On the Fundamental System of Cycles in the Bipartite Graphs of LDPC Code Ensembles

Igal Sason
Department of Electrical Engineering
Technion, Haifa 32000, Israel
sason@ee.technion.ac.il

***Abstract*—This work introduces an information-theoretic lower bound on the number of fundamental cycles for bipartite graphs of low-density parity-check (LDPC) code ensembles. This information-theoretic bound is expressed in terms of the achievable gap to capacity when the transmission of the code ensemble takes place over a memoryless binary-input output-symmetric (MBIOS) channel. The bound shows quantitatively the necessity of cycles in bipartite graphs which represent good LDPC code ensembles. More explicitly, it shows that the number of fundamental cycles should grow at least like $\log \frac{1}{\varepsilon}$ where ε designates the gap in rate to capacity, hence, it is unbounded as the gap to capacity vanishes. For the derivation of this bound, a new information-theoretic lower bound on the average right degree, which also behaves like $\log \frac{1}{\varepsilon}$, is derived. The interested reader is referred to the full paper version [9].**

***Index Terms*—Bipartite graphs, complexity, cycles, low-density parity-check (LDPC) codes, memoryless binary-input output-symmetric (MBIOS) channels.**

I. Introduction

Low-density parity-check (LDPC) codes form a class of powerful error-correcting codes which are efficiently encoded and decoded with low-complexity algorithms.

It is well known that linear block codes which are represented by cycle-free bipartite (Tanner) graphs have poor performance even under ML decoding [3]. The bipartite graphs of capacity-approaching LDPC codes should have cycles. Hence, as a continuation to a previous study in [3] and [8] (see also [6, Problems 4.52 and 4.53]), we address the following question:

Question: How does the average cardinality of the fundamental system of cycles of bipartite graphs behave as a function of the achievable gap to capacity of the underlying LDPC code ensembles ?

This paper is structured as follows: Section II provides some preliminary material and notation, Section III introduces new information-theoretic bounds which are related to the above question, and Section IV provides some numerical results. The interested reader to the full paper version [9].

II. Preliminaries

We introduce in this section some preliminary material and notation which serve for the analysis in this paper. We consider here the cycles in bipartite graphs which represent capacity-approaching LDPC code ensembles. To this end, we define and exemplify some notions which are relevant to the analysis in this work.

A. Lower Bound on the Conditional Entropy for Binary Linear Block Codes Transmitted over MBIOS Channels

For an arbitrary full-rank parity-check matrix of a binary linear block code $\mathcal{C}$, let Γ_k designate the fraction of the parity-checks involving k variables, and let $\Gamma(x) \triangleq \sum_k \Gamma_k x^k$. The following lower bound on the conditional entropy of the transmitted codeword given the received sequence at the channel output is derived in [10]:

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

where

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

The bound in (1) holds for any representation of the code by a full-rank parity-check matrix, and it improves the bound in [2]. The symmetry condition for MBIOS channels states that $a(l) = e^l a(-l)$ for all $l \in \mathbb{R}$, and therefore (2) gives that

$$g_p = \mathbb{E}\left[\tanh^{2p}\left(\frac{L}{2}\right)\right], \quad p \in \mathbb{N} \tag{3}$$

where $\mathbb{E}$ designates the statistical expectation with respect to the L-density function a, and L is a random variable which stands for the LLR at the output of the channel given that the input bit is zero. Eq. (3) implies that the non-negative sequence $\{g_p\}_{p\geq 1}$ is monotonically non-increasing and it only depends on the communication channel (but not on the code). Note also that, from (3), $0 \leq g_p < 1$ for all $p \in \mathbb{N}$ (unless the channel is perfect, which then implies that $g_p = 1$ for all values of p).

We note that the conditional entropy on the LHS of (1) depends only on the code and the communication channel, but its lower bound on the RHS of (1) depends also on the specific representation of the code by a bipartite graph.

B. Cycles in Graphs

Definition 1: **[Cycle and cycle length]** A *cycle* in an undirected graph is a closed path. The length of a cycle is the number of edges on this closed path. The *girth* of an undirected graph is defined as the shortest length of its cycles.

Definition 2: **[Tree]** A *tree* is a connected graph that has no cycles.

From Definition 2, a removal of any edge from a tree makes the graph disconnected. An important property of trees is that any two vertices are connected by a single path.

Every graph $\mathcal{G}$ has subgraphs that are trees. This motivates the following definition:

Definition 3: **[Spanning tree]** A *spanning tree* of a connected graph $\mathcal{G}$ is a tree which spans all the vertices of $\mathcal{G}$. Note that by repeatedly removing edges which originally create cycles in the graph, it follows that every connected graph has a spanning tree.

Definition 4: **[Number of components of a graph]** Let $\mathcal{G}$ be a graph (possibly disconnected). The *number of components* of $\mathcal{G}$ is the minimal number of its connected subgraphs whose union forms the graph $\mathcal{G}$ (clearly, a connected graph has a single component).

Definition 5: **[Cycle rank]** Let $\mathcal{G}$ be an un-directed graph with $|V_{\mathcal{G}}|$ vertices, $|E_{\mathcal{G}}|$ edges and $C(\mathcal{G})$ components. The *cycle rank* of $\mathcal{G}$, denoted by $\beta(\mathcal{G})$, is defined as the maximal number of edges which can be removed from the graph without increasing its number of components (note that each component becomes a spanning tree after the removal of these edges).

From Definition 5, the cycle rank of a graph is a measure of the edge redundancy with respect to the connectedness of this graph. The cycle rank satisfies the following equality (see [4, p. 154]):

$$\beta(\mathcal{G}) = |E_{\mathcal{G}}| - |V_{\mathcal{G}}| + C(\mathcal{G}). \tag{4}$$

Definition 6: **[Full spanning forest]** Let $\mathcal{G}$ be an un-directed graph. A *full spanning forest* $\mathcal{F}$ of the graph $\mathcal{G}$ is the subgraph of $\mathcal{G}$ after removing the $\beta(\mathcal{G})$ edges from Definition 5. Clearly, the number of components of $\mathcal{F}$ and $\mathcal{G}$ is the same. Note that a graph may have a multiplicity of full spanning forests.

Definition 7: **[Fundamental cycle]** Let $\mathcal{F}$ be a full spanning forest of an un-directed graph $\mathcal{G}$, and let e be an edge in the relative complement of $\mathcal{F}$. The cycle of the subgraph $\mathcal{F} \cup \{e\}$ (whose existence and uniqueness is guaranteed by [4, Theorem 3.1.11]) is called a *fundamental cycle* of $\mathcal{G}$ which is associated with $\mathcal{F}$.

Remark 1: Each of the edges in the relative complement of a full spanning forest $\mathcal{F}$ gives rise to a *different* fundamental cycle of the graph $\mathcal{G}$.

Definition 8: **[Fundamental system of cycles]** The *fundamental system of cycles* of a graph $\mathcal{G}$ which is associated with a full spanning forest $\mathcal{F}$ is the set of all fundamental cycles of $\mathcal{G}$ associated with $\mathcal{F}$.

Remark 2: From Remark 1, the cardinality of the fundamental system of cycles of $\mathcal{G}$ associated with a full spanning forest of this graph is equal to the cycle rank $\beta(\mathcal{G})$.

Example 1: **[Fundamental system of cycles in a bipartite graph]** This example refers to the bipartite graph in Fig. 1. This graph is connected, but it is clearly not a tree. As an example, consider the cycle $\langle v_9, c_4, v_{10}, c_5, v_9 \rangle$ whose length is 4. Since the number of vertices in this graph is 15 and the number of its edges is 30, then from (4), the cycle rank of this connected graph is $30 - 15 + 1 = 16$.

In order to get a spanning tree of the graph in Fig. 1, we remove repeatedly 16 edges which create cycles while preserving the connectivity of the graph.

The parity-check matrix $\widetilde{H} = [\widetilde{h}_{i,j}]$ in Fig. 2, with 16 bolded zero entries which correspond to the removed

$$H := \begin{array}{c} \\ 1 \\ \mathbf{2} \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \mathbf{8} & 9 & 10 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & \mathbf{0} & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & \mathbf{1} & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & \mathbf{1} & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & \mathbf{0} & 1 & 1 \end{pmatrix} \end{array}$$

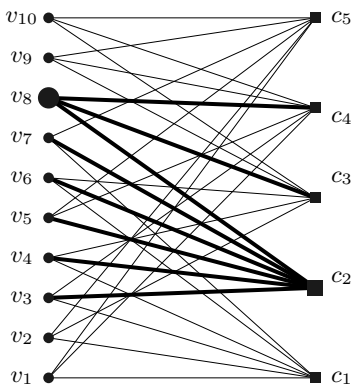

Fig. 1. A parity-check matrix H and the corresponding bipartite graph. For illustrating this relationship, column 8 and row 2 of H are bolded; the corresponding variable and parity-check nodes, and the attached edges are also bolded (this figure appears in [7]).

$$\widetilde{H} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & \mathbf{0} & 0 & \mathbf{0} & \mathbf{0} & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & \mathbf{0} & 1 & 1 & 1 & 0 & 0 \\ 0 & \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{0} & 1 & \mathbf{0} \\ 1 & 0 & \mathbf{0} & 0 & 1 & 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 1 & \mathbf{0} & 0 & 0 & \mathbf{0} & 0 & \mathbf{0} & 0 & 1 & 1 \end{pmatrix} \end{array}$$

Fig. 2. A parity-check matrix which corresponds to a spanning tree of the bipartite graph in Fig. 1. As compared to the parity-check matrix H in Fig. 1, the new parity-check matrix $\widetilde{H}$ is obtained by changing the values of the bolded 16 entries from 1 to 0.

edges from the original graph in Fig. 1, represents a spanning tree of this graph. To exemplify its connectivity, note that the variable nodes v_5 and v_6 are connected by the path $\langle v_6, c_2, v_3, c_1, v_1, c_4, v_5 \rangle$ which is of length 6. This path can be observed directly from the parity-check matrix $\widetilde{H} = [\widetilde{h}_{i,j}]$ by alternate horizontal and vertical moves through the ones of $\widetilde{H}$; explicitly, this path is determined by a horizontal move from $\widetilde{h}_{2,6}$ to $\widetilde{h}_{2,3}$, a vertical move to $\widetilde{h}_{1,3}$, a horizontal move to $\widetilde{h}_{1,1}$, a vertical move to $\widetilde{h}_{4,1}$ and finally a horizontal move to $\widetilde{h}_{4,5}$. In a similar way, it can be verified that every two vertices in the bipartite graph of $\widetilde{H}$ are connected, and it spans all the 15 vertices of the graph in Fig. 1 (since there is no row or column in $\widetilde{H}$ which is a zero vector). Hence, this graph is indeed a spanning tree of the bipartite graph in Fig. 1. This spanning tree enables to obtain a set of 16 fundamental cycles by returning back a single bolded zero in Fig. 2 (among its 16 bolded zeros) to 1. For example, by setting $\widetilde{h}_{1,6} = 1$ (which is equivalent to returning the edge which connects v_6 with c_1), we get the fundamental cycle $\langle v_3, c_2, v_6, c_1, v_3 \rangle$.

III. Information-Theoretic Bounds

This section introduces information-theoretic bounds which are related to the average right degree, and the number of fundamental systems of cycles in the bipartite graphs of LDPC code ensembles.

Theorem 1: **[On the average degree of the parity-check nodes]** Let $\mathcal{C}$ be a binary linear block code of block length n whose transmission takes place over an MBIOS channel. Let $\mathcal{G}$ be a bipartite graph which corresponds to a full-rank parity-check matrix of $\mathcal{C}$. Let C designate the capacity of the channel, in bits per channel use, and a be the L-density function of this channel. Assume that the code rate is (at least) a fraction $1-\varepsilon$ of the channel capacity (where $0<\varepsilon<1$), and the code achieves a block error probability P_{B} or a bit error probability P_{b} under some decoding algorithm. Then, the average right degree of the bipartite graph (i.e., the average degree of the parity-check nodes in $\mathcal{G}$) satisfies

$$a_{\mathrm{R}} \geq \frac{2\ln\left(\frac{1}{1-2h_2^{-1}\left(\frac{1-C-\delta}{1-(1-\varepsilon)C}\right)}\right)}{\ln\left(\frac{1}{g_1}\right)} \tag{5}$$

where $g_1 = \mathbb{E}[\tanh^2(L/2)]$ depends only on the MBIOS communication channel (L is a random variable which refers to the log-likelihood ratio at the channel output, given that the binary input symbol to the channel is zero), and

$$\delta \triangleq \begin{cases} P_{\mathrm{B}} + \frac{h_2(P_{\mathrm{B}})}{n} & \text{for a block error probability } P_{\mathrm{B}} \\ h_2(P_{\mathrm{b}}) & \text{for a bit error probability } P_{\mathrm{b}} \end{cases}. \tag{6}$$

Furthermore, among all the MBIOS channels which exhibit a given capacity C and for which a target block error probability (P_{B}) or a bit error probability (P_{b}) is obtained under some decoding algorithm, a universal lower bound on a_{R} holds by replacing g_1 on the RHS of (5) with C.

For the BEC, the following tightened version of (5) holds:

$$a_{\mathrm{R}} \geq \frac{\ln\left(1+\frac{p-P_{\mathrm{b}}}{(1-p)\varepsilon+P_{\mathrm{b}}}\right)}{\ln\left(\frac{1}{1-p}\right)} \tag{7}$$

where p is the erasure probability of the channel, and P_{b} is the bit erasure probability at the decoder.

Proof: Let $\mathbf{X}$ be a random codeword from the binary linear block code $\mathcal{C}$, and let $\mathbf{Y}$ designate the output of the communication channel when $\mathbf{X}$ is transmitted. Based on the assumption that the code $\mathcal{C}$ is represented by a full-rank parity-check matrix and $\mathcal{G}$ is the corresponding bipartite graph which represents this code, then inequality (1) holds. Since $f(t)=x^t$ is convex for any $x \geq 0$ then Jensen's inequality gives

$$\Gamma(x) = \sum_i \Gamma_i x^i \geq x^{\sum_i i\,\Gamma_i} = x^{a_{\mathrm{R}}}, \quad x \geq 0\,.$$

Substituting the inequality above in (1) implies that

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \geq R - C + \frac{1-R}{2\ln 2}\sum_{k=1}^{\infty}\frac{g_k^{a_{\mathrm{R}}}}{k(2k-1)}\,. \tag{8}$$

Lemma 1:

$$g_k \geq (g_1)^k\,, \quad \forall k \in \mathbb{N}. \tag{9}$$

Proof: For $k \geq 1$, Jensen's inequality and (3) give

$$\begin{aligned} g_k &= \mathbb{E}\left[\tanh^{2k}\left(\frac{L}{2}\right)\right] \\ &\geq \left(\mathbb{E}\left[\tanh^{2}\left(\frac{L}{2}\right)\right]\right)^k \\ &= (g_1)^k\,. \end{aligned}$$

■

The substitution of (9) in (8) gives

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \geq R - C + \frac{1-R}{2\ln 2}\sum_{k=1}^{\infty}\frac{(g_1^{a_{\mathrm{R}}})^k}{k(2k-1)}\,. \tag{10}$$

Using the equality

$$\frac{1}{2\ln 2}\sum_{k=1}^{\infty}\frac{u^k}{k(2k-1)} = 1 - h_2\left(\frac{1-\sqrt{u}}{2}\right),\ \forall\, u \in [0,1]. \tag{11}$$

and substituting it into the RHS of (10) gives the following lower bound on the conditional entropy:

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \geq 1 - C - (1-R)\,h_2\left(\frac{1-g_1^{a_{\mathrm{R}}/2}}{2}\right). \tag{12}$$

On the other hand, Fano's inequality provides the upper bound

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \leq \begin{cases} R\,P_{\mathrm{B}} + \frac{h_2(P_{\mathrm{B}})}{n} \\ R\,h_2(P_{\mathrm{b}}) \end{cases} \tag{13}$$

where, for the bound which is expressed in terms of the bit error probability P_{b}, one can assume without any loss of generality that the first nR bits of the code are its information bits, and their knowledge is sufficient for determining the codeword. In order to make the statement also valid for code ensembles, we rely on the inequality $R \leq 1$, and loosen the bound in (13) to get

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \leq \delta \tag{14}$$

where δ is introduced in (6). Combining (12) and (14) gives

$$\delta \geq 1 - C - (1-R)\,h_2\left(\frac{1-g_1^{a_{\mathrm{R}}/2}}{2}\right). \tag{15}$$

Since the RHS of (15) is monotonically increasing in R, then following our assumption that $R \geq (1-\varepsilon)C$, the bound is loosened by replacing R with $(1-\varepsilon)C$. This gives the inequality

$$h_2\left(\frac{1-g_1^{a_{\mathrm{R}}/2}}{2}\right) \geq \frac{1-C-\delta}{1-(1-\varepsilon)C}\,.$$

Since the binary entropy function h_2 is monotonically increasing on $[0,\frac{1}{2}]$ then

$$g_1^{\frac{a_{\mathrm{R}}}{2}} \leq 1 - 2h_2^{-1}\left(\frac{1-C-\delta}{1-(1-\varepsilon)C}\right)$$

which gives the lower bound on a_{R} in (5).

Let us now consider the particular case where the transmission is over the BEC. Note that for a BEC with erasure probability p, $g_k = 1-p$ for all $k \in \mathbb{N}$ (in this case we have

$L \in \{0, +\infty\}$ with probabilities p and $1-p$, respectively, and the equality $\tanh(+\infty) = 1$ is exploited in (3)). Therefore (8) is particularized to

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \geq R - C + \frac{(1-R)(1-p)^{a_{\mathrm{R}}}}{2\ln 2} \sum_{k=1}^{\infty} \frac{1}{k(2k-1)} \,.$$

Substituting $u = 1$ in (11) gives the equality

$$\frac{1}{2\ln 2} \sum_{k=1}^{\infty} \frac{1}{k(2k-1)} = 1 \tag{16}$$

and

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \geq R - C + (1-R)(1-p)^{a_{\mathrm{R}}} \,. \tag{17}$$

Note that the RHS of (17) is monotonic increasing as a function of the rate R. Following the assumption that $R \geq (1-\varepsilon)C$ where $C = 1-p$ is the capacity of the BEC, we get

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \geq -\varepsilon(1-p) + \big(1-(1-\varepsilon)(1-p)\big)(1-p)^{a_{\mathrm{R}}} \,. \tag{18}$$

Similarly to (13) and (14), we get for the BEC

$$\frac{H(\mathbf{X}|\mathbf{Y})}{n} \leq P_{\mathrm{b}} \tag{19}$$

where the decoder finds X_i with probability $1-P_{\mathrm{b}}$; otherwise, the bit X_i is not determined by the decoder, and its conditional entropy (given the sequence $\mathbf{Y}$) is upper bounded by 1 bit. Combining (18) with (19) gives

$$P_{\mathrm{b}} \geq -\varepsilon(1-p) + \big(1-(1-\varepsilon)(1-p)\big)(1-p)^{a_{\mathrm{R}}} \,. \tag{20}$$

Finally, the lower bound on the average right degree in (7) follows from (20) by simple algebra. Note that in the case where $P_{\mathrm{b}} = 0$, the resulting lower bound coincides with the result obtained in [8, p. 1619] (though it was derived there in a different way), and it gets the form

$$a_{\mathrm{R}} \geq \frac{\ln\left(1 + \frac{p}{(1-p)\varepsilon}\right)}{\ln\left(\frac{1}{1-p}\right)}. \tag{21}$$

■

Remark 3: **[The relation of Theorem 1 to the bound in [10]]** In the particular case where P_{b} vanishes, the bound in (5) forms a tightened version of the bound given in [10, Eq. (77)]. This point is clarified in [9]. In the limit where the gap (in rate) to capacity vanishes (and with vanishing P_{b}), the lower bounds on the average right degree in (5) and [10, Eq. (77)] both grow like the logarithm of the inverse of this gap, and they therefore possess the same asymptotic behavior where

$$a_{\mathrm{R}} \triangleq a_{\mathrm{R}}(\varepsilon) = \Omega\left(\ln \frac{1}{\varepsilon}\right). \tag{22}$$

However, in spite of the similarity in the asymptotic behavior of the two lower bounds as $\varepsilon \to 0$, they may differ significantly even for rather small values of ε (see [9]).

Theorem 1 also provides a universal lower bound on the average right degree for the set of all MBIOS channels with a given capacity C. This theorem states the conditions where the bound in (5) gets its extreme values among all MBIOS channels which exhibit a given capacity.

Remark 4: **[Adaptation of Theorem 1 to LDPC code ensembles]** As is proved in [9, Appendix I], Theorem 1 can be adapted to hold for an arbitrary ensemble of (n, λ, ρ) LDPC codes. In this case, the requirement of a full-rank parity-check matrix of a particular code $\mathcal{C}$ from this ensemble is relaxed by requiring that the design rate of the LDPC code ensemble is equal to a fraction $1-\varepsilon$ of the channel capacity. In this case, P_{b} and P_{B} stand for the average bit and block error (or erasure) probabilities of the ensemble under some decoding algorithm.

Theorem 2: **[On the asymptotic average cardinality of the fundamental system of cycles of LDPC code ensembles]** Let $\big\{(n, \lambda, \rho)\big\}$ be a sequence of LDPC code ensembles whose transmission takes place over an memoryless binary-input output-symmetric (MBIOS) channel. Let the design rate of these ensembles be a fraction $1-\varepsilon$ of the channel capacity C, and assume that the average bit error/ erasure probability of this sequence vanishes under some decoding algorithm as we let the block length (n) tend to infinity. Consider the average cardinality of the fundamental system of cycles in bipartite graphs from the LDPC code ensemble (n, λ, ρ) where the graphs are chosen uniformly at random (the cardinality of the fundamental system of cycles in a graph $\mathcal{G}$ is equal to its cycle rank $\beta(\mathcal{G})$). Then, the following asymptotic lower bound holds:

$$\begin{aligned} &\liminf_{n\to\infty} \frac{\mathbb{E}_{\mathrm{LDPC}(n,\lambda,\rho)}\big[\beta(\mathcal{G})\big]}{n} \\ &\geq \frac{(1-C)\,\ln\Bigg(g_1\,\Big[1-2h_2^{-1}\Big(\frac{1-C}{1-(1-\varepsilon)C}\Big)\Big]^{-2}\Bigg)}{\ln\Big(\frac{1}{g_1}\Big)} - 1. \end{aligned} \tag{23}$$

For a BEC whose erasure probability is p, a tightened bound gets the form:

$$\liminf_{n\to\infty} \frac{\mathbb{E}_{\mathrm{LDPC}(n,\lambda,\rho)}\big[\beta(\mathcal{G})\big]}{n} \geq \frac{p\,\ln\big(1-p+\frac{p}{\varepsilon}\big)}{\ln\Big(\frac{1}{1-p}\Big)} - 1. \tag{24}$$

Outline of the Proof of Theorem 2

We provide in the following an outline of the proof of Theorem 2. Due to space limitations, we refer the reader to [9] for a full proof.

The following lemma relies on the background material in Section IV, and it serves for proving Theorem 2.

Lemma 2: **[Cardinality of the fundamental system of cycles]** Under the assumptions of Theorem 2, the cardinality of the fundamental system of cycles of a bipartite graph $\mathcal{G}$, associated with a full spanning forest of $\mathcal{G}$, is larger than

$$n\big[(1-R)(a_{\mathrm{R}}-1)-1\big] \tag{25}$$

where a_{R} can be replaced by the lower bounds in (5) and (7) for a general MBIOS channel and a BEC, respectively. From [9, Theorem 1], the cardinality of the fundamental system of cycles of the bipartite graph $\mathcal{G}$ which is associated with a full spanning forest of this graph is $\Omega\big(\ln \frac{1}{\varepsilon}\big)$.

Proof: From Remark 2 (see Section II), the cardinality of the fundamental system of cycles of a bipartite graph $\mathcal{G}$, which

is associated with a full spanning forest of $\mathcal{G}$, is equal to the cycle rank $\beta(\mathcal{G})$. From Eq. (4), $\beta(\mathcal{G}) > |E_{\mathcal{G}}| - |V_{\mathcal{G}}|$ where $|E_{\mathcal{G}}|$ and $|V_{\mathcal{G}}|$ designate the number of edges and vertices. Specializing this for a bipartite graph $\mathcal{G}$ which represents a full-rank parity-check matrix of a binary linear block code, the number of vertices satisfies $|V_{\mathcal{G}}| = n(2-R)$ (since there are n variable nodes and $n(1-R)$ parity-check nodes in the graph) and the number of edges satisfies $|E_{\mathcal{G}}| = n(1-R)a_{\mathrm{R}}$. Combining these equalities gives the lower bound on the cardinality of the fundamental system of cycles in (25). ■

Remark 5: Theorem 2 provides two results which are of the type $\Omega\left(\ln \frac{1}{\varepsilon}\right)$. This implies that the average cardinality of the fundamental system of cycles grows at lease like the logarithm of the reciprocal of the gap to capacity.

Lemma 3: **[Extreme values of g_1 among all MBIOS channels with a given capacity]** Among all the MBIOS channels with a given capacity C, the value of g_1 satisfies

$$C \leq g_1 \leq \left(1 - 2h_2^{-1}(1-C)\right)^2 \tag{26}$$

and these upper and lower bounds on g_1 are attained for a BSC and BEC, respectively.

Proof: See [9, Appendix II]. ■

Remark 6: This lemma is in fact equivalent to the statement in [5, Theorem 1]. In [9, Appendix II], we present an alternative proof (which is more elementary).

From Theorem 2 and Lemma 3, the following corollary follows:

Corollary 1: Consider the family of all MBIOS channels which exhibit a given channel capacity C. Then, under the assumptions of Theorem 2, the lower bound in (23) holds for every MBIOS channel from this family when the parameter g_1 is replaced with the capacity C.

IV. Numerical Results

We provide here some numerical results for the information-theoretic lower bound on the cardinality of the fundamental system of cycles of LDPC code ensembles.

Theorem 2 considers an arbitrary sequence of LDPC code ensembles, specified by a pair of degree distributions, whose transmission takes place over an MBIOS channel. This corollary refers to the asymptotic case where we let the block length of the ensembles in this sequence tend to infinity and the bit error (or erasure) probability vanishes; the design rate of these ensembles is assumed to be a fraction $1-\varepsilon$ of the channel capacity (for an arbitrary $\varepsilon \in (0,1)$). In Theorem 2, Eq. (23) applies to a general MBIOS channel and a tightened version of this bound is given in (24) for the BEC. Based on these results, the asymptotic average cardinality of the fundamental system of cycles for bipartite graphs representing codes from LDPC code ensembles as above, where this average cardinality is normalized with respect to the block length, grows at least like $\ln \frac{1}{\varepsilon}$. We consider here the binary symmetric channel (BSC), binary erasure channel (BEC), and binary-input additive white gaussian channel (BIAWGNC) as three representatives of the class of MBIOS channels, and assume that the design rate of the LDPC code ensembles is fixed to one-half bit per channel use. It is shown in Fig. 3 that for a given gap (ε) to the channel capacity and for a fixed design rate, the extreme values of this lower bounds correspond to the BSC and BEC (which attain the maximal and minimal values, respectively). This observation is consistent with Theorem 2.

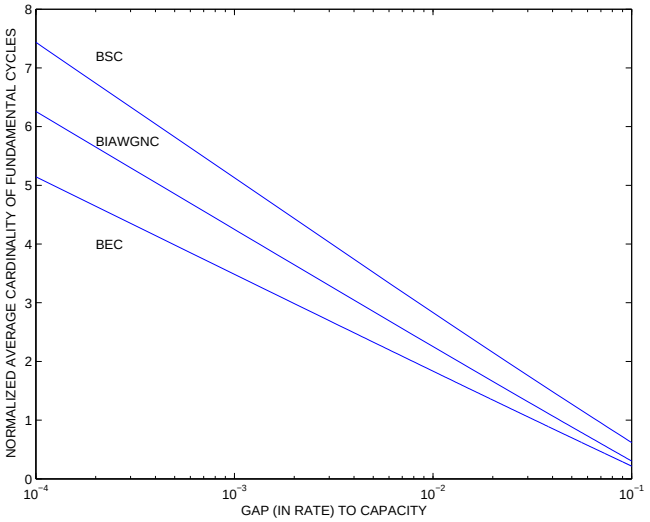

Fig. 3. Plot of the asymptotic lower bounds in Theorem 2 (see Eqs. (23) and (24)) for memoryless binary-input output-symmetric (MBIOS) channels. These lower bounds correspond to the average cardinality of the fundamental system of cycles for bipartite graphs representing codes from an arbitrary LDPC code ensemble; the above quantity is normalized with respect to the block length of the ensemble, and the asymptotic result refers to the case where we consider a sequence of LDPC code ensembles whose block lengths tend to infinity. The bounds are plotted versus the achievable gap (in rate) between the channel capacity and the design rate of the LDPC code ensembles. This figure shows the bounds for the binary symmetric channel (BSC), binary-input AWGN channel (BIAWGNC) and the binary erasure channel (BEC) where it is assumed that the design rate of the LDPC code ensembles is equal to one-half bit per channel use.

References

[1] A. Amraoui and R. Urbanke, LdpcOpt: Software for optimizing the degree distrbutions of LDPC code ensembles. [Online]. Available: http://lthcwww.epfl.ch/research/ldpcopt/index.php.

[2] D. Burshtein, M. Krivelevich, S. Litsyn and G. Miller, "Upper bounds on the rate of LDPC codes," *IEEE Trans. on Information Theory*, vol. 48, no. 9, pp. 2437–2449, September 2002.

[3] 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.

[4] J. Gross and J. Yellen, *Graph Theory and its Applications*, CRC Press Series on Discrete Mathematics and its Applications, 1999.

[5] Y. Jiang, A. Ashikhmin, R. Koetter and A. C. Singer, "Extremal problems of information combining," *IEEE Trans. on Information Theory*, vol. 54, no. 1, pp. 51–71, January 2008.

[6] T. Richardson and R. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008. [Online]. Available: http://lthcwww.epfl.ch/mct/index.php.

[7] T. Richardson and R. Urbanke, "The renaissance of Gallager's low-density parity-check codes," *IEEE Communications Magazine*, vol. 41, no. 8, pp. 126–131, August 2003.

[8] 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.

[9] I. Sason, "On universal properties of capacity-approaching LDPC code ensembles," *IEEE Trans. on Information Theory*, vol. 55, no. 7, July 2009.

[10] G. Wiechman and I. Sason, "Parity-check density versus performance of binary linear block codes: New bounds and applications," *IEEE Trans. on Information Theory*, vol. 53, no. 2, pp. 550–579, February 2007.