Low-Density Parity-Check Codes over the $q$-ary Partial Erasure Channel

Rami Cohen

Department of Electrical Engineering
Technion - Israel Institute of Technology

1 June, 2014

Supervised by Prof. Yuval Cassuto
# Table of Contents

1. **The $q$-ary partial erasure channel (QPEC)**

2. **LDPC codes over $\text{GF}(q)$**
   - Belief propagation decoding

3. **Density evolution**
   - Bounds and approximation models

4. **Results**

5. **Conclusion**
The $q$-ary partial erasure channel (QPEC)

2 LDPC codes over $\text{GF}(q)$
   - Belief propagation decoding

3 Density evolution
   - Bounds and approximation models

4 Results

5 Conclusion
Measurement channel

- Bits/symbols are represented by levels of electric charge
- New flash memories: up to 16 levels (4 bits) per memory cell
- The *read* operation is performed by measuring current/voltage levels

Read operation, stage 1:

The level is either 01 or 00
Bits/symbols are represented by levels of electric charge
New flash memories: up to 16 levels (4 bits) per memory cell
The read operation is performed by measuring current/voltage levels

Read operation, stage 2:

The level is 01
Measurement channel

Uncertainty

- High read rates
- Imperfect current/voltage sensing

Set of possible levels

The level is either 01 or 00
The $q$-ary partial erasure channel (QPEC)

Combinatorial model

$x_i$ are codeword symbols, taken from the alphabet $\mathcal{X} = \{0, 1, \ldots, q - 1\}$

$y_i$ are subsets of $\mathcal{X}$, such that $x_i \in y_i$
**Probabilistic model**

- Probability $\varepsilon$ for a *partial-erasure* event ($2 \leq |y_i| \leq q$)
- Channel transition probabilities (memoryless):

  $$\Pr (Y = y|X = x) = \begin{cases} 1 - \varepsilon, & y = x \\ \varepsilon_{x}^{(i)}, & y = \?_{x}^{(i)} \end{cases}$$

- $\?_{x}^{(i)}$ are subsets of $\mathcal{X}$ that *contain the symbol* $x$
- The number of such subsets is $i_{\text{max}} = \sum_{M=2}^{q} \left( \begin{array}{c} q - 1 \\ M - 1 \end{array} \right)$
The $q$-ary partial erasure channel (QPEC)

Special case: the $q$-ary erasure channel (QEC)

- Input alphabet: $\mathcal{X} = \{0, 1, ..., q - 1\}$
- Output alphabet: $\mathcal{Y} = \{\mathcal{X} \cup ?\}$
- Transition probabilities:

$$\Pr(Y = y | X = x) = \begin{cases} 1 - \varepsilon, & y = x \\
\varepsilon, & y = ? \end{cases}$$

- $y = ?$ corresponds to an erasure event
  - $? = \mathcal{X}$
The $q$-ary Partial Erasure Channel (QPEC)

$M$-uncertainty

- $|?_x^i| = M, 2 \leq M \leq q \ (M = q: \text{ QEC})$
- $i_{\text{max}} = \binom{q - 1}{M - 1}$
- Transition probabilities:

$$\Pr (Y = y | X = x) = \begin{cases} 1 - \varepsilon, & y = x \\ \varepsilon / i_{\text{max}}, & y = ?_x^i \end{cases}$$

- The transmitted symbol is either completely or partially known
- All $?_x^i$ are equally likely, given a partial-erasure event
The $q$-ary Partial Erasure Channel (QPEC)

Example: $q = 4, M = 3$

- $i_{\text{max}} = \binom{q-1}{M-1} = \binom{3}{2} = 3$

- Transition probabilities:
  
  $\Pr(Y = y | X = 0) = \begin{cases} 
  1 - \varepsilon, & y = 0 \\
  \varepsilon/3, & y = \{0, 1, 2\} \text{ or } \{0, 1, 3\} \text{ or } \{0, 2, 3\}
  \end{cases}$

  $\Pr(Y = y | X = 1) = \begin{cases} 
  1 - \varepsilon, & y = 0 \\
  \varepsilon/3, & y = \{1, 0, 2\} \text{ or } \{1, 0, 3\} \text{ or } \{1, 2, 3\}
  \end{cases}$

  :
# Table of Contents

1. The $q$-ary partial erasure channel (QPEC)

2. LDPC codes over $\text{GF}(q)$
   - Belief propagation decoding

3. Density evolution
   - Bounds and approximation models

4. Results

5. Conclusion
An \([n, k]\) low-density parity-check (LDPC) code is a *linear error correcting code*, defined by a parity-check matrix \(H\).

- \(H\) is a *sparse* \((n - k) \times n\) matrix with elements taken from \(\text{GF}(q)\).
- LDPC code can be represented using a bipartite graph:
  - *n variable (left) nodes* (VN): codeword symbols
  - *n - k check (right) nodes* (CN): parity-check equations
  - Variable node \(i\) is connected to check node \(j\) by an edge having the label \(H_{ji}\).
LDPC codes over \( GF(q) \)

Example \((k = 3, n = 7, GF(4))\):

\[
H = \begin{bmatrix}
0 & 2 & 3 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 2 & 0 & 0 & 2 \\
0 & 0 & 1 & 0 & 2 & 1 & 0 \\
3 & 0 & 0 & 1 & 0 & 2 & 0
\end{bmatrix}
\]
Example ($k = 3$, $n = 7$, GF(4)):

$$H = \begin{bmatrix}
0 & 2 & 3 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 2 & 0 & 0 & 2 \\
0 & 0 & 1 & 0 & 2 & 1 & 0 \\
3 & 0 & 0 & 1 & 0 & 2 & 0
\end{bmatrix}$$

$$2 \cdot v_2 + 3 \cdot v_3 + v_5 + v_7 = 0$$
Belief propagation

Message passing

- "Beliefs" (probabilities) about the VN values are transmitted over the graph edges in form of messages, "collecting" information in a structured way.
- We will consider here a non-standard message passing algorithm, in which *sets of symbols* are transmitted.
- In each iteration, messages are first transmitted from CNs to VNs, and then from VNs to CNs.
Belief propagation: QPEC

Check to variable messages (CTV)

- $c_{j \rightarrow i}$ consists of all possible assignments of VN $i$, given the neighbours of CN $j$, except VN $i$

$$2v_1 + 4v_2 + 3v_3 = 0 \text{ (GF(5))}$$
Belief propagation: QPEC

Variable to check messages (VTC)

- $v_{i \rightarrow j}$ consists of the intersection of the channel information and the CTV messages from the neighbours of VN $i$, except CN $j$
Belief propagation: example (GF(3), \( M = 2 \))

Iteration 0
(the labels are assumed to be 1, all-zero codeword was transmitted)

Channel information: 0, \{0, 2\}, \{0, 1\}
Belief propagation: example (GF(3), $M = 2$)

Iteration 1

Current estimate: $0, \{0, 2\}, 0$
Belief propagation: example (GF(3), $M = 2$)

Iteration 2

Final estimate: 0, 0, 0
Table of Contents

1 The $q$-ary partial erasure channel (QPEC)

2 LDPC codes over GF($q$)
   - Belief propagation decoding

3 Density evolution
   - Bounds and approximation models

4 Results

5 Conclusion
Density evolution

- Analytical tool for evaluating the performance of LDPC codes under message-passing decoding
- The probability of each possible message is tracked throughout the decoding process
- Random graphs are considered, sampled uniformly at random from the ensemble of LDPC codes
- Asymptotic analysis: \( n \) is sufficiently large
  - The graph is tree w.h.p.
  - The messages are statistically independent
Density evolution

- There are \( \sum_{i=0}^{q} \binom{q-1}{i} = O(2^q) \) possible messages.

- For complexity reasons, we track the sizes of the messages, only \( q \) possible sizes.

- Due to the symmetry of the QPEC, it can be assumed that the all-zero codeword was transmitted.

- For simplicity, we consider regular codes:
  - Variable (check) nodes have a fixed degree \( d_v \) (\( d_c \)).
CTV messages

- $w_m^{(l)}$: the probability that a CTV message at iteration $l$ is of size $m$

$$w_m^{(l)} = \sum_{\{|S_j|\}_{j=1}^{d_c-1} : |S_j| \leq M} \left( \prod_{j=1}^{d_c-1} z^{(l-1)}_{|S_j|} \right) \cdot P_m \left( \{ |S_j| \}_{j=1}^{d_c-1} \right). \quad (1)$$

- $P_m$: the probability for a CTV message of size $m$, given the incoming VTC messages sizes
Density evolution equations

VTC messages

- $z_m^{(l)}$: the probability that a VTC message at iteration $l$ is of size $m$

$$z_m^{(l)} = \delta [m - 1] \cdot (1 - \varepsilon) + \varepsilon \sum_{\{\|S_j\|\}_{j=1}^{d_v-1} : \|S_j\| \leq q} \left( \prod_{j=1}^{d_v-1} w_j^{(l)} \right) \cdot Q_m \left( \left\{ \|S_j\| \right\}_{j=1}^{d_v-1} , M \right).$$

- $Q_m$: the probability for a VTC message of size $m$, given the incoming CTV messages sizes and the channel information
Density evolution equations

Recurrence relation:

\[
 w_m^{(l)} = \sum_{\left\{ |S_j| \right\}_{j=1}^{d_c-1} : |S_j| \leq M} \left( \prod_{j=1}^{d_c-1} z^{(l-1)}_{|S_j|} \right) \cdot P_m \left( \left\{ |S_j| \right\}_{j=1}^{d_c-1} \right). 
\] (3)

\[
 z_m^{(l)} = \delta [m - 1] \cdot (1 - \varepsilon) + \varepsilon \sum_{\left\{ |S_j| \right\}_{j=1}^{d_v-1} : |S_j| \leq q} \left( \prod_{j=1}^{d_v-1} w^{(l)}_{|S_j|} \right) \cdot Q_m \left( \left\{ |S_j| \right\}_{j=1}^{d_v-1} , M \right). 
\] (4)

Initial conditions: \( z_1^{(0)} = 1 - \varepsilon \), \( z_M^{(0)} = \varepsilon \)
Density evolution

Density evolution equations

$Q_m$

- $Q_m$ is the probability that the intersection size of $d_v$ random GF($q$) subsets with sizes $\left\{ |S_j| \right\}_{j=1}^{d_v-1}, M$ is $m$

Theorem

$$Q_m \left( \left\{ |S_j| \right\}_{j=1}^{J} ; q \right) = \begin{cases} 
    \frac{l_{m-1} \left( \left\{ |S_j|-1 \right\}_{j=1}^{J} ; q-1 \right)}{\prod_{j=1}^{J} \left( \frac{q-1}{|S_j| - 1} \right)} , & \text{if } \min_j |S_j| > 1 \\
    \delta \left[ m - 1 \right], & \text{otherwise} 
\end{cases}$$

(5)

where $l_m \left( \left\{ |S_j| \right\}_{j=1}^{J} ; q \right)$ is the number of ways to choose subsets of GF($q$) with sizes $\left\{ |S_j| \right\}_{j=1}^{J}$ whose intersection is of size $m$
Density evolution equations

Equivalent formulation for $P_m$

- Define the sumset of the sets $\{S_j\}_{j=1}^{d_c-1}$:

$$
\sum_{j=1}^{d_c-1} S_j \triangleq \left\{ \sum_{j=1}^{d_c-1} s_j : s_j \in S_j \right\}
$$

**Example:** $S_1 = \{0, 1\}$, $S_2 = \{0, 2\}$ (GF(5))

$$
S_1 + S_2 = \{0 + 0, 0 + 2, 1 + 0, 1 + 2\} = \{0, 1, 2, 3\}
$$

- $P_m$ is equivalent to $\Pr \left( \left| \sum_{j=1}^{d_c-1} S_j \right| = m \right)$, given $\{|S_j|\}_{j=1}^{d_c-1}$
### Equivalent formulation for $P_m$: example

- $q = 4$, $d_c - 1 = 2$, $|S_1| = |S_2| = 2$
- There are $\binom{3}{1}^2 = 9$ possible realizations of the sets
  1. $S_1 = \{0, 1\}$, $S_2 = \{0, 2\}$:
     $S_1 + S_2 = \{0+0, 0+2, 1+0, 1+2\} = \{0, 2, 1, 3\}$
  2. $S_1 = S_2 = \{0, 1\}$:
     $S_1 + S_2 = \{0+0, 0+1, 1+0, 1+1\} = \{0, 1\}$
  3. And so on...
- Running over all possible realizations, we get:
  
  $$P_1 = 0, P_2 = 1/3, P_3 = 0, P_4 = 2/3$$

- **Inefficient**, but an expression for $P_m$ is unknown...
Bounds on the sumset size

**Lemma**

\[
\max_j |S_j| \leq \left| \sum_{j=1}^{d_c-1} S_j \right| \leq \min \left( q, \prod_{j=1}^{d_c-1} |S_j| \right)
\]

**Proof.**

1. **Lower bound:** denote by \(j_0\) the index of the largest subset. For a particular choice of elements from \(S_{j \neq j_0}\), we get a sumset of size \(\max_j |S_j|\).

2. **Upper bound:** there are \(\prod_{j=1}^{d_c-1} |S_j|\) sums within the sumset.
Bounds on the sumset size

**Cauchy-Davenport theorem**

Consider the finite field $\mathbb{GF}(p)$, $p$ prime. Let $A$ and $B$ be two non-empty subsets of $\mathbb{GF}(p)$. Then:

$$|A + B| \geq \min (p, |A| + |B| - 1).$$

**Károlyi’s theorem**

Let $A$ and $B$ are two non-empty subsets of a finite group $G$. Denote by $p(G)$ the smallest prime factor of $|G|$. Then:

$$|A + B| \geq \min (p(G), |A| + |B| - 1).$$
Bounds on the sumset size

Corollary (using induction)

\[
\max \left( \max_j |S_j| , \min \left( p, \sum_{j=1}^{d_c-1} |S_j| - d_c + 2 \right) \right) \leq \left| \sum_{j=1}^{d_c-1} S_j \right|
\]

\[
\leq \min \left( q, \prod_{j=1}^{d_c-1} |S_j| \right)
\]

q-condition

Consider \( d_c - 1 \) non-empty subsets of GF(\( q \)), \( \{S_j\}_{j=1}^{d_c-1} \). If there is a pair of subsets \( S_a, S_b \in \{S_j\}_{j=1}^{d_c-1} \) (\( a \neq b \)) such that \( |S_a| + |S_b| > q \), then

\[
\left| \sum_{j=1}^{d_c-1} S_j \right| = q.
\]
Bounds on the sumset size

**Worst case bound**

\[
P_m^{(\text{max})} = \begin{cases} 
\delta [m - q], & \text{if the } q\text{-condition holds} \\
\delta [m - B_U], & \text{otherwise}
\end{cases}
\]

- \( B_U \) is the upper bound on the sumset size

**Best case bound**

\[
P_m^{(\text{min})} = \begin{cases} 
\delta [m - q], & \text{if the } q\text{-condition holds} \\
\delta [m - B_L], & \text{otherwise}
\end{cases}
\]

- \( B_L \) is the lower bound on the sumset size
Balls and bins model

- There are $N$ balls and $q$ bins
- Each ball is assigned uniformly and independently at random to one of the bins
- $P_m$ is modelled as the probability that $m$ bins (elements of GF($q$)) are non-empty after $N = \prod_{j=1}^{d_c-1} |S_j|$ balls (sums within the sumset) were assigned

©Aaron Harwood, The university of Melbourne, 2011
Balls and bins model

Markov process formulation

- $q + 1$ states ($i = 0, 1, \ldots, q$): the number of non-empty bins
- Consider two randomly chosen subsets of $\mathrm{GF}(q)$ with sizes $|A|, |B|$. Then:

$$\Pr (|A \cap B| = m) \triangleq T_m (|A|, |B|) = \frac{l_m (|A|, |B|)}{\binom{q}{|A|} \cdot \binom{q}{|B|}}$$

- The $(q + 1) \times (q + 1)$ stochastic matrix:

$$(\Gamma_{\text{balls}})_{i,j} = T_{1+i-j} (1, i), \quad 0 \leq i, j \leq q$$

describes a Markov chain, such that $(\Gamma_{\text{balls}})_{i,j} = P_{\text{balls}} (i \to j)$
Balls and bins model

Approximation model for $P_m$

- Let $g_i^{(l)}$ denote the probability for $i$ non-empty bins after $l$ balls were assigned. According to the Markov property:

$$g^{(l)} = g^{(0)} \Gamma_{\text{balls}}^l, \quad g^{(0)} = (1, 0, \ldots, 0)$$

- We get the following model for $P_m$:

$$P_m^{(\text{balls})} = \begin{cases} 
0, & \text{if } m < B_L \\
\delta [m - q], & \text{if the } q\text{-condition holds} \\
\frac{q}{\sum_{i=B_L} g_i^{(N)}} & \text{otherwise}
\end{cases} \quad (6)$$

where $B_L$ is the lower bound on the sumset size.
The union model

Extending the balls and bins model

\[ \sum_{j=1}^{d_c-1} S_j \triangleq \left\{ \sum_{j=1}^{d_c-1} s_j : s_j \in S_j \right\} \]

- Denote \( \kappa \triangleq \max_j |S_j| \). For each particular choice of the elements which are not in the maximal set, we get \( \kappa \) distinct elements (sums) within the sumset.

- Instead of assigning each ball independently at random to one of the bins, \( N/\kappa \) sets of balls of size \( \kappa \) each are assigned to \( \kappa \) distinct bins.

- The corresponding Markov matrix is:

\[ (\Gamma_{\text{union}})_{i,j} = T_{\kappa+i-j} (\kappa, i), \quad 0 \leq i, j \leq q \]
The union model

Approximation model for $P_m$

- Let $u_i^{(l)}$ denote the probability for $i$ non-empty bins after $l$ balls were assigned according to the union model. We have:

$$u^{(l)} = u^{(0)} \Gamma^l_{\text{union}}, \quad u^{(0)} = (1, 0, \ldots, 0)$$

- We get the following model for $P_m$:

$$P^{(\text{union})}_m = \begin{cases} 
0, & \text{if } m < B_L \\
\delta \left[m - q\right], & \text{if the } q\text{-condition holds} \\
\frac{\sum_{i=B_L}^{q} u_i^{(N/\kappa)}}{u_m^{(N/\kappa)}}, & \text{otherwise}
\end{cases}$$

where $B_L$ is the lower bound on the sumset size.
# Table of Contents

1. The $q$-ary partial erasure channel (QPEC)

2. LDPC codes over $\mathrm{GF}(q)$
   - Belief propagation decoding

3. Density evolution
   - Bounds and approximation models

4. Results

5. Conclusion
Threshold phenomenon

Let $\chi^{(l)} \triangleq \sum_{i=2}^{M} z_i^{(l)}$ denote the expected fraction of VTC messages whose size exceeds 1 at iteration $l$.

**Theorem**

*There exists a threshold for the QPEC, defined as:*

$$\varepsilon_{th} = \sup \left\{ \varepsilon \in [0, 1] : \lim_{l \to \infty} \chi^{(l)}(\varepsilon) = 0 \right\}.$$  

*$\varepsilon_{th}$ is the decoding threshold (maximal allowed erasure probability) under (asymptotic) belief propagation decoding.*
Results \((d_v = 3, d_c = 6)\)

\[ q = 3 \]

\[ q = 4 \]
Results \( (d_v = 3, d_c = 6) \)

\[ q = 5 \]

\[ q = 7 \]
Results ($d_v = 3$, $d_c = 6$)

$q = 8$

$q = 16$
# Table of Contents

1. The $q$-ary partial erasure channel (QPEC)

2. LDPC codes over GF($q$)
   - Belief propagation decoding

3. Density evolution
   - Bounds and approximation models

4. Results

5. Conclusion
Conclusion

- The *q*-ary partial erasure channel (QPEC) was introduced
- Belief propagation decoder and density evolution analysis for GF\( (q) \) LDPC codes over the QPEC were provided
- Bounds and approximation models were obtained for the density evolution equations
- Suggested future research:
  - Extension to partial-erasure channels with non-uniform distribution
  - Analysis of the combinatorial model
This research is ongoing...