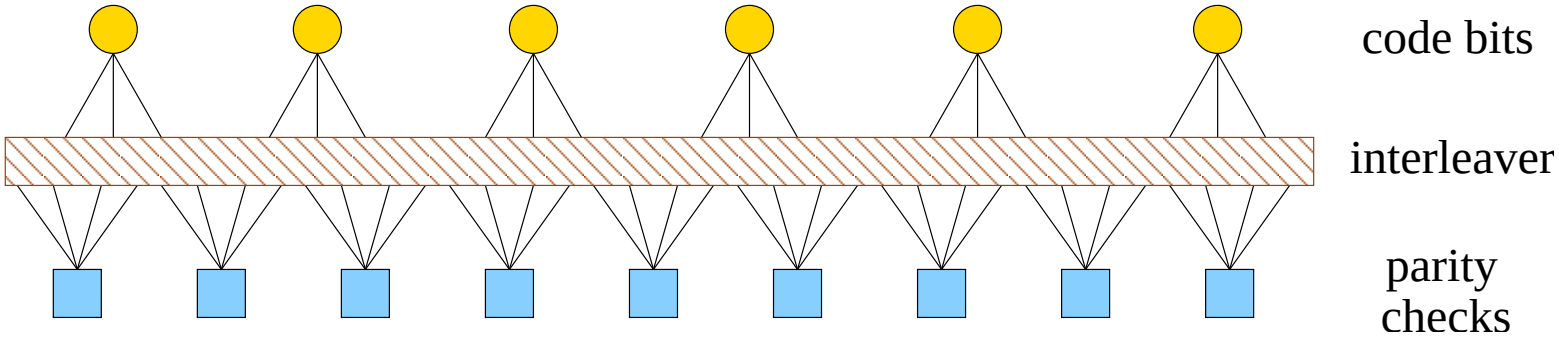
On the Parity-Check Density and Achievable Rates of LDPC Codes for Memoryless Binary-Input Output-Symmetric Channels

Gil Wiechman and Igal Sason
Technion - Israel Institute of Technology
Haifa 32000, Israel
{igillw@tx,sason@ee}.technion.ac.il

Technion - Israel Institute of Technology
December 1, 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
  $\Rightarrow$ 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 λ_i and ρ_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 $\Rightarrow$
  - **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).
  - For LDPC codes, the number of edges in graph proportional to parity-check matrix density, and the complexity per iteration (under iterative decoding).
  - Question: How sparse can the parity-check matrix be in terms of the gap in rate to capacity ?
  - Answer: Density grows at least like $\frac{K_1+K_2\ln\frac{1}{\varepsilon}}{1-\varepsilon}$ for binary linear block codes represented by bipartite graphs. A logarithmic behavior is achievable under ML decoding for general MBIOS channels and under iterative decoding for the BEC (Sason & Urbanke, IEEE Trans. on IT, July '03).

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.

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

$$H(\mathbf{X}|\mathbf{Y}) \;=\; H(\mathbf{X}) + H(\mathbf{Y}|\mathbf{X}) - H(\mathbf{Y})$$

”Un-Quantized” Lower Bound on Conditional Entropy

$$\begin{aligned} H(\mathbf{X}|\mathbf{Y}) &= H(\mathbf{X}) + H(\mathbf{Y}|\mathbf{X}) - H(\mathbf{Y}) \\ &= nR + nH(Y_1|X_1) - H(\mathbf{Y}) \end{aligned}$$

"Un-Quantized" Lower Bound on Conditional Entropy

$$\begin{aligned} H(\mathbf{X}|\mathbf{Y}) &= H(\mathbf{X}) + H(\mathbf{Y}|\mathbf{X}) - H(\mathbf{Y}) \\ &= nR + nH(Y_1|X_1) - H(\mathbf{Y}) \\ &= nR + n[H(Y_1) - I(X_1;Y_1)] - H(\mathbf{Y}) \end{aligned}$$

- $I(X_1;Y_1) \leq C$
- $H(Y_1) = H(|Y_1|) + H(\text{sign}(Y_1)\big||Y|)$
- $H(\mathbf{Y}) = H(|Y_1|,\ldots,|Y_n|) + H(\text{sign}(Y_1),\ldots,\text{sign}(Y_n)\big||Y_1|,\ldots,|Y_n|)$
- Since $Y_i = X_i \cdot Z_i$ and $|X_i| = 1$ we have $|Y_i| = |Z_i|$
- Memoryless channel $\Rightarrow H(|Y_1|,\ldots,|Y_n|) = H(|Z_1|,\ldots,|Z_n|) = nH(|Z_1|))$

"Un-Quantized" Lower Bound on Conditional Entropy

Therefore:

$$H(\mathbf{X}|\mathbf{Y}) \;\geq\; nR + nH(\text{sign}(Y_1)\big||Z_1|) - nC - H(\text{sign}(Y_1),\ldots,\text{sign}(Y_n)\big||Z_1|,\ldots,|Z_n|)$$

"Un-Quantized" Lower Bound on Conditional Entropy

Therefore:

$$H(\mathbf{X}|\mathbf{Y}) \geq nR + nH(\text{sign}(Y_1)\big||Z_1|) - nC - H(\text{sign}(Y_1),\ldots,\text{sign}(Y_n)\big||Z_1|,\ldots,|Z_n|)$$

$$= nR + n(1-C) - H(\text{sign}(Y_1),\ldots,\text{sign}(Y_n)\big||Z_1|,\ldots,|Z_n|)$$

"Un-Quantized" Lower Bound on Conditional Entropy

Therefore:

$$H(\mathbf{X}|\mathbf{Y}) \geq nR + nH(\text{sign}(Y_1)\big||Z_1|) - nC - H(\text{sign}(Y_1),\ldots,\text{sign}(Y_n)\big||Z_1|,\ldots,|Z_n|)$$

$$= nR + n(1-C) - H(\text{sign}(Y_1),\ldots,\text{sign}(Y_n)\big||Z_1|,\ldots,|Z_n|)$$

- sign(Y_i) is binary !
- Define Φ_i by mapping $\{+1,-1\} \rightarrow \{0,1\}$ in $\text{sign}(Y_i)$
- Define the syndrome $\mathbf{S} = (\Phi_1,\ldots\Phi_n)\cdot H^T$
- Define L as the index of $(\Phi_1,\ldots\Phi_n)$ in the coset represented by $\mathbf{S}$.
- Since $(\text{sign}(Y_1),\ldots,\text{sign}(Y_n))$ is uniquely determined by $(\mathbf{S}, L)$ we have $H(\text{sign}(Y_1),\ldots,\text{sign}(Y_n)\big||Z_1|,\ldots,|Z_n|) \leq H(L) + H(\mathbf{S}\big||Z_1|,\ldots,|Z_n|)$

"Un-Quantized" Lower Bound on Conditional Entropy

This gives:

$$H(\mathbf{X}|\mathbf{Y}) \geq nR + n(1-C) - H(L) - H(\mathbf{S}\big||Z_1|,\ldots,|Z_n|)$$

"Un-Quantized" Lower Bound on Conditional Entropy

This gives:

$$H(\mathbf{X}|\mathbf{Y}) \geq nR + n(1-C) - H(L) - H(\mathbf{S}\big||Z_1|,\ldots,|Z_n|)$$

$$\geq n(1-C) - \sum_{j=1}^{n(1-R)} H(S_j\big||Z_1|,\ldots,|Z_n|)$$

"Un-Quantized" Lower Bound on Conditional Entropy

This gives:

$$H(\mathbf{X}|\mathbf{Y}) \geq nR + n(1-C) - H(L) - H(\mathbf{S}\big||Z_1|,\ldots,|Z_n|)$$

$$\geq n(1-C) - \sum_{j=1}^{n(1-R)} H(S_j\big||Z_1|,\ldots,|Z_n|)$$

- Define $\tilde{X}_i$ and Θ_i by mapping $\{+1,-1\} \rightarrow \{0,1\}$ in X_i and $\text{sign}(Z_i)$.
- $\text{sign}(Y_i) = X_i \cdot \text{sign}(Z_i) \Rightarrow \Phi_i = \tilde{X}_i + \Theta_i$
  $\Rightarrow S_j = 1$ iff $\Theta_i = 1$ for an odd number of i's in the j'th equation.
- Due to the symmetry of the channel $P(\Theta_i = 1\big||Z_i| = z) = \frac{e^{-z}}{1+e^{-z}}$.

"Un-Quantized" Lower Bound on Conditional Entropy

Lemma 1 If the j'th component of the syndrome $\mathbf{S}$ involves k active variable whose indices are $\{i_1, \ldots, i_k\}$ then

$$P(S_j = 1 \big| |Z_{i_1}| = z_1, \ldots, |Z_{i_k}| = z_k) = \frac{1}{2}\left[1 - \prod_{m=1}^{k}\left(1 - \frac{2e^{-z_m}}{1+e^{-z_m}}\right)\right]$$

- $H(S_j \big| |Z_1|, \ldots, |Z_n|)$ is given by a k-dimensional integral.
- Applying the Taylor series for h_2 we get a converging sum of one-dimensional integrals raised to the k'th power.
- We have exactly Γ_k components involving k variables.

"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

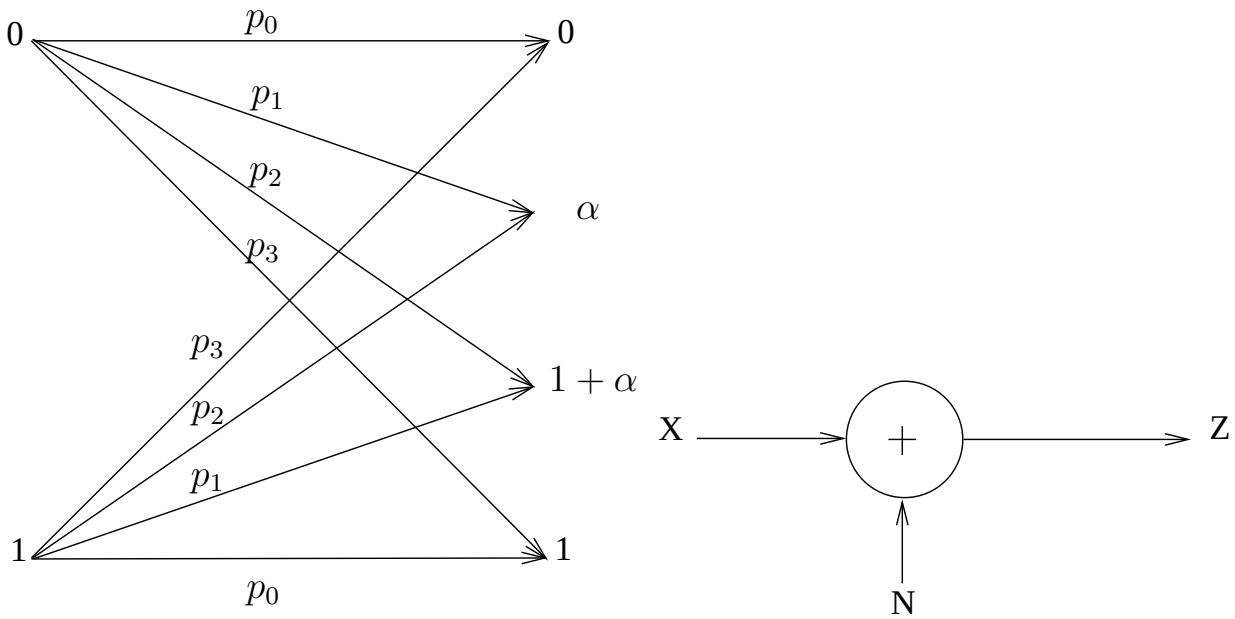
$$R \leq 1 - \frac{1 - C}{1 - \frac{1}{2\ln(2)} \sum_{p=1}^{\infty} \frac{\Gamma(g_p)}{p(2p-1)}}$$

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.

Quantization of the LLR

We replace the two-level quantization with a 2^d-level symmetric quantization of the LLR. The output alphabet of the quantized channel is defined to be $GF(2^d)$.



Quantization Based Lower Bound on Conditional Entropy

Let $\mathcal{C}$ be a binary linear block code of length n and design rate R.

- $\mathbf{x}$ and $\mathbf{y}$ indicate the transmitted codeword and received sequence, respectively.
- Communication over an MBIOS channel with capacity C bits per ch. use.
- For an arbitrary $d \geq 2$ and an arbitrary symmetric quantization with 2^d levels, define the probabilities $\{p_s\}_{s=0}^{2^d-1}$ as

  $p_s = \{$the probability of the LLR being in the s'th level when 0 is transmitted$\}$

Quantization Based Lower Bound on Conditional Entropy (Cont.)

Theorem 4 For an arbitrary parity-check matrix of the code $\mathcal{C}$, let d_k designate the fraction of the parity-checks involving k variables. Then, the conditional entropy of the transmitted codeword given the received sequence satisfies

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \geq 1 - C - (1-R) \sum_{k} \left\{ d_k \sum_{\substack{k_0,\ldots,k_{2^{d-1}-1} \\ \sum_i k_i = k}} \binom{k}{k_0, \ldots, k_{2^{d-1}-1}} \cdot \prod_{i=0}^{2^{d-1}-1} (p_i + p_{2^d-1-i})^{k_i} \; h_2\left(\frac{1}{2} \left[1 - \prod_{i=0}^{2^{d-1}-1} \left(1 - \frac{2p_{2^d-1-i}}{p_i + p_{2^d-1-i}} \right)^{k_i} \right] \right) \right\}.$$

Quantization Based Bounds

- Bounds on parity-check density and achievable rates derived similarly to the derivation of the ”un-quantized” bounds.
- Bound on density of the form $\frac{K_1+K_2\ln(\frac{1}{\varepsilon})}{1-\varepsilon}$.
- The bounds are subject to optimization of the quantization levels.
- For *optimally chosen* quantization levels, the bounds are monotonic with the number of quantization levels.
- For any $d \geq 2$ and any choice of quantization levels, these bounds tighten previously reported results for a general MBIOS channel.
- Give an indication on the effect of quantization at the receiver.

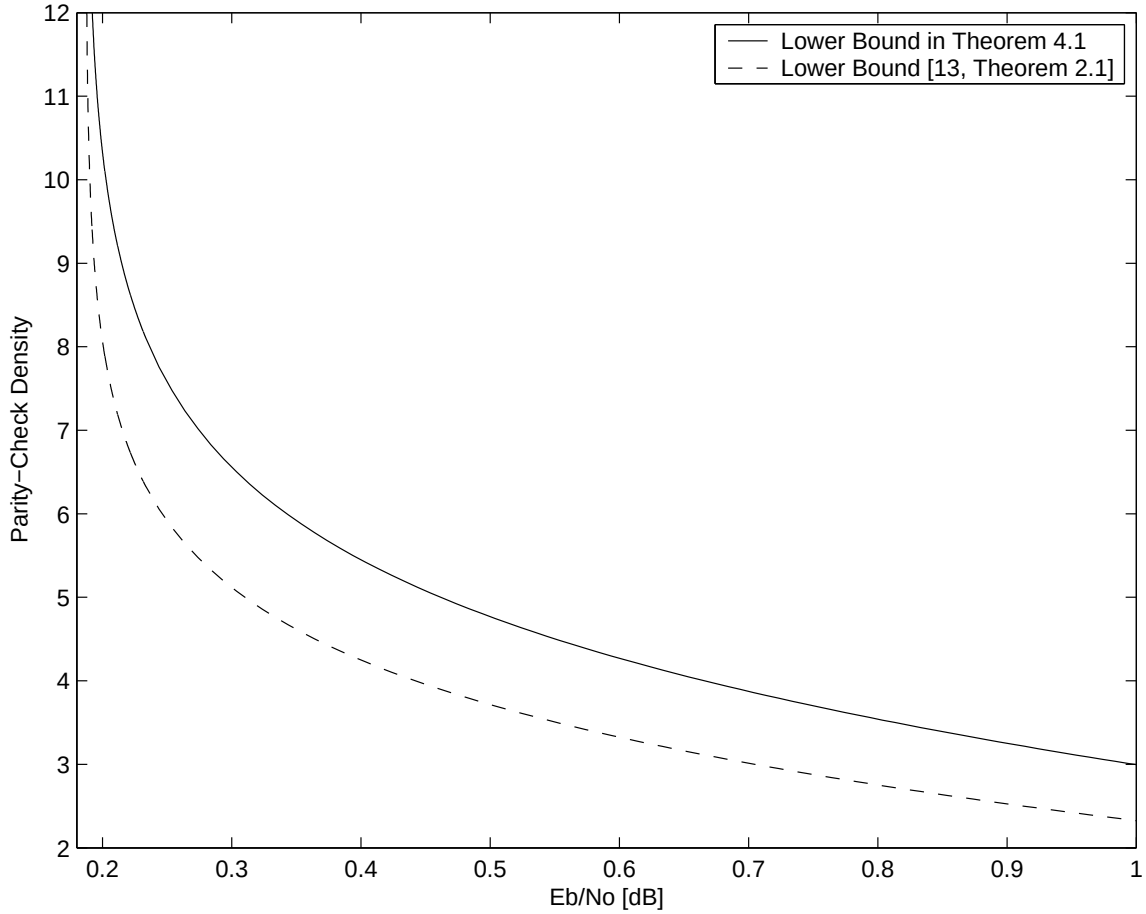
Numerical Results: Thresholds

- 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.



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.

Papers and Continuation of the Work

- The full paper is submitted to *IEEE Transactions on Information Theory* (May 2005).
- Both the full paper version and the Allerton conference version are at:

  `http://www.ee.technion.ac.il/people/sason/` and the ArXiv.
- The 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 is submitted to IEEE Trans. on IT, August 2005, and available in the ArXiv and in Sason's home page).

Thank you for your attention !