Application of Nonbinary LDPC Codes for Communication over Fading Channels Using Higher Order Modulations

Ronghui 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 both single-input single-output (SISO) and multiple-input multiple-output (MIMO) fading channels using higher order modulations. As opposed to the widely studied binary systems that employ joint detection and channel decoding, we propose a nonbinary system where optimal signal detection is performed only once followed by channel decoding. To reduce the complexity of proposed system, we first develop a low complexity LDPC decoding algorithm over GF(q) in the logarithmic domain. We then provide a quasi-cyclic construction of nonbinary LDPC codes which not only allows linear-time encoding, but also gives comparable performance to the best known progressive edge growth (PEG) codes. Our results show that the proposed system that employs regular nonbinary LDPC codes outperforms systems using the best optimized binary irregular LDPC codes in both performance and complexity.**

I. INTRODUCTION

Recently, low-density parity-check (LDPC) codes [1][2] have attracted considerable interest due to their capacity approaching performance and great flexibility in code design and practical implementation. Most of the research, however, focuses on the design and construction of binary LDPC codes. Nonbinary LDPC codes, first investigated by Davey and Mackay [3], was shown to obtain superior performance than the binary codes. Recently, irregular nonbinary LDPC codes over GF(q) were constructed using the progressive edge growth (PEG) algorithm [4]. Nonbinary LDPC codes have recently been applied to the multiple-input multiple-output (MIMO) channel [5] and the nonbinary channel [6].

Despite the advantages of nonbinary LDPC codes, the decoding complexity of these codes remains a major obstacle for their commercial applications. Direct extension of the binary sum-product decoding algorithm (SPA) [7] to nonbinary codes imposes huge complexity when q is large. A *Fast Fourier Transform* (FFT) based q-ary SPA is suggested by Davey [8] which significantly reduces the complexity. Later, a log-domain implementation of q-ary SPA (log q-ary SPA) is proposed by Song *et al.* [9].

In this paper, we consider a nonbinary LDPC coded system for fading channels with higher order modulations. One of our main contributions is to propose a nonbinary LDPC coded system which requires no iterative processing between the optimal signal detector and the channel decoder. This reduces complexity significantly compared to other widely studied binary systems which require joint (iterative) detection and decoding. To the best of our knowledge, this is also the first work that provides performance comparisons between the regular nonbinary LDPC codes and the best optimized irregular binary LDPC codes for fading channels. We demonstrate promising results which show that the proposed system that employs regular nonbinary LDPC codes outperforms systems using the best optimized binary irregular LDPC codes in both performance and complexity. We also investigate the decoding and code construction aspects of the nonbinary LDPC codes. We develop a low-complexity decoding algorithm for the nonbinary LDPC codes based on the Log-SPA which leads to better numerically stability. We also construct a quasi-cyclic nonbinary LDPC code based on quadratic permutation polynomials (QPP) over finite integer rings [10]. This construction is amicable to the design of short LDPC codes. It also achieves comparable performance with the best known PEG construction.

This paper is organized as follows. In Section II, we introduce the system model. Section III includes a novel FFT-based Log-SPA decoding algorithm for the nonbinary LDPC codes which has a lower complexity and better numerical stability. In Section IV, we propose a quasi-cyclic nonbinary LDPC construction that allows for linear-time encoding. Simulation results and performance comparisons with the binary LDPC coded systems are presented in Section V. Conclusions are given in Section VI.

II. SYSTEM MODEL

Fig. 1 describes the proposed nonbinary LDPC coded system. Assume that the LDPC code is defined over GF(q), where $q = 2^p$. At the transmitter side, a sequence of information bits $\{b_i\}$ is mapped to a sequence of nonbinary symbols in GF(q) (every p bits are mapped to a single nonbinary symbol) through a bit-to-symbol mapper g, before passing to the nonbinary LDPC encoder. Assume that 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 $\beta_i \in GF(q)$ 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

This work is supported in part by NSF under grant ECS-0547433.

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

then passed to the transmit filter and sent through the fading channel. Here we assume that every group of n_c constellation symbols is transmitted through n_s consecutive (independent) channel uses. At the receiver side, at the output of the receive filter, the optimal maximum *a posterior* probability (MAP) 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. The proposed system in Fig. 1 is applicable to both the SISO channel and the MIMO channel. In Fig. 2 we show two communication scenarios that employ a nonbinary LDPC code over GF(256). Here we let N_t denote the number of transmit antennas and N_r denote the number of receive antennas. In Fig. 2 (a), we use single transmit and receive antenna ($N_t = N_r = 1$) and 16QAM modulation. Each coded GF(256) symbol β is mapped to two 16QAM symbols ($n_c = 2$) and transmitted through the channel over two consecutive time instances $T = t$ and $T = t + 1$ (namely, $n_s = 2$). In Fig. 2 (b), we use four transmit and receive antennas ($N_t = N_r = 4$) and QPSK modulation. Each coded GF(256) symbol β is mapped to four QPSK symbols ($n_c = 4$) and are transmitted simultaneously through four different transmit antennas. Here we have $n_s = 1$.

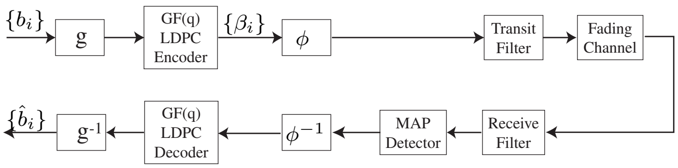


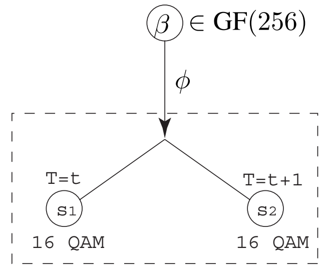
Fig. 1. A schematic block diagram of the proposed nonbinary system.

Next, we explain how the MAP detector shown in Fig. 1 works. Without loss of generality, we express the channel model as

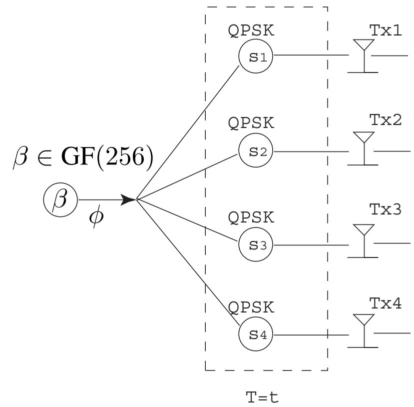
$$\mathbf{Y}_l = \mathbf{H}_l \mathbf{X}_l + \mathbf{N}_l \qquad (1 \le l \le n_s) \tag{1}$$

where l denotes the time index, $\mathbf{X}_l \in C^{N_t \times 1}$ denotes the complex transmitted signal vector, $\mathbf{Y}_l \in C^{N_r \times 1}$ denotes the complex received signal vector, $\mathbf{H}_l \in C^{N_r \times N_t}$ denotes the channel fading matrix with independent and identically distributed (i.i.d.) entries that are complex Gaussian distributed with zero mean and unit variance, $\mathbf{N}_l \in C^{N_r \times 1}$ denotes the vector of zero mean, complex Gaussian white noise with variance σ^2 per dimension. We assume that the channel matrix is known to the receiver but not to the transmitter.

For each block of received signals $\{\mathbf{Y}_l, \cdots, \mathbf{Y}_{n_s}\}$, the MAP detector computes the probability that the group of n_c transmitted constellation symbols corresponds to (through the mapping ϕ) some nonbinary element $\beta \in GF(q)$. This is done through the computation of the log-likelihood-ratio vector (LLRV) over GF(q). Let $\{0, \alpha_1, \cdots, \alpha_{q-1}\}$ denote all the elements in GF(q). The LLRV over GF(q) is defined as: $\mathbf{z} = \{z_0, z_1, \cdots, z_{q-1}\}$ where $z_i = \ln[P(\beta = \alpha_i)/P(\beta = 0)]$.



(a) SISO channel, $N_t = N_r = 1$, each GF(256) symbol is mapped to two 16 QAM symbols



(b) MIMO channel, $N_t = N_r = 4$, each GF(256) symbol is mapped to four QPSK symbols

Fig. 2. Application of the proposed system to SISO and MIMO channels

Here $P(\beta = \alpha_i)$ denotes the probability that the transmitted GF(q) symbol β equals α_i. Here we have

$$z_i = -\frac{1}{2\sigma^2} \sum_{l=1}^{n_s} \left(\|\mathbf{Y}_l - \mathbf{H}_l \mathbf{X}_l^{\alpha_i}\|^2 - \left\|\mathbf{Y}_l - \mathbf{H}_l \mathbf{X}_0^0\right\|^2 \right), \tag{2}$$

where $\|\cdot\|^2$ denotes the norm square of a vector, $\{\mathbf{X}_1^{\alpha_i}, \cdots, \mathbf{X}_{n_s}^{\alpha_i}\} = \phi(\alpha_i)$ denotes the collection of n_s transmitted signal vectors corresponding to α_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. 1 does not require any iterative processing between the MAP detector and the LDPC decoder. This is because the MAP detector produces the prior probabilities for each GF(q) symbols that can be used directly for nonbinary LDPC decoding over GF(q). This is in contrast with a binary LDPC coded system for higher order modulations where iterative processing between the MAP detector and the LDPC decoder is required for optimal performance [11]. In the binary coded system, the MAP detector must generate bit-wise LLR values to be used for binary LDPC decoding. Note that these LLR 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 these dependent bits from the LDPC decoder back to the MAP detector to produce updated bit-wise

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

LLR. These updated LLR will be passed to the LDPC decoder for the next decoding iteration to achieve better performance.

In the following two sections, we treat the decoding and code construction aspects of the nonbinary LDPC code separately to facilitate efficient implementation of the proposed system.

III. Nonbinary Log-SPA decoding based on FFT

In this section, we propose an efficient method for decoding nonbinary LDPC codes using the FFT-based Log-SPA. Here we adopt the sign/logarithmic number system (LNS) ([12][9]) which keeps track of both sign(u) and $\log(|u|)$ for any given number u.

We begin by a brief review of the FFT-based Log-SPA algorithm [9] which uses the LNS.

Algorithm 1([6], [9]):

1) Initialize step: Compute initial LLRV based on the received signal $\mathbf{y}$.
2) Tentative decoding: check whether successful decoding has been achieved. Halt if decoding successful.
3) Horizon step (H): Update variable nodes according to standard Log-SPA (refer to [6],[9]).
4) Vertical step (V): Check node j sends message (denoted by $\mathbf{l} = \mathbf{l}(j, i)$) to adjacent variable node i.
   a) Permute LLRV $\mathbf{r}^{(n)}, n = 1, \cdots, d_j - 1$ over GF(q), where $\mathbf{r}^{(n)}$ denotes the incoming message from all other adjacent variable nodes i' except for variable node i; d_j denotes the degree of variable node j.
   b) Perform p-FFT over $\mathbf{r}^{(n)}$ in LNS. Let $\mathbf{R}^{(n)} \triangleq \mathrm{FFT}(\mathbf{r}^{(n)})$.
   c) Multiple all $\mathbf{R}^{(n)}$ using multiplication in LNS. The result is denoted by $\mathbf{L}$.
   d) Perform p-IFFT over $\mathbf{L}$ in LNS to get $\mathbf{l}'$.
   e) Perform permutation of $\mathbf{l}'$ to get $\mathbf{l}$.

In Algorithm 1, efficient computation of the p-dimensional FFT is made possible by successively applying one-dimensional 2-point FFT on each dimension in turn [13]. Since the one-dimensional 2-point FFT involves only simple addition and subtraction, Algorithm 1 requires only LNS multiplication (which is just a simple addition) and LNS addition and subtraction. While LNS is efficient in performing multiplication and division, LNS addition and subtraction are non-trivial. Hence, due to the limitations of finite precision, it becomes inaccurate to compute the difference of two numbers that are very close in range using LNS [14]. If one chooses to overcome such numerical instability by implementing the LNS addition and subtraction through a look-up table, the size of look-up table increases exponentially with the precision requirement [12].

To overcome this problem while still maintaining the advantages of LNS, we propose the following modified Log-SPA decoding algorithm. The basic idea is to convert data from LNS to plain likelihood before the FFT and IFFT operations and then convert them back afterwards. This way the LNS addition and subtraction are avoided to ensure numerical stability. The complexity of proposed algorithm is also reduced due to the simplicity of 2-point FFT and IFFT in the non-logarithmic domain.

TABLE I
Complexity comparison of GF(2)-LDPC and GF(q)-LDPC

Per coded bit per iteration	# of addition	# of LNS addition/subtraction	# of Log/Exp
GF(2)-LDPC (LLR) (H)	2λ	0	0
GF(q)-LDPC A1 (H)	$2\lambda\frac{q}{p}$	0	0
GF(q)-LDPC A2 (H)	$2\lambda\frac{q}{p}$	0	0
GF(2)-LDPC (LLR) (V)	$4(3\rho-4)(1-R)$	$2(3\rho-4)(1-R)$	0
GF(q)-LDPC A1 (V)	$[\rho(2q+\frac{2q}{p})-q](1-R)$	$2q\rho(1-R)$	0
GF(q)-LDPC A2 (V)	$[\rho(2q+\frac{2q}{p})-q](1-R)$	0	$4\frac{q}{p}\rho(1-R)$

In Table I, A1 and A2 denote Algorithm 1 and 2; (H) and (V) denote the horizon step and the vertical step; λ and ρ denote the degree of variable node and check node; the size of the Galois field satisfies $q = 2^p$; R is the code rate.

Algorithm 2:

Steps from 1) to 4a) are the same as Algorithm 1.

4) b') Constraint the dynamic range of LLRV: $\mathbf{r}'^{(n)} = \mathbf{r}^{(n)} - \max(\mathbf{r}^{(n)})$. If any component of $\mathbf{r}'^{(n)} < \tau$, set it to be τ, where $\tau < 0$ is a threshold of dynamic range.
   c') All vectors in the log-domain are converted to plain-likelihood.
   d') Perform p-FFT over $\mathbf{r}'^{(n)}$. Let $\mathbf{R}^{(n)} \triangleq \mathrm{FFT}(\mathbf{r}'^{(n)})$.
   e') All vectors are converted to LNS.
   f') Multiply all $\mathbf{R}^{(n)}$ using multiplication in LNS. The result is denoted by $\mathbf{L}$.
   g') Constraint the dynamic range of LLR value: $\mathbf{L}' = \mathbf{L} - \max(\mathbf{L})$. If any component of $\mathbf{L} < \tau$, set it to be τ.
   h') All vectors in LNS are converted to plain-likelihood.
   i') Perform p-IFFT over $\mathbf{L}'$ to $\mathbf{l}'$.
   j') All vectors are converted to the log domain.
   k') Perform a permutation of $\mathbf{l}'$ over GF(q) to get $\mathbf{l}$.

In Algorithm 2, we require only the addition, natural logarithm, and natural exponent operations. In Table I, we compute the decoding complexity of binary and nonbinary LDPC codes for the horizon step (H) and the vertical step (V), respectively. The decoding complexity of nonbinary codes is shown to scale by q. Note that the complexity of these two algorithms also depends on the exact implementation of LNS addition/subtraction, natural logarithm, and natural exponent. Assuming that the complexity of these operations is similar, Algorithm 2 clearly has a lower complexity for higher order codes with larger values of q. This is confirmed by our computer simulations where we observe that Algorithm 2 runs about four times faster than Algorithm 1 for the same GF(256) code.

IV. Quasi-cyclic LDPC construction

Quasi-cyclic (QC) LDPC codes form an important class of LDPC codes. The quasi-cyclic structure allows linear-time

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

encoding with shift registers [15]. It also saves much memory for the storage of the parity check matrix. Recently, Lin *et. al.* [16] proposed a general approach to construct GF(q) QC LDPC codes based on finite fields. These codes are defined by a special type of circulant permutation matrix, called a q-ary *α-multiplied circulant permutation matrix*, such that the nonzero entries in the parity check matrix are as uniformly distributed as possible. However, this structure requires that the dimensions of the parity check matrix has to be $m(q-1) \times n(q-1)$. Therefore, this construction is not as flexible when it comes to the design of short nonbinary LDPC codes.

In this section, we propose a modified approach to construct quasi-cyclic nonbinary LDPC codes. In this approach, a q'-ary *β-multiplied circulant permutation matrix* is constructed as a backbone of q-ary LDPC codes, where $q' = 2^{p'}, p' <= p$, β is a primitive element of GF(q'). Since GF(q') is a subfield of GF(q), we must have $\beta = \alpha^{(q-1)/(q'-1)}$, where α is the primitive element in GF(q). The dimension of the circulant permutation matrix is $(q'-1) \times (q'-1)$. Each row is the right cyclic-shift of the row above it multiplied by β and the first row is the right cyclic-shift of the last row multiplied by β. The nonzero element δ in the first row of the circulant matrix is randomly chosen from $\{\alpha^0, \cdots, \alpha^{(q-1)/(q'-1)-1}\}$. Thus, all the nonzero elements $\delta, \beta\delta, \cdots, \beta^{q'-2}\delta$ in the circulant matrix are just the coset of GF(q'). We remark that Lin *et. al.*'s construction [16] is a special case of our construction when $p' = p$, and the nonzero element δ in the first row of the circulant matrix is set to be α^i, where i is the location the nonzero entry in the row. The advantage of our construction is that the dimensions of circulant matrix can be chosen freely, which makes it more flexible to design nonbinary codes of short lengths. The proposed structure is quite general and any binary QC LDPC codes can be converted to nonbinary LDPC codes if the dimension of circulant matrix equals $(q'-1) \times (q'-1)$.

Next, we combine our code construction with quadratic permutation polynomial (QPP) over integer rings [10] to design nonbinary QC codes. The basic idea of the QPP construction is to characterize the edge interleaver using a quadratic permutation polynomial over integer rings $f(x) = f_1x + f_2x^2 \pmod{N}$, where N is the number of the edges in the graph, the input x is the left-label of the edges, and the output $f(x)$ is the right-label of the edges. The code defined by QPP is quasi-cyclic if the coefficients f_1 and f_2 meet certain conditions [10]. Therefore, the code construction problem reduces to a search for good coefficients which meet these conditions. A detailed description of the QPP construction is given in [10].

As shown above, nonbinary QC codes restrict the dimension of the circulant matrix to be $(q'-1) \times (q'-1)$. Hence, more stringent conditions are needed for the search of good coefficients f_1 and f_2. We develop a modified search procedure as follows:

Step 1. Choose the degree distribution (λ, ρ), code size (n, k), and circulant matrix size $q'-1$. Let the interleaver length $N = n\lambda, \eta = n/(q'-1),$ and $\gamma = (n-k)/(q'-1)$.

Step 2. Set f_2 to be the product of every prime factor of N repeated one or multiple times.

Step 3. Search for f_1 to maximize the girth of the corresponding graph and ensure that the size of the circulant matrix is $q'-1$.

Step 4. Repeat the previous step with a larger f_2 until no improvement in girth.

Step 5. Label the edges of the resultant graph according the proposed procedure.

We can apply the procedure above to construct a regular LDPC code over GF(256). We choose the size of the circulant matrix to be 15 in order to obtain a code length of 300 (the coded sequence consists of 300 GF(256) symbols). This is a regular, rate $1/2$ code, where all variable nodes have degree 2 and all check nodes have degree 4. Given these parameters, we construct the code using the QPP $f(x) = 17x + 30x^2$, which gives a local girth of 14 for each variable node. In addition, we also construct another nonbinary LDPC code over GF(256) based on the PEG construction. For the PEG construction, 67.36% of variable nodes have a local girth of 14, 29.17% of variable nodes have a local girth of 12 and 3.47% of variable nodes have a local girth of 10. Both codes will be used in the simulation section.

V. Simulation results

In this section, we compare the performance of the proposed nonbinary system with that of the system using optimized binary irregular LDPC code. All codes have a rate of $1/2$. We use the nonbinary code over GF(256) constructed in Section IV. The code length is 300 GF(256) symbols which represents $300 * 8 = 2400$ bits. The decoding algorithm of the nonbinary code is implemented according to the Algorithm 2 described in Section III. To ensure fair comparisons, we use binary codes of the same length. The optimized degree distribution of the binary codes shown in Table II are found using the EXIT chart approach [11].

TABLE II

Degree distributions of the optimized binary LDPC codes

SISO	$d_v = [2, 3, 11]$	$u_v = [0.256, 0.2075, 0.5365]$
	$d_c = [8, 9]$	$u_c = [0.8530, 0.1470]$
MIMO	$d_v = [2, 3, 8, 9]$	$u_v = [0.403, 0.2877, 0.1133, 0.196]$
	$d_c = [6]$	$u_c = [1]$

In Table II, d_v and d_c denote the degree sequences of the variable nodes and the check nodes, respectively. $u_v(i)$ denotes the fraction of edges that are connected to variables nodes of degree $d_v(i)$. $u_c(i)$ denotes the fraction of edges that are connected to check nodes of degree $d_c(i)$.

First, we consider the SISO channel shown in Fig. 2(a). Fig. 3 shows performance comparison of the nonbinary LDPC code versus the optimized binary code specified in Table II. For the nonbinary system, we compute the initial LLRV only once using (2), followed by 150 inner iterations of LDPC decoding. For the binary system, joint detection and channel decoding is performed iteratively. Namely, the MAP detector is applied after each LDPC decoding iteration. The total number of detector/decoding outer iterations is 150. Fig. 3 shows that the nonbinary system employing the GF(256) code achieves the best performance. At the bit-error-rate (BER) = 10^{-5} or

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

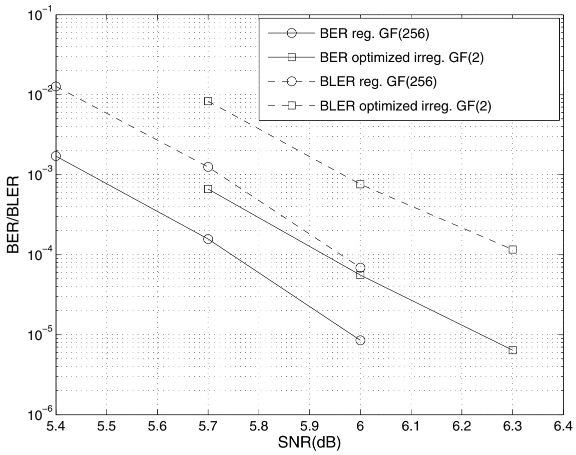


Fig. 3. Performance comparison of regular GF(256) LDPC code with the optimized irregular GF(2) (binary) LDPC code for a SISO channel with 16QAM modulation.

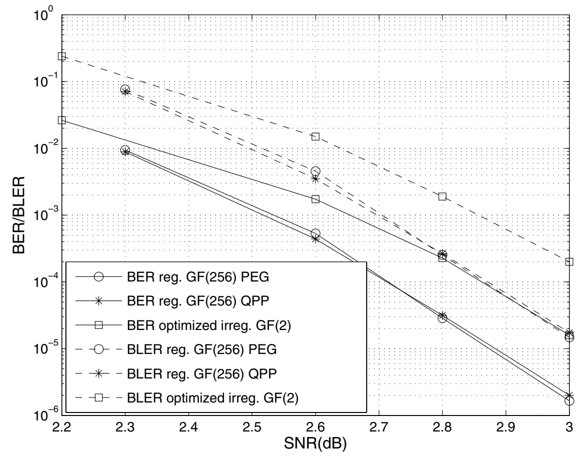


Fig. 4. Performance comparison of regular GF(256) LDPC codes (both PEG and QPP constructions) with the optimized irregular GF(2) (binary) LDPC code for a MIMO channel with $N_t = N_r = 4$ and QPSK modulation.

the block-error-rate (BLER) = 10^{-4}, it has about 0.3 dB gain over the binary system using the optimized irregular binary LDPC code. Next, we consider the MIMO channel shown in Fig. 2(b). Similar to the SISO case, for the nonbinary code, the initial LLRV is computed only once using (2), followed by 150 inner iterations of LDPC decoding. For the binary code, we employ the optimal MAP detector. To reduce complexity, optimal MAP detection is performed after every 10 iterations of LDPC inner decoding. Here we set the number of outer iterations between the MAP detector and the LDPC decoder to be 15. Fig. 4 shows that the nonbinary system outperforms the binary system with the optimized irregular LDPC code by about 0.2 dB at BER= 10^{-5} or BLER = 10^{-4}. It also shows that the QPP construction of the nonbinary code achieves comparable performance with that of the PEG construction.

While a detailed complexity comparison of the nonbinary system with the binary system is out of the scope of this paper, we comment that since the nonbinary system applies the MAP detection only once, its simulation time, mostly spent on LDPC decoding, is much less than that of the binary system in the MIMO case. In comparison, for the binary system, in addition to channel decoding, the MAP detector occupies significantly portion of the simulation time due to joint detection and channel decoding.

VI. Conclusion

In this paper, we propose a nonbinary LDPC coded system for communication over fading channels using high order modulations. The proposed nonbinary system using the regular LDPC code over GF(q) outperforms widely studied binary systems using the optimized irregular binary LDPC code in both performance and complexity. We also develop a low complexity decoding algorithm for the nonbinary LDPC codes that has a superior numerically stability. A quasi-cyclic construction of nonbinary LDPC codes is also proposed which achieves a comparable performance with the PEG codes while allowing linear-time encoding. Future work includes the design of nonbinary LDPC codes for MIMO channels and the design of more efficient decoding algorithms for nonbinary LDPC codes over large Galois fields.

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] M. C. Davey and D. Mackay, “Low-density parity check codes over GF(q),” *IEEE Comm. Letters*, vol. 2, pp. 165–167, June 1998.

[4] 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.

[5] 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.

[6] 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.

[7] F. R. Kschischang, B. J. Frey, and H. A. Loeliger, “Factor graphs and the sum-product algorithm,” *IEEE Trans. Inform. Theory*, vol. 47, pp. 498–519, Feb. 2001.

[8] M. C. Davey, *Error-Correction using Low Density Parity Check Codes*. PhD thesis, University of Cambridge, UK, 1999.

[9] H. Song and J. Cruz, “Reduced-complexity decoding of Q-ary LDPC codes for magnetic recoding,” *IEEE Trans. Magnetics*, vol. 39, pp. 1081–1087, March 2003.

[10] O. Y. Takeshita, “A new construction for LDPC codes using permutation polynomials over integer rings,” *submitted to IEEE Trans. Inform. Theory*, June 2005.

[11] 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.

[12] E. E. Swartzlander, Jr., D. V. S. Chandra, H. T. Nagle, Jr., and S. A. Starks, “Sign/logarithm arithmetic for FFT implementation,” *IEEE Trans. Comput.*, vol. C-32, pp. 526–534, June 1983.

[13] D. E. Dudgeon and R. M. Mersereau, *Multidimensional Digital Signal Processing*. Prentice Hall, 1984.

[14] V. Paliouras and T. Stouraitis, “A novel algorithm for accurate logarithmic number system subtraction,” in *International Symposium on Circuits and Systems*, (Atlanta), pp. 268–271, May 1996.

[15] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*. Cambridge, MA: MIT Press, 2nd ed 1972.

[16] S. Lin, S. Song, L. Lan, L. Zeng, and Y. Y. Tai, “Constructions of nonbinary quasi-cyclic ldpc codes: a finite field approach,” in *Info. Theory and Application Workshop*, (UCSD), 2006.

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.