Design and Analysis of Nonbinary LDPC Codes for Bandwidth-Efficient Wireless Communication

Amir Bennatan, Princeton University, David Burshtein, Tel Aviv University
Outline

• Background, definitions

• Analysis, maximum-likelihood

• Analysis, belief propagation
  – EXIT charts

• Simulation results
Background
Binary LDPC Codes

Exciting classic results: (Richardson et al., Chung et al., Luby et al.):

- BIAWGN, Rate = 0.5, Threshold 0.0045 dB of Shannon limit.
- BIAWGN, Rate = 0.88, Threshold 0.088 dB of Shannon limit.
- BSC, Rate = 0.5, Threshold 0.005 of maximum crossover.
- BEC, any rate: achieve capacity!
Exciting classic results: (Richardson et al., Chung et al., Luby et al.):

- BIAWGN, Rate = 0.5, Threshold 0.0045 dB of Shannon limit.
- BIAWGN, Rate = 0.88, Threshold 0.088 dB of Shannon limit.
- BSC, Rate = 0.5, Threshold 0.005 of maximum crossover.
- BEC, any rate: achieve capacity!

but... all channels are:

- Binary-input
- Symmetric-output
Other important scenarios:

- **Bandwidth efficient (high SNR) channels**
- MIMO channels
- Dirty paper
Constructing Non-Binary Codes

- One approach: **multilevel coding** and **BICM**.
  - Construct non-binary codes from binary ones.
Constructing Non-Binary Codes

- One approach: multilevel coding and BICM.
  - Construct non-binary codes from binary ones.

Our focus: non-binary LDPC codes.
Warning!

- Discussion now is not rigorous.

- Rigorous details available,
  

Nonbinary LDPC Codes
Nonbinary Alphabet: LDPC over Modulo-$q$ Ring

- Gallager, 1963

$x \in \{0, ..., q - 1\}^N$ is codeword if at each check node $j$,

$$\sum_{i \in N(j)} x_i = 0 \pmod{q}$$
Coset Codes


• Given code $C$ and vector $v \in \{0, \ldots, q - 1\}^N$

\[ C + v \triangleq \{ c + v : c \in C \} \]
Coset Codes


• Given code $C$ and vector $v \in \{0, \ldots, q - 1\}^N$

$$C + v \triangleq \{c + v : c \in C\}$$

In ensemble analysis, $v$ selected randomly.
Option 1: PAM

• Signals equally spaced
Mapping to Channel alphabet

Option 1: PAM

- Signals equally spaced

Alternative: Achieve **shaping gain** up to **1.53 dB**

1. “Quantization” mapping
2. Nonuniform-spaced mapping
Modulo-$q$ LDPC
Maximum-Likelihood (ML)
Analysis
Why Maximum-Likelihood (ML) Analysis?

😊 ML not practical. Belief-propagation practical.

😊 Easy to obtain analytic results. With binary LDPC:
  – Belief propagation: Examples *pretty close* to capacity.
  – ML: Analytic proof we can get *arbitrarily close* to capacity.

😊 Bounds performance of belief-propagation:

*Is there hope to achieve capacity?*
Nonbinary Codes

Existing results, nonbinary LDPC

- Gallager, 1963: Symmetric channels

- Erez, Miller, 2003 (parallel work): Modulo-lattice channels
  - Modulo-lattice channels are symmetric
  - Component of scheme to achieve capacity of more channels
Existing results, nonbinary LDPC

- **Gallager, 1963**: Symmetric channels

- **Erez, Miller, 2003** (parallel work): Modulo-lattice channels
  - Modulo-lattice channels are symmetric
  - Component of scheme to achieve capacity of more channels

**Our result**: Coset Modulo-$q$-LDPC achieve capacity of any discrete-memoryless channel.
Background: LDPC (5,10) vs. Random coding
Modulo-$q$-LDPC $(3, 6)$ vs. Random Coding, $q=3$
Mapping to Channel alphabet

Option 1: PAM

- Signals equally spaced

Alternative: Achieve shaping gain

1. “Quantization” mapping
2. Nonuniform-spaced mapping
Mapping to Channel Alphabet

Approximating desired distribution (Gallager 1968, McEliece 2001)

\[
\begin{align*}
0 & \rightarrow a & p = \frac{3}{8} \\
1 & \rightarrow a & p = \frac{3}{8} \\
2 & \rightarrow b & p = \frac{3}{8} \\
3 & \rightarrow b & p = \frac{3}{8} \\
4 & \rightarrow b & p = \frac{3}{8} \\
5 & \rightarrow c & p = \frac{1}{4} \\
6 & \rightarrow c & p = \frac{1}{4} \\
7 & \rightarrow c & p = \frac{1}{4}
\end{align*}
\]
Quantization mapping

- Given $Q(a)$, target probability assignment

- **Quantization** $\delta(\cdot)$ is mapping

  $$\{0, \ldots, q - 1\} \rightarrow \mathcal{A}$$

  no. symbols mapped to $a \in \mathcal{A}$ is $q \cdot Q(a)$. 
ML Analysis, Nonbinary Codes

Theorem

Assume arbitrary discrete memoryless channel, MQC ensemble, quantization tailored to $Q(\cdot)$.

Then:

$$\overline{P_e} \leq q^{-NEQ(R+(\log \alpha)/N)} + \sum_{t \in U} \overline{S_t}D^t$$

$$\alpha = \max_{t \in U^c} \frac{\overline{S_t}}{(M-1) \binom{N}{t_0,...,t_{q-1}} q^{-N}}$$
Theorem

\((c, d)\)-regular modulo-\(q\) LDPC code

\[
\lim_{N \to \infty} \frac{1}{N} \log S_{\theta N} = (1 - c) H(\theta) + (1 - R) \log \inf_{\text{sgn}(x) = \text{sgn}(\theta)} \frac{A(x)}{x^d \theta}
\]

\[
A(x) = \frac{1}{q} \sum_{l=0}^{q-1} \left( \sum_{i=0}^{q-1} x_i e^{j \frac{2\pi li}{q}} \right)^d
\]
Theorem

Assume
$q$ prime, rate $R > 0$ rational number, $\epsilon_1, \epsilon_2 > 0$ arbitrary, $c, d$ and $N$ large enough, ensemble expurgated, appropriate quantization $Q(\cdot)$

Then:
The $(c, d)$-regular coset modulo-$q$ LDPC ensemble of length $N$ and rate $R$,

$$
\overline{P_e} \leq q^{-NE_Q(R+\epsilon_1)} + \sum_{k=1}^{q-1} D_k^{(1-\epsilon_2)N}
$$
Theorem

Assume
$q$ prime, rate $R > 0$ rational number, $\epsilon_1, \epsilon_2 > 0$ arbitrary, $c, d$ and $N$ large enough, ensemble expurgated, appropriate quantization $Q(\cdot)$

Then:
The $(c, d)$-regular coset modulo-$q$ LDPC ensemble of length $N$ and rate $R$,  

\[
\overline{P_e} \leq q^{-NE Q(R+\epsilon_1)} + \sum_{k=1}^{q-1} D_k^{(1-\epsilon_2)N}
\]

Result: We can approach capacity arbitrarily close!
Belief Propagation
Decoding
Belief-Propagation Decoding

Nodes exchange messages

Message \( \mathbf{x} = (x_0, \ldots, x_{q-1}) \)

- \( x_i \) = estimate of probability, transmitted symbol was \( i \)
- \( \sum x_i = 1 \) (so \( x_0 \) not really needed).
Modulo-\(q\) LDPC Belief-Propagation Decoder

- **Rightbound iteration:** To compute LLR \(r\)

  \[
  r = r^{(0)} + \sum_{n=1}^{d_i-1} l^{(n)}
  \]

- **Leftbound iteration:** For plain likelihood \(l = (l_0, \ldots, l_{q-1})\),

  \[
  l_k = \sum_{a_1, \ldots, a_{d-1} \in \{0, \ldots, q-1\}} \prod_{n=1}^{d-1} r_{a_n}^{(n)}
  \] where

  \[
  a_1, \ldots, a_{d-1} \in \{0, \ldots, q-1\}, \quad \sum a_n = -k \pmod q \quad n=1
  \]
Background: Binary Density evolution

(Richardson and Urbanke)

- $q = 2 \Rightarrow$ messages are scalar.

- Analysis tracks densities of “typical message” $X$
  - Channel transitions
  - Tanner graph realizations

- Evolved recursively from one iteration to another.
Background: EXIT Charts for Binary LDPC
(ten Brink, Kramer, Ashikhmin, 2004)

- Message distribution $X$ approximately\(^1\) **Gaussian** (Chung *et al.*).

\[
X \sim \mathcal{N}(m, \sigma^2)
\]

\(^1\)Under all-zero codeword and independence assumptions
Background: EXIT Charts for Binary LDPC
(ten Brink, Kramer, Ashikhmin, 2004)

• Message distribution $X$ approximately\(^1\) **Gaussian** (Chung *et al.*).

\[
X \sim \mathcal{N}(m, \sigma^2)
\]

• Over binary-input symmetric-output channel: $X$ **symmetric** (Richardson *et al.* 2001), and $m = \sigma^2/2 \Rightarrow$

\[
X \sim \mathcal{N}\left(\frac{\sigma^2}{2}, \sigma^2\right)
\]

\(^1\)Under all-zero codeword and independence assumptions
Background: EXIT Charts for Binary LDPC

(ten Brink, Kramer, Ashikhmin, 2004)

• Message distribution $X$ approximately\(^1\) **Gaussian** (Chung *et al.*).

$$X \sim \mathcal{N}(m, \sigma^2)$$

• Over binary-input symmetric-output channel: $X$ **symmetric** (Richardson *et al.* 2001), and $m = \sigma^2/2 \Rightarrow$

$$X \sim \mathcal{N}\left(\frac{\sigma^2}{2}, \sigma^2\right)$$

\(X\) characterized by **scalar** $\sigma > 0$.

---

\(^1\)Under all-zero codeword and independence assumptions
With Nonbinary LDPC

- Messages $X$, **multidimensional** vectors.
With Nonbinary LDPC

- Messages \( \mathbf{X} \), **multidimensional** vectors.

- Multimensional Gaussian \( \mathbf{X} \sim \mathcal{N}(\mathbf{m}, \Sigma) \),

\[
\mathbf{m} = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \end{bmatrix} \quad \Sigma = \begin{bmatrix} \cdots & \cdots \\ \vdots & \Sigma_{i,j} & \cdots \\ \cdots & \cdots \end{bmatrix}
\]
With Nonbinary LDPC

- Messages $X$, **multidimensional** vectors.

- Multimensional Gaussian $X \sim \mathcal{N}(m, \Sigma)$,

  $$m = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \end{bmatrix}, \quad \Sigma = \begin{bmatrix} \cdots & \cdots \\ \cdots & \Sigma_{i,j} & \cdots \\ \cdots & \cdots \end{bmatrix}$$

- Li *et al.*, 2003: $X$ characterized by $q-1$ parameters: ... not good enough for EXIT charts.
With Nonbinary LDPC

- Messages $X$, **multidimensional** vectors.

- Multimimensional Gaussian $X \sim \mathcal{N}(m, \Sigma)$,

  \[
  m = \begin{bmatrix}
  m_1 \\
  m_2 \\
  \vdots
  \end{bmatrix}
  \quad \Sigma = \begin{bmatrix}
  \ldots & \ldots & \ldots \\
  \ldots & \Sigma_{i,j} & \ldots \\
  \ldots & \ldots & \ldots
  \end{bmatrix}
  \]

- Li *et al.*, 2003: $X$ characterized by $q-1$ parameters: 
  ... not good enough for EXIT charts.

**Our result**: $X$ characterized by **one** scalar parameter.
Random Coset Analysis

- Given code $C$, 
  \[ C + v \triangleq \{ c + v : c \in C \} \]
- $v$ randomly selected in $\{0, ..., q - 1\}^N$
Applications of Random-coset Analysis

• All-zero codeword assumption
  – Equivalent to “all-ones” codeword, with binary BPSK signaling.
  – Required for validity of Gaussian approximation, symmetry

• Symmetry
  – Generalization of binary symmetry by Richardson et al., 2001.
  – Messages of decoder satisfy,\(^1\)
    \[
    \Pr[w] = e^{w_i} \Pr[w^+i]
    \]
  – Notice that if \(q = 2\),
    \[
    \Pr[w] = e^w \Pr[-w]
    \]

---

\(^1\)Under the all-zero codeword and independence assumptions.
Nonbinary LDPC over $\text{GF}(q)$

(Davey and MacKay, 1998)

- At each edge $(i, j)$, a label $g_{i,j} \in \text{GF}(q) \setminus \{0\}$

- $x \in \{\text{GF}(q)\}^N$ is codeword if at each check node,

$$\sum_{i \in \mathcal{N}(j)} x_i = 0 \quad \sum_{i \in \mathcal{N}(j)} g_{i,j} \cdot x_i = 0$$
In ensemble analysis, labels selected randomly from $GF(q) \backslash \{0\}$. 
A closer look at leftbound messages

Previous expression, \( l = (l_0, \ldots, l_{q-1}) \)

\[
l_k = \sum_{a_1, \ldots, a_{d-1} \in \{0, \ldots, q-1\}, \sum a_n = -k \pmod{q}} \prod_{n=1}^{d-1} r_{a_n}^{(n)}
\]

New expression,

\[
l_k = \sum_{a_1, \ldots, a_{d-1} \in \text{GF}(q), \sum g_n a_n = -g_d \cdot k} \prod_{n=1}^{d-1} r_{a_n}^{(n)}
\]

Equivalent expression,

\[
l = \left[\prod_{n=1}^{d-1} \left( r^{(n)} \right)^{g_n^{-1}} \right] \times (-g_d)
\]
Equivalent expression:

\[ l = \left[ \bigodot_{n=1}^{d-1} \left( r^{(n)} \right)^{g_n^{-1}} \right] \times (-g_d) \]

where,

\[
\begin{bmatrix}
    x^{(1)} \odot x^{(2)}
\end{bmatrix}_k \triangleq \sum_{a \in \text{GF}(q)} x^{(1)}_a \cdot x^{(2)}_{k-a}
\]

\[ w^\times i \triangleq (w_{1.i}, \ldots, w_{(q-1).i}) \]
Equivalent expression:

\[
1 = \left[ \prod_{n=1}^{d-1} \left( r^{(n)} \right)^{x_n^{-1}} \right] \times (-g_d)
\]

Let \( h \in \text{GF}(q) \backslash \{0\} \) be fixed non-random, and consider \( 1 \times h \),

\[
1 \times h = \left[ \prod_{n=1}^{d-1} \left( r^{(n)} \right)^{x_n^{-1}} \right] \times (-g_d \cdot h)
\]

1 and \( 1 \times h \) are identically distributed!
Definition:

Random variable $\mathbf{W}$ is permutation-invariant if for any fixed $h \in \text{GF}(q) \setminus \{0\}$, $\tilde{\mathbf{W}} \overset{\Delta}{=} \mathbf{W} \times h$ is distributed identically with $\mathbf{W}$. 
Gaussian Approximation

**Theorem**
Let \( \mathbf{W} \) be **Gaussian distributed**, \( \mathbf{W} \sim \mathcal{N}(\mathbf{m}, \Sigma) \). Assume the p.d.f \( f(\mathbf{w}) \) exists and \( \Sigma \) is nonsingular.

Then \( \mathbf{W} \) is both **symmetric** and **permutation-invariant** if and only if there exists \( \sigma > 0 \) such that,

\[
\mathbf{m} = \begin{bmatrix}
\frac{\sigma^2}{2} \\
\frac{\sigma^2}{2} \\
\vdots \\
\frac{\sigma^2}{2}
\end{bmatrix}
\quad
\Sigma = \begin{bmatrix}
\sigma^2 & \sigma^2 / 2 \\
\sigma^2 / 2 & \sigma^2 \\
\vdots & \vdots \\
\sigma^2 / 2 & \sigma^2
\end{bmatrix}
\]
Gaussian Approximation

**Theorem**
Let $W$ be Gaussian distributed, $W \sim \mathcal{N}(m, \Sigma)$. Assume the p.d.f $f(w)$ exists and $\Sigma$ is nonsingular.

Then $W$ is both symmetric and permutation-invariant if and only if there exists $\sigma > 0$ such that,

$$m = \begin{bmatrix} \sigma^2/2 \\ \sigma^2/2 \\ \vdots \\ \sigma^2/2 \end{bmatrix} \quad \Sigma = \begin{bmatrix} \sigma^2 & \sigma^2/2 \\ \sigma^2 & \sigma^2 \\ & \ddots \sigma^2/2 \\ \sigma^2/2 & & \sigma^2 \end{bmatrix}$$

**Result:** $W$ characterized by single scalar $\sigma$!
Technical Details

Gaussian Approximation

- Rightbound messages modelled as sum of Gaussian and fixed random variables.

Further details

- Leftbound messages modelled as Gaussian
- Mutual information $I(C; X)$ used instead of parameter $\sigma$.
  Base of $\log$ is $q$, so $0 \leq I(C; X) \leq 1$. 
Belief-Propagation Decoding

Vector messages:

- **Plain likelihood** representation: \( \mathbf{x} = (x_0, \ldots, x_{q-1}) \)

- **LLR** representation: \( q-1 \) dimensional

\[
\mathbf{w} = \left( \log \frac{x_1}{x_0}, \log \frac{x_2}{x_0}, \ldots, \log \frac{x_{q-1}}{x_0} \right)
\]

\((w_0 = \log \frac{x_0}{x_0} \text{ always 0, hence not needed})\)
Stability Condition - Binary LDPC

**Theorem** (Richardson et al., 2001, Khandekar, 2002)
Assume BI-SO channel, binary LDPC, $\lambda(\cdot)$ and $\rho(\cdot)$.

$$\Delta \triangleq \sum_y \sqrt{P(y|0)P(y|1)}$$

1. If $\lambda'(0)\rho'(1) > 1/\Delta$ then exists $\xi > 0$ such that $P_e^i > \xi$ for all iterations $i$.

2. If $\lambda'(0)\rho'(1) < 1/\Delta$ then exists $\xi > 0$ such that if $P_e^i < \xi$ at some $i$, then $P_e^i \to 0$ as $i \to \infty$. 
Stability Condition - Non-Binary LDPC

Theorem
Assume arbitrary discrete-memoryless channel, coset GF($q$) LDPC, $\lambda(\cdot)$ and $\rho(\cdot)$.

$$\Delta \triangleq \frac{1}{q(q - 1)} \sum_{i,j \in \text{GF}(q), i \neq j} \sum y \sqrt{\Pr[y|\delta(i)] \Pr[y|\delta(j)]}$$

1. If $\lambda'(0)\rho'(1) > 1/\Delta$ then exists $\xi > 0$ such that $P_e^i > \xi$ for all iterations $i$.

2. If $\lambda'(0)\rho'(1) < 1/\Delta$ then exists $\xi > 0$ such that if $P_e^i < \xi$ at some $i$, then $P_e^i \to 0$ as $i \to \infty$. 
Simulation Results
Efficient Implementation

- Richardson *et al.*, 2001: using **multidimensional DFT**.
  - Fast implementation: see e.g. Dugeon and Mersereau.

- Davey and Mackay, 1998

Free code: [www.eng.tau.ac.il/~burstyn](http://www.eng.tau.ac.il/~burstyn)
EXIT chart for a coset GF(32) LDPC code at spectral efficiency 6 bits/s/Hz, at SNR 18.5 dB.
Simulations at 6 bits/s/Hz (3 bits/dimension)

- Unrestricted Shannon limit: 17.99 dB
- Threshold: 18.55 dB
- 32-PAM limit: 19.11 dB
Simulations at 6 bits/s/Hz (3 bits/dimension)

Unrestricted Shannon limit = Not restricted to any signal constellation.
Simulations at 6 bits/s/Hz (3 bits/dimension)

Unrestricted
Shannon limit

Threshold

32-PAM
limit

17.99 dB
18.55 dB
19.11 dB

Shaping gap

- Well within shaping gap
Mapping to Channel alphabet

Option 1: PAM

- Signals equally spaced

Alternative: Achieve shaping gain up to 1.53 dB

1. “Quantization” mapping
2. Nonuniform-spaced mapping
Simulations at 6 bits/s/Hz (3 bits/dimension)

PAM (not used)

• Signals equally spaced

Nonuniform spaced constellation

• (Sun and van Tilborg, 1993, Fragouli et al. 2001)
• 0.86 dB gain “for free”
Simulations at 6 bits/s/Hz (3 bits/dimension)

- Limit for constellations in use:
  - Unrestricted Shannon limit
  - Threshold
  - 32–PAM limit

- Values:
  - Shannon limit: 17.99 dB
  - Threshold: 18.25 dB
  - 32–PAM limit:
    - Gap: 0.3 dB
    - Final: 19.11 dB

- Gap 0.3 dB

- Indicates effectiveness of EXIT charts.
**Comparison, Multilevel at Short Block Lengths**

LDPC with Multilevel Coding: (Hou et al., 2003)

<table>
<thead>
<tr>
<th></th>
<th>LDPC + multilevel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block length</td>
<td>10,000 symbols</td>
</tr>
<tr>
<td>Spectral efficiency</td>
<td>2 bits/s/Hz</td>
</tr>
<tr>
<td>Constellation</td>
<td>4-PAM</td>
</tr>
<tr>
<td>BER</td>
<td>$\sim 10^{-4}$</td>
</tr>
<tr>
<td>SNR</td>
<td>1 dB</td>
</tr>
<tr>
<td>(above 4-PAM Shannon limit)</td>
<td></td>
</tr>
</tbody>
</table>
## Comparison, Multilevel at Short Block Lengths

LDPC with Multilevel Coding: (Hou *et al.*, 2003)

<table>
<thead>
<tr>
<th></th>
<th>LDPC + multilevel</th>
<th>Coset GF(4) LDPC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Block length</strong></td>
<td>10,000 symbols</td>
<td>same</td>
</tr>
<tr>
<td><strong>Spectral efficiency</strong></td>
<td>2 bits/s/Hz</td>
<td>same</td>
</tr>
<tr>
<td><strong>Constellation</strong></td>
<td>4-PAM</td>
<td><strong>same</strong></td>
</tr>
<tr>
<td><strong>BER</strong></td>
<td>$\sim 10^{-4}$</td>
<td>same</td>
</tr>
<tr>
<td><strong>SNR</strong></td>
<td>1 dB</td>
<td>same</td>
</tr>
<tr>
<td>(above 4-PAM Shannon limit)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Comparison, Multilevel at Short Block Lengths

LDPC with Multilevel Coding: (Hou et al., 2003)

<table>
<thead>
<tr>
<th></th>
<th>LDPC + multilevel</th>
<th>Coset GF(4) LDPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block length</td>
<td>10,000 symbols</td>
<td>same</td>
</tr>
<tr>
<td>Spectral efficiency</td>
<td>2 bits/s/Hz</td>
<td>same</td>
</tr>
<tr>
<td>Constellation</td>
<td>4-PAM</td>
<td>same</td>
</tr>
<tr>
<td>BER</td>
<td>$\sim 10^{-4}$</td>
<td>same</td>
</tr>
<tr>
<td>SNR</td>
<td>1 dB</td>
<td>0.55 dB</td>
</tr>
<tr>
<td>(above 4-PAM Shannon limit)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Comparison, Multilevel at Short Block Lengths

LDPC with Multilevel Coding: (Hou et al., 2003)

<table>
<thead>
<tr>
<th></th>
<th>LDPC + multilevel</th>
<th>Coset GF(4) LDPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block length</td>
<td>10,000 symbols</td>
<td>same</td>
</tr>
<tr>
<td>Spectral efficiency</td>
<td>2 bits/s/Hz</td>
<td>same</td>
</tr>
<tr>
<td>Constellation</td>
<td>4-PAM</td>
<td>same</td>
</tr>
<tr>
<td>BER</td>
<td>$\sim 10^{-4}$</td>
<td>same</td>
</tr>
<tr>
<td>SNR</td>
<td>1 dB</td>
<td>0.55 dB</td>
</tr>
<tr>
<td>(above 4-PAM Shannon limit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decoding complexity</td>
<td>-</td>
<td>greater</td>
</tr>
</tbody>
</table>
## Comparison, Multilevel at Short Block Lengths

LDPC with Multilevel Coding: (Hou et al., 2003)

<table>
<thead>
<tr>
<th></th>
<th>LDPC + multilevel</th>
<th>Coset GF(4) LDPC # 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block length</td>
<td>10,000 symbols</td>
<td>same</td>
</tr>
<tr>
<td>Spectral efficiency</td>
<td>2 bits/s/Hz</td>
<td>same</td>
</tr>
<tr>
<td>Constellation</td>
<td>4-PAM</td>
<td>same</td>
</tr>
<tr>
<td>BER</td>
<td>$\sim 10^{-4}$</td>
<td>same</td>
</tr>
<tr>
<td>SNR</td>
<td>1 dB</td>
<td>0.55 dB 0.8 dB</td>
</tr>
<tr>
<td></td>
<td>(above 4-PAM Shannon limit)</td>
<td></td>
</tr>
<tr>
<td>Decoding complexity</td>
<td>-</td>
<td>greater similar</td>
</tr>
</tbody>
</table>
Summary

- **ML decoding**: Achieve capacity.

- **Belief propagation**: Symmetry, perm. invariance, Gaussian approx., stability

- **EXIT charts**

- **Simulation Results**: 0.56 dB from Shannon limit, outperform multilevel coding.
Backup slides
Nonbinary LDPC over Modulo-$q$ Ring

- **(c,d)-regular** LDPC code:
  - All left (variable) nodes are of degree $c$ e.g. $c = 3$.
  - All right (check) nodes are of degree $d$ e.g. $d = 6$. 

![Diagram of LDPC code]

```latex
\begin{array}{c}
V \\
\vdots \\
\vdots \\
\vdots \\
\vdots \\
V
\end{array}
\quad
\begin{array}{c}
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\bullet \\
C
\end{array}
\quad
\begin{array}{c}
V \\
\vdots \\
\vdots \\
\vdots \\
\vdots \\
V
\end{array}
```
Uniform distribution

- Regular 10-PAM:
Nouniform distribution

- We want:
Nonbinary LDPC over Modulo-\(q\) Ring

- **(c,d)-regular** LDPC code:
  - All left (variable) nodes are of degree \(c\) e.g. \(c = 3\).
  - All right (check) nodes are of degree \(d\) e.g. \(d = 6\).

Analysis: Average performance of codes from \((c, d)-ensemble\)
How Accurate is Gaussian Approximation?

\[ r = r^{(0)} + \sum_{n=1}^{d_i-1} l^{(n)} \]

rightbound message

\[ r^{(0)} \]

initial message

\[ \sum_{n=1}^{d_i-1} l^{(n)} \]

sum of leftbound messages
Nonbinary Codes

• $x$ word over $\{0, \ldots, q - 1\}$,

\[
\text{type}(x) \triangleq \text{vector } t = (t_0, \ldots, t_{q-1}) \text{ where, } t_i = \text{number of } i \text{ digits in } x
\]

Example: $\text{type}([0, 1, 2, 2, 2]) = (1, 1, 3)$.

• $C$ code,

\[
S_t \triangleq \text{number of codewords of type } t
\]

• $\mathcal{C}$ ensemble (set) of nonbinary codes,

\[
\overline{S}_t \triangleq \text{average } S_t \text{ in codes } C \in \mathcal{C}
\]
Rightbound LLR Messages: \( r = r^{(0)} + \sum_{n=1}^{d_i-1} I^{(n)} \)

- Initial message, \( r^{(0)} \)
  - Characterized by channel p.d.f.

- Sum of i.i.d\(^2\) leftbound messages, \( \sum_{n=1}^{d_i-1} I^{(n)} \)
  
  Symmetric, permutation-invariant, approximately Gaussian
  \( \Rightarrow \) characterized by \( \sigma > 0 \).

---

**Given fixed channel, message distributions are characterized by scalar \( \sigma > 0 \).**

---

\(^2\)Under the all-zero codeword and independence assumptions
Leftbound Messages

- Resembles “spike”
- Following experience with binary codes, modelled as Gaussian
**Initial Messages**

**Lemma.** Assume AWGN channel, noise variance \( \sigma_z^2 \) and mapping \( \delta \) to the channel signal alphabet. Assume the all-zero codeword assumption. Then

\[
\mathbf{r}^{(0)} = \mathbf{\alpha}(v) + \mathbf{\beta}(v) \cdot z
\]

where,

- \( z \) is the noise produced by the channel
- \( v \) is the coset symbol
- and \( \mathbf{\alpha}(v) \) and \( \mathbf{\beta}(v) \) are \( q-1 \) dimensional vectors, dependent on \( v \), whose components are given by, \( \alpha(v)_i = \frac{1}{2\sigma_z^2}(\delta(v) - \delta(v + i))^2 \), \( \beta(v)_i = \frac{1}{\sigma_z^2}(\delta(v) - \delta(v + i)) \).
Initial Messages
Technical Details

- Leftbound messages modelled as Gaussian.

- Mutual information $I(C; X)$ used instead of parameter $\sigma$. Base of log is $q$, so $0 \leq I(C; X) \leq 1$.

- Additional details provided in proceedings paper.