Bounds on the Convergence Speed of Iterative Message-Passing Decoders over the Binary Erasure Channel

Igal Sason Gil Wiechman

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

5th International Symposium on Turbo Codes & Related Topics
(Turbo Coding 2008)

EPFL, Lausanne, Switzerland
September 1–5, 2008

Outline

Related Work: Approaches for Asymptotic Analysis

- Assume an LDPC code ensemble whose transmission takes place over a memoryless binary-input output-symmetric channel.
- Consider the asymptotic case where the block length tends to ∞.

Ardakani et al. (Allerton & ISIT 2005)

- Numerical approximations for the number of iterations and decoding complexity are provided.
- This enables to numerically optimize LDPC code ensembles with good asymptotic tradeoff between performance and complexity.
- However, this approach does not provide rigorous bounds on the convergence speed of an iterative message-passing decoder.

Related Work (2)

Ma and Yang (ISIT 2004), and Ma's PhD thesis (2007)

- Provide asymptotic bounds on the number of iterations for the case of a binary erasure channel (BEC).
- The bounds serve for numerical optimization of LDPC code ensembles with fast decoding speed over the BEC.
- The bounds do not characterize explicitly how the number of iterations increases when the gap (in rate) to capacity vanishes.

Related Work (3)

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 $\ln \frac{1}{\varepsilon}$.

Scope of This Work

Introduce new lower bounds on the number of iterations for the BEC where these bounds:

- Apply to various code ensembles defined on graphs (e.g., LDPC, RA, IRA, ARA) in the asymptotic case where $n \to \infty$.
- The lower bounds on the required number of iterations are expressed in terms of
  - the achievable gap to capacity
  - the target bit erasure probability
  - the fraction of degree-2 variable nodes (i.e., they don't depend explicitly on the full characterization of the degree distributions).

Theorem

Let $\left\{(n, \lambda, \rho)\right\}$ be a sequence of LDPC code ensembles ($n \to \infty$). Lets assume

- Transmission over a BEC with erasure probability p.
- 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.

Then, the number of iterations (I) required to achieve an average bit erasure probability P_b over the ensemble satisfies

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

provided that $P_\mathrm{b} < p\, L_2(\varepsilon)$.

On the fraction of variable nodes of degree 2

For various capacity-achieving sequences of LDPC ensembles over the BEC

$$L_2(\varepsilon) \xrightarrow[\varepsilon \to 0]{} \frac{1}{2}$$

irrespectively of the erasure probability of the channel.

On the fraction of variable nodes of degree 2

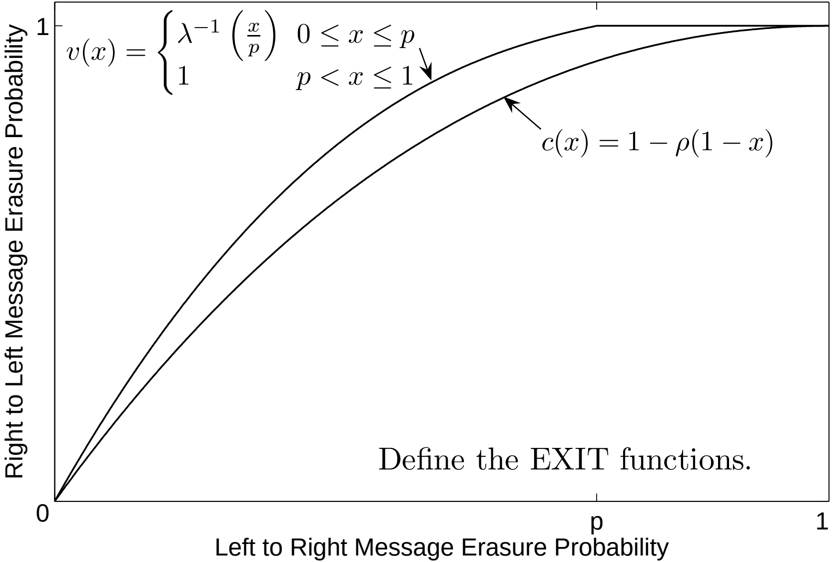
Corollary

If $L_2(\varepsilon)$ does not tend to zero as the gap (ε) to capacity vanishes then

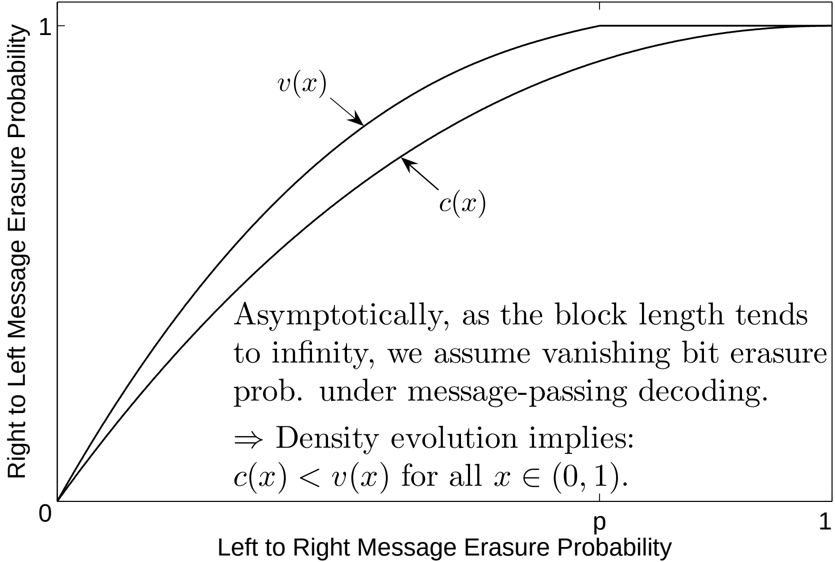
$$I(\varepsilon) = \Omega\left(\frac{1}{\varepsilon}\right).$$

This supports the conjecture by Khandekar and McEliece.

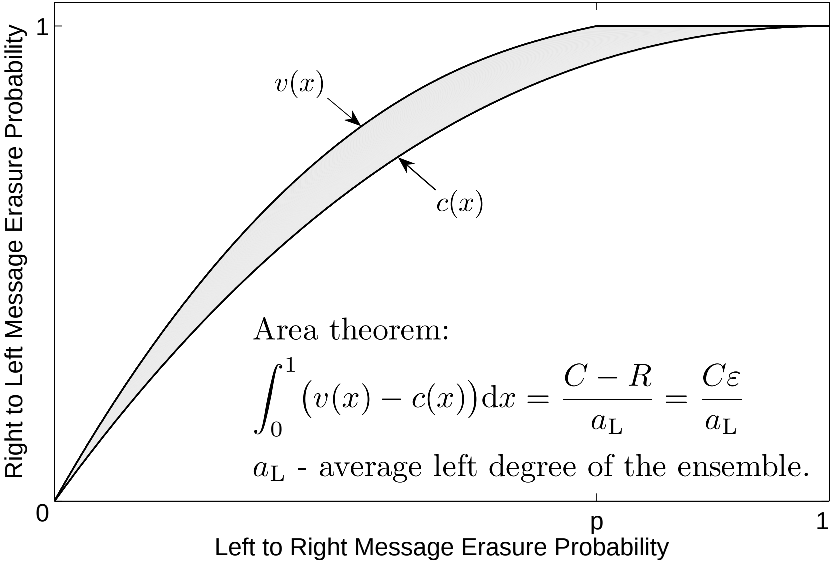
Proof Outline



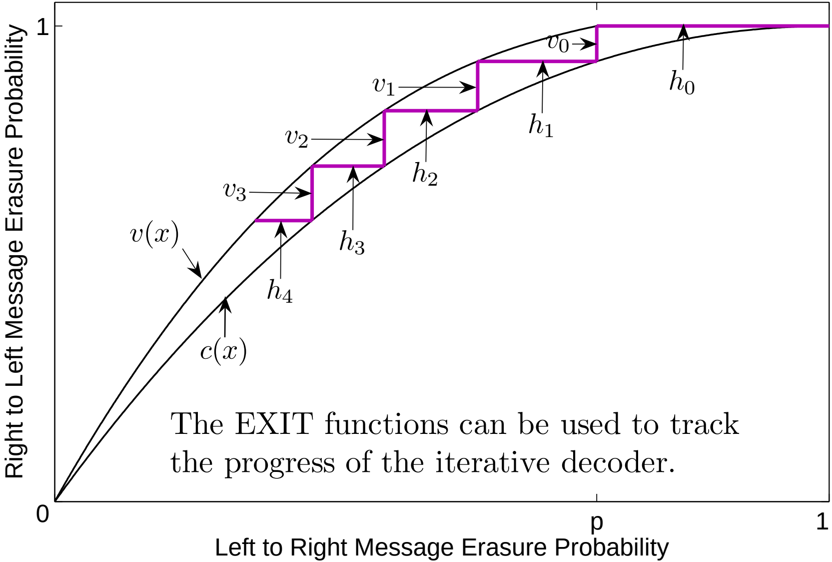
Proof Outline



Proof Outline

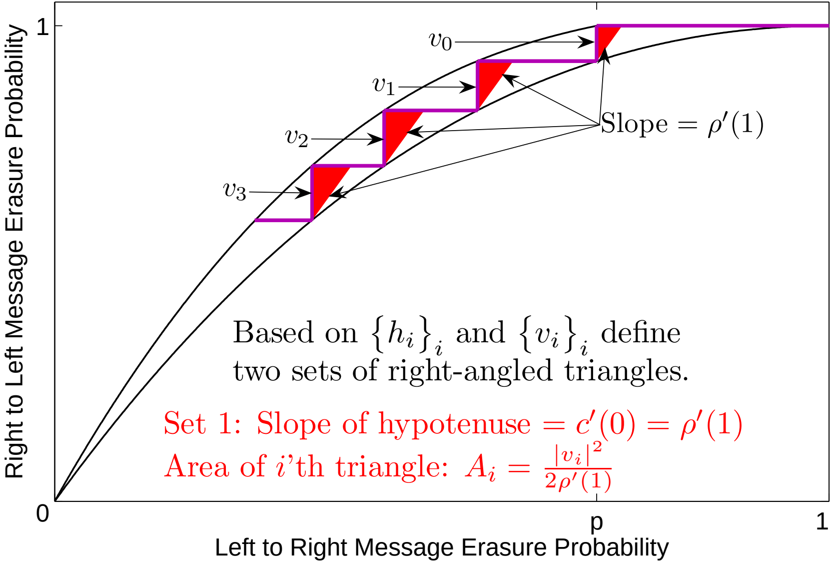


Proof Outline

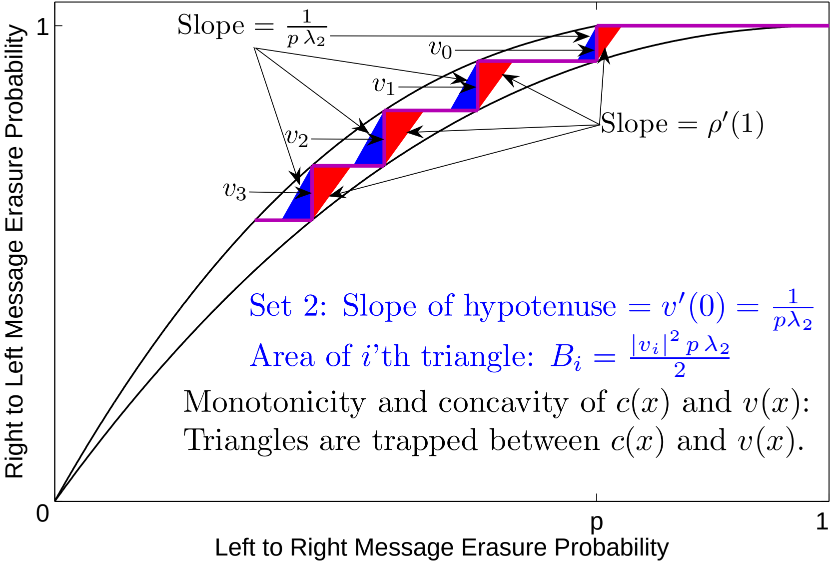


The EXIT functions can be used to track the progress of the iterative decoder.

Proof Outline



Proof Outline



Proof Outline (Cont.)

- Based on the area theorem and the stability condition, we get from the last picture:

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

  where l is an arbitrary natural number.
- Cauchy-Schwartz inequality: $\left(\sum_{i=0}^{l-1} |v_i|\right)^2 \leq l \sum_{i=0}^{l-1} |v_i|^2$

Proof Outline (Cont.)

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

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

The graphical complexity perspective

In the asymptotic case where $n \to \infty$

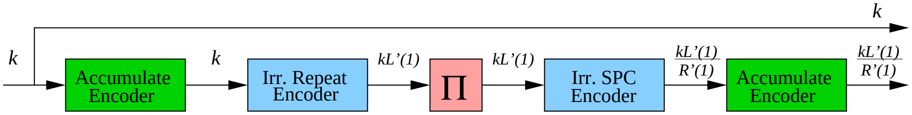
- The graphical complexity of capacity-approaching LDPC and systematic irregular repeat-accumulate (IRA) ensembles is un-bounded as the gap to capacity vanishes and scales at least like $\ln \frac{1}{\varepsilon}$ (I.S. & R. Urbanke, Trans. on IT, 2003 and 2004).
- Adding state nodes to the graph provides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

Question

Can state nodes also reduce the number of decoding iterations?

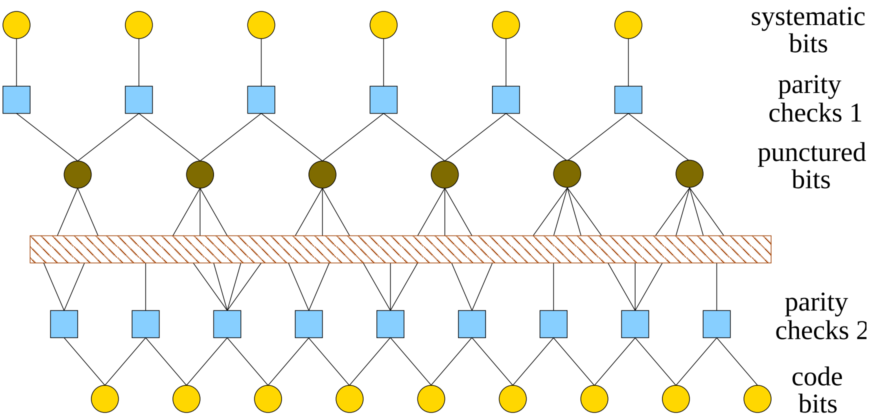
To this end, lets consider variants of repeat-accumulate codes which include state nodes in their Tanner graphs.

Systematic ARA Codes: Encoder



- Encoder diagram for the systematic ARA ensemble
  - "Accumulate" block is the standard rate-1 $\frac{1}{1+D}$ encoder
  - "Irr. Repeat" block repeats each bit a different number of times
  - "Irr. SPC" block groups bit in different size blocks and outputs a single parity bit for each block
  - Block sizes are shown on each arrow for k information bits

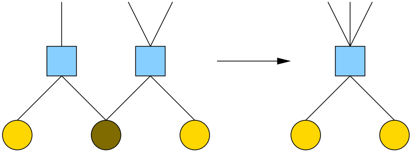
Systematic ARA Codes: Tanner Graph



- Shading is used to denote punctured or erased bits

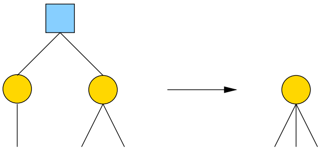
Graph Reduction for Code Bits (Pfister & Sason)

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



Graph Reduction for Systematic Bits (Pfister & Sason)

- The "systematic bit" nodes in the Tanner graph of the systematic ARA codes only provide channel information. Erasures make them worthless, and they can be removed along with their "parity-check 1" nodes without affecting the decoder.
- When the value of a "systematic bit" node is observed (assume the value is zero w.o.l.o.g.), it can be removed leaving a degree 2 parity-check.
- Degree 2 parity-checks imply equality, and allow the connected "punctured bit" nodes to be merged (summing their degrees).



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

$$I(\varepsilon) = \Omega\left(\frac{1}{\varepsilon}\right)$$

The proof relies on graph reduction of the Tanner graph for systematic ARA codes, and also on the previous result for LDPC code ensembles.

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 show that for various families of code ensembles defined on graphs (LDPC, IRA, ARA), the number of iterations on the BEC 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 show that for various families of code ensembles defined on graphs (LDPC, IRA, ARA), the number of iterations on the BEC 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 show that for various families of code ensembles defined on graphs (LDPC, IRA, ARA), the number of iterations on the BEC 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	$\Omega\left(\frac{1}{\varepsilon}\right)$	$\Theta(1)$

Full Paper Version

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.

Thanks

This work benefited from a small unpublished write-up which was written by S. Dusad, C. Measson, A. Montanari and R. Urbanke.