Performance Analysis and Design of Two Edge-Type LDPC Codes for the BEC Wiretap Channel

Vishwambhar Rathi, Mattias Andersson, *Student Member, IEEE*, Ragnar Thobaben, *Member, IEEE*, Joerg Kliewer, *Senior Member, IEEE*, and Mikael Skoglund, *Senior Member, IEEE*

***Abstract*—We consider transmission over a wiretap channel where both the main channel and the wiretapper's channel are binary erasure channels (BEC). A code construction method is proposed using two edge-type low-density parity-check (LDPC) codes based on the coset encoding scheme. Using a single edge-type LDPC ensemble with a given threshold over the BEC, we give a construction for a two edge-type LDPC ensemble with the same threshold. If the given single edge-type LDPC ensemble has degree two variable nodes, our construction gives rise to degree one variable nodes in the code used over the main channel. This results in zero threshold over the main channel. In order to circumvent this problem, the degree distribution of the two edge-type LDPC ensemble is numerically optimized. We find that the resulting ensembles are able to perform close to the boundary of the rate-equivocation region of the wiretap channel. Further, a method to compute the ensemble average equivocation of two edge-type LDPC ensembles is provided by generalizing a recently published approach to measure the equivocation of single edge-type ensembles for transmission over the BEC in the point-to-point setting. From this analysis, we find that relatively simple constructions give very good secrecy performance.**

I. Introduction

Wyner introduced the notion of a wiretap channel in [3]. In this paper, we assume that the channel between the transmitter and the receiver (the main channel) and the channel between the transmitter and the wiretapper (the wiretapper's channel) are both binary erasure channels (BECs). We use the short form BEC-WT for such a wiretap channel. A detailed information theoretic overview of general wiretap channels can be found in [4]. In [5] and [6], the authors have given code design criteria using sparse graph codes. Their approach is based on a coset coding scheme using nested codes [7]. In [8], the authors have suggested a coding scheme for the BEC-WT that guarantees strong secrecy for a noiseless main channel and some range of the erasure probability for the wiretapper's channel using duals of sparse graph codes. In [9], it was shown that random linear codes can achieve the secrecy capacity over the binary symmetric wiretap channel and an upper bound on the information leakage was derived. Recently, it has been shown that using Arikan's polar codes [10], it is possible to achieve the whole rate-equivocation region [11]–[14].

We propose a code construction method using two edge-type LDPC codes based on the coset encoding scheme. The *threshold* of a code (or an ensemble) for transmission over the BEC is the largest erasure probability for which reliable communication is possible. Using a single edge-type LDPC ensemble with a given threshold over the BEC, we give a construction for a two edge-type LDPC ensemble with the same threshold. Thus, if the single edge-type LDPC ensemble is capacity achieving over the wiretapper's channel, our construction of the two edge-type LDPC ensemble guarantees perfect secrecy. Hence, it achieves secrecy capacity if the main channel is noiseless.

However, our construction cannot guarantee reliability over a noisy main channel if the given single edge-type LDPC ensemble has degree two variable nodes. This is because our approach gives rise to degree one variable nodes in the code used over the main channel. This results in zero threshold over the main channel. In order to circumvent this problem, we numerically optimize the degree distribution of the two edge-type LDPC ensemble. We find that the resulting codes approach the rate-equivocation region of the wiretap channel. Note that reliability, which corresponds to the probability of decoding error for the intended receiver, can be easily measured using density evolution recursion. However, secrecy, which is given by the equivocation of the message conditioned on the wiretapper's observation, cannot be easily calculated. Méasson *et al*. have derived a method to measure equivocation for a broad range of single edge-type LDPC ensembles for point-to-point transmission over the BEC [15]. From now onward, we call it the MMU method.[1] The MMU method was extended to nonbinary LDPC codes for transmission over the BEC in [16] and [17]. By generalizing the MMU method for two edge-type LDPC ensembles, we show how the equivocation for the wiretapper can be computed. We find that relatively simple constructions give very good secrecy performance.

[1]We call it the MMU method in acknowledgment of Méasson, Montanari, and Urbanke, the authors of [15].

Manuscript received September 22, 2010; revised November 30, 2011; accepted August 03, 2012. Date of publication October 02, 2012; date of current version January 16, 2013. This work was supported in part by the Swedish Research Council and in part by the U.S. National Science Foundation under Grants CCF-0830666, CCF-1017632, and CCF-1161774. This paper was presented in part at the 43rd Annual Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, November 2009 [1], and the 44th Annual Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, November 2010.

V. Rathi is with Nvidia Corporation, Santa Clara, CA 95050 USA (e-mail: vrathi@gmail.com).

M. Andersson, R. Thobaben, and M. Skoglund are with the School of Electrical Engineering and the ACCESS Linnaeus Centre, KTH Royal Institute of Technology, 100 44 Stockholm, Sweden (e-mail: amattias@ee.kth.se; ragnar.thobaben@ee.kth.se; skoglund@ee.kth.se).

J. Kliewer is with the Klipsch School of Electrical and Computer Engineering, New Mexico State University, Las Cruces, NM 88003 USA (e-mail: jkliewer@nmsu.edu).

Communicated by I. Sason, Associate Editor for Coding Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2012.2219577

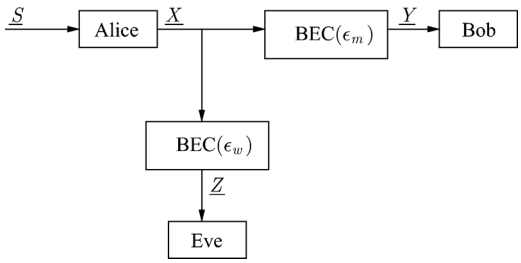

Fig. 1. BEC wiretap channel.

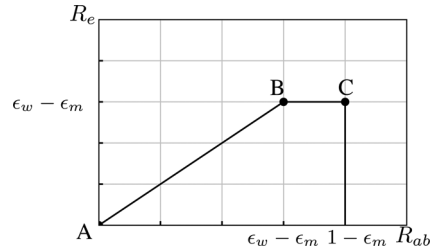

Fig. 2. Achievable rate equivocation region for the BEC-WT(ϵ_m, ϵ_w).

Our paper is organized in the following way. Section II is a preliminary section which consists of well-known results and techniques. In Section II, we give various definitions, describe the coset encoding method and two edge-type LDPC ensembles, and give the density evolution recursion for two edge-type LDPC ensembles. Section III contains the code design and optimization for the BEC-WT. In Section IV, we show that the task of computing the equivocation is equivalent to generalizing the MMU method for two edge-type LDPC ensembles for point-to-point transmission over the BEC. We generalize the MMU method for two edge-type LDPC ensembles in Section V. In Section VI, we present various examples to elucidate the computation of equivocation and show that our optimized degree distributions also approach the information theoretic equivocation limit. Finally, we conclude in Section VII with some discussion and open problems.

II. Preliminaries

A. Definitions

A wiretap channel is depicted in Fig. 1. In general, the channel from Alice to Bob and the channel from Alice to Eve can be any discrete memoryless channels. In this paper, we will restrict ourselves to the setting where both channels are BECs. We denote a BEC with erasure probability ϵ by BEC(ϵ). In a wiretap channel, Alice communicates a message $\underline{S}$, which is chosen uniformly at random from the message set $\mathcal{S}$, to Bob through the main channel which is a BEC(ϵ_m). Alice performs this task by encoding $\underline{S}$ as an n bit vector $\underline{X}$ and transmitting $\underline{X}$ across the BEC(ϵ_m). Bob receives a noisy version of $\underline{X}$ which is denoted by $\underline{Y}$. Eve observes $\underline{X}$ via the wiretapper's channel BEC(ϵ_w) and receives a noisy version of $\underline{X}$ denoted by $\underline{Z}$. We denote such a wiretap channel by BEC-WT(ϵ_m, ϵ_w).

The encoding of a message $\underline{S}$ by Alice should be such that Bob is able to decode $\underline{S}$ reliably and $\underline{Z}$ provides as little information as possible to Eve about $\underline{S}$. In the following section, we define a code for the wiretap channel and give relevant definitions.

Definition 1 (Code for Wiretap Channel): A code of rate R_{ab} with blocklength n for the wiretap channel is given by a message set $\mathcal{S}$ of cardinality $|\mathcal{S}| = 2^{nR_{ab}}$, and a set of disjoint subcodes $\{\mathcal{C}(\underline{s}) \subset \mathcal{X}^n\}_{\underline{s} \in \mathcal{S}}$. To encode the message $\underline{s} \in \mathcal{S}$, Alice chooses one of the codewords in $\mathcal{C}(\underline{s})$ uniformly at random and transmits it. Bob uses a decoder $\phi : \mathcal{Y}^n \to \mathcal{S}$ to determine which message was sent.

We now define the achievability of rate of communication from Alice to Bob and equivocation of the message from Alice to Bob for Eve.

Definition 2 (Achievability of Rate Equivocation): A rate-equivocation pair (R_{ab}, R_e) is said to be achievable if $\forall \delta > 0$, there exists a sequence of codes of rate R_{ab} of length n and decoders ϕ_n such that the following reliability and secrecy criteria are satisfied:

$$\text{Reliability: } \lim_{n\to\infty} \quad P(\phi_n(\underline{Y}) \neq \underline{S}) < \delta \tag{1}$$

$$\text{Secrecy: } \liminf_{n\to\infty} \frac{1}{n} H(\underline{S}|\underline{Z}) > R_e - \delta. \tag{2}$$

Note that in this paper, we use the weak notion of secrecy as opposed to the strong notion of secrecy [4]. With a slight abuse of terminology, when we say equivocation we mean the normalized equivocation as defined in the left-hand side of (2). From the achievable rate-equivocation region for general wiretap channels given in [3], the set of achievable pairs (R_{ab}, R_e) for the BEC-WT(ϵ_m, ϵ_w) is given by

$$R_e \leq R_{ab} \leq 1 - \epsilon_m, \quad 0 \leq R_e \leq \epsilon_w - \epsilon_m. \tag{3}$$

The rate region described by (3) is depicted in Fig. 2.

The line segment AB in Fig. 2 corresponds to perfect secrecy.

Definition 3 (Perfect Secrecy and Secrecy Capacity [3]): The points in the achievable region where $R_{ab} = R_e$ correspond to *perfect secrecy*, i.e., for these points $I(\underline{Z}; \underline{S})/n \to 0$. The highest achievable rate R_{ab} at which we can achieve perfect secrecy is called the *secrecy capacity* and we denote it by C_S.

For the BEC-WT(ϵ_w, ϵ_m), we have $C_S = \epsilon_w - \epsilon_m$.

We now describe the coset encoding and syndrome decoding method. Let H be an $n(1-R) \times n$ LDPC matrix. Let $\mathcal{C}$ be the code whose parity-check matrix is H. Let H_1 and H_2 be the submatrices of H such that

$$H = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}$$

where H_1 is an $n(1-R_1) \times n$ matrix. Clearly, $R_1 > R$. Let $\mathcal{C}_1$ be the code with parity-check matrix H_1. $\mathcal{C}$ is the coarse code and $\mathcal{C}_1$ is the fine code in the nested code $(\mathcal{C}_1, \mathcal{C})$[7]. Also, $\mathcal{C}_1$ is partitioned into $2^{n(R_1-R)}$ disjoint subsets given by the

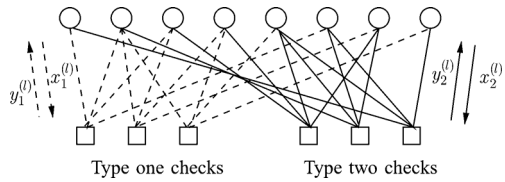

Fig. 3. Two edge-type LDPC code.

cosets of $\mathcal{C}$. Alice uses the *coset encoding method*, which we now describe to communicate her message to Bob.

Definition 4 (Coset Encoding Method [3]): Assume that Alice wants to transmit a message whose binary representation is given by an $n(R_1 - R)$-bit vector $\underline{S}$. To do this, she performs coset encoding by transmitting $\underline{X}$, which is a randomly chosen solution of

$$\begin{bmatrix} H_1 \\ H_2 \end{bmatrix} \underline{X} = [0 \cdots 0 \ \underline{S}]^T.$$

Bob uses the following *syndrome decoding* to retrieve the message from Alice.

Definition 5 (Syndrome Decoding): After observing $\underline{Y}$, Bob obtains an estimate $\hat{\underline{X}}$ for $\underline{X}$ using the parity check equations $H_1 \underline{X} = 0$. Then, he computes an estimate $\hat{\underline{S}}$ for $\underline{S}$ as $\hat{\underline{S}} = H_2 \hat{\underline{X}}$, where $\hat{\underline{S}}$ is the syndrome of $\hat{\underline{X}}$ with respect to the matrix H_2.

A natural candidate for coset encoding is a two edge-type LDPC code [18]. In the following section, we describe two edge-type LDPC ensemble.

B. Two Edge-Type LDPC Ensemble

A two edge-type matrix H has form

$$H = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}. \tag{4}$$

The two types of edges are the edges connected to check nodes in H_1 and those connected to check nodes in H_2. An example of a two edge-type LDPC code is shown in Fig. 3.

We now define the degree distribution of a two edge-type LDPC ensemble. Let $\lambda_{l_1 l_2}^{(j)}$ denote the fraction of type j ($j = 1$ or 2) edges connected to variable nodes with l_1 outgoing type one edges and l_2 outgoing type two edges. The fraction $\lambda_{l_1 l_2}^{(j)}$ is calculated with respect to the total number of type j edges. Let $\Lambda_{l_1 l_2}$ be the fraction of variable nodes with l_1 outgoing edges of type one and l_2 outgoing edges of type two. This gives the following relationships between Λ, $\lambda^{(1)}$, and $\lambda^{(2)}$:

$$\lambda_{l_1 l_2}^{(1)} = \frac{l_1 \Lambda_{l_1 l_2}}{\sum_{i_1, i_2} i_1 \Lambda_{i_1 i_2}} \tag{5}$$

$$\lambda_{l_1 l_2}^{(2)} = \frac{l_2 \Lambda_{l_1 l_2}}{\sum\limits_{i_1, i_2} i_2 \Lambda_{i_1 i_2}} \tag{6}$$

$$\Lambda_{l_1 l_2} = \frac{\frac{\lambda_{l_1 l_2}^{(1)}}{l_1}}{\sum_{i_1, i_2} \frac{\lambda_{i_1 i_2}^{(1)}}{i_1}} = \frac{\frac{\lambda_{l_1 l_2}^{(2)}}{l_2}}{\sum_{i_1, i_2} \frac{\lambda_{i_1 i_2}^{(2)}}{i_2}}. \tag{7}$$

Remark: Note that if a two edge-type LDPC ensemble is specified on the variable node side using the degree distributions $\lambda^{(1)}$, $\lambda^{(2)}$ (from the edge perspective), then the second equality in (7) must be satisfied.

Similarly, let $\rho_r^{(j)}$ and $\Gamma_r^{(j)}$ denote the degree distribution of type j edges on the check node side from the edge and node perspective, respectively. Note that only one type of edges is connected to a particular check node. $\Gamma_r^{(j)}$ and $\rho_r^{(j)}$ are related as follows:

$$\rho_r^{(j)} = \frac{r \Gamma_r^{(j)}}{\sum\limits_i i \Gamma_i^{(j)}} \tag{8}$$

$$\Gamma_r^{(j)} = \frac{\frac{\rho_r^{(j)}}{r}}{\sum\limits_i \frac{\rho_i^{(j)}}{i}}. \tag{9}$$

An equivalent definition of the degree distribution is given by the following polynomials:

$$\Lambda(x, y) = \sum_{l_1, l_2} \Lambda_{l_1 l_2} x^{l_1} y^{l_2} \tag{10}$$

$$\lambda^{(1)}(x, y) = \sum_{l_1, l_2} \lambda_{l_1 l_2}^{(1)} x^{l_1 - 1} y^{l_2} \tag{11}$$

$$\lambda^{(2)}(x, y) = \sum_{l_1, l_2} \lambda_{l_1 l_2}^{(1)} x^{l_1} y^{l_2 - 1} \tag{12}$$

$$\Gamma^{(j)}(x) = \sum_r \Gamma_r^{(j)} x^r, \quad j = 1, 2 \tag{13}$$

$$\rho^{(j)}(x) = \sum_r \rho_r^{(j)} x^{r-1}, \quad j = 1, 2. \tag{14}$$

Like the single edge-type LDPC ensemble of [19], the two edge-type LDPC ensemble with blocklength n and degree distribution $\{\lambda^{(1)}, \lambda^{(2)}, \rho^{(1)}, \rho^{(2)}\}$ ($\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$ from node perspective) is the collection of all bipartite graphs satisfying the degree distribution constraints, where we allow multiple edges between two nodes. We will denote a *left regular* two edge-type LDPC ensemble for which $\Lambda(x, y) = x^{l_1} y^{l_2}$ by $\{l_1, l_2, \Gamma^{(1)}, \Gamma^{(2)}\}$.

Consider the two edge-type LDPC ensemble $\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$. If we consider the ensemble of the subgraph induced by one particular type of edges, then it is easy to see that the resulting ensemble is the single edge-type LDPC ensemble and we can easily calculate its degree distribution. Let $\{\Lambda^{(j)}, \Gamma^{(j)}\}$ be the degree distribution from node perspective ($\{\lambda^{(j)}, \rho^{(j)}\}$ from edge perspective) of the ensemble induced by type j edges, $j = 1, 2$. Then, $\Lambda^{(j)}$, for $j = 1, 2$, is given by

$$\Lambda_{l_1}^{(1)} = \sum_{l_2} \Lambda_{l_1 l_2}, \quad \Lambda_{l_2}^{(2)} = \sum_{l_1} \Lambda_{l_1 l_2}. \tag{15}$$

The corresponding polynomials are defined as

$$\Lambda^{(1)}(x) = \sum_i \Lambda_i^{(1)} x^i, \quad \Lambda^{(2)}(x) = \sum_i \Lambda_i^{(2)} x^i. \tag{16}$$

To illustrate the relationship between various degree distributions, we consider a two edge-type LDPC ensemble with degree distribution

$$\Lambda(x, y) = 0.2x^3 y^4 + 0.4x^3 y^5 + 0.4x^6 y^6$$
$$\Gamma^{(1)}(x) = 0.6x^7 + 0.4x^8$$
$$\Gamma^{(2)}(x) = x^{10}.$$

Using (5)–(9) and (15), we obtain

$$\begin{aligned}\lambda^{(1)}(x,y) &= \frac{1}{7}x^2y^4 + \frac{2}{7}x^2y^5 + \frac{4}{7}x^5y^6\\ \lambda^{(2)}(x,y) &= \frac{2}{13}x^3y^3 + \frac{5}{13}x^3y^4 + \frac{6}{13}x^6y^5\\ \rho^{(1)}(x) &= \frac{21}{37}x^6 + \frac{16}{37}x^7\\ \rho^{(2)}(x) &= x^9\\ \Lambda^{(1)}(x) &= 0.6x^3 + 0.4x^6\\ \Lambda^{(2)}(x) &= 0.2x^4 + 0.4x^5 + 0.4x^6.\end{aligned}$$

We now derive the density evolution equations for two edge-type LDPC ensembles, assuming that transmission takes place over the $\mathrm{BEC}(\epsilon)$. Let $x_j^{(l)}$ denote the probability that a message from a variable node to a check node on an edge of type j in iteration l is erased. Clearly

$$x_j^{(1)} = \epsilon, \quad j = 1, 2. \tag{17}$$

In the same way, let $y_j^{(l)}$ be the probability that a message from a check node to a variable node on an edge of type j in iteration l is erased. This probability is

$$y_j^{(l)} = 1 - \rho^{(j)}(1 - x_j^{(l)}), \quad j = 1, 2. \tag{18}$$

Using this, we can write down the following recursions for $x_j^{(l)}$:

$$x_1^{(l+1)} = \epsilon\lambda^{(1)}(y_1^{(l)}, y_2^{(l)}) \tag{19}$$

$$x_2^{(l+1)} = \epsilon\lambda^{(2)}(y_1^{(l)}, y_2^{(l)}). \tag{20}$$

Remark: From (17)–(20), we note that the density evolution recursion for a two edge-type LDPC ensemble is a 2-D recursion.

We denote the binary entropy function by

$$h(x) \stackrel{\triangle}{=} -x\log_2(x) - (1-x)\log_2(1-x).$$

The indicator variable $\mathbb{1}_{\{S\}}$ corresponding to a statement S is given by

$$\mathbb{1}_{\{S\}} = \begin{cases} 1, & \text{if } S \text{ is true} \\ 0, & \text{otherwise.}\end{cases}$$

By $\mathrm{coef}\left\{\sum_i F_i D^i, D^j\right\}$, we mean the coefficient of D^j in the formal power sum $\sum_i F_i D^i$, i.e., $\mathrm{coef}\left\{\sum_i F_i D^i, D^j\right\} = F_j$.

In the next section, we show how the degree distribution of a two edge-type LDPC ensemble can be chosen such that it has the same density evolution recursion as that of a given single edge-type LDPC ensemble. We also numerically optimize the degree distribution of two edge-type LDPC ensembles and show that we can approach points on the boundary of the achievable rate-equivocation region.

III. Design and Optimization

As the density evolution recursion is a 2-D recursion for two edge-type LDPC ensembles, it is difficult to analyze. Thus, we look for degree distributions which reduce the 2-D recursion to a single dimension. This will enable us to use density evolution recursion for single edge-type LDPC ensembles over the BEC, which has been very well studied. In the next lemma, we give sufficient conditions on the degree distribution of a two edge-type LDPC ensemble such that its 2-D density evolution recursion is equivalent to a 1-D density evolution recursion of a single edge-type LDPC ensemble.

Lemma III.1: Let (λ, ρ) be a single edge-type LDPC degree distribution. Let $\{\lambda^{(1)}, \lambda^{(2)}, \rho^{(1)}, \rho^{(2)}\}$ be a two edge-type LDPC ensemble from edge perspective such that the following conditions are satisfied:

$$\rho^{(1)}(x) = \rho^{(2)}(x) = \rho(x) \tag{21}$$

$$\lambda^{(1)}(x,x) = \lambda^{(2)}(x,x) = \lambda(x). \tag{22}$$

Then, the density evolution recursion of $\{\lambda^{(1)}, \lambda^{(2)}, \rho^{(1)}, \rho^{(2)}\}$ is same as the density evolution recursion of (λ, ρ). More precisely, let $x^{(l)}$ (resp. $y^{(l)}$) be the probability that a message from variable to check node (resp. check to variable node) on a randomly chosen edge is erased for density evolution recursion corresponding to (λ, ρ). Then, $x_1^{(l)} = x_2^{(l)} = x^{(l)}$ and $y_1^{(l)} = y_2^{(l)} = y^{(l)}$.

Proof: Note that since for $j = 1, 2$

$$\begin{aligned}\lambda^{(j)}(x,x) &= \sum_{l_1,l_2} \lambda_{l_1 l_2}^{(j)} x^{l_1+l_2-1}\\ &= \sum_k \left(\sum_{l_1+l_2=k} \lambda_{l_1 l_2}^{(j)}\right) x^{k-1}\end{aligned}$$

(22) implies

$$\sum_{l_1+l_2=k} \lambda_{l_1 l_2}^{(1)} = \sum_{l_1+l_2=k} \lambda_{l_1 l_2}^{(2)} \quad \forall k. \tag{23}$$

From the density evolution recursion for two edge-type LDPC ensembles given in (17)–(20), we see that (21) ensures that $y_1^{(l)} = y_2^{(l)}$ whenever $x_1^{(l)} = x_2^{(l)}$, and (22) ensures that $x_1^{(l+1)} = x_2^{(l+1)}$ whenever $y_1^{(l)} = y_2^{(l)}$. Since $x_j^{(1)} = \epsilon$ for $j \in \{1, 2\}$, by induction we see that $x_1^{(l)} = x_2^{(l)}$ and $y_1^{(l)} = y_2^{(l)}$ for $l \geq 1$. Thus, we can reduce the 2-D density evolution recursion to the 1-D density evolution recursion for the single edge-type LDPC ensemble

$$x^{(l+1)} = \epsilon\lambda(1 - \rho(1 - x^{(l)})) \tag{24}$$

where $\lambda(x) = \sum_k \lambda_k x^{k-1}$, and

$$\lambda_k = \sum_{l_1+l_2=k} \lambda_{l_1 l_2}^{(1)}. \tag{25}$$

■

Using Lemma III.1, in the next theorem, we give a two edge-type LDPC ensemble such that its design rate and threshold for transmission over the BEC is the same as that of a single edge-type LDPC ensemble.

Theorem III.2: Let (λ, ρ) be a single edge-type LDPC degree distribution with design rate R and threshold $\epsilon^\star$ over the BEC.

Let $\{\lambda^{(1)}, \lambda^{(2)}, \rho^{(1)}, \rho^{(2)}\}$ be degree distributions given by the following assignment:

$$\rho^{(1)}(x) = \rho^{(2)}(x) = \rho(x) \tag{26}$$

$$\lambda^{(1)}_{ll} = \lambda^{(2)}_{ll} = \lambda_{2l} \tag{27}$$

$$\lambda^{(1)}_{ll+1} = \lambda^{(2)}_{l+1l} = \frac{l}{2l+1}\lambda_{2l+1} \tag{28}$$

$$\lambda^{(1)}_{l+1l} = \lambda^{(2)}_{ll+1} = \frac{l+1}{2l+1}\lambda_{2l+1} \tag{29}$$

$$\lambda^{(1)}_{l_1l_2} = \lambda^{(2)}_{l_1l_2} = 0, \quad |l_1 - l_2| > 1. \tag{30}$$

Then, the two edge-type LDPC ensemble $\{\lambda^{(1)}, \lambda^{(2)}, \rho^{(1)}, \rho^{(2)}\}$ also has design rate R and threshold $\epsilon^\star$.

Proof: Note that by (27)–(30)

$$\frac{\lambda^{(1)}_{l_1l_2}}{l_1} = \frac{\lambda^{(2)}_{l_1l_2}}{l_2} \quad \forall l_1, l_2. \tag{31}$$

This ensures that (7) is fulfilled. This guarantees that the proposed degree distribution is a valid two edge-type degree distribution.

We now show that (27)–(30) guarantees that $\lambda^{(1)}(x,x) = \lambda^{(2)}(x,x) = \lambda(x)$. Then, from Lemma III.1, the 2-D density evolution recursion becomes a 1-D recursion as given in (24) and the two edge-type ensemble will have the same threshold as the single edge-type LDPC ensemble. We have

$$\begin{aligned}
\lambda^{(1)}(x,x) &= \sum_{l_1,l_2} \lambda^{(1)}_{l_1l_2} x^{l_1+l_2-1} \\
&\overset{(a)}{=} \sum_l \left(\lambda^{(1)}_{ll+1} x^{2l} + \lambda^{(1)}_{ll} x^{2l-1} + \lambda^{(1)}_{l+1l} x^{2l}\right) \\
&\overset{(b)}{=} \sum_l \left(\frac{l}{2l+1}\lambda_{2l+1} x^{2l} + \lambda_{2l} x^{2l-1}\right) + \\
&\quad \sum_l \frac{l+1}{2l+1}\lambda_{2l+1} x^{2l} \\
&= \sum_l \left(\lambda_{2l+1} x^{2l} + \lambda_{2l} x^{2l-1}\right) \\
&= \lambda(x)
\end{aligned}$$

where (a) is due to (30) and (b) is due to (27)–(29). The proof for $\lambda^{(2)}(x,x)$ is done in the same way.

We now show that the design rate of the resulting two edge-type LDPC ensemble is the same as the design rate of the given single edge-type LDPC ensemble. The design rate of the two edge-type ensemble is

$$R_{\text{des}} = 1 - (m_1 + m_2)/n$$

where m_j is the number of parity checks of type j, $j \in \{1,2\}$, and n is the number of variable nodes. If we let d_{avg} denote the average check node degree (which is the same for both types of edges because of (26)) and count the number of type j edges in two different ways, we get

$$n \sum_{l_1,l_2} l_j \Lambda_{l_1l_2} = m_j d_{\text{avg}}, \quad j = 1,2$$

or

$$\begin{aligned}
\frac{m_j}{n} &= \frac{\sum_{l_1,l_2} l_j \Lambda_{l_1l_2}}{d_{\text{avg}}} \\
&\overset{(a)}{=} \frac{1}{d_{\text{avg}}} \frac{\sum_{l_1,l_2} l_j \frac{\lambda^{(j)}_{l_1l_2}}{l_j}}{\sum_{l_1,l_2} \frac{\lambda^{(j)}_{l_1l_2}}{l_j}} \\
&\overset{(b)}{=} \frac{1}{d_{\text{avg}}} \frac{1}{\sum_{l_1,l_2} \frac{\lambda^{(j)}_{l_1l_2}}{l_j}}
\end{aligned}$$

where (a) is due to (7) and (b) follows since $\sum_{l_1,l_2} \lambda^{(j)}_{l_1l_2} = 1$. The design rate then becomes

$$\begin{aligned}
R_{\text{des}} &= 1 - (m_1 + m_2)/n \\
&= 1 - \frac{1}{d_{\text{avg}}} \left(\frac{1}{\sum_{l_1,l_2} \frac{\lambda^{(1)}_{l_1l_2}}{l_1}} + \frac{1}{\sum_{l_1,l_2} \frac{\lambda^{(2)}_{l_1l_2}}{l_2}}\right) \\
&\overset{(a)}{=} 1 - \frac{2}{d_{\text{avg}}} \left(\frac{1}{\sum_{l_1,l_2} \frac{\lambda^{(1)}_{l_1l_2}}{l_1}}\right) \\
&\overset{(b)}{=} 1 - \frac{2}{d_{\text{avg}}} \left(\frac{1}{\sum_l \left(\frac{\lambda_{2l+1}}{2l+1} + \frac{\lambda_{2l}}{l} + \frac{\lambda_{2l+1}}{2l+1}\right)}\right) \\
&= 1 - \frac{1}{d_{\text{avg}}} \frac{1}{\sum_l \left(\frac{\lambda_{2l+1}}{2l+1} + \frac{\lambda_{2l}}{2l}\right)} \\
&= 1 - \frac{1}{d_{\text{avg}}} \frac{1}{\sum_l \frac{\lambda_l}{l}}
\end{aligned}$$

where (a) is due to (31) and (b) follows using (27)–(30). Since this expression is the same as the design rate of the single edge-type LDPC ensemble (λ, ρ), we have shown that the two edge-type LDPC ensemble has design rate R. This completes the proof of the theorem. ■

To compute the threshold achievable on the main channel, we need to compute the threshold of the ensemble of parity-check matrices H_1 corresponding to type one edges. The ensemble of matrices H_1 is a single edge-type LDPC ensemble and its degree distribution can be easily calculated from the degree distribution of the two edge-type ensemble. Hence, we can easily compute its threshold.

Since all capacity approaching sequences of single edge-type degree distributions have some degree two variable nodes [20, Ch. 3], because of (27) we see that our construction will have some degree one variable nodes in the matrix H_1. This means that the threshold over the main channel will be zero. However, in order to achieve perfect secrecy, it is required that the two edge-type LDPC ensemble is capacity achieving [5]. This means that the single edge-type degree distribution should be capacity achieving. Thus, using our construction we can achieve perfect secrecy and nonzero rate of reliable communication only for BEC-WT$(0, \epsilon_w)$. If the main channel is noisy, to achieve nonzero rate of reliable communication with our construction, we need to relax the requirement of perfect secrecy.

To get around this problem, we use linear programming methods to find good degree distributions for two edge-type LDPC ensembles based on their 2-D density evolution recursion. Our main objective is to find a two edge-type LDPC ensemble such that it is capacity achieving on the wiretapper's channel and the single edge-type degree distribution induced by its type one edges is capacity achieving on the main channel. This would guarantee that our code construction achieves secrecy capacity.

First, we optimize the degree distribution of H_1 for the main channel using the methods described in [20] and obtain a good ensemble $(\Lambda^{(1)}, \Gamma^{(1)})$. For a given two edge-type ensemble, we can find the corresponding single edge-type ensemble for H_1 by summing over the second index, since the fraction of variable nodes with l_1 outgoing type one edges is given by $\sum_{l_2} \Lambda_{l_1 l_2}$. To fix the degree distribution of H_1, we then impose the constraint

$$\sum_{l_2} \Lambda_{l_1 l_2} = \Lambda_{l_1}^{(1)} \text{for all } l_1.$$

For successful decoding, we further impose the two constraints $x_1^{(l+1)} \leq x_1^{(l)}$ and $x_2^{(l+1)} \leq x_2^{(l)}$ which can be written as

$$\begin{aligned} x_1 &\geq \epsilon \lambda^{(1)}(y_1, y_2) \\ &= \epsilon \sum_{l_1, l_2} \lambda_{l_1 l_2}^{(1)} y_1^{l_1 - 1} y_2^{l_2} \\ &= \epsilon \sum_{l_1, l_2} \frac{l_1 \Lambda_{l_1, l_2}}{\sum_{k_1, k_2} k_1 \Lambda_{k_1, k_2}} y_1^{l_1 - 1} y_2^{l_2} \end{aligned}$$

where we have used (5) in the last step, and $y_1 \text{and} y_2$ are given by

$$y_j = 1 - \rho_j(1 - x_j), j = 1, 2.$$

This simplifies to the linear constraint

$$0 \leq \sum_{l_1, l_2} l_1 (x_1 - \epsilon y_1^{l_1 - 1} y_2^{l_2}) \Lambda_{l_1 l_2}. \tag{32}$$

The corresponding constraint for x_2 is

$$0 \leq \sum_{l_1, l_2} l_1 (x_2 - \epsilon y_1^{l_1} y_2^{l_2 - 1}) \Lambda_{l_1 l_2}. \tag{33}$$

The design rate can be written as

$$R_{\text{des}} = 1 - \frac{\sum_{l_1, l_2} l_1 \Lambda_{l_1 l_2}}{\sum_{l_1} l_1 \Gamma_{l_1}^{(1)}} - \frac{\sum_{l_1, l_2} l_2 \Lambda_{l_1 l_2}}{\sum_{l_2} l_2 \Gamma_{l_2}^{(2)}}$$

where the term $\frac{\sum_{l_1, l_2} l_1 \Lambda_{l_1 l_2}}{\sum_{l_1} l_1 \Gamma_{l_1}^{(1)}}$ is a constant because of the fixed degree distribution of H_1. If $\Gamma^{(2)}$ is fixed, we see that maximizing the design rate is the same as minimizing $\sum_{l_1, l_2} l_2 \Lambda_{l_1 l_2}$. Thus, we end up with the following linear program, which we will solve iteratively:

$$\text{minimize} \sum_{l_1, l_2} l_2 \Lambda_{l_1 l_2} \tag{34}$$

subject to

$$\sum_{l_2} \Lambda_{l_1 l_2} = \Lambda_{l_1}^{(1)}, \; l_1 = 2, \ldots, I \tag{35}$$

$$\sum_{l_1, l_2} l_1 (x_1(k) - \epsilon y_1(k)^{l_1 - 1} y_2(k)^{l_2}) \Lambda_{l_1 l_2} \geq 0, k = 1, \ldots, K \tag{36}$$

$$\sum_{l_1, l_2} l_1 (x_2(k) - \epsilon y_1(k)^{l_1} y_2(k)^{l_2 - 1}) \Lambda_{l_1 l_2} \geq 0, k = 1, \ldots, K \tag{37}$$

where I is the largest degree in $\Lambda^{(1)}(x)$. Since the constraints (32) and (33) correspond to infinitely many constraints, we replace them by the first K steps of the density evolution path followed by the degree distribution used in the previous iteration. Thus, the points $\{x_1(k), x_2(k)\}_{k=1}^K$ are chosen by generating a distribution Λ_0 and then running the density evolution recursion

$$x_1^{(1)} = x_2^{(1)} = \epsilon \tag{38}$$

$$x_1^{(l+1)} = \epsilon \lambda_0^{(1)}(y_1^{(l)}, y_2^{(l)}) \tag{39}$$

$$x_2^{(l+1)} = \epsilon \lambda_0^{(2)}(y_1^{(l)}, y_2^{(l)}) \tag{40}$$

K times. The program is then solved repeatedly, each time updating $\{x_1(k), x_2(k)\}_{k=1}^K$. This process is repeated several times for different check node degree distributions $\Gamma^{(2)}$ until there is negligible improvement in rate. The complete optimization procedure is summarized in the following steps.

1) Find an optimized degree distribution $(\Lambda^{(1)}, \Gamma^{(1)})$ of H_1 for the main channel using the methods described in [20]. Fix a check node degree distribution $\Gamma^{(2)}$ corresponding to type two edges.
2) Choose a two edge-type variable node degree distribution Λ which satisfies (35).
3) Generate K density evolution points $\{x_1(k), x_2(k)\}_{k=1}^K$ by using (38)–(40).
4) Solve the linear program given by (34)–(37).
5) Repeat Steps 3) and 4) until there is negligible improvement in rate.

As aforementioned, we repeat the optimization procedure for several $\Gamma^{(2)}$. A good choice of $\Gamma^{(2)}$ is either regular or with two different degrees.

We now present some optimized degree distributions obtained by this method. We use the following degree distribution

Standard LDPC Degree Distribution 1:

$$\begin{aligned} \Lambda^{(1)}(x) =& 0.5572098x^2 + 0.1651436x^3 + 0.07567923x^4 \\ &+ 0.0571348x^5 + .043603x^7 + 0.02679802x^8 \\ &+ 0.013885518x^{13} + 0.0294308x^{14} + 0.02225301x^{31} \\ &+ 0.00886105x^{100} \\ \Gamma^{(1)}(x) =& 0.25x^9 + 0.75x^{10} \end{aligned}$$

as the ensemble $(\Lambda^{(1)}, \Gamma^{(1)})$ for the main channel. It has rate 0.498826, threshold 0.5, and multiplicative gap to capacity $(1 - \epsilon - R_{\text{des}})/(1 - \epsilon) = 0.00232857$. We use it to obtain two optimized degree distributions, one for $\epsilon_w = 0.6$ and one for $\epsilon_w = 0.75$.

TABLE I
SUMMARY OF RESULTS FOR OPTIMIZED DEGREE DISTRIBUTIONS, WHERE D.D. NUMBER IS TWO EDGE-TYPE DEGREE DISTRIBUTION NUMBER

D.D. Number	Channel	R_{ab}	R_e	C_s
1	BEC-WT(0.5, 0.6)	0.099906	0.0989137	0.1
2	BEC-WT(0.5, 0.75)	0.250131	0.248837	0.25

The degree distribution for the ensemble optimized for $\mathrm{BEC\text{-}WT}(0.5, 0.6)$ is given by

Two Edge-Type Degree Distribution 1:

$$\begin{aligned}\Lambda(x,y) &= 0.463846x^2 + 0.0814943x^2y + 0.0118691x^2y^2 \\ &\quad + 0.14239x^3 + 0.0201658x^3y + 0.00258812x^3y^2 \\ &\quad + 0.0292241x^4 + 0.0464551x^4y + 0.0564162x^5 \\ &\quad + 0.000718585x^5y + 0.0436039x^7y \\ &\quad + 0.0258926x^8y + 0.000905503x^8y^2 \\ &\quad + 0.00631474x^{13}y^2 + 0.00757076x^{13}y^5 \\ &\quad + 0.011051x^{14}y + 0.0173718x^{14}y^2 \\ &\quad + 0.00100807x^{14}y^5 + 0.00240762x^{31} \\ &\quad + 0.0012626x^{31}y^4 + 0.0185828x^{31}y^5 \\ &\quad + 0.000326117x^{100}y^4 + 0.00383319x^{100}y^{17} \\ &\quad + 0.00470174x^{100}y^{18} \\ \Gamma^{(1)}(x) &= 0.25x^9 + 0.75x^{10} \\ \Gamma^{(2)}(x) &= x^6.\end{aligned}$$

This ensemble has design rate 0.39893, threshold 0.6, and the multiplicative gap to capacity is 0.00267632. The rate R_{ab} from Alice to Bob is 0.099906, and R_e, the equivocation of Eve, is 0.0989137. However, R_{ab} is very close to the secrecy capacity $C_S = 0.1$, and R_e is very close to R_{ab}.

The degree distribution for the ensemble optimized for $\mathrm{BEC\text{-}WT}(0.5, 0.75)$ is given by

Two Edge-Type Degree Distribution 2:

$$\begin{aligned}\Lambda(x,y) &= 0.367823x^2 + 0.166244x^2y + 0.0231428x^2y^2 \\ &\quad + 0.125727x^3 + 0.0394166x^3y + 0.00286773x^4 \\ &\quad + 0.0728115x^4y + 0.0571348x^5y \\ &\quad + 0.0300989x^7y^2 + 0.013505x^7y^3 \\ &\quad + 0.0196622x^8y^3 + 0.00713582x^8y^4 \\ &\quad + 0.000565918x^{13}y^2 + 0.0133196x^{13}y^5 \\ &\quad + 0.0149732x^{14}y^2 + 0.0132215x^{14}y^5 \\ &\quad + 0.0012361x^{14}y^6 + 0.00490831x^{31}y^8 \\ &\quad + 0.0173447x^{31}y^9 + 0.00130606x^{100}y^{17} \\ &\quad + 0.00498932x^{100}y^{30} + 0.00256567x^{100}y^{31} \\ \Gamma^{(1)}(x) &= 0.25x^9 + 0.75x^{10} \\ \Gamma^{(2)}(x) &= 0.25x^4 + 0.75x^5.\end{aligned}$$

This ensemble has design rate 0.248705 and threshold 0.75. The multiplicative gap to capacity is 0.00518359. The rate R_{ab} from Alice to Bob is 0.250131, and R_e, the equivocation of Eve, is 0.248837. Note that the secrecy capacity C_s for this channel is 0.25. Thus, the obtained point is slight to the right and below the point B in Fig. 2. We summarize the results for the obtained optimized degree distributions in Table I.

As aforementioned, computing the equivocation of Eve is not as straightforward as computing the reliability on the main channel. In the next section, we show how to compute the equivocation of Eve by generalizing the methods from [15] to two edge-type LDPC codes.

IV. PRELIMINARY RESULTS FOR COMPUTATION OF EQUIVOCATION

In order to compute the average equivocation of Eve over an ensemble of two edge-type LDPC codes, we generalize the MMU method of [15] to two edge-type LDPC codes. In [15], the equivocation of single edge-type LDPC ensembles for point-to-point communication over the $\mathrm{BEC}(\epsilon)$ was computed. More precisely, let $\underline{\tilde{X}}$ be a randomly chosen codeword of a randomly chosen code G from the single edge-type LDPC ensemble. Let $\underline{\tilde{X}}$ be transmitted over the $\mathrm{BEC}(\epsilon)$ and let $\underline{\tilde{Z}}$ be the channel output. Then, the MMU method computes

$$\lim_{n\to\infty} \frac{\mathbb{E}\left(H_G(\underline{\tilde{X}}|\underline{\tilde{Z}})\right)}{n} \tag{41}$$

where $H_G(\underline{\tilde{X}}|\underline{\tilde{Z}})$ is the conditional entropy of the transmitted codeword given the channel observation for the code G and the expectation denotes the ensemble average. The MMU method is described in the following.

1) Consider decoding the all-zero codeword using the peeling decoder [20, pp. 115], which is described in the following.
   a) Initially, remove all the known (not erased from the channel) variable nodes and the edges connected to them. Now remove all the degree zero check nodes.
   b) Pick a degree one check node. Declare its neighboring variable node to be known. Remove all the edges connected to this variable node. Remove all the degree zero check nodes.
   c) If there are no degree one check nodes, then go to the next step. Otherwise, repeat the previous step.
   d) Output the remaining graph which is called the *residual graph*.
2) The peeling decoder gets stuck in the largest stopping set contained in the set of erased variable nodes [20]. Thus, the residual graph is the subgraph induced by this stopping set. The residual graph is again a code whose codewords are compatible with the erasure set.
3) The degree distribution of the residual graph and its edge connections are random variables. It was shown in [21] that if the erasure probability is above the BP threshold, then almost surely the residual graph has a degree distribution close to the *average residual degree distribution*. The average residual degree distribution can be computed by the asymptotic analysis of the peeling decoder. Also, conditioned on the degree distribution of the residual graph, the induced probability distribution is uniform over all graphs with the given degree distribution. This implies that almost surely a residual graph is an element of the single edge-type LDPC ensemble with degree distribution equal to the average residual degree distribution, which we refer to as the *residual ensemble*.

4) The normalized expectation of the conditional entropy given in (41) can be determined from the average rate of the residual ensemble. One can easily compute the design rate of the residual ensemble from its degree distribution. However, the design rate is only a lower bound on the average rate. A criterion was derived in [15], which, when satisfied, guarantees that the average rate is equal to the design rate. If the average rate is equal to the design rate, then the normalized expectation of the conditional entropy can be determined from the design rate of the residual ensemble.

For transmission over the BEC-WT(ϵ_m, ϵ_w), to compute the equivocation of Eve $H(\underline{S}|\underline{Z})$, we write $H(\underline{S}, \underline{X}|\underline{Z})$ in two different ways using the chain rule and obtain

$$H(\underline{X}|\underline{Z}) + H(\underline{S}|\underline{X}, \underline{Z}) = H(\underline{S}|\underline{Z}) + H(\underline{X}|\underline{S}, \underline{Z}). \quad (42)$$

By noting that $H(\underline{S}|\underline{X}, \underline{Z}) = 0$ and substituting it in (42), we obtain

$$\frac{H(\underline{S}|\underline{Z})}{n} = \frac{H(\underline{X}|\underline{Z})}{n} - \frac{H(\underline{X}|\underline{S}, \underline{Z})}{n}. \quad (43)$$

In the following two sections, we show how the normalized averages of $H(\underline{X}|\underline{Z})$ and $H(\underline{X}|\underline{S}, \underline{Z})$ can be computed. The next section deals with $H(\underline{X}|\underline{Z})$.

A. Computing the Normalized $H(\underline{X}|\underline{Z})$

In the following lemma, we show that the average of $\lim_{n\to\infty} H(\underline{X}|\underline{Z})/n$ can be computed by the MMU method.

Lemma IV.1: Consider transmission over the BEC-WT(ϵ_m, ϵ_w) using the syndrome encoding method with a two edge-type LDPC code $H = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}$, where the dimensions of H, H_1, and H_2 are $n(1-R) \times n$, $n(1-R_1) \times n$, and $n(R_1 - R) \times n$, respectively. Let $\underline{S}$ be a randomly chosen message from Alice for Bob and $\underline{X}$ be the transmitted vector which is a randomly chosen solution of $H\underline{X} = \begin{bmatrix} \underline{0} \\ \underline{S} \end{bmatrix}$. Let $\underline{Z}$ be the channel observation of the wiretapper Eve. Consider a point-to-point communication setup over the BEC(ϵ_w) using a single edge-type LDPC code H_1. Let $\underline{\hat{X}}$ be a randomly chosen transmitted codeword of the code given by H_1, i.e., $\underline{\hat{X}}$ is a randomly chosen solution of $H_1\underline{X} = \underline{0}$. Further, let $\underline{\hat{Z}}$ be the channel output. Then

$$H(\underline{X}|\underline{Z}) = H\left(\underline{\hat{X}}|\underline{\hat{Z}}\right).$$

Proof: We prove the lemma by showing that $(\underline{X}, \underline{Z})$ and $(\underline{\hat{X}}, \underline{\hat{Z}})$ have the same joint distribution. Clearly, $P(\underline{Z} = \underline{z}|\underline{X} = \underline{x}) = P(\underline{\hat{Z}} = \underline{z}|\underline{\hat{X}} = \underline{x})$ as transmission takes place over the BEC(ϵ_w) in both cases. Now

$$\begin{aligned} P(\underline{X} = \underline{x}) &= \sum_{\underline{s}} P(\underline{X} = \underline{x}, \underline{S} = \underline{s}) \\ &\overset{(a)}{=} \frac{1}{2^{n(R_1-R)}} \sum_{\underline{s}} P(\underline{X} = \underline{x}|\underline{S} = \underline{s}) \\ &= \frac{1}{2^{n(R_1-R)}} \sum_{\underline{s}} \frac{1}{2^{nR}} \mathbb{1}_{\{H_1\underline{x}=\underline{0}\}} \mathbb{1}_{\{H_2\underline{x}=\underline{s}\}} \\ &\overset{(b)}{=} \frac{\mathbb{1}_{\{H_1\underline{x}=\underline{0}\}}}{2^{nR_1}} \end{aligned} \quad (44)$$

where (a) follows from the uniform *a priori* distribution on $\underline{S}$ and (b) follows because for a fixed $\underline{x}$

$$\sum_{\underline{s}} \mathbb{1}_{\{H_2\underline{x}=\underline{s}\}} = 1.$$

Now, the *a priori* distribution of $\underline{\hat{X}}$ is also the right-hand side (RHS) of (44). This is because $\underline{\hat{X}}$ is a randomly chosen solution of $H_1\underline{\hat{X}} = \underline{0}$. This proves the lemma. ■

From Lemma IV.1, we see that when we consider transmission over the BEC-WT(ϵ_m, ϵ_w) using the two edge-type LDPC ensemble $\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$, we can compute the average of $\lim_{n\to\infty} H(\underline{X}|\underline{Z})/n$ by applying the MMU method to the single edge-type LDPC ensemble $\{\Lambda^{(1)}, \Gamma^{(1)}\}$ for transmission over the BEC(ϵ_w). We formally state this in the following theorem.

Theorem IV.2: Consider transmission over the BEC-WT(ϵ_m, ϵ_w) using a randomly chosen code G from the two edge-type LDPC ensemble $\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$ and the coset encoding method. Let $\underline{X}$ be the transmitted word and $\underline{Z}$ be the wiretapper's observation.

Consider a point-to-point communication setup for transmission over the BEC(ϵ_w) using a randomly chosen code $\hat{G}$ from the single edge-type LDPC ensemble $\{\Lambda^{(1)}, \Gamma^{(1)}\}$. Let $\underline{\hat{X}}$ be a randomly chosen transmitted codeword and $\underline{\hat{Z}}$ be the channel output. Let $\{\Omega, \Phi\}$ (from the node perspective) be the average residual degree distribution[2] of the residual ensemble given by the peeling decoder and let R^r_{des} be the design rate of the average residual ensemble $\{\Omega, \Phi\}$. If almost every element of the average residual ensemble $\{\Omega, \Phi\}$ has its rate equal to the design rate R^r_{des}, then

$$\begin{aligned} \lim_{n\to\infty} \frac{\mathbb{E}\left(H_G(\underline{X}|\underline{Z})\right)}{n} &= \lim_{n\to\infty} \frac{\mathbb{E}\left(H_{\hat{G}}(\underline{\hat{X}}|\underline{\hat{Z}})\right)}{n} \\ &= \epsilon_w \Lambda^{(1)}\left(1 - \rho^{(1)}(1-x)\right) R^r_{\text{des}} \end{aligned} \quad (45)$$

where x is the fixed point of the density evolution recursion for $\{\Lambda^{(1)}, \Gamma^{(1)}\}$ initialized with erasure probability ϵ_w, and $\rho^{(1)}$ is the check node degree distribution of H_1 from the edge perspective.

Remark: Note that the condition that almost every element of the average residual ensemble $\{\Omega, \Phi\}$ has its rate equal to the design rate can be verified by using [20, Lemma 3.22] or [15, Lemma 7].

Proof: The first equality in (45) is the result of Lemma IV.1. The second equality of (45) follows from [15, Th. 10]. The factor $\epsilon_w \Lambda^{(1)}\left(1 - \rho^{(1)}(1-x)\right)$, which is the ratio of the blocklength of the average residual ensemble $\{\Omega, \Phi\}$ to the initial ensemble $\{\Lambda^{(1)}, \Gamma^{(1)}\}$, takes care of the fact that we are normalizing $H_G(\underline{X}|\underline{Z})$ by the blocklength of the initial ensemble $\{\Lambda^{(1)}, \Gamma^{(1)}\}$. ■

In the following section, we generalize the MMU method to two edge-type LDPC ensembles in order to compute $H(\underline{X}|\underline{S}, \underline{Z})$.

[2] Ω corresponding to the variable node degree distribution, and Φ corresponding to the check node degree distribution.

B. Computing Normalized $H(\underline{X}|\underline{S},\underline{Z})$ by Generalizing the MMU Method to the Two EDGE-Type LDPC Ensembles

Similarly to Lemma IV.1, in the following lemma, we show that computing $H(\underline{X}|\underline{S},\underline{Z})$ for transmission over the BEC-WT(ϵ_m,ϵ_w) using the coset encoding method and two edge-type LDPC ensemble $\{\Lambda,\Gamma^{(1)},\Gamma^{(2)}\}$ is equivalent to computing the equivocation of the same ensemble for point-to-point communication over the BEC(ϵ_w).

Lemma IV.3: Consider transmission over the BEC-WT(ϵ_m,ϵ_w) using the syndrome encoding method with a two edge-type LDPC code $H=\begin{bmatrix}H_1\\H_2\end{bmatrix}$, where the dimensions of H, H_1, and H_2 are $n(1-R)\times n$, $n(1-R_1)\times n$, and $n(R_1-R)\times n$, respectively. Let $\underline{S}$ be a randomly chosen message from Alice for Bob and $\underline{X}$ be the transmitted vector which is a randomly chosen solution of $H\underline{X}=\begin{bmatrix}\underline{0}\\\underline{S}\end{bmatrix}$. Let $\underline{Z}$ be the channel observation of the wiretapper Eve.

Consider a point-to-point communication setup for transmission over the BEC(ϵ_w) using a two edge-type LDPC code $H=\begin{bmatrix}H_1\\H_2\end{bmatrix}$. Let $\hat{\underline{X}}$ be the transmitted codeword which is a randomly chosen solution of $H\underline{X}=\underline{0}$ and $\hat{\underline{Z}}$ be the channel output. Then

$$H(\underline{X}|\underline{S},\underline{Z})\overset{(a)}{=}H(\underline{X}|\underline{S}=\underline{0},\underline{Z})\overset{(b)}{=}H(\hat{\underline{X}}|\hat{\underline{Z}}).$$

Proof: Equality (b) is obvious. To prove equality (a), note that for a solution $\underline{x}$ of $H\underline{x}=\begin{bmatrix}\underline{0}\\\underline{s}\end{bmatrix}$, we can write $\underline{x}=\underline{x}'\oplus\underline{x}_{\underline{s}}$, where $H\underline{x}'=\underline{0}$ and $H\underline{x}_{\underline{s}}=\begin{bmatrix}\underline{0}\\\underline{s}\end{bmatrix}$. Let $\underline{z}$ be a specific received vector and let $\underline{z}'$ be the vector that has the same erased positions as $\underline{z}$ and is equal to the corresponding position in $\underline{x}'$ in the nonerased positions. The proof is completed by noting that

$$P(\underline{X}=\underline{x},\underline{Z}=\underline{z}|\underline{S}=\underline{s})=P(\underline{X}=\underline{x}',\underline{Z}=\underline{z}'|\underline{S}=\underline{0}). \quad (46)$$

■

Note that as in the setting of the MMU method for single edge-type LDPC ensembles, the equivocation for Eve can be computed under the assumption of transmission of the all-zero codeword. This is because from (43), we see that the equivocation is the difference of two entropy terms. From Lemma IV.1, we know that the first term of this difference is the same as computing the conditional entropy of a single edge-type LDPC ensemble for point-to-point transmission over the BEC(ϵ_w). This is the setting of the MMU method for which the all-zero codeword assumption is valid [15]. From Lemma IV.3, we see that the second term of the difference can be computed by computing the conditional entropy of transmission over the BEC(ϵ_w) using a two edge-type LDPC ensemble. This can also be done under the all-zero codeword assumption by generalizing the MMU method to two edge-type LDPC ensembles. The proof of the validity of the all-zero codeword assumption for two edge-type LDPC ensembles is the same as that of single edge-type LDPC ensembles. In the next section, we generalize the MMU method to two edge-type LDPC ensembles.

V. MMU Method for Two Edge-Type LDPC Ensembles

The peeling decoder described in Step 1 of the MMU method and its termination described in Step 2 is the same for two edge-type LDPC ensembles. The proof of Step 3 of the MMU method for two edge-type LDPC ensembles is the same as that for single edge-type LDPC ensembles. We state it in the following two lemmas.

Lemma V.1: Consider transmission over the BEC(ϵ_w) using the two edge-type LDPC ensemble $\{\Lambda,\Gamma^{(1)},\Gamma^{(2)}\}$ and decoding using the peeling decoder. Let G be a random residual graph. Conditioned on the event that G has degree distribution $\{\Omega,\Phi^{(1)},\Phi^{(2)}\}$, it is equally likely to be any element of the two edge-type ensemble $\{\Omega,\Phi^{(1)},\Phi^{(2)}\}$.

Proof: The proof is the same as for the single edge-type LDPC ensemble [22]. However, for completeness the proof is given in Appendix A. ■

Lemma V.2: Consider transmission over the BEC(ϵ_w) using the two edge-type LDPC ensemble $\{\Lambda,\Gamma^{(1)},\Gamma^{(2)}\}$ and decoding using the peeling decoder. Let $\{\Omega,\Phi^{(1)},\Phi^{(2)}\}$ be the average residual degree distribution. Let $\{\Omega_G,\Phi_G^{(1)},\Phi_G^{(2)}\}$ be the residual degree distribution of a random residual graph G. Then, for any $\delta>0$

$$\lim_{n\to\infty}P\left\{d\left(\left(\Omega,\Phi^{(1)},\Phi^{(2)}\right),\left(\Omega_G,\Phi_G^{(1)},\Phi_G^{(2)}\right)\right)\geq\delta\right\}=0.$$

The distance $d(\cdot,\cdot)$ is the L_1 distance

$$d\left(\left(\Omega,\Phi^{(1)},\Phi^{(2)}\right),\left(\tilde{\Omega},\tilde{\Phi}^{(1)},\tilde{\Phi}^{(2)}\right)\right)=\sum_{i_1i_2}|\Omega_{i_1i_2}-\tilde{\Omega}_{i_1i_2}|+\sum_{j_1}|\Phi_{j_1}^{(1)}-\tilde{\Phi}_{j_1}^{(1)}|+\sum_{j_2}|\Phi_{j_2}^{(2)}-\tilde{\Phi}_{j_2}^{(2)}|.$$

Proof: The proof is very similar to the proof for the single edge-type LDPC ensemble given in [20, Th. 3.106]. We provide an outline of the proof in Appendix B. ■

In the following lemma, we compute the average residual degree distribution of two edge-type LDPC ensembles.

Lemma V.3: Consider transmission over the BEC(ϵ_w) using the two edge-type LDPC ensemble $\{\Lambda,\Gamma^{(1)},\Gamma^{(2)}\}$ and decoding using the peeling decoder. Let (x_1,x_2) be the fixed points of (19) and (20) when initialized with channel erasure probability ϵ_w. Let $y_j=1-\rho^{(j)}(1-x_j)$, $j=1,2$, where $\rho^{(j)}$ is the degree distribution of check nodes of type j from the edge perspective. Then, the average residual degree distribution $\{\Omega,\Phi^{(1)},\Phi^{(2)}\}$ is given by

$$\begin{aligned}\Omega(z_1,z_2)&=\epsilon_w\Lambda(z_1y_1,z_2y_2)\\\Phi^{(j)}(z)&=\Gamma^{(j)}(1-x_j+x_jz)-x_jz\Gamma'^{(j)}(1-x_j)\\&\quad-\Gamma^{(j)}(1-x_j),\quad j=1,2\end{aligned}$$

where $\Gamma'^{(j)}(x)$ is the derivative of $\Gamma^{(j)}(x)$. Note that the degree distributions are normalized with respect to the number of variable (check) nodes in the original graph.

Proof: The proof follows by the analysis of the peeling decoder for general multiedge-type LDPC ensembles in [23]. However, as we are only interested in two edge-type LDPC ensembles, the proof also follows from the analysis for the single edge-type LDPC case [22]. ■

Lemmas V.1–V.3 generalize Step 3 of the MMU method for two edge-type LDPC ensembles. The key technical task in extending Step 4 to two edge-type LDPC ensembles is to derive a criterion, which when satisfied guarantees that almost every code in the residual ensemble has its rate equal to the design rate. The rate is equal to the normalized logarithm of the total number of codewords. However, as the average of the logarithm of the total number of codewords is hard to compute, we compute the normalized logarithm of the average of the total number of codewords. By Jensen's inequality, this is an upper bound on the average rate. More precisely, let N be the total number of codewords corresponding to a randomly chosen code. Then, by Jensen's inequality

$$\lim_{n\to\infty}\frac{\mathbb{E}(\log_2(N))}{n}\leq\lim_{n\to\infty}\frac{\log_2\left(\mathbb{E}(N)\right)}{n}.$$

If this upper bound is equal to the design rate, then by the same arguments as in [15, Lemma 7], we can show that almost every code in the ensemble has its rate equal to the design rate. In the following lemma, we derive the average of the total number of codewords of a two edge-type LDPC ensemble.

Lemma V.4: Let N be the total number of codewords of a randomly chosen code from the two edge-type LDPC ensemble $(\Lambda,\Gamma^{(1)},\Gamma^{(2)})$. Then, the average of N over the ensemble is given by

$$\mathbb{E}(N)=\sum_{E_1=0,E_2=0}^{n\Lambda_1'(1,1),n\Lambda_2'(1,1)}\operatorname{coef}\left\{\prod_{l_1,l_2}(1+u_1^{l_1}u_2^{l_2})^{n\Lambda_{l_1,l_2}},u_1^{E_1}u_2^{E_2}\right\}\times\frac{\operatorname{coef}\left\{\prod_{r_1,r_2}q_{r_1}(v_1)^{\frac{n\Lambda_1'(1,1)}{\Gamma'^{(1)}(1)}\Gamma_{r_1}^{(1)}}q_{r_2}(v_2)^{\frac{n\Lambda_2'(1,1)}{\Gamma'^{(2)}(1)}\Gamma_{r_2}^{(2)}},v_1^{E_1}v_2^{E_2}\right\}}{\binom{n\Lambda_1'(1,1)}{E_1}\binom{n\Lambda_2'(1,1)}{E_2}}$$

where $\Lambda_j'(1,1)=\sum_{l_1,l_2}l_j\Lambda_{l_1,l_2}$, $\Gamma'^{(j)}(1)=\sum_{r_j}r_j\Gamma_{r_j}^{(j)}$, $j\in\{1,2\}$. The polynomial $q_r(v)$ is defined as

$$q_r(v)=\frac{(1+v)^r+(1-v)^r}{2}. \tag{47}$$

Proof: Let $\mathcal{W}(E_1,E_2)$ be the set of assignments of ones and zeros to the variable nodes which result in E_1 (resp. E_2) type one (resp. type two) edges connected to variable nodes assigned value one. Denote the cardinality of $\mathcal{W}(E_1,E_2)$ by $|\mathcal{W}(E_1,E_2)|$. For an assignment w, let $\mathbb{1}_w$ be a random indicator variable which evaluates to one if w is a codeword of a randomly chosen code, and zero otherwise. Let $N(E_1,E_2)$ be the number of codewords belonging to the set $\mathcal{W}(E_1,E_2)$. Then, we have the following relationships:

$$N(E_1,E_2)=\sum_{w\in\mathcal{W}(E_1,E_2)}\mathbb{1}_w \tag{48}$$

$$N=\sum_{E_1=0,E_2=0}^{n\Lambda_1'(1,1),n\Lambda_2'(1,1)}N(E_1,E_2). \tag{49}$$

Equation (48) follows simply by checking if every word in the set $\mathcal{W}(E_1,E_2)$ is a codeword. We obtain (49) by partitioning the set of codewords based on the number of type one and type two edges connected to variable nodes assigned value one. By linearity of expectation, we obtain

$$\mathbb{E}(N(E_1,E_2))=\sum_{w\in\mathcal{W}(E_1,E_2)}\mathbb{E}(\mathbb{1}_w) \tag{50}$$

$$\mathbb{E}(N)=\sum_{E_1=0,E_2=0}^{n\Lambda_1'(1,1),n\Lambda_2'(1,1)}\mathbb{E}(N(E_1,E_2)). \tag{51}$$

From the symmetry of code generation, we observe that $\mathbb{E}(\mathbb{1}_w)$, for $w\in\mathcal{W}(E_1,E_2)$, is independent of w. Thus, we can fix w to any one element of $\mathcal{W}(E_1,E_2)$ and obtain

$$\mathbb{E}(N(E_1,E_2))=|\mathcal{W}(E_1,E_2)|\Pr\left(w\text{ is a codeword}\right). \tag{52}$$

Note that $|\mathcal{W}(E_1,E_2)|$ is given by

$$|\mathcal{W}(E_1,E_2)|=\operatorname{coef}\left\{\prod_{l_1,l_2}(1+u_1^{l_1}u_2^{l_2})^{n\Lambda_{l_1,l_2}},u_1^{E_1}u_2^{E_2}\right\}. \tag{53}$$

To understand (53), note that when a variable node with type one degree l_1 and type two degree l_2 is assigned a one, it gives rise to l_1 (resp. l_2) type one (resp. type two) edges connected to a variable node assigned value one, and when it is assigned a zero, it gives rise to no such edges. Thus, the generating function of such a variable node to count the number of edges it gives rise to, which are connected to a variable node assigned one, is given by $1+u_1^{l_1}u_2^{l_2}$. Hence, the overall generating function is given by $\prod_{l_1,l_2}(1+u_1^{l_1}u_2^{l_2})^{n\Lambda_{l_1,l_2}}$.

We now evaluate the probability that an assignment w, $w\in\mathcal{W}(E_1,E_2)$, is a codeword, which is given by

$$\Pr\left(w\text{ is a codeword}\right)=\frac{\text{Total number of graphs for which }w\text{ is a codeword}}{\text{Total number of graphs}}. \tag{54}$$

Similar to the arguments for the single edge-type LDPC ensemble in [15], the total number of graphs for which w is a codeword is given by

$$E_1!E_2!(n\Lambda_1'(1,1)-E_1)!(n\Lambda_2'(1,1)-E_2)!\operatorname{coef}\left\{\prod_{r_1,r_2}q_r(v_1)^{\frac{n\Lambda_1'(1,1)}{\Gamma'^{(1)}(1)}\Gamma_{r_1}^{(1)}}q_r(v_2)^{\frac{n\Lambda_2'(1,1)}{\Gamma'^{(2)}(1)}\Gamma_{r_2}^{(2)}},v_1^{E_1}v_2^{E_2}\right\}. \tag{55}$$

The factorial term $E_1!$ in (55) corresponds to the fact that given a graph for which w is a codeword, we can permute the check node side position of the E_1 type one edges connected to a variable node assigned value one, and w will be a codeword for the resulting graph. Similarly, we obtain the other factorial terms in (55). The generating function in (55) is the generating function to count the number of ways edges can be assigned on the check node side such that w is a codeword [20].

By noting that the total number of graphs is equal to $(n\Lambda_1'(1,1))!(n\Lambda_2'(1,1))!$, and combining (51)–(55), we obtain the expression for the average of the total number of codewords. ■

Remark: Note that in Lemma V.4, we count the number of codewords which give rise to E_1 type one (resp. E_2 type two) edges which are connected to a variable node assigned value one. A related quantity is the weight distribution of a code which counts the number of codewords with a given weight. The average weight distribution of two edge-type and more generally multiedge-type LDPC ensembles has been computed in [24] and [25].

Let $(e_1, e_2) = (E_1/(n\Lambda_1'(1,1)), E_2/(n\Lambda_2'(1,1)))$, i.e., e_j is E_j normalized by the total number of type j edges, $j = 1, 2$. In the following lemma, we find the set of (e_1, e_2) for which $\lim_{n\to\infty} |\mathcal{W}(e_1 n\Lambda_1'(1,1), e_2 n\Lambda_2'(1,1))| \neq 0$.

Lemma V.5: Let $\mathcal{E}(n)$ be the set of (e_1, e_2) such that

$$\operatorname{coef}\left\{\prod_{l_1,l_2}(1+u_1^{l_1}u_2^{l_2})^{n\Lambda_{l_1,l_2}}, u_1^{e_1 n\Lambda_1'(1,1)}u_2^{e_2 n\Lambda_2'(1,1)}\right\} \neq 0. \tag{56}$$

Let $\mathcal{E} \triangleq \lim_{n\to\infty} \mathcal{E}(n)$. Then, $\mathcal{E}$ is given by

$$\mathcal{E} = \{(e_1,e_2) : \left(\frac{\sum_{l_1,l_2} l_1\Lambda_{l_1,l_2}\sigma(l_1,l_2)}{\Lambda_1'(1,1)}, \frac{\sum_{l_1,l_2} l_2\Lambda_{l_1,l_2}\sigma(l_1,l_2)}{\Lambda_2'(1,1)}\right)\}$$

where $0 \leq \sigma(l_1, l_2) \leq 1$.

Proof: The proof is given in Appendix C. ■

In the next lemma, we show that $\mathcal{E}$ as defined in Lemma V.5 is the set enclosed between two piecewise linear curves.

Lemma V.6: Let $\mathcal{E}$ be as defined in Lemma V.5. Then, $\mathcal{E}$ is the subset of $[0,1]^2$ enclosed between two piecewise linear curves. Order the pairs (l_1, l_2) for which $\Lambda_{l_1,l_2} > 0$ in decreasing order of l_1/l_2 and assume that there are D distinct such values. Let

$$\sigma_d(l_1,l_2) = \begin{cases} 1, & \text{if } l_1/l_2 \text{ takes the } d\text{th largest possible value} \\ 0, & \text{otherwise} \end{cases} \tag{57}$$

and let

$$p_d = \left(\frac{\sum_{l_1,l_2} l_1\Lambda_{l_1,l_2}\sigma_d(l_1,l_2)}{\Lambda_1'(1,1)}, \frac{\sum_{l_1,l_2} l_2\Lambda_{l_1,l_2}\sigma_d(l_1,l_2)}{\Lambda_2'(1,1)}\right). \tag{58}$$

Then, $\mathcal{E}$ is the set above the piecewise linear curve connecting the points $\{(0,0), p_1, p_1 + p_2, \ldots, (1,1)\}$ and below the piecewise linear curve connecting the points $\{(0,0), p_D, p_D + p_{D-1}, \ldots, (1,1)\}$, where addition of points $p_1 + p_2$ is the point obtained by componentwise addition of p_1 and p_2.

Proof: The proof is given in Appendix D. ■

In the following theorem and its corollary, we present a criterion for two edge-type LDPC ensembles, which, when satisfied, guarantees that the actual rate is equal to the design rate. In order to state the theorem, we define the function $\theta(e_1, e_2)$, which is used to calculate the difference between the growth rate of the average of the total number of codewords and the design rate

$$\begin{aligned}\theta(e_1,e_2) &= \sum_{l_1,l_2}\Lambda_{l_1,l_2}\log_2(1+u_1^{l_2}u_2^{l_2}) - \Lambda_1'(1,1)e_1\log_2 u_1 \\ &\quad - \Lambda_2'(1,1)e_2\log_2 u_2 + \frac{\Lambda_1'(1,1)}{\Gamma'(1)(1)}\sum_{r_1}\Gamma_{r_1}^{(1)}\log_2 q_{r_1}(v_1) \\ &\quad - \Lambda_1'(1,1)e_1\log_2 v_1 + \frac{\Lambda_2'(1,1)}{\Gamma'(2)(1)}\sum_{r_2}\Gamma_{r_2}^{(2)}\log_2 q_{r_2}(v_2) \\ &\quad - \Lambda_2'(1,1)e_2\log_2 v_2 - \Lambda_1'(1,1)h(e_1) - \Lambda_2'(1,1)h(e_2) - R_{\text{des}}\end{aligned} \tag{59}$$

where u_1, u_2, v_1, and v_2 are positive solutions to the following equations:

$$\frac{v_1}{\Gamma^{(1)\prime}(1)}\sum_{r_1} r_1\Gamma_{r_1}^{(1)}\frac{(1+v_1)^{r_1-1} - (1-v_1)^{r_1-1}}{(1+v_1)^{r_1} + (1-v_1)^{r_1}} = ve_1 \tag{60}$$

$$\frac{v_2}{\Gamma^{(2)\prime}(1)}\sum_{r_2} r_2 v\Gamma_{r_2}^{(2)}\frac{(1+v_2)^{r_2-1} - (1-v_2)^{r_2-1}}{(1+v_2)^{r_2} + (1-v_2)^{r_2}} = e_2 \tag{61}$$

$$\frac{1}{\Lambda_1'(1,1)}\sum_{l_1,l_2}\Lambda_{l_1,l_2}l_1\frac{u_1^{l_1}u_2^{l_2}}{1+u_1^{l_1}u_2^{l_2}} = e_1 \tag{62}$$

$$\frac{1}{\Lambda_2'(1,1)}\sum_{l_1,l_2}\Lambda_{l_1,l_2}l_2\frac{u_1^{l_1}u_2^{l_2}}{1+u_1^{l_1}u_2^{l_2}} = e_2. \tag{63}$$

Theorem V.7: Consider the two edge-type LDPC ensemble $(\Lambda, \Gamma^{(1)}, \Gamma^{(2)})$ with design rate R_{des}. Let N be the total number of codewords of a randomly chosen code G from this ensemble and let R_G be the actual rate of the code G. Then

$$\lim_{n\to\infty}\frac{\log_2(\mathbb{E}[N])}{n} = \sup_{(e_1,e_2)\in\mathcal{E}}\theta(e_1,e_2) + R_{\text{des}}$$

where $\theta(e_1, e_2)$ is defined in (59) and the set $\mathcal{E}$ is defined in Lemma V.5.

Proof: By (51), we have

$$\lim_{n\to\infty}\frac{\log_2(\mathbb{E}[N])}{n} = \sup_{(e_1,e_2)\in\mathcal{E}}\lim_{n\to\infty}\frac{\log_2(\mathbb{E}[N(e_1 n\Lambda_1'(1,1), e_2 n\Lambda_2'(1,1))])}{n}.$$

Using Stirling's approximation for the binomial coefficients and [26, Th. 2] for the coefficient growths in Lemma V.4, we know that

$$\lim_{n\to\infty} \frac{\log_2(\mathbb{E}[N(e_1 n\Lambda_1'(1,1), e_2 n\Lambda_2'(1,1))])}{n} = \sup_{(e_1,e_2)\in\mathcal{E}} \inf_{u_1,u_2,v_1,v_2>0} \psi(e_1,e_2,u_1,u_2,v_1,v_2) \quad (64)$$

where $\psi(e_1,e_2,u_1,u_2,v_1,v_2)$ is given by

$$\begin{aligned}&\sum_{l_1,l_2} \Lambda_{l_1,l_2} \log_2(1+u_1^{l_2}u_2^{l_2}) - \Lambda_1'(1,1)e_1\log_2 u_1 \\ &\quad - \Lambda_2'(1,1)e_2\log_2 u_2 + \frac{\Lambda_1'(1,1)}{\Gamma'(1)(1)}\sum_{r_1}\Gamma_{r_1}^{(1)}\log_2 q_{r_1}(v_1) \\ &\quad - \Lambda_1'(1,1)e_1\log_2 v_1 + \frac{\Lambda_2'(1,1)}{\Gamma'(2)(1)}\sum_{r_2}\Gamma_{r_2}^{(2)}\log_2 q_{r_2}(v_2) \\ &- \Lambda_2'(1,1)e_2\log_2 v_2 - \Lambda_1'(1,1)h(e_1) - \Lambda_2'(1,1)h(e_2). \end{aligned} \quad (65)$$

Further, the infimum of ψ with respect to u_1, u_2, v_1, and v_2 is given by solving the following saddle point equations:

$$\frac{\partial\psi}{\partial u_1} = \frac{\partial\psi}{\partial u_2} = \frac{\partial\psi}{\partial v_1} = \frac{\partial\psi}{\partial v_2} = 0 \quad (66)$$

which are equivalent to (60)–(63). ■

We now state the condition, which, when satisfied, guarantees that the actual rate is equal to the design rate.

Corollary 5.8: Let $\theta(e_1,e_2)$ be as defined in (59). If $\sup_{(e_1,e_2)\in\mathcal{E}}\theta(e_1,e_2) = 0$, i.e., if $\theta(1/2,1/2) \geq \theta(e_1,e_2), \forall (e_1,e_2)\in\mathcal{E}$, then for any $\delta>0$

$$\lim_{n\to\infty} P\left(R_G \geq R_{\text{des}} + \delta\right) = 0.$$

The set $\mathcal{E}$ is defined in Lemma V.5.

Proof: From Theorem V.7, $\mathbb{E}[N] = 2^{n(R_{\text{des}}+o(1))}$. Now, from Markov's inequality

$$\begin{aligned}P\left(R_G \geq R_{\text{des}}+\delta\right) &= P\left(N \geq 2^{n(R_{\text{des}}+o(1)+\delta)}\right) \\ &\overset{(a)}{\leq} 2^{-n\delta}\end{aligned}$$

where (a) follows from Markov's inequality. This proves the corollary. ■

Note that in general for a two edge-type LDPC ensemble, in order to check if the actual rate is equal to the design rate, we need to compute the maximum of a two variable function over the set $\mathcal{E}$. However, the set $\mathcal{E}$ is just a line for two edge-type left regular LDPC ensembles. Thus, we deal with the case of left regular LDPC ensembles in the following lemma.

Lemma V.9: Consider the left regular two edge-type LDPC ensemble $\{l_1,l_2,\Gamma^{(1)},\Gamma^{(2)}\}$ with design rate R_{des}. Let N be the total number of codewords of a randomly chosen code G from this ensemble and R_G be its actual rate. Then

$$\lim_{n\to\infty}\frac{\log_2(\mathbb{E}[N])}{n} = \sup_{e\in(0,1)}\theta(e) + R_{\text{des}}.$$

If $\sup_{e\in(0,1)}\theta(e)=0$, i.e., if $\theta(1/2)\geq\theta(e), \forall e\in(0,1)$, then for any $\delta>0$

$$\lim_{n\to\infty}\mathbb{P}\left(R_G > R_{\text{des}}+\delta\right) = 0.$$

The function $\theta(e)$ is defined as

$$\begin{aligned}\theta(e) &= (1-l_1-l_2)h(e) + \frac{l_1}{\Gamma^{(1)\prime}(1)}\sum_r \Gamma_r^{(1)}\log q_r(v_1) \\ &+ \frac{l_2}{\Gamma^{(2)\prime}(1)}\sum_r\Gamma_r^{(2)}\log q_r(v_2) - el_1\log v_1 - el_2\log v_2 - R_{\text{des}}\end{aligned}$$

where v_1 (resp. v_2) is the unique positive solution of (60) (resp. (61)) with e_1 (resp. e_2) substituted by e on the RHS.

Proof: Most of the arguments in this lemma are the same as those of Theorem V.7, so we will omit them. First, note that the cardinality of the set $\mathcal{W}(E_1,E_2)$, as defined in Lemma V.4, is given by

$$\begin{aligned}|\mathcal{W}(E_1,E_2)| &= \text{coef}\left\{(1+u_1^{l_1}u_2^{l_2})^n, u_1^{E_1}u_2^{E_2}\right\} \\ &= \begin{cases}0, & \frac{E_2}{l_2}\neq\frac{E_1}{l_1} \\ \binom{n}{E_1/l_1}, & \text{otherwise.}\end{cases}\end{aligned}$$

Let $e = E_1/(nl_1) = E_2/(nl_2)$. By Stirling's approximation and the saddle point approximation for the coefficient terms [20, pp. 517], we obtain

$$\begin{aligned}\lim_{n\to\infty}\frac{\log_2(\mathbb{E}[N])}{n} &= \lim_{n\to\infty}\sup_{e\in(0,1)}\frac{\log_2(\mathbb{E}[N(enl_1,enl_2)])}{n} \\ &= \sup_{e\in(0,1)}\inf_{v_1,v_2>0}\psi(e,v_1,v_2)\end{aligned}$$

where

$$\begin{aligned}\psi(e,v_1,v_2) &= (1-l_1-l_2)h(e) \\ &+ \frac{l_1}{\Gamma^{(1)\prime}(1)}\sum_{r_1}\Gamma_{r_1}^{(1)}\log_2 q_{r_1}(v_1) - el_1\log_2 v_1 \\ &+ \frac{l_1}{\Gamma^{(2)\prime}(1)}\sum_r\Gamma_r^{(2)}\log_2 q_r(v_2) - el_2\log_2 v_2.\end{aligned}$$

The saddle point equations are obtained by taking the partial derivatives of ψ with respect to $v_j, j\in\{1,2\}$ and setting them equal to 0. These equations are the same as (60) (resp. (61)) with e_1 (resp. e_2) substituted by e on the RHS. ■

Remark: Note that as in [15], we can change the order of $\inf$ and $\sup$. Taking the derivatives after changing the order gives a function which is an upper bound on $\theta(e)$. The advantage of this upper bound is that it can be computed without solving any saddle point equations. However, as opposed to the single

edge-type LDPC ensembles, for two edge-type LDPC ensembles, this upper bound is not tight and does not provide a meaningful criterion to check if the rate is equal to the design rate.

The following two lemmas show that in the case of a left regular ensemble where $\Gamma^{(1)}$ and $\Gamma^{(2)}$ both have only either odd or even degrees, the function $\theta(e)$ attains its maximum inside the interval $[0, 1/2]$.

Lemma V.10: Consider the left regular two edge-type LDPC ensemble $\{l_1, l_2, \Gamma^{(1)}, \Gamma^{(2)}\}$. Let $\theta(e)$ be the function as defined in Lemma V.9. If both $\Gamma^{(1)}$ and $\Gamma^{(2)}$ are such that both the type of check nodes only have odd degrees, then for $e > 1/2$

$$\theta(e) < \theta(1/2).$$

Proof: The proof is given in Appendix E. ■

Lemma V.11: Consider the left regular two edge-type LDPC ensemble $\{l_1, l_2, \Gamma^{(1)}, \Gamma^{(2)}\}$. Let $\theta(e)$ be the function as defined in Lemma V.9. If both $\Gamma^{(1)}$ and $\Gamma^{(2)}$ are such that both the type of check nodes only have even degrees, then for $e \in (0, 1/2)$

$$\theta(e) = \theta(1 - e).$$

Proof: The proof is given in Appendix F. ■

In the following theorem, we state how we can compute the quantity $H(\underline{X}|\underline{S}, \underline{Z})$ appearing in (43).

Theorem V.12: Consider transmission over the $\text{BEC-WT}(\epsilon_m, \epsilon_w)$ using a random code G from the two edge-type LDPC ensemble $\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$ and the coset encoding method. Let $\underline{S}$ be the information word from Alice for Bob, $\underline{X}$ be the transmitted word, and $\underline{Z}$ be the wiretapper's observation.

Also consider a point-to-point communication setup for transmission over the $\text{BEC}(\epsilon_w)$ using the two edge-type LDPC ensemble $\{\Lambda, \Gamma^{(1)}, \Gamma^{(2)}\}$. Assume that the erasure probability ϵ_w is above the BP threshold of the ensemble. Let $\{\Omega, \Phi^{(1)}, \Phi^{(2)}\}$ be the average residual ensemble resulting from the peeling decoder. Let R^r_{des} be the design rate of the residual ensemble $\{\Omega, \Phi^{(1)}, \Phi^{(2)}\}$. If $\{\Omega, \Phi^{(1)}, \Phi^{(2)}\}$ satisfies the condition of Theorem V.7, i.e., if the design rate of the residual ensemble is equal to the rate, then

$$\lim_{n\to\infty} \frac{\mathbb{E}(H_G(\underline{X}|\underline{S}, \underline{Z}))}{n} = \epsilon_w \Lambda(y_1, y_2) R^r_{\text{des}} \tag{67}$$

where x_1, x_2, y_1, and y_2 are the fixed points of the density evolution equations (19) and (20) obtained when initializing them with $x_1^{(1)} = x_2^{(2)} = \epsilon_w$.

Proof: From Lemma IV.3, we know that the conditional entropy in the point-to-point setup is identical to $H(\underline{X}|\underline{S}, \underline{Z})$. The conditional entropy in the point-to-point case is equal to the RHS of (67). This follows from the same arguments as in [15, Th. 10]. The quantity $\epsilon_w \Lambda(y_1, y_2)$ on the RHS of (67) is the ratio of the number of variable nodes in the residual ensemble to that in the initial ensemble. ■

This gives us the following method to calculate the equivocation of Eve when using two edge-type LDPC ensembles for the $\text{BEC-WT}(\epsilon_m,\ \epsilon_w)$ based on the coset encoding method.

1) If the threshold of the two edge-type LDPC ensemble is lower than ϵ_w, calculate the residual degree distribution for the two edge-type LDPC ensemble for transmission over the $\text{BEC}(\epsilon_w)$. Check that the rate of this residual ensemble is equal to the design rate using Theorem V.7. Calculate $H(\underline{X}|\underline{S}, \underline{Z})$ using Theorem V.12. If the threshold is higher than ϵ_w, $H(\underline{X}|\underline{S}, \underline{Z})$ is trivially zero.
2) If the threshold of the single edge-type LDPC ensemble induced by type one edges is higher than ϵ_w, calculate the residual degree distribution of this ensemble for transmission over the $\text{BEC}(\epsilon_w)$. Check that its rate is equal to the design rate using [15, Lemma 7]. Calculate $H(\underline{X}|\underline{Z})$ using Theorem IV.2. If the threshold is higher than ϵ_w, $H(\underline{X}|\underline{Z})$ is trivially zero.
3) Finally, calculate $H(\underline{S}|\underline{Z})$ using (43).

In the next section, we demonstrate this procedure by computing the equivocation of Eve for various two edge-type LDPC ensembles.

VI. Examples

Example 1: Consider using the ensemble defined by single edge-type LDPC degree distribution 1, defined in Section III, for transmission over the $\text{BEC-WT}(0.5, 0.6)$ at rate $R_{ab} = 0.498836$ b.p.c.u. (the full rate of the ensemble), without using the coset encoding scheme. Here, every possible message $\underline{s}$ corresponds to a single codeword $\underline{x}$, and encoding and decoding are done as with a single edge-type LDPC code. Since the threshold is 0.5, Bob can decode with error probability approaching zero. The equivocation of Eve is given by $H(\underline{S}|\underline{Z}) = H(\underline{X}|\underline{Z})$ which can be calculated using the MMU method. In Fig. 4, we plot the function $\Psi_{\{\Omega^{(1)}, \Phi^{(1)}\}}(u)$ defined in [15, Lemma 7] corresponding to the single edge-type LDPC ensemble $\{\Omega^{(1)}, \Phi^{(1)}\}$, which is the average residual degree distribution of the ensemble for transmission over the $\text{BEC}(\epsilon_w)$. From [15, Lemma 7], if the maximum of $\Psi_{\{\Omega^{(1)}, \Phi^{(1)}\}}(u)$ over the unit interval occurs at $u = 1$, which holds in this case, the design rate of the residual graph is equal to the actual rate. Thus, we can calculate the equivocation $R_e = 0.0989137$ b.p.c.u. Using this ensemble, we can achieve the point $(R_{ab}, R_e) = (0.498836, 0.0989137)$ in the rate-equivocation region which is very close to the point C = $(0.5, 0.1)$ in Fig. 2.

Example 2: Now consider the two edge-type ensemble defined by two edge-type degree distribution 1, defined in Section III, for transmission over the $\text{BEC-WT}(0.5, 0.6)$ using the coset encoding scheme. Again, Bob can decode, since the threshold of the ensemble induced by type one edges is 0.5. Since the threshold of the two edge-type ensemble is 0.6, we get $H(\underline{X}|\underline{S}, \underline{Z}) = 0$, and we get $H(\underline{S}|\underline{Z}) = H(\underline{X}|\underline{Z})$. The degree distribution of the type one edges is the same as the degree distribution in Example 1, so we again get $\lim_{n\to\infty} \mathbb{E}(H(\underline{X}|\underline{Z}))/n = 0.0989137$. Using this scheme, we achieve the point $(R_{ab}, R_e) = (0.0999064, 0.0989137)$ in the rate-equivocation region which is very close to point B = $(0.1, 0.1)$ in Fig. 2.

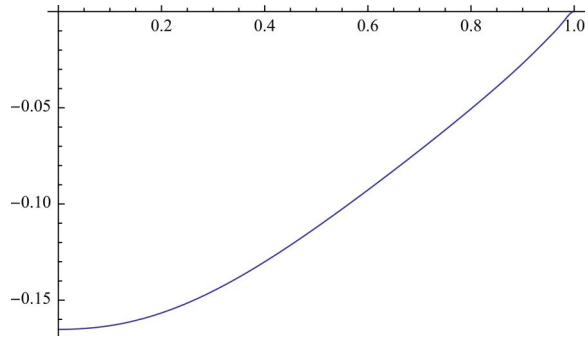

Fig. 4. $\Psi_{\{\Omega^{(1)},\Phi^{(1)}\}}(u)$ for Examples 1 and 2.

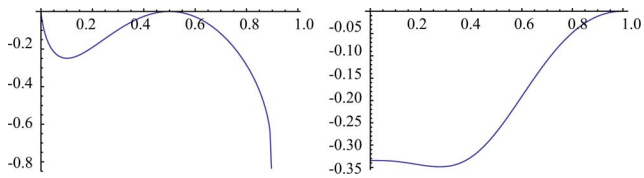

Fig. 5. $\theta(e)$ and $\Psi_{\{\Omega^{(1)},\Phi^{(1)}\}}(u)$ for Example 3.

Example 3: Consider transmission over the BEC-WT$(0.429, 0.75)$ using the coset encoding scheme and the regular two edge-type ensemble defined by

Two Edge-Type Degree Distribution 3:

$$\Lambda(x,y) = x^3y^3 \tag{68}$$
$$\Gamma^{(1)}(x) = x^6 \tag{69}$$
$$\Gamma^{(2)}(x) = x^{12}. \tag{70}$$

The design rate of this ensemble is 0.25 and the threshold is 0.469746. The threshold for the ensemble induced by type one edges is 0.4294, so it can be used for reliable communication if $\epsilon_m < 0.4294$.

To calculate the equivocation of Eve, we first calculate $\lim_{n\to\infty} H(\underline{X}|\underline{Z})/n$ by the MMU method. We calculate the average residual degree distribution $\{\Omega^{(1)}, \Phi^{(1)}\}$ of the ensemble induced by type one edges for erasure probability ϵ_w and plot $\Psi_{\{\Omega^{(1)},\Phi^{(1)}\}}(u)$ in Fig. 5. As in Examples 1 and 2, we see that it takes its maximum at $u = 1$. Thus, by [15, Lemma 7], we obtain that the conditional entropy is equal to the design rate of the residual ensemble normalized with respect to the number of variable nodes in the original ensemble, i.e., $\lim_{n\to\infty} \mathbb{E}(H(\underline{X}|\underline{Z}))/n = 0.250124$.

We now calculate the average residual degree distribution $(\Omega, \Phi^{(1)}, \Phi^{(2)})$ of the two edge-type ensemble corresponding to erasure probability ϵ_w and plot the function $\theta(e)$ defined in Lemma V.9. If $\theta(e)$ is less than or equal to zero for $e \in [0,1]$, then the rate of the residual ensemble is equal to the design rate by Lemma V.9. Then, we can calculate $H(\underline{X}|\underline{S}, \underline{Z})$ using Lemma V.12. In Fig. 5, we see that $\sup_{e\in[0,1]} \theta(e) = 0$, and we get $\lim_{n\to\infty} \mathbb{E}(H(\underline{X}|\underline{S}, \underline{Z}))/n = 0.000124297$.

Finally, using (43), we get $\mathbb{E}(H(\underline{S}|\underline{Z}))/n = 0.24999998$. We thus achieve the point $(R_{ab}, R_e) = (0.25, 0.24999998)$ in the rate-equivocation region. We see that we are very close to perfect secrecy. The reason that we are so far away from the secrecy capacity $C_s = 0.321$ is that the $(3, 6)$ ensemble for the main channel is far from being capacity achieving.

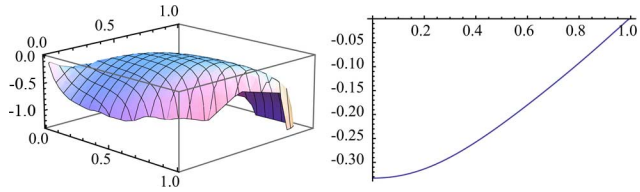

Fig. 6. $\theta(e_1, e_2)$ and $\Psi_{\{\Omega^{(1)},\Phi^{(1)}\}}(u)$ for Example 4.

Example 4: Consider the two edge-type ensemble

Two Edge-Type Degree Distribution 4:

$$\begin{aligned}\Lambda(x,y) = {} & 0.5572098x^2y^3 + 0.1651436x^3y^3 \\ & + 0.07567923x^4y^3 + 0.0571348x^5y^3 \\ & + .043603x^7y^3 + 0.02679802x^8y^3 \\ & + 0.013885518x^{13}y^3 + 0.0294308x^{14}y^3 \\ & + 0.02225301x^{31}y^3 + 0.00886105x^{100}y^3 \\ \Gamma^{(1)}(x) = {} & 0.25x^9 + 0.75x^{10} \\ \Gamma^{(2)}(x) = {} & x^{12}\end{aligned}$$

where the graph induced by type one edges has the same degree distribution as single edge-type LDPC degree distribution 1 and the graph induced by type two edges is $(3, 12)$ regular. The rate of the overall ensemble is 0.248836 and the rate from Alice to Bob is $R_{ab} = 0.25$. Consider transmission over the BEC-WT$0.5, 0.751164)$.

In Fig. 6, we plot $\Psi_{\{\Omega^{(1)},\Phi^{(1)}\}}(u)$ for the residual ensemble $\{\Omega^{(1)}, \Phi^{(1)}\}$ induced by type one edges for transmission over the BEC(ϵ_w). Since the maximum of $\Psi_{\{\Omega^{(1)},\Phi^{(1)}\}}(u)$ over the unit interval occurs at $u = 1$, we obtain by [15, Lemma 7] that the rate is equal to the design rate for this residual ensemble. In Fig. 6, we plot $\theta(e_1, e_2)$ for the residual ensemble $(\Omega, \Phi^{(1)}, \Phi^{(2)})$ of the two edge-type LDPC ensemble for transmission over the BEC(ϵ_w). Since the maximum of $\theta(e_1, e_2)$ over the unit square is zero, we obtain by Theorem V.7 that the rate is equal to the design rate for this residual two edge-type ensemble. In this case, we can calculate the equivocation of Eve and find it to be 0.24999999, which is very close to the rate. Thus, this ensemble achieves the point $(R, R_e) = (0.25, 0.24999999)$ in the capacity-equivocation region in Fig. 2. Note that the secrecy capacity is 0.251164.

These examples demonstrate that simple ensembles have very good secrecy performance when the weak notion of secrecy is considered.

VII. Conclusion

We consider the use of two edge-type LDPC codes for the binary erasure wiretap channel. The reliability performance can be easily measured using density evolution recursion. We generalize the method of [15] to two edge-type LDPC codes in order to measure the security performance. We find that relative simple ensembles have very good secrecy performance. We have constructed a capacity achieving sequence of two edge-type LDPC ensembles for the BEC based on capacity achieving sequences for the single edge-type LDPC ensemble. However, this construction introduces some degree one variable nodes in the ensemble for the main channel, requiring an erasure free main

channel. We use linear programming methods to find ensembles that operate close to secrecy capacity. However, as the underlying channel in our setup is a BEC, it is highly desirable to construct explicit sequences of secrecy capacity achieving ensembles. Due to the 2-D recursion of density evolution for two edge-type LDPC ensembles, this is a much harder problem. In our opinion, this is one of the fundamental open problems in the setting of using sparse graph codes for transmission over the BEC-WT(ϵ_m, ϵ_w).

Appendix A
Proof of Lemma V.1

Proof: Consider a residual graph G. Consider two type one edges e_1 and e_2 (the argument is the same for type two edges). Swap the check node side end points of e_1 and e_2. We denote the resulting graph by G'. The proof is completed by noting that the number of erasure patterns which result in G is equal to the number of erasure patterns which result in G'. This is because if the variable nodes in G form the largest stopping set in the erasure pattern, then so do the variable nodes in G'. ■

Appendix B
Proof Outline of Lemma V.2

Proof: The proof for the single edge-type LDPC case uses the Wormald technique described in [20, Appendix C]. Our proof is the same as that for the single edge-type LDPC case except that we have to keep track of the degree distribution of two different types of edges.

Assume that in the peeling decoder, a degree one check node is chosen randomly from the set of degree one check nodes. Let $G(t)$ be the residual graph after the tth iteration of the peeling decoder. Let $V^{(1)}_{i_1 i_2}(t)$ (resp. $V^{(2)}_{i_1 i_2}(t)$) be the number of type one (resp. type 2) edges which are connected to a variable node of degree (i_1, i_2) in $G(t)$. For $j \in \{1, 2\}$, let $V^{(j)}(t)$ be the vector of number of type j edges of different degrees i.e., $V^{(j)}(t) = \{V^{(j)}_{i_1 i_2}(t)\}_{i_1, i_2}$. Let $C^{(1)}_i(t)$ (resp. $C^{(2)}_i(t)$) be the number of type one (resp. type two) edges which are connected to type one (resp. type two) check nodes of degree i at time t. For $j \in \{1, 2\}$, let $C^{(j)}(t) = \{C^{(j)}_i(t)\}_i$. To show the concentration of the residual degree distribution using the Wormald technique, we note that $\big(V^{(1)}(t), V^{(2)}(t), C^{(1)}(t), C^{(2)}(t)\big)$ is a Markov process. The next requirement is that the maximum possible change in $V^{(j)}_{i_1 i_2}(t)$ and $C^{(j)}_i(t)$ for $j \in \{1, 2\}$, for all (i_1, i_2) and for all i after an iteration of the peeling decoder should be bounded. This is true as all the degrees are finite. The functions which describe the expected change in $V^{(j)}_{i_1 i_2}(t)$ and $C^{(j)}_i(t)$ are also Lipschitz continuous in $\big(V^{(1)}(t)/n, V^{(2)}(t)/n, C^{(1)}(t)/n, C^{(2)}(t)/n\big)$, where n is the number of variable nodes. For example, as long as $C^{(1)}_1(t) + C^{(2)}_1(t) > 0$, for $j \in \{1, 2\}$

$$\mathbb{E}\left[V^{(j)}_{i_1 i_2}(t+1) - V^{(j)}_{i_1 i_2}(t) | V^{(1)}(t), V^{(2)}(t), C^{(1)}(t), C^{(2)}(t)\right] = -\frac{i_j V^{(j)}_{i_1 i_2}}{\sum_{l_1, l_2} V^{(j)}_{l_1 l_2}}.$$

The RHS of the previous equation is the same as that for the single edge-type LDPC ensemble which has been shown to be Lipschitz continuous.

The last required condition is that of initial concentration, i.e., the concentration condition should be satisfied at the beginning of the peeling decoder. This proof is the same as that for the single edge-type LDPC ensemble given in [20, Appendix C]. ■

Appendix C
Proof of Lemma V.5

Proof: The terms in the expansion of $\prod_{l_1, l_2}(1 + u_1^{l_1} u_2^{l_2})^{n\Lambda_{l_1, l_2}}$ have the form

$$u_1^{\sum_{l_1, l_2} l_1 k(l_1, l_2)\Lambda_{l_1, l_2}} u_2^{\sum_{l_1, l_2} l_2 k(l_1, l_2)\Lambda_{l_1, l_2}}$$

where $0 \leq k(l_1, l_2) \leq n$. If the coefficient of $u_1^{e_1 n\Lambda'_1(1,1)} u_2^{e_2 n\Lambda'_2(1,1)}$ is nonzero, there exist $\{k(l_1, l_2)\}_{l_1, l_2}$ such that

$$\sum_{l_1, l_2} l_1 k(l_1, l_2)\Lambda_{l_1, l_2} = e_1 n\Lambda'_1(1, 1)$$

and

$$\sum_{l_1, l_2} l_2 k(l_1, l_2)\Lambda_{l_1, l_2} = e_2 n\Lambda'_2(1, 1)$$

which is the same as

$$(e_1, e_2) = \left(\frac{\sum_{l_1, l_2} l_1 \Lambda_{l_1, l_2}\sigma(l_1, l_2)}{\Lambda'_1(1, 1)}, \frac{\sum_{l_1, l_2} l_2 \Lambda_{l_1, l_2}\sigma(l_1, l_2)}{\Lambda'_2(1, 1)}\right)$$

where $0 \leq \sigma(l_1, l_2) = k(l_1, l_2)/n \leq 1$. When n grows, this is the same as (56). ■

Appendix D
Proof of Lemma V.6

Proof: We show that $\mathcal{E}$ is the set between the two piecewise linear curves described in the statement of this lemma. We show this by varying $\sigma(l_1, l_2)$ between 0 and 1 while trying to make the ratio e_1/e_2 as large as possible. Start by letting $\sigma(l_1, l_2) = 0$ if l_1/l_2 is not maximal, and letting $\sigma(l_1, l_2)$ increase to 1 if l_1/l_2 is maximal. This traces out the line between $(0, 0)$ and p_1, and clearly, we cannot have (e_1, e_2) below this line for $(e_1, e_2) \in \mathcal{E}$. Then, increase $\sigma(l_1, l_2)$ for l_1, l_2 such that l_1/l_2 takes the second largest value. This traces out the line between p_1 and $p_1 + p_2$ and again it is clear that we cannot have (e_1, e_2) below this line for $(e_1, e_2) \in \mathcal{E}$. We continue like this until we have $\sigma(l_1, l_2) = 1$ for all l_1, l_2, which corresponds to the point $(1, 1)$. The upper curve is obtained by reversing the order and starting with the line between $(0, 0)$ and p_D. ■

Appendix E
Proof of Lemma V.10

Proof: Take the derivative of $\theta(e)$ with respect to e to get

$$\begin{aligned}\frac{d\theta}{de} &= (1 - l_1 - l_2)\log\left(\frac{1-e}{e}\right) - l_1 \log v_1 - l_2 \log v_2 \\ &= \log\left(\frac{1-e}{e}\right) - l_1 \log\left(\frac{(1-e)v_1}{e}\right) \\ &\quad - l_2 \log\left(\frac{(1-e)v_2}{e}\right).\end{aligned}$$

Using (60) and (61), we obtain

$$\begin{aligned}\frac{1-e}{e} &= \frac{1-\frac{v_1}{\Gamma^{(1)\prime}(1)}\sum_{r_1} r_1\Gamma_{r_1}^{(1)}\frac{(1+v_1)^{r_1-1}-(1-v_1)^{r_1-1}}{(1+v_1)^{r_1}+(1-v_1)^{r_1}}}{\frac{v_1}{\Gamma^{(1)\prime}(1)}\sum_{r_1} r_1\Gamma_{r_1}^{(1)}\frac{(1+v_1)^{r_1-1}-(1-v_1)^{r_1-1}}{(1+v_1)^{r_1}+(1-v_1)^{r_1}}} \\ &= \frac{\sum_{r_1} r_1\Gamma_{r_1}^{(1)}\left(1-v_1\frac{(1+v_1)^{r_1-1}-(1-v_1)^{r_1-1}}{(1+v_1)^{r_1}+(1-v_1)^{r_1}}\right)}{\sum_{r_1} r_1\Gamma_{r_1}^{(1)}v_1\frac{(1+v_1)^{r_1-1}-(1-v_1)^{r_1-1}}{(1+v_1)^{r_1}+(1-v_1)^{r_1}}} \\ &= \frac{\sum_{r_1} r_1\Gamma_{r_1}^{(1)}\frac{(1+v_1)^{r_1-1}+(1-v_1)^{r_1-1}}{(1+v_1)^{r_1}+(1-v_1)^{r_1}}}{\sum_{r_1} r_1\Gamma_{r_1}^{(1)}v_1\frac{(1+v_1)^{r_1-1}-(1-v_1)^{r_1-1}}{(1+v_1)^{r_1}+(1-v_1)^{r_1}}}\end{aligned}$$

or

$$\frac{(1-e)v_1}{e} = \frac{\sum_{r_1} r_1\Gamma_{r_1}^{(1)}\frac{(1+v_1)^{r_1-1}+(1-v_1)^{r_1-1}}{(1+v_1)^{r_1}+(1-v_1)^{r_1}}}{\sum_{r_1} r_1\Gamma_{r_1}^{(1)}\frac{(1+v_1)^{r_1-1}-(1-v_1)^{r_1-1}}{(1+v_1)^{r_1}+(1-v_1)^{r_1}}}. \tag{71}$$

We obtain a similar expression for $(1-e)v_2/e$. Note that $v_j(e)$ are increasing functions of e and $v_j(1/2) = 1$. Thus, for $e > 1/2,\ v_j > 1$ which together with (71) implies $\frac{(1-e)v_j}{e} > 1$ when all r are odd. This in turn implies that $\frac{d\theta}{de} < 0$ for $e > 1/2$. ■

Appendix F
Proof of Lemma V.11

Proof: First, we show that $v(1-e) = 1/v(e)$ if there are only even degrees. Let $v_j(e) = v$ and $1/v = \tilde{v}$. Then

$$\begin{aligned}e &= \frac{1/\tilde{v}}{\Gamma^{(j)\prime}(1)}\sum_r r\Gamma_r^{(j)}\frac{(1+1/\tilde{v})^{r-1}-(1-1/\tilde{v})^{r-1}}{(1+1/\tilde{v})^r+(1-1/\tilde{v})^r} \\ &= \frac{1}{\Gamma^{(j)\prime}(1)}\sum_r r\Gamma_r^{(j)}\frac{(1+\tilde{v})^{r-1}+(1-\tilde{v})^{r-1}}{(1+\tilde{v})^r+(1-\tilde{v})^r}\end{aligned}$$

and

$$\begin{aligned}1-e &= 1-\frac{v}{\Gamma^{(j)\prime}(1)}\sum_r r\Gamma_r^{(j)}\frac{(1+v)^{r-1}-(1-v)^{r-1}}{(1+v)^r+(1-v)^r} \\ &= \frac{1}{\Gamma^{(j)\prime}(1)}\sum_r \Gamma_r^{(j)}\left(1-v\frac{(1+v)^{r-1}-(1-v)^{r-1}}{(1+v)^r+(1-v)^r}\right) \\ &= \frac{1}{\Gamma^{(j)\prime}(1)}\sum_r r\Gamma_r^{(j)}\frac{(1+v)^{r-1}+(1-v)^{r-1}}{(1+v)^r+(1-v)^r}.\end{aligned}$$

These two equations imply that $v(1-e) = 1/v(e)$. Now note that

$$q_r(1/v) = \frac{q_r(v)}{v^r}$$

for r even, so

$$\begin{aligned}\theta(1-e) &= (1-l_1-l_2)h(1-e)+\frac{l_1}{\Gamma^{(1)\prime}(1)}\sum_r\Gamma_r^{(1)}\log\frac{q_r(v_1)}{v_1^r} \\ &\quad+\frac{l_2}{\Gamma^{(2)\prime}(1)}\sum_r\Gamma_r^{(2)}\log\frac{q_r(v_2)}{v_2^r}-(1-e)l_1\log(1/v_1) \\ &\quad-(1-e)l_2\log(1/v_2)-R_{\mathrm{des}} \\ &= (1-l_1-l_2)h(1-e)+\frac{l_1}{\Gamma^{(1)\prime}(1)}\sum_r\Gamma_r^{(1)}\log q_r(v_1) \\ &\quad-l_1\log v_1+\frac{l_2}{\Gamma^{(2)\prime}(1)}\sum_r\Gamma_r^{(2)}\log q_r(v_2)-l_2\log v_2 \\ &\quad+(1-e)l_1\log(v_1)+(1-e)l_2\log(v_2)-R_{\mathrm{des}} \\ &= \theta(e)\end{aligned}$$

using that

$$\begin{aligned}\frac{l_j}{\Gamma^{(j)\prime}(1)}\sum_r 08820\Gamma_r^{(j)}\log v_j^r &= \frac{l_j}{\Gamma^{(j)\prime}(1)}\sum_r r\Gamma_r^{(j)}\log v_j \\ &= l_j\log v_j\end{aligned}$$

in the second equality. ■

References

[1] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Two edge type LDPC codes for the wiretap channel," in *Proc. 43rd Asilomar Conf. Signals, Syst. Comput.*, 2009, pp. 834–838.

[2] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Equivocation of Eve using two edge type LDPC codes for the erasure wiretap channel," in *Proc. 44th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2010, pp. 2045–2049.

[3] A. D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[5] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[6] R. Liu, H. Poor, P. Spasojevic, and Y. Liang, "Nested codes for secure transmission," in *Proc. IEEE 19th Int. Symp. Pers. Indoor Mobile Radio Commun. Conf.*, Sep. 2008, pp. 1–5.

[7] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun. 2002.

[8] A. T. Suresh, A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy for erasure wiretap channels," presented at the Inform. Theory Workshop, Dublin, Ireland, Aug. 2010.

[9] Y. Chen and A. J. H. Vinck, "On the binary symmetric wiretap channel," in *Proc. Int. Zurich Semin. Commun.*, Mar. 2010, pp. 17–20.

[10] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[11] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Commun. Lett.*, vol. 14, no. 8, pp. 752–754, Aug. 2010.

[12] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," in *Proc. Int. Symp. Inf. Theory*, Austin, TX, Jun. 2010, pp. 913–917.

[13] O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," in *Proc. IEEE 21st Int. Symp. Pers. Indoor Mobile Radio Commun. Conf.*, Sep. 2010, pp. 2698–2703.

[14] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *Proc. IEEE Inf. Theory Workshop*, Dublin, Ireland, Aug. 2010, pp. 1–5.

[15] C. Méasson, A. Montanari, and R. Urbanke, "Maxwell construction: The hidden bridge between iterative and maximum a posteriori decoding," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5277–5307, Dec. 2008.

[16] V. Rathi, "Non-binary LDPC codes and EXIT like functions," Ph.D. dissertation, Swiss Federal Institute of Technology, Lausanne, Switzerland, 2008.

[17] V. Rathi and I. Andriyanova, "Some results on map decoding of non-binary LDPC codes over the BEC," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2225–2242, Apr. 2011.

[18] D. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.

[19] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.

[20] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[21] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 569–584, Feb. 2001.

[22] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 585–598, Feb. 2001.

[23] R. Hinton and S. Wilson, "Analysis of peeling decoder for met ensembles," in *Proc. IEEE Inf. Theory Workshop*, Jan. 2010, pp. 1–5.

[24] R. Ikegaya, K. Kasai, Y. Shimoyama, T. Shibuya, and K. Sakaniwa, "Weight and stopping set distributions of two-edge type LDPC code ensembles," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E88-A, no. 10, pp. 2745–2761, 2005.

[25] K. Kasai, T. Awano, D. Declercq, C. Poulliat, and K. Sakaniwa, "Weight distributions of multi-edge type LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 60–64.
[26] D. Burshtein and G. Miller, "Asymptotic enumeration methods for analyzing LDPC codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1115–1131, Jun. 2004.

Vishwambhar Rathi obtained the Bachelor of Technology (B.Tech) degree in Electrical Engineering from Indian Institute of Technology, Bombay (IITB), India. He obtained his Ph.D. degree in the domain of sparse graph codes from Swiss Federal Institute of Technology, Lausanne (EPFL), Switzerland. In 2009–2010, he was a post doctoral researcher at Royal Institute of Technology (KTH), Stockholm, Sweden. In 2010, he joined a wireless communication start up Icera Semiconductors which was acquired by Nvidia Corporation in 2011. He is currently a modem software engineer at Nvidia. His main research interests are information theory, coding theory, wireless communication, and graphical models.

Mattias Andersson (S'07) received the M.Sc. degree in Engineering Physics from the KTH Royal Institute of Technology, Stockholm, Sweden in 2007. In 2007 he joined the Communication Theory laboratory of the School of Electrical Engineering at the KTH Royal Institute of Technology, Stockholm, Sweden. His research interests include digital communications and information theory with focus on code design for physical layer security.

Ragnar Thobaben (M'07) received the Dipl.-Ing. degree (M.Sc.) in electrical engineering in 2001 and the Dr.-Ing. degree (Ph.D.) in electrical engineering in 2007 from the University of Kiel, Germany. In December 2006, Dr. Thobaben joined the Communication Theory Lab at the Royal Institute of Technology (KTH), Stockholm, Sweden, as a post-doctoral researcher, where he serves since July 2008 as an Assistant Professor.

Dr. Thobaben's current research activities are dedicated to the design and analysis of coding and transmission schemes for communication networks with a special focus on cognitive radio, cooperative communication, coordination, as well as physical-layer and network security.

Dr. Thobaben serves currently on the technical program committees for the 2012 IEEE PIMRC and the 2012 ISWCS and as publicity chair for the 2012 International Symposium on Turbo Codes & Iterative Information Processing. He served as well as publicity chair for the 2011 IEEE Swedish Communication Technologies Workshop.

Joerg Kliewer (S'97–M'99–SM'04) received the Dipl.-Ing. (M.Sc.) degree in electrical engineering from Hamburg University of Technology, Germany, in 1993 and the Dr.-Ing. degree (Ph.D.) in electrical engineering from the University of Kiel, Germany, in 1999, respectively.

From 1993 to 1998, he was a Research Assistant at the University of Kiel, and from 1999 to 2004, he was a Senior Researcher and Lecturer with the same institution. In 2004, he visited the University of Southampton, Southampton, U.K., for one year, and from 2005 until 2007, he was with the University of Notre Dame, Notre Dame, IN, as a Visiting Assistant Professor. In August 2007, he joined New Mexico State University, Las Cruces, NM, as an Assistant Professor. His research interests include information theory, error correcting codes, network coding, and communication networks.

Dr. Kliewer was the recipient of a Leverhulme Trust Award and a German Research Foundation Fellowship Award in 2003 and 2004, respectively. He was a Member of the Editorial Board of the *EURASIP Journal on Advances in Signal Processing* from 2005–2009 and is an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS since 2008.

Mikael Skoglund (S'93–M'97–SM'04) received the Ph.D. degree in 1997 from Chalmers University of Technology, Sweden. In 1997, he joined the Royal Institute of Technology (KTH), Stockholm, Sweden, where he was appointed to the Chair in Communication Theory in 2003. At KTH, he heads the Communication Theory Lab and he is the Assistant Dean for Electrical Engineering.

Dr. Skoglund's research interests are in the theoretical aspects of wireless communications. He has worked on problems in source-channel coding, coding and transmission for wireless communications, Shannon theory and statistical signal processing. He has authored and co-authored more than 300 scientific papers in these areas, and he holds six patents.

Dr. Skoglund has served on numerous technical program committees for IEEE conferences. During 2003–2008 he was an associate editor with the IEEE TRANSACTIONS ON COMMUNICATIONS and he is presently on the editorial board for IEEE TRANSACTIONS ON INFORMATION THEORY.