On Universal Properties of Capacity-Approaching LDPC Code Ensembles

Igal Sason

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

2009 Information Theory and Applications (ITA) Workshop,
UCSD, San-Diego, California, USA

February 8–13, 2009.
Degree Distributions of LDPC Code Ensembles

Consider the case where transmission takes place over a memoryless, binary-input output-symmetric (MBIOS) channel.

- Let $a$ designate the pdf of the log-likelihood ratio (LLR) at the channel output given that the channel input is zero. Then, the symmetry property holds (i.e., $a(l) = e^{-l} a(-l)$ for $l \in \mathbb{R}$).
- Consider LDPC code ensembles whose design rate forms a fraction $1 - \varepsilon$ of the channel capacity with a target bit error probability $P_b$.

**Question**

What can be said about the degree distributions of the LDPC code ensembles in this setting?
Degree Distributions of LDPC Code Ensembles (Cont.)

In this work

- Linear programming (LP) bounds on the degree distributions of LDPC code ensembles are derived.
- They provide upper bounds on the fraction of edges or nodes up to degree $k$ where $k$ is a parameter.
- They are general since they hold even under ML decoding (and, hence, also under any sub-optimal decoding algorithm).
- The bounds also apply to finite-length codes.
- Analytical solutions of these bounds are obtained via Lagrange duality, and these bounds are easy to calculate.
A Brief Outline of the Derivation of the LP Bounds

A lower bound on the conditional entropy for binary linear block codes transmitted over MBIOS channels gets the form

\[
\frac{H(X|Y)}{n} \geq R - C + \frac{1 - R}{2 \ln 2} \sum_{p=1}^{\infty} \frac{\Gamma(g_p)}{p(2p - 1)}
\]

where

\[
g_p \triangleq \int_{0}^{\infty} a(l)(1 + e^{-l}) \tanh^{2p} \left( \frac{l}{2} \right) dl, \quad p \in \mathbb{N}.
\]

and \( \Gamma(x) \triangleq \sum_{k} \Gamma_k x^k \) forms the degree distribution of the parity-check nodes, from the node perspective, of an arbitrary representation of the code by a **full-rank** parity-check matrix (Wiechman & Sason, IEEE Trans. on IT, Feb. 2007).
Fano inequality.

\[ g_p \geq (g_1)^p, \text{ for every } p \in \mathbb{N}, \text{ with equality for the BSC}. \]

An adaptation of these results to LDPC code ensembles, whose parity-check matrices are not necessarily full rank (i.e., the parity-check equations are linearly dependent), is needed.

The above IT bound is proved to hold for every code from a binary LDPC code ensemble when the code rate \( R \) is replaced by the design rate \( (R_d) \) of the ensemble \( (R \geq R_d) \).

The derivation of the LP bounds finally relies on the equality

\[
\frac{1}{2 \ln 2} \sum_{k=1}^{\infty} \frac{u^k}{k(2k - 1)} = 1 - h_2 \left( \frac{1 - \sqrt{u}}{2} \right), \quad \forall \ u \in [0, 1].
\]

where \( h_2 \) designates the binary entropy function on base 2.
LP1 bound for the degree distribution of the parity-check nodes for LDPC code ensembles

\[
\text{maximize } \sum_{i=1}^{k} \rho_i, \quad k = 1, 2, \ldots \\
\text{subject to } \left\{ \begin{array}{l}
\sum_{i=1}^{\infty} \left\{ \left[ 1 - h_2 \left( \frac{1-g_1^2}{2} \right) \right] \rho_i \right\} \leq \frac{\varepsilon C + h_2(P_b)}{1-(1-\varepsilon)C} \sum_{i=1}^{\infty} \rho_i \\
\sum_{i=1}^{\infty} \rho_i = 1 \\
\rho_i \geq 0, \quad i = 1, 2, \ldots
\end{array} \right.
\]

where the optimization variables are \( \{\rho_i\}_{i \geq 1} \). The quantity \( g_1 \) above depends on the channel statistics only.
LP2 bound for the degree distribution: Universal for all equi-capacity MBIOS channels

Replace the parameter $g_1$ with the channel capacity $C$ (where, in general, $g_1 \geq C$ with equality for the BEC).
Figure: The universal LP2 bound versus the heavy-tail Poisson degree distribution, and the degree distribution of the right-regular LDPC ensemble. It refers to the fraction of edges which are attached to parity-check nodes of degree $\leq k$ for an integer $k \geq 2$. Considered here is a BEC whose capacity is $\frac{1}{2}$ bit per channel use, and where 99.9% of capacity is achieved under iterative message-passing decoding with vanishing bit erasure probability.
Corollary

If the asymptotic bit error/erasure probability vanishes, then the following properties hold for an arbitrary finite degree $i$

$$L_i = O(1), \quad R_i = O(\varepsilon),$$

$$\lambda_i = O\left(\frac{1}{\ln \frac{1}{\varepsilon}}\right), \quad \rho_i = O\left(\frac{\varepsilon}{\ln \frac{1}{\varepsilon}}\right).$$

where $\{L_i\}$ and $\{R_i\}$ are the degree distributions of the variable and parity-check nodes, respectively, and $\{\lambda_i\}$ and $\{\rho_i\}$ are the corresponding degree distributions from the edge perspective.
These bounds hold under ML decoding (or any other algorithm).

The upper bounds on the left degree distribution look at first glance looser than those for the right degree distribution (due to the additional factor $\varepsilon$ in the latter case).

However, it is not an artifact of the bounding technique, as it indeed reflects reality, e.g.:

- For various capacity-achieving degree distributions on the BEC with iterative message-passing decoding, the fraction of degree-2 variable nodes tends to $\frac{1}{2}$.
- The upper bound on the fraction of edges connected to degree-2 variable nodes ($\lambda_2$) is shown in this work to be obtained for the right-regular LDPC code ensemble of Shokrollahi which achieves capacity on the BEC under iterative decoding.
Information-Theoretic Lower Bounds on the Tradeoff Between the Graphical Complexity and Performance

Question

Consider the representation of a finite-length binary linear block code by an arbitrary bipartite graph. How simple can such a graphical representation be as a function of the channel model, target block error probability, and code rate?

Answer ⇒

- Information-theoretic lower bounds which measure the inherent graphical complexity of finite-length LDPC codes as a function of their achievable gap to capacity.
- Provides a measure of the sub-optimality of explicit constructions of LDPC codes by comparing to information-theoretic bounds.
We provide in this work an information-theoretic lower bound on the graphical complexity which depends on the channel model, target block error probability, and the code rate.

This bound relies on two previous information-theoretic results:

- A new lower bound on the average left/ right degrees in the bipartite graph as a function of the channel, target block/ bit error probability, and the achievable gap to capacity.
- Sphere-packing lower bounds: We rely here on the classical 1959 sphere-packing bound of Shannon, and the recently introduced ISP bound (Wiechman & Sason, IEEE Trans. on IT, May 2008).

The graphical complexity, defined as the number of edges in the bipartite graph, is simply the product of the block length and the average left degree.
Figure: A comparison between the graphical complexity of various efficient LDPC code ensembles and an information-theoretic lower bound.
Cardinality of the Fundamental System of Cycles of Good LDPC Code Ensembles

- Binary Linear block codes which are represented by cycle-free bipartite graphs are not good even under ML decoding.
- A theoretical treatment of cycle-free codes was provided by T. Etzion, A. Trachtenberg and A. Vardy, “Which codes have cycle-free Tanner graphs ?,” *IEEE Trans. on Information Theory*, vol. 45, no. 6, pp. 2173–2181, September 1999.

Question

*What can be said about the cardinality of the fundamental system of cycles of LDPC code ensembles as a function of the achievable gap (in rate) to capacity ?*
Theorem

Let \( \{(n, \lambda, \rho)\} \) be a sequence of LDPC code ensembles transmitted over an MBIOS channel. Suppose that the design rate is a fraction \( 1 - \varepsilon \) of the channel capacity \( C \), and the average bit error probability of this sequence vanishes under some decoding algorithm as \( n \to \infty \).

Consider the average cardinality of the fundamental system of cycles, \( \beta_n(G) \), where the graphs \( G \) are chosen uniformly at random from the LDPC code ensemble \( (n, \lambda, \rho) \). Then, the following result holds:

\[
\liminf_{n \to \infty} \frac{\mathbb{E}[\beta_n(G)]}{n} \geq \frac{(1 - C) \ln \left( g_1 \left[ 1 - 2h_2^{-1} \left( \frac{1-C}{1-(1-\varepsilon)C} \right) \right]^{-2} \right)}{\ln \left( \frac{1}{g_1} \right)} - 1
\]

where \( g_1 \triangleq \mathbb{E} \left[ \tanh^2 \left( \frac{L}{2} \right) \right] \) and \( L \) forms the LLR at the channel output.
Corollary

The average cardinality of the fundamental system of cycles grows at least like \( \log \frac{1}{\varepsilon} \) where the achievable design rate forms a fraction \( 1 - \varepsilon \) of the channel capacity.

⇒ The fundamental system of cycles becomes unbounded as the achievable gap to capacity vanishes (even under ML decoding).

Essence of the proof of this theorem: A combination of an improved lower bound on the average right degree (which behaves like \( \log \frac{1}{\varepsilon} \)), which follows from the lower bound on the conditional entropy, with some simple arguments from graph theory.
Figure: Asymptotic lower bounds on the average cardinality of the fundamental system (see Theorem 1). The bounds refer to the BSC, BIAWGNC and BEC where the design rate is $\frac{1}{2}$ bit per channel use.
I. Sason, “On Universal Properties of Capacity-Approaching LDPC Code Ensembles”, accepted to *IEEE Trans. on Information Theory*, February 2009.