5682, 0.298, 0.029, 0.0761, 0.0117, 0.017]$ Curve fit at 4.1dB
GF(16) code 1	$d_v = [2, 8, 10], d_c = [5]$ $u_v = [0.9244, 0.0402, 0.0354]$ Curve fit at 4.1dB
GF(16) code 2	$d_v = [2, 8, 9], d_c = [5]$ $u_v = [0.9299, 0.0378, 0.0323]$ Curve fit at 4.16dB

In Table I, d_v and d_c denote the degree sequence of the variable nodes and the check nodes, respectively. $u_v(i)$ denotes the fraction of variables nodes of degree $d_v(i)$.

the performance of different systems. For the iterative systems (employing either the binary LDPC code or nonbinary code over GF(16)), iterative processing is done by performing 5 inner decoder iterations per detector/decoder iteration, and 40 outer detector/decoder iterations. For the non-iterative system, 100 inner decoding iterations are performed. All codes have a code length of 2304 bits. Fig. 9 shows that the non-iterative

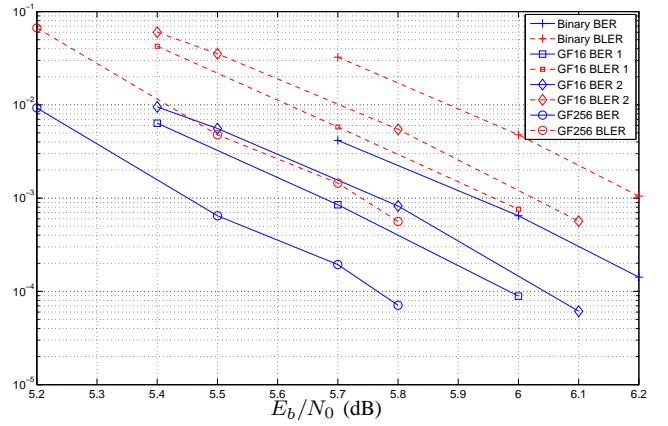


Fig. 9. Bit-error-rate (BER) and block-error-rate (BLER) comparisons of different systems.

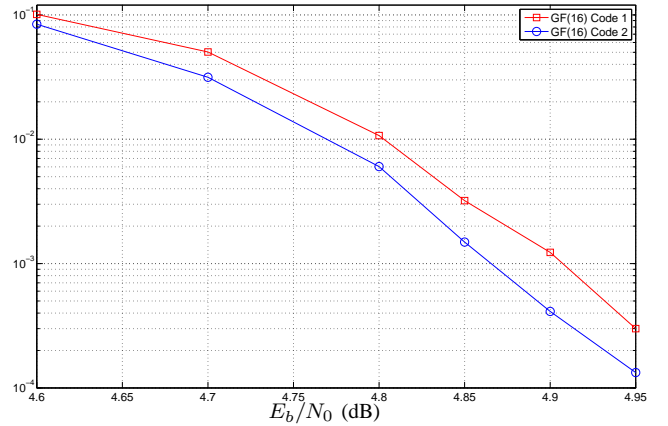


Fig. 10. Comparison of the two GF(16) codes with a code length of 10000 symbols.

system with regular LDPC code over GF(256) achieves the best performance at the cost of an increase decoding complexity. It is about 0.46 dB better than the binary iterative system. The best nonbinary iterative system is the system employing the optimized LDPC code 2 over GF(16). It is about 0.06 dB better than code 1 and is about 0.25 dB better than the binary iterative system.

In Fig. 10, we also plot the performance curves of the nonbinary iterative system using the two optimized codes over GF(16), assuming a longer code length of 10000 symbols. Again, the system employing code 2 is about 0.05 dB better than code 1. Note that the predicted convergence threshold of code 2 is at 4.16 dB, whereas the predicted convergence threshold of code 1 is at 4.1 dB. The better performance of code 2 shows that the second approach in Section IV produces more accurate EXIT curves and therefore leads to better code design and more reliable prediction of the convergence threshold.

VII. COMPLEXITY ANALYSIS

In this section, we compare the complexity of iterative and non-iterative systems. First, we note that employing nonbinary codes does increase the decoding complexity. Efficient decoding algorithms for nonbinary LDPC codes are discussed

in [17], which shows that the decoding complexity increases linearly with q . Specifically, the decoding complexity of the GF(256) code is about 60 times higher than the binary LDPC code. However, it is also important to point out that for the non-iterative system, no iteration between the MIMO detector and the channel decoder is required. The complexity saving in using the MIMO detector only once contributes to the complexity reduction of the overall system.

The complexity bottleneck of the iterative system lies in the MIMO detector. To reduce the detection complexity, we first compute the channel condition probability in the logarithm domain ($\log P(\mathbf{y}|\mathbf{s})$) for all possible input symbol combinations. This requires computing all the terms inside the summation of (4), which amounts to $2^{N_{\epsilon}m}/(N_{\epsilon}m)$ operations per bit. Using the Jacobi algorithm:

$$\max^*(x_1, x_2) \triangleq \max(x_1, x_2) + \ln(1 + e^{-|x_1 - x_2|}),$$

the complexity of the summation step needed to compute the LLR for the binary system is $2^{N_{\epsilon}m}/2 - 1$ per bit and is $(2^{N_{\epsilon}m} - 2^m)/m$ per symbol LLRV for the nonbinary system. Using this implementation, we are able to reduce the complexity of the MIMO detector as much as possible at the cost of increased memory. Table II shows the complexity comparison per bit and per iteration. Here we ignore the complexity of the ML detection of the non-iterative system since it is done only once and not iteratively. We also do not take into account the complexity of simple operations such as addition and subtraction. From Table II, we see that the complexity of the nonbinary iterative system is much lower than that of the binary iterative system. The complexity comparison with the non-iterative system depends greatly on the complexity of computing $\log P(\mathbf{y}|\mathbf{s})$. In our simulation, we observe that the binary iterative system has a complexity close to that of the non-iterative system, and the latter usually converges faster. Therefore, in terms of simulation time, the non-iterative system runs slightly faster than the binary iterative system. It is also noted that the complexity of the iterative system can be reduced by increasing the number of inner decoding iterations per outer detector/decoder iteration and decreasing the number of outer iterations at the cost of slightly degraded performance.

TABLE II
ESTIMATED COMPLEXITY OF DIFFERENT SYSTEMS PER BIT PER
ITERATION

	$\log P(\mathbf{y} \mathbf{s})$	\max^*	\log/\exp
Binary iterative	32	160	0
Nonbinary iterative	32	60	80
Non-iterative	\	\	512

VIII. CONCLUSION

In this paper, we study the application of nonbinary LDPC codes for MIMO fading channels. We consider both the iterative system and the non-iterative system employing nonbinary LDPC codes. For the iterative system, symbol-wise MIMO MAP detector is concatenated with the nonbinary LDPC decoder to perform joint (iterative) detection and decoding. We

develop nonbinary LDPC code design methods for the iterative system based on EXIT chart and the notion of coset MIMO detector. For the non-iterative system, we propose to use regular nonbinary LDPC codes over large Galois field. Our simulation results show that the nonbinary iterative system achieves the best balance between complexity and performance. It has the lowest complexity and achieves a performance better than the binary iterative system. The non-iterative system achieves a performance about 0.46 dB better than that of the iterative binary system, however, at an increase complexity compared to the nonbinary iterative system.

REFERENCES

- [1] R. G. Gallager, *Low density parity check codes*. Cambridge, MA: MIT Press, 1963.
- [2] D. J. C. MacKay and R. M. Neal, "Near shannon limit performance of low density parity check codes," *Electronics Letters*, vol. 32, pp. 1645–1646, Aug. 1996.
- [3] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619–637, Feb. 2001.
- [4] S. ten Brink, G. Kramer, and A. Ashikhmin, "Design of low-density parity-check codes for modulation and detection," *IEEE Trans. Commun.*, vol. 52, pp. 670–678, Apr. 2004.
- [5] J. Hou, P. H. Siegel, L. B. Milstein, and H. D. Pfister, "Capacity-approaching bandwidth-efficient coded modulation schemes based on low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2141–2155, Sept. 2003.
- [6] M. C. Davey and D. Mackay, "Low-density parity check codes over GF(q)," *IEEE Comm. Letters*, vol. 2, pp. 165–167, June 1998.
- [7] X. Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE Trans. Inform. Theory*, vol. 51, pp. 386–398, Jan. 2005.
- [8] A. Bennatan and D. Burshtein, "Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels," *IEEE Trans. Inform. Theory*, vol. 52, pp. 549–583, Feb. 2006.
- [9] F. Guo and L. Hanzo, "Low complexity non-binary LDPC and modulation schemes communicating over MIMO channels," in *VTC2004-Fall*, vol. 2, pp. 1294–1298, IEEE, Sept. 2004.
- [10] P. Meshkat and H. Jafarkhani, "Space-time low density parity check codes," in *Asilomar Conference on Signals, Systems, and Computers*, Nov. 2002.
- [11] G. Caire, G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Trans. Inform. Theory*, vol. 44, pp. 927–945, May 1998.
- [12] G. Li, I. J. Fair, and W. A. Krzymieri, "Analysis of nonbinary ldpc codes using gaussian approximation," in *Proc. 2003 IEEE Int. Symp. Information Theory*, (Yokohama, Japan), p. 234, 2003.
- [13] A. Kavčić, X. Ma, and M. Mitzenmacher, "Binary intersymbol interference channels: Gallager codes, density evolution and code performance bounds," *IEEE Trans. Inform. Theory*, vol. 49, pp. 1636–1652, July. 2003.
- [14] C.-C. Wang, S. R. Kulkarni, and H. V. Poor, "On the typicality of the linear code among the LDPC coset code ensemble," in *Proc. the 39th Conference on Information Sciences and Systems*, (Baltimore, USA), March 2005.
- [15] S. R. Kollu and H. Jafarkhani, "On the EXIT chart analysis of low-density parity-check codes," in *Proc. IEEE Globecom'05*, Dec. 2005.
- [16] H. Song and J. Cruz, "Reduced-complexity decoding of Q-ary LDPC codes for magnetic recording," *IEEE Trans. Magnetics*, vol. 39, pp. 1081–1087, March 2003.
- [17] R.-H. Peng and R.-R. Chen, "Application of nonbinary ldpc codes for communication over fading channels using higher modulations," to appear: *Proc. IEEE Globecom'06*.
- [18] X.-Y. Hu and E. Eleftheriou, "Binary representation of cycle Tanner-graph GF(2^b) codes," in *Proc. ICC'04*, June. 2004.