On the Tradeoff Between Performance and Complexity for Codes on Graphs: Bounds and Constructions

Dr. Igal Sason
Department of Electrical Engineering
Technion - Israel Institute of Technology
Haifa 32000, Israel

Collaborators: Dr. Henry Pfister (EPFL, Lausanne, Switzerland)
Prof. Rüdiger Urbanke (EPFL, Lausanne, Switzerland)
Mr. Gil Wiechman (Technion, Haifa, Israel)

Princeton University, New Jersey, USA
September 26, 2005
Low-Density Parity-Check Codes

- Low-density parity-check (LDPC) codes are well-known capacity-approaching linear codes which are characterized by sparse parity-check matrices.

- Sparse parity-check matrices
  ⇒ Low-complexity encoding and iterative message-passing decoding algorithms.

- An ensemble of irregular codes is defined by its degree distributions (d.d.)

- Let $\lambda(x) = \sum_{i \geq 2} \lambda_i x^{i-1}$ and $\rho(x) = \sum_{i \geq 2} \rho_i x^{i-1}$, where $\lambda_i$ and $\rho_i$ are the fraction of edges attached to bit and parity-check nodes of degree $i$. 
LDPC Codes (Cont.)

• For LDPC codes, the sub-optimal iterative decoding algorithm is very efficient, achieving rates close to the Shannon capacity limit with feasible complexity.

• In general, it would be very interesting to explore the relation between performance and encoding/decoding complexity for finite block lengths.

• Unfortunately, this central issue is too hard for rigorous analysis.

• In this talk, we are mostly concerned about the tradeoff between performance and complexity in the asymptotic case where the block length goes to infinity.
Some Questions Regarding the Performance of LDPC Codes

- Question 1: How sparse can parity-check matrices of binary linear codes be, as a function of their gap (in rate) to capacity?
Some Questions Regarding the Performance of LDPC Codes

• Question 1: How sparse can parity-check matrices of binary linear codes be, as a function of their gap (in rate) to capacity?

• Question 2: How good can LDPC codes be (even under ML decoding), as a function of their degree distributions?
Some Questions Regarding the Performance of LDPC Codes

• Question 1: How sparse can parity-check matrices of binary linear codes be, as a function of their gap (in rate) to capacity?

• Question 2: How good can LDPC codes be (even under ML decoding), as a function of their degree distributions?

• The density of a parity-check matrix of an LDPC code is related to the decoding complexity per iteration and the number of fundamental cycles in its bipartite graph.
Significance of these Questions Regarding the Performance of LDPC Codes

• Answer to Question 1 ⇒
  – Quantitative measure to the statement that bipartite graphs representing good error-correction codes should have cycles (even under optimal ML decoding).
Significance of these Questions Regarding the Performance of LDPC Codes (Cont.)

• Answer to Question 1 ⇒
  – Quantitative measure to the statement that bipartite graphs representing good error-correction codes should have cycles (even under ML decoding).
  – Lower bounds on the decoding complexity per iteration.
Significance of these Questions Regarding the Performance of LDPC Codes (Cont.)

- Answer to Question 1 ⇒
  - Quantitative measure to the statement that bipartite graphs representing good error-correction codes should have cycles (even under ML decoding).
  - Lower bounds on the decoding complexity per iteration.
  - Lower bounds on the bit-error probability under ML decoding.
Significance of these Questions Regarding the Performance of LDPC Codes (Cont.)

• Answer to Question 1 ⇒
  – Quantitative measure to the statement that bipartite graphs representing good error correction codes should have cycles (even under ML decoding).
  – Lower bounds on the decoding complexity per iteration.
  – Lower bounds on the bit-error probability.

• Answer to Question 2 ⇒
  Quantitative measure of the inherent loss of sub-optimal and practical iterative message-passing decoding algorithms.
Related Work

• Achievable Rates of LPDC Codes

  – Right-regular LDPC codes cannot achieve channel capacity on a BSC, even under ML decoding (Gallager, 1961).

  – For LDPC ensembles with fixed right degree (call it $a_R$), this inherent gap to capacity is well approximated by an expression which decreases to zero exponentially fast in $a_R$ (Gallager, 1961).

  – Burshtein et al. generalized Gallager’s bound for memoryless binary-input output-symmetric (MBIOS) channels (IEEE Trans. on IT, September 2002).

  – Etzion et al. proved that cycle-free codes are bad even under ML decoding (IEEE Trans. on IT, September 1999).
Related Work (Cont)

- Results for Ensembles
  - **Generalized EXIT (GEXIT)** charts provide upper bounds on the thresholds of turbo-like ensembles under MAP decoding for general MBIOS channels (Measson, Montanari, Richardson and Urbanke, ITW 2004).
  - **Statistical Physics** - Upper bounds on achievable rates for LDPC and LDGM codes over MBIOS channels - a statistical physics approach. Conjectured to be tight (Montanari’s paper, IEEE Trans. on IT, September 2005).
  - Montanari’s bound involves optimization over probability densities which makes the calculation difficult.
Related Work (Cont.)

- Goal: Achieving a fraction $1 - \varepsilon$ of Capacity for sufficiently small enough values of $\varepsilon$.
  
  - Define minimum complexity of encoding and decoding per information bit as $\chi_{E}(\varepsilon)$ and $\chi_{D}(\varepsilon)$

- Conjecture: For LDPC codes over MBIOS channels, $\chi_{D}(\varepsilon) = O\left(\frac{1}{\varepsilon} \ln \frac{1}{\varepsilon}\right)$, but for the BEC $\chi_{D}(\varepsilon) = O\left(\ln \frac{1}{\varepsilon}\right)$ (Khandekar and McEliece, ISIT 2001).

- For LDPC codes, the number of edges in graph proportional to parity-check matrix density, and the complexity per iteration (under iterative decoding).
Parity-Check Density (Definition)

- Let $C$ be a binary linear code of rate $R$ and block length $n$, which is represented by a parity-check matrix $H$.
- The *density* of $H$, call it $\Delta = \Delta(H)$, is defined as the normalized number of ones in $H$ per information bit.
  $\Rightarrow$ The total number of ones in $H$ is therefore equal to $nR\Delta$. 

13
Parity-Check Density (Theorem)

**Theorem 1** [Sason and Urbanke, IEEE Trans. on IT, July ’03]: Let \( \{C_m\} \) be a sequence of binary linear block codes achieving a fraction \( 1 - \varepsilon \) of the capacity of a memoryless binary-input output-symmetric channel with vanishing bit error probability. Then for every sequence of codes and any representation of the codes by parity-check matrices

\[
\liminf_{m \to \infty} \Delta_m > \frac{K_1 + K_2 \ln \frac{1}{\varepsilon}}{1 - \varepsilon},
\]

where

\[
K_1 = \frac{(1 - C) \cdot \ln \left( \frac{1 - 2 \ln 2}{2 \ln 2} \cdot \frac{1 - C}{C} \right)}{2C \cdot \ln \left( \frac{1}{1 - 2w} \right)} \quad \quad K_2 = \frac{1 - C}{2C \cdot \ln \left( \frac{1}{1 - 2w} \right)}.
\]

Here, \( C \) is the channel capacity, \( w = \frac{1}{2} \int_{-\infty}^{\infty} \min(f(y), f(-y)) \, dy \), and \( f(y) \triangleq p(y| x = 1) \).
Parity-Check Density (Cont.)

For the Binary Erasure Channel (BEC), these coefficients can be improved to

\[ K_1 = \frac{p \cdot \ln \left( \frac{p}{1-p} \right)}{(1-p) \cdot \ln \left( \frac{1}{1-p} \right)}, \]

\[ K_2 = \frac{p}{(1-p) \cdot \ln \left( \frac{1}{1-p} \right)} \]

where \( p \) designates the probability of erasure in the BEC.

This improvement at least doubles the previous lower bound for the BEC.
Some More Questions

Question 3: Is the logarithmic behavior of the information-theoretic lower bound in Theorem 1 true or just an artifact of the bounding technique?
Some More Questions (Cont.)

Question 3: Is the logarithmic behavior of the information-theoretic lower bound in Theorem 1 true or just an artifact of the bounding technique?

Question 4: If it is indeed the true behavior for an MBIOS channel, then are the coefficients $K_1$ and $K_2$ of the bound in Theorem 1 tight in general?
Some More Questions (Cont.)

Question 3: Is the logarithmic behavior of the information-theoretic lower bound in Theorem 1 true or just an artifact of the bounding technique?

Question 4: If it is indeed the true behavior for an MBIOS channel, then are the coefficients $K_1$ and $K_2$ of the bound in Theorem 1 tight in general?

Question 5: Is the new bound on the parity-check density tight for the BEC?
On the ML Performance of Gallager’s Regular LDPC Codes

**Theorem 2** [Sason and Urbanke, IEEE Trans. on IT, July ’03]:
For every memoryless binary-input output-symmetric channel, there exists a sequence of ensembles of regular LDPC codes which achieves under ML decoding a fraction $1 - \varepsilon$ of the channel capacity with vanishing block error probability, and

$$\lim_{n \to \infty} \Delta_n \leq \frac{K_3 + K_4 \ln \frac{1}{\varepsilon}}{1 - \varepsilon},$$

where $K_3$ and $K_4$ are appropriate constants which only depend on the channel.

$\Rightarrow$ A logarithmic behavior of the information-theoretic lower bound on the parity-check density is the correct one, answering Question no. 3 in the affirmative.
Shokrollahi’s Right-Regular LDPC Ensembles

\[ \lambda_{\alpha,N}(x) = \frac{\alpha \sum_{k=1}^{N-1} \binom{\alpha}{k} (-1)^{k+1} x^k}{\alpha - N \binom{\alpha}{N} (-1)^{N+1}} \]

\[ \rho_{\alpha}(x) = x^{\frac{1}{\alpha}}, \quad 0 < \alpha < 1. \]
Right-Regular LDPC Ensembles (Cont.)

Theorem 3 [Sason and Urbanke, IEEE Trans. on IT, July 2003]: For suitable parameters of $\alpha$ and $N$ and under *iterative message-passing decoding*, this sequence achieves asymptotically at least a fraction $1 - \varepsilon$ of the channel capacity with vanishing bit error probability. The asymptotic density of its parity-check matrices satisfies

$$\lim_{n \to \infty} \Delta_n \leq \frac{K_1 + K_2 \ln \frac{1}{\varepsilon} + g(\varepsilon, p)}{1 - \varepsilon},$$

where $K_1, K_2$ are the coefficients in the lower bound of Theorem 1, and in the limit where the gap to capacity goes to zero

$$\lim_{\varepsilon \to 0^+} g(\varepsilon, p) \leq 0.5407 \quad \forall \ 0 < p < 1.$$

$\Rightarrow$ Answering Question no. 5 in the affirmative: The improved bound on the parity-check density of the BEC (see Theorem 1) is extremely tight as the gap to capacity vanishes!
Discussion

- Theorems 1 & 3 ⇒ For any iterative decoder based on the standard Tanner graph there is a tradeoff between performance and complexity. This tradeoff cannot be surpassed!
Discussion (Cont.)

- Theorems 1 & 3 ⇒ For any iterative decoder based on the standard Tanner graph there is a tradeoff between performance and complexity. This tradeoff cannot be surpassed!

⇒ Are better tradeoffs can be achieved by allowing more complicated graphical models (e.g., graphs which involve state nodes, in addition to variable nodes and parity-check nodes used for representing codes by bipartite graphs)?

Fortunately, we will see that this is possible!.

The recent results in the respect rely on a joint work with Dr. Henry Pfister and Prof. Ruediger Urbanke (published in the IEEE Trans. on IT, July 2005). This will be addressed in the second part of this talk.
• Is it possible to improve the tightness of the lower bound in Theorem 1 for the family of memoryless binary-input output-symmetric channels?

Fortunately, we will see that this is possible!

The recent results in the respect rely on a joint work with Mr. Gil Wiechman (submitted to IEEE Trans. on IT, May 2005).

This will be addressed in the third part of this talk.
On the Decoding Complexity of Punctured Codes on Graphs Communicated over the Binary Erasure Channel (BEC)

Joint work with Dr. Henry Pfister and Prof. Ruediger Urbanke
Theorem 4 [Sason and Urbanke, IEEE Trans. on IT, June 2004]
Under iterative message-passing decoding on the BEC, the decoding complexity per information bit of systematic IRA (SIRA) codes scales at least like the $\log \frac{1}{\epsilon}$ (i.e., the log of the inverse of the gap to capacity).

⇒ For SIRA codes with an iterative message-passing decoder, the decoding complexity becomes un-bounded as the gap to capacity vanishes.
Could These Results Be Further Improved?

Question 6: What about non-systematic IRA codes where the information bits are punctured before transmission?
Non-Systematic IRA Codes

\begin{align*}
    x_1 &= 1 - (1 - x_2) R (1 - x_0), \\
    x_2 &= p x_1, \\
    x_3 &= 1 - (1 - x_2)^2 \rho (1 - x_0), \\
    x_0 &= \lambda(x_3)
\end{align*}
Capacity-Achieving Codes for the BEC with Bounded Complexity

IEEE Trans. on IT, July 2005 [Pfister et al.]: Two sequences of non-systematic IRA (NSIRA) codes are presented, which asymptotically achieve capacity on the BEC with **bounded complexity per information bit**.

The new bounded complexity result was achieved by puncturing bits and allowing in this way a sufficient number of state nodes in the Tanner graph representing the codes.
Bit-Regular Construction

• Ensemble of bit-regular non-sys IRA codes with \( \lambda(x) = x^{q-1} \)
  
  – The parity-check d.d. which satisfies the DE equality for this \( \lambda(x) \) is

\[
\rho(x) = \frac{1 - (1 - x)^{\frac{1}{q-1}}}{\left[1 - p \left(1 - qx + (q - 1) \left[1 - (1 - x)^{\frac{q}{q-1}}\right]\right)\right]^2}
\]

  – For \( q = 3 \), the power series expansion of \( \rho(x) \) is non-negative iff \( p \in [0, 1/13] \)

• Truncating the check d.d. to degree \( M(\varepsilon) \) (via degree 1 checks)
  
  – Let \( \rho_\varepsilon(x) = \left(1 - \sum_{n=1}^{M(\varepsilon)} \rho_n\right) + \sum_{n=1}^{M(\varepsilon)} \rho_n x^{n-1} \) where

\[
\sum_{n=M(\varepsilon)+1}^{\infty} \rho_n < \frac{\varepsilon}{q(1 - p)}
\]
Bit-Regular Construction (Cont.)

**Theorem 5** [Pfister et al., Trans. on IT, July 2005]

- In this case, bit erasure probability converges to zero and
  \[ R_{\text{IRA}} \geq (1 - \varepsilon)(1 - p). \]

- Complexity (edges per info bit) upper bounded by
  \[ q + \frac{2}{(1-p)(1-\varepsilon)}. \]
Check-Regular Construction

- Ensemble of check-regular non-sys IRA codes with $\rho(x) = x^2$.
  - The information-bit d.d. which satisfies the DE equality for this $\rho(x)$ is

  $$
  \lambda(x) = 1 + \frac{2p(1 - x)^2 \sin \left( \frac{1}{3} \arcsin \left( \sqrt{-\frac{27p(1-x)^3}{4(1-p)^3}} \right) \right)}{\sqrt{3} (1 - p)^4 \left( -\frac{p(1-x)^{3/2}}{(1-p)^3} \right)^{3/2}}.
  $$

  - Can show the power series expansion of $\lambda(x)$ is non-negative for $p \in [0, 0.95]$.

- Truncating the bit d.d. to degree $M(\varepsilon)$ (via pilot bits).
  - Treat all information bits with degree $> M(\varepsilon)$ as pilot bits.
Check-Regular Construction (Cont.)

- Effective bit d.d. $\lambda_\varepsilon(x) = \sum_{n=2}^{M(\varepsilon)} \lambda_n x^{n-1}$ where

$$\sum_{n=M(\varepsilon)+1}^{\infty} \frac{\lambda_n}{n} < \frac{(1-p)\varepsilon}{3}$$

**Theorem 6** [Pfister et al., Trans. on IT, July 2005]

- The bit erasure probability converges to zero and $R^{IRA} \geq (1 - \varepsilon)(1 - p)$

- Complexity (edges per info bit) upper bounded by $\frac{5}{1-p}$ (this bound is tight when the gap to capacity vanishes, i.e., $\varepsilon \rightarrow 0$).

$\Rightarrow$ Achieving capacity of the BEC with bounded complexity per information bit.
Capacity-Achieving and Bounded-Complexity Ensembles for the BEC

- Previous constructions for the BEC have provably unbounded complexity which grows at least like $O(\ln \frac{1}{\varepsilon})$ where $\varepsilon$ designates the gap in rate to channel capacity.

- Our main results are:
  
  – Showing the existence of capacity-achieving codes for the BEC with bounded complexity due to state nodes in the Tanner graph. The state nodes in the Tanner graph are introduced here by puncturing all the information bits.
  
  – For fixed complexity, the new codes eventually (for $n$ large enough) outperform any code proposed to date. On the other hand, the convergence speed to the ultimate performance limit happens to be quite slow, so for small to moderate block lengths, the new codes are not record breaking.
Drawback:

The convergence speed to the ultimate performance limit happens to be quite slow in terms of the block length, so for small to moderate block lengths, the new codes are not record breaking.
Further research into the construction of (systematic) codes which approach capacity for moderate block lengths and have bounded complexity per information bit is an ongoing work.

Some recent results which will be presented in the Allerton conference are based on a joint work with Henry Pfister. These results rely on efficient constructions of capacity-achieving and systematic accumulate-repeat-accumulate codes.
Accumulate-Repeat-Accumulate (ARA) Codes

• These codes form a generalization of the IRA codes. The ARA codes were recently introduced by Abbasfar, Divsalar and Yao (ISIT 2004).

• The codes have outstanding performance and a simple linear-time encoding.

In this work, we examine the suitability of irregular and systematic ARA codes for the construction of capacity-achieving ensembles for the BEC with bounded complexity. We also examine by computer simulations their performance for moderate to large block length.
Encoder diagram for the systematic ARA ensemble

- ”Accumulate” block is the standard rate-1 $\frac{1}{1+D}$ encoder
- “Irr. Repeat” block repeats each bit a different number of times
- “Irr. SPC” block groups bit in different size blocks and outputs a single parity bit for each block
- Block sizes are shown on each arrow for $k$ information bits
Systematic ARA Codes: Tanner Graph

- Shading is used to denote punctured or erased bits
Graph Reduction for Code Bits

- Any “code bit” node whose value is not erased by the BEC can be removed from the graph by absorbing its value into its two “parity-check 2” nodes.
- When the value of a “code bit” node is erased, one can merge the two “parity-check 2” nodes which are connected to it (by summing the equations) and this removes the “code bit” from the graph.
- Merging two “parity-check 2” nodes causes their degrees to be summed.
Graph Reduction for Systematic Bits

• The “systematic bit” nodes in the Tanner graph of the systematic ARA codes only provide channel information. Erasures make them worthless, and they can be removed along with their “parity-check 1” nodes without affecting the decoder.

• When the value of a “systematic bit” node is observed (assume the value is zero w.o.l.o.g.), it can be removed leaving a degree 2 parity-check.

• Degree 2 parity-checks imply equality, and allow the connected “punctured bit” nodes to be merged (summing their degrees).
Density Evolution via Graph Reduction (Cont.)

After the graph reduction, we are left with a standard LDPC code with new edge-perspective degree distributions given by

\[ \tilde{\lambda}(x) = \frac{\tilde{L}'(x)}{\tilde{L}'(1)} = \frac{p^2\lambda(x)}{(1 - (1 - p)L(x))^2} \]

\[ \tilde{\rho}(x) = \frac{\tilde{R}'(x)}{\tilde{R}'(1)} = \frac{(1 - p)^2\rho(x)}{(1 - pR(x))^2}. \]
Density Evolution via Graph Reduction (Cont.)

Let us define

\[ \tilde{f}_p(x) \triangleq \frac{(1 - p)^2 f(x)}{\left( 1 - p \frac{\int_0^x f(t)dt}{\int_0^1 f(t)dt} \right)^2}. \]

After the graph reduction, all the “systematic bit” nodes and “code bit” nodes are removed.

⇒ The residual LDPC code effectively sees a BEC whose erasure probability is 1,
⇒ The fixed point DE equation is given by

\[ \tilde{\lambda}_{1-p} (1 - \tilde{\rho}_p(1 - x)) = x. \]
Symmetry Properties of Capacity-Achieving Codes

In the following, we discuss the symmetry between the bit and check degree distributions of c.a. ensembles for the BEC. First, we describe this relationship for LDPC codes, and then we extend it to ARA codes. The extension is based on analyzing the decoding of ARA codes in terms of graph reduction and the DE analysis of LDPC codes.
Symmetry Properties of Capacity-Achieving LDPC Codes

The relationship between the bit d.d. and check d.d. of c.a. ensembles of LDPC codes can be expressed in a number of ways. Starting with the DE fixed point equation

\[ p\lambda (1 - \rho (1 - x)) = x \]  

where \( p \) designates the erasure probability of the BEC, we see that picking either the d.d. \( \lambda \) or \( \rho \) determines the other d.d. exactly.
A few definitions are needed to discuss things properly. Following the notation by Oswald and Shokrollahi (IT, Dec. 2002), let

\[ \mathcal{P} \triangleq \left\{ f : f(x) = \sum_{k=1}^{\infty} f_k x^k, \ x \in [0, 1], \ f_k \geq 0, \ f(0) = 0, \ f(1) = 1 \right\}. \]

Let \( \mathcal{T} \) be an operator which transforms any invertible function \( f : [0, 1] \rightarrow [0, 1] \) to

\[ \mathcal{T} f(x) \triangleq 1 - f^{-1}(1 - x) \]

where \( f^{-1} \) is the inverse function of \( f \).

Let \( \mathcal{A} \) be the set of all functions \( f \in \mathcal{P} \) such that \( \mathcal{T} f \in \mathcal{P} \), i.e.,

\[ \mathcal{A} \triangleq \left\{ f : f \in \mathcal{P}, \ \mathcal{T} f \in \mathcal{P} \right\}. \]
The connection with LDPC codes is that finding some $f \in \mathcal{A}$ is typically the first step towards proving that $(f, \mathcal{T}f)$ is a c.a. d.d. pair.

Truncation and normalization issues which depend on the erasure probability of the BEC must also be considered.

When $p = 1$, many of these issues disappear, so we denote the set of d.d. pairs which satisfy the DE fixed point equation (1) by

$$\mathcal{C}_{LDPC} \triangleq \left\{ (\lambda, \rho) \in \mathcal{P} \times \mathcal{P} \mid \lambda(1 - \rho(1 - x)) = x \right\}$$

$$= \left\{ (\lambda, \rho) \mid \lambda \in \mathcal{A}, \rho = \mathcal{T}\lambda \right\}.$$
The symmetry property of c.a. LDPC codes (with rate 0) asserts that

\[(\lambda, \rho) \in \mathcal{C}_{\text{LDPC}} \xrightarrow{\text{symmetry}} (\rho, \lambda) \in \mathcal{C}_{\text{LDPC}}.\]
Symmetry Properties of ARA Codes

The symmetry relationship between c.a. ensembles of ARA codes and LDPC codes is given by

\[(\lambda, \rho) \in C_{\text{ARA}}(p) \quad \text{ARA symmetry} \quad (\rho, \lambda) \in C_{\text{ARA}}(1 - p)\]

\[G_{\text{ARA}} \quad \tilde{\lambda}_{1-p}, \tilde{\rho}_p \in C_{\text{LDPC}} \quad \text{LDPC symmetry} \quad (\tilde{\rho}_p, \tilde{\lambda}_{1-p}) \in C_{\text{LDPC}}\]

The inverse of the graph reduction mapping is represented by the dashed arrow because this inverse transformation is only valid if it is known ahead of time that the power series expansions of \(\lambda\) and \(\rho\) are non-negative.
Matched Functions

Definition 1. The functions $f$ and $g$ are said to be matched if

$$\mathcal{T} f = g.$$ 

Note that for any function $f$

$$\mathcal{T}^2 f \equiv f$$

so

$$\mathcal{T} f = g \iff \mathcal{T} g = f.$$ 

Example 1. The function

$$f(x) = \frac{(1 - b)x}{1 - bx} \quad 0 < b < 1$$

is matched to itself (i.e., $\mathcal{T} f = f$), and it also has a non-negative power series expansion around zero.
Construction of Capacity-Achieving ARA codes for the BEC

The algorithm proceeds as follows:

• Choose a function \( f \in \mathcal{A} \), and set the pair of tilted degree distributions from the edge perspective (after graph reduction) as

\[
\widetilde{\lambda} = f, \quad \widetilde{\rho} = \mathcal{T} f.
\]

• Calculate the pair of tilted degree distributions from the edge perspective

\[
\widetilde{L}(x) = \frac{\int_0^x \widetilde{\lambda}(t) \, dt}{\int_0^1 \widetilde{\lambda}(t) \, dt}, \quad \widetilde{R}(x) = \frac{\int_0^x \widetilde{\rho}(t) \, dt}{\int_0^1 \widetilde{\rho}(t) \, dt}.
\]
Construction of Capacity-Achieving ARA codes for the BEC (Cont.)

- Calculate the original d.d. pair w.r.t. the nodes (i.e., the original d.d. pair before the graph reduction) by the equations

\[
L(x) = \frac{\tilde{L}(x)}{p + (1 - p)\tilde{L}(x)}, \quad R(x) = \frac{\tilde{R}(x)}{1 - p + p\tilde{R}(x)}
\]

- **Critical Point:** Check if \( L \) and \( R \) have non-negative power series expansions around zero.

- If this is indeed the case, calculate d.d. pair w.r.t. the edges

\[
\lambda(x) = \frac{L'(x)}{L'(1)}, \quad \rho(x) = \frac{R'(x)}{R'(1)}.
\]
A Capacity-Achieving Systematic ARA codes with Bounded Complexity

Construction of a capacity-achieving systematic ARA codes for the BEC with bounded complexity per information bit

- From Example 1, let
  \[ \tilde{\lambda}(x) = \tilde{\rho}(x) = \frac{(1 - b)x}{1 - bx} \quad 0 < b < 1. \]

- According to the algorithm, this gives
  \[ L(x) = \frac{bx + \ln(1 - bx)}{p [b + \ln(1 - b)] + (1 - p) [bx + \ln(1 - bx)]}, \]
  \[ R(x) = \frac{bx + \ln(1 - bx)}{(1 - p) [b + \ln(1 - b)] + p [bx + \ln(1 - bx)]}. \]
A Capacity-Achieving Systematic ARA codes with Bounded Complexity

(Cont.)

- It has been observed empirically, that the power series expansions of both $R$ and $L$ are non-negative if and only if $p$ satisfies the inequality

$$\frac{1}{1 - \frac{13 - \sqrt{61}}{9} \left( b + \ln(1 - b) \right)} \leq p \leq 1 - \frac{1}{1 - \frac{13 - \sqrt{61}}{9} \left( b + \ln(1 - b) \right)}$$

and

$$b \in [b^*, 1), \quad b^* \triangleq W(-e^{-\frac{25 + \sqrt{61}}{12}}) + 1 \approx 0.9304$$

where $W$ designates the Lambert W-function.
A Capacity-Achieving Systematic ARA codes with Bounded Complexity

(Cont.)

• The asymptotic behavior of the d.d. pairs w.r.t. the nodes and the edges is

\[ L_k, R_k = O \left( \frac{b^k}{k \ln^2(k)} \right), \quad \lambda_k, \rho_k = O \left( \frac{b^k}{\ln^2(k)} \right). \]

• We believe the performance advantage of this ensemble over other c.a. ensembles is mainly due to the exponential decay of the d.d. coefficients.
The encoding and decoding complexities per information bit of the considered c.a. ensembles of ARA codes for the BEC are bounded and given by

$$
\chi_E, \chi_D = \frac{3 - p}{1 - p} - \frac{b^2 p}{(1 - b)[b + \ln(1 - b)]}.
$$

For fixed $p$, the complexity is a monotonic increasing function of $b$ (which becomes unbounded as $b \to 1^-$).
Symmetry Properties of NSIRA Codes

The symmetry relationship between c.a. ensembles of NSIRA codes and ALDPC codes is given in the following diagram.

\[(\lambda, \rho) \in \mathcal{C}_{NSIRA}(p) \overset{\text{symmetry}}{\longrightarrow} (\rho, \lambda) \in \mathcal{C}_{ALDPC}(1 - p)\]

\[\mathcal{G}_{NSIRA} \quad \mathcal{G}_{ALDPC}\]

\[(\lambda, \tilde{\rho}_p) \in \mathcal{C}_{LDPC} \overset{\text{LDPC symmetry}}{\longrightarrow} (\tilde{\rho}_p, \lambda) \in \mathcal{C}_{LDPC}\]

As before, the inverse of each graph reduction mapping is represented by a dashed arrow because this inverse transformation is only valid if it is known ahead of time that the power series expansions of \(\lambda\) and \(\rho\) are non-negative.
Construction of Capacity-Achieving NSIRA codes for the BEC

By graph reduction for NSIRA codes, the same algorithm for ARA codes holds also here, except that for NSIRA codes $\tilde{\lambda} = \lambda$.

**Example 2.** Starting with the same function $f$, we get that there are no degree-1 “information bit” nodes, and that the fraction of “information bit” nodes with degree $i$ is given by

$$L_i = \frac{1}{i} \frac{b^i}{b + \ln(1 - b)} , \quad i = 2, 3, \ldots .$$

The non-negativity of the sequence $\{L_i\}$ holds when $0 < b < 1$ (so $b + \ln(1 - b) < 0$).
Construction of Capacity-Achieving NSIRA codes for the BEC (Cont.)

- For the NSIRA ensemble, there is no requirement on the erasure probability $p$ for keeping the power series expansion of the d.d. $L$ to be non-negative.
- It has been empirically observed that the following condition on $p$ needs to be satisfied so that the power series expansion of the d.d. $R$ will be non-negative:

$$p \leq 1 - \frac{1}{1 - \frac{13 - \sqrt{61}}{9} [b + \ln(1 - b)]}.$$

By comparing it to the parallel requirement for the ARA ensemble, one observes that the latter condition requires a weaker condition on $p$ which is only the upper bound on $p$ in the previous condition for ARA codes.

- The d.d. $R$ is the same as for the ARA ensemble in Example 1.
- The encoding and decoding complexities of this ensemble are equal and have the form

$$\chi_E = \chi_D = \frac{2}{1 - p} - \frac{b^2}{(1 - b) [b + \ln(1 - b)]}.$$
Computer Simulation (1)

ARA vs. IRA vs. LDPC n=8192 Rate 0.5

Erasure Probability (p)
Word/Bit Error Rate
ARA WER
ARA BER
LDPC WER
LDPC BER
IRA WER
IRA BER
Computer Simulation (2)

ARA vs. IRA vs. LDPC n=65536 Rate 0.5

Erasure Probability (p)

Word/Bit Error Rate

ARA WER
ARA BER
LDPC WER
LDPC BER
IRA WER
IRA BER

0.465 0.47 0.475 0.48 0.485 0.49 0.495 ...
Summary for Capacity-Achieving Code Constructions with Bounded Complexity over the BEC

- Introduced capacity-achieving ARA codes for the BEC
  - Systematic codes whose decoding complexity per information bit is bounded as the gap to capacity vanishes
  - Simulations show improved performance over other c.a. ensembles
- Introduced density evolution via graph reduction
  - Exposes natural symmetry between LDPC, ARA and NSIRA codes
  - Allows c.a. LDPC codes to be mapped onto other code structures
Improved Information-Theoretic Bounds on the Tradeoff Between Performance and Complexity for LDPC Codes

The rest of the talk is focused on the study of the information-theoretic limitations inherent in the construction of LDPC codes. We assume a memoryless binary-input output-symmetric channel.

• Upper bounds on the achievable rates under ML decoding
  ⇒ valid also for any sub-optimal decoding algorithm.

• Lower bounds on the parity check density
  ⇒ serve as lower bounds on the decoding complexity of the iterative decoder.
Improvement of the Lower Bound on the Parity-Check Density and Its Implications

Burshtein et al. and Sason and Urbanke (see Theorem 1) relied on a two-level quantization of the log-likelihood ratio (LLR), essentially replacing the general MBIOS channel with a BSC. The bounding technique relies on the syndrome of the received sequence.

- Can we generalize the results for a larger set of quantization levels, which give a more accurate representation of the MBIOS channel?
- Can we use the same technique for the original (or an equivalent) channel?

In the last part of the talk, we reply both questions in the affirmative.
The work of Burshtein et al. and Sason and Urbanke was based on a two-level quantization of the log-likelihood ratio (LLR). This quantization essentially replaces the general MBIOS channel with a physically-degraded channel which is a BSC. The bounding technique depends on the fact that the output of the degraded channel is binary, by considering the syndrome of the received sequence.
Underlying Idea

The work of Burshtein *et al.* and Sason and Urbanke was based on a two-level quantization of the log-likelihood ratio (LLR). This quantization essentially replaces the general MBIOS channel with a physically-degraded channel which is a BSC. The bounding technique relies on the fact that the output of the degraded channel is binary, by considering the syndrome of the received sequence.

Our work introduces two approaches to circumvent the two level quantization.

- Applying a finer quantization to the LLR which allows a number of levels which is an arbitrary integer power of 2. To this end, we use Galois fields $\Rightarrow$ Gives an indication on the effect of quantization on the achievable rates of LDPC codes under ML decoding.
- Work directly on the LLR without quantization.
"Un-Quantized" Lower Bound on Conditional Entropy

- Let $C$ be a binary linear block code of length $n$ and rate $R$.
  - Let $x$ and $y$ be the transmitted codeword and received sequence, respectively.
  - Communication over an MBIOS channel with capacity $C$ bits per ch. use.
  - Denote by $a$ the pdf of the LLR given that the transmitted symbol is 0.
  - For an arbitrary full-rank parity-check matrix of $C$, let $\Gamma_k$ designate the fraction of the parity-checks involving $k$ variables, and define $\Gamma(x) \triangleq \sum_k \Gamma_k x^k$.

**Theorem 7** [Wiechman and Sason, Allerton 2005]
The conditional entropy of the transmitted codeword given the received sequence satisfies

$$\frac{H(X|Y)}{n} \geq 1 - C - (1 - R) \left( 1 - \frac{1}{2 \ln(2)} \sum_{p=1}^{\infty} \frac{\Gamma(g_p)}{p(2p - 1)} \right)$$

$$g_p \triangleq \int_0^\infty a(l)(1 + e^{-l}) \tanh^{2p} \left( \frac{l}{2} \right) dl$$
"Un-Quantized" Lower Bound on the Parity-Check Density

Let \( \{C_m\} \) be a sequence of binary linear block codes, and assume

- Communication over an MBIOS channel with capacity \( C \) bits per ch. use.
- Assume that the sequence \( \{C_m\} \) achieves a fraction \( 1 - \varepsilon \) of the channel capacity with vanishing bit error probability.

**Theorem 8 [Wiechman and Sason, Allerton 2005]**

The asymptotic density of their parity-check matrices satisfies

\[
\lim_{m \to \infty} \inf \Delta_m \geq \frac{K_1 + K_2 \ln \frac{1}{\varepsilon}}{1 - \varepsilon}
\]

where

\[
K_1 = \frac{1 - C}{C} \frac{\ln \left( \frac{\xi (1-C)}{C} \right)}{\ln \left( \frac{1}{g_1} \right)}, \quad K_2 = \frac{1 - C}{C} \frac{1}{\ln \left( \frac{1}{g_1} \right)}.
\]

\( g_1 \) is introduced in Theorem 7, and

\[
\xi \triangleq \begin{cases} 
\frac{1}{2 \ln(2)} & \text{for a BEC} \\
\frac{1}{2 \ln(2)} & \text{otherwise}
\end{cases}
\]
"Un-Quantized" Upper Bound on Asymptotic Achievable Rates

- Let \( \{C_m\} \) be a sequence of binary linear block codes
  - Communication over an MBIOS channel with capacity \( C \) bits per ch. use.
  - The block length of this sequence of codes tends to infinity as \( m \to \infty \)

**Theorem 9** [Wiechman and Sason, Allerton 2005]

A necessary condition for this sequence to achieve vanishing bit error probability as \( m \to \infty \) is that the asymptotic rate \( R \) of this sequence satisfies

\[
R \leq 1 - \frac{1 - C}{1 - \frac{1}{2 \ln(2)} \sum_{p=1}^{\infty} \frac{\Gamma(g_p)}{p(2p - 1)}}
\]

Theorems 7–9 are valid when considering LDPC ensembles of codes and replacing the rate with the design rate of the ensemble. In that case, one can relax the requirement that the parity-check matrices are full rank.
Numerical Results: Thresholds

- Comparison of the bounds for rate-1/2 irregular ensembles
  - AWGN Channel.
  - Average right degree increases with ensemble number.
  - Shannon Capacity limit for $R=\frac{1}{2}$ is 0.187 dB
  - Provides bounds on the inherent loss due to MPI decoding.

<table>
<thead>
<tr>
<th>Ensemble Number</th>
<th>2-Levels Bound</th>
<th>4-Levels Bound</th>
<th>8-Levels Bound</th>
<th>Un-Quantized Lower Bound</th>
<th>DE Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.269 dB</td>
<td>0.370 dB</td>
<td>0.404 dB</td>
<td>0.417 dB</td>
<td>0.809 dB</td>
</tr>
<tr>
<td>2</td>
<td>0.201 dB</td>
<td>0.226 dB</td>
<td>0.236 dB</td>
<td>0.239 dB</td>
<td>0.335 dB</td>
</tr>
<tr>
<td>3</td>
<td>0.198 dB</td>
<td>0.221 dB</td>
<td>0.229 dB</td>
<td>0.232 dB</td>
<td>0.310 dB</td>
</tr>
<tr>
<td>4</td>
<td>0.194 dB</td>
<td>0.208 dB</td>
<td>0.214 dB</td>
<td>0.216 dB</td>
<td>0.274 dB</td>
</tr>
</tbody>
</table>
Numerical Results: Parity-Check Density

• Setup
  – Transmission over AWGN Channel
  – Rate $= \frac{1}{2}$

• Observations
  – Difference between the bounds increases as $\varepsilon$ decreases.
  – As the $\frac{E_b}{N_0}$ approaches 0.187 dB (Capacity $= \frac{1}{2}$) the lower bounds go to infinity.
Summary on the Information-Theoretic Bounds

- Improved information-theoretic bounds on the thresholds and parity-check density of binary linear block codes (as opposed to probabilistic bounds which apply to ensembles of codes as their block length tends to infinity).
Summary on the Information-Theoretic Bounds

- Improved information-theoretic bounds on the thresholds and parity-check density of binary linear block codes (as opposed to probabilistic bounds which apply to ensembles of codes as their block length tends to infinity).
- Lower bounds on the parity-check density enable to assess more accurately the tradeoff between performance and complexity under MPI decoding.
Summary on the Information-Theoretic Bounds

- Improved information-theoretic bounds on the thresholds and parity-check density of binary linear block codes (as opposed to probabilistic bounds which apply to ensembles of codes as their block length tends to infinity).

- Lower bounds on the parity-check density enable to assess more accurately the tradeoff between performance and complexity under MPI decoding.

- Upper bounds on the thresholds under ML decoding and exact thresholds under MPI decoding calculated using density evolution enable to assess more accurately the inherent loss due to the structure of the codes and the sub-optimality of iterative decoding.
Summary on the Information-Theoretic Bounds

- Improved information-theoretic bounds on the thresholds and parity-check density of binary linear block codes (as opposed to probabilistic bounds which apply to ensembles of codes as their block length tends to infinity).
- Lower bounds on the parity-check density enable to assess more accurately the tradeoff between performance and complexity under MPI decoding.
- Upper bounds on the thresholds under ML decoding and exact thresholds under MPI decoding calculated using density evolution enable to assess more accurately the inherent loss due to the structure of the codes and the sub-optimality of iterative decoding.
- Comparison of quantized and un-quantized results gives insight on the inherent loss due to quantization of the received sequence.
Summary on the Information-Theoretic Bounds (Cont.)

- These bounds were recently generalized for parallel MBIOS channels. This generalization was used to obtain bounds on the achievable rates and decoding complexity per iteration of ensembles of punctured LDPC codes. The new paper (joint work with G. Wiechman) is submitted to IEEE Trans. on IT, August 2005, and available in the ArXiv and my home page).
Journal Papers Related to this Talk


Thank you for your attention!