

## Motivation

Future communication standards ask for both, high reliability and low delay. While low delay asks for short buffers and therefore short codes, reliable codes improve in block length. We want to present non-binary LDPC codes [1, 2] as an example of good mid range codes.

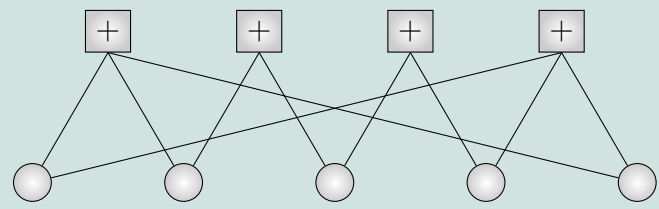
## Binary LDPC Codes [3]

- any parity check matrix  $H$  can be decomposed into a Tanner graph[4] with check- and variable nodes. Check nodes correspond to rows and variable nodes correspond to columns. A 1 indicates a edge between check and variable node.
- variable nodes  $\circ$ : soft decoding of a repetition code.
- check nodes  $\oplus$ : soft decoding of a single parity check code.

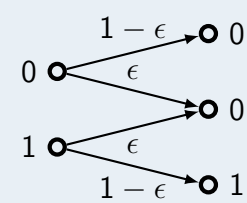
### LDPC

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

corresponds to

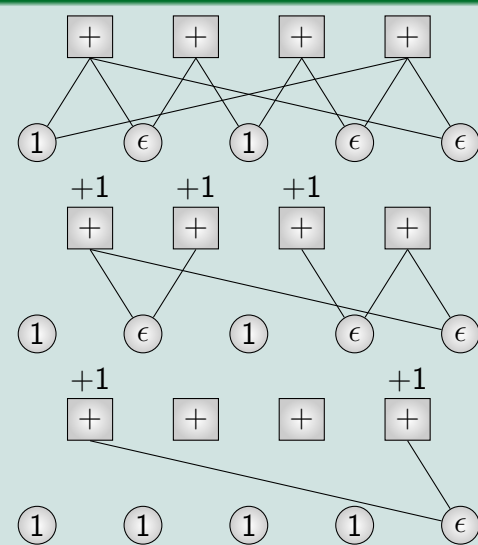


## Belief Propagation Decoding for Erasure Channels



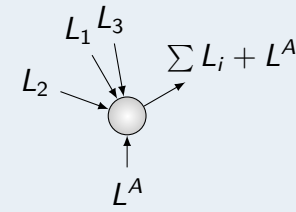
- either a symbol is erased or transmitted correctly.

### Decoding Example

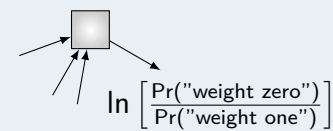


## Belief Propagation Decoding for biAWGN Channels

- information is passed via log likelihood ratios, i.e.  $L_j = \ln \left[ \frac{\Pr(y_j|0)}{\Pr(y_j|1)} \right]$   $L^A = \ln \left[ \frac{\Pr(C_j=0)}{\Pr(C_j=1)} \right]$ .
- variable node iteration:



- check node iteration:



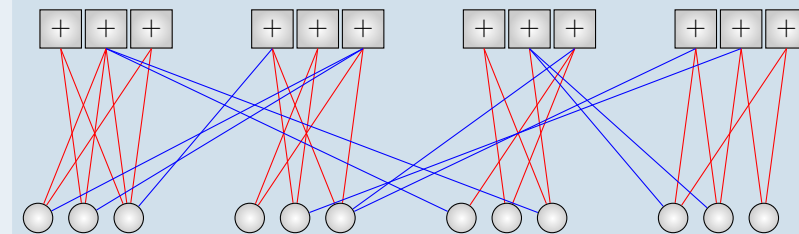
## From Binary to Non-Binary

- girth is the length of the smallest loop in the Tanner graph.
- a small girth leads to bad LDPC codes because belief propagation gets biased.

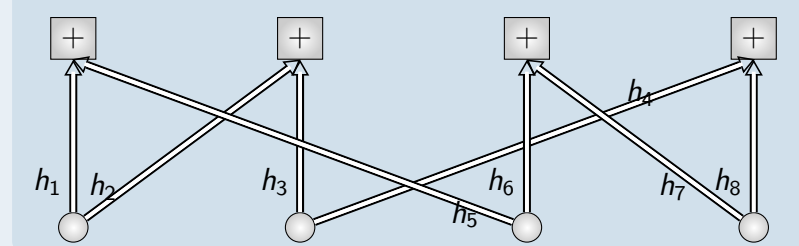
### Intuition for non-binary codes

- create bundles of p binary nodes by a non-binary node.
- replace edges belonging to the same bundles by one edge with weight  $h_i \in GF(2^p)$ .

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

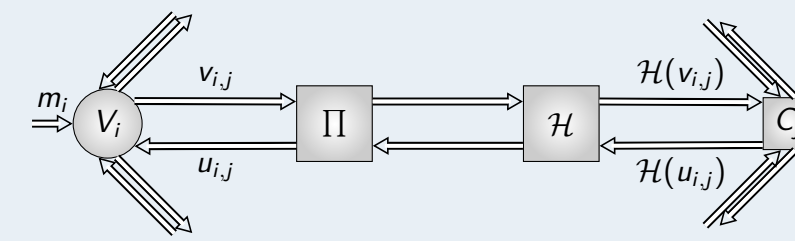


$$H = \begin{bmatrix} h_1 & 0 & h_5 & 0 \\ h_2 & h_3 & 1 & 0 \\ 0 & 0 & h_6 & h_8 \\ 0 & h_4 & 0 & h_8 \end{bmatrix}$$



- improved girth compared to the original graph.

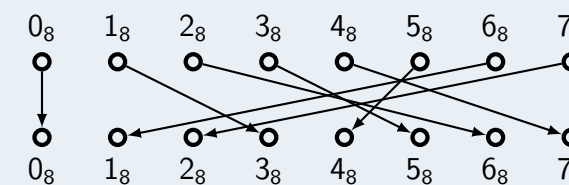
## Belief Propagation Decoding of Non-Binary LDPC Codes [5]



- messages passed on the graph are vectors of length  $GF(2^p)$ , representing on the left side of the Hadamard transform the likelihood of the corresponding element in  $GF(2^p)$ .
- processing at variable node and check node can be done in probability domain.
- variable node: find the probability all incoming edges being equal to  $c_i \in GF(2^p)$ .
- multiply all incoming edges element wise except the one sending to.

$$v_{i,j} = m_i \prod_{k \neq j} (v_{i,k})$$

- multiplication of the edge with  $h_i$  corresponds to a permutation of the entries.



- check node operation: sum probability of all sequences with  $c_i \in GF(2^p)$  that fulfill equation

$$\sum_i h_i c_i = 0$$

- can be expressed as a convolution of probability vectors in  $GF(2^p)$ .

$$u_{i,j} = u_{1,j} * \dots * u_{i-1,j} * u_{i+1,j} * \dots$$

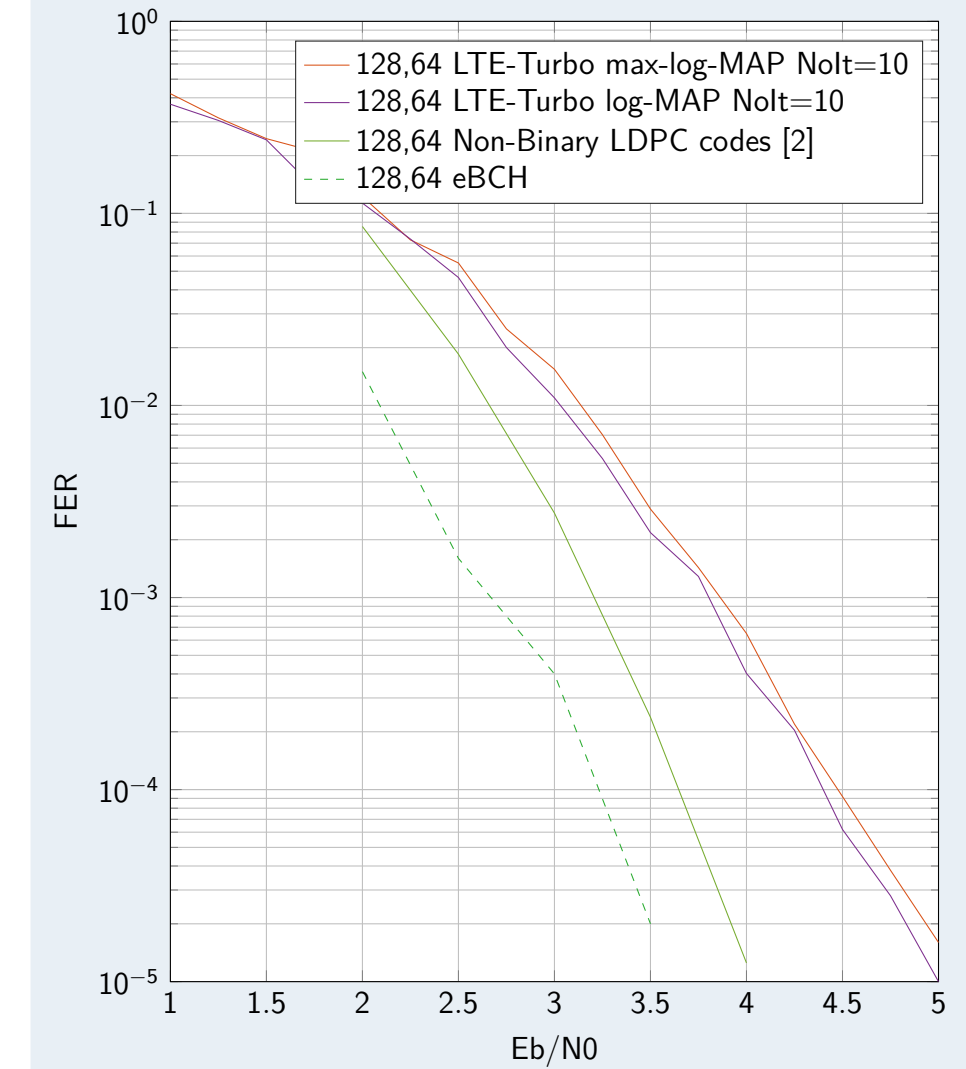
- using Hadamard transform twice we can replace the convolution by an element-wise product over all but one incoming messages

$$u_{i,j} = \mathcal{H} \left( \prod_{k \neq i} \mathcal{H}(u_{k,j}) \right)$$

### Computational complexity

decoding complexity scales with field size  $q$   $\mathcal{O}(q \log(q))$

## Simulation Results



## Acknowledgement

I want to thank Yuan Peihong for providing the reference curves.

## References

- M. C. Davey and D. J. C. MacKay, "Low density parity check codes over  $gf(q)$ ," in *Information Theory Workshop, 1998*, Jun 1998, pp. 70-71.
- B.-Y. Chang, D. Divsalar, and L. Dolecek, "Non-binary protograph-based ldpc codes for short block-lengths," in *Information Theory Workshop (ITW), 2012 IEEE*, Sept 2012, pp. 282-286.
- R. G. Gallager, "Low density parity check codes," Ph.D. dissertation, Massachusetts Institute of Technology, 1960.
- R. M. Tanner, "A recursive approach to low complexity codes," *Information Theory, IEEE Transactions on*, vol. 27, no. 5, pp. 533-547, 1981.
- L. Costantini, B. Matuz, G. Liva, E. Paolini, and M. Chiani, "Non-binary protograph low-density parity-check codes for space communications," *International Journal of Satellite Communications and Networking*, vol. 30, no. 2, pp. 43-51, 2012.