Theoretic and Practical Aspects on the Performance versus Complexity Tradeoff for LDPC-Based Codes

Gil Wiechman

Supervised by Dr. Igal Sason

Department of Electrical Engineering
Technion - Israel Institute of Technology
Haifa 32000, Israel

January 14, 2008

Dissertation Overview

This work can generally be divided into two parts:

1. Aspects of the asymptotic tradeoff between performance and decoding complexity for graph-based codes.
2. Fundamental performance limitations of finite-length block codes.

On the asymptotic performance vs. complexity tradeoff

The research in this part is motivated by two core questions:

Question

How good can LDPC codes be, even under optimal decoding?

- This question is addressed via information-theoretic upper bounds on the achievable rates of optimally decoded binary linear block codes.
- The bounds refer to transmission over
  - A memoryless binary-input output-symmetric (MBIOS) channel.
  - A set of independent parallel MBIOS channels.

On the asymptotic performance vs. complexity tradeoff

The research in this part is motivated by two core questions:

Question

What are the fundamental limitations on the complexity of iterative decoding algorithms, as a function of the gap between the code rate and the channel capacity?

The complexity of iterative decoding algorithms is composed of two main factors:

- The graphical complexity of the Tanner graph representing the code (which serves to measure decoding complexity per iteration).
- The number of iterations required for successful decoding.

On the asymptotic performance vs. complexity tradeoff

The research in this part is motivated by two core questions:

Question

What are the fundamental limitations on the complexity of iterative decoding algorithms, as a function of the gap between the code rate and the channel capacity?

This question is addressed by deriving

- Information-theoretic lower bounds on the parity-check density of binary linear block codes
  - For memoryless binary-input output-symmetric (MBIOS) channels.
  - For parallel MBIOS channels with application to puncturing.
- Lower bounds on the number of decoding iterations for graph-based codes transmitted over the binary erasure channel.

Fundamental limitations of finite-length block codes

This study is performed by examining sphere-packing lower bounds on the block error probability.

We present

- A new sphere-packing bound for finite-length block codes transmitted over symmetric memoryless channels.
- A log-domain algorithm which facilitates the exact calculation of the 1959 sphere-packing bound regardless of the block length.

Parity-check density versus performance of binary linear block codes over memoryless symmetric channels: New bounds and applications

Related work - Achievable rates of LDPC codes

- Right-regular LDPC codes cannot achieve capacity on a BSC, even under ML decoding. Gap to capacity is lower bounded by an expression which decreases to zero exponentially fast in a_{R} (Gallager, 1961).
- Burshtein *et al.* generalized Gallager's bound for MBIOS channels (IEEE Trans. on IT, September 2002).
- Sason and Urbanke observed that Gallager's result holds when considering the *average* right degree of irregular ensembles. (IEEE Trans. on IT, July 2003).

Related work - Graphical Complexity

Goal: Achieving a fraction $1-\varepsilon$ of capacity.

Conjecture (Khandekar and McEliece, ISIT 2001)

For a large class of channels, if the design rate of a suitably designed ensemble forms a fraction $1-\varepsilon$ of the channel capacity, then the decoding complexity scales like $\frac{1}{\varepsilon}\ln\frac{1}{\varepsilon}$.

The logarithmic term in this expression is attributed to the graphical complexity (i.e., the decoding complexity per iteration) and the number of iterations scales like $\frac{1}{\varepsilon}$.

For the BEC, the absolute reliability of the messages allows every edge in the graph to be used only once during the iterative decoding so the decoding complexity behaves like $\ln\frac{1}{\varepsilon}$.

Related work - Graphical Complexity

Goal: Achieving a fraction $1-\varepsilon$ of capacity.

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

- For a sequence of binary linear block codes achieving a fraction $1-\varepsilon$ of the capacity of an MBIOS channel (under any 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 (for the right-regular ensembles introduced by Shokrollahi).

Motivation

- Previous work is based on applying a two-level quantization to the channel information.
  $\Rightarrow$ replaces information from the MBIOS channel with information from a physically-degraded BSC.
- Bounding technique depends on binary information by considering the syndrome of the information sequence.

Questions

1. Can we apply a finer quantization which gives a more accurate representation of the information available from the channel?
2. Can we work with the original (or equivalent) information?

In this work, we reply both questions in the affirmative.

Bounds without quantization of the channel information

- Define a new channel whose output is the LLR of the original.
- The LLR is equivalent to the original channel information.
- Channel symmetry property $\Rightarrow$ new channel is a multiplicative channel, where the binary input (converted to +1,-1) multiplies an independent noise (so it only effects the sign of the output).
- The noise is distributed according to the *pdf* of the LLR of the original channel, given that the transmitted symbol is 0.
- The absolute value of the output provides side info. on the noise.
- The syndrome is calculated w.r.t. the sign of the channel output.

Theorem ("Un-Quantized" Lower Bound on Conditional Entropy)

- Let $\mathcal{C}$ be a binary linear block code of length n and rate R.
  - Communication over an MBIOS channel with capacity $C \frac{\text{bits}}{\text{ch. use}}$.
  - $\mathbf{x}$, $\mathbf{y}$ – transmitted codeword and received sequence, respectively.
  - a – *pdf* of the LLR given that the transmitted symbol is 0.
  - For an arbitrary full-rank parity-check matrix of $\mathcal{C}$:
    Γ_k – fraction of the parity-checks involving k variables
    $\Gamma(x) \triangleq \sum_k \Gamma_k x^k$.

Theorem ("Un-Quantized" Lower Bound on Conditional Entropy)

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

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

where

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

Sequences of Codes

- From Fano's inequality, for a sequence of codes achieving vanishing bit error probability (under any decoding algorithm)

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

- Substituting this in the lower bound on conditional entropy and solving for R yields an upper bound on the achievable rates.

Sequences of Codes

- Assume also $R = (1-\varepsilon)C$, this gives:

$$
\begin{aligned}
0 &\geq 1 - C - (1-(1-\varepsilon)C)\left(1 - \frac{1}{2\ln(2)}\sum_{p=1}^{\infty}\frac{\Gamma(g_p)}{p(2p-1)}\right) \\
&\overset{g_p \geq 0}{\geq} 1 - C - (1-(1-\varepsilon)C)\left(1 - \frac{\Gamma(g_1)}{2\ln(2)}\right) \\
&\overset{\text{Jensen}}{\geq} 1 - C - (1-(1-\varepsilon)C)\left(1 - \frac{g_1^{a_R}}{2\ln(2)}\right)
\end{aligned}
$$

  where a_R is the average right degree of the sequence.

- The lower bound on the density of the considered parity-check matrix H follows from the equality $\Delta(H) = \frac{1-R}{R}\, a_R$.

Notes on the "Un-Quantized" Bounds

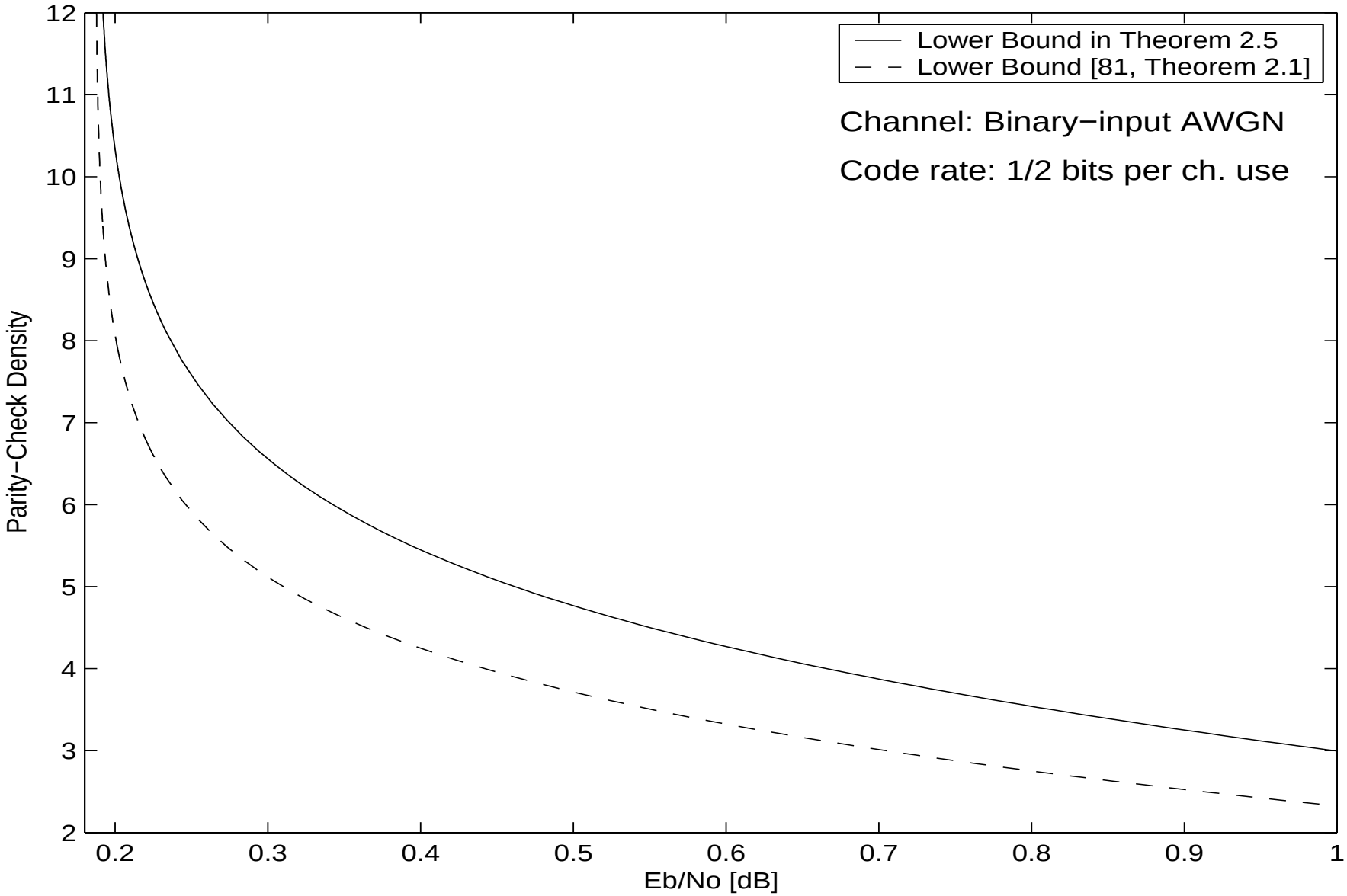
- The "un-quantized" bounds are not subject to optimization therefore their calculation is rapid.
- Tighter than the quantized bounds for any number of quantization levels.
- For the BEC, the "un-quantized" bound on the asymptotic parity-check density merges with the bound of Sason and Urbanke, which was shown to be tight.
- The bounds are valid when considering ensembles of LDPC 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
  - Binary-input AWGN Channel.
  - Average right degree increases with ensemble number.
  - Shannon capacity limit for $R = \frac{1}{2}$ is 0.187 dB
  - Provides bounds on loss due to message-passing 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

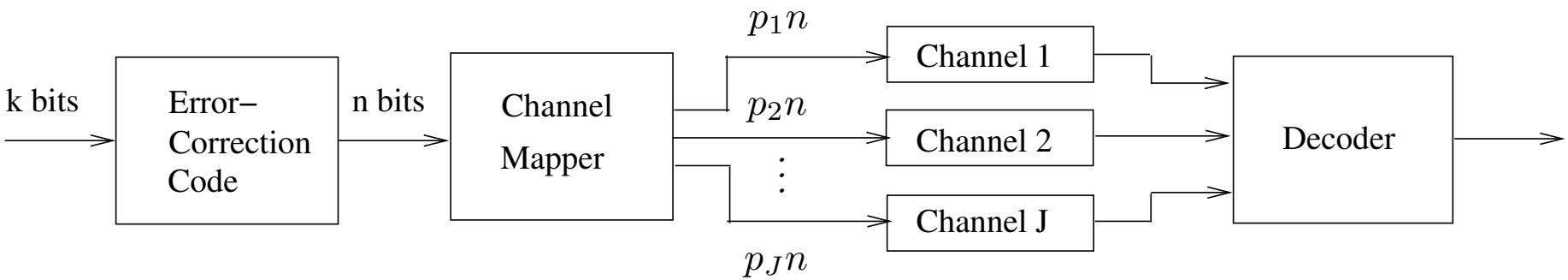
Numerical Results: Parity-Check Density



On achievable rates and complexity of LDPC codes over parallel channels: Bounds and applications

Parallel Channels

- Transmission takes place over J independent 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.

Lower Bound on Cond. Entropy for Parallel Channels

Theorem

Let $\mathcal{C}$ be a binary linear block code of length n and design rate R_{d}. The conditional entropy of the transmitted codeword given the received sequence satisfies

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

where

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

Notes

Problem

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

Notes

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.

Notes

Problem

The calculation of the expectation over the bound is not tractable

Notes

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.

Notes

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 $n \to \infty$.

Notes

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 resulting bounds are valid only for sequences of *ensembles.*

Intentionally punctured codes

- Introduced by Ha and McLaughlin (IEEE Trans. on IT, Nov. 2004).
  - Code bits are separated according to the degree of the corresponding node.
  - Each set is punctured at a different rate.
- 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.

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%

Bounds on the number of iterations for turbo-like ensembles over the binary erasure channel

Conjecture (Khandekar and McEliece, ISIT 2001)

For a large class of channels, if the design rate of a suitably designed ensemble forms a fraction $1-\varepsilon$ of the channel capacity, then the decoding complexity scales like $\frac{1}{\varepsilon}\ln\frac{1}{\varepsilon}$.

The logarithmic term in this expression is attributed to the graphical complexity (i.e., the decoding complexity per iteration) and the number of iterations scales like $\frac{1}{\varepsilon}$.

For the BEC, the absolute reliability of the messages allows every edge in the graph to be used only once during the iterative decoding so the decoding complexity behaves like $\ln\frac{1}{\varepsilon}$.

Theorem (Lower bound on the number of iterations for LDPC ensembles transmitted over the BEC)

Let $\left\{(n_m, \lambda, \rho)\right\}_{m \in \mathbb{N}}$ be a sequence of LDPC ensembles ($n_m \xrightarrow[m \to \infty]{} \infty$).

- Transmission over a BEC with erasure probability p.
- Assume that the sequence achieves $1 - \varepsilon$ of the channel capacity with vanishing bit erasure prob. under message-passing decoding.
- $L_2(\varepsilon)$ - fraction of variable nodes of degree 2.
- $I(\varepsilon, p, P_{\mathrm{b}})$ - number of iterations which is required to achieve an average bit erasure probability P_{b} over the ensemble.

Under the condition that $P_{\mathrm{b}} < p\, L_2(\varepsilon)$:

$$I(\varepsilon, p, P_{\mathrm{b}}) \geq \frac{2}{1-p} \left(\sqrt{p\, L_2(\varepsilon)} - \sqrt{P_{\mathrm{b}}} \right)^2 \frac{1}{\varepsilon}\,.$$

On the fraction of variable nodes of degree 2

- The lower bound on the number of iterations becomes trivial when $L_2(\varepsilon)$ vanishes.
- For various capacity-achieving sequences of LDPC ensembles $L_2(\varepsilon) \xrightarrow[\varepsilon \to \infty]{} \frac{1}{2}$.
- In fact, under some mild conditions, it can be proved that the fraction of degree-2 variable nodes for capacity-achieving LDPC ensembles is strictly positive (for more details, see Lemma 5 in a preprint of a paper by Sason, Sept. 2007).

On the fraction of variable nodes of degree 2

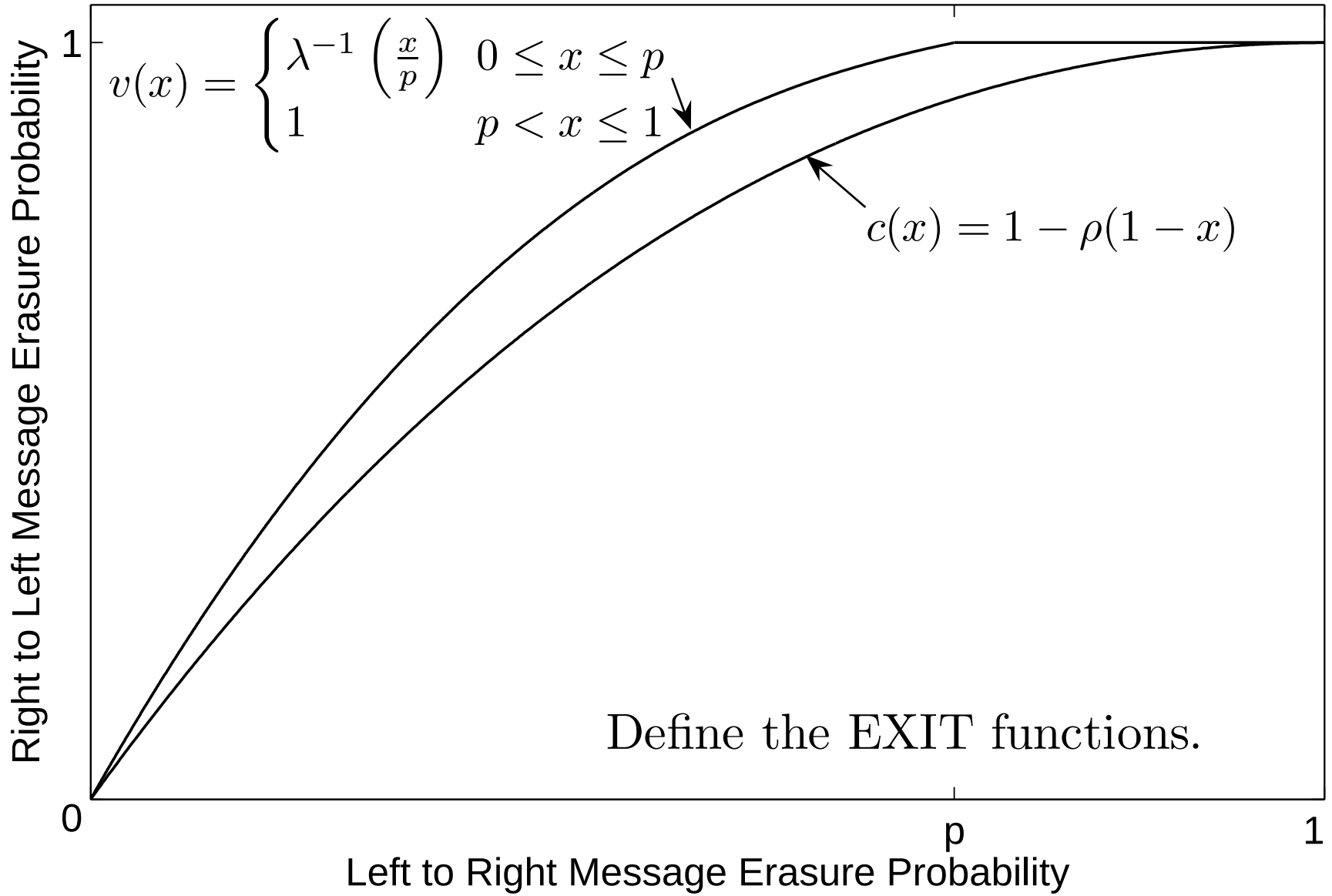
Corollary

If $L_2(\epsilon)$ does not vanish and $P_{\mathrm{b}} < p\, L_2(\varepsilon)$ then

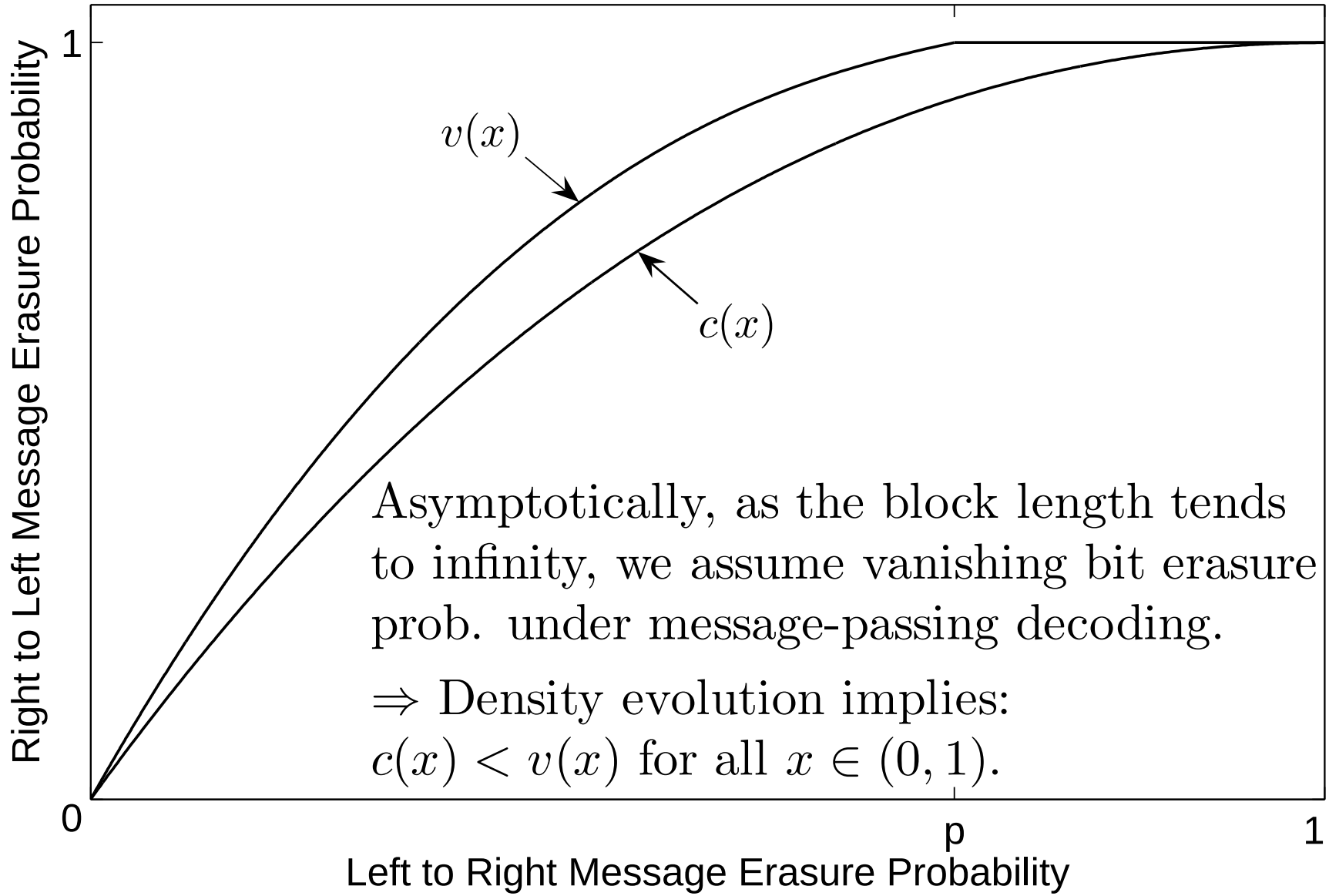
$$I(\varepsilon, p, P_{\mathrm{b}}) = \Omega\left(\frac{1}{\varepsilon}\right) .$$

This supports the conjecture by Khandekar and McEliece.

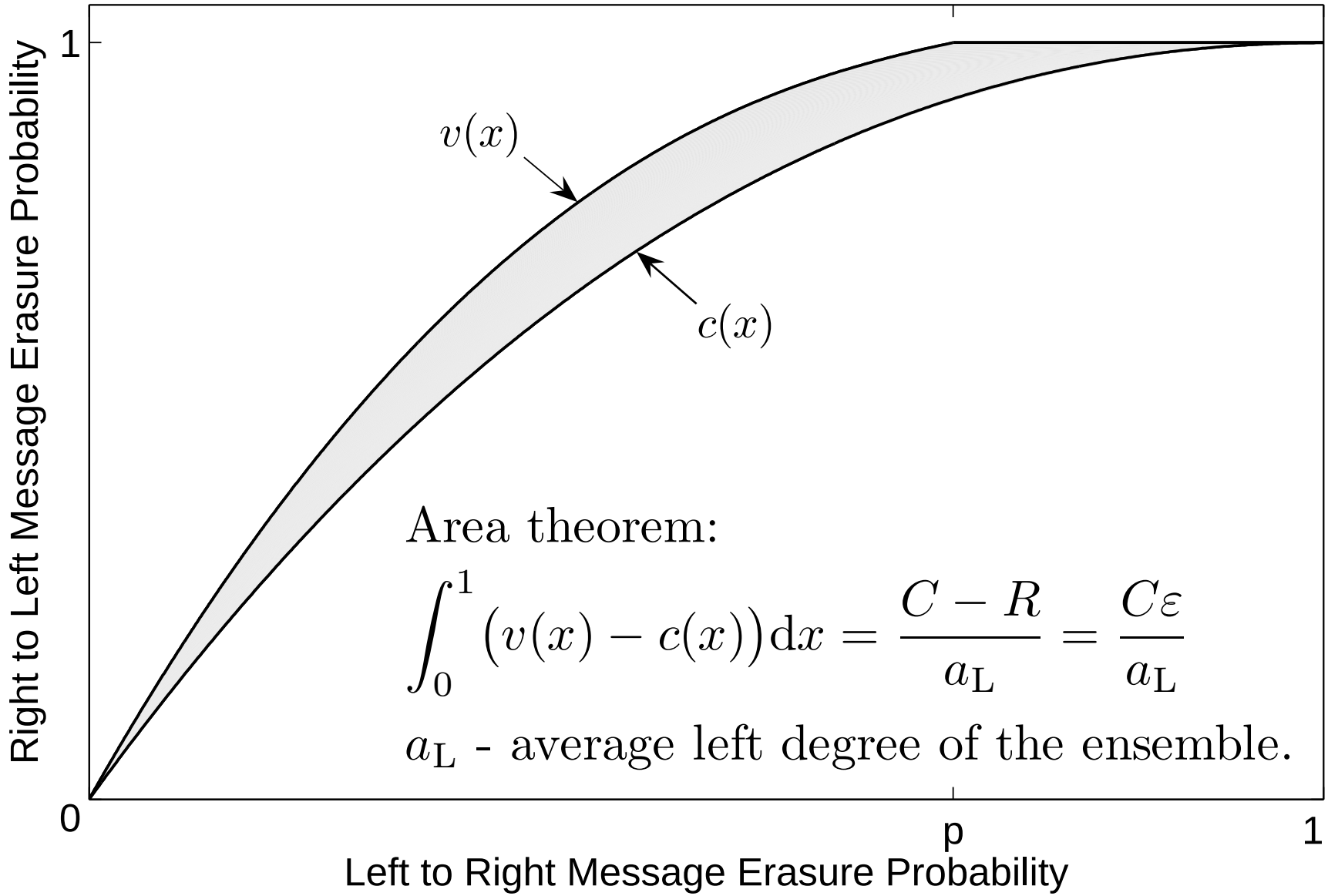
Proof Outline



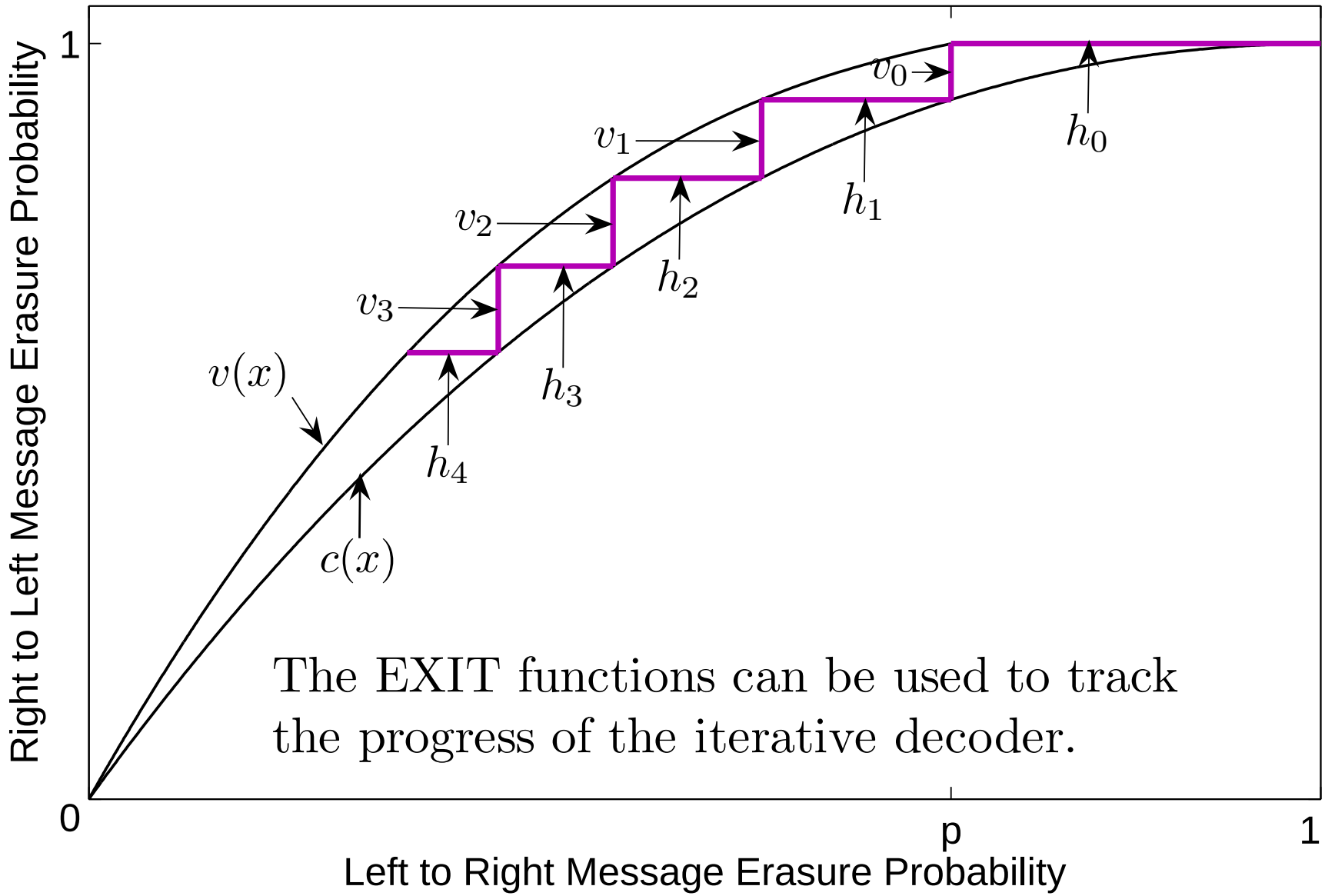
Proof Outline



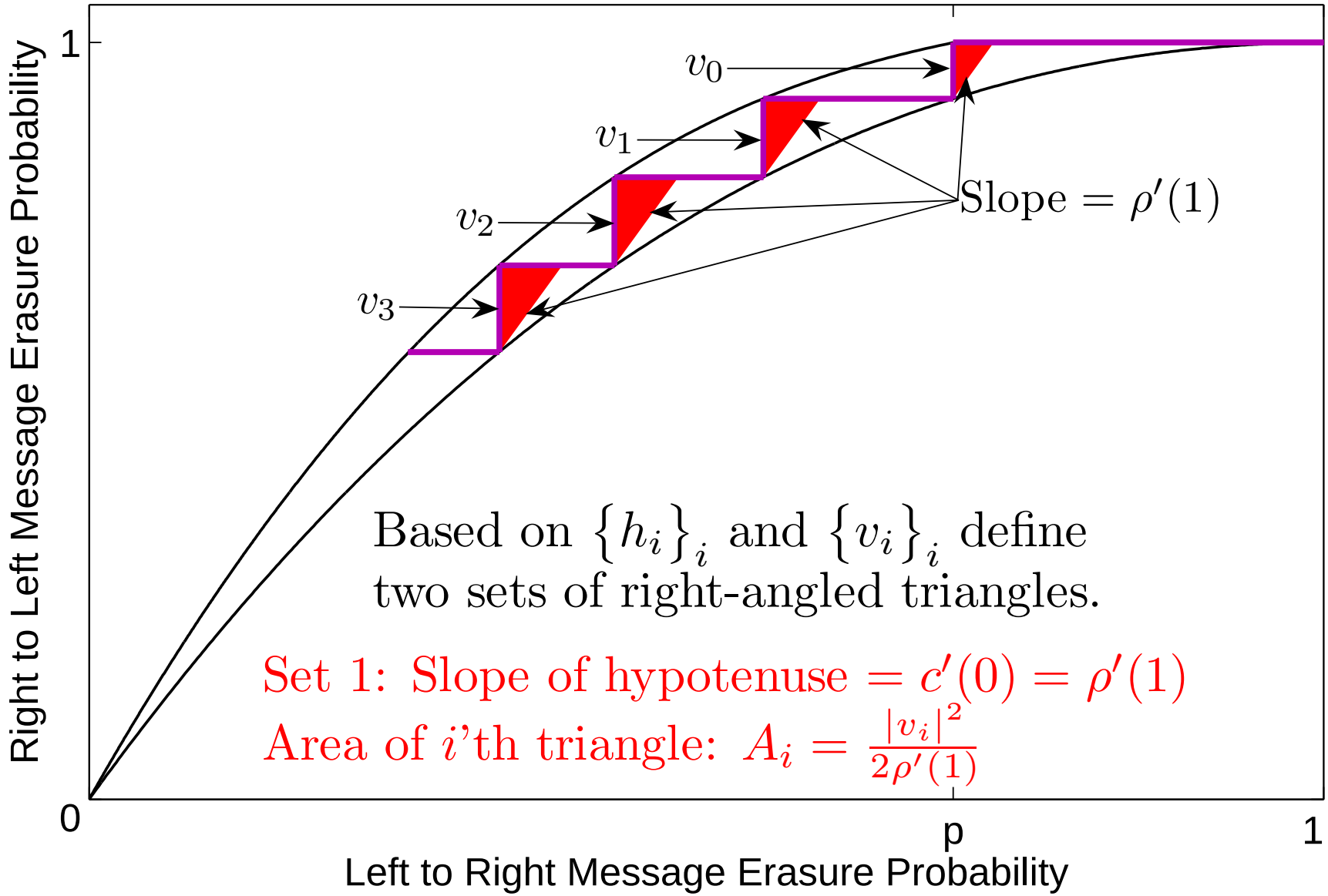
Proof Outline



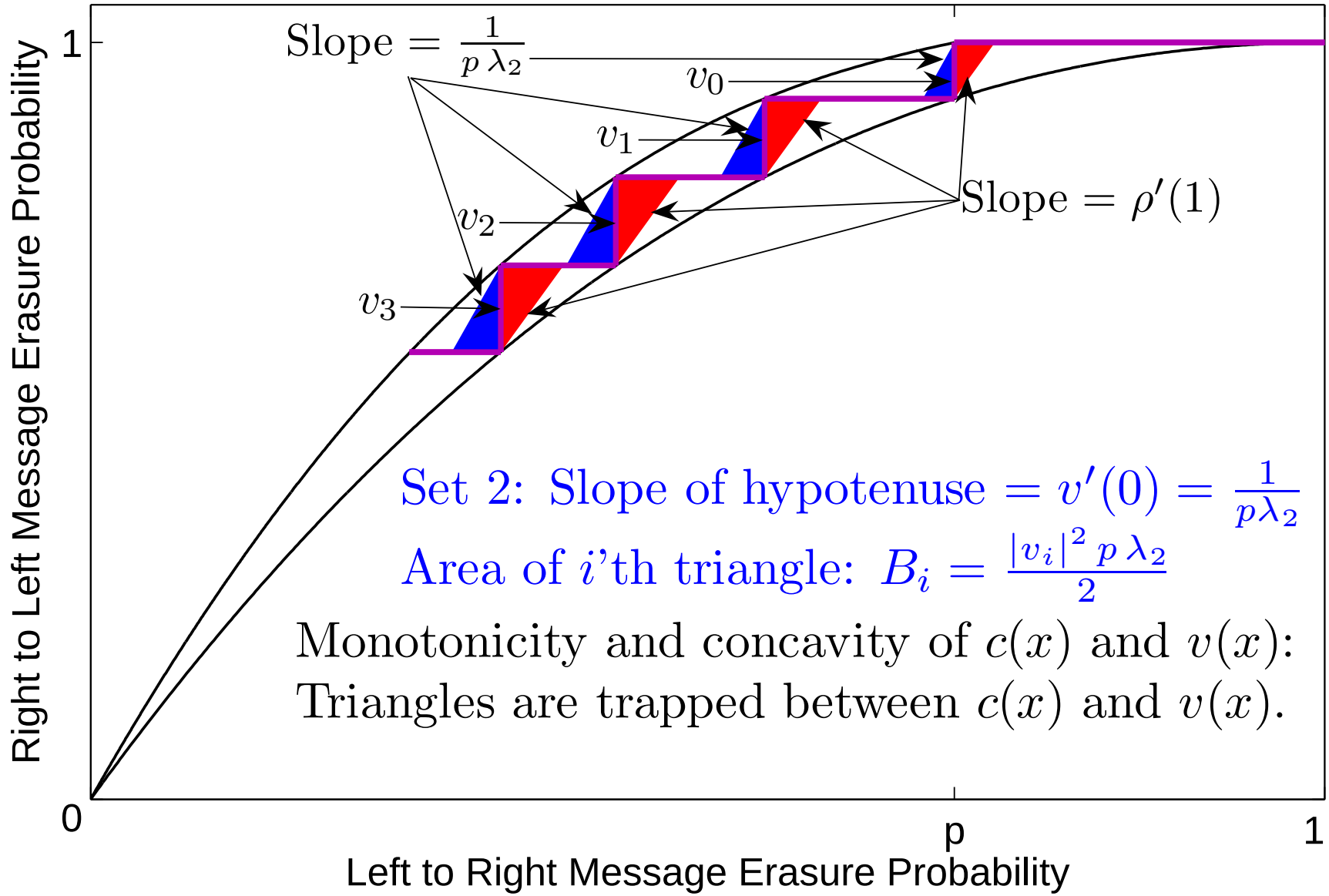
Proof Outline



Proof Outline



Proof Outline



Proof Outline (Cont.)

- Based on the previous statements and the stability condition

$$\frac{C\,\varepsilon}{a_{\mathsf{L}}} \geq \frac{1}{2}\left(\frac{1}{\rho'(1)} + p\lambda_2\right)\sum_{i=0}^{l-1}|v_i|^2$$

$$\geq p\lambda_2\sum_{i=0}^{l-1}|v_i|^2$$

  where l is an arbitrary natural number.

- Cauchy-Schwartz inequality: $\left(\sum_{i=0}^{l-1}|v_i|\right)^2 \leq l\sum_{i=0}^{l-1}|v_i|^2$

$$\Rightarrow \qquad C\,\varepsilon \geq \frac{a_{\mathsf{L}}\,p\lambda_2\left(\sum_{i=0}^{l-1}|v_i|\right)^2}{l}$$

Proof Outline (Cont.)

- l – Number of iterations required to achieve a bit erasure prob. P_{b}.
- Based on density evolution $\sum_{i=0}^{l-1} |v_i| \geq 1 - L^{-1}\left(\frac{P_{\mathrm{b}}}{p}\right)$.
- Substituting this and solving for l

$$
\begin{aligned}
l &\geq \frac{a_{\mathrm{L}}\, p \lambda_2 \left(1 - L^{-1}\left(\frac{P_{\mathrm{b}}}{p}\right)\right)^2}{(1-p)\varepsilon} \\
&\overset{(a)}{\geq} \frac{a_{\mathrm{L}}\, \lambda_2 \left(\sqrt{p\, L_2} - \sqrt{P_{\mathrm{b}}}\right)^2}{L_2\,(1-p)\varepsilon} \\
&\overset{(b)}{=} \frac{2}{1-p} \left(\sqrt{p\, L_2} - \sqrt{P_{\mathrm{b}}}\right)^2 \frac{1}{\varepsilon}\,.
\end{aligned}
$$

(a) follows since $L(x) \leq L_2\, x^2$ for $x > 0$ and also $P_{\mathrm{b}} < p\, L_2$.
(b) is based on the equality $a_{\mathrm{L}}\, \lambda_2 = 2\, L_2$

The graphical complexity perspective

In the asymptotic case where we let the block length tend to infinity

- The graphical complexity of capacity-approaching LDPC and systematic irregular repeat-accumulate (IRA) ensembles is un-bounded as the gap to capacity vanishes and scales at least like $\ln \frac{1}{\varepsilon}$ (Sason & Urbanke, Trans. on IT, 2003 and 2004).
- Adding state nodes to the graph enables an improved tradeoff:
  - Capacity-achieving ensembles of non-systematic IRA codes with bounded graphical complexity (Pfister et al., Trans. on IT, July 2005).
  - Capacity-achieving ensembles of systematic accumulate-repeat-accumulate (ARA) codes with bounded graphical complexity (Pfister & Sason, Trans. on IT, June 2007).

Question

Can state nodes also reduce the number of decoding iterations?

Theorem

For:

- systematic ARA ensembles.
- systematic and non-systematic IRA ensembles.

Under mild conditions, the number of iterations required to achieve an average bit erasure probability P_{b} satisfies

$$I(\varepsilon, p, P_{\mathrm{b}}) = \Omega\left(\frac{1}{\varepsilon}\right).$$

Proof outline: Graph reduction (Pfister & Sason '07)

- Graph reduction transforms the Tanner graphs of variants of RA codes transmitted over a BEC to Tanner graphs of LDPC codes.
- The degree-distributions of the resulting LDPC ensembles are given in terms of the channel erasure probability and the original degree-distributions of the RA-based ensemble.
- The information from the channel is also used in the graph-reduction process.
- The resulting LDPC codes do not receive channel information (i.e., they are transmitted over a BEC with erasure prob. 1).

Proof outline (Cont.)

Based on density evolution:

Lemma

In the asymptotic case where the block length tends to infinity, let us define

- $l_{\mathrm{ARA}}(\varepsilon, p, P_{\mathrm{b}})$ - number of iterations required to achieve an average bit erasure prob. P_{b} of the systematic bits over the ARA ensemble.
- $l_{\mathrm{LDPC}}(\varepsilon, p, P_{\mathrm{b}})$ - number of iterations required to achieve an average bit erasure probability $1 - \sqrt{1 - \frac{P_{\mathrm{b}}}{p}}$ over the LDPC ensemble resulting from graph reduction.

Then

$$l_{\mathrm{ARA}}(\varepsilon, p, P_{\mathrm{b}}) \geq l_{\mathrm{LDPC}}(\varepsilon, p, P_{\mathrm{b}})$$

Similar lemmas are derived for the other RA-based codes.

Proof outline (Cont.)

$\Rightarrow$ It suffices to find a lower bound on the number of iterations for the LDPC ensemble.

Problem:

The LDPC ensemble created by graph reduction is transmitted over the BEC with erasure probability 1.
$\Rightarrow$ The gap to capacity is not defined.
$\Rightarrow$ The lower bound on the number of iterations for LDPC ensembles cannot be applied.

To circumvent this obstacle, the proof of this theorem follows along the same lines as the one for LDPC ensembles with minor technical adjustments to relate between properties of the RA-based and the LDPC ensembles.

An improved sphere-packing bound for finite-length codes on symmetric memoryless channels

Sphere-Packing Bounds

- Lower bounds on the decoding error probability of optimal block codes, given in terms of
  1. block length
  2. rate
  3. communication channel
- Based on geometrical properties of the decoding regions.
- Decay to zero exponentially with the block length.

The 1967 sphere-packing (SP67) bound (Shannon, Gallager & Berlekamp)

- Applies to codes transmitted over discrete memoryless channels (DMCs).
- Valid under optimal ML decoding or even under list decoding.
- Error exponent is exact between the critical rate and the channel capacity.

Notes on the Classical SP67 Bound

- The original focus in the derivation of the SP67 bound was on asymptotic analysis.
- The aim was to make the derivation as simple as possible, as long as there is no loss in the asymptotic behavior.
- Problem: The SP67 bound is in general very loose for codes of short to moderate block lengths.
- Goal: Improve the tightness of the sphere-packing bound for finite-length codes, especially in light of the remarkable performance of codes defined on graphs (e.g., turbo, LDPC, RA codes etc.) even for short to moderate block lengths.

In order to consider possible improvements of the SP67 bound for finite-length codes, we first outline the original derivation of this bound.

Derivation of the 1967 Sphere-Packing Bound

Step 1: Lower bound on the error prob. for a code of two codewords

- Consider a code which consists of two codewords $\mathbf{x}_1$ and $\mathbf{x}_2$.
- $P_i(\mathbf{y})$ - Probability of receiving $\mathbf{y}$ when $\mathbf{x}_i$ is transmitted ($i = 1, 2$).
- $\mathcal{Y}_i$ - Decoding region of $\mathbf{x}_i$ ($\mathcal{Y}_2 = \mathcal{Y}_1^c$).
- By considering typical output sequences w.r.t. a certain prob. distribution, it was shown that for all $s \in (0, 1)$

$$P_{e,1} \triangleq \sum_{\mathbf{y} \in \mathcal{Y}_2} P_1(\mathbf{y}) > \frac{1}{4} \exp\Big(\mu(s) - s\mu'(s) - s\sqrt{2\mu''(s)}\Big)$$

or

$$P_{e,2} \triangleq \sum_{\mathbf{y} \in \mathcal{Y}_1} P_2(\mathbf{y}) > \frac{1}{4} \exp\Big(\mu(s) + (1-s)\mu'(s) - (1-s)\sqrt{2\mu''(s)}\Big).$$

where $\mu(s) \triangleq \ln\Big(\sum_{\mathbf{y}} P_1(\mathbf{y})^{1-s} P_2(\mathbf{y})^s\Big), \quad 0 < s < 1.$

Step 2: Fixed-composition block codes

- Consider a fixed-composition block code containing M codewords of length N, transmitted over a DMC, and decoded by a list decoder of size L.
- An arbitrary memoryless probability measure F_N over channel output vectors of length N is introduced. It is used to measure the size of the decoding regions.
- It is easy to show that there is a codeword $\mathbf{x}_m$ so that the size of its decoding region does not exceed $\frac{L}{M}$.

Step 2: Fixed-composition block codes

- Use in Step 1 with the setting: $P_1(\mathbf{y}) = P_N(\mathbf{y}|\mathbf{x}_m)$, $P_2(\mathbf{y}) = F_N(\mathbf{y})$. $\Rightarrow$ Step 1 provides a lower bound on the conditional error prob. of this codeword for all values of s for which the inequality related to the size of the decoding region is violated (we do not know the exact size of this set, but it is upper bounded by $\frac{L}{M}$).
- Since we do not know this specific codeword, we replace its conditional error probability by an upper bound which is the maximal error probability (over all codewords).

To achieve the tightest universal lower bound:

1. Find F_N which *maximizes* the lower bound.
2. Find the composition which *minimizes* the lower bound.

Step 3: Lower bound on the average error prob. of general block codes

Proposition: The average error probability of an (N, M) block code defined over an alphabet of size K is not less than half the maximal error probability of a certain $(N, \frac{M}{2\,N^K})$ fixed composition subcode.

Proof outline:

- For a block code of length N and alphabet size K, there are at most $\binom{N+K-1}{K-1}$ possible compositions.
- Since $\binom{N+K-1}{K-1} < N^K$, there exists a fixed composition subcode with at least $\frac{M}{N^K}$ codewords.
- Expurgation $\Rightarrow$ The average error probability of a general block code is at least half the maximal error probability of the subcode containing half of the codewords with the lowest error probability.

Combine this conclusion with the lower bound in Step 2 for fixed composition codes, and the SP67 bound follows.

Theorem (The 1967 Sphere-Packing Bound)

- Let $\mathcal{C}$ be a block code consisting of M codewords each of length N.
- Assume communication over a DMC, and let $P(j|k)$ designate the transition probabilities where $k \in \{1,\ldots,K\}$ and $j \in \{1,\ldots,J\}$ are the channel input and output alphabets, respectively.
- Assume a list decoder where the size of the list is limited to L.
- Define

$$R \triangleq \frac{\ln\left(\frac{M}{L}\right)}{N} \quad - \text{ code rate in nats per channel use}$$

$$P_{\min} \quad - \text{ smallest non-zero transition probability of the DMC.}$$

- Then, the *average decoding error probability* is lower bounded by

$$P_e(N,M,L) \geq \exp\left\{-N\left[E_{sp}\left(R - O_1\left(\frac{\ln N}{N}\right)\right) + O_2\left(\frac{1}{\sqrt{N}}\right)\right]\right\}$$

Theorem (The 1967 Sphere-Packing Bound)

where

$$
\begin{aligned}
E_{\text{sp}}(R) &\triangleq \sup_{\rho \geq 0} \left(E_0(\rho) - \rho R \right) \\
E_0(\rho) &\triangleq \max_{\mathbf{q}} E_0(\rho, \mathbf{q}) \\
E_0(\rho, \mathbf{q}) &\triangleq -\ln \left(\sum_{j=1}^{J} \left[\sum_{k=1}^{K} q_k P(j|k)^{\frac{1}{1+\rho}} \right]^{1+\rho} \right) \\
O_1\left(\frac{\ln N}{N} \right) &\triangleq \frac{\ln 8}{N} + \frac{K \ln N}{N} \\
O_2\left(\frac{1}{\sqrt{N}} \right) &\triangleq \sqrt{\frac{8}{N}} \ln\left(\frac{e}{\sqrt{P_{\min}}} \right) + \frac{\ln 8}{N} \, .
\end{aligned}
$$

The Valembois & Fossorier (VF) Bound

A. Valembois and M. Fossorier, "Sphere-packing bounds revisited for moderate block length," *IEEE Trans. on IT*, Vol. 50, Decemeber 2004.

- Valembois and Fossorier revisited the derivation of the SP67 bound, and found four points where the bound could be tightened for codes of short to moderate block lengths.
- These improvements also make the bound valid for memoryless channels with discrete input and continuous output.
- The resulting sphere-packing bound (referred to as the VF bound) is uniformly tighter than the SP67 bound.
- Derivation of the VF and SP67 bounds rely on similar steps
  $\Rightarrow$ Rate loss due to the use of fixed-comp. codes and expurgation.

Notes on the SP67 and VF bounds

- While the SP67 bound can be applied only to a DMC, the VF bound can be also applied to memoryless channels of continuous output alphabet (since it does not require that $P_{\min} > 0$, and calculate instead the second derivative of μ exactly).
- The rate shift in their error exponents scales like $\frac{\ln N}{N}$ for both bounds. This is due to the need to consider fixed composition codes (i.e., Step 2 in the derivation of the SP67 and VF bounds).
- Both bounds use expurgation of half of the codewords to transform a lower bound on the *maximal* error probability to a lower bound on the *average* error probability.

Discussion on Sphere-Packing Bounds

Question

Is it necessary to consider fixed composition codes first ?

Discussion on Sphere-Packing Bounds

Question

Is it necessary to consider fixed composition codes first ?

Answer

In general, yes! Since it is required to fix the codeword composition in order to find the optimal tilting measure F_N.

Discussion on Sphere-Packing Bounds

Question

Is it necessary to consider fixed composition codes first ?

Answer

In general, yes! Since it is required to fix the codeword composition in order to find the optimal tilting measure F_N.

However, for symmetric memoryless channels, the lower bound on the maximal error probability is independent of the composition.

This observation yields that for symmetric memoryless channels, the sphere-packing bounding technique can be directly applied to general block codes (without necessarily a fixed composition).

Discussion on Sphere-Packing Bounds

Question

Is it necessary to consider the maximal error probability first?

Discussion on Sphere-Packing Bounds

Question

Is it necessary to consider the maximal error probability first?

Answer

By modifying the first step of the derivation to consider the average error probability over M pairs of codewords, where the index m of the selected pair is chosen uniformly at random and known at the decoder, it is possible to directly consider the *average* error probability.

This stage also requires that the lower bound on the conditional error probability is independent of the considered codeword.

Symmetry conditions

- The symmetry conditions required for the ISP bound are mild:
  - All memoryless binary-input output-symmetric (MBIOS) channels are symmetric in this sense
  - All M-ary input and symmetric output (MI-SO) channels (see [Wang et al.,IT Jan 07]) are symmetric in this sense.
- The ISP bound is valid in particular for coherently detected M-ary PSK modulated signals, over fully-interleaved fading channels, when the decoder has full knowledge of the fading samples.

An Improved Sphere-Packing (ISP) Bound

- The derivation of the ISP bound relies on
  - the observation that for symmetric memoryless channels, the lower bound on the maximal error probability is independent of the codeword composition.
  - the improvements suggested by Valembois and Fossorier for the derivation of the VF bound.

An Improved Sphere-Packing (ISP) Bound

- The derivation of the ISP bound relies on
  - the observation that for symmetric memoryless channels, the lower bound on the maximal error probability is independent of the codeword composition.
  - the improvements suggested by Valembois and Fossorier for the derivation of the VF bound.
- The ISP bound forms a tighter sphere-packing bound
  1. by considering M codeword pairs in the first step of the derivation

     $\Rightarrow$ direct analysis of the *average* error probability,

     eliminating the need for expurgation of half of the codewords
  2. by the independence of the lower bound on the conditional error probability from codeword composition

     $\Rightarrow$ direct analysis of general block codes,

     eliminating the need for considering fixed-composition codes.

An Improved Sphere-Packing (ISP) Bound

- The derivation of the ISP bound relies on
  - the observation that for symmetric memoryless channels, the lower bound on the maximal error probability is independent of the codeword composition.
  - the improvements suggested by Valembois and Fossorier for the derivation of the VF bound.
- Though this observation has no effect on asymptotic analysis, it affects the tightness of the bound for finite-length codes (especially, for short to moderate block lengths).

This gives the following improvement on the SP67 and VF bounds.

Theorem (Improved Sphere-Packing Bound)

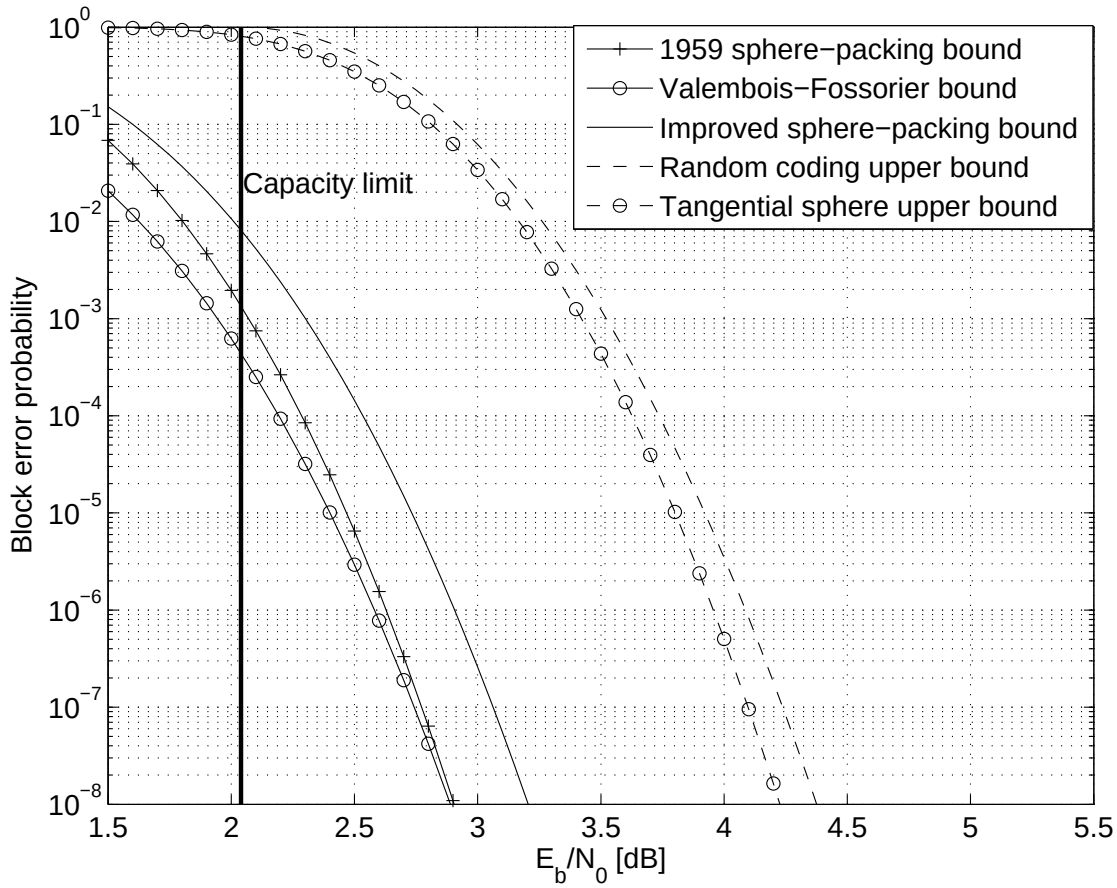
- Let $\mathcal{C}$ be an arbitrary block code consisting of M codewords, each of length N.
- Assume communication over a symmetric memoryless channel specified by the transition probabilities (or densities) $P(j|k)$.
- Assume a list decoder where the size of the list is limited to L.
- Then, the *average decoding error probability* is lower bounded by

$$P_e(N,M,L) \geq \exp\Big\{-NE_{\text{ISP}}(R,N)\Big\}$$

where

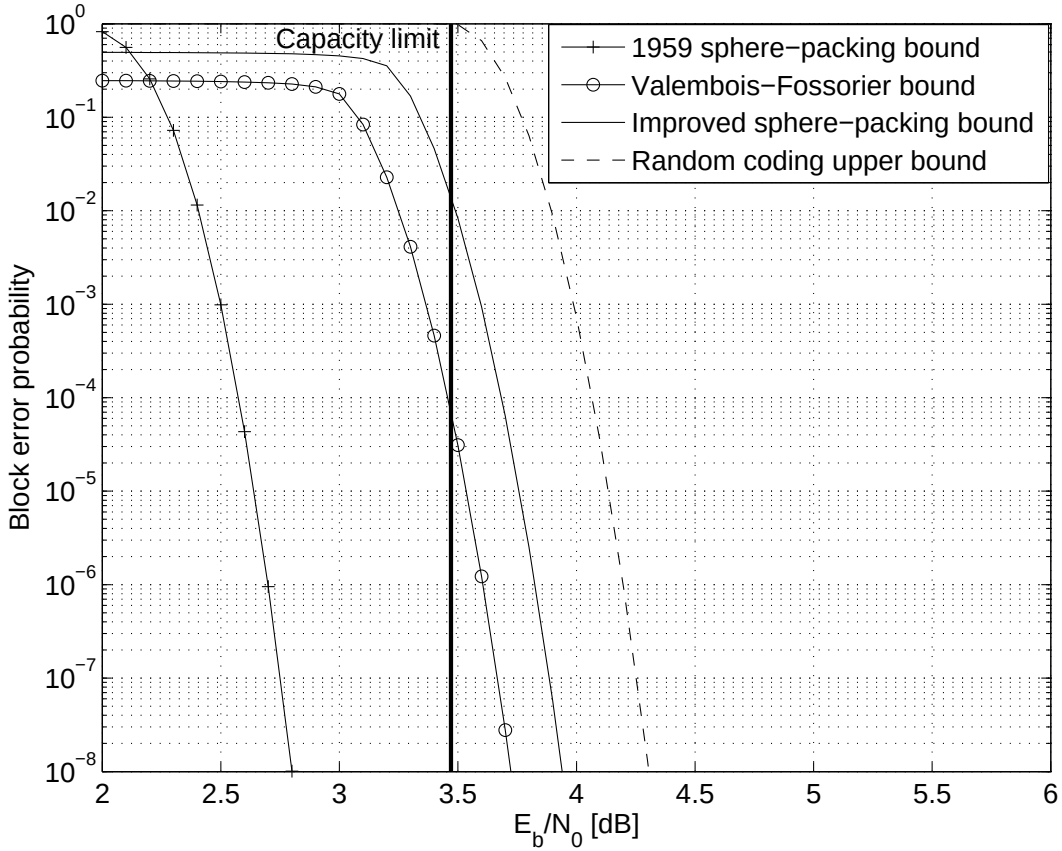
$$E_{ISP}(R,N) \triangleq \inf_{x>\frac{\sqrt{2}}{2}} \left\{E_0(\rho_x) - \rho_x\left(R - O_1\left(\frac{1}{N},x\right)\right) + O_2\left(\frac{1}{\sqrt{N}},x,\rho_x\right)\right\}$$

Numerical Results



- Transmission over a BPSK modulated AWGN channel
- $N = 500$ bits, $R = 0.8 \frac{\text{bits}}{\text{channel use}}$.
- The ISP bound gives an improvement of 0.26 and 0.33 dB over the SP59 and VF bounds, respectively.

Numerical Results

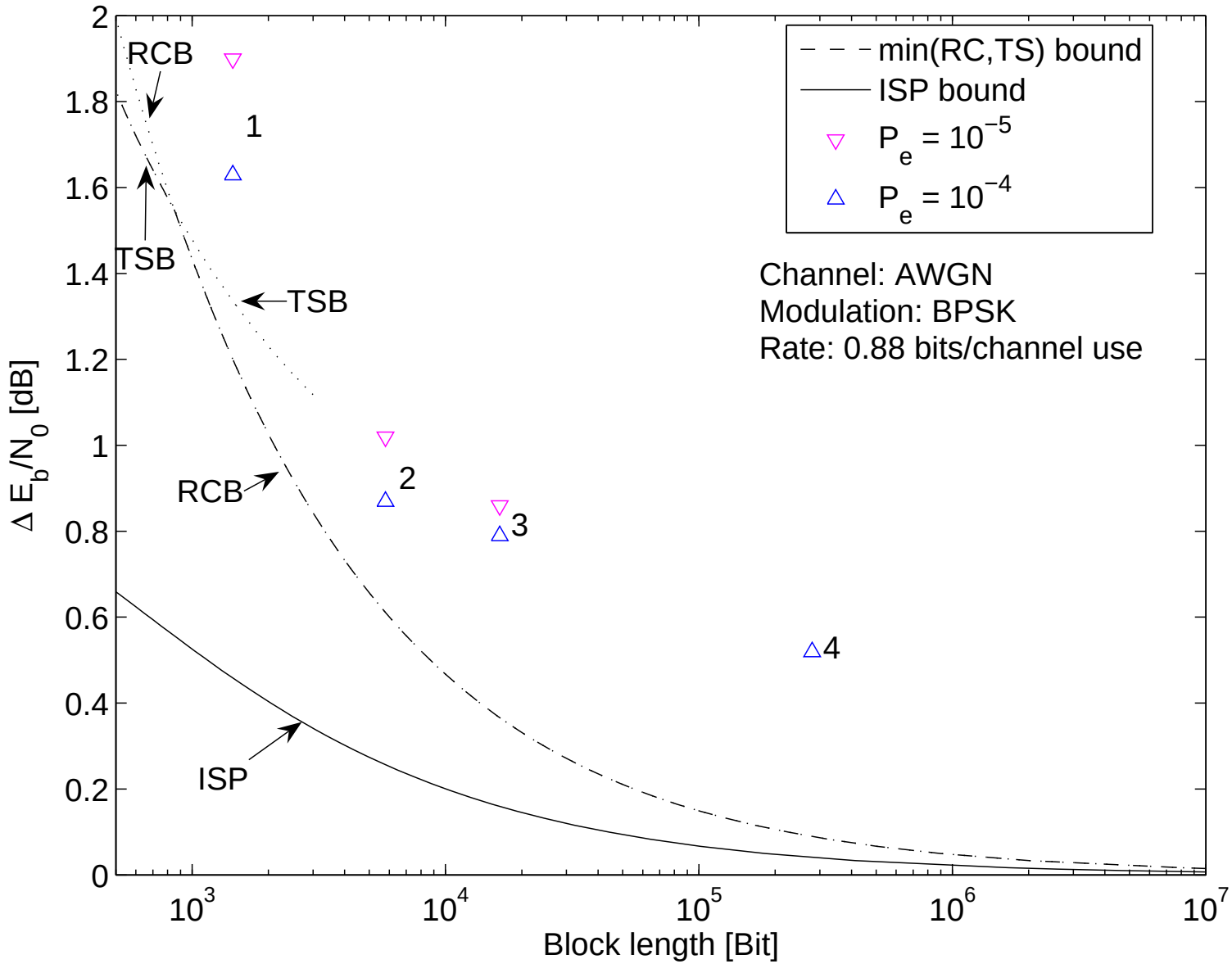


- Transmission over a 8-PSK modulated AWGN channel
- $N = 5580$ bits (1680 channel symbols), $R = 2.2 \frac{\text{bits}}{\text{channel use}}$.
- ISP bound gives an improvement of 0.2 dB over the VF bound.
- 0.4 dB gap between ISP lower bound and random-coding upper bound.

Minimal Block Length as a Function of Performance

- Fixing:
  1. the communication channel model
  2. the code rate
  3. the block error probability
- Sphere-packing bounds $\Rightarrow$ lower bounds on the minimal block length required to achieve the desired performance on the given channel using an arbitrary block code and decoding algorithm.
- Upper bounds on the error prob. of random codes $\Rightarrow$ upper bounds on the block length required for ML decoded random codes to achieve the desired performance on the given communication channel.

Comparison of upper and lower bounds on the block the length with the performance of iteratively decoded codes.



Summary

- We present new information-theoretic bounds on the thresholds and parity-check density of binary linear block codes.

Summary

- We present new 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 more accurately the tradeoff between performance and complexity under iterative decoding.

Summary

- We present new 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 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 code structure and the sub-optimality of iterative decoding.

Summary

- We present new 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 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 code structure 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

- We present new 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 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 code structure 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.

Summary

- We introduce analytic lower bounds on the number of iterations for the asymptotic case where the block length tends to infinity.

Summary

- We introduce analytic lower bounds on the number of iterations for the asymptotic case where the block length tends to infinity.
- The bounds refer to iteratively decoded ensembles of codes defined on graphs whose transmission takes place over the BEC.

Summary

- We introduce analytic lower bounds on the number of iterations for the asymptotic case where the block length tends to infinity.
- The bounds refer to iteratively decoded ensembles of codes defined on graphs whose transmission takes place over the BEC.
- The bounds show that for all these code families the number of iterations grows at least like the inverse of the gap to capacity.

Summary

- We introduce analytic lower bounds on the number of iterations for the asymptotic case where the block length tends to infinity.
- The bounds refer to iteratively decoded ensembles of codes defined on graphs whose transmission takes place over the BEC.
- The bounds show that for all these code families the number of iterations grows at least like the inverse of the gap to capacity.
- The bounds are simple to evaluate and are given in terms of the channel erasure probability, the required bit erasure probability, the gap to capacity and the fraction of variable nodes of degree 2.

Summary

- We introduce analytic lower bounds on the number of iterations for the asymptotic case where the block length tends to infinity.
- The bounds refer to iteratively decoded ensembles of codes defined on graphs whose transmission takes place over the BEC.
- The bounds show that for all these code families the number of iterations grows at least like the inverse of the gap to capacity.
- The bounds are simple to evaluate and are given in terms of the channel erasure probability, the required bit erasure probability, the gap to capacity and the fraction of variable nodes of degree 2.
- The behavior of these lower bounds matches experimental results and a previous conjecture of Khandekar and McEliece.

Summary

Code family	Number of iterations as function of ε	Graphical complexity as function of ε
LDPC	$\Omega\left(\frac{1}{\varepsilon}\right)$	$\Theta\left(\ln\frac{1}{\varepsilon}\right)$
Systematic IRA	$\Omega\left(\frac{1}{\varepsilon}\right)$	$\Theta\left(\ln\frac{1}{\varepsilon}\right)$
Non-systematic IRA	$\Omega\left(\frac{1}{\varepsilon}\right)$	$\Theta(1)$
Systematic ARA	$\Omega\left(\frac{1}{\varepsilon}\right)$	$\Theta(1)$

Summary

- We introduce an improved sphere-packing (ISP) bound for finite-length codes whose transmission takes place over symmetric memoryless channels.

Summary

- We introduce an improved sphere-packing (ISP) bound for finite-length codes whose transmission takes place over symmetric memoryless channels.
- The ISP bound is uniformly tighter than the SP67 and VF bounds, especially for codes of short to moderate block lengths.

Summary

- We introduce an improved sphere-packing (ISP) bound for finite-length codes whose transmission takes place over symmetric memoryless channels.
- The ISP bound is uniformly tighter than the SP67 and VF bounds, especially for codes of short to moderate block lengths.
- Applications of the ISP bound are exemplified.

Summary

- We introduce an improved sphere-packing (ISP) bound for finite-length codes whose transmission takes place over symmetric memoryless channels.
- The ISP bound is uniformly tighter than the SP67 and VF bounds, especially for codes of short to moderate block lengths.
- Applications of the ISP bound are exemplified.
- The ISP bound provides an interesting alternative to the sphere-packing bound of Shannon for the Gaussian channel, especially for high code rates.

Summary

- We introduce an improved sphere-packing (ISP) bound for finite-length codes whose transmission takes place over symmetric memoryless channels.
- The ISP bound is uniformly tighter than the SP67 and VF bounds, especially for codes of short to moderate block lengths.
- Applications of the ISP bound are exemplified.
- The ISP bound provides an interesting alternative to the sphere-packing bound of Shannon for the Gaussian channel, especially for high code rates.
- The sphere-packing bounds are employed as lower bounds on minimal block length required to achieve a desired performance on a given channel model.

Topics for further research

- Performance vs. complexity tradeoff for generalized LDPC codes.
- Application of the information-theoretic bounds for parallel channels to common communication scenarios.
- Generalization of the bounds on the number of iterations to arbitrary MBIOS channels.
- Further improvement of sphere-packing bounds for finite-length codes.
- Sphere-packing bounds on the symbol error probability of optimal codes.

Published 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,” *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 for parallel channels with application to puncturing,” *IEEE Trans. on Information Theory*, vol. 53, no. 2, pp. 580 - 598, February 2007.

Submitted papers:

- G. Wiechman and I. Sason, “An improved sphere-packing bound for finite-length codes on symmetric memoryless channels,” submitted to *IEEE Trans. on Information Theory*, March 2007. [Online]. Available: `http://www.arxiv.org/abs/cs.IT/0608042`.

- I. Sason and G. Wiechman, “Bounds on the number of iterations for turbo-like ensembles over the binary erasure channel,” submitted to *IEEE Trans. on Information Theory*, November 2007. [Online]. Available: `http://www.arxiv.org/abs/0711.1056`.