Performance versus Complexity Per Iteration for LDPC Codes: An Information Theoretic Approach

Igal Sason and Gil Wiechman

Technion - Israel Institute of Technology

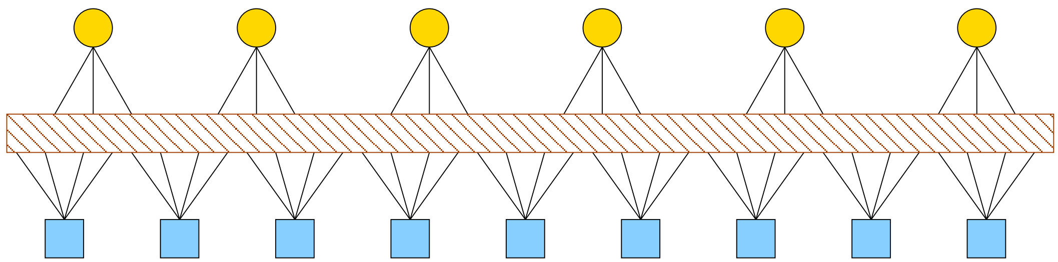
Haifa 32000, Israel

{sason@ee,igillw@tx}.technion.ac.il

4th International Symposium on Turbo Codes and Related Topics

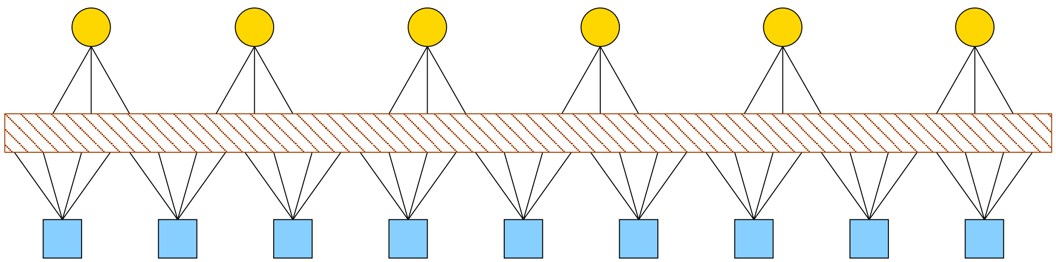
Munich, Germany, April 3–7, 2006

Low-Density Parity-Check Codes



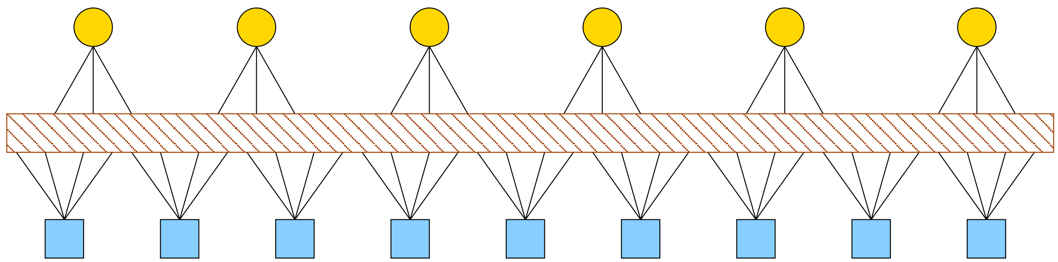
- Low-density parity-check (LDPC) codes are well-known capacity-approaching linear block codes which are characterized by sparse parity-check matrices.
- Sparse parity-check matrices $\Rightarrow$ Low-complexity encoding and decoding.

Low-Density Parity-Check Codes



- Low-density parity-check (LDPC) codes are well-known capacity-approaching linear block codes which are characterized by sparse parity-check matrices.
- Sparse parity-check matrices $\Rightarrow$ Low-complexity encoding and decoding.
- **The density of a parity-check matrix of an LDPC code is related to the decoding complexity per iteration under iterative message-passing decoding.**

Low-Density Parity-Check Codes



- Low-density parity-check (LDPC) codes are well-known capacity-approaching linear block codes which are characterized by sparse parity-check matrices.
- Sparse parity-check matrices $\Rightarrow$ Low-complexity encoding and decoding.
- The density of a parity-check matrix of an LDPC code is related to the decoding complexity per iteration under iterative message-passing decoding.
- **The density of a parity-check matrix of an LDPC code is related to the number of fundamental cycles in its bipartite graph.**

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 ?**

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 $\Rightarrow$
  - 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 $\Rightarrow$
  - 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 $\Rightarrow$
  - 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 $\Rightarrow$
  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 capacity on a BSC, even under ML decoding. 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).
  - Sason and Urbanke observed that Gallagers result holds when considering the *average* right degree of irregular ensembles. (IEEE Trans. on IT, July 2003)

Related Work

- 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).
  - These results are valid for ensembles and not code by code. Based on concentration arguments they asymptotically hold in probability 1.

Related Work (Cont.)

- Goal: Achieving a fraction $1-\varepsilon$ of Capacity
  - Define minimum decoding complexity per information bit as $\chi_D(\varepsilon)$
  - 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).

Answer to Question 1: (Sason & Urbanke, IEEE Trans. on IT, July '03)

- For any sequence of binary linear block codes achieving a fraction $1-\varepsilon$ of channel capacity (under ML decoding or any other decoding algorithm), the parity-check density grows at least like $\frac{K_1+K_2\ln\frac{1}{\varepsilon}}{1-\varepsilon}$.
- A logarithmic behavior is achievable under ML decoding for general MBIOS channels.
- For the BEC, it is even achievable under iterative decoding (Shokrollahi 1999).

Motivation

- Previous work based on two-level quantization of the log-likelihood ratio (LLR).
  $\Rightarrow$ replaces general MBIOS channel with a physically-degraded BSC.
- Bounding technique depends on binary output, by considering the syndrome of the received sequence.

Motivation

- Previous work based on two-level quantization of the log-likelihood ratio (LLR).
  $\Rightarrow$ replaces general MBIOS channel with a physically-degraded BSC.
- Bounding technique depends on binary output, by considering 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 work with the original (or an equivalent) channel ?

In this work, we reply both questions in the affirmative. It gives insight about the tradeoff between performance and complexity in the asymptotic case where the block length goes to infinity.

Bounds without Quantization of the LLR

- We define an *equivalent* channel whose output is the LLR of the original.
- LLR divided into sign and absolute value.
- Channel symmetry property $\Rightarrow$ new channel is a multiplicative channel, where the binary input (converted to +1,-1) multiplies an independent noise. Noise is distributed according to the *pdf* of the LLR of the original channel, given that the transmitted symbol is 0.
- Therefore we may use the absolute value of the output as side information on the noise, and calculate the syndrome of the sign of the received sequence.

”Un-Quantized” Lower Bound on Conditional Entropy

- Let $\mathcal{C}$ be a binary linear block code of length n and rate R.
  - Let $\mathbf{x}$ and $\mathbf{y}$ 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 $\mathcal{C}$, let Γ_k designate the fraction of the parity-checks involving k variables, and define $\Gamma(x) \triangleq \sum_k \Gamma_k x^k$.

”Un-Quantized” Lower Bound on Conditional Entropy

Theorem 1 The conditional entropy of the transmitted codeword given the received sequence satisfies

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

$$g_p \triangleq \int_0^{\infty} a(l)(1+e^{-l}) \tanh^{2p}\left(\frac{l}{2}\right) dl$$

Sequences of Codes

- From Fano's inequality, for a sequence of codes vanishing bit error probability we get

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \to 0$$

- The bound on conditional entropy yields an upper bound on the asymptotic achievable rate.

- Assume also $R = (1 - \varepsilon)C$, using convexity arguments we get a lower bound on the asymptotic parity-check density.

”Un-Quantized” Lower Bound on the Parity-Check Density

Let $\{\mathcal{C}_m\}$ 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 $\{\mathcal{C}_m\}$ achieves a fraction $1-\varepsilon$ of the channel capacity with vanishing bit error probability.

”Un-Quantized” Lower Bound on the Parity-Check Density

Theorem 2 The asymptotic density of their parity-check matrices satisfies

$$\liminf_{m\to\infty} \Delta_m \geq \frac{K_1 + K_2 \ln \frac{1}{\varepsilon}}{1-\varepsilon}$$

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 1, and

$$\xi \triangleq \begin{cases} 1 & \text{for a BEC} \\ \frac{1}{2\ln(2)} & \text{otherwise} \end{cases}\,.$$

"Un-Quantized" Upper Bound on Asymptotic Achievable Rates

- Let $\{\mathcal{C}_m\}$ 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 3 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

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

This theorem is valid under ML decoding, and hence, under any sub-optimal decoding algorithm (since we provide an upper bound on the achievable rate).

Notes on ”Un-Quantized” Bounds

- The ”un-quantized” bounds are not subject to optimization therefore their calculation is rapid.
- Tighter than the quantized bounds for any number of quantization levels.
- For the BEC, the ”un-quantized” bound on the asymptotic parity-check density merges with the bound of Sason and Urbanke, which was shown to be tight.
- Theorems 1–3 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.

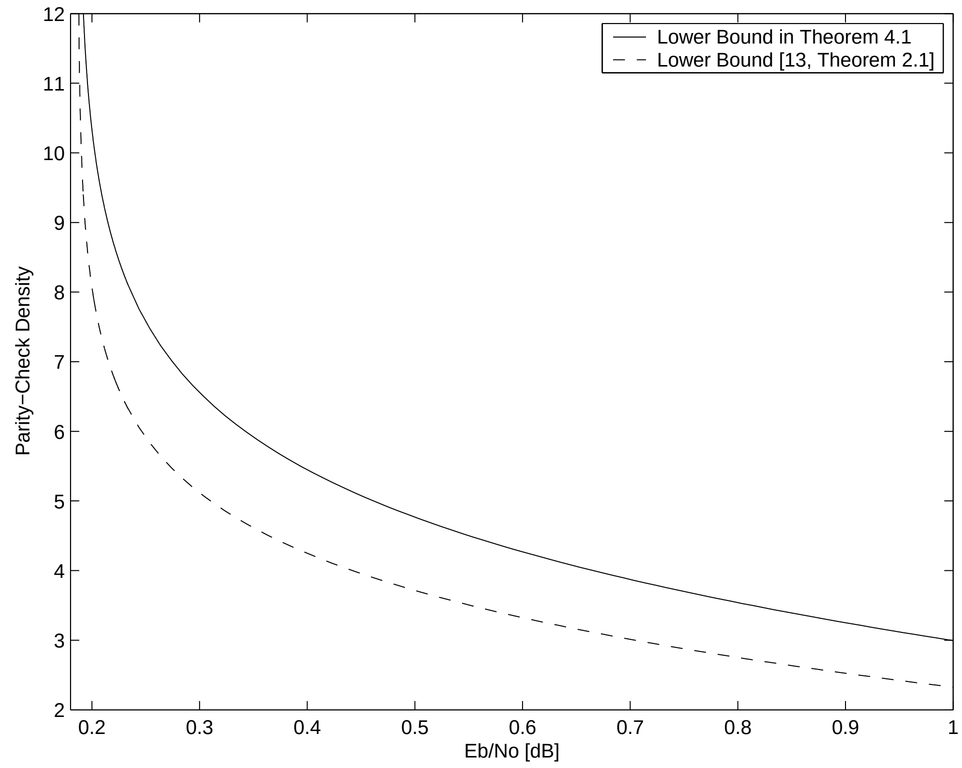
Numerical Results: Thresholds

- 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 inherent loss due to message-passing iterative decoding.

Ensemble Number	2-Levels Bound	4-Levels Bound	8-Levels Bound	Un-Quantized Lower Bound	DE Threshold
1	0.269 dB	0.370 dB	0.404 dB	0.417 dB	0.809 dB
2	0.201 dB	0.226 dB	0.236 dB	0.239 dB	0.335 dB
3	0.198 dB	0.221 dB	0.229 dB	0.232 dB	0.310 dB
4	0.194 dB	0.208 dB	0.214 dB	0.216 dB	0.274 dB

Numerical Results: Parity-Check Density

- Setup
  - Transmission over AWGN Channel
  - Rate = $\frac{1}{2}$
- Observations
  - Difference between the bounds increases as ε decreases.
  - As the $\frac{E_\mathrm{b}}{N_\mathrm{o}}$ approaches 0.187 dB (Capacity = $\frac{1}{2}$) the lower bounds go to infinity.



Parallel Channels

Scenario: Transmission over a set of independent MBIOS channels. Each code bit a-priori assigned to one channel.

- Let $\mathcal{C}$ be a binary linear block code of length n and rate R.
  - Let $\mathbf{x}$ and $\mathbf{y}$ be the transmitted codeword and received sequence, respectively.
  - Communication over J parallel MBIOS channels, capacity of j'th channel: C_j bits per ch. use.
  - $a(\cdot; j)$ denotes the *pdf* of the LLR of j'th channel, given input symbol is 0.
  - p_j designates the fraction of code bits transmitted over j'th channel.
  - For an arbitrary parity-check matrix of $\mathcal{C}$, $\beta_{j,m}$ is the number of bits transmitted over ch. j and involved in the m'th parity-check equation.

Lower Bound on Conditional Entropy for Parallel Channels

Theorem 4 The conditional entropy of the transmitted codeword given the received sequence satisfies

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \geq 1 - \sum_{j=1}^{J} p_j C_j - (1 - R_{\text{d}}) \cdot \left(1 - \frac{1}{2n(1-R_{\text{d}}) \ln 2} \sum_{p=1}^{\infty} \left\{ \frac{1}{p(2p-1)} \sum_{m=1}^{n(1-R_{\text{d}})} \prod_{j=1}^{J} (g_{j,p})^{\beta_{j,m}} \right\} \right)$$

where

$$g_{j,p} \triangleq \int_0^{\infty} a(l;j)\, (1+e^{-l}) \tanh^{2p}\left(\frac{l}{2}\right) dl, \qquad j \in \{1,\ldots,J\}, \quad p \in \mathbb{N}.$$

Upper Bound on Achievable Rates for Parallel Channels

- Consider a sequence of LDPC ensembles, whose block length tends to infinity.
  - J parallel MBIOS channels. Capacity of j'th channel: C_j bits/ch. use.
  - p_j denotes asymptotic fraction of code bits transmitted over j'th channel.
  - q_j denotes asymptotic fraction of edges in graph connected to code bits sent over j'th channel.

Theorem 5 A necessary condition for this sequence to achieve vanishing bit error probability (even under ML decoding) is that the design rate $R_{\rm d}$ satisfies

$$R_{\rm d} \leq 1 - \frac{1 - \sum_{j=1}^{J} p_j C_j}{1 - \frac{1}{2\ln 2} \sum_{p=1}^{\infty} \left\{ \frac{1}{p(2p-1)} \, \Gamma\left(\sum_{j=1}^{J} q_j \; g_{j,p} \right) \right\}}$$

where $\Gamma(x) = \sum_{i=2}^{\infty} \Gamma_i x^i$ is the left degree distribution from the node perspective.

Application: Intentionally Punctured LDPC Codes

- Introduced by Ha and McLaughlin (IEEE Trans. on IT, November 2004)
- Code bits are separated according to the degree of the corresponding node.
- Each set punctured at a different rate.
- Can be modeled as transmission over parallel channels. Each channel transmits bits whose corresponding nodes have a fixed degree.

Numerical Results: Intentionally Punctured LDPC Codes

- Original ensemble design rate 1/2.
- Transmission over binary input AWGN channel.
- Puncturing patterns optimized for iterative decoding.
- Provides bound on inherent loss due to iterative decoding.

Design rate	Capacity limit	Lower bound (ML decoding)	Iterative (IT) Decoding	Fractional gap to capacity (ML vs. IT)
0.500	0.187 dB	0.270 dB	0.393 dB	$\geq 40.3\%$
0.592	0.635 dB	0.716 dB	0.857 dB	$\geq 36.4\%$
0.671	1.083 dB	1.171 dB	1.330 dB	$\geq 35.6\%$
0.774	1.814 dB	1.927 dB	2.115 dB	$\geq 37.2\%$
0.838	2.409 dB	2.547 dB	2.781 dB	$\geq 37.1\%$
0.912	3.399 dB	3.607 dB	3.992 dB	$\geq 35.1\%$

Summary

- 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

- 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 iterative decoding.

Summary

- 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 iterative decoding.
- Upper bounds on the thresholds under ML decoding and exact thresholds under iterative 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

- 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 iterative decoding.
- Upper bounds on the thresholds under ML decoding and exact thresholds under iterative 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

- 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 iterative decoding.
- Upper bounds on the thresholds under ML decoding and exact thresholds under iterative 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.
- Generalization of the bounds for parallel channels enables to study the performance-complexity tradeoff for punctured codes.

Papers

This talk is based on two papers:

- G. Wiechman and I. Sason, ”Improved bounds on the parity-check density and achievable rates of binary linear block codes with applications to LDPC codes,” submitted to *IEEE Trans. on Information Theory*, May 2005.
- I. Sason and G. Wiechman, “On achievable rates and complexity of LDPC codes for parallel channels with application to puncturing,” submitted to *IEEE Trans. on Information Theory*, August 2005.

- Both papers as well as the conference versions are at:

  `http://www.ee.technion.ac.il/people/sason/` and the ArXiv.

Thank you for your attention !