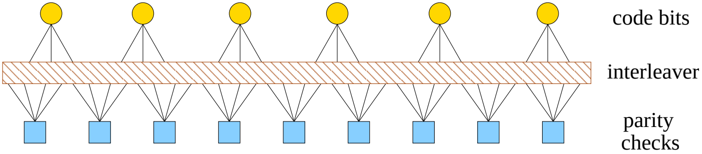
Information-Theoretic Bounds on the Parity-Check Density of LDPC Codes: Old and New Results

Igal Sason (Technion)

Joint Work with

Ruediger Urbanke (EPFL)   Gil Wiechman (Technion)

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

Low-Density Parity-Check Codes (Cont.)

- 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.

Fundamental Questions Regarding LDPC Codes

Question

How good can LDPC codes be, even under ML Decoding ?

Answer to this question ⇒

- Quantitative measure of the inherent loss of sub-optimal and practical iterative message-passing decoding algorithms.

Fundamental Questions Regarding LDPC Codes

Question

How good can LDPC codes be, even under ML Decoding ?

Answer to this question ⇒

- Quantitative measure of the inherent loss of sub-optimal and practical iterative message-passing decoding algorithms.

Question

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

Answer to this question⇒

- Lower bounds on the decoding complexity per iteration.
- Quantitative measure to the statement that bipartite graphs representing good codes have cycles (even under ML decoding).

Information-Theoretic Bounds on Achievable Rates

- Gallager: Right-regular LDPC codes cannot achieve capacity on a BSC, even under ML decoding (Ph.D. dissertation, 1961).

  Gap to capacity decreases to zero exponentially fast in a_{R}.
- Burshtein *et al.* generalized Gallager's bound for MBIOS channels (IEEE Trans. on IT, September 02).
- Etzion *et al.* showed that cycle-free codes are bad even under ML decoding (IEEE Trans. on IT, September 99).

Bounds referring to ensemble averages

- 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, IEEE Trans. on IT, September 05).
- These results are valid for ensembles and not code by code. Based on concentration arguments, they asymptotically hold in probability 1.

Information-Theoretic Bounds on Parity-Check Density

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

Information-Theoretic Bounds on Parity-Check Density

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

Conjecture (Khandekar and McEliece, ISIT 2001)

For LDPC codes over MBIOS channels, $\chi_D(\varepsilon) = O\left(\frac{1}{\varepsilon} \ln \frac{1}{\varepsilon}\right)$,
but for the BEC $\chi_D(\varepsilon) = O\left(\ln \frac{1}{\varepsilon}\right)$

Parity-Check Density

Definition

- Let $\mathcal{C}$ 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 $nR\Delta$.

Theorem (Sason and Urbanke, IEEE Trans. on IT, July '03)

Let $\{\mathcal{C}_m\}$ *be a sequence of binary linear block codes achieving a fraction* $1-\varepsilon$ *of the capacity of a memoryless binary-input output-symmetric (MBIOS) channel with vanishing* bit error probability. *Then for every sequence of codes and any representation of the codes by full-rank parity-check matrices*

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

where

$$K_1 = \frac{(1-C)\cdot\ln\left(\frac{1}{2\ln 2}\cdot\frac{1-C}{C}\right)}{2C\cdot\ln\left(\frac{1}{1-2w}\right)} \qquad K_2 = \frac{1-C}{2C\cdot\ln\left(\frac{1}{1-2w}\right)}.$$

Here, C is the capacity, and $w = \frac{1}{2}\int_{-\infty}^{\infty} \min\left(p(y|0), p(y|1)\right) dy$*.*

Theorem (Cont.)

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

$$\begin{aligned} K_1 &= \frac{p \cdot \ln\left(\frac{p}{1-p}\right)}{(1-p) \cdot \ln\left(\frac{1}{1-p}\right)}, \\ K_2 &= \frac{p}{(1-p) \cdot \ln\left(\frac{1}{1-p}\right)} \end{aligned}$$

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 (Cont.)

Question

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

Some More Questions (Cont.)

Question

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

Question

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

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

Question

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

Is the new bound on the parity-check density tight for the BEC ?

Gallager's Ensembles of Regular LDPC Codes

Theorem (Sason and Urbanke, IEEE Trans. on IT, July '03)

For every memoryless binary-input output-symmetric channel, there exists a sequence of Gallager's 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 some constants which only depend on the channel.*

Gallager's Ensembles of Regular LDPC Codes

Theorem (Sason and Urbanke, IEEE Trans. on IT, July '03)

For every memoryless binary-input output-symmetric channel, there exists a sequence of Gallager's 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 some constants which only depend on the channel.*

$\Rightarrow$ The general 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

$$\begin{aligned}\lambda_{\alpha,N}(x) &= \frac{\alpha \sum_{k=1}^{N-1} \binom{\alpha}{k} (-1)^{k+1} x^k}{\alpha - N \binom{\alpha}{N} (-1)^{N+1}} \\ \rho_\alpha(x) &= x^{\frac{1}{\alpha}} \, , \quad 0 < \alpha < 1 \, .\end{aligned}$$

Right-Regular LDPC Ensembles (Cont.)

Theorem (Sason and Urbanke, IEEE Trans. on IT, July 2003)

For suitable parameters of α *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*

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

Right-Regular LDPC Ensembles (Cont.)

Theorem (Sason and Urbanke, IEEE Trans. on IT, July 2003)

For suitable parameters of α *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*

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

⇒ Answering Question no. 5 in the affirmative: The improved bound for the BEC (see Theorem 1) is tight as the gap to capacity vanishes !

Interim Conclusions

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

Interim Conclusions

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

Question

Can better tradeoffs 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) ?

Interim Conclusions

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

Question

Can better tradeoffs 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) ?

- Pfister et al. showed that, fortunately, a better tradeoff can be achieved by introducing state nodes in the graph (e.g., punctured bits). For the BEC, ensembles of irregular repeat-accumulate (IRA) codes and variants were constructed so that they achieve capacity with bounded complexity per information bit.

Discussion (Cont.)

Question

Is it possible to improve the tightness of the lower bound in Theorem 1 for the family of memoryless binary-input output-symmetric channels ?

Discussion (Cont.)

Question

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 !

Motivation

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

- Is it possible to generalize the results for a finer quantization which gives a more accurate representation of the MBIOS channel ?
- Is it possible to derive a bound directly for the original (or an equivalent) channel ?

The second part of this work replies both questions in the affirmative, based on a recent joint work with Mr. Gil Wiechman.

The Un-Quantized Approach

- Define an *equivalent* channel whose output is the LLR of the original communication channel.
- LLR is divided into sign and absolute value.
- For the characterization of the equivalent channel, let the function a designate the conditional *pdf* of the LLR given that the channel input is zero.
- We randomly generate an i.i.d. sequence $\{L_i\}_{i=1}^{n}$ w.r.t. the conditional *pdf* a, and define

$$\Omega_i \triangleq |L_i|, \quad \Theta_i \triangleq \begin{cases} 0 & \text{if} \quad L_i > 0 \\ 1 & \text{if} \quad L_i < 0 \\ 0 \text{ or } 1 \text{ w.p. } \frac{1}{2} & \text{if} \quad L_i = 0 \end{cases}.$$

The Un-Quantized Approach (Cont.)

- The output of the equivalent channel is $\widetilde{\mathbf{Y}} = (\widetilde{Y}_1, \ldots, \widetilde{Y}_n)$ where
$$\widetilde{Y}_i = (\Phi_i, \Omega_i), \quad i = 1, \ldots, n$$
and $\Phi_i = \Theta_i + X_i$ where this addition is modulo-2.
- The output of this equivalent channel at time i is therefore the pair (Φ_i, Ω_i) where $\Phi_i \in \{0, 1\}$ and $\Omega_i \in \mathbb{R}^+$.
- This defines the memoryless mapping
$$X \rightarrow \widetilde{Y} \triangleq (\Phi, \Omega)$$
where Φ is a binary random variable which is affected by X, and Ω is a non-negative random variable which is not affected by X.
- Due to the symmetry of the communication channel
$$f_\Omega(\omega) = \begin{cases} a(\omega) + a(-\omega) = (1 + e^{-\omega})\, a(\omega) & \text{if } \omega > 0 \\ a(0) & \text{if } \omega = 0. \end{cases}$$

"Un-Quantized" Lower Bound on Conditional Entropy

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

- **X** and **Y** - 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

$$\begin{aligned} H(\mathbf{X}|\mathbf{Y}) &= H(\mathbf{X}|\widetilde{\mathbf{Y}}) \\ &= H(\mathbf{X}) + H(\widetilde{\mathbf{Y}}|\mathbf{X}) - H(\widetilde{\mathbf{Y}}) \\ &= nR + nH(\widetilde{Y}_1|X_1) - H(\widetilde{\mathbf{Y}}) \\ &= nR + n[H(\widetilde{Y}_1) - I(X_1;\widetilde{Y}_1)] - H(\mathbf{Y}) \end{aligned}$$

- $I(X_1;\widetilde{Y}_1) = I(X_1;Y_1) \leq C$

"Un-Quantized" Lower Bound on Conditional Entropy

- $$\begin{aligned} H(\widetilde{Y}) &= H(\Phi, \Omega) \\ &= H(\Omega) + H(\Phi|\Omega) \\ &= H(\Omega) + 1. \end{aligned}$$

  The last transition is due to the fact that given the absolute value of the LLR, its sign is equally likely to be positive or negative. The entropy $H(\Omega)$ is not expressed explicitly as it will cancel out later.

- $$\begin{aligned} H(\widetilde{\mathbf{Y}}) &= H\big(\Phi_1, \Omega_1, \ldots, \Phi_n, \Omega_n\big) \\ &= H(\Omega_1, \ldots, \Omega_n) + H\big(\Phi_1, \ldots, \Phi_n \mid \Omega_1, \ldots, \Omega_n\big) \\ &= nH(\Omega) + H\big(\Phi_1, \ldots, \Phi_n \mid \Omega_1, \ldots, \Omega_n\big). \end{aligned}$$

"Un-Quantized" Lower Bound on Conditional Entropy (Cont.)

- Define the syndrome vector $\mathbf{S} = (\Phi_1, \ldots, \Phi_n)H^T$ where H is an arbitrary full-rank parity-check matrix of $\mathcal{C}$.
- Let M be the index of the vector $(\Phi_1, \ldots, \Phi_n)$ in the coset.
- $H(M) = nR$, and we get

$$\begin{aligned} & H\big((\Phi_1, \ldots, \Phi_n) \,|\, (\Omega_1, \ldots, \Omega_n)\big) \\ & = H\big(\mathbf{S}, M \,|\, (\Omega_1, \ldots, \Omega_n)\big) \\ & \leq H(M) + H\big(\mathbf{S} \,|\, (\Omega_1, \ldots, \Omega_n)\big) \\ & \leq nR + \sum_{j=1}^{n(1-R)} H\big(S_j \,|\, (\Omega_1, \ldots, \Omega_n)\big). \end{aligned}$$

- Since $\mathbf{X}H^T = \mathbf{0}$ for any codeword $\mathbf{X}$, and $\Phi_i = X_i + \Theta_i$ for all i, then $\mathbf{S} = (\Theta_1, \ldots, \Theta_n)H^T$ which is independent of the transmitted codeword.

"Un-Quantized" Lower Bound on Conditional Entropy (Cont.)

This gives:

$$H(\mathbf{X}|\mathbf{Y}) \geq n(1-C) - \sum_{j=1}^{n(1-R)} H(S_j \big| \Omega_1, \ldots, \Omega_n)$$

"Un-Quantized" Lower Bound on Conditional Entropy (Cont.)

This gives:

$$H(\mathbf{X}|\mathbf{Y}) \geq n(1-C) - \sum_{j=1}^{n(1-R)} H(S_j \big| \Omega_1, \ldots, \Omega_n)$$

- $S_j = 1$ if and only if $\Theta_i = 1$ for an odd number of i's in the j'th parity-check equation.
- Due to the symmetry of the channel

$$P(\alpha_i) \triangleq P(\Theta_i = 1 \big| \Omega_i = \alpha_i) = \frac{1}{1+e^{\alpha_i}}.$$

"Un-Quantized" Lower Bound on Conditional Entropy (Cont.)

Lemma

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

$$\begin{aligned} P(S_j &= 1 \big| \Omega_{i_1} = \alpha_1, \ldots, \Omega_{i_k} = \alpha_k) \\ &= \frac{1}{2}\left[1 - \prod_{m=1}^{k} \left(1 - 2P(\alpha_m)\right)\right] \end{aligned}$$

where

$$1 - 2P(\alpha) = \tanh\left(\frac{\alpha}{2}\right).$$

"Un-Quantized" Lower Bound on Conditional Entropy

- For an arbitrary full-rank parity-check matrix of a binary linear block code $\mathcal{C}$:
  - Γ_k – fraction of parity-checks involving k variables
  - $\Gamma(x) \triangleq \sum_k \Gamma_k x^k$.

"Un-Quantized" Lower Bound on Conditional Entropy

- For an arbitrary full-rank parity-check matrix of a binary linear block code $\mathcal{C}$:
  - Γ_k – fraction of parity-checks involving k variables
  - $\Gamma(x) \triangleq \sum_k \Gamma_k x^k$.
- For a parity-check equation of degree k, the conditional entropy $H(S_j \big| \Omega_1, \ldots, \Omega_n)$ is given by the k-dimensional integral:

$$\int_0^\infty \ldots \int_0^\infty h_2\left(\frac{1}{2}\left[1 - \prod_{m=1}^{k} \tanh\left(\frac{\alpha_m}{2}\right)\right]\right) \prod_{m=1}^{k} f_\Omega(\alpha_m) d\alpha_1 \ldots d\alpha_k$$

where f_Ω designates the *pdf* of the absolute value of the LLR, and h_2 designates the binary entropy function to base 2.

"Un-Quantized" Lower Bound on Conditional Entropy

- For an arbitrary full-rank parity-check matrix of a binary linear block code $\mathcal{C}$:
  - Γ_k – fraction of parity-checks involving k variables
  - $\Gamma(x) \triangleq \sum_k \Gamma_k x^k$.
- For a parity-check equation of degree k, the conditional entropy $H(S_j \big| \Omega_1, \ldots, \Omega_n)$ is given by the k-dimensional integral:

$$\int_0^\infty \ldots \int_0^\infty h_2\left(\frac{1}{2}\left[1 - \prod_{m=1}^{k} \tanh\left(\frac{\alpha_m}{2}\right)\right]\right) \prod_{m=1}^{k} f_\Omega(\alpha_m) d\alpha_1 \ldots d\alpha_k$$

  where f_Ω designates the *pdf* of the absolute value of the LLR, and h_2 designates the binary entropy function to base 2.
- Applying the Taylor series for h_2 (around one-half) transforms it to a <u>one-dimensional</u> integral raised to the k'th power.

"Un-Quantized" Lower Bound on Conditional Entropy

Theorem

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

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

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

where a denotes the pdf *of the LLR given that the transmitted symbol is 0, and n is the block length of the code* $\mathcal{C}$*.*

Sequences of Codes

- From Fano's inequality, for a sequence of codes vanishing bit error probability we get
$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \longrightarrow 0$$
- The bound on conditional entropy yields an upper bound on the asymptotic achievable rate.
- Assume $R = (1 - \varepsilon)C$. Using convexity arguments, we get a lower bound on the asymptotic parity-check density.

"Un-Quantized" Upper Bound on Achievable Rates

Let $\{\mathcal{C}_m\}$ be a sequence of binary linear block codes, and assume

- Communication over an MBIOS channel with capacity $C \ \frac{\text{bits}}{\text{ch. use}}$.
- The block length tends to infinity as $m \to \infty$

Theorem

A necessary condition for this sequence to achieve vanishing bit error probability as $m \to \infty$ is that the asymptotic rate R 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.

"Un-Quantized" Lower Bound on Parity-Check Density

Let $\{\mathcal{C}_m\}$ be a sequence of binary linear block codes, and assume

- Communication over an MBIOS channel with capacity $C \ \frac{\text{bits}}{\text{ch. use}}$.
- The sequence $\{\mathcal{C}_m\}$ achieves a fraction $1 - \varepsilon$ of the channel capacity with vanishing bit error probability.

"Un-Quantized" Lower Bound on Parity-Check Density

Theorem

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

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

g_1 is introduced above, and

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

Notes on "Un-Quantized" Bounds

- No optimization of quantization levels ⇒ rapid calculation.
- Tighter than the bounds derived for quantized channels, regardless of the number of quantization levels.
- For the BEC, the lower bound on the asymptotic parity-check density merges with the bound of Sason and Urbanke, which was shown to be tight.
- The theorems are valid when considering LDPC ensembles and replacing the rate with the design rate of the ensemble. In that case, it is not required that the parity-check matrices are full rank.

Numerical Results: Thresholds

Comparison of the bounds for rate-1/2 irregular LDPC-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	Lower Bounds				DE Threshold
	2-Level	4-Level	8-Level	Un-Quantized	
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: Thresholds (Cont.)

Question

Does it make sense that the bounds on the thresholds become more pessimistic as the number of quantization levels is increased (as we can see from the table in the previous slide) ?

Answer

Note that the "quantized bounds" rely on quantized values of the LLR as side information used for the derivation of these bounds, but the channel itself is not quantized. Hence, by increasing the number of quantization levels used for these bounds, the corresponding values of the $\frac{E_b}{N_0}$ *thresholds under ML decoding get farther from the channel capacity.*

Numerical Results: Thresholds (Cont.)

- Numerical results refer to the following ensembles of irregular LPDC codes of rate $\frac{1}{2}$
  1. $\lambda(x) = 0.38354x + 0.04237x^2 + 0.57409x^3, \quad \rho(x) = 0.24123x^4 + 0.75877x^5$
  2. $\lambda(x) = 0.23802x + 0.20997x^2 + 0.03492x^3 + 0.12015x^4 + 0.01587x^6 + 0.00480x^{13} + 0.37627x^{14}, \quad \rho(x) = 0.98013x^7 + 0.01987x^8$
  3. $\lambda(x) = 0.21991x + 0.23328x^2 + 0.02058x^3 + 0.08543x^5 + 0.06540x^6 + 0.04767x^7 + 0.01912x^8 + 0.08064x^{18} + 0.22798x^{19}, \quad \rho(x) = 0.64854x^7 + 0.34747x^8 + 0.00399x^9$
  4. $\lambda(x) = 0.19606x + 0.24039x^2 + 0.00228x^5 + 0.05516x^6 + 0.16602x^7 + 0.04088x^8 + 0.01064x^9 + 0.00221x^{27} + 0.28636x^{29}, \quad \rho(x) = 0.00749x^7 + 0.99101x^8 + 0.00150x^9$
- $\lambda_2 > 0$ for all ensembles.
- taken from `http://lthcwww.epfl.ch/research/ldpcopt/index.php`

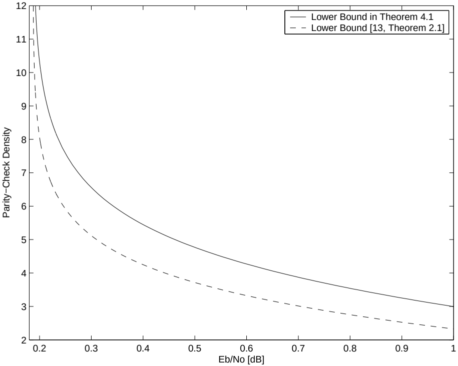
Numerical Results: Parity-Check Density

Setup

- AWGN Channel
- Rate = $\frac{1}{2}$

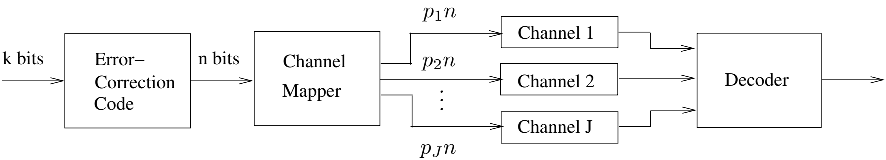
Observations

- Difference between bounds increases as ε decreases.
- As $\frac{E_\mathrm{b}}{N_\mathrm{o}} \to 0.187$ dB ($C = \frac{1}{2}$) the bounds tend to infinity.
- The lower bounds and their difference behave like ln $\left(\frac{1}{\varepsilon}\right)$.



Parallel Channels

- Transmission takes place over a set of J independent memoryless binary-input output-symmetric (MBIOS) channels.
- Each code bit is a-priori assigned to one of the J channels.
- A fraction p_j of the code bits is transmitted over the j'th channel.



Why Parallel Channels ?

Parallel channels are used to model various scenarios:

- Punctured LDPC codes.
- Non-uniformly error protected codes.
- Multi-level codes.
- LDPC coded modulation.
- etc.

Related Work

Bounds for punctured codes

- Pfister *et al.* extended the bounds of Sason & Urbanke to randomly punctured codes on graphs (IEEE Trans. on IT, July 05).

Bounds for parallel MBIOS channels

- Pishro-Nik *et al.* considered unequal error protection and derived an upper bound on the achievable rates for LDPC ensembles transmitted over parallel BECs (IEEE Trans. on IT, July 05).
- Liu *et al.* derived inner bounds on the attainable channel regions for parallel MBIOS channels via Gallager bounds (IEEE Trans. on IT, April 06).
- These inner bounds were recently improved by Goldenberg & Sason (submitted to the IEEE Trans. on Information Theory, June 2006).

Lower Bound on Cond. Entropy for Parallel Channels

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

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

Lower Bound on Cond. Entropy for Parallel Channels

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

Theorem

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

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

where

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

Is it just a trivial generalization of the bounds for a single MBIOS channel?

Problem

The values $\beta_{j,m}$ are not usually known.
Therefore the bound cannot be practically evaluated for specific codes.

Is it just a trivial generalization of the bounds for a single MBIOS channel?

Problem

The values $\beta_{j,m}$ are not usually known.
Therefore the bound cannot be practically evaluated for specific codes.

Solution

Consider the expected conditional entropy over an ensemble of codes.

Is it just a trivial generalization of the bounds for a single MBIOS channel?

Problem

The calculation of the expectation over the bound is not tractable

Is it just a trivial generalization of the bounds for a single MBIOS channel?

Problem

The calculation of the expectation over the bound is not tractable

Suggestion

Bound the expectation using Jensen's inequality.
Leads to an inherent loss in the tightness of the bounds.

Is it just a trivial generalization of the bounds for a single MBIOS channel?

Problem

The calculation of the expectation over the bound is not tractable

Observation

- We only consider sequences of ensembles where $n \to \infty$.
- We only need the limit of the expectation when $n \to \infty$.

Is it just a trivial generalization of the bounds for a single MBIOS channel?

Problem

The calculation of the expectation over the bound is not tractable

Observation

- We only consider sequences of ensembles where $n \to \infty$.
- We only need the limit of the expectation when $n \to \infty$.

- The calculation of the limit is possible !
- The following bounds are valid only for sequences of ensembles.

Upper Bound on the Achievable Rates

Consider a sequence of LDPC ensembles, whose block lengths tend to infinity.

- Transmission over J parallel MBIOS channels.
  Capacity of j'th channel: C_j bits/ch. use.
- p_j denotes the asymptotic fraction of code bits transmitted over the j'th channel.
- q_j denotes the asymptotic fraction of edges in graph connected to code bits transmitted over the j'th channel.

Upper Bound on the Achievable Rates

Theorem

A necessary condition for this sequence to achieve vanishing bit error probability (even under ML decoding) is that the design rate R_d satisfies

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

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

Example: Parallel BECs

Example

For the particular case where the J parallel MBIOS channels are BECs where the erasure probability of the j^{th} channel is ε_j, the common design rate of the sequence of LDPC ensembles is upper bounded by

$$R_{\mathrm{d}} \leq 1 - \frac{\displaystyle\sum_{j=1}^{J} p_j \varepsilon_j}{1 - \Gamma\left(1 - \displaystyle\sum_{j=1}^{J} q_j\ \varepsilon_j\right)} \ .$$

This coincides with [Pishro-Nik et al. IEEE Trans. on IT, July 05].

Lower Bound on the Parity Check Density

- Consider a sequence of LDPC ensembles, whose block lengths tend to infinity.
- Assume this sequence achieves a fraction $1 - \varepsilon$ of the average capacity $\overline{C} \triangleq \sum_{j=1}^{J} p_j C_j$ with vanishing bit-error probability.

Theorem

The asymptotic density of their parity-check matrices satisfies

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

where K_1 and K_2 are coefficients which depend on the *pdf*s of the J parallel channels and on the values of p_j and q_j.

- Same form as the bound for a single MBIOS channel.

Application: Intentionally Punctured LDPC Codes

- Introduced by Ha and McLaughlin (IEEE Trans. on IT, November 04)
- Code bits are separated according to the degree of the corresponding node.
- Each set is punctured at a different rate.

Application: Intentionally Punctured LDPC Codes

Intentional puncturing can be modeled as transmission over a set of parallel channels.

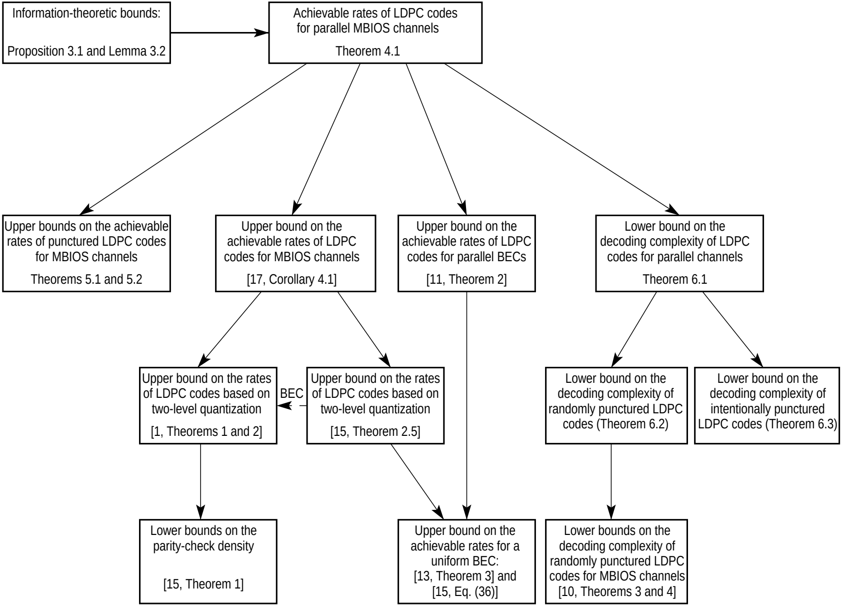
- Each channel transmits bits whose corresponding nodes have a fixed degree.
- The channels are composed of a concatenation of a BEC (which models the puncturing) and the communication channel.
- The fraction q_j of edges transmitted over channel j depends on the left degree distribution of the ensemble.
- The bounds depend on both the left and right degree distributions.

Numerical Results

- 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 cap. (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%

Connections with Previously Reported Results



Information-theoretic bounds:

Proposition 3.1 and Lemma 3.2

Achievable rates of LDPC codes for parallel MBIOS channels

Theorem 4.1

Upper bounds on the achievable rates of punctured LDPC codes for MBIOS channels

Theorems 5.1 and 5.2

Upper bound on the achievable rates of LDPC codes for MBIOS channels

[17, Corollary 4.1]

Upper bound on the achievable rates of LDPC codes for parallel BECs

[11, Theorem 2]

Lower bound on the decoding complexity of LDPC codes for parallel channels

Theorem 6.1

Upper bound on the rates of LDPC codes based on two-level quantization

[1, Theorems 1 and 2]

Upper bound on the rates of LDPC codes based on two-level quantization

[15, Theorem 2.5]

Lower bound on the decoding complexity of randomly punctured LDPC codes (Theorem 6.2)

Lower bound on the decoding complexity of intentionally punctured LDPC codes (Theorem 6.3)

Lower bounds on the parity-check density

[15, Theorem 1]

Upper bound on the achievable rates for a uniform BEC:
[13, Theorem 3] and
[15, Eq. (36)]

Lower bounds on the decoding complexity of randomly punctured LDPC codes for MBIOS channels
[10, Theorems 3 and 4]

Summary

- Improved information-theoretic bounds on the thresholds and parity-check density of binary linear block codes.
- Lower bounds on the parity-check density enable to assess the tradeoff between performance and complexity per iteration.
- Upper bounds on thresholds under ML and exact thresholds under iterative decoding enable to assess the inherent loss due to code structure and the sub-optimality of iterative decoding.
- Comparison of bounds for quantized and un-quantized channels 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 versus complexity tradeoff for ensembles of punctured LDPC codes.

Journal Papers Related to this Talk

- I. Sason and R. Urbanke, “Parity-check density versus performance of binary linear block codes over memoryless symmetric channels,” *IEEE Trans. on Information Theory*, vol. 49, no. 7, pp. 1611-1635, July 2003.
- G. Wiechman and I. Sason, “Parity-Check Density versus Performance of binary linear block codes over memoryless symmetric channels: New bounds and applications,” *IEEE Trans. on Information Theory*, vol. 53, no. 2, pp. 550–579, February 2007.
- I. Sason and G. Wiechman, “On achievable rates and complexity of LDPC codes over parallel channels: Bounds and applications,” *IEEE Trans. on Information Theory*, vol. 53, no. 2, pp. 580–598, February 2007.