On the Error Exponent and the Use of LDPC Codes for Cooperative Sensor Networks with Misinformed Nodes

Zhiyu Yang and Lang Tong†

***Abstract*— The problem of retrieving information by a mobile access point from a sensor network where sensors cooperatively transmit messages using a common codebook is considered. It is assumed that there is a probability that a sensor is misinformed with a wrong message, which complicates the information retrieval process. The access point uses the capacity achieving stay-k scheduler that schedules a sensor to transmit for k consecutive code-letters before switching to a new sensor. The random coding exponent is derived as a function of k, and it is shown that there is an optimal k that gives the largest error exponent. The application of LDPC codes is considered next. It is shown in simulations that the optimal k of the stay-k scheduler for LDPC codes can be inferred from that for the random coding exponent.**

I. INTRODUCTION

We consider the problem of extracting information from a large sensor network in which sensors cooperatively deliver messages to a mobile access point using a common codebook. If all collaborating sensors have agreed on a message, each sensor may transmit some part of the codeword that corresponds to the agreed message according to some schedule. In such a way, errors caused by channel noise can be corrected at the access point. Between the access point and the cooperative sensor network, there is a maximum achievable rate $C^{(0)}$ of information retrieval, below which the detection error at the access point can be made arbitrarily small by making the codeword length sufficiently long.

But for large sensor networks in which sensors are distributed geographically and inexpensive with limited transmission and processing power, making all sensors agree on a common message is not easy. It is thus inevitable that some sensors will be mistaken on the message that is to be delivered cooperatively. Not knowing their mistakes, these misinformed sensors will transmit signals corresponding to the wrong codewords. The capacity of the sensor network with misinformed nodes is the maximum achievable rate C of information retrieval in the presence of not only channel noise but also sensor mistakes. Referred to as the capacity of the network with misinformed sensors, C is expected to be less than $C^{(0)}$.

†Corresponding author.

This work was supported in part by the Army Research Laboratory CTA on Communications and Networks under Grant DAAD19-01-2-0011, the National Science Foundation under Contract CNS-0435190, and the National Science Foundation under Contract CCR-0311055.

Z. Yang is with Marvell Semiconductor Inc., Santa Clara, CA 95054 USA (e-mail: zyang@marvell.com). L. Tong is with the School of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14853 USA (e-mail: ltong@ece.cornell.edu).

In characterizing the capacity C or in designing practical coding schemes that are capable of coping with both channel and sensor errors, it may seem, at first glance, that sensor errors can be modeled as part of the channel. This is not the case; the errors produced by misinformed sensors depend on the correct message and the codebook used by the cooperating sensors, which is different from the way errors caused by channel noise are generated.

We consider the case when sensors cooperate under a predetermined schedule, *i.e.*, the sensor activation sequence does not adapt to the previous receptions. At the ith interval, the mobile access point may choose randomly a sensor, and ask it to transmit the ith letter of the message codeword. Any sensor asked by the access point for transmission has a probability of β being misinformed. More generally, the access point may use the so-called stay-k scheduling, asking a sensor to transmit the next k consecutive letters of the codeword. It is shown in [1] that the capacity of the sensor network when the sensor error probability is β is $C = (1-\beta)C^{(0)}$, and the stay-k scheduling used by the access point achieves the capacity as $k \to \infty$.

In this paper, we treat the coding aspect of information retrieval assuming that the codebook used has a rate R below the capacity. For the fixed code rate R, we are interested in designing the parameter k of the stay-k scheduling so that the decoder has the fastest decay rate of error probability. To this end, we first derive the random coding error exponent as a function of rate R and the scheduling parameter k. We show next that, for any $R < C$, the error exponent approaches to zero as $k \to \infty$, which means that, in contrast to the capacity achieving strategy, there is an optimal k^* that the access point should ask a randomly chosen sensor to transmit consecutive code-letters. Finally, we consider the use of an LDPC code, which has been shown to approach channel capacity closely, [2] and the references therein. We assume that stay-k scheduling is used. The performance of the LDPC code is simulated. It is shown that the bit error rate (BER) versus k resembles the random coding exponent versus k. Thus it makes practical sense to use the random coding exponent, which can be calculated easily, to find a good k for practical LDPC codes.

The problem considered in this paper was originally formulated in [1] where capacities of cooperative sensor network with misinformed sensors are analyzed under a number of settings. In this paper, we are not interested in capacity achieving schemes. We focus instead on a more practical

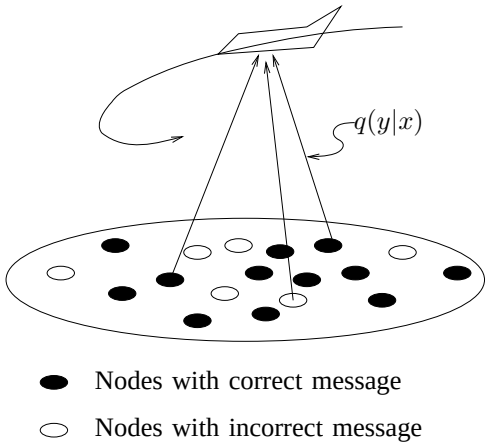

Fig. 1. Cooperative SEnsor Networks with Mobile Access (C-SENMA).

issue: when practical coding schemes such as the LDPC codes are used, what is the best stay-k strategy that makes detection error probability decay the fastest. The practical implication is that an optimized scheduling will require a less number of transmissions from the sensors for a prescribed error probability.

The idea of cooperation among nodes for the purpose of delivering information reliably and efficiently has attracted much attention in recent years. See, for example, [3]–[7]. Cooperation can be made at different levels: a collection of nodes collaborating at the signal level, transmitting as if they are part of an antenna array and beaming a common message to the receiving node [6]. Nodes can also collaborate using information theoretic strategies [4], jointly encoding information and delivering the message at a rate that ensures reliable recovery at the receiver. Our setup is different from existing ones in several aspects. First, we are not considering a source transmitting a sequence of messages in time. For the sensor network application, we assume that sensors cooperate to transmit a single message. Thus coding in our case is done across sensors (instead of over time), and each sensor transmits only part of the codeword (instead of the entire codeword). Second, we model explicitly the cooperation error, which has been mostly ignored in the literature.

This paper is organized as follows. We present the system model and definitions in Section II. The main theoretical results are presented in in Section III where we derive the random coding exponent and show the existence of the optimal stay-k scheduling. The implementation of LDPC is discussed in Section IV, and simulation results are presented in Section V.

II. Model and Definitions

The problem of information retrieval from a Cooperative SEsor Network with a Mobile Access point (C-SENMA) is illustrated in Fig. 1 where infinite number of nodes[1] are geographically distributed, and a mobile access point (fusion center) is capable of scheduling sensors to transmit. By assuming the mobility of the access point we imply that a sufficiently large number of sensors can be made to transmit. Some of the nodes are assumed to be misinformed.

The communication of a uniformly distributed global message $W \in \{1, \ldots, M\}$ from the network to the mobile access point has three phases: (a) orientation, (b) information retrieval by scheduling sensors to transmit, (c) decoding at the mobile access point.

A. Orientation and Sensor Error Models

In the first phase, nodes are informed with the global message $W \in \{1, \ldots, M\}$. We assume that each node receives the global message correctly with a certain probability and the reception is independent of other nodes. Specifically, the state of node i is represented by a Bernoulli random variable U_i with $U_i = 1$ indicating that sensor i has the correct global message and $U_i = 0$ otherwise. We assume that U_i's and W are jointly independent, and U_i's are independent and identically distributed (i.i.d.) across sensors with distribution

$$p(u_i) = \begin{cases} \beta & \text{if } u_i = 0 \\ 1-\beta & \text{if } u_i = 1 \end{cases}$$

where $\beta \in [0, 1]$ is a constant that controls the reception of the global message by individual nodes and is referred to as the *orientation error probability* of the network.

Let $\widetilde{W}_i$ be the message obtained at sensor i after the orientation process. When $U_i = 1$, the sensor has no error, and $\widetilde{W}_i = W$. Otherwise, we assume that $\widetilde{W}_i$ is uniformly distributed from 1 to M. Thus

$$p(\tilde{w}_i \big| w, u_i) = \begin{cases} \delta(\tilde{w}_i, w) & \text{if } u_i = 1 \\ \frac{1}{M} & \text{if } u_i = 0 \end{cases}$$

where $\delta(a, b)$ is equal to 1 if $a = b$, or 0 otherwise.

B. Scheduling and Channel Model

The mobile access point comes to retrieve information from the field after the information orientation has been accomplished. In the information retrieval phase, only one node is scheduled to transmit at any time slot. The scheduling is predetermined in the sense that the sequence of transmitting nodes does not depend on the channel outputs. This scheduling can be programmed before the deployment of the sensors, and it does not require a polling channel from the mobile access point.

During the information retrieval phase, one node is scheduled to transmit one symbol at each time slot: at time t, node K_t transmits the tth code letter of the codeword corresponding to its local message $\widetilde{W}_{K_t}$. The stay-k scheduling schedules a sensor to transmit k consecutive code letters before choosing the next sensor.

The uplink channels from each node to the receiver are assumed to be identical and are modeled by a discrete memoryless channel (DMC) $\{\mathcal{X}, \mathcal{Y}, q(y\big|\, x)\}$, where $\mathcal{X}$ and $\mathcal{Y}$ are the input and output alphabets respectively, and $q(y\big|\, x)$ is the transition probability of the channel.

[1]The large network assumption is necessary for a non-zero capacity since, if the network has only finite nodes, there is a positive probability that all the nodes are misinformed.

C. Error Probability, Achievable Rate, and Capacity

Let X_t and Y_t denote the input and output of the DMC from the scheduled sensor to the access point at time t. Let n be the number of slots the mobile access point spends to retrieve information from the field. The mobile access point decodes the global message based on the channel outputs Y^n and the scheduling K^n. The *rate* of a codebook is defined as $R \triangleq \log(M)/n$, where M is the number of messages in the codebook and n is the length of a codeword.

The decoded message is denoted by $\hat{W} \in \{1, \ldots, M\}$. An decoding error occurs if $\hat{W} \neq W$, and the *probability of error* is defined as $P_e \triangleq \mathcal{P}(\hat{W} \neq W)$, where $W \in \{1, \cdots, M\}$ is uniformly distributed.

A rate R is called *achievable* if for any given error $\epsilon > 0$, there exist a scheduling K^n, a codebook with a rate larger than $R - \epsilon$ and probability of error less that ϵ. The *capacity* of a system configuration is defined as the maximum of all achievable rates for the system configuration.

It has been shown in [1] that the capacity of C-SENMA is given by

$$C = (1 - \beta)C^{(0)}.$$

While this result is intuitive in the sense that roughly a β fraction of the transmissions are wasted by misinformed sensors, the proof is not trivial. Using the random coding argument, it is shown that, as $k \to \infty$, the stay-k scheduling along with the codebook generated from an optimally chosen distribution achieves the capacity [1]. Thus, to optimize the achievable rate, the optimal k is infinity in the stay-k scheduling family.

For a fixed code rate and a given codeword length, to minimize the error probability, the optimal k among the stay-k scheduling family need not to be infinity. In this work, we derive a random error exponent for C-SENMA with stay-k scheduling. We make connection between the optimal k for a random coding exponent and that for LDPC codes via simulations.

III. Random Coding Exponent

In this section, we derive a random coding exponent for C-SENMA when using the family of stay-k scheduling. We first define the codebook ensemble of interest. An (n, R) codebook is a matrix in $\mathcal{X}^{2^{nR} \times n}$, each row representing a codeword. For a given k, assume n is a multiple of k. An (n, R) codebook is said to be generated from distribution $Q^{(k)}(s^k)$ if every k consecutive entries in each row of the codebook, viewed as a vector, are drawn from distribution $Q^{(k)}(s^k)$. When $k = 1$, we omit k and use $Q(s)$ as the notation.

Consider the stay-k scheduling. Let $\mathbb{C}$ be an (n, R) codebook. Let $s_i(\mathbb{C}, w)$ denote the ith symbol in the wth codeword of codebook $\mathbb{C}$. Let $s_a^b(\mathbb{C}, w) \triangleq [s_a(\mathbb{C}, w), \ldots, s_b(\mathbb{C}, w)]$. Let $\mathrm{f_r}(s^k, \mathbb{C}, j)$ be the frequency of symbol vector s^k in columns $(j-1)k+1$ to jk of codebook $\mathbb{C}$, *i.e.*,

$$\mathrm{f_r}(s^k, \mathbb{C}, j) = \frac{1}{M} \sum_{w=1}^{M} 1_{s^{jk}_{(j-1)k+1}(\mathbb{C}, w) = s^k}$$

where

$$M = 2^{nR},$$

and the indicator function 1_A is equal to 1 if the event A is true, or 0 otherwise. The probability of output y^n given that $\mathbb{C}$ is the codebook and w is the intended message is given by

$$p(y^n|\mathbb{C}, w) = \prod_{j=1}^{n/k} p_j\big(y^{jk}_{(j-1)k+1}|\mathbb{C}, w\big) \tag{1}$$

where

$$\begin{aligned} &p_j\big(y^{jk}_{(j-1)k+1}|\mathbb{C}, w\big) \\ &= (1-\beta) \prod_{i=(j-1)k+1}^{jk} q(y_i|s_i(\mathbb{C}, w)) \\ &\quad + \beta \sum_{s'^k \in \mathcal{X}^k} \mathrm{f_r}(s'^k, \mathbb{C}, j) \prod_{l=1}^{k} q(y_{(j-1)k+l}|s'_l). \end{aligned} \tag{2}$$

Equation (1) holds because, under the stay-k scheduling, $Y^{jk}_{(j-1)k+1}$'s for different j are independent given the codebook $\mathbb{C}$ and the message w. Equation (2) holds because, with probability $1-\beta$, the node scheduled to transmit in time slots from $(j-1)k+1$ to jk is well-informed, hence transmitting the vector $s^{jk}_{(j-1)k+1}(\mathbb{C}, w)$ to the DMC $q(y|x)$ in the k consecutive slots. With probability β, the node is misinformed, transmitting vector s'^k with probability $\mathrm{f_r}(s'^k, \mathbb{C}, j)$.

Notice that $p_j(y^{jk}_{(j-1)k+1}|\mathbb{C}, w)$ cannot be rewritten as a DMC with the intended transmission vector being $s^{jk}_{(j-1)k+1}(\mathbb{C}, w)$ because $p_j(y^{jk}_{(j-1)k+1}|\mathbb{C}, w)$ depends on the codebook frequencies $\mathrm{f_r}(s'^k, \mathbb{C}, j)$ besides the transmission vector $s^{jk}_{(j-1)k+1}(\mathbb{C}, w)$. Therefore, random coding exponent results developed for DMCs cannot be applied directly here.

We present a random coding exponent in the following proposition for C-SENMA with the stay-k scheduling. The idea is to introduce a DMC to which $p_j(y^{jk}_{(j-1)t+1}|\mathbb{C}, w)$ converges in probability. We then apply known random coding exponent results on the induced DMC and bound the difference of the error probabilities for the induced DMC and the original channel $p_j(y^{jk}_{(j-1)t+1}|\mathbb{C}, w)$.

Proposition 1: Consider C-SENMA using the stay-k scheduling and (n, R) codebooks generated from $Q^{(k)}(s^k)$. Suppose $R > 0$. Let $P_e(n, R, k)$ denote the average probability of error of C-SENMA with the stay-k scheduling, average over the codebook ensemble. Then the error exponent is lower bounded by

$$\lim_{n\to\infty} -\frac{1}{n} \log_2 P_e(n, R, k) \geq E_k(R, Q^{(k)})$$

where the random coding exponent

$$\begin{aligned} E_k(R, Q^{(k)}) = \max_{0 \leq \rho \leq 1} \Bigg(-\frac{1}{k} \log_2 \sum_{y^k \in \mathcal{Y}^k} \Big(\sum_{s^k \in \mathcal{X}^k} \\ q^{(k)}_{\mathrm{eq}}(y^k|s^k; Q^{(k)})^{\frac{1}{1+\rho}} Q^{(k)}(s^k) \Big)^{1+\rho} - \rho R \Bigg), \end{aligned} \tag{3}$$

and

$$q_{\text{eq}}^{(k)}(y^k|s^k;Q^{(k)}) = (1-\beta)\prod_{i=1}^{k} q(y_i|s_i) + \beta \sum_{s'^k\in\mathcal{X}^k} Q^{(k)}(s'^k)\prod_{i=1}^{k} q(y_i|s'_i).$$

Proof: See Appendix. □

The k to achieve the capacity must be unbounded as shown in [1]. The next proposition, however, indicates that the optimal k for the random coding exponent is finite.

Proposition 2: For $\beta > 0$ and all $R > 0$,

$$\lim_{k\to\infty} \max_{Q^{(k)}} E_k(R, Q^{(k)}) = 0.$$

Proof: Applying the inequality

$$q_{\text{eq}}^{(k)}(y^k|s^k;Q^{(k)}) \geq \beta \sum_{s'^k\in\mathcal{X}^k} Q^{(k)}(s'^k)\prod_{i=1}^{k} q(y_i|s'_i)$$

to (3), carrying out the summation over s^k, and cancelling the $\frac{1}{1+\rho}$ and $1+\rho$ exponents, we have

$$\begin{aligned}\max_{Q^{(k)}} E_k(R,Q^{(k)}) &\leq \max_{Q^{(k)}} \max_{0\leq\rho\leq 1}\Bigg(-\frac{1}{k}\log_2 \sum_{y^k\in\mathcal{Y}^k}\Big(\beta \cdot \sum_{s'^k\in\mathcal{X}^k} Q^{(k)}(s'^k)\prod_{i=1}^{k} q(y_i|s'_i)\Big) - \rho R\Bigg)\\ &= \max_{0\leq\rho\leq 1}\Big(-\frac{1}{k}\log_2\beta - \rho R\Big)\\ &= -\frac{1}{k}\log_2\beta\\ &\to 0 \qquad\qquad \text{as } k\to\infty.\end{aligned}$$

Since $E_k(R, Q^{(k)}) \geq 0$, the proof is completed. □

Next we consider a special case where the DMC associated with C-SENMA is a BSC with crossover probability ϵ, *i.e.*,

$$q(y|x) = \begin{cases} 1-\epsilon & \text{if } y = x,\\ \epsilon & \text{otherwise.}\end{cases} \tag{4}$$

Fixed the distribution $Q^{(k)}$ to be the uniform distribution over $\{0,1\}^k$, *i.e.*, $Q^{(k)}(s^k) = 2^{-k}$. Then (3) reduces to

$$E_k(R) = \max_{0\leq\rho\leq 1}\Bigg[\rho - \frac{1+\rho}{k}\log_2\Bigg(\sum_{i=0}^{k}\binom{k}{i}\Big(\frac{\beta}{2^k} + (1-\beta)\epsilon^{k-i}(1-\epsilon)^i\Big)^{\frac{1}{1+\rho}}\Bigg) - \rho R\Bigg]. \tag{5}$$

We will compare (5) with the bit error rate (BER) of LDPC codes in the simulations section. The LDPC decoding is described in the next section.

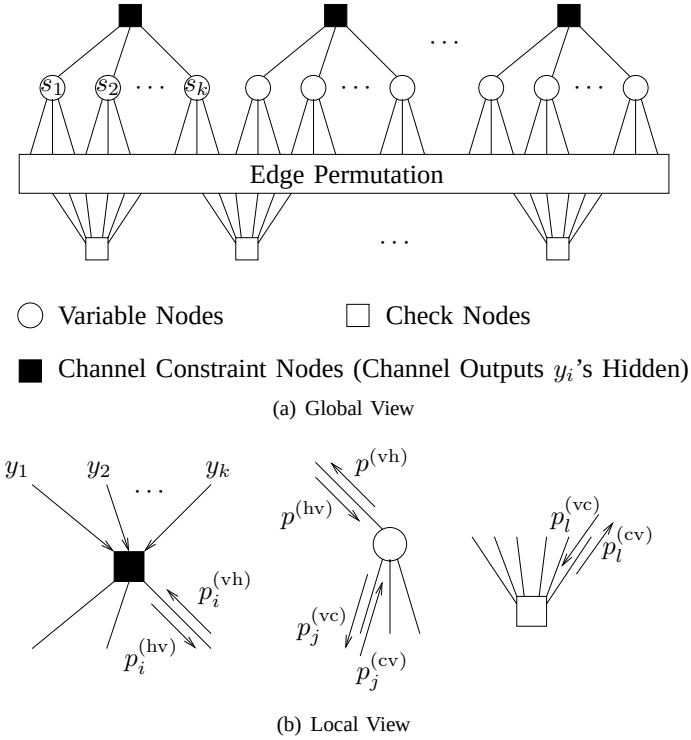

Fig. 2. Factor Graph.

IV. LDPC Decoding

In this section we describe an encoding/decoding scheme for C-SENMA with misinformed nodes where the associated DMC is the BSC with cross over probability ϵ as in (4). We use LDPC codes and the stay-k scheduling for transmission and information retrieval. To decode, we use the sum-product algorithm operating on the factor graph of the system illustrated in Fig. 2.

Fig. 2(a) is the global view of the the factor graph with the channel outputs y_i's hidden, while Fig. 2(b) depicts the local views of the factor graph centered at a channel constraint node, a variable node, and a check node, respectively. Let $p^{(\text{vh})}(\cdot)$ denote a message from a variable node to a channel constraint node: $p^{(\text{vh})}(s)$ is proportional to the *a posteriori* probability of the associated variable node being equal to s, $s = 0, 1$. Similarly, let $p^{(\text{hv})}(\cdot)$ denote a message from a channel constraint node to a variable node, $p^{(\text{vc})}(\cdot)$ a message from a variable node to a check node, $p^{(\text{cv})}(\cdot)$ a message from a check node to a variable node. In Fig. 2(b), all subscript indices are numbered with respect to the center note (channel constraint node, variable node, or check node). For example, $p_i^{(\text{vh})}(\cdot)$ and $p_i^{(\text{hv})}(\cdot)$ associated with the channel constraint node are the messages on the ith edge of the channel constraint note, $1 \leq i \leq k$. The indices are numbered locally with respect to the center note since it is easier in this way to express the updating rules for the sum-product algorithm.

The sum-product algorithm iteratively updates the messages $p^{(\text{hv})}$'s, $p^{(\text{cv})}$'s, $p^{(\text{vc})}$'s, and $p^{(\text{vh})}$'s in a batch fashion, *i.e.*, updating all messages in one category (for example, $p^{(\text{hv})}$) in the factor graph before updating messages in other categories. In one decoding iteration, all messages in the factor graph

are updated once. Next we will present the message updating rules.

Message updating rules in the sum-product algorithm are local optimal updating rules assuming all incoming messages are independent. Since the message exchange of the sum-product algorithm between variable nodes and check nodes for LDPC codes is well understood, we give the updating rules for $p^{(\mathrm{cv})}$'s, $p^{(\mathrm{vc})}$'s, and $p^{(\mathrm{vh})}$'s directly. For details, see *e.g.* [8].

To update $p^{(\mathrm{vc})}$'s and $p^{(\mathrm{vh})}$'s, for every variable nodes, calculate

$$p_j^{(\mathrm{vc})}(s) = p^{(\mathrm{hv})}(s) \cdot \prod_{h \neq j} p_h^{(\mathrm{cv})}(s) \tag{6}$$

$$p^{(\mathrm{vh})}(s) = \prod_{h} p_h^{(\mathrm{cv})}(s) \tag{7}$$

where $s = 0, 1$.

To update $p^{(\mathrm{cv})}$'s, for every check node, calculate

$$p_l^{(\mathrm{cv})}(s) = \sum_{\mathcal{S}_l(s)} \prod_{h \neq l} p_h^{(\mathrm{vc})}(s_h), \tag{8}$$

where $\mathcal{S}_l(s) \triangleq \{s_1, \ldots, s_{l-1}, s_{l+1}, \ldots, s_c : s_h \in \{0,1\} \text{ for } h \neq l, (\sum_{h \neq l} s_h + s) \mod 2 = 0\}$, and c is the number of edges of the check node. An efficient algorithm to calculate (8) has been discussed in [8].

Next we derive the updating rule for $p^{(\mathrm{hv})}$'s. Let $G \in \{0,1\}^{m \times n}$ denote the LDPC code generator matrix, where the rate of G is $R = m/n$. The codebook $\mathbb{C}$ consists of codewords

$$\{\mathbf{z}^T G \mod 2 : \mathbf{z}^T \in \{0,1\}^{1 \times m}\}.$$

Fix k. Let $G_j \in \{0,1\}^{m \times k}$ be the sub-matrix of G consisting of columns from $(j-1)k+1$ to jk. If G_j is of rank k, then the frequency of symbols $s^k \in \{0,1\}^k$ in the $((j-1)k+1)$th to the (jk)th columns of $\mathbb{C}$ is $1/2^k$, *i.e.*, $(\mathbf{z}^T G_i \mod 2)$ is uniformly distributed over $\{0,1\}^{1\times k}$ when $\mathbf{z}^T$ is uniformly distributed over $\{0,1\}^{1\times m}$. Assume that G_j is of rank k for all j. Therefore, $\mathrm{f_r}(s^k, \mathbb{C}, j) = 1/2^k$ for all j and all s^k. Hence, (2) reduced to a DMC

$$p_j\big(y_{(j-1)k+1}^{jk} | \mathbb{C}, w\big) = q_{\mathrm{LDPC}}\big(y_{(j-1)k+1}^{jk} | s_{(j-1)k+1}^{jk}(\mathbb{C}, w)\big)$$

where

$$q_{\mathrm{LDPC}}(y^k|s^k) = (1-\beta)\prod_{i=1}^{k} q(y_i|s_i) + \frac{\beta}{2^k}\prod_{i=1}^{k}\sum_{s'=0}^{1} q(y_i|s').$$

q_{LDPC} describes the channel constraint node in the factor graph Fig. 2(b).

To update $p^{(\mathrm{hv})}$'s, for every channel constraint node, calculate

$$\begin{aligned} p_i^{(\mathrm{hv})}(s) &= p(y^k | s_i = s) \\ &= \sum_{s^k : s_i = s} q_{\mathrm{LDPC}}(y^k|s^k) \prod_{h \neq i} p_h^{(\mathrm{vh})}(s_h) \qquad (9) \\ &= \sum_{s^k : s_i = s} \Big(\frac{\beta}{2^k} \prod_{i=1}^{k} \sum_{s'=0}^{1} q(y_i|s') \\ &\quad + (1-\beta) \prod_{i=1}^{k} q(y_i|s_i) \Big) \prod_{h \neq i} p_h^{(\mathrm{vh})}(s_h) \\ &= \frac{\beta}{2^k} + (1-\beta) q(y_i|s) \cdot \prod_{h \neq i} \sum_{s'=0}^{1} q(y_h|s') p_h^{(\mathrm{vh})}(s'), \qquad (10) \end{aligned}$$

where (9) uses the assumption that the incoming messages to the channel constraint node are independent, (10) uses the fact that $\sum_{s=0}^{1} q(y|s) = 1$, and $q(y|s)$ is given by (4).

To summarize, in each decoding iteration,

1) for every channel constraint node, use (10) to update all $p_i^{(\mathrm{hv})}$'s associated with the channel constraint node;
2) for every check node, use (8) to update all $p_l^{(\mathrm{cv})}$'s associated with the check node;
3) for every variable node, use (6) and (7) to update all $p_j^{(\mathrm{vc})}$'s and $p^{(\mathrm{vh})}$, respectively.

To prevent overflow or underflow, the messages should be normalized after update. For example, normalize $p^{(\mathrm{vh})}(s)$ by $p^{(\mathrm{vh})}(0) + p^{(\mathrm{vh})}(1)$.

V. Simulations

In the simulations, we use $(3, 6)$-regular LDPC codes, where variable nodes have degree 3, and check nodes have degree 6. The parity-check matrix is randomly generated and length-4 short circles are avoided. Each simulation point corresponds 10^6 messages, each consisting of nR information bits, where n is the codeword length and R is the code rate. Only information bits are counted toward the BER statistics. Each message is decoded up to 200 iterations in the sum-product algorithm.

Fig. 3 shows BER versus k when $R = 0.5$, $\beta = 0.14$, $\epsilon = 0.01$, and $n = 2048, 4096, 8192$. For $n = 8192$ and $k = 10, 20, 50$, no errors were detected during the trials of 10^6 messages. As shown in the simulation, k around 10 achieves the minimum BER. For comparison, we plot the random coding exponent (5). Fig. 4 shows $-E_k$ versus k under the same conditions. In Fig. 4, k slightly less than 10 achieves the minimum $-E_k$, hence achieving the maximum random coding exponent. It is interesting that the two plots have similar shapes, although the random coding exponent is derived for random codebooks drawn i.i.d. from Bernoulli$(\frac{1}{2})$ distribution.

Fig. 5 shows BER versus k when $R = 0.5$, $\beta = 0.03$, $\epsilon = 0.05$, and $n = 2048, 4096, 8192$. In this case, the BER is quite flat from $k = 1$ to $k = 100$. Similar shape is also observed in Fig. 6, which plots $-E_k$ versus k under the same conditions.

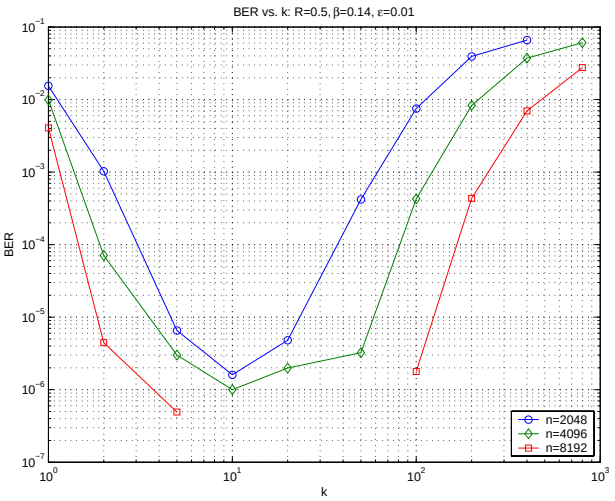

Fig. 3. BER versus k: $R = 0.5$, $\beta = 0.14$, $\epsilon = 0.01$, and $n = 2048, 4096, 8192$. For $n = 8192$ and $k = 10, 20, 50$, no errors were detected during the trials of 10^6 messages.

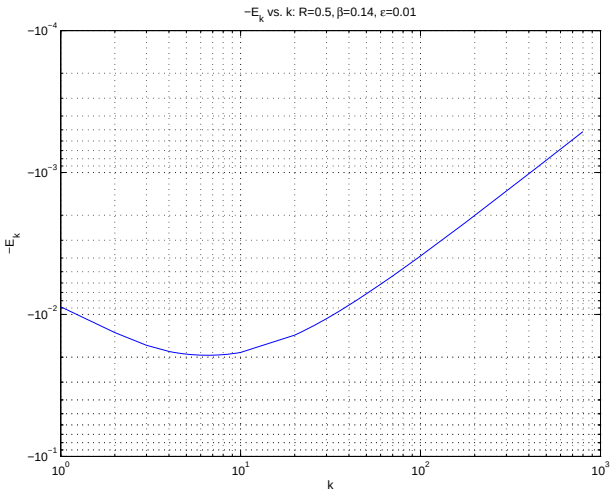

Fig. 4. $-E_k$ versus k: $R = 0.5$, $\beta = 0.14$, and $\epsilon = 0.01$.

The similarity of the BER curve and $-E_k$ indicates that, to search for a k that gives good performance in LDPC codes, we can start with a k that gives large random coding exponent, which is much easier to compute.

VI. Conclusion

In this work, we derive a random coding exponent for C-SENMA with the stay-k scheduling. It is shown that the random coding exponent converges to zero as k goes to infinity. Hence, in contrast to maximizing the achievable rate where the optimal k is infinity, the optimal k for the random coding exponent is finite. We also propose an LDPC coding scheme for C-SENMA. From simulation, a k that gives a large random coding exponent also gives good performance in the LDPC scheme. Hence, to search for a k that produces low BER in the LDPC scheme, we can start with a k that produces large random coding exponent, which is computationally inexpensive.

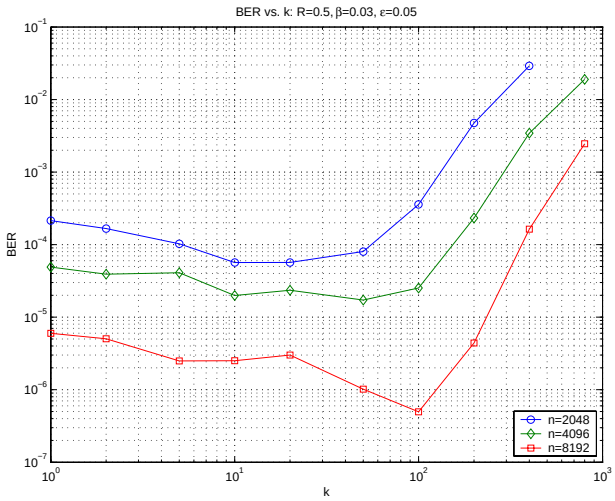

Fig. 5. BER versus k: $R = 0.5$, $\beta = 0.03$, $\epsilon = 0.05$, and $n = 2048, 4096, 8192$.

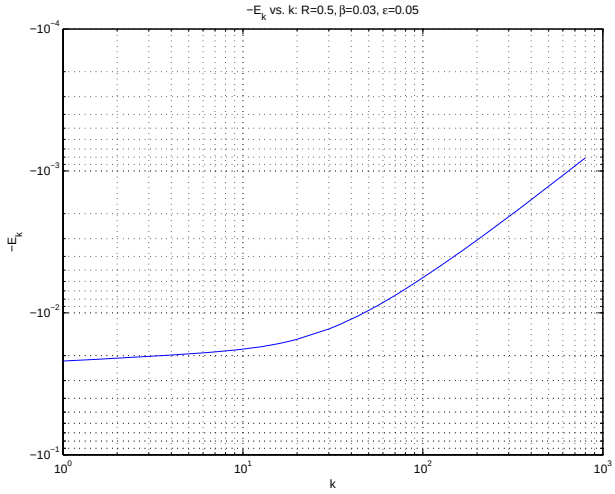

Fig. 6. $-E_k$ versus k: $R = 0.5$, $\beta = 0.03$, and $\epsilon = 0.05$.

Appendix
Proof of Proposition 1

We first prove the $k = 1$ case, and then extend the result to general k.

For $k = 1$, rewrite (1) and (2) as

$$p(y^n|\mathbb{C}, w) = \prod_{i=1}^{n} p_i(y_i|\mathbb{C}, w) \tag{11}$$

and

$$p_i(y_i|\mathbb{C}, w) = (1-\beta)q(y_i|s_i(\mathbb{C}, w)) + \beta \sum_{s' \in \mathcal{X}} \mathrm{f_r}(s', \mathbb{C}, i) q(y_i|s').$$

We will first introduce a DMC to which $p_j(y_i|\mathbb{C}, w)$ converges in probability. We will then apply known random coding results on the DMC and bound the difference of the error probabilities for the DMC and the original channel $p_j(y_i|\mathbb{C}, w)$. It will be shown that the error exponent for the original channel is the same as the induced DMC.

Assume that codebook $\mathbb{C}$ is generated from distribution $Q(s)$. Then as M goes to infinity, $\mathrm{f_r}(s', \mathbb{C}, i)$ converges to $Q(s')$ in probability. Hence, we introduce an "equivalent" DMC that is independent of the codebook $\mathbb{C}$,

$$q_{\mathrm{eq}}(y|s;Q) = (1-\beta)q(y|s) + \beta \sum_{s'\in\mathcal{X}} Q(s')q(y|s'),$$

where Q is included in the parameter set of q_{eq} to indicate the dependence of q_{eq} on Q. If we use the codebook $\mathbb{C}$ on the DMC q_{eq}, then the output probability is

$$p_{\mathrm{eq}}(y^n|\mathbb{C}, w) = \prod_{i=1}^{n} q_{\mathrm{eq}}(y_i|s_i(\mathbb{C}, w); Q). \tag{12}$$

Applying the random coding exponent on DMCs [9, Theorem 5.6.2] to the equivalent DMC, we have the following lemma:

Lemma 3: Fix $Q(s)$. Consider using (n, R) codebooks generated from $Q(s)$ and the maximum likelihood decoder over the equivalent DMC q_{eq}. Let $P_{e,\mathrm{eq}}(n, R)$ denote the average probability of error, averaged over the codebook ensemble,

$$P_{e,\mathrm{eq}}(n,R) = \sum_{\mathbb{C}} p(\mathbb{C}) \frac{1}{M} \cdot \sum_{w=1}^{M} \sum_{y^n\in\mathcal{Y}^n} p_{\mathrm{eq}}(y^n|\mathbb{C}, w)\delta_{\mathrm{eq}}(y^n, \mathbb{C}, w)$$

where $\delta_{\mathrm{eq}}(y^n, \mathbb{C}, w) = 0$ if the ML decoder makes no decoding error when $\mathbb{C}$ is the codebook, w is the message, and y^n is received; or $\delta_{\mathrm{eq}}(y^n, \mathbb{C}, w) = 1$ otherwise. Then

$$P_{e,\mathrm{eq}}(n,R) \le 2^{-nE_{\mathrm{eq}}(R,Q)}$$

where the random coding exponent

$$E_{\mathrm{eq}}(R,Q) = \max_{0\le\rho\le 1}\Bigg(-\log_2 \sum_{y\in\mathcal{Y}}\Big(\sum_{s\in\mathcal{X}} q_{\mathrm{eq}}(y|s;Q)^{\frac{1}{1+\rho}} \cdot Q(s)\Big)^{1+\rho} - \rho R\Bigg).$$

The next proposition states that the random coding exponent for C-SENMA is the same as that for the DMC $q_{\mathrm{eq}}(y|s;Q)$.

Proposition 4: Fix $Q(s)$. Consider C-SENMA using the stay-1 scheduling, (n, R) codebooks generated from $Q(s)$, and the ML decoder for the equivalent DMC q_{eq} as in Lemma 3. Suppose $R > 0$. Let $P_e(n, R, 1)$ denote the average probability of error of C-SENMA with the stay-1 scheduling, average over the codebook ensemble,

$$P_e(n,R,1) = \sum_{\mathbb{C}} p(\mathbb{C}) \frac{1}{M} \sum_{w=1}^{M} \sum_{y^n\in\mathcal{Y}^n} p(y^n|\mathbb{C}, w)\delta_{\mathrm{eq}}(y^n, \mathbb{C}, w).$$

Then the error exponent is lower bounded by

$$\lim_{n\to\infty} -\frac{1}{n}\log_2 P_e(n,R,1) \ge E_{\mathrm{eq}}(R,Q). \tag{13}$$

Proof: We first define a subset of the codebook space such that the probability of a randomly generated codebook not belonging to the subset is small. The subset is defined such that, for any codebook in the subset, (11) is very close to (12). Therefore, the probability of error of C-SENMA when using a codebook in the subset is close to that of the equivalent DMC q_{eq} when using the same codebook. In this way, we prove the error exponent of C-SENMA is equal to that of the equivalent DMC q_{eq}. The detailed proof is as follows.

Without lose of generality, assume that $Q(s) > 0$ for $1 \le s \le A$ and $Q(s) = 0$ for $s > A$. For $\delta > 0$, let $\mathcal{C}_\delta^{(n)}$ be a subset of (n, R) codebooks,

$$\mathcal{C}_\delta^{(n)} \triangleq \Big\{\mathbb{C} \in \mathcal{X}^{2^{nR}\times n} : \forall s \in \mathcal{X}, \forall i \in \{1,\dots,n\}, \mathrm{f_r}(s, \mathbb{C}, i) \le Q(s)(1+\delta)\Big\}.$$

If $\mathbb{C} \in \mathcal{C}_\delta^{(n)}$, then

$$\begin{aligned} p(y^n|\mathbb{C}, w) &= \prod_{i=1}^{n} p_i(y_i|\mathbb{C}, w) \\ &\le \prod_{i=1}^{n} (1+\delta) q_{\mathrm{eq}}(y_i|s_i(\mathbb{C}, w); Q) \\ &= (1+\delta)^n p_{\mathrm{eq}}(y^n|\mathbb{C}, w). \end{aligned} \tag{14}$$

Let $\mathbb{C}_r$ be a random (n, R) codebook generated with distribution $Q(s)$. The next lemma bounds the probability of $\mathbb{C}_r$ not in $\mathcal{C}_\delta^{(n)}$.

Lemma 5: For all integer $r > 1$, there exists a $K(Q, r) < \infty$ that only depends on Q and r, such that for all n, for all $0 < \delta < 1$, and for all $R > 0$,

$$\mathcal{P}_r\{\mathbb{C}_r \notin \mathcal{C}_\delta^{(n)}\} \le \frac{nAK(Q,r)}{\delta^{2r} 2^{rnR}}. \tag{15}$$

We first apply Lemma 5 to prove the proposition and postpone the proof of Lemma 5. The average probability of error is bounded as follows,

$$\begin{aligned} &P_e(n,R,1) \\ &\le \mathcal{P}_r\{\mathbb{C}_r \notin \mathcal{C}_\delta^{(n)}\} \\ &\quad + \sum_{\mathbb{C}\in\mathcal{C}_\delta^{(n)}} p(\mathbb{C}) \frac{1}{M} \sum_{w=1}^{M} \sum_{y^n\in\mathcal{Y}^n} p(y^n|\mathbb{C}, w)\delta_{\mathrm{eq}}(y^n, \mathbb{C}, w) \\ &\le \frac{nAK(Q,r)}{\delta^{2r}2^{rnR}} + (1+\delta)^n \\ &\quad \cdot \sum_{\mathbb{C}} p(\mathbb{C}) \frac{1}{M} \sum_{w=1}^{M} \sum_{y^n\in\mathcal{Y}^n} p_{\mathrm{eq}}(y^n|\mathbb{C}, w)\delta_{\mathrm{eq}}(y^n, \mathbb{C}, w) \quad (16) \\ &= \frac{nAK(Q,r)}{\delta^{2r}2^{rnR}} + (1+\delta)^n P_{e,\mathrm{eq}}(n,R) \\ &\le \frac{nAK(Q,r)}{\delta^{2r}2^{rnR}} + (1+\delta)^n 2^{-nE_{\mathrm{eq}}(R,Q)} \quad (17) \end{aligned}$$

where (16) is due to (14), and (17) due to Lemma 3.

Let $\delta = \frac{1}{n}$. The first term of (17) has exponent

$$\lim_{n\to\infty} \frac{1}{n}\log_2 \frac{nAK(Q,r)n^{2r}}{2^{rnR}} = -rR.$$

The second term in (17) has exponent

$$\lim_{n\to\infty} \frac{1}{n}\log_2\Big(\big(1+\frac{1}{n}\big)^n 2^{-nE_{\mathrm{eq}}(R,Q)}\Big) = -E_{\mathrm{eq}}(R,Q).$$

Based on the "largest-exponent-wins" principle [10, page 4], the right hand side of (17) has exponent

$$\lim_{n\to\infty}\frac{1}{n}\log_2\Big(\text{RHS of (17)}\Big)=\max(-rR,-E_{\rm eq}(R,Q)).$$

Therefore,

$$\begin{aligned}\lim_{n\to\infty}-\frac{1}{n}\log_2 P_e(n,R,1)&\geq\lim_{n\to\infty}-\frac{1}{n}\log_2\Big(\text{RHS of (17)}\Big)\\&=\min(rR,E_{\rm eq}(R,Q)).\end{aligned}$$

Because r can be arbitrarily large and $R>0$, we select r such that rR is greater than $E_{\rm eq}(R,Q)$. Thus, we obtain (13).

Next we present the proof of Lemma 5, and then the proof of Proposition 4 is complete.

Proof of Lemma 5: Since $\mathrm{f_r}(s,\mathbb{C}_r,i)$ is the frequency of symbol s in the ith column of codebook $\mathbb{C}_r$, whose entries are i.i.d., we have, from the independence of $\mathrm{f_r}(s,\mathbb{C}_r,i)$ for different i,

$$\begin{aligned}&\mathcal{P}_r\{\mathbb{C}_r\in\mathcal{C}_\delta^{(n)}\}\\&=\prod_{i=1}^n\mathcal{P}_r\Big\{\bigcap_{s\in\mathcal{X}}\Big\{\mathrm{f_r}(s,\mathbb{C}_r,i)\leq Q(s)(1+\delta)\Big\}\Big\}\\&=\Big(\mathcal{P}_r\Big\{\bigcap_{s\in\mathcal{X}}\Big\{\mathrm{f_r}(s,\mathbb{C}_r,1)\leq Q(s)(1+\delta)\Big\}\Big\}\Big)^n\\&=\Big(\mathcal{P}_r\Big\{\bigcap_{s=1}^A\Big\{\mathrm{f_r}(s,\mathbb{C}_r,1)\leq Q(s)(1+\delta)\Big\}\Big\}\Big)^n,\end{aligned}\tag{18}$$

where (18) holds because $\mathcal{P}_r\{\mathrm{f_r}(s,\mathbb{C}_r,1)=0\}=1$ for $s>A$.

Define

$$\delta_s\triangleq\frac{\delta}{\sum_{j=0}^{A-1}Q(A)^{-j}}\sum_{j=0}^{s-1}Q(A)^{-j}.$$

We have $0<\delta_1<\ldots<\delta_A=\delta$. Define

$$\mathcal{F}_s\triangleq\Big\{f:\Big|\frac{f}{Q(s)}-1\Big|\leq\delta_s\Big\}.$$

Let $B_{s,i}$, $1\leq i\leq M, 1\leq s\leq A$, be Bernoulli with mean

$$b_s\triangleq\frac{Q(s)}{\sum_{j=s}^A Q(j)}.$$

And assume that $B_{s,i}$'s are independent across i and s. For $1\leq s\leq A$, let

$$\begin{aligned}M_s&=M\Big(1-\sum_{j=1}^{s-1}F_j\Big),\\F_s&=\frac{1}{M}\sum_{i=1}^{M_s}B_{s,i}.\end{aligned}$$

It can be shown that the frequency vector $(\mathrm{f_r}(1,\mathbb{C}_r,1),\ldots,\mathrm{f_r}(A,\mathbb{C}_r,1))$ has the same joint distribution as $(F_1,\ldots,F_A)$. Therefore,

$$\begin{aligned}&\mathcal{P}_r\Big\{\bigcap_{s=1}^A\Big\{\mathrm{f_r}(s,\mathbb{C}_r,1)\leq Q(s)(1+\delta)\Big\}\Big\}\\&=\mathcal{P}_r\Big\{\bigcap_{s=1}^A\Big\{F_s\leq Q(s)(1+\delta)\Big\}\Big\}\\&\geq\mathcal{P}_r\Big\{\bigcap_{s=1}^A\Big\{\Big|\frac{F_s}{Q(s)}-1\Big|\leq\delta_s\Big\}\Big\}\qquad(19)\\&=\mathcal{P}_r\Big\{\bigcap_{s=1}^A\{F_s\in\mathcal{F}_s\}\Big\}\\&=\prod_{s=1}^A\mathcal{P}_r\Big\{F_s\in\mathcal{F}_s\Big|\bigcap_{j=1}^{s-1}\{F_j\in\mathcal{F}_j\}\Big\},\qquad(20)\end{aligned}$$

where (19) holds because $\delta_s\leq\delta$. For $1\leq s\leq A$,

$$\begin{aligned}&\mathcal{P}_r\Big\{F_s\in\mathcal{F}_s\Big|\bigcap_{j=1}^{s-1}\{F_j\in\mathcal{F}_j\}\Big\}\\&\geq\min_{\substack{f_j\in\mathcal{F}_j,\\1\leq j<s}}\mathcal{P}_r\Big\{F_s\in\mathcal{F}_s\Big|F_j=f_j,1\leq j<s\Big\}\qquad(21)\\&=\min_{\substack{f_j\in\mathcal{F}_j,\\1\leq j<s}}\mathcal{P}_r\Big\{\sum_{i=1}^{M(1-\sum_{j=1}^{s-1}f_j)}\frac{B_{s,i}}{M}\in\mathcal{F}_s\Big|F_j=f_j,1\leq j<s\Big\}\\&=\min_{\substack{f_j\in\mathcal{F}_j,\\1\leq j<s}}\mathcal{P}_r\Big\{\sum_{i=1}^{M(1-\sum_{j=1}^{s-1}f_j)}\frac{B_{s,i}}{M}\in\mathcal{F}_s\Big\}\qquad(22)\end{aligned}$$

where (21) holds because of the fact that, if $\mathcal{A}$ is an event, $\mathcal{B}$ is a set, and B is a random variable, then

$$\mathcal{P}_r\{\mathcal{A}|B\in\mathcal{B}\}\geq\min_{b\in\mathcal{B}}\mathcal{P}_r\{\mathcal{A}|B=b\},$$

(22) holds because $B_{s,1},B_{s,2},\ldots$ are independent of $F_1,\ldots,F_{s-1}$.

If $f_j\in\mathcal{F}_j,1\leq j<s$, then

$$\begin{aligned}1-\sum_{j=1}^{s-1}f_j&\leq1-\sum_{j=1}^{s-1}Q(j)(1-\delta_j)\\&\leq1-(1-\delta_{s-1})\sum_{j=1}^{s-1}Q(j)\qquad(23)\\&\leq\delta_{s-1}+\sum_{j=s}^{A}Q(j)\end{aligned}$$

where (23) holds because $\delta_j<\delta_{s-1}$ for $j<s$. Similarly,

$$1-\sum_{j=1}^{s-1}f_j\geq-\delta_{s-1}+\sum_{j=s}^{A}Q(j).$$

Therefore, if $f_j\in\mathcal{F}_j,1\leq j<s$, then

$$M\Big(1-\sum_{j=1}^{s-1}f_1\Big)\in\mathcal{M}_s\triangleq\Big\{m:\Big|\frac{m}{M}-\sum_{j=s}^{A}Q(j)\Big|\leq\delta_{s-1}\Big\}.$$

Hence,

$$\begin{aligned}
&\min_{\substack{f_j\in\mathcal{F}_j,\\ 1\le j<s}} \mathcal{P}_r\Big\{\sum_{i=1}^{M(1-\sum_{j=1}^{s-1}f_j)}\frac{B_{s,i}}{M}\in\mathcal{F}_s\Big\}\\
&\ge \min_{m\in\mathcal{M}_s}\mathcal{P}_r\Big\{\sum_{i=1}^{m}\frac{B_{s,i}}{M}\in\mathcal{F}_s\Big\}\\
&= \min_{m\in\mathcal{M}_s}\mathcal{P}_r\Big\{\Big|\frac{\sum_{i=1}^m B_{s,i}}{MQ(s)}-1\Big|\le\delta_s\Big\}\\
&\ge \min_{m\in\mathcal{M}_s}\mathcal{P}_r\Big\{\Big|\frac{\sum_{i=1}^m B_{s,i}}{MQ(s)}-\frac{m/M}{\sum_{j=s}^A Q(j)}\Big|\\
&\qquad\qquad\le\delta_s-\Big|\frac{m/M}{\sum_{j=s}^A Q(j)}-1\Big|\Big\}\\
&\ge \min_{m\in\mathcal{M}_s}\mathcal{P}_r\Big\{\Big|\frac{\sum_{i=1}^m B_{s,i}}{MQ(s)}-\frac{m/M}{\sum_{j=s}^A Q(j)}\Big|\\
&\qquad\qquad\le\delta_s-\frac{\delta_{s-1}}{\sum_{j=s}^A Q(j)}\Big\} \qquad (24)\\
&\ge \min_{m\in\mathcal{M}_s}\mathcal{P}_r\Big\{\Big|\frac{\sum_{i=1}^m B_{s,i}}{MQ(s)}-\frac{m/M}{\sum_{j=s}^A Q(j)}\Big|\le\delta_s-\frac{\delta_{s-1}}{Q(A)}\Big\}\\
&= \min_{m\in\mathcal{M}_s}\mathcal{P}_r\Big\{\Big|\sum_{i=1}^m(B_{s,i}-b_s)\Big|\le\delta_1 MQ(s)\Big\}\\
&\ge \min_{m\in\mathcal{M}_s}1-\frac{E[(\sum_{i=1}^m(B_{s,i}-b_s))^{2r}]}{(\delta_1 MQ(s))^{2r}} \qquad (25)
\end{aligned}$$

where (24) holds because $m\in\mathcal{M}_s$, and (25) because of Markov's Inequality when applied to $|\sum_{i=1}^m(B_{s,i}-b_s)|^{2r}$.

Since $E[B_{s,i}-b_s]=0$, it can be shown that there exists a $K_1(b_s,r)<\infty$ such that for all m,

$$E\Big[\Big(\sum_{i=1}^m(B_{s,i}-b_s)\Big)^{2r}\Big]\le K_1(b_s,r)m^r.$$

Let $K(Q,r)<\infty$ be a constant that only depends on Q and r such that

$$K(Q,r)\ge\max_{1\le s\le A}\frac{K_1(b_s,r)(1+1)^r(\sum_{j=0}^{A-1}Q(A)^{-j})^{2r}}{Q(s)^{2r}}.$$

Assuming $\delta\le 1$, we have

$$\begin{aligned}
&\min_{m\in\mathcal{M}_s}1-\frac{E[(\sum_{i=1}^m(B_{s,i}-b_s))^{2r}]}{(\delta_1 MQ(s))^{2r}}\\
&\ge\min_{m\in\mathcal{M}_s}1-\frac{K_1(b_s,r)m^r}{(\delta_1 MQ(s))^{2r}}\\
&\ge 1-\frac{K_1(b_s,r)M^r(\delta_{s-1}+\sum_{j=s}^A Q(j))^r}{(\delta_1 MQ(s))^{2r}}\\
&\ge 1-\frac{K(Q,r)}{\delta^{2r}M^r}. \qquad (26)
\end{aligned}$$

Combining (22), (25), and (26), and noticing that probability is non-negative, we have

$$\mathcal{P}_r\Big\{F_s\in\mathcal{F}_s\Big|\bigcap_{j=1}^{s-1}\{F_j\in\mathcal{F}_j\}\Big\}\ge 1-\min\Big(1,\frac{K(Q,r)}{\delta^{2r}M^r}\Big).$$

The above inequality, together with (18) and (20), gives

$$\begin{aligned}
\mathcal{P}_r\{\mathbb{C}_r\in\mathcal{C}_\delta^{(n)}\}&\ge\Big(1-\min\Big(1,\frac{K(Q,r)}{\delta^{2r}M^r}\Big)\Big)^{nA}\\
&\ge 1-nA\min\Big(1,\frac{K(Q,r)}{\delta^{2r}M^r}\Big) \qquad (27)\\
&\ge 1-\frac{nAK(Q,r)}{\delta^{2r}2^{rnR}} \qquad (28)
\end{aligned}$$

where (27) holds because of the fact that, if $0\le x\le 1$, then

$$(1-x)^n\ge 1-nx.$$

From (28), we obtain (15). □

□

With Proposition 4, we are ready to extend the random coding exponent result to general k and prove Proposition 1. Consider the kth extended C-SENMA where the associated DMC

$$q^{(k)}(y^k|x^k)=\prod_{i=1}^k q(y_i|x_i)$$

is the kth extended channel of the original DMC $q(y|x)$. The input and output alphabets are $\mathcal{X}^k$ and $\mathcal{Y}^k$, respectively. Use the (n,R) random codebooks generated from $Q^{(k)}(s^k)$ for the original system to the extended system: group every k symbols in a codeword and transmit them in one channel use to the kth extended system. The codebooks, viewed from the extended system, are $(n^{(k)},R^{(k)})$ codebooks, where

$$n^{(k)}=n/k,\qquad\qquad R^{(k)}=kR.$$

Let $P_e^{(k)}(n^{(k)},R^{(k)},1)$ denote the average probability of error of the kth extended C-SENMA when using the stay-1 scheduling and the $(n^{(k)},R^{(k)})$ codebooks. By Proposition 4, the error exponent of the kth extended C-SENMA with the stay-1 scheduling is bounded by

$$\lim_{n^{(k)}\to\infty}-\frac{1}{n^{(k)}}\log_2 P_e^{(k)}(n^{(k)},R^{(k)},1)\ge E_1^{(k)}(R^{(k)},Q^{(k)})$$

where

$$\begin{aligned}
&E_1^{(k)}(R^{(k)},Q^{(k)})\\
&=\max_{0\le\rho\le 1}\Big(-\log_2\sum_{y^k\in\mathcal{Y}^k}\Big(\sum_{s^k\in\mathcal{X}^k}\\
&\quad q_{\rm eq}^{(k)}(y^k|s^k;Q^{(k)})^{\frac{1}{1+\rho}}Q^{(k)}(s^k)\Big)^{1+\rho}-\rho R^{(k)}\Big). \qquad (29)
\end{aligned}$$

Now consider the original C-SENMA when using the stay-k scheduling and the (n,R) codebooks. It can be shown that

$$P_e(n,R,k)=P_e^{(k)}(n^{(k)},R^{(k)},1).$$

Therefore,

$$\begin{aligned}
\lim_{n\to\infty}-\frac{1}{n}\log_2 P_e(n,R,k)&=\lim_{n\to\infty}-\frac{1}{n}\log_2 P_e^{(k)}(\frac{n}{k},kR,1)\\
&\ge\frac{1}{k}E_1^{(k)}(kR,Q^{(k)}) \qquad (30)\\
&\triangleq E_k(R,Q^{(k)}).
\end{aligned}$$

Substituting (29) into (30) concludes the proof of (3). □

REFERENCES

[1] Z. Yang and L. Tong, "Cooperative sensor networks with misinformed nodes," to appear in *IEEE Trans. Inform. Theory*, Dec. 2005.

[2] S.-Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon Limit," *IEEE Communications Letters*, vol. 5, no. 2, pp. 58–60, Feb. 2001.

[3] J. N. Laneman and G. W. Wornell, "Distributed Space-Time-Coded Protocols for Exploiting Cooperative Diversity in Wireless Networks," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2415–2425, Oct. 2003.

[4] A. Sendonaris, E. Erkip, and B. Aazhang, "User Cooperation Diversity – Part I: System Description," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[5] ——, "User Cooperation Diversity – Part II: Implementation Aspects and Performance Analysis," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1939–1948, Nov. 2003.

[6] S. Cui, A. J. Goldsmith, and A. Bahai, "Energy-efficiency of MIMO and Cooperative MIMO Techniques in Sensor Networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 6, pp. 1089–1098, Aug. 2004.

[7] H. E. Gammal and D. Aktas, "Distributed Space-Time Filtering for Cooperative Wireless Networks," in *Proc. of IEEE GLOBECOM*, San Francisco, CA, Dec. 2003.

[8] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 399–431, March 1999.

[9] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY: John Wiley and Sons, Inc., 1968.

[10] F. den Hollander, *Large Deviations (Fields Institute Monographs, 14)*. American Mathematical Society, 2000.