Decoding and Performance of Nonbinary LDPC codes

Discussion and Perspectives

David Declercq
ETIS ENSEA/UCP/CNRS UMR 8051

NewCom SWP1 meeting - 28th April 2005
**Ususal Definition**

\[ C_H = \left\{ \mathbf{c} \in GF(q)^{N} : H\mathbf{c} \equiv 0 \pmod{GF(q)} \right\} \quad C_G = \left\{ \mathbf{c} = G\mathbf{u}, \forall \mathbf{u} \in GF(q)^{K} \right\} \]

\( H(M \times N) \) : parity check matrix with entries from \( GF(q) \),
\( G(N \times K) \) : codeword generating matrix obtained from \( H \) by Gauss elimination on \( GF(q) \).

Length \[
\begin{align*}
&\text{of the codeword} & N \\
&\text{of the information symbols} & K \\
&\text{of the redundant symbols} & M
\end{align*}
\]

Density of \( H \) :
\[
d_H = \frac{\text{nb. nonzeros elements in } H}{MN}
\]

**LDPC**
\[ d_H \xrightarrow{N \to +\infty} 0 \]

NewCom SWP1 meeting - 28th April 2005
NonBinary LDPC codes decoded under iterative Belief Propagation are good candidates for:

1. medium code lengths \((500 \leq N \leq 3000\) coded bits),
2. high spectral efficiency communications \((M\text{-QAM with } M \geq 16)\),

As for now, I will consider only:

- regular \((d_v, d_c)\) nonbinary LDPC codes,
- AWGN channels either with BPSK inputs or M-QAM inputs.
Factor Graph of a regular 
\((d_v, d_c) = (2, 4)\) code in \(GF(8)\).

\[
H = \begin{pmatrix}
3 & 0 & 7 & 1 & 0 & 0 & 0 & 2 \\
4 & 3 & 0 & 5 & 0 & 0 & 1 & 0 \\
0 & 0 & 5 & 0 & 3 & 6 & 0 & 7 \\
0 & 6 & 0 & 0 & 1 & 2 & 1 & 0
\end{pmatrix}
\]
**Why choosing** $d_v = 2$?

**Consequence**: non-binary LDPC codes should be ultra-sparse [McKay’98]

- if $q \leq 32$, it is possible to consider irregularity in the graph,
- if $q \geq 64$, almost none irregularity can be considered and $d_v = 2$. 

NewCom SWP1 meeting - 28th April 2005
BP decoding of LDPC codes over $GF(q)$

[ITW03] L. Barnault and D. Declercq, Fast Decoding Algorithm for LDPC over $GF(2^q)$

**1st step**
Data pass (term by term product):

$$U_{tp} = L \times \prod_{v=1, v\neq t}^{d_v} V_{pv} \quad t = 1 \ldots d_v$$

**2nd step**
Permutation step (nonzeros values in $H$):

$$U_{pc} = P_{h(x)} U_v \quad t = 1 \ldots d_v$$

where $P_{h(x)}$ is a $q \times q$ permutation matrix corresponding to $h(x) \in GF(q)$

**3rd step**
Check Pass with $\mathcal{F}(.)$ the Fourier transform in $GF(q)$:

$$V_{tp} = \mathcal{F} \left( \prod_{c=1, c\neq t}^{d_c} \mathcal{F}(U_{pc}) \right) \quad t = 1 \ldots d_c$$

NewCom SWP1 meeting - 28th April 2005
**Simplification of BP decoding, the LogEMS algo.**

[IEEE Trans. Com. 05] D. Declercq and M.P. Fossorier *Decoding Algorithms for LDPC codes over GF(q)*, submitted


**Goal**: decode nonbinary LDPC codes with “reasonable” complexity compared to existing competing codes (Turbo-Codes, binary LDPC codes, RS codes, etc).

**Solution**: by replacing the check node update with a generalization of the Min-Sum algorithm in $GF(2)$: LogEMS = “Extended Min-Sum algorithm in the log. domain”.

<table>
<thead>
<tr>
<th></th>
<th>BP</th>
<th>BP/FFT</th>
<th>LogEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity per Check Node:</td>
<td>$\mathcal{O}(d_c q^2)$</td>
<td>$\mathcal{O}(d_c q \log_2(q))$</td>
<td>$\mathcal{O}(d_c n_m^2)$</td>
</tr>
</tbody>
</table>

with $n_m << q$ (for example $n_m = 13$ for $q = 256$).
Performance of LDPC codes for
N = 848 bits (ATM size)

(2, 4) code over GF(256)

(2, 8) code over GF(128)
NonBinary LDPC codes for high order QAM signals

[ISITA 04] D. Declercq, M. Colas and G. Gelle, Regular $GF(2^q)$-LDPC coded Modulations for higher order QAM-AWGN Channels

- if the channel is memoryless and $Q > M \Rightarrow$ no loss of performance due to the demapping.
Performance results on QAM-AWGN channels

$GF(256)$ $(2, 4)$ codes on 16-QAM and 256-QAM, Gray labelling

16-QAM

256-QAM

Performance of regular $(2, x)$−$GF(256)$ LDPC codes at BER=$10^{-5}$

NewCom SWP1 meeting - 28th April 2005
Key Issues in Nonbinary LDPC Codes - Open to Discussion Tomorrow

- Under BP decoding, the class of powerful nonbinary LDPC codes is rather small ($d_v = 2$, concentrated checks).
  - change the decoder (but obviously more complex),
  - focus on the careful design of the parity matrix ($H$ with long cycles, choice of the matrix values, etc).

- For M-QAM constellations, take advantage of the properties that if $q \geq M$:
  - the LDPC decoder is insensitive to the labelling choice,
  - the messages at the decoder input are independent (no loss of information between demapper and decoder).
  - maybe allow some change at the constellation/mapping level?

- Finally, when $q$ is relatively small $q \leq 32$, optimize the code irregularity by means of Density Evolution.