Non-binary Protograph LDPC Codes for Short Blocklengths

Dariush Divsalar Lara Dolecek

NASA-JPL-Caltech UCLA

CCSDS Fall Meeting, October 16, 2012

Motivation and related work

- Non-binary and binary LDPC codes were invented by Gallager 50 years ago.

Motivation and related work

- Non-binary and binary LDPC codes were invented by Gallager 50 years ago.
- Early work in modern coding theory by MacKay and Davey (1998) recognized the superiority of non-binary LDPC codes over binary LDPC codes.

Motivation and related work

- Non-binary and binary LDPC codes were invented by Gallager 50 years ago.
- Early work in modern coding theory by MacKay and Davey (1998) recognized the superiority of non-binary LDPC codes over binary LDPC codes.
- Curiously, the majority of the subsequent results on graph-based codes and iterative decoding has focused on binary codes.

Motivation and related work

- Non-binary and binary LDPC codes were invented by Gallager 50 years ago.
- Early work in modern coding theory by MacKay and Davey (1998) recognized the superiority of non-binary LDPC codes over binary LDPC codes.
- Curiously, the majority of the subsequent results on graph-based codes and iterative decoding has focused on binary codes.
- Recent exciting results Poulliat, Fossorier, Declercq (2008), and Liva, Paolini, Scalise, Chiani, Costantini, Matuz(2011-2012) on design and analysis of non-binary LDPC codes.

Motivation and related work

Our previous results:

- EXIT chart analysis (Milcom 2011); weight enumerator polynomials and ensemble analysis (ISIT 2011, ITW 2011, ISIT 2012); typical minimum distance properties (ITA 2012); non-binary protograph-based LDPC codes for short blocks (ITW 2012).

Motivation and related work

Our previous results:

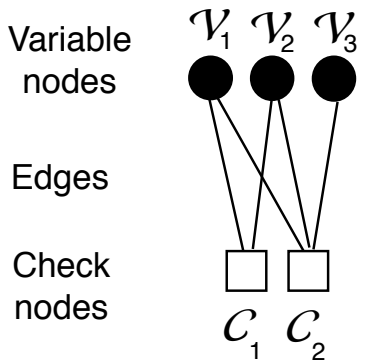
- EXIT chart analysis (Milcom 2011); weight enumerator polynomials and ensemble analysis (ISIT 2011, ITW 2011, ISIT 2012); typical minimum distance properties (ITA 2012); non-binary protograph-based LDPC codes for short blocks (ITW 2012).

This work:

- Design of short non-binary protograph-based LDPC codes over lower field size for lower complexity.

Non-Binary Protograph-Based LDPC Codes

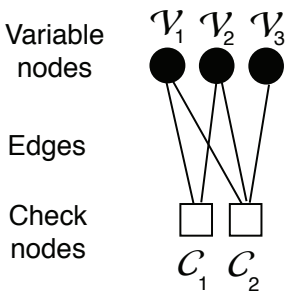
The basic building block is a *protograph* (Thorpe, 2003).



$$G = (V, C, E)$$

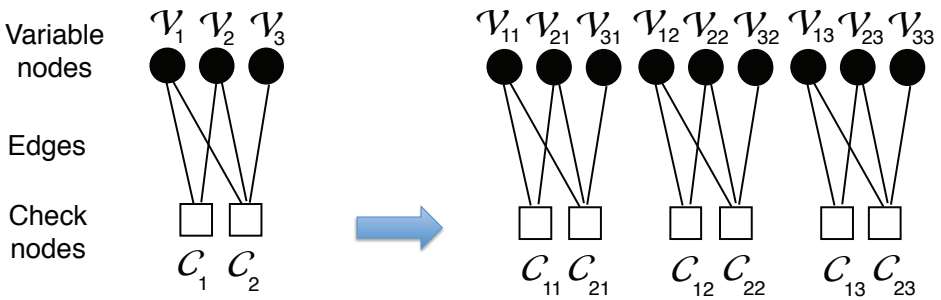
Non-Binary Protograph-Based LDPC Codes

The protograph-based non-binary LDPC code is obtained by a copy-permute-scale operation.



Non-Binary Protograph-Based LDPC Codes

The protograph-based non-binary LDPC code is obtained by a copy-permute-scale operation.

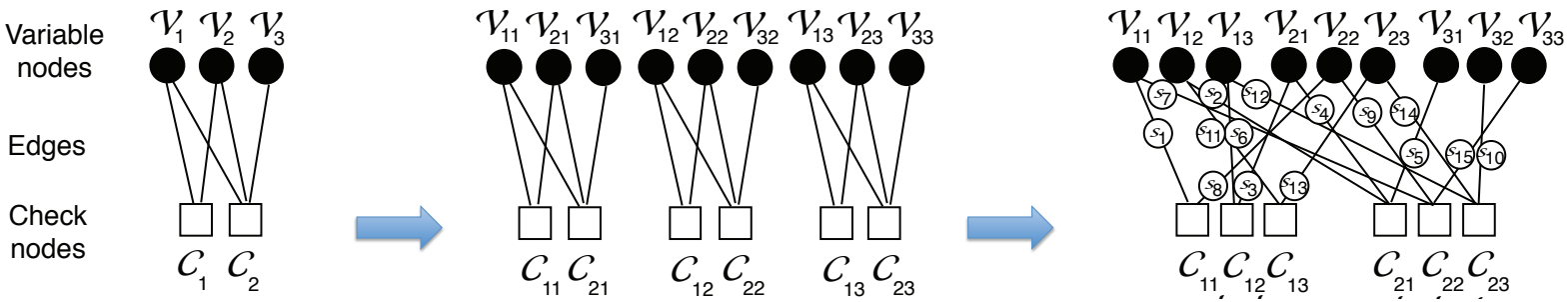


$N = 3$ replications

Edges are weighted by s_i's as non-zero elements of $GF(q)$.

Non-Binary Protograph-Based LDPC Codes

The protograph-based non-binary LDPC code is obtained by a copy-permute-scale operation.

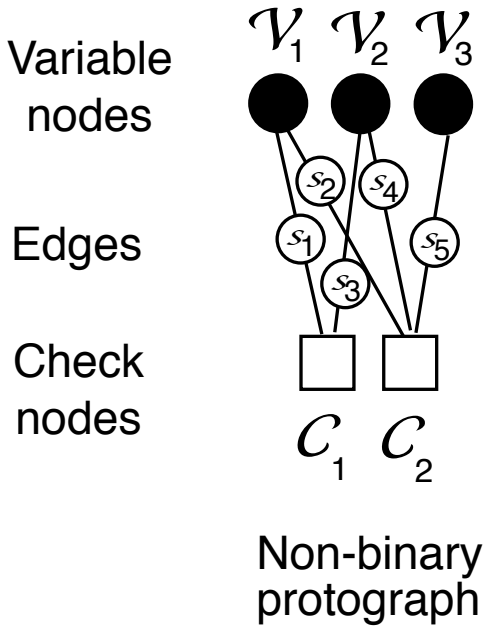


$N = 3$ replications

Edges are weighted by s_i's as non-zero elements of $GF(q)$.

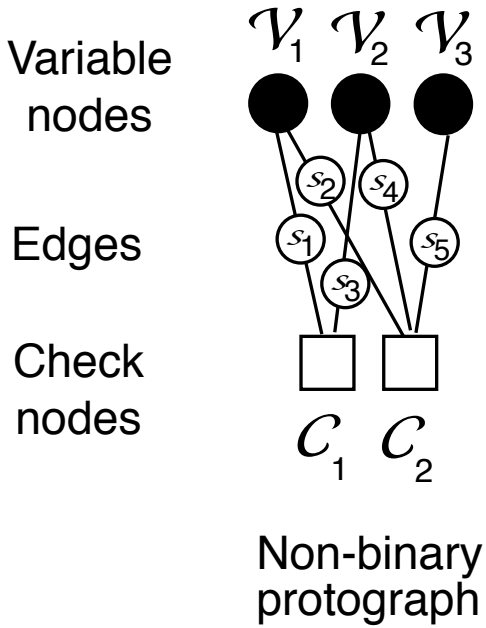
Graph Cover of Non-binary Protograph LDPC Codes

We introduce the *non-binary protograph* $G = (V, C, E, S)$ as a basic building block. It is a natural extension of binary protograph (Thorpe, 2003).



Graph Cover of Non-binary Protograph LDPC Codes

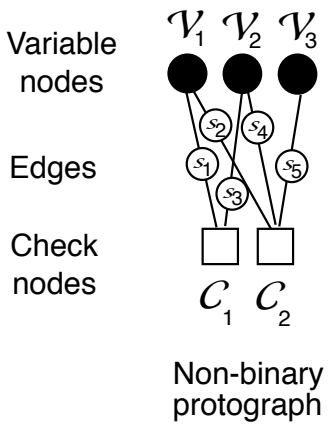
We introduce the *non-binary protograph* $G = (V, C, E, S)$ as a basic building block. It is a natural extension of binary protograph (Thorpe, 2003).



Edges are weighted by s_i's as non-zero elements of $GF(q)$.

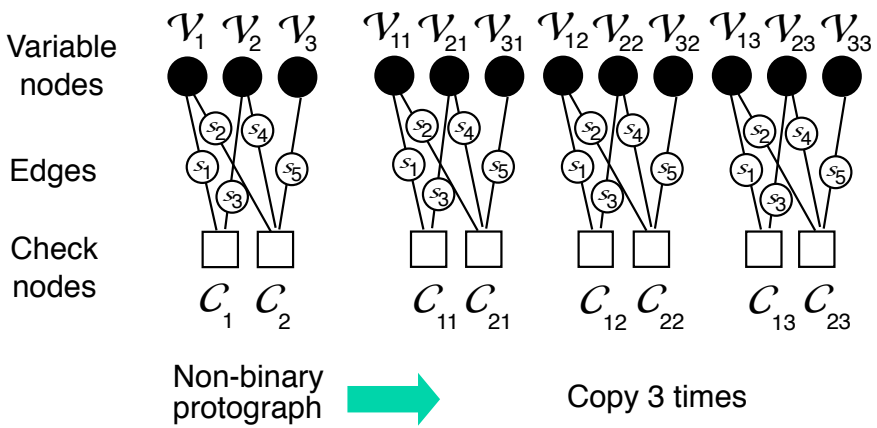
Graph Cover of Non-binary Protograph LDPC Codes

The protograph-based non-binary LDPC code is obtained by a copy-permute operation.



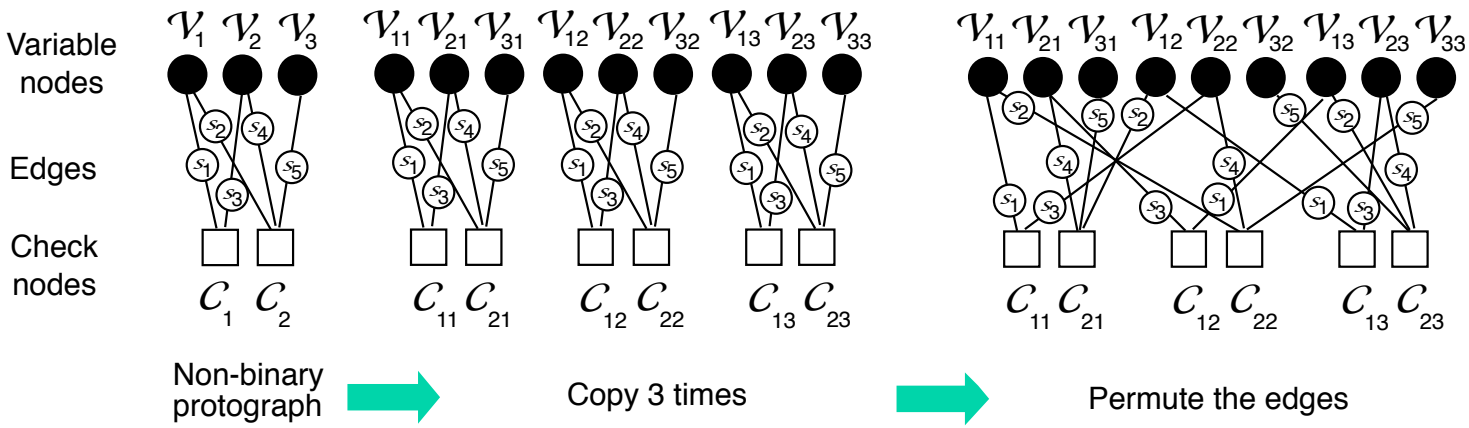
Graph Cover of Non-binary Protograph LDPC Codes

The protograph-based non-binary LDPC code is obtained by a copy-permute operation.

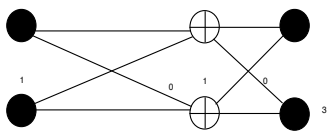


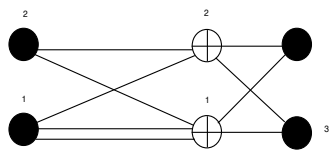
Graph Cover of Non-binary Protograph LDPC Codes

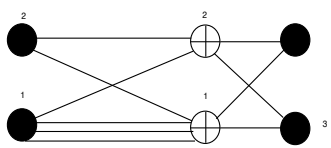
The protograph-based non-binary LDPC code is obtained by a copy-permute operation.

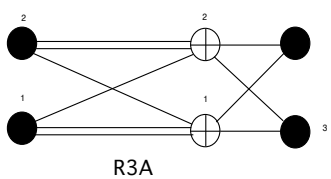


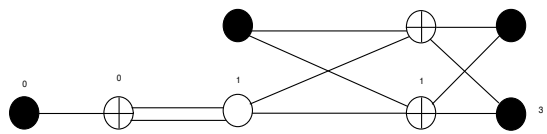
Protograph for construction of NB codes

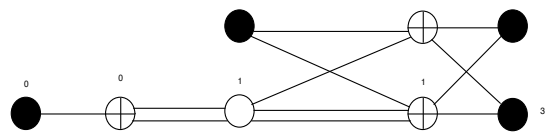


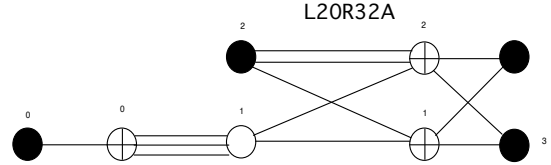


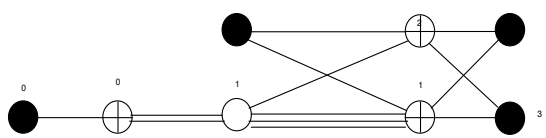


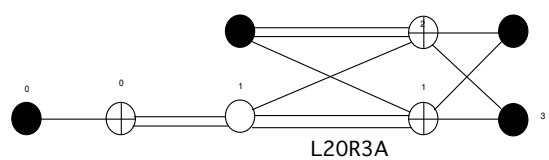




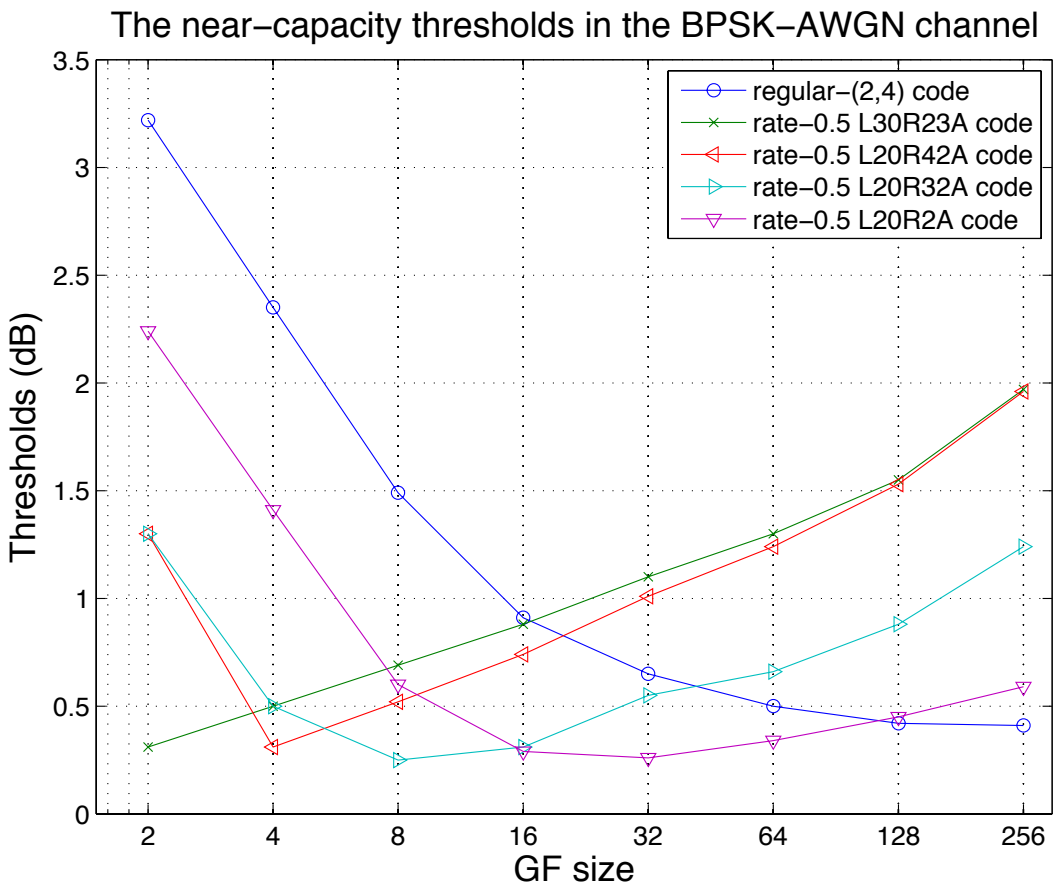




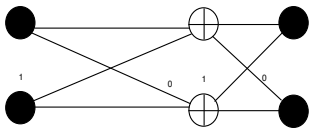




EXIT of NB protograph codes

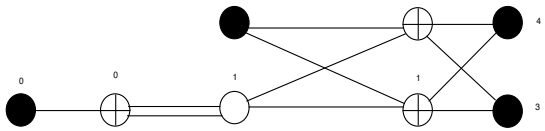


Selected NB protograph codes over GF(256) and GF(16)



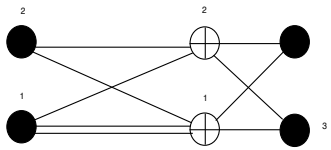
Regular (2,4) protogrph (R2A)
for NB codes over GF(256)
Threshold 0.31 dB

Selected to be used for both for
C-NBPB and U-NBPB over GF(256)



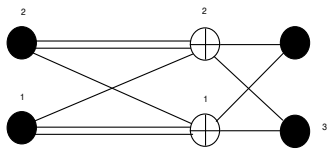
L20R2A protograph
for NB codes over GF(16)
Threshold 0.37 dB

A good protograph for NB
construction over GF(16)
at low SNR (shows error floor
at high SNR)



R32A protograph
for NB codes over GF(16)
Threshold 0.59

A good protograph for NB
construction over GF(16)
at moderate SNR (shows error floor
at higher SNR)



R3A protograph
for NB codes over GF(16)
Threshold 0.62

Selected to be used for U-NBPB
construction over GF(16)
due to low error floor

Cycles of lifted protographs with circulants for construction of C-NBPB and U-NBPB codes over GF(256)

N / cycle size	8	12	16	20	24	28	32
4	36	96	72	0	0	0	0
8	20	160	634	2304	5184	5632	1464
16	0	208	788	5760	28392	146192	614872

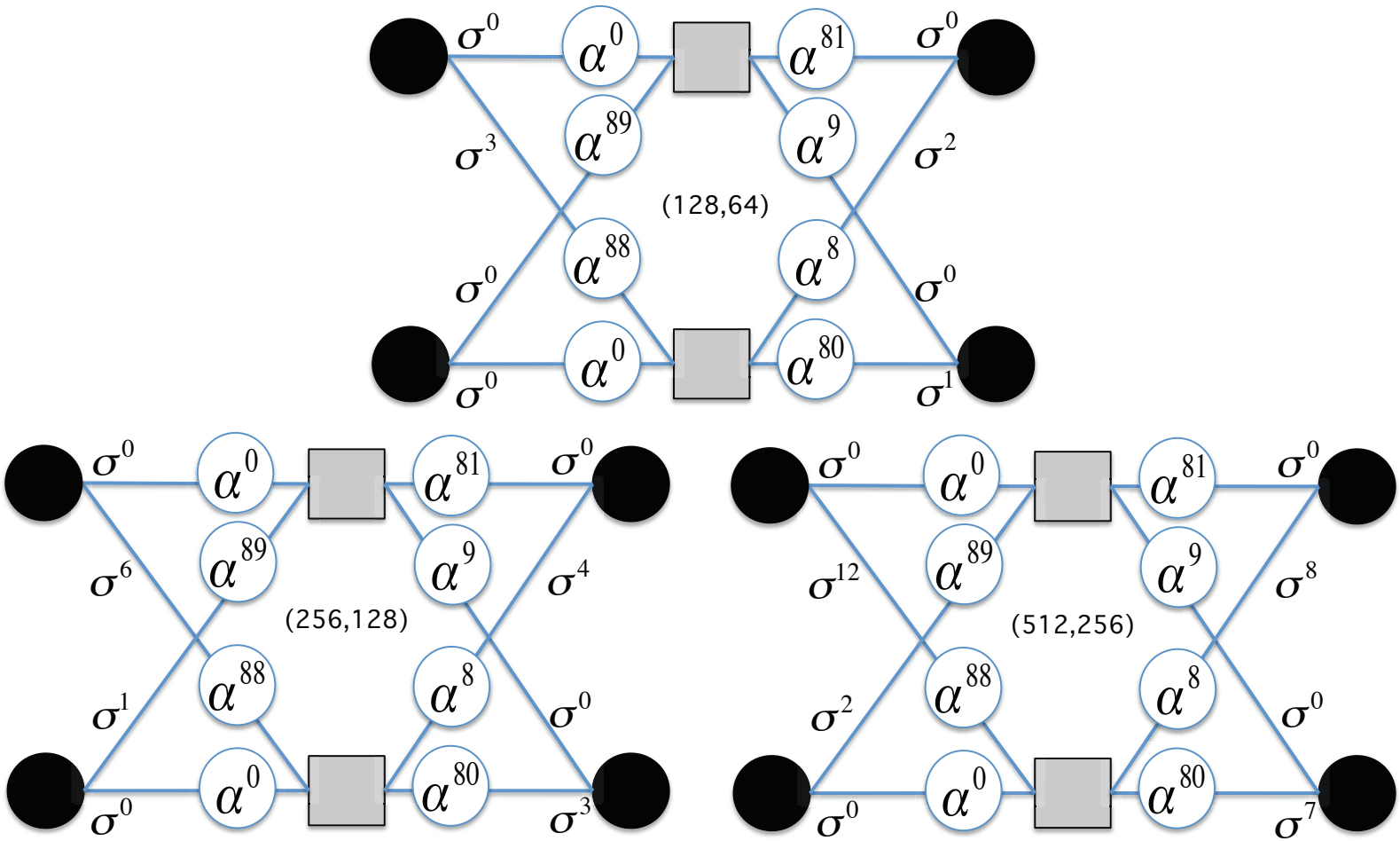
Table: Distribution of cycles for expanded graph with 4 variable nodes and 2 check nodes by circulant permutation matrices of size $N \times N$.

Selected primitive polynomial for GF(256)

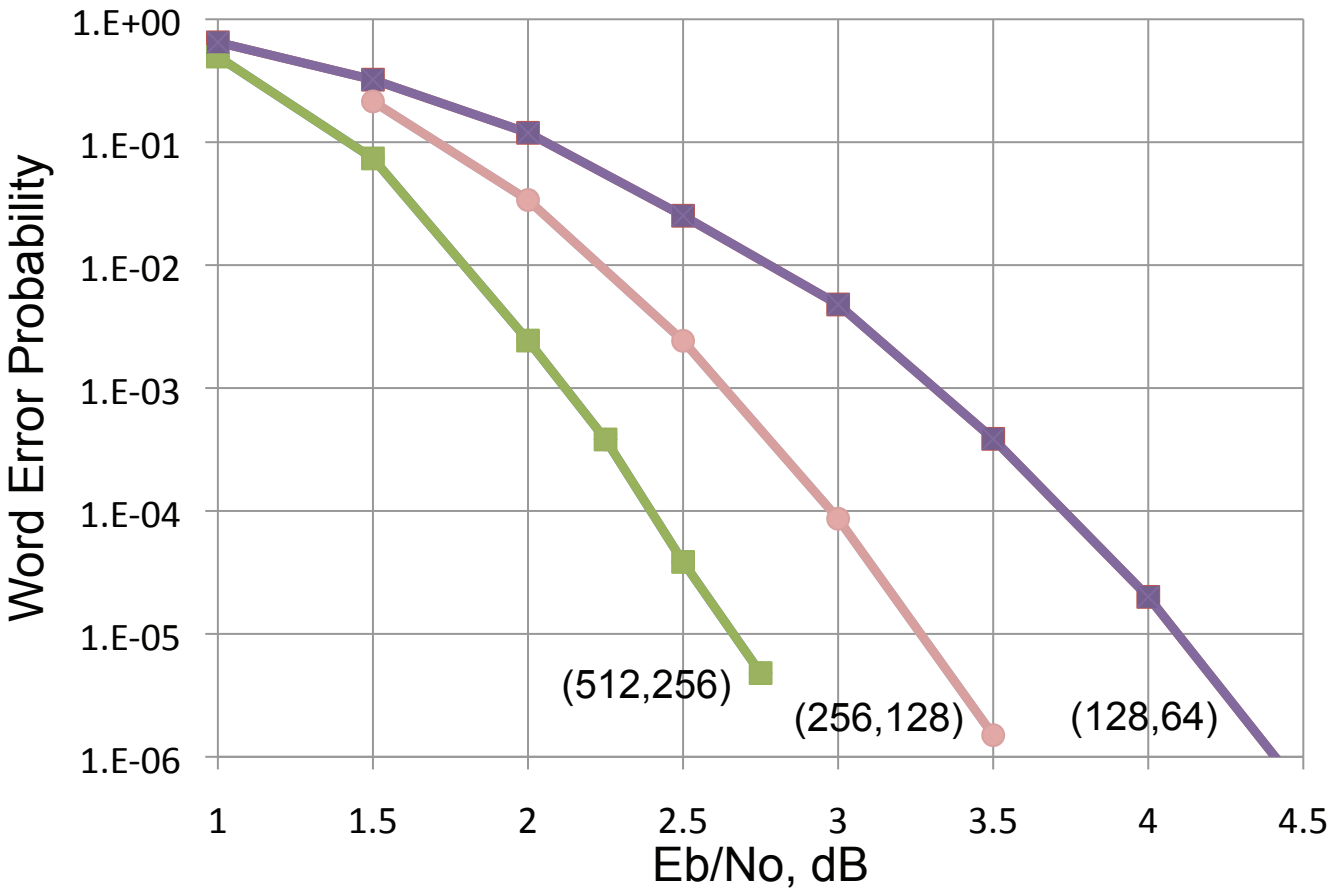
let α be a primitive element of GF(256)
Let $p(x) = 1 + x^2 + x^3 + x^4 + x^8$ be a primitive polynomial
Primitive element can be represented with a matrix

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

Graph cover NBPB (C-NBPB) codes



Performance of Graph cover NBPB (C-NBPB) codes

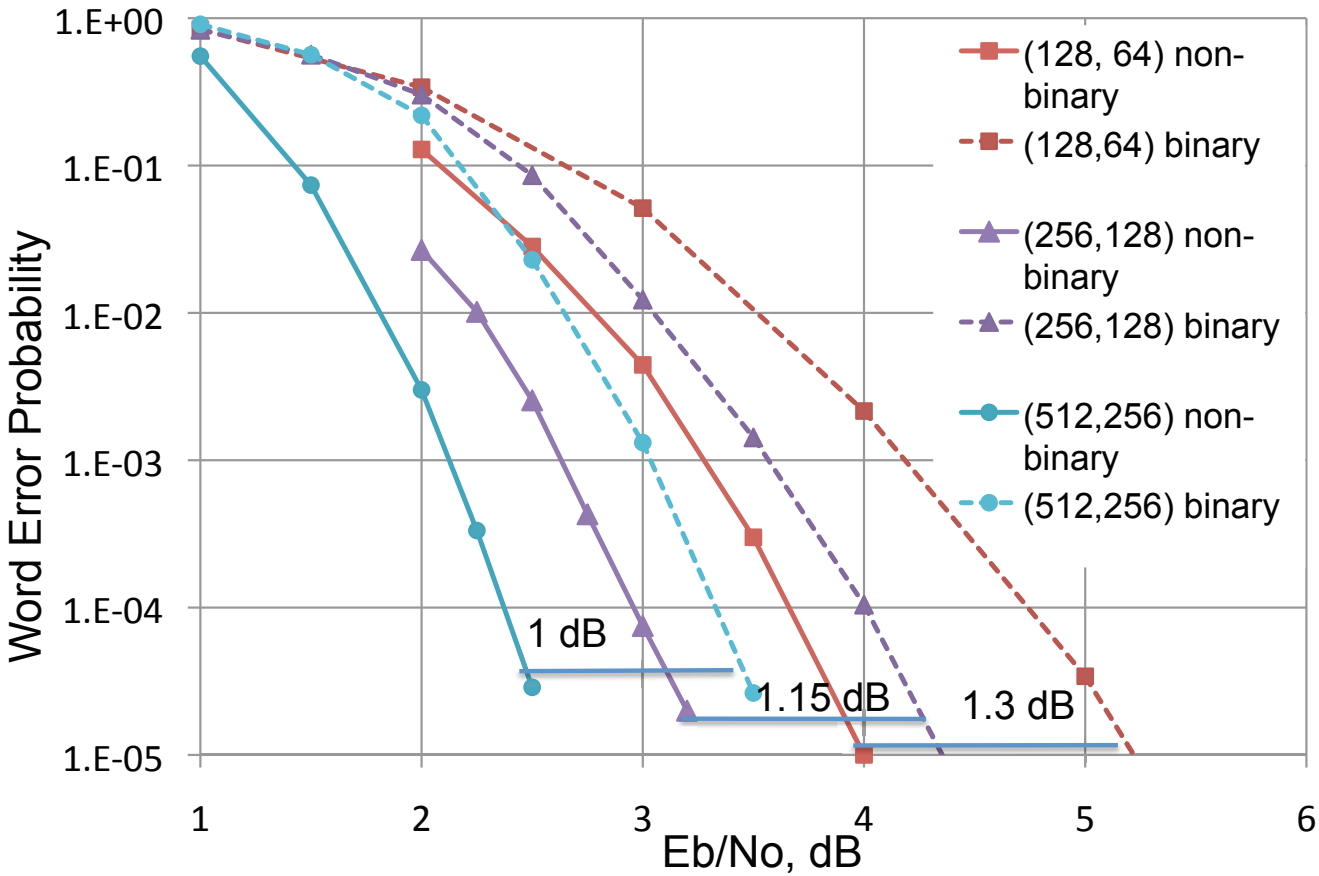


Parity check matrix of U-NBPB codes over GF(256)

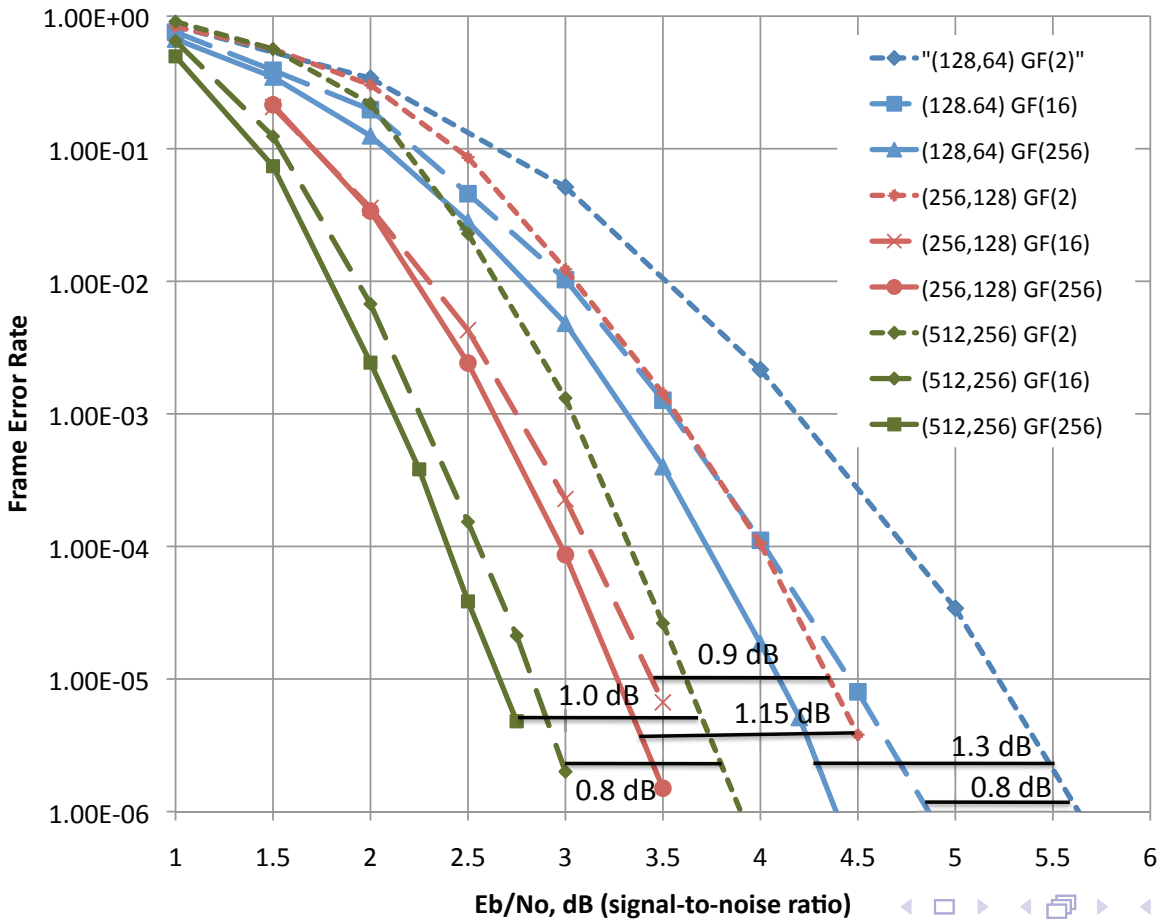
Example of parity check matrix of NB protograph code for (128,64) (in bits)

$$H = \begin{bmatrix}
\alpha^{0} & 0 & 0 & 0 & 0 & \alpha^{89} & 0 & 0 & 0 & 0 & 0 & \alpha^{81} & 0 & 0 & \alpha^{9} & 0 \\
0 & \alpha^{8} & 0 & 0 & 0 & 0 & \alpha^{0} & 0 & \alpha^{182} & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{173} \\
0 & 0 & \alpha^{173} & 0 & 0 & 0 & 0 & \alpha^{8} & 0 & \alpha^{0} & 0 & 0 & \alpha^{183} & 0 & 0 & 0 \\
0 & 0 & 0 & \alpha^{8} & \alpha^{0} & 0 & 0 & 0 & 0 & 0 & \alpha^{88} & 0 & 0 & \alpha^{80} & 0 & 0 \\
\alpha^{183} & 0 & 0 & 0 & \alpha^{173} & 0 & 0 & 0 & \alpha^{8} & 0 & 0 & 0 & \alpha^{0} & 0 & 0 & 0 \\
0 & \alpha^{0} & 0 & 0 & 0 & \alpha^{88} & 0 & 0 & 0 & \alpha^{80} & 0 & 0 & 0 & \alpha^{8} & 0 & 0 \\
0 & 0 & \alpha^{0} & 0 & 0 & 0 & \alpha^{167} & 0 & 0 & 0 & \alpha^{127} & 0 & 0 & 0 & \alpha^{40} & 0 \\
0 & 0 & 0 & \alpha^{0} & 0 & 0 & 0 & \alpha^{182} & 0 & 0 & 0 & \alpha^{173} & 0 & 0 & 0 & \alpha^{8}
\end{bmatrix}$$

Performance of U-NBPB codes over GF(256)



Performance of U-NBPB codes over GF(16) compared with U-NBPB codes over GF(256)



Conclusions

Conclusions

- We constructed *graph cover non-binary protograph LDPC codes*. We simply call it Constrained NBPB codes (C-NBPB).
- We also constructed non-binary protograph LDPC codes. We simply call it Unconstrained NBPB codes (U-NBPB).
- We designed these codes both for GF(256) and GF(16).
- Performance of binary image of proposed rate 1/2 non-binary protograph codes simulated for three information block sizes k=64, 128, and 256 bits over BIAWGN channel.
- Graph cover non-binary protograph (C-NBPB) codes have lower complexity for implementation. However in expense of slightly more complexity the U-NBPB codes have more degree of freedom. Thus slightly better codes at low error rates can be obtained.

Future Work

- We will concentrate on non-binary (U-NBPB) codes over GF(16) for low complexity and good performance.