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

Rong-Hui Peng and Rong-Rong Chen

Department of Electrical and Computer Engineering
University of Utah

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

Outline

- Motivation
- Apply nonbinary LDPC codes over large Galois fields to fading channels
- Low complexity nonbinary LDPC decoding
- Quasi-cyclic construction
- Simulation results
- Conclusion

Motivation

- Binary LDPC coded system has been studied extensively.
- Optimal binary code has been designed to approach channel capacity.
- Nonbinary LDPC code design has been studied for AWGN and shows better performance than binary codes [1][2].

[1] 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.

[2] 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.

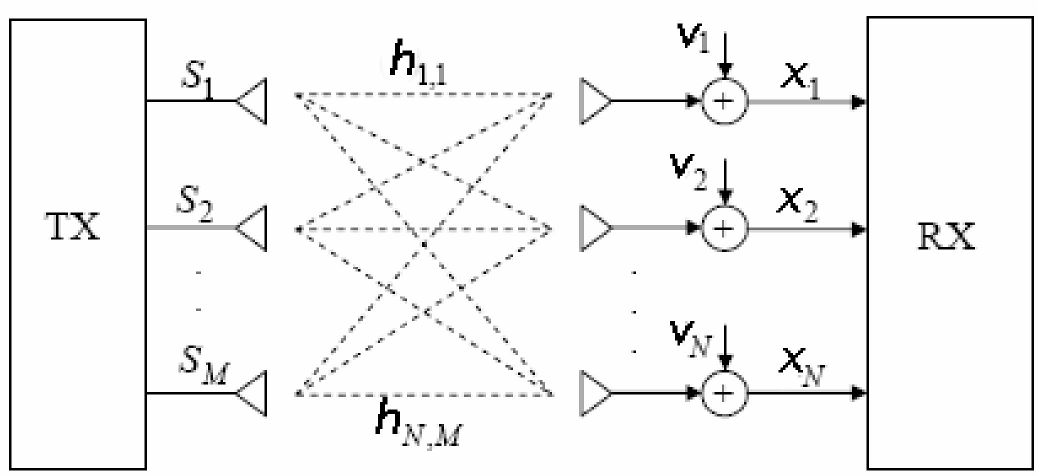
Motivation

- Our contribution
  - Apply large field nonbinary LDPC codes to fading channel
  - Propose efficient nonbinary LDPC decoding algorithm.
  - Construct nonbinary QC LDPC codes based on QPP[3]
  - Provide comparison with optimal binary LDPC coded systems

[3] Oscar. Y. Takeshita "A New Construction for LDPC Codes using Permutation Polynomials over Integer Rings" Submitted to *IEEE Trans. Inform. Theory*

Application to fading channels

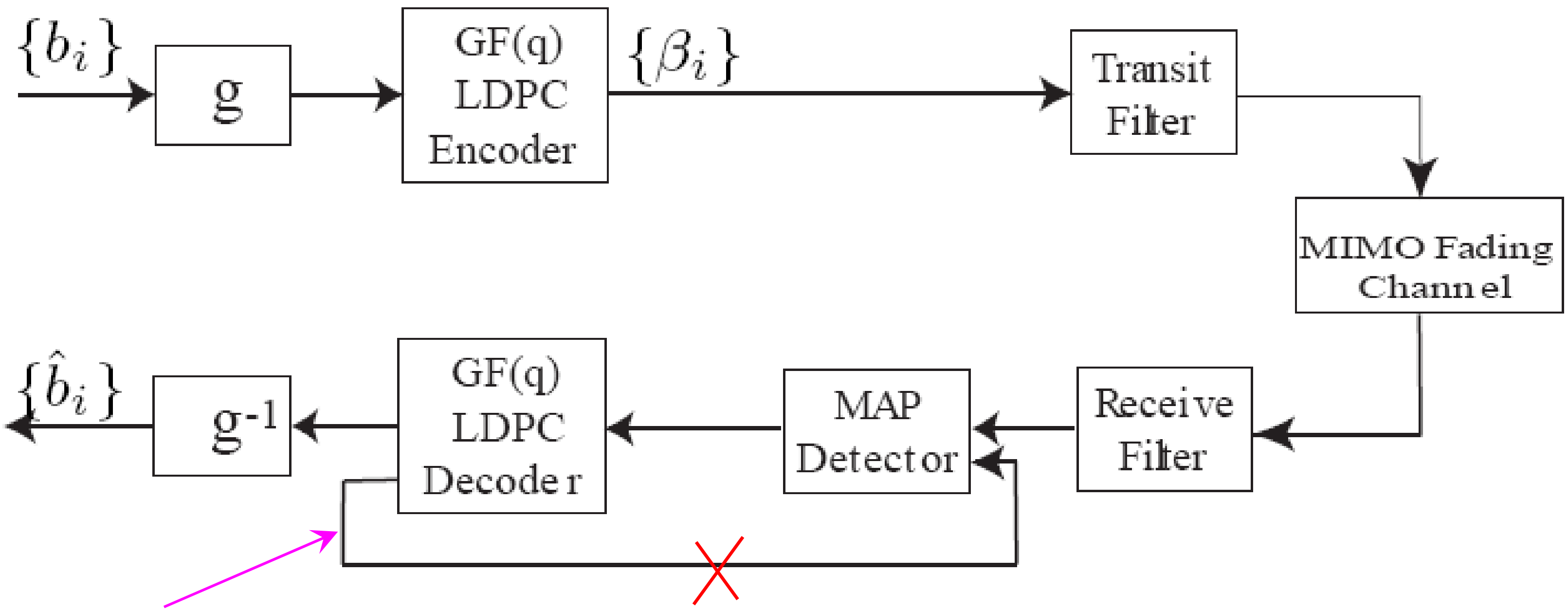
- Channel model



$$\mathbf{X} = \sqrt{\frac{\rho}{M}}\mathbf{HS} + \mathbf{V}$$

Assume each entry of channel matrix is independent, follows Rayleigh fading, and is known by receiver

System block diagram



Non-iterative system: the detection is performed only once.

Iterative system: Soft messages are exchanged between detector and decoder iteratively.

R.-H. Peng and R.-R. Chen, "*Good LDPC Codes over GF(*q*) for Multiple-Antenna Transmission*", Presented on MILCOM 2006

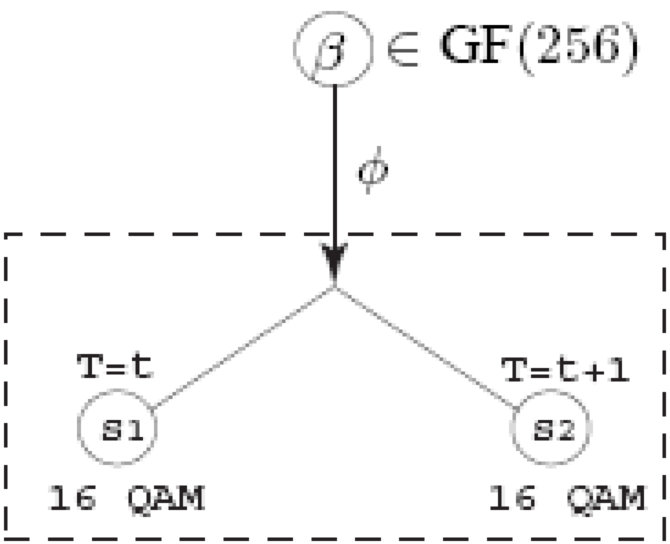
Non-iterative system

- Used for the systems with small number of antennas

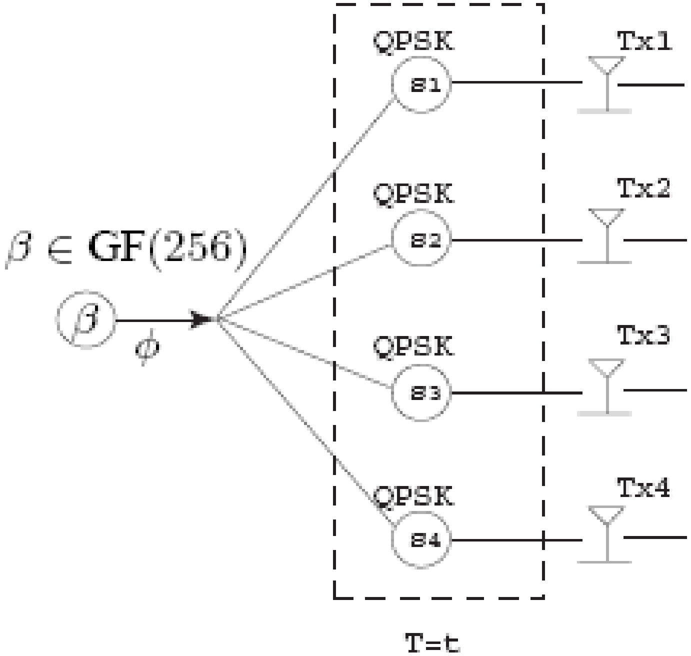
  $\log_2 q = N_s m \quad m$: the number of constellation bits

  N_s denote the number of independent channel use

- Large GF(q)



(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

Log-likelihood ratio vector

- Soft message in binary system is LLR.

$$\ln \frac{\mathrm{p}(b=0)}{\mathrm{p}(b=1)}$$

- Soft message in nonbinary system is a vector-LLRV denote the log-likelihood ratio of being one element in GF(q).

$$\mathbf{z} = \{z_0, z_1, \cdots, z_{q-1}\}$$

$$\text{where}\, z_i = \ln \frac{\mathrm{p}(\beta=0)}{\mathrm{p}(\beta=i)}$$

$$i \in \{0,1,\cdots,q-1\}$$

Symbol-wise MAP detection

- Symbol-wise MAP detection

$$z_i = -\frac{1}{2\sigma^2}\sum_{l=1}^{N_s}\left(\left\|\mathbf{Y}_l - \mathbf{H}_l\mathbf{X}_l^i\right\|^2 - \left\|\mathbf{Y}_l - \mathbf{H}_l\mathbf{X}_l^0\right\|^2\right)$$

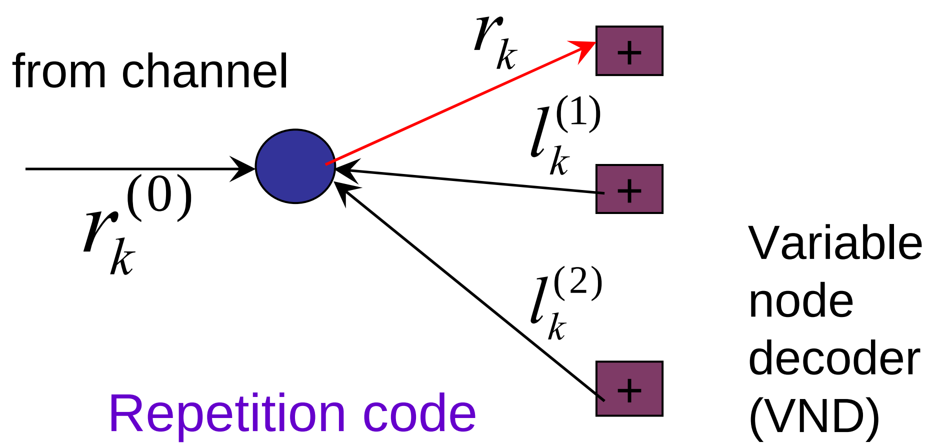
$\{\mathbf{X}_1^i, \mathbf{X}_2^i, \cdots, \mathbf{X}_{N_s}^i\} = \varphi(\beta = i)$ denotes the collection of N_s

transimitted constellation symbols corresponding

$i \in \mathrm{GF}(q)$

- No prior information feed back from LPDC decoder is required:
  - Detection is only performance once
  - Large complexity could be saved

Nonbinary LDPC decoding



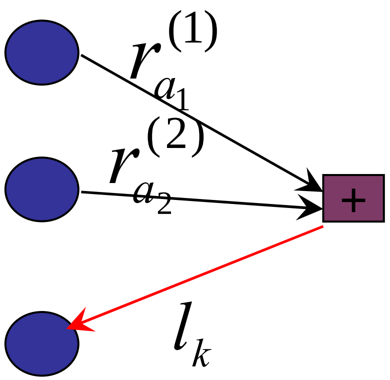
Vertical step:

$$r_k \propto r_k^{(0)} \prod_{n=1}^{d_v - 1} l_k^{(n)}$$

In log domain:

$$r_k^{'} = r_k^{'(0)} + \sum_{n=1}^{d_v - 1} l_k^{'(n)}$$

Nonbinary LDPC decoding



Check node decoder (CND)

Single parity check code

Horizon step:

$$l_k = \sum_{\sum g_n a_n = -g_{d_c} k} \prod_{n=1}^{d_c - 1} r_{a_n}^{(n)}$$

Direct computation has huge complexity!

Nonbinary LDPC decoding

- Horizon step can be considered as a multiple convolution over GF(q)
- Multi-dimensional FFT can be applied

$$R^{(n)} = \mathrm{DFT}(\bar{r}^{(n)})$$

$$\bar{l} = \mathrm{IDFT}\left(\prod_{n=1}^{d_c-1} R^{(n)}\right)$$

- The complexity is $O(q\log q)$

Log domain implementation

- $R^{(n)}$ may be negative value, can be represented by sign/logarithmic number system (LNS)

$$\mathrm{LNS}(u) = \begin{cases} \mathrm{sign}(u) \\ \log(|u|) \end{cases}$$

- In FFT, lots of LNS additions and subtractions required
- LNS addition/subtraction requires one comparison, two additions and one table look-up.

Log domain implementation

- To avoid LNS addition/subtraction, we propose to convert data from LNS to plain likelihood before the FFT and IFFT operations and then convert them back afterwards.
- Only additions, subtractions and conversions between log to normal domain are required.
- Complexity saving:

$$\text{Full log}: 2qd_c \quad \text{LNS addition/subtraction}$$

$$\text{Partial log}: 4\frac{q}{p}d_c \quad \text{Conversion between log and normal domain}$$

$$p = \log_2 q$$

  - 75% computation can be saved for GF(256) codes
- Accumulated errors could be reduced.

Quasi-cyclic construction

- Propose to use regular $(2, d_c)$ code for MIMO channels
- Modify the QPP method to construct nonbinary QC codes
  - with flexible code length
  - support pre-determined circulant size
  - allow linear-time encoding
  - perform close to the PEG construction

Quasi-cyclic construction

- Quasi-cyclic structure

$$\mathbf{H} = \begin{bmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} & \cdots & \mathbf{A}_{1,n} \\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2} & \cdots & \mathbf{A}_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{m,1} & \mathbf{A}_{m,2} & \cdots & \mathbf{A}_{m,n} \end{bmatrix}$$

- $\mathbf{A}_{i,j}$ is a circulant: each row is a right cycle-shift of the row above it and the first row is the right cycle-shift of the last row
- The advantage of QC structure
  - Allow linear-time encoding using shift register
  - Allow partially parallel decoding
  - Save memory

QC structure for GF(q)

- $\mathbf{A}_{i,j}$ is a $q^{'}-$ary $\beta-$*multiplied circulant permutation matrix*

$$\mathbf{A}_{i,j}=\begin{pmatrix} \cdots & 0 & \delta_{i,j} & 0 & \cdots & \cdots & 0 \\ \cdots & & 0 & \delta_{i,j}\beta & 0 & \cdots & \vdots \\ \vdots & \cdots & \cdots & 0 & \delta_{i,j}\beta^2 & 0 & \vdots \\ \vdots & & & \vdots & 0 & \ddots & 0 \\ \vdots & & & & \vdots & 0 & \ddots \\ \ddots & \vdots & \vdots & & & \vdots & 0 \\ \cdots & \delta_{i,j}\beta^{q^{'}-2} & 0 & \cdots & & & 0 \end{pmatrix}$$

$\mathrm{GF}(q') \subset \mathrm{GF}(q)$; β is a primitive element of $\mathrm{GF}(q')$

$\delta_{i,j}$ is randomly choosen from $\{\alpha^0, \alpha^1, \cdots, \alpha^{(q-1/(q'-1)-1}\}$

α is a primitive element of $\mathrm{GF}(q)$

QC structure for GF(q)

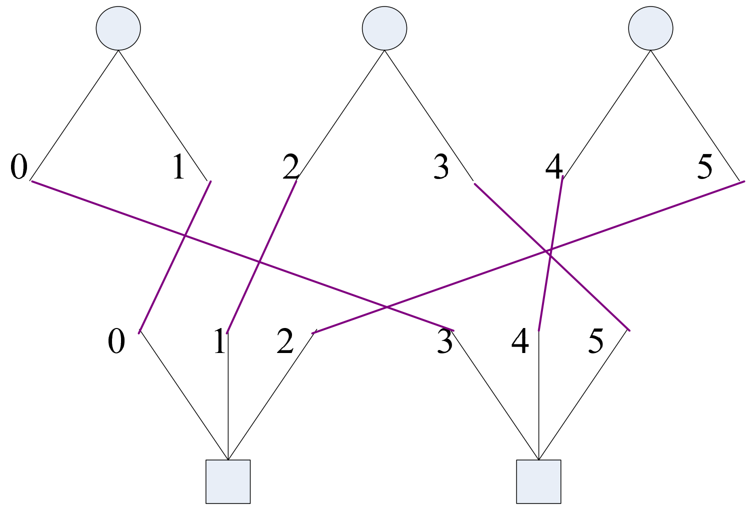
- With above structure, the nonzero elements are chosen as randomly as possible with equal probability for each element
- For each circulant, only the cyclic shift and the power of the first nonzero element need to be saved
- Many existing binary QC construction methods may be extended to nonbinary LDPC codes using this structure.
  - $\text{Code size}: n(q'-1)\times m(q'-1)$

    $\text{Circulant}: (q'-1)\times(q'-1)$

- Use QPP based method to construct nonbinary QC codes with large girth

QPP based method

- Code construction is based on edge interleaver $f(x)$



$f(0) = 3$
$f(1) = 0$
$f(2) = 1$
$f(3) = 5$
$f(4) = 4$
$f(5) = 2$

- Quadratic permutation polynomial over integer rings (QPP)

$$f(x) = f_1 x + f_2 x^2 \pmod{N}$$

N : the number of edges

QPP based method

- To be Quasi-cyclic, need to search f_1, f_2 with largest girth such that

$$f(x+\beta d_v)-f(x)\equiv 2f_2\,\beta d_v x+f(\beta d_v)\pmod N$$

$$\Rightarrow \qquad 2f_2\,\beta d_v\equiv 0\pmod N \qquad (1)$$

- Given (1), we have

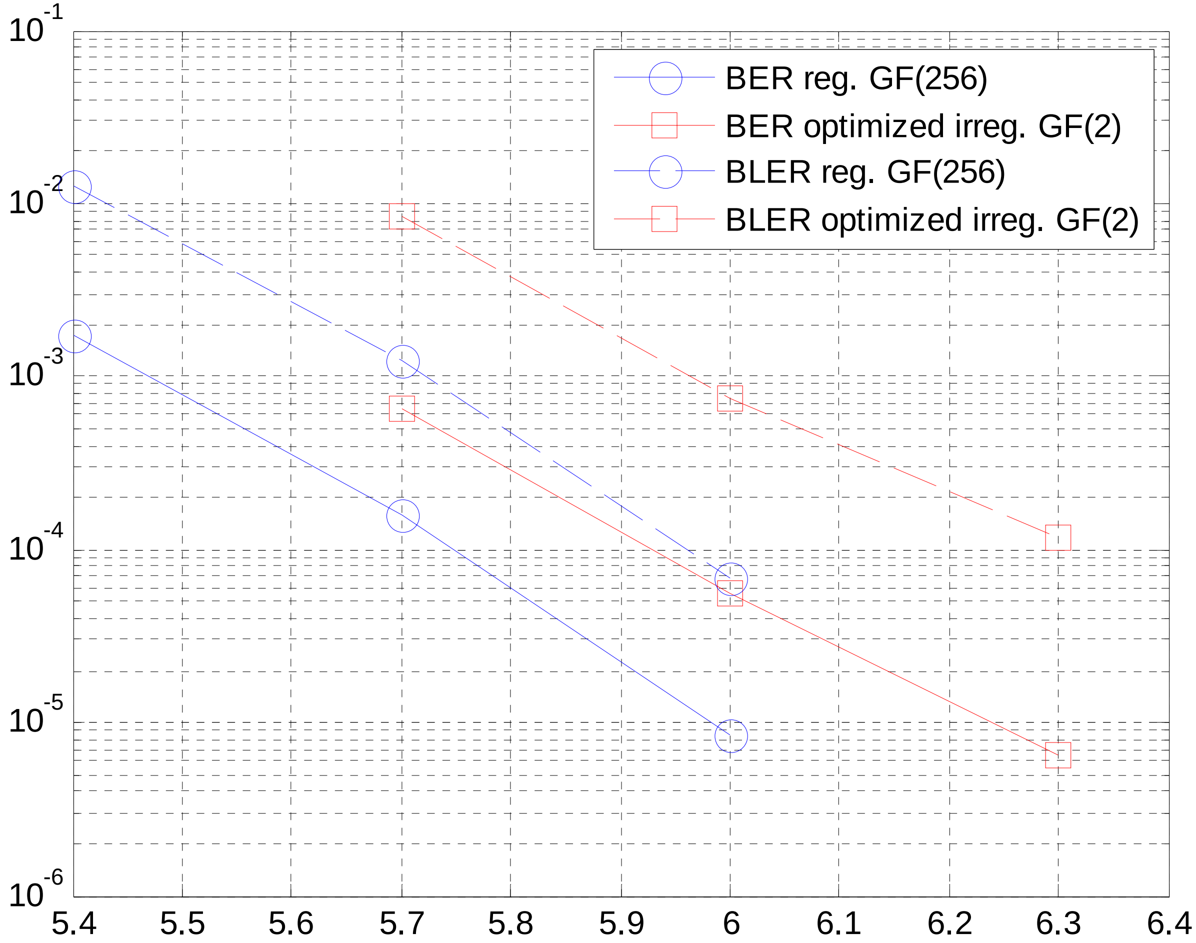
$$H(i,j)=H(i+k\beta,\,j+k\gamma),k=1,2,\cdots,q'-2,\gamma=f(\beta d_v)/d_c$$

- By grouping variable nodes $\{v_i, v_{i+\beta},\cdots v_{i+(q'-2)\beta}\}$, check nodes $\{c_i, c_{i+\gamma},\cdots c_{i+(q'-2)\gamma}\}$, obtain a QC code.

QPP based method

- Code example: Regular (2, 4) GF(256) code
  - Code length: 300
  - Circulant: 15x15
  - $f(x) = 17x + 30x^2$
  - Each node has local girth 14
- Compare with PEG construction
  - 68% variable nodes have local girth 14, 29% have local girth 12, 3% have local girth 10

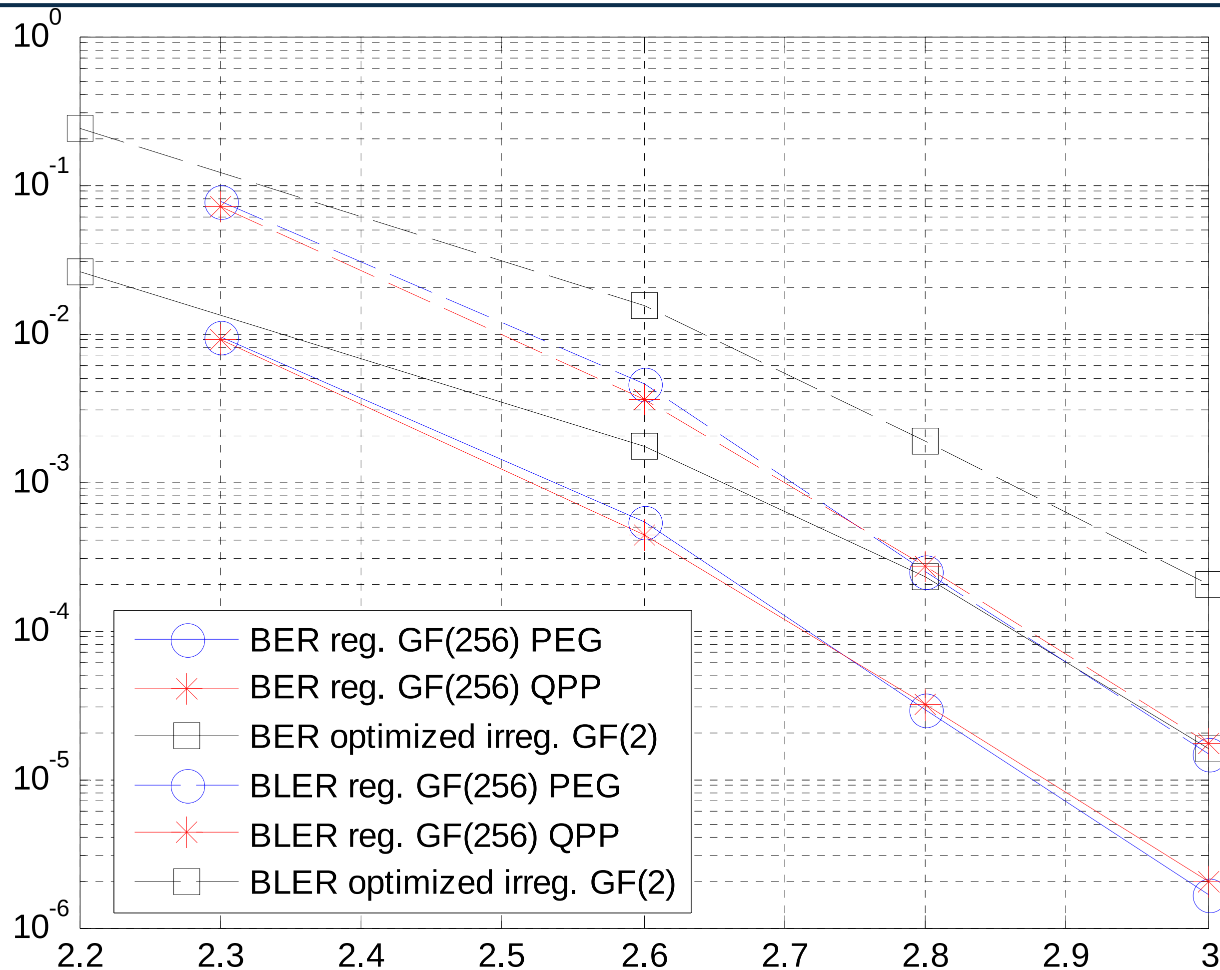
Simulation results



Nonbinary codes outperform optimized irrgular binary codes by 0.26dB in BER and by 0.35dB in BLER

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

Simulation results



Nonbinary codes outperform optimized irrgular binary codes by 0.16dB in BER and by 0.2dB in BLER

QPP codes have very close performance with PEG codes

Performance comparison of a regular GF(256) LDPC codes (both PEG and QPP constructions) with the optimized irregular GF(2) (binary) LDPC code for a MIMO channel with 4 transmit and receive antennas and QPSK modulation.

Conclusion

- Study the application of nonbinary LDPC codes for MIMO system
- Propose an efficient decoding algorithm for nonbinary LDPC codes
- Construct nonbinary LDPC codes based on QPP methods that are flexible in code length and circulant size
- Provide performance comparisons between regular nonbinary LDPC codes with optimized irregular binary LDPC codes
- Demonstrate that nonbinary LDPC codes are good candidates for MIMO channels based on both performance and complexity

Thanks !