Chalmers Publication Library

Threshold Saturation for Nonbinary SC-LDPC Codes on the Binary Erasure Channel

(article starts on next page)

Threshold Saturation for Nonbinary SC-LDPC Codes on the Binary Erasure Channel

Iryna Andriyanova, *Member, IEEE*, and Alexandre Graell i Amat, *Senior Member, IEEE*

Abstract—We analyze the asymptotic performance of nonbinary spatially-coupled low-density parity-check (SC-LDPC) code ensembles defined over the general linear group on the binary erasure channel. In particular, we prove threshold saturation of belief propagation decoding to the so called potential threshold, using the proof technique based on potential functions introduced by Yedla *et al.*, assuming that the potential function exists. We rewrite the density evolution of nonbinary SC-LDPC codes in an equivalent vector recursion form which is suited for the use of the potential function. We then discuss the existence of the potential function for the general case of vector recursions defined by multivariate polynomials, and give a method to construct it. We define a potential function in a slightly more general form than one by Yedla *et al.*, in order to make the technique based on potential functions applicable to the case of nonbinary LDPC codes. We show that the potential function exists if a solution to a carefully designed system of linear equations exists. Furthermore, we show numerically the existence of a solution to the system of linear equations for a large number of nonbinary LDPC code ensembles, which allows us to define their potential function and thus prove threshold saturation.

I. INTRODUCTION

Spatially-coupled low-density parity-check (SC-LDPC) codes have been shown to achieve outstanding performance for a myriad of channels and communication problems. Their excellent performance is due to the so-called *threshold saturation phenomenon*. For the binary erasure channel (BEC) it was proved in [1] that the belief propagation (BP) decoding of binary SC-LDPC codes *saturates* to the maximum a posteriori (MAP) threshold of the underlying regular ensemble. This result was later extended to binary memoryless channels (BMS) [2], and the same threshold phenomenon has been observed for many channels and systems. Recently, an alternative proof technique for the threshold saturation phenomenon has been introduced in [3] and [4], based on the notion of potential functions. The proof relies on the observation that a fixed point of the density evolution (DE) corresponds to a stationary point of the corresponding potential function. In [3], for a class of coupled systems characterized by a scalar DE recursion, this technique was used to prove that the BP threshold saturates to the conjectured MAP threshold, known as the Maxwell threshold. This result was later extended in [4] to coupled systems characterized by vector DE recursions and, more recently, to SC-LDPC codes on BMS channels in [5]. It has also been shown that potential functions belong to a wider class of Lyapunov functions [6].

Nonbinary LDPC codes designed over Galois fields of order 2^m ($GF(2^m)$), where m is the number of bits per symbol, have received a significant interest in the last few years [7], [8].

For short-to-moderate block lengths, they have been shown to outperform binary LDPC codes. Nonbinary SC-LDPC codes have been considered recently in [9] and [10]. In [10] it was shown that the MAP threshold of regular ensembles improves with m and approaches the Shannon limit, and that, contrary to regular and irregular nonbinary LDPC codes for which the BP decoding threshold worsens for high values of m, the BP threshold of nonbinary SC-LDPC codes with large termination length improves with m and tends to the Shannon limit. It was also empirically shown in [10] that threshold saturation also occurs for nonbinary SC-LDPC codes.

One of the main contributions of this paper is to prove that, indeed, threshold saturation occurs for a large number of nonbinary SC-LDPC codes on the BEC. However, the contributions of this paper go further. We first prove the existence of a fixed point in the DE of nonbinary LDPC codes. To do so, we rewrite the DE in an equivalent vector recursion form based on complementary cumulative distribution function (CCDF) vectors, for which we can prove the monotonicity of the variable node and check node updates, and thus the existence of a fixed point in the DE. This equivalent form is also suited for the application of the proof technique introduced in [3], [4], based on potential functions. However, here we use a more general definition of the potential function, since, as we will show, the potential function in the form defined in [4] does not exist for nonbinary LDPC codes. This motivated another main contribution of this paper: the analysis of the existence of the potential function for vector recursions defined by general multivariate polynomials [4], [11]. We show that the potential function exists if a solution to a system of linear equations exists. As discussed in Section V, this system of linear equations is simply a new way of representing the design constraints from the definition of the potential function in [4]. Furthermore, our result is constructive: if a solution to the system of equations exists, then the potential function can be obtained by simply solving the system of equations. Throughout the paper we give some examples to compute the potential function.

The remainder of the paper is organized as follows. In Section II, we briefly discuss DE for nonbinary regular LDPC code ensembles and we present an equivalent formulation based on CCDF vectors. We also discuss the monotonicity of the variable node and check node updates and the existence of a fixed point in the DE. The potential function for the regular nonbinary LDPC code ensemble is discussed in Section III, while in Section IV we introduce the potential function for the spatially-coupled ensemble and give a proof of the threshold saturation. Some DE results are also provided in Section IV for

several SC-LDPC code ensembles. In Section V, we discuss the existence of the potential function and its calculation, and we provide some examples. Finally, some conclusions are provided in Section VI.

A. Notation and Some Definitions

We use upper case letters F to denote scalar functions, bold lowercase letters $\boldsymbol{x}$ to denote vectors, and bold uppercase letters $\boldsymbol{X}$ for matrices. We denote by $[\boldsymbol{X}]_{i,j}$ the element in the ith row and jth column of a matrix $\boldsymbol{X}$, and by $[\boldsymbol{X}]_i$ the ith row of the matrix. Sometimes we will also use the alternative notation $x_{ij} = [\boldsymbol{X}]_{i,j}$. We assume all vectors to be row vectors, and we denote by $\mathrm{vec}(\boldsymbol{X})$ the row vector obtained by transposing the vector of stacked columns of matrix $\boldsymbol{X}$. The transpose of a matrix/vector is denoted by $[\,\cdot\,]^{\mathsf{T}}$. Let $\boldsymbol{x} \triangleq (x_1, \ldots, x_m)$ be a nonnegative vector of length m. For two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ of length m, we use the partial order $\boldsymbol{x} \preceq \boldsymbol{y}$ defined by $x_i \leq y_i$, for $i = 1, \ldots, m$.

The Jacobian of a scalar function $F(\boldsymbol{x})$ is defined as

$$F' = \frac{\partial F(\boldsymbol{x})}{\partial \boldsymbol{x}} \triangleq \left(\frac{\partial F}{\partial x_1}, \ldots, \frac{\partial F}{\partial x_m} \right).$$

Also, we define the Jacobian of a vector function $\boldsymbol{f}$ as

$$\boldsymbol{F}_{\mathrm{d}}(\boldsymbol{x}) = \boldsymbol{f}'(\boldsymbol{x}) \triangleq \begin{bmatrix} \frac{\partial f_1(\boldsymbol{x})}{\partial x_1} & \cdots & \frac{\partial f_1(\boldsymbol{x})}{\partial x_m} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m(\boldsymbol{x})}{\partial x_1} & \cdots & \frac{\partial f_m(\boldsymbol{x})}{\partial x_m} \end{bmatrix}$$

where we denote by $f_k(\,\cdot\,)$ the kth component of the vector function $\boldsymbol{f}(\,\cdot\,)$. We also define the Hessian of a vector function $\boldsymbol{f}$ as

$$\boldsymbol{F}_{\mathrm{dd}}(\boldsymbol{x}) \triangleq \boldsymbol{f}''(\boldsymbol{x}).$$

II. DENSITY EVOLUTION FOR $(d_{\mathrm{v}}, d_{\mathrm{c}}, m)$ AND $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ LDPC CODE ENSEMBLES OVER GF(2^m)

We consider transmission over the BEC with erasure probability ε, denoted as BEC(ε), using nonbinary LDPC codes from an ensemble defined over the general linear group. The code symbols are elements of the binary vector space GF(2^m), of dimension m, and we transmit on the BEC the m-tuples representing their binary images. We denote a regular nonbinary LDPC code ensemble over GF(2^m) as $(d_{\mathrm{v}}, d_{\mathrm{c}}, m)$, where d_{v} and d_{c} denote the variable node degree and the check node degree, respectively. Given a code in this ensemble, we associate to each edge of the corresponding bipartite graph a bijective linear mapping $\xi : \mathrm{GF}(2^m) \to \mathrm{GF}(2^m)$, chosen uniformly at random. The set of mappings is the general linear group GL(2^m) over the binary field, which is the set of all $m \times m$ invertible matrices whose entries take values on $\{0, 1\}$. The design rate r of a code in the ensemble does not depend on m and can be expressed as $r = 1 - \frac{d_{\mathrm{v}}}{d_{\mathrm{c}}}$. We will also consider the regular $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ SC-LDPC code ensembles, which are similar to the $(d_{\mathrm{v}}, d_{\mathrm{c}}, L, w)$ ensemble defined in [1], where L denotes the spatial dimension and w is the *smoothing* parameter. This ensemble is obtained by placing L sets of variable nodes of degree d_{v} at positions $\{1, \ldots, L\}$. A variable node at position t has d_{v} connections to check

nodes at positions in the range $\{t, t+1, \ldots, t+w-1\}$. For each connection, the position of the check node is uniformly and independently chosen from that range. A (terminated) $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ SC-LDPC code ensemble is defined by the parity-check matrix

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{H}_0(1) & & & \\ \vdots & \ddots & & \\ \boldsymbol{H}_{w-1}(1) & & \boldsymbol{H}_0(L) & \\ & \ddots & & \vdots \\ & & & \boldsymbol{H}_{w-1}(L) \end{bmatrix}.$$

Each submatrix $\boldsymbol{H}_i(t)$ is a sparse $(Md_{\mathrm{v}}/d_{\mathrm{c}}) \times M$ nonbinary matrix, where M is the number of variable nodes in each position and $Md_{\mathrm{v}}/d_{\mathrm{c}}$ is the number of check nodes in each position. It is important to note that the check node degrees corresponding to the first and last couple of positions is lower than d_{c}, i.e., the graph shows some irregularities. These irregularities lead to a locally better decoding (at the expense of a rate loss, which vanishes with L) and are the responsible for the outstanding performance of SC-LDPC codes.

In general, the messages exchanged in the BP decoding of nonbinary LDPC codes are real vectors $\boldsymbol{v} = (v_0, v_1, \ldots, v_{2^m-1})$, of length 2^m, where v_i represents the a posteriori probability that the code symbol c is c_i. For instance, for $m = 2$, there are four possible code symbols, $c_0 = 00$, $c_1 = 01$, $c_2 = 10$ and $c_3 = 11$, and the message $\boldsymbol{v} = (0.25, 0.25, 0.25, 0.25)$ means that $\Pr(c = 00) = \Pr(c = 01) = \Pr(c = 10) = \Pr(c = 11) = 0.25$. In the case of transmission over the BEC, the performance does not depend on the transmitted codeword and, without loss of generality, the transmission of the all-zero codeword can be considered [8]. Under this assumption, the messages arising in the BP decoder assume a simplified form. In particular, the nonzero entries of a message $\boldsymbol{v}$ are all equal and the message itself is equivalent to a subspace of GF(2^m). Since the nonzero elements of a message are equal, it is sufficient to keep track of the dimension of the messages [8]. We say that a message $\boldsymbol{v}$ has dimension k if it has 2^k nonzero elements. For instance, the message $\boldsymbol{v} = (0.5, 0.5, 0, 0)$ has dimension 1. If a message coming from a node has dimension k, it means that the symbol is known to be one out of 2^k possible symbols (in this example, either 00 or 01) or, equivalently, that at that node $m - k$ relations on the bits composing the symbol are known. Consider as an example the three subspaces of dimension one of GF(2^m), $S_1 = \{00, 01\}$, $S_2 = \{00, 10\}$ and $S_3 = \{00, 11\}$. Subspaces S_1 and S_2 are representative of the case where one bit has been recovered and the other is still erased, while S_3 represents the case where the two bits are erased but their sum modulo-2 is known. Therefore, the DE simplifies to the exchange of messages of length $m+1$, where the ith entry of the message is the probability that the message has dimension i. For more details the reader is referred to [8]. In the following, we define the DE for nonbinary LDPC codes over the BEC for $(d_{\mathrm{v}}, d_{\mathrm{c}}, m)$ regular ensembles and $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ coupled ensembles.

A. (d_v, d_c, m) Regular LDPC Code Ensemble over GF(2^m)

Consider the (d_v, d_c, m) ensemble over GF(2^m), used for transmission over the BEC(ε). Let $\boldsymbol{x}_\circ^{(\ell)} \triangleq (x_{\circ 0}^{(\ell)}, \ldots, x_{\circ m}^{(\ell)})$ be the probability (row) vector of length $m + 1$, where $x_{\circ i}^{(\ell)}$ is the probability that a message from variable nodes to check nodes at iteration ℓ has dimension i, $0 \leq i \leq m$. Likewise, $\boldsymbol{y}_\circ^{(\ell)} \triangleq (y_{\circ 0}^{(\ell)}, \ldots, y_{\circ m}^{(\ell)})$ is the probability vector where $y_{\circ i}^{(\ell)}$ is the probability that a message from check nodes to variable nodes at iteration ℓ has dimension i.

The variable node and check node DE updates at iteration ℓ are described by

$$\boldsymbol{x}_\circ^{(\ell)} = \boldsymbol{f}_\circ(\boldsymbol{y}_\circ^{(\ell)}; \varepsilon), \qquad \boldsymbol{y}_\circ^{(\ell)} = \boldsymbol{g}_\circ(\boldsymbol{x}_\circ^{(\ell-1)})$$

where $\boldsymbol{f}_\circ = (f_{\circ 0}, \ldots, f_{\circ m})$ and $\boldsymbol{g}_\circ = (g_{\circ 0}, \ldots, g_{\circ m})$ are, for a fixed ε, functions from $[0,1]^{m+1}$ to $[0,1]^{m+1}$, defined by

$$\boldsymbol{f}_\circ(\boldsymbol{y}_\circ; \varepsilon) \triangleq \boldsymbol{p}_\circ(\varepsilon) \boxdot \left(\boxdot^{d_v - 1} \boldsymbol{y}_\circ \right) \tag{1}$$

$$\boldsymbol{g}_\circ(\boldsymbol{x}_\circ) \triangleq \boxtimes^{d_c - 1} \boldsymbol{x}_\circ \tag{2}$$

where we define $\boxdot^{d_v - 1} \boldsymbol{a}_\circ = \boldsymbol{a}_\circ \boxdot \boldsymbol{a}_\circ \boxdot \cdots \boxdot \boldsymbol{a}_\circ$ with $d_v - 1$ terms $\boldsymbol{a}_\circ$ (i.e., $\boxdot^1 \boldsymbol{a}_\circ = \boldsymbol{a}_\circ$), and $\boxtimes^{d_c - 1} \boldsymbol{a} = \boldsymbol{a}_\circ \boxtimes \boldsymbol{a}_\circ \boxtimes \cdots \boxtimes \boldsymbol{a}_\circ$ with $d_c - 1$ terms $\boldsymbol{a}_\circ$ (i.e., $\boxtimes^1 \boldsymbol{a}_\circ = \boldsymbol{a}_\circ$). $\boldsymbol{p}_\circ$ is a row vector of length $m + 1$, the ith element of which being the probability that the channel message has dimension i,

$$\boldsymbol{p}_{\circ i}(\varepsilon) \triangleq \binom{m}{i} \varepsilon^i (1 - \varepsilon)^{m-i}, \quad i = 0, \cdots, m. \tag{3}$$

For two probability vectors $\boldsymbol{a}_\circ$ and $\boldsymbol{b}_\circ$ of length $m + 1$, the operations $\boldsymbol{a}_\circ \boxdot \boldsymbol{b}_\circ$ and $\boldsymbol{a}_\circ \boxtimes \boldsymbol{b}_\circ$ are defined as

$$[\boldsymbol{a}_\circ \boxdot \boldsymbol{b}_\circ]_k \triangleq \sum_{i=k}^{m} \sum_{j=k}^{m+k-i} V_{i,j,k}^m a_{\circ i} b_{\circ j}, \quad k = 0, \ldots, m \tag{4}$$

$$[\boldsymbol{a}_\circ \boxtimes \boldsymbol{b}_\circ]_k \triangleq \sum_{i=0}^{k} \sum_{j=k-i}^{k} C_{i,j,k}^m a_{\circ i} b_{\circ j}, \quad k = 0, \ldots, m \tag{5}$$

where $V_{i,j,k}^m$ is the probability of choosing a subspace of dimension j whose intersection with a subspace of dimension i has dimension k, and $C_{i,j,k}^m$ is the probability of choosing a subspace of dimension j whose sum with a subspace of dimension i has dimension k,

$$V_{i,j,k}^m = \frac{G_{i,k} G_{m-i,j-k} 2^{(i-k)(j-k)}}{G_{m,j}}$$

$$C_{i,j,k}^m = \frac{G_{m-i,m-k} G_{i,k-j} 2^{(k-i)(k-j)}}{G_{m,m-j}}.$$

$G_{m,k}$ is the Gaussian binomial coefficient,

$$G_{m,k} = \begin{bmatrix} m \\ k \end{bmatrix} = \begin{cases} 1, & \text{if } k = m \text{ or } k = 0 \\ \prod_{\ell=0}^{k-1} \dfrac{2^m - 2^\ell}{2^k - 2^\ell}, & \text{if } 0 < k < m \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

which gives the number of different subspaces of dimension k of GF(2^m).

In Appendix A we derive some results on the coefficients $V_{i,j,k}^m$ and $G_{m,k}$ which will be useful for the proof of Theorem 1 below.

The DE recursion can be written in compact form as

$$\boldsymbol{x}_\circ^{(\ell+1)} = \boldsymbol{f}_\circ(\boldsymbol{g}_\circ(\boldsymbol{x}_\circ^{(\ell)}); \varepsilon) \tag{7}$$

and starts from $\boldsymbol{x}_\circ^{(0)} = \boldsymbol{p}_\circ$. Note that decoding is successful when the DE converges to $\boldsymbol{x}_\circ^{(\infty)} = (1, 0, \ldots, 0)$. The DE equations (1) and (2) were first defined in [8].

In the following, we rewrite the DE recursion in (7) in a more suitable form to prove threshold saturation based on potential functions. The reason for this is that the approach in [4] requires monotone vector functions for the variable node and check node updates. It can be shown that $\boldsymbol{f}_\circ(\boldsymbol{y}_\circ; \varepsilon)$ and $\boldsymbol{g}_\circ(\boldsymbol{x}_\circ)$ are not monotone, and, therefore, cannot be used directly.

We introduce the notion of a CCDF vector.

Definition 1. *Given a probability vector* $\boldsymbol{x}_\circ = (x_{\circ 0}, x_{\circ 1}, \ldots, x_{\circ m})$ *of length* $m + 1$*, we define a CCDF vector* $\boldsymbol{x} = (x_1, \ldots, x_m)$ *of length* m *by means of the following bijective function* $\mathcal{H}$*,*

$$\boldsymbol{x}_\circ \overset{\mathcal{H}}{\to} \boldsymbol{x}: \quad x_i = \sum_{k=i}^{m} x_{\circ k}, \qquad 1 \leq i \leq m \tag{8}$$

$$\boldsymbol{x} \overset{\mathcal{H}^{-1}}{\to} \boldsymbol{x}_\circ: \quad x_{\circ i} = \begin{cases} 1 - x_1, & i = 0 \\ x_i - x_{i+1}, & 1 \leq i < m \\ x_m, & i = m. \end{cases} \tag{9}$$

By considering the CCDF vectors $\boldsymbol{x} = (x_1, \ldots, x_m)$, $\boldsymbol{y} = (y_1, \ldots, y_m)$ and $\boldsymbol{p} = (p_1, \ldots, p_m)$ and the mapping $\mathcal{H}$ above, we can define new vector functions $\boldsymbol{f}(\boldsymbol{y}; \varepsilon) = (f_1, \ldots, f_m) = \mathcal{H}(\boldsymbol{f}_\circ)$ and $\boldsymbol{g}(\boldsymbol{x}) = (g_1, \ldots, g_m) = \mathcal{H}(\boldsymbol{g}_\circ)$, with

$$f_i(\boldsymbol{y}; \varepsilon) = \sum_{k=i}^{m} f_{\circ k}(\boldsymbol{y}_\circ; \varepsilon) \tag{10}$$

and

$$g_i(\boldsymbol{x}) = \sum_{k=i}^{m} g_{\circ k}(\boldsymbol{x}_\circ).$$

Then, the variable node and check node DE updates at iteration ℓ can be written in an equivalent form as

$$\boldsymbol{x}^{(\ell)} = \boldsymbol{f}(\boldsymbol{y}^{(\ell)}; \varepsilon), \qquad \boldsymbol{y}^{(\ell)} = \boldsymbol{g}(\boldsymbol{x}^{(\ell-1)}) \tag{11}$$

and the DE recursion (7) can be rewritten as

$$\boldsymbol{x}^{(\ell+1)} = \boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x}^{(\ell)}); \varepsilon). \tag{12}$$

Theorem 1. *The functions* $\boldsymbol{f}(\boldsymbol{x}; \varepsilon)$ *and* $\boldsymbol{g}(\boldsymbol{x})$ *are increasing in* $\boldsymbol{x}$ *with respect to the partial order* $\preceq$*.*

Proof: The proof is given in Appendix B. $\square$

For later use, we denote by $\mathcal{X}$ the set of all possible values of $\boldsymbol{x}$. Likewise, we denote by $\mathcal{Y}$ and $\mathcal{E}$ the set of all possible values of $\boldsymbol{y}$ and ε, respectively. Therefore,

$$\begin{aligned} \mathcal{E}: \quad & 0 \leq \varepsilon \leq 1 \\ \mathcal{X}: \quad & 0 \leq x_i \leq 1, & 1 \leq i \leq m \\ \mathcal{Y}: \quad & 0 \leq y_i \leq 1, & 1 \leq i \leq m \end{aligned}$$

Definition 2. *Let* $\boldsymbol{x} \in \mathcal{X}$*,* $\varepsilon \in \mathcal{E}$*, and* $\boldsymbol{x}^{(0)} = \boldsymbol{x}$*. Then* $\boldsymbol{x}^\infty(\boldsymbol{x}; \varepsilon) \triangleq \lim_{\ell \to \infty} \boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x}^{(\ell)}; \varepsilon))$*.*

Corollary 1. *For regular nonbinary LDPC codes, $\boldsymbol{x}^\infty(\boldsymbol{1};\varepsilon)$ exists, i.e., the DE converges to a fixed point $\boldsymbol{x}^\infty(\boldsymbol{1};\varepsilon)$.*

Proof: Since $\boldsymbol{f}(\boldsymbol{x};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ are increasing in $\boldsymbol{x}$ with respect to the partial order $\preceq$, the DE sequence in (11) is monotonic with the number of iterations and, thus, converges to a limit. This limit is a fixed point of the recursion because the function $\boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x});\varepsilon)$ is continuous in $\boldsymbol{x}$. $\qquad\square$

Note that successful decoding corresponds to convergence of the DE equation (12) to the fixed point $\boldsymbol{x}^{(\infty)} = \boldsymbol{0} = (0, 0, \ldots, 0)$, because the CCDF of $(1, 0, \ldots, 0)$ is $(0, \ldots, 0)$.

For nonbinary codes and for some ε, the domain and range of $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ are given by $\mathcal{X}$ and $\mathcal{Y}$ respectively. Also, the vector functions $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ have several properties which will be useful for the proof of threshold saturation in Sections III and IV.

Lemma 1. *Consider $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ defined above. For $\boldsymbol{x} \in \mathcal{X}$ and $\boldsymbol{y} \in \mathcal{Y}$,*

1) *$\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ are nonnegative vectors;*
2) *$\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ is differentiable in $\boldsymbol{y}$ and $\boldsymbol{g}(\boldsymbol{x})$ is twice differentiable in $\boldsymbol{x}$;*
3) *$\boldsymbol{f}(\boldsymbol{0};\varepsilon) = \boldsymbol{f}(\boldsymbol{y};0) = \boldsymbol{g}(\boldsymbol{0}) = \boldsymbol{0}$;*
4) *$\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}) > 0$, and it is positive definite for $\boldsymbol{x} \in \mathcal{X}\backslash\{\boldsymbol{0}\}$;*
5) *$\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ is strictly increasing with ε.*

Proof: The first property follows from the fact that $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ are CCDF vectors. The second property follows from $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ being multivariate polynomials. The third property follows from $(1, 0, \ldots, 0) \boxtimes (1, 0, \ldots, 0) = (1, 0, \ldots, 0)$, $(1, 0, \ldots, 0) \boxdot \boldsymbol{x}_\circ = (1, 0, \ldots, 0)$ and $\boldsymbol{p}_\circ = (1, 0, \ldots, 0)$ for $\varepsilon = 0$. For the fourth property, due to the fact that the coefficients $C^m_{i,j,k} = 0$ for $k < i, j$, $\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x})$ is of special form. In fact, it is a lower triangular matrix, whose entries (i, j), $i \leq j$, are multivariate polynomials in $\boldsymbol{x}$ with positive coefficients. Thus, for any $\boldsymbol{x} > \boldsymbol{0}$, the lower triangular part of $\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x})$ is positive. From the positiveness of the elements of the diagonal, it follows that all eigenvalues of $\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x})$ are positive for $\boldsymbol{x} \in \mathcal{X}\backslash\{\boldsymbol{0}\}$ and, thus, $\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x})$ is positive definite[1]. Finally, to prove the fifth property we can write

$$\frac{\partial f_i}{\partial \varepsilon} = \sum_{k=1}^{m} \frac{\partial f_i}{\partial p_k} \frac{\partial p_k}{\partial \varepsilon}. \tag{13}$$

As shown in Appendix B, $\frac{\partial f_i}{\partial p_k} > 0$. The second term in each product is

$$\frac{\partial p_k}{\partial \varepsilon} = \sum_{\ell=0}^{m} \binom{m}{\ell} \varepsilon^{\ell-1}(1-\varepsilon)^{m-\ell-1}(\ell - \varepsilon m)\mathbb{1}\{\ell \geq k\} \tag{14}$$

$$= \frac{1}{(1-\varepsilon)\varepsilon} \sum_{\ell=0}^{m} \binom{m}{\ell} \varepsilon^{\ell}(1-\varepsilon)^{m-\ell}(\ell - \varepsilon m)\mathbb{1}\{\ell \geq k\}. \tag{15}$$

It is easy to verify that

$$\frac{\partial p_k}{\partial \varepsilon} > \frac{\partial p_0}{\partial \varepsilon} = 0, \qquad \forall k \geq 1 \text{ and } 0 < \varepsilon < 1. \tag{16}$$

[1] In [4], the positive definite property is needed for matching the potential threshold and the Maxwell threshold. Furthermore, a positive definite matrix is invertible, which will be used in Lemma 2.

It then follows that (13) is positive for all values of i, $i = 1, \ldots, m$, therefore $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ is increasing in ε. $\qquad\square$

B. $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ SC-LDPC Code Ensemble over GF(2^m)

Consider the $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ ensemble over GF(2^m) and transmission over the BEC(ε). In the form of (12), the DE equations for the $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ ensemble can be written as

$$\boldsymbol{x}_i = \frac{1}{w} \sum_{k=0}^{w-1} \boldsymbol{f}(\boldsymbol{y}_{i-k};\varepsilon_{i-k}), \qquad \boldsymbol{y}_i = \frac{1}{w} \sum_{k=0}^{w-1} \boldsymbol{g}(\boldsymbol{x}_{i+k})$$

where $1 \leq i < L + w$, and

$$\varepsilon_i = \begin{cases} \varepsilon, & 1 \leq i \leq L \\ 0, & 1 \leq i - L < w. \end{cases}$$

Collect the CCDF vectors $\boldsymbol{x}_i$ into the $(L + w - 1) \times m$ matrix $\boldsymbol{X} = (\boldsymbol{x}_1^\mathsf{T}, \ldots, \boldsymbol{x}_{L+w-1}^\mathsf{T})^\mathsf{T}$ and the CCDF vectors $\boldsymbol{y}_i$ into the $L \times m$ matrix $\boldsymbol{Y} = (\boldsymbol{y}_1^\mathsf{T}, \ldots, \boldsymbol{y}_L^\mathsf{T})^\mathsf{T}$. Also, let $\boldsymbol{A}$ be the $L \times (L + w - 1)$ matrix

$$\boldsymbol{A} = \frac{1}{w} \begin{pmatrix} 1 & 1 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 1 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 1 \end{pmatrix}.$$

$$\underbrace{\qquad\qquad}_{w} \underbrace{\qquad\qquad}_{L-1}$$

The fixed-point DE equation for the $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ ensemble can then be written in matrix form, similarly as in [4]

$$\boldsymbol{X} = \boldsymbol{A}^\mathsf{T} \boldsymbol{F}(\boldsymbol{A}\boldsymbol{G}(\boldsymbol{X});\varepsilon)$$

where $\boldsymbol{F}(\boldsymbol{Y};\varepsilon)$ is an $L \times m$ matrix, $\boldsymbol{F}(\boldsymbol{Y};\varepsilon) = (\boldsymbol{f}(\boldsymbol{y}_1;\varepsilon)^\mathsf{T}, \ldots, \boldsymbol{f}(\boldsymbol{y}_L;\varepsilon)^\mathsf{T})^\mathsf{T}$, and $\boldsymbol{G}(\boldsymbol{X})$ is an $(L+w-1) \times m$ matrix, $\boldsymbol{G}(\boldsymbol{X}) = (\boldsymbol{g}(\boldsymbol{x}_1)^\mathsf{T}, \ldots, \boldsymbol{g}(\boldsymbol{x}_{L+w-1})^\mathsf{T})^\mathsf{T}$.

III. POTENTIAL FUNCTION FOR THE $(d_{\mathrm{v}}, d_{\mathrm{c}}, m)$ ENSEMBLE

The DE equation (12) for the $(d_{\mathrm{v}}, d_{\mathrm{c}}, m)$ regular ensemble describes a vector system for which we can properly define a potential function, similarly to [4].

Definition 3. *The potential function $U(\boldsymbol{x};\varepsilon)$ of the system defined by functions $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ above is given by*

$$U(\boldsymbol{x};\varepsilon) \triangleq \boldsymbol{g}(\boldsymbol{x})\boldsymbol{D}\boldsymbol{x}^\mathsf{T} - G(\boldsymbol{x}) - F(\boldsymbol{g}(\boldsymbol{x});\varepsilon) \tag{17}$$

where $F : \mathcal{X} \times \mathcal{E} \mapsto \mathbb{R}$ and $G : \mathcal{Y} \times \mathcal{E} \mapsto \mathbb{R}$ are scalar functions that satisfy $F(\boldsymbol{0}) = 0$, $G(\boldsymbol{0}) = 0$, $F'(\boldsymbol{y};\varepsilon) = \boldsymbol{f}(\boldsymbol{y};\varepsilon)\boldsymbol{D}$, and $G'(\boldsymbol{x}) = \boldsymbol{g}(\boldsymbol{x})\boldsymbol{D}$, for a symmetric, invertible $m \times m$ matrix $\boldsymbol{D}$ with positive elements d_{ij}.

The definition of $U(\boldsymbol{x};\varepsilon)$ above is slightly more general than the one in [4], since $\boldsymbol{D}$ is assumed to be a positive, symmetric and invertible matrix, instead of being a diagonal matrix as in [4]. In Section V, we discuss the existence of the potential function for the general case of vector recursions defined by multivariate polynomials, and we show that, for the nonbinary codes considered here, the potential function in the form of (17), with $F'(\boldsymbol{y};\varepsilon) = \boldsymbol{f}(\boldsymbol{y};\varepsilon)\boldsymbol{D}$, and $G'(\boldsymbol{x}) = \boldsymbol{g}(\boldsymbol{x})\boldsymbol{D}$, does not exist for a diagonal matrix $\boldsymbol{D}$. The fact that we assume $\boldsymbol{D}$ in Definition 3 to be positive, symmetric and invertible is used to prove Assertion 1 and Assertion 2 in Lemma 2 below.

For a positive, symmetric and invertible matrix $\boldsymbol{D}$, it is shown in Section V-C that the potential function may exist.

Definition 4. *For $\boldsymbol{x} \in \mathcal{X}$ and $\varepsilon \in \mathcal{E}$, $\boldsymbol{x}$ is a fixed point of the DE if $\boldsymbol{x} = \boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x}); \varepsilon)$; $\boldsymbol{x}$ is a stationary point of the potential function if $U'(\boldsymbol{x}; \varepsilon) = \boldsymbol{0}$.*

Let the fixed point set be defined as

$$\mathcal{F} \triangleq \{(\boldsymbol{x}; \varepsilon) | \boldsymbol{x} = \boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x}); \varepsilon)\}.$$

Lemma 2. *For the vector system defined by $\boldsymbol{f}(\boldsymbol{y}; \varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$, the following assertions hold.*

1) *$\boldsymbol{x} \in \mathcal{X}$ is a fixed point if and only if it is a stationary point of the potential function $U(\boldsymbol{x}; \varepsilon)$;*
2) *$U(\boldsymbol{x}; \varepsilon)$ is strictly decreasing in ε, for $\boldsymbol{x} \in \mathcal{X} \backslash \boldsymbol{0}$ and $\varepsilon \in \mathcal{E}$;*
3) *$U'(\boldsymbol{x}; \varepsilon)$ is strictly decreasing in ε;*
4) *For some $\varepsilon_1 > 0$ and $\varepsilon_2 > 0$ such that $\varepsilon_1 \neq \varepsilon_2$, if $(\boldsymbol{x}_1, \varepsilon_1) \in \mathcal{F}$ and $(\boldsymbol{x}_2, \varepsilon_2) \in \mathcal{F}$, then $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$.*

  Proof:

1) $U'(\boldsymbol{x}; \varepsilon)$ is obtained as (see Appendix C)

$$U'(\boldsymbol{x}; \varepsilon) = (\boldsymbol{x} - \boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x}); \varepsilon)) \boldsymbol{D} \boldsymbol{g}'(\boldsymbol{x}). \quad (18)$$

Since $\boldsymbol{D}$ is positive, it follows $\boldsymbol{D} \boldsymbol{g}'(\boldsymbol{x}) > 0$. Furthermore, since $\boldsymbol{D}$ is invertible, $\boldsymbol{D} \boldsymbol{g}'(\boldsymbol{x})$ is also invertible. Therefore, if $\boldsymbol{x}$ is a stationary point of $U(\boldsymbol{x}; \varepsilon)$, it follows $\boldsymbol{x} - \boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x}); \varepsilon) = 0$, i.e., $\boldsymbol{x}$ is a fixed point of the DE. The converse statement is trivial.

2) $U(\boldsymbol{x}; \varepsilon)$ is given in (17). The only term depending on ε is $F(\boldsymbol{y}; \varepsilon)$. Therefore, it is sufficient to prove that $F(\boldsymbol{y}; \varepsilon)$ is increasing in ε. $F(\boldsymbol{y}; \varepsilon)$ is the line integral of $\boldsymbol{f}(\boldsymbol{y}; \varepsilon) \boldsymbol{D}$,

$$F(\boldsymbol{y}; \varepsilon) = \int_{\boldsymbol{0}}^{\boldsymbol{y}} \boldsymbol{f}(\boldsymbol{z}; \varepsilon) \boldsymbol{D} d\boldsymbol{z}.$$

Since the integrand is an increasing function of ε (which follows from the fact that $\boldsymbol{f}(\boldsymbol{y}; \varepsilon)$ is increasing in ε (see Lemma 1) and $\boldsymbol{D}$ is a positive matrix), then the line integral is also an increasing function of ε.

3) $U'(\boldsymbol{x}; \varepsilon)$ is given in (18). Note that the only term that depends on ε is $\boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x}); \varepsilon)$, therefore it is sufficient to show that $\boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x}); \varepsilon)$ is increasing in ε. This was already proven in Lemma 1.

4) The fourth assertion is true because $(\boldsymbol{x} - \boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x}); \varepsilon))$ is strictly decreasing in ε.

$\square$

We can now define the BP and the potential thresholds, denoted respectively by $\varepsilon^{\mathrm{BP}}$ and ε^*.

Definition 5. *The BP threshold is*

$$\varepsilon^{\mathrm{BP}} \triangleq \sup \{\varepsilon \in \mathcal{E} | \boldsymbol{x}^{\infty}(\boldsymbol{1}; \varepsilon) = \boldsymbol{0}\}.$$

In order to define the potential threshold ε^*, let us define the *energy gap* $\Delta E(\varepsilon)$ with the help of the following definition of the basin of attraction of the fixed point $\boldsymbol{x}^{(\infty)} = \boldsymbol{0}$ (successful decoding) [4]:

Definition 6. *The basin of attraction for $\boldsymbol{x}^{(\infty)} = \boldsymbol{0}$ is*

$$\mathcal{U}_{\boldsymbol{0}}(\varepsilon) \triangleq \{\boldsymbol{x} \in \mathcal{X} | \boldsymbol{x}^{\infty}(\boldsymbol{x}; \varepsilon) = \boldsymbol{0}\}.$$

Definition 7. *The energy gap $\Delta E(\varepsilon)$ for some ε, $\varepsilon^{\mathrm{BP}} \leq \varepsilon \leq \varepsilon^*$, is defined as*

$$\Delta E(\varepsilon) \triangleq \inf_{\boldsymbol{x} \in \mathcal{X} \backslash \mathcal{U}_{\boldsymbol{0}}(\varepsilon)} U(\boldsymbol{x}; \varepsilon).$$

We are ready to define ε^*.

Definition 8. *The potential threshold is*

$$\varepsilon^* \triangleq \sup \left\{\varepsilon \in (\varepsilon^{\mathrm{BP}}, 1] \mid \Delta E(\varepsilon) > 0, \ \forall \boldsymbol{x} \in \mathcal{X} \right\}.$$

Remark 1. *The definition of ε^* is similar to the one given in [11]. It is equivalent to the definition given in [4] if $U(\boldsymbol{x}; \varepsilon)$ is positive for $\varepsilon \in (\varepsilon^{\mathrm{BP}}, \varepsilon^*)$ and $\Delta E(\varepsilon^*) = 0$.*

Remark 2. *It has been shown for several systems in [3], [11], [12], that the MAP threshold $\varepsilon^{\mathrm{MAP}}$ and the potential threshold ε^* are identical. The idea to prove this result is given in [12]. It implies the calculation of the trial entropy $P(x)$, a quantity related to the BP EXIT function $h^{\mathrm{BP}}(\varepsilon)$, which was first defined in [13]. Unfortunately, this approach cannot be applied to nonbinary LDPC codes, since the general expression of $h^{\mathrm{BP}}(\varepsilon)$ for an arbitrary value of m is not yet known. In this paper, we do not address the question of the equality between $\varepsilon^{\mathrm{MAP}}$ and ε^* for nonbinary LDPC codes.*

IV. POTENTIAL FUNCTION FOR THE SPATIALLY-COUPLED SYSTEM AND A PROOF OF THRESHOLD SATURATION

Definition 9. *The potential function $U(\boldsymbol{X}; \varepsilon)$ for the spatially-coupled case is defined similarly as in [4]*

$$U(\boldsymbol{X}; \varepsilon) \triangleq \mathrm{Tr}(\boldsymbol{G}(\boldsymbol{X}) \boldsymbol{D} \boldsymbol{X}^{\mathsf{T}}) - G(\boldsymbol{X}) - F(\boldsymbol{A}\boldsymbol{G}(\boldsymbol{X}); \varepsilon) \quad (19)$$

where $G'(\boldsymbol{X}) = \sum_{i=1}^{L+w-1} G'(\boldsymbol{x}_i) = \sum_{i=1}^{L+w-1} \boldsymbol{g}(\boldsymbol{x}_i) \boldsymbol{D}$, and $F'(\boldsymbol{X}) = \sum_{i=1}^{L} F'(\boldsymbol{x}_i) = \sum_{i=1}^{L} \boldsymbol{f}(\boldsymbol{x}_i) \boldsymbol{D}$.

To prove threshold saturation, we will need the partial derivative of $U(\boldsymbol{X}; \varepsilon)$. It is given in the following theorem.

Theorem 2. *The partial derivative of $U(\boldsymbol{X}; \varepsilon)$ is*

$$U'(\boldsymbol{X}; \varepsilon) \triangleq \begin{bmatrix} \frac{\partial}{\partial \boldsymbol{x}_1} U(\boldsymbol{X}; \varepsilon) \\ \vdots \\ \frac{\partial}{\partial \boldsymbol{x}_L} U(\boldsymbol{X}; \varepsilon) \end{bmatrix}$$

where the ith row of $U'(\boldsymbol{X}; \varepsilon)$ is

$$[U'(\boldsymbol{X}; \varepsilon)]_i = \left(\boldsymbol{x}_i - [\boldsymbol{A}^{\mathsf{T}}]_i \boldsymbol{F}(\boldsymbol{A}\boldsymbol{G}(\boldsymbol{X}); \varepsilon)\right) \boldsymbol{D} \boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}_i).$$

Proof: The proof of the theorem is given in Appendix D.

$\square$

We also need the following property of $U''(\boldsymbol{X}; \varepsilon)$.

Lemma 3. *The norm of the second derivative of $U(\boldsymbol{X}; \varepsilon)$ is upper bounded by*

$$||U''(\boldsymbol{X}; \varepsilon)||_{\infty} \leq ||\boldsymbol{D}||_{\infty}(\alpha + \beta + \alpha^2 \gamma) = K$$

where $\alpha = \sup_{\boldsymbol{x} \in \mathcal{X}} ||\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x})||_{\infty}$, $\beta = \sup_{\boldsymbol{x} \in \mathcal{X}} ||\boldsymbol{G}_{\mathrm{dd}}(\boldsymbol{x})||_{\infty}$, and $\gamma = \sup_{\boldsymbol{y} \in \mathcal{Y}} ||\boldsymbol{F}_{\mathrm{d}}(\boldsymbol{y}; \varepsilon)||_{\infty}$.

Proof: The proof of the lemma is similar to the one given in [4, Lemma 8].

$\square$

The following theorem proves successful decoding for $\varepsilon < \varepsilon^*$, i.e., the BP decoder saturates to the potential threshold for large enough values of w.

TABLE I: DE thresholds for nonbinary SC-LDPC codes

Ensemble	Rate	$\varepsilon_{\mathrm{BP}}^1$	$\varepsilon_{\mathrm{BP}}^3$	$\varepsilon_{\mathrm{BP}}^5$	$\varepsilon_{\mathrm{BP}}^8$	$\varepsilon_{\mathrm{MAP}}$	δ_{Sh}
$(3,6)$	$1/2$	0.4880	0.4978	0.4995	0.4998	0.4999	0.0002
$(3,9)$	$2/3$	0.3196	0.3307	0.3328	0.3331	0.3332	0.0002
$(3,12)$	$3/4$	0.2372	0.2476	0.2495	0.2497	0.2499	0.0003
$(3,15)$	$4/5$	0.1886	0.1978	0.1995	0.1996	0.1999	0.0004

Theorem 3. *Given the spatially coupled $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ LDPC code ensemble, for $\varepsilon < \varepsilon^*$ and $w > \frac{mK}{2\Delta E(\varepsilon)}$, the only fixed point of the system is $\boldsymbol{x}^\infty = \boldsymbol{0}$.*

Proof: The proof of the theorem follows the same lines as the proof in [11] and [12] and is omitted for brevity. □

A. Numerical Results

In Table I we give the BP threshold of nonbinary SC-LDPC code ensembles with $d_{\mathrm{v}} = 3$ for several code rates and $m = 1, 3, 5$ and 8, denoted by $\varepsilon_{\mathrm{BP}}^1$, $\varepsilon_{\mathrm{BP}}^3$, $\varepsilon_{\mathrm{BP}}^5$, and $\varepsilon_{\mathrm{BP}}^8$, respectively, for $L \to \infty$. In particular, we consider the $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L)$ coupled ensemble defined in [1], properly extended to the nonbinary case. We observe that, for a given rate, the BP threshold improves with increasing values of m. A significant improvement is observed from $m = 1$ (binary) to $m = 3$. It is interesting to note that $\varepsilon_{\mathrm{BP}}$ approaches the Shannon limit as m increases (the last column of the table gives the gap to the Shannon limit for the coupled ensembles with $m = 8$, δ_{Sh}). We have observed that the BP threshold tends to the MAP threshold $\varepsilon_{\mathrm{MAP}}$ for large L for all values of m, suggesting that threshold saturation to the MAP threshold occurs. As an example, we report in the table the MAP threshold for $m = 8$.

V. EXISTENCE OF THE POTENTIAL FUNCTION: CALCULATION OF $F(\boldsymbol{y}; \varepsilon)$ AND $G(\boldsymbol{x})$, AND PROPERTIES OF $\boldsymbol{D}$

In this section, we discuss the existence of the potential function in the form of (17) and its calculation. The existence of $U(\boldsymbol{x}; \epsilon)$ in (17) depends crucially on the existence of the functions $F(\boldsymbol{y}; \epsilon)$ and $G(\boldsymbol{x})$ that satisfy

$$F'(\boldsymbol{y}; \varepsilon) = \boldsymbol{f}(\boldsymbol{y}; \varepsilon)\boldsymbol{D}, \qquad G'(\boldsymbol{x}) = \boldsymbol{g}(\boldsymbol{x})\boldsymbol{D}. \qquad (20)$$

We first discuss (Section V-A below) the calculation of $F(\boldsymbol{y}; \varepsilon)$ and $G(\boldsymbol{x})$ in the general case where $\boldsymbol{f}(\boldsymbol{y}; \varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ are defined by multivariate polynomials [4], [11], without making any assumption on the form of matrix $\boldsymbol{D}$. The discussion encompasses any class of sparse-graph codes (coupled or not) used for transmission over the BEC. In particular, we show that the potential function exists if there exists a solution to a carefully defined system of linear equations. In this case, $F(\boldsymbol{y}; \varepsilon)$ and $G(\boldsymbol{x})$ can be obtained by solving the system of linear equations. We then consider in Section V-B the choice of $\boldsymbol{D}$ so that a solution to the system of linear equations exists. The particular case of nonbinary $(d_{\mathrm{v}}, d_{\mathrm{c}}, m)$ and $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ LDPC ensembles is considered in Section V-C.

A. Calculation of $F(\boldsymbol{y}; \varepsilon)$ and $G(\boldsymbol{x})$ from $\boldsymbol{f}(\boldsymbol{y}; \varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$

The problem of calculating $F(\boldsymbol{y}; \varepsilon)$ and $G(\boldsymbol{x})$ corresponds to the problem of reconstructing two multivariate polynomial functions from their multivariate polynomial gradient vector functions $\boldsymbol{f}(\boldsymbol{y}; \varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$. The main result of this section (Theorem 4) is that this reconstruction problem is equivalent to the relatively simple problem of solving a system of linear equations. It is important to note that, indeed, (20) leads to a system of linear equations. Therefore, to determine the existence of $F(\boldsymbol{y}; \varepsilon)$ and $G(\boldsymbol{x})$ one needs to determine whether a solution of this system exists or not.

First, note that (20) can be equivalently written as

$$\frac{\partial F}{\partial y_i}(\boldsymbol{y}; \varepsilon) = \sum_{j=1}^m d_{ji} f_j(\boldsymbol{y}, \varepsilon) \qquad (21)$$

$$\frac{\partial G}{\partial x_i}(\boldsymbol{x}) = \sum_{j=1}^m d_{ji} g_j(\boldsymbol{x}) \qquad (22)$$

for $i = 1, \ldots, m$.

In what follows, we will make use of the following definition.

Definition 10. *Let $\mathcal{S}_j^f$ and $\mathcal{S}_j^g$, $j = 1 \ldots, m$, be the set of nonzero coefficients of the multivariate polynomial functions $f_j(\boldsymbol{y}; \varepsilon)$ and $g_j(\boldsymbol{x})$, respectively, defined as*

$$\mathcal{S}_j^f \triangleq \left\{ (i_1, \ldots, i_m) : \mathrm{coeff}\left(f_j(\boldsymbol{y}), \prod_{k=1}^m y_k^{i_k} \right) \neq 0 \right\} \qquad (23)$$

$$\mathcal{S}_j^g \triangleq \left\{ (i_1, \ldots, i_m) : \mathrm{coeff}\left(g_j(\boldsymbol{x}), \prod_{k=1}^m x_k^{i_k} \right) \neq 0 \right\}. \qquad (24)$$

Let also $\mathcal{S}^f = \cup_j \mathcal{S}_j^f$ and $\mathcal{S}^g = \cup_j \mathcal{S}_j^g$.

Now, in order that (21)–(22) hold, the sets of coefficients of the monomials in the left and right hand side of (21)–(22) must be the same. We define in the following the sets of coefficients which are related to the left hand side of (21)–(22).

Definition 11. *Let $\mathcal{S}_{j,k}^F$ and $\mathcal{S}_{j,k}^G$ be the sets defined by (25) and (26) respectively. Then, the sets of non-zero coefficients of the functions $F(\boldsymbol{y}; \varepsilon)$ and $G(\boldsymbol{x})$, denoted by $\mathcal{S}^F$ and $\mathcal{S}^G$, respectively, are*

$$\mathcal{S}^F \triangleq \bigcup_{s=1}^m \bigcup_{(j,s) \in \mathcal{S}_s^D} \mathcal{S}_{j,s}^F, \qquad \mathcal{S}^G \triangleq \bigcup_{s=1}^m \bigcup_{(j,s) \in \mathcal{S}_s^D} \mathcal{S}_{j,s}^G \quad (27)$$

where

$$\mathcal{S}_s^D \triangleq \{ (j, s) : d_{js} \neq 0, \ 1 \leq j \leq m \} \qquad (28)$$

for any $1 \leq s \leq m$.

Remark 3. *For any $j = 1, \ldots, m$ and $k = 1, \ldots, m$, the sets $\mathcal{S}_{j,k}^F$ and $\mathcal{S}_{j,k}^G$ can be equivalently defined as*

$$\mathcal{S}_{j,k}^F \triangleq \left(\mathcal{S}_j^f + \boldsymbol{e}_k \right)$$

$$\mathcal{S}_{j,k}^G \triangleq \left(\mathcal{S}_j^g + \boldsymbol{e}_k \right)$$

where $\boldsymbol{e}_k$ is the standard basis vector of length m with a one in the kth position and zero elsewhere, and the summation of a set $\mathcal{S}$ with a vector $\boldsymbol{e}_k$ is performed element-by-element.

$$\mathcal{S}_{j,k}^F \triangleq \left\{ (i_1,\ldots,i_m) : \text{coeff}\left(\int_0^{y_k} f_j(y_1,\ldots,y_{k-1},z,y_{k+1},\ldots y_m)dz, \prod_{l=1}^m y_l^{i_l} \right) \neq 0 \right\}, \quad \text{for } j,k=1,\ldots,m \tag{25}$$

$$\mathcal{S}_{j,k}^G \triangleq \left\{ (i_1,\ldots,i_m) : \text{coeff}\left(\int_0^{x_k} g_j(x_1,\ldots,x_{k-1},z,x_{k+1},\ldots x_m)dz, \prod_{l=1}^m x_l^{i_l} \right) \neq 0 \right\}, \quad \text{for } j,k=1,\ldots,m \tag{26}$$

Given the expressions from Remark 3, it is easy to verify that $|\mathcal{S}_{j,k}^F| \leq |\mathcal{S}_j^f| + 1$ and $|\mathcal{S}_{j,k}^G| \leq |\mathcal{S}_j^g| + 1$.

Lemma 4. *For any coefficients d_{ij},*

$$\mathcal{S}^F \subseteq \bigcup_{j,k=1}^m \mathcal{S}_{j,k}^F, \qquad \mathcal{S}^G \subseteq \bigcup_{j,k=1}^m \mathcal{S}_{j,k}^G. \tag{29}$$

Moreover,
- *$\mathcal{S}^F = \bigcup_{j,k=1}^m \mathcal{S}_{j,k}^F$ and $\mathcal{S}^G = \bigcup_{j,k=1}^m \mathcal{S}_{j,k}^G$ if $d_{ij} \neq 0$ for all i,j (i.e., if $\boldsymbol{D}$ does not have zero entries);*
- *$\mathcal{S}^F = \bigcup_{j=1}^m \mathcal{S}_{j,j}^F$ and $\mathcal{S}^G = \bigcup_{j=1}^m \mathcal{S}_{j,j}^G$ if $d_{ij} \neq 0$ for $i = j$ and 0 otherwise (i.e., if $\boldsymbol{D}$ is diagonal).*

Proof: The proof follows from direct calculation and is therefore omitted. □

We now address the existence of the potential function for the general case of a sparse-graph ensemble over the BEC defined by a vector recursion with multivariate polynomial functions $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$, without imposing any constraint on the matrix $\boldsymbol{D}$. The special form of $\boldsymbol{D}$ is discussed in Section V-B. We can state the following theorem.

Theorem 4. *Consider a sparse-graph code ensemble, used for transmission over the BEC, whose density evolution updates $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ satisfy Lemma 1. Let the corresponding potential function be*

$$U(\boldsymbol{x};\varepsilon) \triangleq \boldsymbol{g}(\boldsymbol{x})\boldsymbol{D}\boldsymbol{x}^\mathsf{T} - G(\boldsymbol{x}) - F(\boldsymbol{g}(\boldsymbol{x});\varepsilon)$$

with functions $F(\boldsymbol{y};\varepsilon)$ and $G(\boldsymbol{x})$ satisfying $F'(\boldsymbol{y};\varepsilon) = \boldsymbol{f}(\boldsymbol{y};\varepsilon)\boldsymbol{D}$, $G'(\boldsymbol{x}) = \boldsymbol{g}(\boldsymbol{x})\boldsymbol{D}$, $F(\boldsymbol{0}) = 0$ and $G(\boldsymbol{0}) = 0$, for some $m \times m$ matrix $\boldsymbol{D}$. Then, for any value of ε, $F(\boldsymbol{y};\varepsilon)$ and $G(\boldsymbol{x})$ exist (hence $U(\boldsymbol{x};\varepsilon)$ exists) if there exist sets of values $\{d_{js}\}$, $\{\varphi_{(i_1,\ldots,i_m)}\}$ and $\{\mu_{(k_1,\ldots k_m)}\}$ that satisfy the following system of linear equations,

$$\begin{cases} i_s\varphi_{(i_1,\ldots,i_s,\ldots,i_m)} = \sum_{j=1}^m d_{js}\phi_{(i_1,\ldots i_s-1,\ldots,i_m)}^{(j)} \\ k_t\mu_{(k_1,\ldots,k_t,\ldots,k_m)} = \sum_{j=1}^m d_{jt}\gamma_{(k_1,\ldots,k_t-1,\ldots k_m)}^{(j)} \end{cases} \tag{30}$$

for all possible m-tuples $(i_1,\ldots,i_m)$ and $(k_1,\ldots,k_m)$, and all values of i_s and k_t for $1 \leq s \leq m$ and $1 \leq t \leq m$. The coefficients ϕ and γ in (30) are given by

$$\phi_{(i_1,\ldots,i_m)}^{(j)} = \text{coeff}(f_j(\boldsymbol{y};\varepsilon), y_1^{i_1}\cdots y_m^{i_m}) \tag{31}$$

$$\gamma_{(k_1,\ldots k_m)}^{(j)} = \text{coeff}(g_j(\boldsymbol{x}), x_1^{i_1}\cdots x_m^{i_m}). \tag{32}$$

Proof: Functions $F(\boldsymbol{y};\varepsilon)$ and $G(\boldsymbol{x})$ are multivariate polynomials, which can be written as

$$F(\boldsymbol{y};\varepsilon) = \sum_{(i_1,\ldots,i_m)\in\mathcal{S}^F} \varphi_{(i_1,\ldots,i_m)}y_1^{i_1}\cdots y_m^{i_m} \tag{33}$$

$$G(\boldsymbol{x}) = \sum_{(k_1,\ldots,k_m)\in\mathcal{S}^G} \mu_{(k_1,\ldots,k_m)}x_1^{k_1}\cdots x_m^{k_m} \tag{34}$$

where $\mathcal{S}^F$ and $\mathcal{S}^G$ are the coefficient sets given in Definition 11 and Lemma 4.

We can also write $f_j(\boldsymbol{y},\varepsilon)$ and $g_j(\boldsymbol{x})$ in polynomial form as

$$f_j(\boldsymbol{y},\varepsilon) = \sum_{(i_1,\ldots,i_m)\in\mathcal{S}_j^f} \phi_{(i_1,\ldots,i_m)}^{(j)}y_1^{i_1}\cdots y_m^{i_m} \tag{35}$$

$$g_j(\boldsymbol{x}) = \sum_{(k_1,\ldots,k_m)\in\mathcal{S}_j^g} \gamma_{(k_1,\ldots,k_m)}^{(j)}x_1^{k_1}\cdots x_m^{k_m} \tag{36}$$

where $\mathcal{S}_j^f$ and $\mathcal{S}_j^g$ are the coefficient sets given in (23)–(24). Now, using (33)–(34) and (35)–(36) in (21)–(22), we obtain the relationship between ϕ's, γ's, d's, φ's and μ's, given by (30). □

It is important to note that, given the coefficients ϕ and γ (which are fixed and known), (30) is a fixed homogenous linear system with respect to a single vector containing all the d_{ij} coefficients, all the φ coefficients, and all the μ coefficients. We remark that (30) is a structured system of equations, so the existence of a solution does not follow from dimensional arguments: even though there might exist more equations than free variables d_{ij}, φ and μ, a solution might still exist as some of the equations in (30) are usually linearly dependent. Moreover, to show the existence of a solution for (30), one should rather consider the matching of the sets $\mathcal{S}^F$ and $\mathcal{S}^G$ with the sets $\mathcal{S}_{j,k}^F$ and $\mathcal{S}_{j,k}^G$. As this matching happens by means of the sets $\mathcal{S}_s^D$ (i.e., using nonzero coefficients in the matrix $\boldsymbol{D}$), the existence of the solution depends on the form of $\boldsymbol{D}$. The existence of a solution of (30) for various forms of $\boldsymbol{D}$ is addressed in the next section.

Furthermore, note that, by definition, the coefficients ϕ depend on ε. Therefore, the coefficients φ will also be functions of ε. We also remark that if we consider $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ defined by spatially-coupling a single-system DE, the discussion above also applies. The main difference is that the dimension of the system of equations will be larger.

B. Necessary Condition on the Existence of $U(\boldsymbol{X};\varepsilon)$

In Theorem 5 below, we give a necessary condition for the existence of the potential function for any matrix $\boldsymbol{D}$. We then consider the condition for a diagonal matrix $\boldsymbol{D}$ and for a matrix $\boldsymbol{D}$ with strictly positive entries. We will make use of the following definition.

Definition 12. *For a set $\mathcal{S}$ of vectors of length m and a vector $\boldsymbol{e}_k$, let the subtraction operation $\mathcal{S} - \boldsymbol{e}_k$ be defined as*

$$\mathcal{S} - \boldsymbol{e}_k = \{(i_1,\ldots,i_k,\ldots,i_m) : \\ (i_1,\ldots,i_k-1,\ldots,i_m) \in \mathcal{S} \text{ and } i_k > 0\}.$$

Theorem 5. *If the system of equations (30) exists then, for all $s = 1, \ldots, m$ and $j = 1, \ldots, m$, it holds that*

$$\left(\bigcup_{(i,s)\in\mathcal{S}_s^D} \mathcal{S}_{i,s}^F - \boldsymbol{e}_j \right) \subseteq \left(\bigcup_{(j,s')\in\mathcal{S}^D} \mathcal{S}_j^f \right) \qquad (37)$$

and

$$\left(\bigcup_{(i,s)\in\mathcal{S}_s^D} \mathcal{S}_{i,s}^G - \boldsymbol{e}_j \right) \subseteq \left(\bigcup_{(j,s')\in\mathcal{S}^D} \mathcal{S}_j^g \right) \qquad (38)$$

where $\mathcal{S}^D = \bigcup_{k=1}^m \mathcal{S}_k^D$. Equivalently, (37)–(38) can be written as

$$\left(\bigcup_{(i,s)\in\mathcal{S}_s^D} \left(\mathcal{S}_i^f + \boldsymbol{e}_s \right) - \boldsymbol{e}_j \right) \subseteq \left(\bigcup_{(j,s')\in\mathcal{S}^D} \mathcal{S}_j^f \right) \qquad (39)$$

and

$$\left(\bigcup_{(i,s)\in\mathcal{S}_s^D} (\mathcal{S}_i^g + \boldsymbol{e}_s) - \boldsymbol{e}_j \right) \subseteq \left(\bigcup_{(j,s')\in\mathcal{S}^D} \mathcal{S}_j^g \right). \qquad (40)$$

Proof: Consider the sets $\mathcal{S}_{i,s}^G$. Assume that there exist an element $\boldsymbol{a} = (i_1, \ldots, i_s+1, \ldots, i_j-1, \ldots, i_m)$ such that $\boldsymbol{a} \in \left(\bigcup_{(i,s)\in\mathcal{S}_s^D} (\mathcal{S}_i^g + \boldsymbol{e}_s) - \boldsymbol{e}_j \right)$ but $\boldsymbol{a} \notin \left(\bigcup_{(j,s')\in\mathcal{S}^D} \mathcal{S}_j^g \right)$. Since $\boldsymbol{a} \in \left(\bigcup_{(i,s)\in\mathcal{S}_s^D} (\mathcal{S}_i^g + \boldsymbol{e}_s) - \boldsymbol{e}_j \right)$, then $\tilde{\boldsymbol{a}} = \boldsymbol{a} + \boldsymbol{e}_j \in \mathcal{S}^G$. We get $\tilde{\boldsymbol{a}} = (i_1, \ldots, i_s+1, \ldots, i_j, \ldots, i_m)$, i.e., the monomial $x_1^{i_1} \cdots x_i^{i_s+1} \cdots x_j^{i_j} \cdots x_m^{i_m}$ appears in $G(\boldsymbol{x})$. But now $\frac{\partial G(\boldsymbol{x})}{\partial x_j}$ contains the monomial $x_1^{i_1} \cdots x_i^{i_s+1} \cdots x_j^{i_j-1} \cdots x_m^{i_m}$, which is a contradiction, since by assumption

$$(i_1, \ldots, i_s+1, \ldots, i_j-1, \ldots, i_m) \notin \left(\cup_{(j,s')\in\mathcal{S}^D} \mathcal{S}_j^g \right).$$

The same reasoning holds for the sets $\mathcal{S}_{i,s}^F$. $\qquad\square$

Corollary 2. *For a diagonal $\boldsymbol{D}$, the condition is*

$$\left(\mathcal{S}_i^f + \boldsymbol{e}_i \right) - \boldsymbol{e}_j \in \mathcal{S}_j^f \quad \text{and} \quad (\mathcal{S}_i^g + \boldsymbol{e}_s) - \boldsymbol{e}_j \in \mathcal{S}_j^g \quad (41)$$

for $1 \le i \le m$, $1 \le j \le m$.

Corollary 3. *For a strictly positive $\boldsymbol{D}$, the conditions are*

$$\left(\bigcup_{s=1}^m \left(\mathcal{S}_i^f + \boldsymbol{e}_s \right) - \boldsymbol{e}_j \right) \in \cup_{j=1}^m \mathcal{S}_j^f \qquad (42)$$

$$\left(\bigcup_{s=1}^m (\mathcal{S}_i^g + \boldsymbol{e}_s) - \boldsymbol{e}_j \right) \in \cup_{j=1}^m \mathcal{S}_j^g \qquad (43)$$

for $1 \le i \le m$, $1 \le j \le m$.

In the following, we give an example where the necessary condition for a diagonal matrix $\boldsymbol{D}$ is satisfied and we compute the potential function by solving the system of linear equations (30).

Example 1 (Bilayer LDPC code for the relay channel [14])**.** *We compute the potential function for a regular bilayer LDPC code with parameters $(\ell_1, \ell_2, r_1, r_2)$ for transmission over the binary erasure relay channel with equal erasure probabilities ε. ℓ_1 and ℓ_2 are the variable node degrees for the first and*

second layer, respectively. r_1 and r_2 are the check node degrees for the first and second layer. The extension to irregular codes is straightforward. The DE for the bilayer code is given by

$$\begin{cases} x_1 = \varepsilon y_1^{\ell_1-1} y_2^{\ell_2}, & y_1 = 1 - (1-x_1)^{r_1-1}, \quad \textit{(first layer)} \\ x_2 = \varepsilon y_1^{\ell_1} y_2^{\ell_2-1}, & y_2 = 1 - (1-x_2)^{r_2-1}, \quad \textit{(second layer)} \end{cases} \tag{44}$$

where x_1 is the erasure probability of messages from variable nodes to check nodes in the first layer, and y_1 is the erasure probability of messages from check nodes in the first layer to variable nodes. Likewise, x_2 is the erasure probability of messages from variable nodes to check nodes in the second layer, and y_2 is the erasure probability of messages from check nodes in the second layer to variable nodes.

We write the corresponding vector functions

$$\boldsymbol{f}(\boldsymbol{y}; \varepsilon) = (f_1, f_2) = (\varepsilon y_1^{\ell_1-1} y_2^{\ell_2}, \varepsilon y_1^{\ell_1} y_2^{\ell_2-1}) \tag{45}$$

$$\boldsymbol{g}(\boldsymbol{x}) = (g_1, g_2) = (1 - (1-x_1)^{r_1-1}, 1 - (1-x_2)^{r_2-1}) \tag{46}$$

and obtain the following coefficient sets,

$$\mathcal{S}_1^f = \{(\ell_1-1, \ell_2)\}, \quad \mathcal{S}_1^g = \{(0,0), (1,0), \ldots, (r_1-1, 0)\},$$
$$\mathcal{S}_2^f = \{(\ell_1, \ell_2-1)\}, \quad \mathcal{S}_2^g = \{(0,0), (0,1), \ldots, (0, r_2-1)\}.$$

It is easy to verify that the necessary condition in Corollary 2 holds.

Assume a diagonal matrix $\boldsymbol{D} = \begin{bmatrix} d_{11} & 0 \\ 0 & d_{22} \end{bmatrix}$. We obtain

$$\mathcal{S}^F \triangleq \bigcup_{j=1}^m \mathcal{S}_{j,j}^F = \bigcup_{j=1}^2 \left(\mathcal{S}_j^f + \boldsymbol{e}_j \right) = \{(\ell_1, \ell_2)\}$$

$$\mathcal{S}^G \triangleq \bigcup_{j=1}^m \mathcal{S}_{j,j}^G = \bigcup_{j=1}^2 \left(\mathcal{S}_j^g + \boldsymbol{e}_j \right)$$
$$= \{(1,0), \ldots, (r_1, 0), (0,1), \ldots, (0, r_2)\}.$$

To derive $F(\boldsymbol{y}; \varepsilon)$, $G(\boldsymbol{x})$, and $\boldsymbol{D}$, we first write the system of linear equations, as explained above, as

$$\begin{cases} \ell_1 \varphi_{(\ell_1, \ell_2)} & = d_{11} \phi_{(\ell_1-1, \ell_2)}^{(1)} \\ \ell_2 \varphi_{(\ell_1, \ell_2)} & = d_{22} \phi_{(\ell_1, \ell_2-1)}^{(2)} \\ i \mu_{(i,0)} & = d_{11} \gamma_{(i-1, 0)}^{(1)} \\ i \mu_{(0,i)} & = d_{22} \gamma_{(0, i-1)}^{(2)} \end{cases} \tag{47}$$

for $i = 1, \ldots, r_1$.

From (45)-(46), and using the binomial formula to expand $(1-x)^a$, we obtain the coefficients

$$\phi_{(\ell_1-1, \ell_2)}^{(1)} = \varepsilon, \quad \phi_{(\ell_1, \ell_2-1)}^{(2)} = \varepsilon$$

$$\gamma_{(0,0)}^{(1)} = 0, \quad \gamma_{(i,0)}^{(1)} = -\binom{r_1-1}{i}(-1)^i$$

$$\gamma_{(0,1)}^{(2)} = 0, \quad \gamma_{(0,i)}^{(2)} = -\binom{r_2-1}{i}(-1)^i.$$

Using these coefficients in (47) and solving the system of linear equations, we obtain[2] $d_{11} = \ell_1$, $d_{22} = \ell_2$, $\varphi_{(\ell_1,\ell_2)} = \varepsilon$, $\mu_{(1,0)} = \mu_{(0,1)} = 0$, *and, for* $2 \le i < r$,

$$\mu_{(i,0)} = -\frac{d_{11}}{i}\binom{r_1 - 1}{i - 1}(-1)^{i-1}$$

$$\mu_{(0,i)} = -\frac{d_{22}}{i}\binom{r_1 - 1}{i - 1}(-1)^{i-1}.$$

Finally, the functions $F(\boldsymbol{y}; \varepsilon)$ *and* $G(\boldsymbol{x})$ *are found as (see (33) and (34))*

$$F(\boldsymbol{y}; \varepsilon) = \sum_{(i_1,i_2) \in \mathcal{S}^F} \varphi_{(i_1,i_2)} y_1^{i_1} y_2^{i_2} = \varphi_{(\ell_1,\ell_2)} y_1^{\ell_1} y_2^{\ell_2} = \varepsilon y_1^{\ell_1} y_2^{\ell_2}$$

and

$$G(\boldsymbol{x}) = \sum_{(k_1,k_2) \in \mathcal{S}^G} \mu_{(k_1,k_2)} x_1^{k_1} x_2^{k_2}$$

$$= \sum_{i=1}^{r_1} \mu_{(i,0)} x_1^i + \sum_{i=1}^{r_2} \mu_{(0,i)} x_2^i. \tag{48}$$

The first summation term in right hand side of (48) becomes

$$\sum_{i=1}^{r_1} \mu_{(i,0)} x_1^i = \mu_{(1,0)} - \sum_{i=2}^{r_1} \frac{d_{11}}{i}\binom{r_1 - 1}{i - 1}(-1)^{i-1} x_1^i$$

$$= \frac{d_{11}}{r_1} \sum_{i=2}^{r_1} \binom{r_1}{i}(-1)^i x_1^i$$

$$= \frac{d_{11}}{r_1}\left(-1 + r_1 x_1 + \sum_{i=0}^{r_1}\binom{r_1}{i}(-1)^i x_1^i\right)$$

$$\overset{(a)}{=} d_{11}\left(x_1 + \frac{(1 - x_1)^{r_1} - 1}{r_1}\right)$$

where in (a) *we used the binomial formula.*

Developing the second term in the summation (48) in a similar way, and setting $d_{11} = \ell_1$ *and* $d_{22} = \ell_2$, *we finally obtain*

$$G(\boldsymbol{x}) = \ell_1\left(x_1 + \frac{(1 - x_1)^{r_1} - 1}{r_1}\right)$$
$$+ \ell_2\left(x_2 + \frac{(1 - x_2)^{r_2} - 1}{r_2}\right). \tag{49}$$

It is easy to verify that $F(\boldsymbol{y}; \varepsilon)$ *and* $G(\boldsymbol{x})$ *satisfy* $F(\boldsymbol{0}; \varepsilon) = 0$, $G(\boldsymbol{0}) = 0$, $F'(\boldsymbol{y}; \varepsilon) = \boldsymbol{f}(\boldsymbol{y}; \varepsilon)\boldsymbol{D}$, *and* $G'(\boldsymbol{x}) = \boldsymbol{g}(\boldsymbol{x})\boldsymbol{D}$. △

C. Existence of $U(\boldsymbol{x}; \varepsilon)$ for $(d_{\mathrm{v}}, d_{\mathrm{c}}, m)$ and $(d_{\mathrm{v}}, d_{\mathrm{c}}, m, L, w)$ Ensembles

In [4], [11], the potential function was defined using a diagonal matrix $\boldsymbol{D}$. It is easy to verify that all the examples in [4] (noisy Slepian-Wolf problem with erasures, LDPC codes over the erasure multiple access channel, and protograph codes over the BEC) satisfy the necessary condition in Corollary 2. However, in the case of nonbinary LDPC codes, the following proposition is true.

Proposition 1. *For the* $(d_{\mathrm{v}}, d_{\mathrm{c}}, m)$ *nonbinary LDPC code ensemble, if* $\boldsymbol{D}$ *is a diagonal matrix, the solution to (30) does not exist.*

Proof: First consider the variable node operation in (1) using (4). Consider $\mathcal{S}_m^f$, the set of nonzero coefficients of f_m (from (9), $f_m = f_{\circ m}$). From (4), $[\boldsymbol{a}_\circ \boxdot \boldsymbol{b}_\circ]_m = V_{m,m,m}^m a_{\circ m} b_{\circ m}$. Therefore, $f_m = p_m(V_{m,m,m}^m)^{d_{\mathrm{v}}-1} y_m^{d_{\mathrm{v}}-1}$, and $\mathcal{S}_m^f = \{(0, \ldots, 0, d_{\mathrm{v}} - 1)\}$. Developing $[\boldsymbol{a}_\circ \boxdot \boldsymbol{b}_\circ]_{m-1}$ in (1) and using $[\boldsymbol{a}_\circ \boxdot \boldsymbol{b}_\circ]_m$ earlier, it is also easy to see that

$$\mathcal{S}_{m-1}^f = \{(0, \ldots, 0, d_{\mathrm{v}} - 1, 0),$$
$$(0, \ldots, 0, d_{\mathrm{v}} - 2, 1), \ldots, (0, \ldots, 0, d_{\mathrm{v}} - 1)\}.$$

Therefore, the condition (41) is not verified. A similar proof holds for the check node operation. □

As a result of Proposition 1, for nonbinary LDPC codes, the potential function does not exist for a diagonal matrix $\boldsymbol{D}$. Thus, one should consider a more general form of $\boldsymbol{D}$. In the following, we show that, indeed, the potential function exists if a more general form of $\boldsymbol{D}$ is considered. We first give an example of the existence and computation of the potential function for the $(2, 3, 3)$ nonbinary LDPC code, and then discuss the existence of a solution to the system of linear equations (30) for nonbinary LDPC codes in general.

Example 2 (Existence and calculation of the potential function for the $(2, 3, 3)$ nonbinary LDPC code)**.** *We have* $\boldsymbol{x}_\circ = (x_{\circ 0}, x_{\circ 1}, x_{\circ 2})$, $\boldsymbol{y}_\circ = (y_{\circ 0}, y_{\circ 1}, y_{\circ 2})$, $\boldsymbol{p}_\circ = ((1 - \varepsilon)^2, 2\varepsilon(1 - \varepsilon), \varepsilon^2)$, $\boldsymbol{f}_\circ(\boldsymbol{y}_\circ; \varepsilon) = \boldsymbol{p}_\circ(\varepsilon) \boxdot \boldsymbol{y}_\circ$ *and* $\boldsymbol{g}_\circ(\boldsymbol{x}_\circ) = \boldsymbol{x}_\circ \boxtimes \boldsymbol{x}_\circ$. *Moreover,* $\boldsymbol{x} = (x_1, x_2)$, $\boldsymbol{y} = (y_1, y_2)$ *and* $\boldsymbol{f}(\boldsymbol{y}; \varepsilon) = (f_1, f_2)$. *Using (4) we obtain*

$$f_{\circ 0} = 1 - f_{\circ 1} - f_{\circ 2}$$
$$f_{\circ 1} = V_{1,1,1}^2 p_{\circ 1} y_{\circ 1} + V_{1,2,1}^2 p_{\circ 1} y_{\circ 2} + V_{2,1,1}^2 p_{\circ 2} y_{\circ 1}$$
$$= \left(\frac{2}{3}\varepsilon(1 - \varepsilon) + \varepsilon^2\right) y_{\circ 1} + 2\varepsilon(1 - \varepsilon) y_{\circ 2}$$
$$f_{\circ 2} = V_{2,2,2}^2 p_{\circ 2} y_{\circ 2} = \varepsilon^2 y_{\circ 2}.$$

Using (8) and (9) we obtain,

$$\boldsymbol{f} = (f_1, f_2) = \left(\frac{2\varepsilon + \varepsilon^2}{3} y_1 + \frac{4\varepsilon - 4\varepsilon^2}{3} y_2, \varepsilon^2 y_2\right).$$

It follows that $S_1^f = \{(1, 0), (0, 1)\}$ *and* $S_2^f = \{(0, 1)\}$.
Similarly, we obtain

$$g_{\circ 0} = 1 - g_{\circ 1} - g_{\circ 2}$$
$$g_{\circ 1} = 2x_{\circ 1} - \frac{5}{3}x_{\circ 1}^2 - 2x_{\circ 1}x_{\circ 2}$$
$$g_{\circ 2} = \frac{2}{3}x_{\circ 1}^2 - \frac{4}{3}x_{\circ 1}x_{\circ 2} + 2x_{\circ 2} - \frac{1}{3}x_{\circ 2}^2$$

and

$$\boldsymbol{g} = (g_1, g_2) = \left(2x_1 - x_1^2, \frac{2}{3}x_1^2 - \frac{4}{3}x_1 x_2 + 2x_2 - \frac{1}{3}x_2^2\right).$$

It follows that $S_1^g = \{(1, 0), (2, 0)\}$ *and* $S_2^g = \{(2, 0), (1, 1), (0, 1), (0, 2)\}$.
With the sets above, (41) is not satisfied. Therefore, the potential function does not exist for a diagonal matrix $\boldsymbol{D}$.

$$\boldsymbol{f}(\boldsymbol{y};\varepsilon)\boldsymbol{D} = \left(\frac{(2\varepsilon+\varepsilon^2)d_{11}}{3}y_1 + \frac{(4\varepsilon-4\varepsilon^2)d_{11}+3\varepsilon^2 d_{21}}{3}y_2, \frac{(2\varepsilon+\varepsilon^2)d_{12}}{3}y_1 + \frac{(4\varepsilon-4\varepsilon^2)d_{12}+3\varepsilon^2 d_{22}}{3}y_2 \right) \tag{50}$$

$$\boldsymbol{g}(\boldsymbol{x})\boldsymbol{D} = \left(2d_{11}x_1 + \frac{2d_{21}-3d_{11}}{3}x_1^2 - \frac{4d_{21}}{3}x_1 x_2 + 2d_{21}x_2 - \frac{d_{21}}{3}x_2^2, 2d_{12}x_1 + \frac{2d_{22}-3d_{12}}{3}x_1^2 - \frac{4d_{22}}{3}x_1 x_2 + 2d_{22}x_2 - \frac{d_{22}}{3}x_2^2 \right) \tag{51}$$

However, the potential function exists if a matrix with non-zero elements is used. In this case the sets $\mathcal{S}^F$ and $\mathcal{S}^G$ are (see (27)),

$$\mathcal{S}^F = \{(2,0),(1,1),(0,2)\}$$
$$\mathcal{S}^G = \{(2,0),(3,0),(1,1),(1,2),(2,1),(0,2),(0,3)\}.$$

Using these sets, we can write the functions $F(\boldsymbol{y};\varepsilon)$ and $G(\boldsymbol{x})$ as (cf. (33) and (34))

$$F(\boldsymbol{y};\varepsilon) = \varphi_{(2,0)}y_1^2 + \varphi_{(1,1)}y_1 y_2 + \varphi_{(0,2)}y_2^2$$
$$G(\boldsymbol{x}) = \mu_{(2,0)}x_1^2 + \mu_{(3,0)}x_1^3 + \mu_{(1,1)}x_1 x_2 + \mu_{(1,2)}x_1 x_2^2$$
$$+ \mu_{(2,1)}x_1^2 x_2 + \mu_{(0,2)}x_2^2 + \mu_{(0,3)}x_2^3.$$

We also obtain

$$F'(\boldsymbol{y};\varepsilon) = \frac{\partial F(\boldsymbol{y};\varepsilon)}{\partial \boldsymbol{y}}$$
$$= \left(2\varphi_{(2,0)}y_1 + \varphi_{(1,1)}y_2, \varphi_{(1,1)}y_1 + 2\varphi_{(0,2)}y_2 \right)$$
$$G'(\boldsymbol{x}) = \frac{\partial G(\boldsymbol{x})}{\partial \boldsymbol{x}}$$
$$= \left(2\mu_{(2,0)}x_1 + 3\mu_{(3,0)}x_1^2 + \mu_{(1,1)}x_2 + \mu_{(1,2)}x_2^2 \right.$$
$$+ 2\mu_{(2,1)}x_1 x_2, \mu_{(1,1)}x_1 + 2\mu_{(1,2)}x_1 x_2$$
$$\left. + \mu_{(2,1)}x_1^2 + 2\mu_{(0,2)}x_2 + 3\mu_{(0,3)}x_2^2 \right).$$

On the other hand, $\boldsymbol{f}(\boldsymbol{y};\varepsilon)\boldsymbol{D}$ and $\boldsymbol{g}(\boldsymbol{x})\boldsymbol{D}$ are given by (50) and (51), respectively, at the top of the page.

We can now write the system of linear equations (30) as

$$2\varphi_{(2,0)} = \frac{(2\varepsilon+\varepsilon^2)d_{11}}{3}, \quad \varphi_{(1,1)} = \frac{(4\varepsilon-4\varepsilon^2)d_{11}+3\varepsilon^2 d_{21}}{3},$$
$$\varphi_{(1,1)} = \frac{(2\varepsilon+\varepsilon^2)d_{12}}{3}, \quad 2\varphi_{(0,2)} = \frac{(4\varepsilon-4\varepsilon^2)d_{12}+3\varepsilon^2 d_{22}}{3},$$
$$2\mu_{(2,0)} = 2d_{11}, \quad 3\mu_{(3,0)} = \frac{2d_{21}-3d_{11}}{3},$$
$$\mu_{(1,1)} = 2d_{21}, \quad \mu_{(1,2)} = -\frac{d_{21}}{3},$$
$$2\mu_{(2,1)} = -\frac{4d_{21}}{3}, \quad \mu_{(1,1)} = 2d_{12},$$
$$2\mu_{(1,2)} = -\frac{4d_{22}}{3}, \quad \mu_{(2,1)} = \frac{2d_{22}-3d_{12}}{3},$$
$$2\mu_{(0,2)} = 2d_{22}, \quad 3\mu_{(0,3)} = -\frac{d_{22}}{3}.$$

Note that solving the system above is equivalent to solve the following subsystem of linear equations,

$$\begin{cases} (2\varepsilon+\varepsilon^2)d_{12} &= (4\varepsilon-4\varepsilon^2)d_{11}+3\varepsilon^2 d_{21} \\ 2d_{21} &= 2d_{12} \\ -\frac{4}{6}d_{22} &= -\frac{1}{3}d_{21} \end{cases}$$

This subsystem gives us the solution

$$d_{12} = 2d_{11}, \quad d_{21} = 2d_{11}, \quad d_{22} = d_{11}$$

and the induced coefficients φ and μ are then obtained as

$$\varphi_{(2,0)} = \frac{2\varepsilon+\varepsilon^2}{6}d_{11}, \quad \mu_{2,0} = d_{11}, \quad \mu_{1,2} = -\frac{2}{3}d_{11},$$
$$\varphi_{(1,1)} = \frac{4\varepsilon+2\varepsilon^2}{3}d_{11}, \quad \mu_{3,0} = \frac{1}{9}d_{11}, \quad \mu_{1,1} = 4d_{11}$$
$$\varphi_{(0,2)} = \frac{8\varepsilon-5\varepsilon^2}{6}d_{11}, \quad \mu_{2,1} = -\frac{4}{3}d_{11}, \quad \mu_{0,2} = d_{11},$$
$$\mu_{0,3} = -\frac{1}{9}d_{11}.$$

Therefore, the system has an infinite number of solutions. Choosing the free parameter $d_{11} = 1$ we finally obtain

$$F(\boldsymbol{y};\varepsilon) = \frac{2\varepsilon+\varepsilon^2}{6}y_1^2 + \frac{4\varepsilon+2\varepsilon^2}{3}y_1 y_2 + \frac{8\varepsilon-5\varepsilon^2}{6}y_2^2$$
$$G(\boldsymbol{x}) = x_1^2 + \frac{1}{9}x_1^3 + 4x_1 x_2 - \frac{2}{3}x_1 x_2^2 - \frac{4}{3}x_1^2 x_2 + x_2^2 - \frac{1}{9}x_2^3.$$

It is easy to verify that this solution satisfies $F'(\boldsymbol{y};\varepsilon) = \boldsymbol{f}(\boldsymbol{y};\varepsilon)\boldsymbol{D}$ and $G'(\boldsymbol{x}) = \boldsymbol{g}(\boldsymbol{x})\boldsymbol{D}$. Note also that the resulting $\boldsymbol{D}$ is symmetric. △

We now discuss the general case of nonbinary LDPC codes. Assume that the necessary condition on the existence of functions $F(\boldsymbol{y};\varepsilon)$ and $G(\boldsymbol{x})$ is satisfied. We would like to determine whether (30) has always a solution. To do so, we analyze the form of the system of equations (30) for nonbinary LDPC codes.

Lemma 5. *For nonbinary $(d_{\mathrm{v}}, d_{\mathrm{c}}, m)$ LDPC codes,*

$$|\mathcal{S}^F| = \sum_{n=3}^{d_{\mathrm{v}}} \sum_{t=1}^{n} \binom{n-1}{t-1}\binom{m}{t} \tag{52}$$

$$|\mathcal{S}^G| = \sum_{n=2}^{d_{\mathrm{c}}} \sum_{t=1}^{n} \binom{n-1}{t-1}\binom{m}{t}. \tag{53}$$

Moreover, the number of equations in (30), containing $\varphi_{(i_1,\ldots,i_m)}$ and $\mu_{(i_1,\ldots,i_m)}$ is respectively

$$N_\varphi = \sum_{n=3}^{d_{\mathrm{v}}} \sum_{t=1}^{n} t\binom{n-1}{t-1}\binom{m}{t} \tag{54}$$

$$N_\mu = \sum_{n=2}^{d_{\mathrm{c}}} \sum_{t=1}^{n} t\binom{n-1}{t-1}\binom{m}{t}. \tag{55}$$

Proof: Consider (33). It defines a multivariate polynomial $F(\boldsymbol{y};\varepsilon)$ which, by construction, contains all monomials $y_1^{i_1} \cdots y_m^{i_m}$ such that

$$3 \leq \sum_{s=1}^{m} i_s \leq d_{\mathrm{v}}.$$

Therefore, in order to find the number of elements in $\mathcal{S}^F$, we count the number of vectors $(i_1,\ldots,i_m) \in \mathcal{S}^F$ of length m

with t nonzero entries, and $\sum_{s=1}^{m} i_s = n$, for $3 \leq n \leq d_v$ and $1 \leq t \leq m$,. As for some fixed value of n, the number of vectors with exactly t nonzero entries and $\sum_{s=1}^{m} i_s = n$ is given by the binomial coefficient $\binom{n-1}{t-1}$, and these t nonzero entries can be placed in a vector of length m in $\binom{m}{t}$ various ways, the expression for $|\mathcal{S}^F|$ follows directly. The same reasoning holds for $|\mathcal{S}^G|$, with the only difference that $G(\boldsymbol{x})$ is constructed in a way that it contains all monomials $x_1^{i_1} \cdots x_m^{i_m}$ such that

$$2 \leq \sum_{s=1}^{m} i_s \leq d_c.$$

Now, to obtain (54), it is sufficient to notice from (30) that any variable $\varphi_{(i_1, \dots, i_m)}$ having t nonzero entries within its index vector $(i_1, \dots, i_m)$ participates in exactly t equations. The same holds for variables $\gamma_{(i_1, \dots, i_m)}$. $\square$

The system of linear equations (30) has $|\mathcal{S}^F| + |\mathcal{S}^G| + \frac{m(m-1)}{2}$ free variables (which are the coefficients φ, μ and d_{ij}) and $N_\varphi + N_\gamma$ equations. Therefore, if d_v, d_c and m are such that

$$|\mathcal{S}^F| + |\mathcal{S}^G| + \frac{m(m-1)}{2} \geq N_\varphi + N_\gamma \qquad (56)$$

then (30) would have a solution. Unfortunately, for almost all interesting choices of d_v, d_c and m this condition is not verified. However, the solution of (30) does exist in most cases. This has been verified numerically, and is discussed in the following. The reason that a solution exists lies in the fact that, due to the structural properties of $V_{i,j,k}$ and $C_{i,j,k}$ in $\boldsymbol{f}(\boldsymbol{y}; \varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$, the system (30) contains many linearly dependent equations, so the condition (56) is too weak. To verify the existence of $F(\boldsymbol{y}; \varepsilon)$ and $G(\boldsymbol{x})$ for nonbinary LDPC codes, we verified numerically the existence of a solution for regular codes with degrees $(2,3)$, $(3,4)$, $(3,5)$ and $(3,6)$, for values of m starting from 2 until the largest value that was feasible to simulate (e.g., for $(3,4)$ LDPC codes we considered m up to 20). For all the considered examples, the number of equations in (30) was larger than the number of free variables. However, in all cases, similarly to Example 2, after eliminating linearly dependent equations, we obtained a subsystem of $m^2 - 1$ equations with m^2 variables d_{ij}, which results in a symmetric matrix $\boldsymbol{D}$, parametrized by d_{11}. Then, all coefficients φ and μ are obtained as a function of d_{11}, as in Example 2. The subsystems of linear equations for the $(3,4,2)$ and $(3,4,3)$ nonbinary LDPC codes are given in Table II. Our numerical results strongly suggest that, for (d_v, d_c, m) nonbinary LDPC code ensembles, the functions $F(\boldsymbol{y}; \varepsilon)$ and $G(\boldsymbol{x})$ always exist, and the corresponding matrix $\boldsymbol{D}$ is always symmetric. Choosing d_{11} to be positive, the resulting matrix is positive, symmetric and invertible, properties that are used in Lemma 2 and subsequently in the proof of threshold saturation.

VI. Conclusion

We studied threshold saturation for nonbinary SC-LDPC codes when transmission takes place over the BEC. We used the proof technique based on the potential function $U(\boldsymbol{x}; \epsilon)$ for vector recursions, recently proposed by Yedla *et al.* [4]

and showed that threshold saturation occurs for nonbinary SCLDPC codes, under the condition of the existence of the potential function. Our proof is a non-straightforward extension of the proof in [4] to accommodate nonbinary SC-LDPC codes. In particular, during the proof of the threshold saturation, we have shown the following important facts:

- *Existence of a fixed point in the DE of nonbinary LDPC codes:* In their probability vector form, the variable and check node updates $\boldsymbol{f}(\boldsymbol{y}; \varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ are not monotone with respect to the input variables. However, monotonicity can be shown by using an equivalent representation based on CCDF vectors. The property of monotonicity implies the existence of a fixed point in the DE equation of nonbinary LDPC ensembles, and also allows to use the proof technique of [4].
- *Existence and calculation of the potential function:* We derived a necessary condition on the existence of the potential function. Furthermore, we showed that, if it exists, the potential function can be obtained by finding the functions $F(\boldsymbol{y}; \varepsilon)$ and $G(\boldsymbol{x})$ as the solution of a system of linear equations.
- *Use of a diagonal matrix $\boldsymbol{D}$ in the definition of $U(\boldsymbol{x}; \epsilon)$:* In [4] $\boldsymbol{D}$ is assumed to be diagonal. For many vector coupled systems a diagonal matrix $\boldsymbol{D}$ satisfies the necessary condition for the existence of $U(\boldsymbol{x}; \epsilon)$. However, the condition is not verified in the case of nonbinary codes.
- *Positive, symmetric and invertible form of $\boldsymbol{D}$ and threshold saturation for nonbinary LDPC codes:* We showed numerically that, for multiple families of nonbinary LDPC code ensembles, $F(\boldsymbol{y}; \varepsilon)$ and $G(\boldsymbol{x})$ exist for a positive, symmetric and invertible matrix $\boldsymbol{D}$. In such cases, we are able to prove threshold saturation following the same lines as the proof by Yedla *et al.*. Unfortunately, the general problem of the existence of a solution to the system of linear equations (and thus of the potential function) for arbitrary nonbinary LDPC code ensembles still remains open. However, based on our observations, we conjecture that threshold saturation occurs in general.

Appendix A
Some Useful Results

Consider the Gaussian binomial coefficient in (6) and the definition of the coefficients V_{ijk},

$$V_{i,j,k}^m = \begin{cases} \frac{G_{i,k} G_{m-i,j-k} 2^{(i-k)(j-k)}}{G_{m,j}}, & \text{if (C1) holds} \\ 0, & \text{otherwise} \end{cases} \qquad (57)$$

where the condition (C1) is

$$\text{(C1)}: \quad 0 \leq i, j \leq m \quad \text{and}$$
$$\max(i + j - m, 0) \leq k \leq \min(i, j).$$

TABLE II: Subsystems of linearly independent equations from (30), for some values of d_{v}, d_{c} and m.

$(d_{\mathrm{v}}, d_{\mathrm{c}}, m)$	$\lvert \mathcal{S}^F \rvert + \lvert \mathcal{S}^G \rvert$	$N_\varphi + N_\gamma$	Equivalent subsystem of equations	Resulting $\boldsymbol{D}$
$(3,4,2)$	16	24	$\begin{cases} -\frac{4}{10}d_{21} + \frac{9}{10}d_{12} = d_{22} \\ -d_{21} + \frac{3}{2}d_{12} = d_{22} \\ 2\varepsilon(1-\varepsilon)d_{11} = \varepsilon^2 d_{12} \end{cases}$	$\begin{bmatrix} d_{11} & 2d_{11} \\ 2d_{11} & d_{11} \end{bmatrix}$
$(3,4,3)$	41	75	$\begin{cases} 3d_{21} = 3d_{12} \\ d_{31} = 4_{d33} \\ 3d_{31} = 3d_{13} \\ 6d_{32} = 12d_{33} \\ d_{32} = d_{23} \\ d_{21} + 15d_{33} = 6d_{22} \\ 4\varepsilon d_{11} = 2\varepsilon d_{12} \\ 8\varepsilon d_{11} = 2\varepsilon d_{13} \end{cases}$	$\begin{bmatrix} d_{11} & 3d_{11} & 4d_{11} \\ 3d_{11} & 3d_{11} & 2d_{11} \\ 4d_{11} & 2d_{11} & d_{11} \end{bmatrix}$

We give without proof the following lemmas.

Lemma 6. *Assume $m > 0$. Then for all $0 \le i \le m$,*

$$\frac{G_{m,i+1}}{G_{m,i}} = \frac{2^{m-i}-1}{2^{i+1}-1} \tag{58}$$

$$\frac{G_{m+1,i}}{G_{m,i}} = \frac{2^{m+1}-1}{2^{m-i+1}-1} \tag{59}$$

$$\frac{G_{m+1,i+1}}{G_{m,i}} = \frac{2^{m+1}-1}{2^{i+1}-1}. \tag{60}$$

Lemma 7. *Let i, j, ℓ be such that $V_{ij\ell} > 0$ and $V_{(i-1)j\ell} > 0$ (i.e., by (57), $0 \le \ell \le m$, $\ell < i \le m$ and $\ell \le j \le m+\ell-i$). Then*

$$\frac{V_{ij\ell}}{V_{(i-1)j\ell}} = \frac{2^{i-\ell}-2^{-\ell}}{2^{i-\ell}-1} \cdot \frac{2^{m+\ell-i+1}-2^j}{2^{m-i+1}-1}. \tag{61}$$

Moreover, if $\ell > 0$,

$$\frac{V_{ij\ell}}{V_{(i-1)j\ell}} > 2^\ell \frac{2^{m-i+1}-2^{j-\ell}}{2^{m-i+1}-1}. \tag{62}$$

Further, if $j - \ell \le m - i$ and $\ell > 0$,

$$\frac{V_{ij\ell}}{V_{(i-1)j\ell}} > 2^{\ell-1}. \tag{63}$$

Lemma 8. *Let i, j, ℓ be such that $V_{ij\ell} > 0$ and $V_{(i-1)j(\ell-1)} > 0$ (i.e., by (57), $0 < \ell \le i \le m$ and $\ell < j \le m+\ell-i$). Then*

$$\frac{V_{ij\ell}}{V_{(i-1)j(\ell-1)}} = \frac{2^i-1}{2^{m+1}-2^i} \cdot \frac{2^{j+1}-2^\ell}{2^\ell-1}. \tag{64}$$

Moreover, if $i = \ell$ and $j = m$, $\frac{V_{\ell m\ell}}{V_{(\ell-1)m(\ell-1)}} = 1$.

APPENDIX B
PROOF OF THEOREM 1

We prove the monotonicity of $\boldsymbol{f}(\boldsymbol{y};\varepsilon)$ and $\boldsymbol{g}(\boldsymbol{x})$ by induction. We first prove that the variable node operation in the CCDF form is non-decreasing in $\boldsymbol{y}$. Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be two CCDF vectors. The variable node performs the intersection of two random subspaces, $\mathbf{W} = \mathbf{U} \otimes \mathbf{V}$. We define

$$c_{\circ k} = [\boldsymbol{a}_\circ \boxdot \boldsymbol{b}_\circ]_k = \sum_{i=k}^{m} a_{\circ i} \sum_{j=k}^{m+k-i} V_{i,j,k} b_{\circ j}. \tag{65}$$

We can write the CCDF element c_k as

$$c_k \triangleq \sum_{\ell=k}^{m} c_{\circ \ell} \tag{66}$$

$$= \sum_{\ell=k}^{m} \sum_{i=\ell}^{m} a_{\circ i} \sum_{j=\ell}^{m+\ell-i} V_{i,j,\ell} b_{\circ j} \tag{67}$$

We also remind that (cf. (9))

$$a_{\circ i} = \begin{cases} 1 - a_1, & i = 0 \\ a_i - a_{i+1}, & 1 \le i < m \\ a_m, & i = m. \end{cases} \tag{68}$$

In the following, we prove that $\frac{\partial c_k}{\partial a_i} \ge 0$ by proving that $\frac{\partial c_{\circ\ell}}{\partial a_i} \ge 0$. Given (68), there are two cases to treat, $\ell = m$ and $1 \le \ell < m$.

First, consider $\ell = m$. Then,

$$c_{\circ m} = a_m V_{mmm} b_m$$

and

$$\frac{\partial c_{\circ m}}{\partial a_i} = \begin{cases} V_{mmm} b_m, & i = m \\ 0, & \text{otherwise}. \end{cases} \tag{69}$$

Now, assume $1 \le \ell < m$. We develop

$$c_{\circ\ell} = a_m V_{m\ell\ell} b_{\circ\ell} + \sum_{i=\ell}^{m-1} (a_i - a_{i+1}) \sum_{j=\ell}^{\ell+m-i} V_{ij\ell} b_{\circ j} \tag{70}$$

$$= a_m V_{m\ell\ell} b_{\circ\ell} + \sum_{i=\ell}^{m-1} a_i \sum_{j=\ell}^{\ell+m-i} V_{ij\ell} b_{\circ j}$$

$$- \sum_{i=\ell}^{m-1} a_{i+1} \sum_{j=\ell}^{\ell+m-i} V_{ij\ell} b_{\circ j} \tag{71}$$

$$= \sum_{i=\ell}^{m} a_i \sum_{j=\ell}^{\ell+m-i} V_{ij\ell} b_{\circ j} - \sum_{i=\ell}^{m-1} a_{i+1} \sum_{j=\ell}^{\ell+m-i} V_{ij\ell} b_{\circ j} \tag{72}$$

$$= \sum_{i=\ell}^{m} a_i \sum_{j=\ell}^{\ell+m-i} V_{ij\ell} b_{\circ j} - \sum_{i=\ell+1}^{m} a_i \sum_{j=\ell}^{\ell+m-(i-1)} V_{(i-1)j\ell} b_{\circ j} \tag{73}$$

$$= \sum_{i=\ell}^{m} a_i \sum_{j=\ell}^{\ell+m-i} V_{ij\ell} b_{\circ j} - \sum_{i=\ell+1}^{m} a_i \sum_{j=\ell}^{\ell+m-i} V_{(i-1)j\ell} b_{\circ j}$$
$$- \sum_{i=\ell+1}^{m} a_i V_{(i-1)(\ell+m-i+1)\ell} b_{\circ\ell+m-i+1}. \tag{74}$$

We continue

$$c_{\circ\ell} = a_\ell \sum_{j=\ell}^{m} V_{\ell j\ell} b_{\circ j} + \sum_{i=\ell+1}^{m} a_i \sum_{j=\ell}^{\ell+m-i} \left(V_{ij\ell} - V_{(i-1)j\ell}\right) b_{\circ j}$$
$$- \sum_{i=\ell+1}^{m} a_i V_{(i-1)(\ell+m-i+1)\ell} b_{\circ\ell+m-i+1}. \tag{75}$$

Given all above, for all values of ℓ, $1 \le \ell \le m$, the derivative $\frac{\partial c_{\circ\ell}}{\partial a_i}$ is

$$\frac{\partial c_{\circ\ell}}{\partial a_i} = \begin{cases} 0, & i < \ell \\ \sum_{j=\ell}^{m} V_{\ell j\ell} b_{\circ j} > 0, & i = \ell \\ (77), & \ell+1 \le i \le m \end{cases} \tag{76}$$

where (77) is

$$-V_{(i-1)(\ell+m-i+1)\ell} b_{\circ\ell+m-i+1} + \sum_{j=\ell}^{\ell+m-i} \left(V_{ij\ell} - V_{(i-1)j\ell}\right) b_{\circ j}. \tag{77}$$

Putting together (66) and (76), we obtain

$$\frac{\partial c_k}{\partial a_i} = \begin{cases} 0, & i < k; \\ \sum_{j=k}^{m} V_{kjk} b_{\circ j} > 0, & i = k \\ \sum_{\ell=k}^{i-1} \frac{\partial c_{\circ\ell}}{\partial a_i} + \frac{\partial c_{\circ i}}{\partial a_i} + \sum_{\ell=i+1}^{m} \frac{\partial c_{\circ\ell}}{\partial a_i}, & k < i < m \\ \sum_{\ell=k}^{m-1} \frac{\partial c_{\circ\ell}}{\partial a_m} + \frac{\partial c_{\circ m}}{\partial a_m}, & i = m. \end{cases} \tag{78}$$

For $k < i < m$,

$$\sum_{\ell=k}^{i-1} \frac{\partial c_{\circ\ell}}{\partial a_i} + \frac{\partial c_{\circ i}}{\partial a_i} + \sum_{\ell=i+1}^{m} \frac{\partial c_{\circ\ell}}{\partial a_i} = \sum_{\ell=k}^{i-1} \frac{\partial c_{\circ\ell}}{\partial a_i} + \frac{\partial c_{\circ i}}{\partial a_i} + 0. \tag{79}$$

Therefore, we rewrite (78) as

$$\frac{\partial c_k}{\partial a_i} = \begin{cases} 0, & i < k \\ \sum_{j=k}^{m} V_{kjk} b_{\circ j} > 0, & i = k \\ \sum_{\ell=k}^{i-1} \frac{\partial c_{\circ\ell}}{\partial a_i} + \frac{\partial c_{\circ i}}{\partial a_i}, & k < i \le m. \end{cases} \tag{80}$$

To show that $\frac{\partial c_k}{\partial a_i}$ is nonnegative, one should prove it for the case when $1 \le k < i \le m$. We have

$$\frac{\partial c_k}{\partial a_i} = \sum_{\ell=k}^{i-1} \left(-V_{(i-1)(\ell+m-i+1)\ell} b_{\circ\ell+m-i+1}\right.$$
$$\left.+ \sum_{j=\ell}^{\ell+m-i} \left(V_{ij\ell} - V_{(i-1)j\ell}\right) b_{\circ j}\right) + \sum_{j=i}^{m} V_{iji} b_{\circ j}. \tag{81}$$

Letting $\sum_{j=i}^{m} V_{iji} b_{\circ j} = \sum_{\ell=i}^{m} V_{i\ell i} b_{\circ\ell}$,

$$\frac{\partial c_k}{\partial a_i} = \sum_{\ell=i}^{m} V_{i\ell i} b_{\circ\ell} - \sum_{\ell=k}^{i-1} V_{(i-1)(\ell+m-i+1)\ell} b_{\circ\ell+m-i+1}$$
$$+ \sum_{\ell=k}^{i-1} \sum_{j=\ell}^{\ell+m-i} \left(V_{ij\ell} - V_{(i-1)j\ell}\right) b_{\circ j}. \tag{82}$$

By substituting $\ell' = \ell + m - i + 1$ in the second summation,

$$\frac{\partial c_k}{\partial a_i} = \sum_{\ell=i}^{m} V_{i\ell i} b_{\circ\ell} - \sum_{\ell'=m+k-i+1}^{m} V_{(i-1)\ell'(\ell'+i-m-1)} b_{\circ\ell'}$$
$$+ \sum_{\ell=k}^{i-1} \sum_{j=\ell}^{\ell+m-i} \left(V_{ij\ell} - V_{(i-1)j\ell}\right) b_{\circ j}. \tag{83}$$

Now, depending on the value of i, we have two cases to consider: $i \le m + k - i + 1$ and $i > m + k - i + 1$.

A. Case $i \le m + k - i + 1$

Consider $\sum_{\ell=k}^{i-1} \sum_{j=\ell}^{\ell+m-i} \left(V_{ij\ell} - V_{(i-1)j\ell}\right) b_{\circ j}$ and let exchange the sums in ℓ and j. It can be verified that

- if $k \le j < i - 1$, then ℓ varies from k to j;
- if $i - 1 \le j \le k + m - i$, then ℓ varies from k to $i - 1$;
- if $k + m - i < j \le m - 1$, then ℓ varies from $i + j - m$ to $i - 1$.

Therefore, (83) can be written as

$$\frac{\partial c_k}{\partial a_i} = \sum_{\ell=i}^{m} V_{i\ell i} b_{\circ\ell} - \sum_{\ell=m+k-i+1}^{m} V_{(i-1)\ell(\ell+i-m-1)} b_{\circ\ell}$$
$$+ \sum_{j=k}^{i-2} b_{\circ j} \sum_{\ell=k}^{j} \left(V_{ij\ell} - V_{(i-1)j\ell}\right) + \sum_{j=i-1}^{k+m-i} b_{\circ j} \sum_{\ell=k}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell}\right)$$
$$+ \sum_{j=k+m-i+1}^{m-1} b_{\circ j} \sum_{\ell=i+j-m}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell}\right). \tag{84}$$

By rearranging terms in $b_{\circ m+k-i+1}, \ldots, b_{\circ m}$, we obtain

$$\frac{\partial c_k}{\partial a_i} = \sum_{\ell=i}^{k+m-i} V_{i\ell i} b_{\circ\ell} + \left(V_{imi} - V_{(i-1)m(i-1)}\right) b_{\circ m}$$
$$+ \sum_{j=k}^{i-2} b_{\circ j} \sum_{\ell=k}^{j} \left(V_{ij\ell} - V_{(i-1)j\ell}\right)$$
$$+ \sum_{j=i-1}^{k+m-i} b_{\circ j} \sum_{\ell=k}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell}\right)$$
$$+ \sum_{j=k+m-i+1}^{m-1} b_{\circ j} \left(V_{i\ell i} - V_{(i-1)j(j+i-m-1)}\right.$$
$$\left.+ \sum_{\ell=i+j-m}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell}\right)\right) \tag{85}$$

Note that $V_{imi} - V_{(i-1)m(i-1)} = 0$ by Lemma 8. Thus,

$$\frac{\partial c_k}{\partial a_i} = \sum_{\ell=i}^{k+m-i} V_{i\ell i} b_{\circ\ell} + \sum_{j=k}^{i-2} b_{\circ j} \sum_{\ell=k}^{j} \left(V_{ij\ell} - V_{(i-1)j\ell} \right)$$
$$+ \sum_{j=i-1}^{k+m-i} b_{\circ j} \sum_{\ell=k}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell} \right)$$
$$+ \sum_{j=k+m-i+1}^{m-1} b_{\circ j} \Big(V_{i\ell i} - V_{(i-1)j(j+i-m-1)}$$
$$+ \sum_{\ell=i+j-m}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell} \right) \Big) \tag{86}$$
$$= A_1 + A_2 + A_3 + A_4 \tag{87}$$

where

$$A_1 = \sum_{\ell=i}^{k+m-i} V_{i\ell i} b_{\circ\ell} \tag{88}$$

$$A_2 = \sum_{j=k}^{i-2} b_{\circ j} \sum_{\ell=k}^{j} \left(V_{ij\ell} - V_{(i-1)j\ell} \right) \tag{89}$$

$$A_3 = \sum_{j=i-1}^{k+m-i} b_{\circ j} \sum_{\ell=k}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell} \right) \tag{90}$$

$$A_4 = \sum_{j=k+m-i+1}^{m-1} b_{\circ j} \Big(V_{i\ell i} - V_{(i-1)j(j+i-m-1)}$$
$$+ \sum_{\ell=i+j-m}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell} \right) \Big). \tag{91}$$

Clearly, $A_1 \geq 0$. Let us now show that A_2 and A_3 are nonnegative. We have $\ell > 0$, and $j - \ell \leq i - 1 - k$ and $i \leq m + k - i + 1$, so that $j - \ell \leq m - i$. Therefore, using (63) in Lemma 7,

$$A_2 \geq \sum_{j=k}^{i-2} b_{\circ j} \sum_{\ell=k}^{j} V_{(i-1)j\ell} \left(2^{\ell-1} - 1 \right) \geq 0. \tag{92}$$

Similarly,

$$A_3 \geq \sum_{j=i-1}^{k+m-i} b_{\circ j} \sum_{\ell=k}^{i-1} V_{(i-1)j\ell} \left(2^{\ell-1} - 1 \right) \geq 0. \tag{93}$$

We show now that $A_4 > 0$. For this, consider the term $V_{i\ell i} - V_{(i-1)j(j+i-m-1)} + \sum_{\ell=i+j-m}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell} \right)$. Remind that $\ell \geq i + j - m$. Therefore, by Lemma 7,

$$V_{ij\ell} - V_{(i-1)j\ell} \geq V_{(i-1)j\ell} \left(2^{\ell} \frac{2^{m-i+1} - 2^{j-\ell}}{2^{m-i+1} - 1} - 1 \right) \tag{94}$$

$$\geq V_{(i-1)j\ell} \left(2^{\ell} \frac{2^{m-i+1} - 2^{j-(i+j-m)}}{2^{m-i+1} - 1} - 1 \right) \tag{95}$$

$$> V_{(i-1)j\ell} (2^{\ell-1} - 1). \tag{96}$$

Then the expression of interest is lower bounded as

$$V_{i\ell i} - V_{(i-1)j(j+i-m-1)} + \sum_{\ell=i+j-m}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell} \right)$$
$$> V_{i\ell i} - V_{(i-1)j(j+i-m-1)} + \sum_{\ell=i+j-m}^{i-1} V_{(i-1)j\ell} (2^{\ell-1} - 1)$$
$$> V_{i\ell i} - V_{(i-1)j(j+i-m-1)} + V_{(i-1)j(i+j-m)} (2^{i+j-m-1} - 1). \tag{97}$$

Consider

$$V_{i\ell i} - V_{(i-1)j(j+i-m-1)} + V_{(i-1)j(i+j-m)} (2^{i+j-m-1} - 1).$$

We first compute

$$\frac{V_{i\ell i}}{V_{(i-1)j(j+i-m-1)}} = \frac{G_{m-i,m-\ell}}{G_{m,m-\ell}} \frac{G_{m,m-j} 2^{-(m-j)(m-i+1)}}{G_{i-1,m-j}} \tag{98}$$

$$= \prod_{t_1=0}^{m-\ell-1} \frac{2^{m-i-t_1} - 1}{2^{m-t_1} - 1} \cdot \prod_{t_2=0}^{m-j-1} \frac{2^{m-t_2} - 1}{2^{m-t_2} - 2^{m-i+1}} \tag{99}$$

$$\geq \prod_{t_1=0}^{m-\ell-1} \frac{2^{m-i-t_1} - 1}{2^{m-t_1} - 1} \cdot \frac{2^m - 1}{2^m - 2^{m-i+1}} \tag{100}$$

$$\geq 2^{(i-1)(m-\ell-1)} \frac{2^m - 1}{2^m - 2^{m-i+1}} \tag{101}$$

$$\geq 2^{(m-\ell-1)} \frac{2^m - 1}{2^m - 2^{m-i+1}} \tag{102}$$

$$\geq 2^{(m-i)} \tag{103}$$

$$\geq 2^{m/2} > 1. \tag{104}$$

Hence, we have $V_{i\ell i} > V_{(i-1)j(j+i-m-1)}$. This implies $A_4 > 0$.

Finally, putting together A_1, A_2, A_3, and A_4, it follows that $\frac{\partial c_k}{\partial a_i} > 0$ for $i \leq m + k - i + 1$.

B. Case $i > m + k - i + 1$

Consider $\sum_{\ell=k}^{i-1} \sum_{j=\ell}^{\ell+m-i} \left(V_{ij\ell} - V_{(i-1)j\ell} \right) b_{\circ j}$ and let exchange the sums in ℓ and j. It can be verified that,

- if $k \leq j \leq k + m - i$, then ℓ varies from k to j;
- if $k + m - i < j \leq i - 1$, then ℓ varies from $i + j - m$ to j;
- if $i - 1 < j \leq m - 1$, then ℓ varies from $i + j - m$ to $i - 1$.

Thus, (83) is written as

$$\frac{\partial c_k}{\partial a_i} = \sum_{\ell=i}^{m} V_{i\ell i} b_{\circ\ell} - \sum_{\ell=m+k-i+1}^{m} V_{(i-1)\ell(\ell+i-m-1)} b_{\circ\ell}$$
$$+ \sum_{j=k}^{k+m-i} b_{\circ j} \sum_{\ell=k}^{j} \left(V_{ij\ell} - V_{(i-1)j\ell} \right)$$
$$+ \sum_{j=k+m-i+1}^{i-1} b_{\circ j} \sum_{\ell=i+j-m}^{j} \left(V_{ij\ell} - V_{(i-1)j\ell} \right)$$
$$+ \sum_{j=i}^{m-1} b_{\circ j} \sum_{\ell=i+j-m}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell} \right). \tag{105}$$

By rearranging terms in $b_{\circ m+k-i+1}, \ldots, b_{\circ m}$, we obtain

$$
\begin{aligned}
\frac{\partial c_k}{\partial a_i} = {} & \left(V_{imi} - V_{(i-1)m(i-1)}\right) b_{\circ m} \\
& + \sum_{j=k}^{k+m-i} b_{\circ j} \sum_{\ell=k}^{j} \left(V_{ij\ell} - V_{(i-1)j\ell}\right) \\
& + \sum_{j=k+m-i+1}^{i-1} b_{\circ j} \left(V_{i\ell i} - V_{(i-1)\ell(\ell+i-m-1)}\right. \\
& \left. + \sum_{\ell=i+j-m}^{j} \left(V_{ij\ell} - V_{(i-1)j\ell}\right)\right) \\
& + \sum_{j=i}^{m-1} b_{\circ j} \left(V_{i\ell i} - V_{(i-1)\ell(\ell+i-m-1)}\right. \\
& \left. + \sum_{\ell=i+j-m}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell}\right)\right).
\end{aligned}
\tag{106}
$$

As before, $V_{imi} - V_{(i-1)m(i-1)} = 0$ by Lemma 8. Hence

$$
\frac{\partial c_k}{\partial a_i} = B_1 + B_2 + B_3 \tag{107}
$$

where

$$
B_1 = \sum_{j=k}^{k+m-i} b_{\circ j} \sum_{\ell=k}^{j} \left(V_{ij\ell} - V_{(i-1)j\ell}\right) \tag{108}
$$

$$
\begin{aligned}
B_2 = {} & \sum_{j=k+m-i+1}^{i-1} b_{\circ j} \left(V_{i\ell i} - V_{(i-1)\ell(\ell+i-m-1)}\right. \\
& \left. + \sum_{\ell=i+j-m}^{j} \left(V_{ij\ell} - V_{(i-1)j\ell}\right)\right)
\end{aligned}
\tag{109}
$$

$$
\begin{aligned}
B_3 = {} & \sum_{j=i}^{m-1} b_{\circ j} \left(V_{i\ell i} - V_{(i-1)\ell(\ell+i-m-1)}\right. \\
& \left. + \sum_{\ell=i+j-m}^{i-1} \left(V_{ij\ell} - V_{(i-1)j\ell}\right)\right).
\end{aligned}
\tag{110}
$$

We need to show that B_1, B_2 and B_3 are nonnegative. For B_1, $j - \ell \leq m - i$, hence, by Lemma 7, $B_1 \geq 0$. The fact that $B_2 > 0$ and $B_3 > 0$ is proven exactly in the same way as for A_4.

Finally, given that B_1, B_2 and B_3 are nonnegative, $\frac{\partial c_k}{\partial a_i} > 0$ for $i > m + k - i + 1$.

For the general variable node operation $\boxdot^{d_v-1}$, we do the following. Consider the implicitly defined vector function $c = h(a, b)$ given by (67). Using this, we define the recursion $h^t(a, b) = h(a, h^{t-1}(a, b))$ starting from $h^1(a, b) = h(a, b)$. From the fact that c_k is a non-decreasing function of a_i and b_i it follows that the Jacobian derivatives $\frac{\partial h(a,b)}{\partial a}$ and $\frac{\partial h(a;b)}{\partial b}$ are nonnegative matrices. Using the recursion defined above, one can show that the Jacobian derivative of $h^t(a)$ is a nonnegative matrix because it is the sum of products of nonnegative matrices. Therefore, $h^{d_v-1}(a, b)$ is increasing in

a. Hence, $f(y; \varepsilon)$ is increasing in y, i.e., if $y_1 \preceq y_2$ then $f(y_1; \varepsilon) \preceq f(y_2; \varepsilon)$

The proof for the monotonicity of $g(x)$ follows the same lines.

APPENDIX C
DERIVATIVE OF $U(x; \varepsilon)$

We compute the derivative of $U(x; \varepsilon)$ with respect to x,

$$
U'(x; \varepsilon) = \frac{\partial}{\partial x} \left(g(x) D x^\mathsf{T} - G(x) - F(g(x); \varepsilon)\right) \tag{111}
$$

We consider separately the derivatives of the three terms,

1)

$$
\begin{aligned}
\frac{\partial}{\partial x} \left(g(x)\right) \left(D x^\mathsf{T}\right) &= g(x) \frac{\partial D x^\mathsf{T}}{\partial x} + \left(D x^\mathsf{T}\right)^\mathsf{T} \frac{\partial g(x)}{\partial x} \\
&= g(x) D + x D^\mathsf{T} g'(x)
\end{aligned}
\tag{112}
$$

2)

$$
\frac{\partial G}{\partial x} = g(x) D \tag{113}
$$

3)

$$
\frac{\partial F}{\partial x} = f(g(x); \varepsilon) D g'(x) \tag{114}
$$

Assuming D symmetric, i.e., $D = D^\mathsf{T}$, substituting (112)–(114) in (111) we obtain (18).

APPENDIX D
PROOF OF THEOREM 2

We compute the partial derivative of the three terms in (19).
1) Derivative of $\mathrm{Tr}(G(X) D X^\mathsf{T})$. First note that

$$
\mathrm{Tr}(G(X) D X^\mathsf{T}) = \sum_{j=1}^{L} [G(X) D]_j \, x_j^\mathsf{T} = \sum_{j=1}^{L} g(x_j) D x_j^\mathsf{T}.
\tag{115}
$$

We will use the following lemma.

Lemma 9. *Let $g(x_i)$ and $s(x_i)$ be two $1 \times m$ vectors. Define*

$$
\begin{aligned}
\frac{\partial g(x_i)}{\partial x_i} &= \left(\frac{\partial [g(x_i)]_k}{\partial x_{i\ell}}\right)_{k=1,\ldots,m, \ \ell=1,\ldots,m} \\
\frac{\partial s(x_i)}{\partial x_i} &= \left(\frac{\partial [s(x_i)]_k}{\partial x_{i\ell}}\right)_{k=1,\ldots,m, \ \ell=1,\ldots,m}.
\end{aligned}
$$

Then,

$$
\frac{\partial}{\partial x_i} g(x_i) s(x_i)^\mathsf{T} = s(x_i) \frac{\partial g(x_i)}{\partial x_i} + g(x_i) \frac{\partial s(x_i)^\mathsf{T}}{\partial x_i}.
$$

The proof of the lemma is omitted for brevity.

Applying Lemma 9 to (115) with $g(x_j)$ and $s(x_j) = (D x_j^\mathsf{T})^\mathsf{T} = x_j D^\mathsf{T}$, and taking into account that

$$
\frac{\partial D x_j^\mathsf{T}}{\partial x_j} = \left(\frac{\partial [D x_j^\mathsf{T}]_k}{\partial x_{j\ell}}\right)_{k=1,\ldots,m, \ \ell=1,\ldots,m} = D
$$

we obtain

$$
\frac{\partial}{\partial x_j} \mathrm{Tr}(G(X) D X^\mathsf{T}) = x_j D G_\mathrm{d}(x_j) + g(x_j) D.
$$

where we have used the fact that $\boldsymbol{D}^{\mathsf{T}} = \boldsymbol{D}$ if $\boldsymbol{D}$ is symmetric.

2) Derivative of $G(\boldsymbol{X})$. It is easy to see that $\frac{\partial G(\boldsymbol{X})}{\partial \boldsymbol{x}_j} = \boldsymbol{g}(\boldsymbol{x}_j)\boldsymbol{D}$.

3) Derivative of $F(\boldsymbol{AG}(\boldsymbol{X}); \varepsilon)$. Let $\boldsymbol{Y} = \boldsymbol{AG}(\boldsymbol{X})$. Then

$$\frac{\partial}{\partial \boldsymbol{x}_i} F(\boldsymbol{Y}; \varepsilon) = \sum_{j=1}^{L} \frac{\partial}{\partial \boldsymbol{x}_i} F(\boldsymbol{y}_j; \varepsilon)$$

$$= \sum_{j=1}^{L} \left[\frac{\partial}{\partial \boldsymbol{x}_{i1}} F(\boldsymbol{y}_j; \varepsilon), \ldots, \frac{\partial}{\partial \boldsymbol{x}_{im}} F(\boldsymbol{y}_j; \varepsilon) \right]$$

Note that

$$\frac{\partial F(\boldsymbol{y}_j; \varepsilon)}{\partial x_{i\ell}} = \sum_{n=1}^{m} \frac{\partial F(\boldsymbol{y}_j; \varepsilon)}{\partial y_{jn}} \frac{\partial y_{jn}}{\partial x_{i\ell}}. \qquad (116)$$

Define the matrix $\boldsymbol{B} = \frac{\partial F(\boldsymbol{Y}; \varepsilon)}{\partial \boldsymbol{y}}$ such that its (j, m)-th entry $[\boldsymbol{B}]_{j,n} = B_{jn} = \frac{\partial F(\boldsymbol{y}_j; \varepsilon)}{\partial y_{jn}}$. By definition $\boldsymbol{B} = \boldsymbol{f}(\boldsymbol{Y}; \varepsilon)\boldsymbol{D}$ and $B_{jn} = [\boldsymbol{f}(\boldsymbol{y}_j; \varepsilon)\boldsymbol{D}]_{j,n}$. Now let us find $\frac{\partial y_{jn}}{\partial x_{i\ell}}$. As

$$y_{jn} = [\boldsymbol{AG}(\boldsymbol{X})]_{j,n} = \sum_{t=1}^{L} A_{jt}[\boldsymbol{G}(\boldsymbol{X})]_{t,n}$$

we can write

$$\frac{\partial y_{jn}}{\partial x_{il}} = \sum_{t=1}^{L} A_{jt} \frac{\partial [\boldsymbol{G}(\boldsymbol{X})]_{tn}}{\partial x_{i\ell}}$$

$$\overset{(a)}{=} A_{ji} \frac{\partial [\boldsymbol{G}(\boldsymbol{X})]_{in}}{\partial x_{i\ell}} \overset{(b)}{=} A_{ji} [\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}_i)]_{n,\ell}$$

where $A_{jt} = [\boldsymbol{A}]_{j,t}$ and (a) follows from the fact that the only non-zero term in the sum over t is for $t = i$, and (b) follows from the definition of $\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}_i)$, $\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}_i) = \left(\frac{\partial [\boldsymbol{g}(\boldsymbol{x}_i)]_k}{\partial x_{i\ell}} \right)_{k=1,\ldots,m,\ \ell=1,\ldots,m}$. Therefore, (116) becomes

$$\frac{\partial F_j(\boldsymbol{y}_j; \varepsilon)}{\partial x_{i\ell}} = A_{ji} \sum_{n=1}^{m} B_{jn} [\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}_i)]_{n,l}$$

and

$$\frac{\partial}{\partial \boldsymbol{x}_i} F(\boldsymbol{Y}; \varepsilon) = \sum_{j=1}^{L} \left[\frac{\partial}{\partial \boldsymbol{x}_{i1}} F(\boldsymbol{y}_j; \varepsilon), \ldots, \frac{\partial}{\partial \boldsymbol{x}_{im}} F(\boldsymbol{y}_j; \varepsilon) \right]$$

$$= \sum_{j=1}^{L} A_{ji} \left[\sum_{n=1}^{m} B_{jn} [\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}_i)]_{n,1}, \ldots, \sum_{n=1}^{m} B_{jn} [\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}_i)]_{n,m} \right]$$

$$= \sum_{j=1}^{L} A_{ji}[\boldsymbol{B}]_j \boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}_i) = [\boldsymbol{A}^{\mathsf{T}}]_i \boldsymbol{B}\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}_i).$$

Finally, we obtain

$$\frac{\partial}{\partial \boldsymbol{x}_i} F(\boldsymbol{AG}(\boldsymbol{X}); \varepsilon) = [\boldsymbol{A}^{\mathsf{T}}]_i \boldsymbol{F}(\boldsymbol{AG}(\boldsymbol{X}); \varepsilon)\boldsymbol{D}\boldsymbol{G}_{\mathrm{d}}(\boldsymbol{x}_i).$$

References

[1] S. Kudekar, T. J. Richardson, and R. L. Urbanke, "Threshold saturation via spatial coupling: Why convolutional LDPC ensembles perform so well over the BEC," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 803–834, Feb. 2011.

[2] S. Kudekar, C. Méasson, T. J. Richardson, and R. L. Urbanke, "Threshold saturation on BMS channels via spatial coupling," in *Proc. 6th Int. Symp. Turbo Codes & Iterative Inf. Processing (ISTC)*, Sep. 2010.

[3] A. Yedla, Y.-Y. Jian, P. S. Nguyen, and H. D. Pfister, "A simple proof of Maxwell saturation for coupled scalar recursions," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6943–6965, Nov. 2014.

[4] ——, "A simple proof of threshold saturation for coupled scalar recursions," in *Proc. 7th Int. Symp. Turbo Codes & Iterative Inf. Processing (ISTC)*, Aug. 2012.

[5] S. Kumar, A. J. Young, N. Macris, and H. D. Pfister, "Threshold saturation for spatially coupled LDPC and LDGM codes on BMS channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7389–7415, Dec 2014.

[6] C. Schlegel and M. Burnashev, "Thresholds of spatially coupled systems via lyapunov's method," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Sep. 2013.

[7] M. C. Davey and D. J. C. MacKay, "Low density parity check codes over GF(q)," in *Proc. Inf. Theory Workshop (ITW)*, Jun. 1998.

[8] V. Rathi and R. L. Urbanke, "Density evolution, thresholds and the stability condition for non-binary LDPC codes," *IEE Proc. Commun.*, no. 6, pp. 1069–1074, Dec. 2005.

[9] H. Uchikawa, K. Kasai, and K. Sakaniwa, "Design and performance of rate-compatible non-binary LDPC convolutional codes," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E94-A, no. 11, pp. 2135–2143, Nov. 2011.

[10] A. Piemontese, A. Graell i Amat, and G. Colavolpe, "Nonbinary spatially-coupled LDPC codes on the binary erasure channel," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013.

[11] A. Yedla, Y.-Y. Jian, P. Nguyen, and H. Pfister, "A simple proof of threshold saturation for coupled vector recursions," in *Proc. Inf. Theory Workshop (ITW)*, Sep. 2012, pp. 25–29.

[12] A. Yedla, Y.-Y. Jian, P. S. Nguyen, and H. D. Pfister, "A simple proof of threshold saturation for coupled vector recursions," 2012. [Online]. Available: http://arxiv.org/abs/1208.4080/

[13] C. Measson, 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.

[14] P. Razaghi and W. Yu, "Bilayer low-density parity-check codes for decode-and-forward in relay channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3723–3739, Oct. 2007.