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 medium range codes.

Binary LDPC Codes [3]

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

LDPC

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

Belief Propagation Decoding for biAWGN Channels

- information is passed via log likelihood ratios, i.e.
  - $L_i = \ln \frac{\Pr(x_i=1|y)}{\Pr(x_i=0|y)}$
  - variable node iteration:
    $$L_i = \sum_{c \in \text{check node}} \L(c)$$
  - check node iteration:
    $$\L(c) = \sum_{i \in \text{variable node}} L_i$$

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

- messages passed on the graph are vectors of length $\mathbb{G}F(2^m)$, representing on the left side of the Hadamard transform the likelihood of the corresponding element in $\mathbb{G}F(2^m)$.
- processing at variable node and check node can be done in probability domain.
- variable node: find the probability all incoming edges being equal to $c_i \in \mathbb{G}F(2^m)$.
- multiply all incoming edges element wise except the one sending to $v_i$. 
  $$w_i = m \prod \L(c_{ij})$$
- multiplication of the edge with $h_i$ corresponds to a permutation of the entries.
- check node operation: sum probability of all sequences with $c_i \in \mathbb{G}F(2^m)$ that fulfill equation
  $$\sum_i h_i c_i = 0$$
- can be expressed as a convolution of probability vectors in $\mathbb{G}F(2^m)$.
  $$w_j = \sum_i \L_{ij} \cdot \L(c_{ij})$$
- using Hadamard transform twice we can replace the convolution by an element-wise product over all but one incoming messages
  $$w_j = H \left( \prod \L(c_{ij}) \right)$$

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 $h_i \in \mathbb{G}F(2^p)$.

Computational complexity

- decoding complexity scales with field size $q$ $O(q \log(q))$