

# Simple Capacity-Achieving Ensembles of Rateless Erasure-Correcting Codes

Xiaojun Yuan, *Member, IEEE*, Rong Sun, and Li Ping, *Senior Member, IEEE*

**Abstract**—This paper is concerned with a simple binary erasure-recovery coding scheme that falls into the family of so-called semi-random low-density-parity-check (SR-LDPC) codes. Based on a constrained random-scrambling technique, the proposed coding scheme is systematic, rateless, and capacity-achieving. We provide simulation examples comparing the new scheme with the well-known Luby Transform (LT) and raptor codes. It is shown that the new scheme has advantages in complexity and performance over its counterparts especially in channels with a relatively low erasure rate.

**Index Terms**—LT codes, raptor codes, tornado codes, SR-LDPC codes, rateless codes.

## I. INTRODUCTION

**R**ATELESS binary erasure codes have been studied for automatic retransmission and digital fountain applications [1][2]. A coding scheme is said to be rateless if it can generate coded bits potentially limitlessly and deliver good<sup>1</sup> performance without knowing the channel condition at the transmitter. Luby Transform (LT) and raptor codes are two well-known families of rateless codes which can asymptotically achieve the capacity of binary erasure channels.

An LT encoder [1] is based on a simple and elegant principle as follows. Suppose that the encoder is driven by  $K$  information bits to produce parity bits. Each parity bit is first assigned with a degree  $m$  randomly drawn from a given distribution. The value of each parity bit is the exclusive-or (XOR) of  $m$  randomly selected information bits. Since the parity bits are generated independently, LT codes can be expanded by adding extra parity bits without limitation and hence are rateless. The encoding and decoding complexities of LT codes (i.e., the number of XOR operations per bit in encoding and decoding, respectively) grow at least logarithmically with the number of information bits to ensure a vanishing bit error probability. The complexity can be reduced to be linear in the number

of information bits by concatenating a low-density parity-check (LDPC) precoder before the LT coding scheme [2]. The resulting concatenated codes are known as “raptor codes”.

Both LT and raptor codes are, in their straightforward forms, non-systematic. Only parity bits are transmitted, and so a decoding process is necessary regardless of the channel condition. Upon receiving a sufficient number (that is usually slightly larger than  $K$ ) of parity bits, the LT (or raptor) decoder applies an iterative process to recover the information bits. The same decoding process is required even for a perfect channel without any erasure, which implies unnecessary detection cost. To overcome this problem, a precoding technique is proposed in [2] for the design of systematic raptor codes. However, this technique increases the encoding complexity to  $O(K^2)$ , which motivates us to seek an alternative low-cost solution. LDPC codes [3]-[8] and the related irregular repeat-accumulate (IRA) codes [9][10] are powerful forward-error-control (FEC) codes. Conventionally, an LDPC code is defined on the kernel of a parity-check matrix  $\mathbf{H}$ , rather than directly on the image of a generator matrix. This implies that, for a randomly generated low-density  $\mathbf{H}$ , a small modification of  $\mathbf{H}$  (for rate adjustment) may result in a significantly different generation matrix, which violates the basic requirement of a rateless scheme. Puncturing techniques [4] have been studied recently to address this issue at the cost of a certain performance loss.

In this paper, we develop a family of rateless IRA codes for binary erasure channels using a scrambling technique. The new scheme is systematic, rateless, and capacity-achieving. Both the encoding and decoding complexities of the new scheme are linear with  $K$  (i.e.,  $O(K)$ ). Particularly, due to its systematic property, the encoding and decoding cost of the proposed scheme is trivial when no erasure occurs in transmission. These features are attractive for applications in transmission environments with rare erasure. For convenience of discussion, we henceforth refer to the proposed codes as semi-random LDPC (SR-LDPC) codes, following the nomenclature of [11].

## II. TORNADO CODES AND DEGREE SEQUENCES

This section outlines the basic principle of tornado codes [12]. The discussion will prove useful when we introduce our new scheme in the next section.

### A. Channel Models

The following channel models will be used in this paper.

- A *partial* erasure channel allows random erasures only on information bits.
- A *general* erasure channel allows random erasures on both information and parity bits.

Manuscript received July 28, 2005; revised February 1, 2008. This work was jointly supported by grants from the Research Grant Council of the Hong Kong SAR, China [Project No. CityU 1182/02E and CityU 117508].

Xiaojun Yuan was with the Department of Electrical Engineering, City University of Hong Kong, HK SAR. He is now with the Department of Electrical Engineering, University of Hawaii at Manoa, Hawaii, USA, 96822 (e-mail: xyuan24@hawaii.edu).

Rong Sun was with the Department of Electrical Engineering, City University of Hong Kong, HK SAR. She is now with the State Key Lab of ISN, Xidian University, Xi'an, 710071, P. R. China (e-mail: rsun@mail.xidian.edu.cn).

Li Ping is with the Department of Electrical Engineering, City University of Hong Kong, HK SAR (e-mail: eeliping@cityu.edu.hk).

Communicated by Ender Ayanoglu, Editor of *IEEE Transactions on Communications*.

<sup>1</sup>Loosely speaking, “good” means reasonably near-capacity (but not necessarily capacity-achieving) performance. Examples of good codes include turbo and low-density parity-check (LDPC) codes.

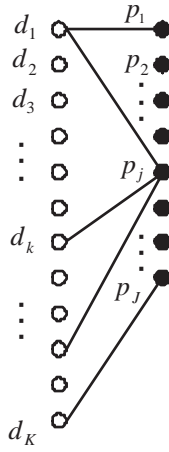


Fig. 1. The structure of a two-column tornado code.

### B. Tornado Codes

Fig. 1 illustrates a coding scheme, consisting of the first two columns of the tornado structure introduced in [12]. This scheme is referred to as a two-column tornado code in this paper. Nodes  $\{d_k\}$  in the left column of Fig. 1 are called information nodes which represent the information bits. They are connected to parity nodes  $\{p_j\}$  (which represent the parity bits) in the right column via edges, with the values of parity nodes determined by the following encoding rule<sup>2</sup>

$$p_j = \sum_{d_k \in B_j} d_k \pmod{2}, \quad j = 1, 2, \dots, J \quad (1)$$

where  $B_j = \{\text{all } d_k \text{ connected via edges to } p_j\}$ , and  $J$  is the number of parity nodes. In [12], optimal design rules are derived for a two-column tornado code over partial erasure channels. In a general erasure channel, extra protection on  $\{p_j\}$  is required. (For a detailed discussion, see [12].) The SR-LDPC code studied in this paper will be derived based on the two-column tornado code. Interestingly, the new coding structure does not require extra protection on the parity bits due to its “self-healing property”, as will be discussed later.

For the code in Fig. 1, the degree of a node is defined as the number of the edges connected to it. The left (respectively, right) degree of an edge is the degree of its left (respectively, right) node. Let  $\lambda_i$  (respectively,  $\rho_i$ ) be the fraction of edges with left (respectively, right) degree  $i$ . Define the left and right edge degree polynomials respectively as

$$\lambda(x) \equiv \sum_i \lambda_i x^{i-1} \quad \text{and} \quad \rho(x) \equiv \sum_i \rho_i x^{i-1}. \quad (2)$$

The following remark is a direct consequence of the above definitions.

*Remark 1:* The necessary and sufficient conditions for realizable  $\lambda(x)$  and  $\rho(x)$  are:

- (a)  $\lambda(x)$  and  $\rho(x)$  are polynomials with finite orders and non-negative coefficients; and
- (b)  $\lambda(1) = \rho(1) = 1$ .

<sup>2</sup>Here  $p_j$  and the addend  $d_k$  actually represent the values of nodes  $p_j$  and  $d_k$ , respectively. Similar expressions will be used later without notice.

Throughout this paper, we denote by  $K$ ,  $J$ , and  $E$ , respectively, the total numbers of information nodes, parity nodes, and edges. Then  $\lambda_i E$  is the number of edges with left degree  $i$  and  $\lambda_i E/i$  the number of information nodes with degree  $i$ . Therefore, we have

$$K = E \sum_i \lambda_i / i \quad \text{and} \quad J = E \sum_i \rho_i / i. \quad (3)$$

Define left and right nodal degree polynomials respectively as

$$A(x) \equiv \sum_i A_i x^i \equiv \frac{\sum_i \lambda_i x^i / i}{\sum_i \lambda_i / i} = \frac{E}{K} \sum_i \lambda_i x^i / i \quad (4a)$$

and

$$P(x) \equiv \sum_i P_i x^i \equiv \frac{\sum_i \rho_i x^i / i}{\sum_i \rho_i / i} = \frac{E}{J} \sum_i \rho_i x^i / i. \quad (4b)$$

From (2)-(4),  $A_i$  (respectively,  $P_i$ ) is the fraction of information (respectively, parity) nodes with degree  $i$ . We also have the following relationships.

$$A(x) = \frac{E}{K} \int_0^x \lambda(t) dt \quad \text{and} \quad \lambda(x) = \frac{K}{E} \frac{dA(x)}{dx} \quad (5a)$$

$$P(x) = \frac{E}{J} \int_0^x \rho(t) dt \quad \text{and} \quad \rho(x) = \frac{J}{E} \frac{dP(x)}{dx} \quad (5b)$$

### C. Criteria for Capacity-Achieving Codes

We henceforth use post-decoding erasure rate (PDER) [13] to denote the fraction of un-recovered information bits after decoding. Theorem 1 below is a fundamental result from [12].

*Theorem 1:* Let  $\delta$  be the erasure rate of a partial erasure channel. When  $K \rightarrow \infty$ , the PDER of a two-column tornado code (with iterative decoding) goes to zero, provided that

$$\rho(1 - \delta \cdot \lambda(x)) > 1 - x, \quad 0 < x \leq 1. \quad (6)$$

### D. A New Pair of Optimal Degree Distributions

Based on Theorem 1, optimal degree distributions are derived in [12]. We now present a new pair of optimal degree distributions that will be used later in the new scheme. Denote

$$\alpha \equiv 1 - J/E \quad (7)$$

where  $J$  and  $E$  are, respectively, the number of parity nodes and edges. Let

$$\lambda(x) = \frac{K}{E} \left( \frac{1}{\sqrt{1-x}} - 1 \right) \quad (8a)$$

$$\rho(x) = \left( \frac{1-\alpha}{1-\alpha x} \right)^2 \quad (8b)$$

$$A(x) = \frac{E}{K} \int_0^x \lambda(t) dt = 2 - x - 2\sqrt{1-x}, \quad \text{and} \quad (8c)$$

$$P(x) = \frac{E}{J} \int_0^x \rho(t) dt = \frac{(1-\alpha)x}{1-\alpha x}. \quad (8d)$$

The equations (8a) and (8b), respectively, can be expanded into power series as

$$\lambda(x) = \frac{K}{E} \sum_{i=2}^{\infty} i \gamma_i x^{i-1} \quad (9a)$$

$$\rho(x) = (1 - \alpha)^2 \sum_{i=1}^{\infty} i \alpha^{i-1} x^{i-1} \quad (9b)$$

where, for any integer  $i > 1$ ,

$$\gamma_i \equiv \frac{(2i-3)!!}{2^{i-1} \cdot i!}. \quad (9c)$$

It is clear that all the coefficients of  $\lambda(x)$  and  $\rho(x)$  are positive. Also, it can be shown that, provided that

$$\delta < \frac{J}{\alpha K}, \quad (9d)$$

the functions defined in (8) satisfy (6). Thus, they may potentially lead to good codes. However, such codes are not realizable since, for a finite  $K$ , (8a) requires  $E \rightarrow \infty$  for satisfying the constraint of  $\lambda(1) = 1$  in Remark 1. To overcome this difficulty, we truncate  $\lambda(x)$  to a polynomial with a finite order. Denote by  $M$  the truncation order to which the left nodal and edge polynomials are clipped. Define

$$A_M(x) \equiv \frac{1}{A_M} \sum_{i=2}^M \gamma_i x^i, \text{ and} \quad (10a)$$

$$\lambda_M(x) \equiv \frac{K}{E} \cdot \frac{dA_M(x)}{dx} = \frac{1}{B_M} \sum_{i=2}^M i \gamma_i x^{i-1} \quad (10b)$$

where

$$A_M \equiv \sum_{i=2}^M \gamma_i \quad \text{and} \quad B_M \equiv \sum_{i=2}^M i \gamma_i. \quad (11a)$$

Note that  $E$ ,  $K$ ,  $A_M$ , and  $B_M$  are related by

$$E/K = B_M/A_M. \quad (11b)$$

It can be shown that<sup>3</sup>

$$A_M < 1, \lim_{M \rightarrow \infty} A_M = 1, \text{ and } \lim_{M \rightarrow \infty} B_M = \infty. \quad (12)$$

From (8a), (9a) and (10b), we have

$$\lambda_M(x) < \frac{1}{B_M} \left( \frac{1}{\sqrt{1-x}} - 1 \right), \quad 0 < x \leq 1. \quad (13)$$

Therefore, by some straightforward manipulations,  $\lambda_M(x)$  and  $\rho(x)$  satisfies

$$\rho(1 - \delta \cdot \lambda_M(x)) > 1 - x, \quad 0 < x \leq 1 \quad (14a)$$

provided that

$$\delta < \delta_M \equiv \frac{1}{\frac{K}{JA_M} - \frac{1}{B_M}}. \quad (14b)$$

We can construct a realizable two-column tornado code  $C$  as follows: select a finite integer  $M > 0$  and  $\alpha \in (0, 1)$ ; then construct a code  $C$  based on  $\lambda_M(x)$  in (10b) and  $\rho(x)$  in

(9b). It is straightforward to verify that the criteria in Remark 1 are met<sup>4</sup>, and so  $C$  is realizable. From (14) and the related discussions above, we further have the following theorem.

*Theorem 2:* When  $K \rightarrow \infty$ , the PDER of  $C$  goes to zero in a partial erasure channel provided that  $\delta < \delta_M$ .

Now consider the asymptotic effect of  $M$ . From (12) and (14b), we have

$$\delta_M \equiv \frac{1}{\frac{K}{JA_M} - \frac{1}{B_M}} < \frac{JA_M}{K} < \frac{J}{K} \quad (15a)$$

and

$$\lim_{M \rightarrow \infty} \delta_M = J/K. \quad (15b)$$

Thus,  $J/K$  is an upper bound of  $\delta$  that is tight when  $M$  is sufficiently large. Note that  $R = K/(J + K) = 1/(1 + \delta)$  (or equivalently,  $\delta = J/K$ ) is the capacity of the partial erasure channel [12]. This implies that  $C$  with a finite  $M$  cannot achieve the channel capacity, but the gap diminishes to zero as  $M \rightarrow \infty$ . In practice,  $M$  cannot be too large since  $E/K$  (as a measure of the encoding and decoding complexities) in (11b) increases unboundedly with  $M$ .

#### E. Parity-Check Matrix of Two-Column Tornado Code

A two-column tornado code can be defined using a parity-check matrix. Decompose the codeword of a linear binary systematic code into  $\mathbf{c} = [\mathbf{p}, \mathbf{d}]$ , where  $\mathbf{p} = [p_j]$  and  $\mathbf{d} = [d_k]$  contain the parity and information bits, respectively. Accordingly, we decompose the corresponding parity-check matrix  $\mathbf{H}$  into  $\mathbf{H} = [\mathbf{H}^p, \mathbf{H}^d]$ . Then

$$[\mathbf{H}^p, \mathbf{H}^d] [\mathbf{p}, \mathbf{d}]^T = \mathbf{0} \quad (16)$$

where notation “ $T$ ” represents the transpose operation, and “ $\mathbf{0}$ ” an all-zero vector. For the two-column tornado code, it can be shown that  $\mathbf{H}^p$  is an identity matrix, i.e.

$$\mathbf{H}^p = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}. \quad (17)$$

This indicates

$$p_j = \sum_{d_k \in B_j} d_k \bmod 2, \quad j = 1, 2, \dots, J \quad (18)$$

where  $B_j = \{d_k | H_{j,k}^d = 1\}$  with  $H_{j,k}^d$  being the  $(j, k)$ th element in  $\mathbf{H}^d$ . Comparing (18) with (1), we can see that  $H_{j,k}^d = 1$  implies that there is an edge between  $d_k$  and  $p_j$  in Fig. 1. Define the weight of a binary vector as the number of its non-zero entries. Then,  $\lambda_i$  and  $P_i$  in (4) are respectively the fraction of columns and rows in  $\mathbf{H}^d$  with weight  $i$ .

<sup>4</sup>Strictly speaking, truncation should also be applied to  $P(x)$  for finite-length codes. However, such truncation is not explicitly required in encoding since the parity nodes are generated using the constrained-random-scrambling rule described in Appendix I.B. The resulting right nodal degree distribution asymptotically approaches  $P(x)$ , as detailed in Appendix I.A.

<sup>3</sup>From (9c), we have  $\gamma_i/\gamma_{i+1} = (2i+2)/(2i-1) = 1+1.5i^{-1}+O(i^{-2})$ . According to Gauss's test (see p.567 in [26]), the series  $\sum \gamma_i$  converges. Thus,  $\lim_{M \rightarrow \infty} A_M = \lim_{M \rightarrow \infty} A_M(1) = A(1) = 1$ .

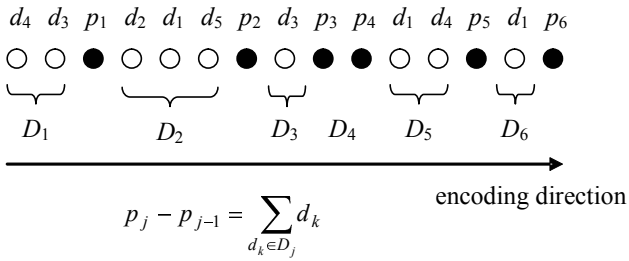


Fig. 2. The encoding line for an SR-LDPC code  $C$ . Here  $K = 5$ ,  $J = 6$ ,  $E = 9$ . The degrees of  $\{d_1, d_2, d_3, d_4, d_5\}$  are  $\{3, 1, 2, 2, 1\}$ .

*Remark 2:* For a two-column tornado code, the column and row weight distributions of  $\mathbf{H}^d$  are given by left and right nodal degree distributions  $\Lambda(x)$  and  $P(x)$ , respectively. The total number of ones in  $\mathbf{H}^d$  equals  $E$ , the number of edges.

### III. SR-LDPC CODES

We now proceed to discuss the proposed SR-LDPC codes using both matrix and graphic representations. We establish a connection between tornado codes and SR-LDPC codes, based on which we show that the new codes are systematic, capacity-approaching, and rateless.

#### A. Matrix Representation of SR-LDPC Encoder

Reconsider the decomposition  $\mathbf{H} = [\mathbf{H}^p, \mathbf{H}^d]$  as in (16). An SR-LDPC code defined in [11] has a parity sub-block  $\mathbf{H}^p$  of the form

$$\mathbf{H}^p = \begin{pmatrix} 1 & & & & 0 \\ 1 & 1 & & & \\ & & \ddots & \ddots & \\ 0 & & & 1 & 1 \end{pmatrix}. \quad (19)$$

Encoding is based on the following recursion (setting  $p_0 \equiv 0$ ):

$$p_j - p_{j-1} = \sum_{d_i \in B_j} d_i \bmod 2, \quad j = 1, 2, \dots, J \quad (20)$$

where  $B_j = \{d_k | H_{j,k}^d = 1\}$ . The order in which the parity values in the above recursion are evaluated is referred to as the encoding direction. The similarities and differences between (18) and (20) are crucial: the similarity greatly facilitates the analysis of SR-LDPC codes while the differences result in some distinctive properties of SR-LDPC codes.

The codes so defined form a sub-class of LDPC codes [5][14]. Repeat accumulate (RA) codes [9] and concatenated tree (CT) codes [15][16] both have the structure shown in (19). We briefly compare these codes in Appendix I.C.

#### B. Graphic Representation of SR-LDPC encoder

We now consider an alternative graphic encoding method for an SR-LDPC code. The encoding line in Fig. 2 is constructed as follows. Assume that every information bit  $d_k$  is assigned with a degree  $m_k$  randomly drawn from the distribution  $\Lambda_M(x)$  in (10a). For every  $d_k$ , we generate  $m_k$  equivalent white nodes, all labeled by  $d_k$ . In total, we obtain  $E$  white

nodes. We scramble<sup>5</sup> these white nodes together with  $J$  black nodes. Then we label the black nodes by parity bits  $\{p_j\}$  in a sequential order. Let  $D_j$  be the segment of consecutive white nodes between  $p_{j-1}$  and  $p_j$  and denote by  $|D_j|$  the length of  $D_j$ . We say that  $d_k \in D_j$  if a white node representing  $d_k$  falls in  $D_j$ . The encoding rule is defined by a recursion as

$$p_j - p_{j-1} = \sum_{d_k \in D_j} d_k \bmod 2, \quad j = 1, 2, \dots, J. \quad (21a)$$

Note that: (i)  $D_j$  may contain multiple white nodes labeled by the same  $d_k$ ; (ii)  $D_j$  may be empty, such as  $D_4$  in Fig. 2; (iii) Eq. (21a) can be equivalently rewritten as

$$p_j = \sum_{m=1}^j \sum_{d_k \in D_m} d_k \bmod 2. \quad (21b)$$

For given  $\{D_j\}$ , we can construct  $\mathbf{H}^d$  in (16) as

$$H_{j,k}^d = 1, \text{ if } d_k \in D_j, \text{ for any } j \text{ and } k. \quad (22)$$

As mentioned above, in (21a), an information bit  $d_k$  can appear in  $D_j$  more than once. However, the probability of such an event is arbitrarily close to zero when  $K \rightarrow \infty$ , provided that the truncation length  $M$  is finite and the encoding rule in Appendix I is employed. It is also shown in Appendix I that the distribution of  $|D_j| \rightarrow P(x)$  (the row weight distribution of  $\mathbf{H}^d$ , see Remark 2) when  $K \rightarrow \infty$  (at the same time maintaining  $\alpha$  as a constant).

#### C. Performance in Partial Erasure Channels

Eq. (16) can be rewritten as

$$\mathbf{H}^d \mathbf{d}^T = \mathbf{H}^p \mathbf{p}^T. \quad (23)$$

If  $\mathbf{p}$  is received without erasure, the right hand side of (23) is fixed. Thus, from a decoding point of view, all linear systematic codes with the same sub-block  $\mathbf{H}^d$  are equivalent in a partial erasure channel. This fact, together with Theorem 2, leads to the following.

*Remark 3:* Let  $C$  be an SR-LDPC code with left and right nodal degree distributions specified in (10a) and (8d), respectively. When  $K \rightarrow \infty$ , the PDER of  $C$  goes to zero in a partial erasure channel with erasure rate  $\delta < \delta_M$ .

#### D. Performance in General Erasure Channels

Now consider a general erasure channel with erasures on both information and parity bits. Let  $C$  be defined in Fig. 2. Suppose that  $E$  and  $J$  are sufficiently large. We generate an encoding line with the asymptotic distribution of  $|D_j|$  defined in (8d) using the constrained random-scrambling rule in Appendix I.B. Suppose that we randomly delete  $J - \tilde{J}$  black nodes and use the  $E$  white nodes together with the remaining  $\tilde{J}$  black nodes to form a new code  $\tilde{C}$ . Remark 4 below shows the similarity between  $C$  and  $\tilde{C}$ . It is a direct consequence of the discussion in Appendix I.B.

*Remark 4:* The right nodal degree distribution of  $\tilde{C}$  is  $\tilde{P}(x) = \frac{(1-\tilde{\alpha})x}{1-\tilde{\alpha}x}$ , where  $\tilde{\alpha} \equiv 1 - \tilde{J}/E$ .

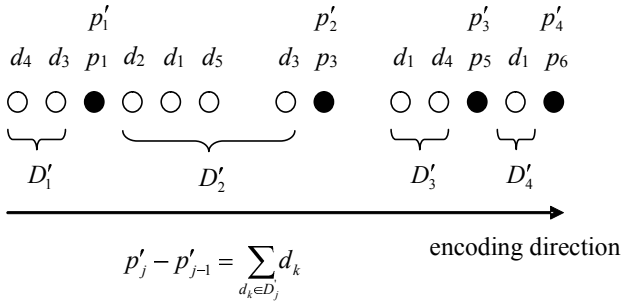


Fig. 3. The residual encoding line formed by erasing  $J - \tilde{J} = 2$  parity nodes in Fig. 2. Here  $\{p'_j\}$  are the re-sequenced parity node labels and  $\{D'_j\}$  are the new sets of consecutive white nodes.

Fig. 3 is a graphical illustration of  $\tilde{C}$  obtained from  $C$  in Fig. 2, where we have re-labeled the remaining parity nodes as  $\{p'_1, p'_2, \dots\}$ . From (21a), it can be shown that

$$p'_j - p'_{j-1} = \sum d_k \bmod 2 \quad (24)$$

where the summation is over all white nodes between  $p'_{j-1}$  and  $p'_j$ . Eq. (24) shows a “self-healing property”, i.e., we can construct new constraints as in (24) using the received parity nodes to replace the old ones in (21a). By considering this together with Remark 4, we have the following property with respect to the structural equivalence between  $C$  and  $\tilde{C}$ .

*Remark 5:*  $\tilde{C}$  and  $C$  have the same structure except that the number of parity nodes involved are different. The performance of  $\tilde{C}$  can be determined using Remark 3 with  $J$  changed to  $\tilde{J}$ .

Let  $C$  be an SR-LDPC code in Remark 5. Decompose a general erasure channel into two cascade sub-channels. After the first sub-channel,  $\delta_{\text{prt}}J$  parity bits in  $C$  are randomly erased to form the sub-code  $\tilde{C}$ . After the second sub-channel,  $\delta_{\text{inf}}K$  information bits in  $\tilde{C}$  are randomly erased. From Remarks 3 and 5,  $\tilde{C}$  (or equivalently,  $C$ ) is recoverable provided that

$$\delta_{\text{inf}} < \frac{1}{\frac{K}{JA_M} - \frac{1}{B_M}} = \frac{1}{\frac{K}{J(1-\delta_{\text{prt}})A_M} - \frac{1}{B_M}}. \quad (25a)$$

For a general erasure channel, we have  $\delta = \delta_{\text{prt}} = \delta_{\text{inf}}$ . Thus, the condition in (25a) indicates that  $\tilde{C}$  is recoverable provided that

$$\delta < \delta'_M \equiv \frac{1}{2} \left( \sqrt{D_M^2 + 4B_M} - D_M \right) \quad (25b)$$

where  $D_M \equiv \frac{KB_M}{JA_M} + B_M - 1$ . It can be verified that  $\lim_{M \rightarrow \infty} \delta'_M = J/(J+K)$ . By definition, the code rate

$$R = K/(J+K) = 1 - J/(J+K)$$

and so, for a sufficiently large  $M$ , (25b) becomes  $R < 1 - \delta$  with  $1 - \delta$  being the capacity of the channel [12]. The above results are summarized as follows.

*Theorem 3:* Let  $C$  be an SR-LDPC code designed using the left and right nodal degree distributions specified in (10a) and

(8d) respectively. When  $K \rightarrow \infty$ , the PDER of  $C$  goes to zero in a general erasure channel provided that  $\delta < \delta'_M$ . In particular, the scheme achieves channel capacity when  $M \rightarrow \infty$  and  $K \rightarrow \infty$ .

Here is a brief summary of the construction procedure for SR-LDPC codes. We first select a proper truncation order  $M$  and obtain  $\Lambda_M(x)$  in (10a). Then construct the encoding line based on  $\Lambda_M(x)$  using random scrambling and generate the parity bits by random insertion (as detailed in Appendix I). The information and parity bits are randomly mixed before transmission. Note that  $\Lambda_M(x)$  is independent of the channel erasure rate, and that one can generate as many new parity bits as necessary since, from (21b), adding new parity bits do not affect the value of the existing ones. This implies that the resultant code is potentially rateless. However, to claim ratelessness, it remains to show that SR-LDPC codes have “good performance” (see Footnote 1) for all rates, as detailed below.

#### E. Ratelessness

To compare the proposed codes with LT and raptor codes in a common platform, we introduce the decoding inefficiency index  $\eta$ , defined as the ratio of the number of un-erased received bits to the information length, i.e.

$$\eta = (1 - \delta)/R. \quad (26)$$

Using (26), the constraint in (25b) can be equivalently rewritten in term of  $\eta$  as

$$\eta > \eta_M \equiv \frac{1}{2} \left( \Delta_M - \sqrt{\Delta_M^2 - \frac{4B_M}{A_M R(1-R)}} \right) \quad (27)$$

where  $\Delta_M \equiv \frac{B_M+1}{R} + \frac{B_M}{A_M(1-R)}$ . Clearly, the threshold  $\eta_M$  depends on both the code rate  $R$  and the truncation order  $M$ , as illustrated in Fig. 4. Note that  $\eta_M$  is bounded away from 1 for  $R \neq 1$  and  $M < \infty$ .

We next show the ratelessness of the proposed coding scheme. It is straightforward to verify that

$$\lim_{R \rightarrow 0} \eta_M = \frac{B_M}{A_M(B_M+1)} \text{ and } \lim_{R \rightarrow 1} \eta_M = 1.$$

Furthermore, it can be shown that  $\eta_M$  uniformly converges to 1 (the capacity limit) for  $0 < R \leq 1$  when  $M \rightarrow \infty$ . Therefore, the proposed scheme is indeed rateless.<sup>6</sup> The above result is verified numerically in Fig. 4.

## IV. SIMULATION RESULTS AND DISCUSSIONS

In this section, simulation results are provided to verify the performance of SR-LDPC codes in general binary erasure channels. The performance of LT and raptor codes is also

<sup>6</sup>For a rateless scheme,  $R$  can be interpreted as the proportion of information bits in all received bits. The performance of the proposed SR-LDPC codes varies slightly with  $R$  due to the use of a finite truncation order  $M$ .

<sup>5</sup>Different scrambling rules are discussed in Appendix I.

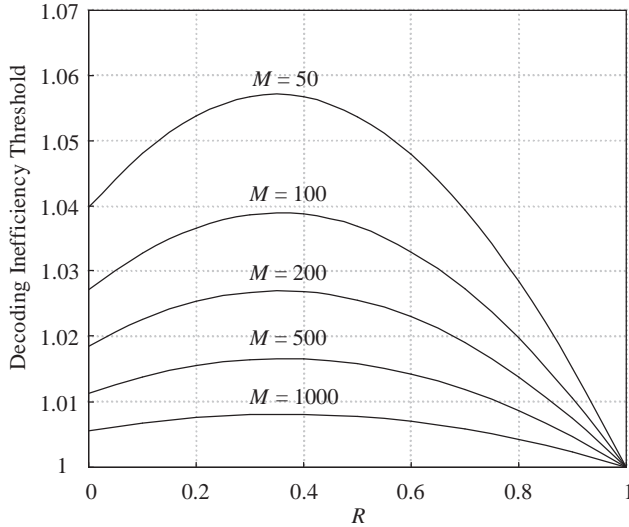


Fig. 4. The effect of truncation length  $M$  and code rate  $R$  on the decoding inefficiency threshold.

TABLE I

THE DENSITY  $E/K$  OF SR-LDPC CODES VERSUS TRUNCATION LENGTH  $M$ , WHERE  $E$  DENOTES THE NUMBER OF EDGES IN THE BIPARTITE GRAPH OF THE CODE, AND  $K$  THE NUMBER OF INFORMATION BITS.

$M$	50	100	200	500	1000
$E/K$	8.28	11.57	16.24	25.51	35.96

included for comparison. The right nodal degree polynomial of an LT code is given in [2] as

$$\begin{aligned}
 P_{LT}(x) = & 0.008x + 0.494x^2 + 0.166x^3 + 0.073x^4 \\
 & + 0.083x^5 + 0.056x^8 + 0.037x^9 \\
 & + 0.056x^{19} + 0.025x^{65} + 0.003x^{66}. \quad (28)
 \end{aligned}$$

Table I lists  $E/K$ , referred to as the density of SR-LDPC codes, versus truncation length  $M$ . The decoding complexity of a code is roughly proportional to its density  $E/K$ . The LT code realized by (28) has a density of approximately 6. As shown in simulation, this LT code suffers from a severe error-floor problem. Raptor codes can solve this problem by concatenating an LDPC pre-coder before the LT encoding structure. The precoder used in [2] has roughly the same decoding complexity as the LT code based on (28). For comparison, we choose  $M = 100$  for the SR-LDPC code, resulting in a density value of 11.6.

In our simulations, we generally follow the principles outlined in Appendix I.C to construct the SR-LDPC codes. Analysis in [12] shows that the main contribution of the error probability in the error-floor region comes from degree-2 information nodes (cf., Lemma 1 in [12] and the discussions therein). To reduce the error floor, we introduce a small number of extra parity nodes to further protect the degree-2 information nodes. The proportion of such extra parity nodes is kept at about 1% of the total number of parity nodes so that their impact on the overall code rate is negligible. (Note: A similar treatment of degree-2 nodes is described in [12] for tornado codes.) More specifically, we generate an extra replica for each degree-2 information node. We collect these extra

replicas and use them to extend the encoding line (cf., Fig. 2). The extra parity nodes are then randomly inserted into the extended part of the encoding line<sup>7</sup>, with the last extra parity node appended to the end for termination. In this way, we increase the minimum left degree to 3. Note that, for a fair comparison, the extra parity nodes have been considered in determining the code rate in simulation.

The decoding algorithm of the tornado code [12] can be easily applied to SR-LDPC codes due to their similarity. An SR-LDPC decoder can recover the erasure bits by searching through the lost information bits in the residue decoding line in Fig. 3 based on the following rule: between any two adjacent black nodes, if there is only one lost white node, the corresponding bit can be recovered together with its replicas.

The performance of the LT, raptor and SR-LDPC codes is compared in Fig. 5. The information length is fixed at 65536 for all codes. The performance curve of the raptor code is cited from Fig. 2 in [3] (with  $\sigma = 0$  at which the BIAWGN channel reduces to a perfect channel with erasure rate  $\delta = 0$ ). There is only one curve for the raptor code since the performance of raptor codes in terms of decoding inefficiency is invariant to the code rate. Conventionally, it is not necessary to fix the “code rate” for a rateless scheme [3]. However, the theoretical bound in (27) shows that the proposed SR-LDPC codes performs slightly differently at different code rates. For easy comparison with this bound, we simulate the SR-LDPC codes at different code rates, namely,  $R = 0.1, 0.36, 0.5, 0.7, 0.9$  and  $0.95$ , in Fig. 5. It can be seen in Fig. 5 that the LT code suffers from a severe error-floor problem. Thus we only compare the SR-LDPC codes with the raptor code below. From Fig. 5, compared with the raptor code, the proposed SR-LDPC codes performs slightly better when rate  $R$  is 0.9 or higher, but slightly worse when  $R$  is lower. For SR-LDPC codes, the distance from the capacity at different rates agree well with the theoretical thresholds shown in Fig. 4. In particular, the worst code performance occurs at  $R = 0.36$ . It is also worth mentioning that, from Fig. 5, one may readily obtain the performance of SR-LDPC codes against  $\delta$  by noting that  $\eta$  and  $\delta$  are related by (26).

The SR-LDPC coding scheme requires a lower decoding complexity than the raptor or LT codes in channels with rare erasure. This can be seen as follows. For the LT and raptor codes, only parity bits are transmitted so that an iterative decoding process is always necessary regardless of channel condition (even for a perfect channel without any erasure). On the other hand, the decoding complexity of the SR-LDPC coding scheme depends on the channel condition. When the proportion of lost bits is very high, its decoding complexity is roughly the same as that of the raptor codes compared in Fig. 5. However, when the channel condition is good and only a few information bits need to be recovered, the decoding process ends quickly for the SR-LDPC code. In particular, the decoding process can be completely avoided if there is no erasure. This clearly shows the advantage of the proposed scheme for transmission in channels with a low erasure rate.

<sup>7</sup>Different insertion rules may lead to slightly different performance.

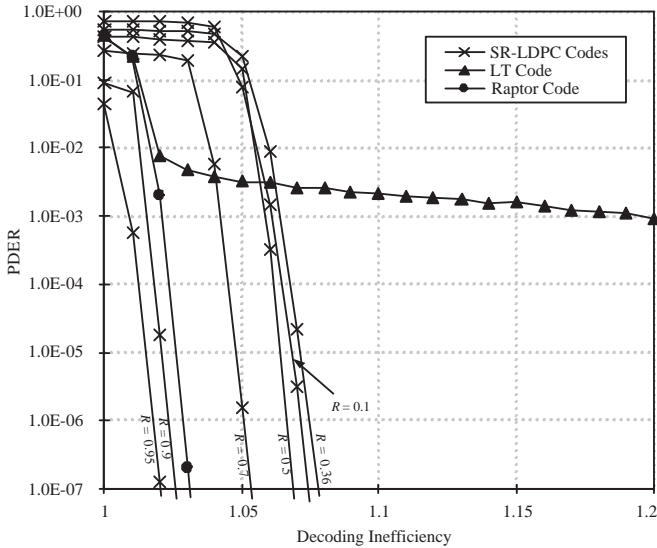


Fig. 5. The PDER performance of the SR-LDPC codes at different code rate  $R$ . The information length is 65536. The performance curves of the corresponding LT and raptor codes are also included for comparison.

## V. CONCLUSIONS

We have developed a simple erasure-recovery coding scheme based on the so-called SR-LDPC codes. Similarly to the LT codes and the more recently proposed raptor codes, the new scheme is rateless and capacity-achieving. Furthermore, the new scheme is also systematic, which provides an advantage for transmission over erasure channels with a relatively low erasure rate. Particularly, the encoding and decoding process can be completely avoided if there is no erasure.

## APPENDIX A SCRAMBLING PRINCIPLES

In this appendix, we derive the degree distributions for different scrambling methods.

### A. Random Scrambling

Suppose that  $E$  white nodes and  $J$  black nodes are scrambled to form a circle. For convenience, we call the block of consecutive white nodes between two adjacent black nodes a *segment*, with its length defined as the total number of white nodes in it. Note that the length of a segment can be zero, which corresponds to the situation of two consecutive black nodes. Take a black node as a reference, and let  $W$  be the length of the segment (either clockwise or anticlockwise) adjacent to it. If the scrambling is random, we obtain that, for  $i = 0, 1, \dots, E$ ,

$$\begin{aligned} \Pr\{W = i\} &= \left( \prod_{n=0}^{i-1} \frac{E-n}{J+E-n-1} \right) \cdot \frac{J-1}{J+E-i-1} \\ &= \left( \prod_{n=0}^{i-1} \frac{\beta - \frac{n}{J+E}}{1 - \frac{n+1}{J+E}} \right) \cdot \frac{1-\beta - \frac{1}{J+E}}{1 - \frac{i+1}{J+E}} \end{aligned} \quad (29)$$

where  $\beta \equiv E/(J+E)$ . Letting  $J$  and  $E$  go to infinity while keeping  $\beta$  as a constant, the asymptotic distribution polynomial of  $W$  is given by

$$\hat{P}(x) = \sum_{i=0}^{\infty} \beta^i (1-\beta)x^i = \frac{1-\beta}{1-\beta x}. \quad (30)$$

Due to the centrosymmetry of a circle, the distribution in (29) holds for any reference node. Thus, it can be more generally treated as the distribution of the segment length in the circle. By breaking the circle at a randomly selected point, we can obtain the corresponding distribution in a line. This operation divides the segment containing the breaking point into two segments while the others remain intact. Note that the total number of segments is  $J+1$ . Thus, the impact of such an operation can be ignored for a sufficiently long code, which implies that the asymptotic distribution (30) still holds for random scrambling on a line. Note that (30) and (8d) are different only by a factor of  $x$ .

### B. Constrained Random Scrambling

We now discuss the realization of  $P(x)$  in (8d). Assume that  $E \geq J$ , which can be ensured by using a sufficiently large  $M$  in (10). Consider the following two methods.

*Method a:* Randomly scramble  $E-J$  white nodes and  $J$  black nodes to form a line. Then insert an extra white node right in front of each black node.<sup>8</sup> (In total,  $J$  extra white nodes are inserted.)

*Method b:* Randomly scramble  $E$  white nodes and arrange them into a line. Randomly select (either one by one or in bunch)  $J$  white nodes in this line and insert a black node behind each of them.

The equivalence of the above two methods can be seen from the fact that, if all the nodes are indexed, they have the same pool of equally possible outcomes. Thus, they also have the same distribution of segment length  $W$  (as defined in Appendix I.A). Similarly, we can see that Method c below is also equivalent to the above two methods.

*Method c:* Apply Method a (or b) to a set of  $E$  white nodes and  $J+J'$  black nodes to form a line, where  $J'$  is an arbitrary integer. Then randomly delete  $J'$  black nodes from this line.

Before the insertion of extra white nodes in Method a, the distribution of  $W$  is given by (30) as  $\frac{1-\alpha}{1-\alpha x}$  with  $\alpha = 1 - J/E$  for sufficiently large  $J$  and  $E$ . After the insertion, the distribution polynomial is shifted by one position to the higher order. Thus, we have the following.

*Remark 6:* Methods a, b and c lead to the same resultant distribution of the segment length given by  $P(x) = \frac{(1-\alpha)x}{1-\alpha x}$  with  $\alpha = 1 - J/E$ .

Returning to Remark 4,  $\tilde{C}$  can be obtained by applying Method c to  $C$  and so, based on Remark 6, the right nodal degree distribution of  $\tilde{C}$  is  $\tilde{P}(x) = \frac{(1-\alpha)x}{1-\alpha x}$ .

<sup>8</sup>In an encoding line, “node A is in front of node B” if node A is processed before node B in the encoding process, and vice versa.

### C. Concatenated Tree (CT) Technique

The scrambling methods described in the previous subsections all fall into the family of IRA codes in which the relative positions among white nodes are purely random. However, as shown in the notes below (21a), the contribution of  $d_k$  in (21a) may be canceled out if  $D_j$  contains an even number of the replicas of  $d_k$ . In this case, the check equation (21a) will not provide any protection for  $d_k$ . Although the probability of such an event approaches zero for infinitely long codes, it requires careful consideration for codes with finite length. The following encoder design provides a treatment to this problem by segmenting the overall encoding line into several components. Let  $W_n$ , for  $n = 1, 2, \dots, M$ , be subsets to which white nodes will be added, where  $M$  is the truncation length used in (10). Initially, set every  $W_n$  to be empty.

Step 1: For  $k = 1$  to  $K$ : randomly draw a number  $m_k$  from  $\Lambda_M(x)$  as the degree of the information bit  $d_k$ ; then randomly select  $m_k$  subsets among  $\{W_n\}$  and add one white node labeled by  $d_k$  to each of the selected subsets.

Step 2: Randomly scramble the white nodes in each  $W_n$  and arrange them into a line as the  $n$ th component. Concatenate the  $M$  components one by one to form an overall encoding line. Randomly selected  $J$  out of the  $E$  white nodes in this line and insert a black node right behind each of them.

Step 3: Apply the encoding procedure defined in (21).

With the above encoder design, the number of consecutive white nodes follows the asymptotic distribution  $P(x)$ . Each  $W_n$  does not contain any node with more than one replica. Thus, only those segments of consecutive white nodes that straddle two adjacent components may contain nodes with more than one replica, but the probability of such an event is marginal. The resulting code belongs to the family of CT codes as introduced in [15].

### ACKNOWLEDGMENT

The authors wish to thank Dr. Weimin Zhang and Dr. Julija Tovirac for their valuable comments. The authors also wish to thank the anonymous reviewers for many comments and suggestions that have helped to greatly improve the quality of the paper.

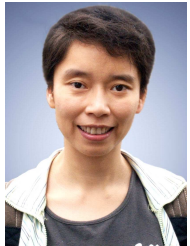
### REFERENCES

- [1] M. G. Luby, "LT codes," in *Proc. 43rd Annual IEEE Symposium on Foundations of Computer Science*, Vancouver, BC, Canada, pp. 271-280, Nov. 2002.
- [2] A. Shokrollahi, "Raptor codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 6, pp. 2551-2567, June 2006.
- [3] O. Etesami and A. Shokrollahi, "Raptor codes on binary memoryless symmetric channels," *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2033-2051, May 2006.
- [4] J. Ha, J. Kim, S. W. McLaughlin, "Rate-compatible puncturing of low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 50, no. 11, pp. 2824 - 2836, Nov. 2004.
- [5] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, vol. IT-8, no. 1, pp. 21-28, Jan. 1962.
- [6] T. Richardson, A. Shokrollahi and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 619-637, Feb. 2001.
- [7] I. Sason and R. Urbanke, "Parity-check density versus performance of binary linear block codes over memoryless symmetric channels," *IEEE Trans. Inform. Theory*, vol. 49, no. 7, pp. 1611-1635, July 2003.
- [8] H. D. Pfister, I. Sason and R. Urbanke, "Capacity-achieving ensembles for the binary erasure channel with bounded complexity," *IEEE Trans. Inform. Theory*, vol. 51, no. 7, pp. 2352 - 2379, July 2005.
- [9] H. Jin, A. Khandekar, and R. J. McEliece, "Irregular repeat-accumulate codes," in *Proc. 2nd International Symposium on Turbo codes and related topics*, pp. 1-8, France, Sep. 2000.
- [10] I. Sason and R. Urbanke, "Complexity versus performance of capacity-achieving irregular repeat-accumulate codes on the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 50, pp. 1247-1256, June 2004.
- [11] Li Ping, W. K. Leung, and Nam Phamdo, "Low density parity check codes with semi-random parity check matrix," *Electronics Letters*, vol. 35, no. 1, pp. 38-39, Jan. 1999.
- [12] M. G. Luby, M. Mitzenmacher, A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 569-584, Feb. 2001.
- [13] M. A. Kousa, "A novel approach for evaluating the performance of SPC product codes under era-sure decoding," *IEEE Trans. Communications*, vol. 50, no. 1, pp.7-11, Jan. 2002.
- [14] N. Wiberg, H. A. Loeliger, and R. Kotter, "Codes and iterative decoding on general graphs," *Euro. Trans. Telecommun.*, vol. 6, no. 5, pp. 513-526, Sept. 1995.
- [15] Li Ping and K. Y. Wu, "Concatenated tree codes: a low-complexity, high-performance approach," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 791-799, Feb. 2001.
- [16] Li Ping, X. L. Huang, and Nam Phamdo, "Zigzag codes and concatenated zigzag codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 800-807, Feb. 2001.
- [17] A. Shokrollahi, "Capacity-achieving sequences," in *Codes, Systems, and Graphical Models* (Minneapolis, MN, 1999), Springer Verlag, New York, Inc., pp. 153-166, 2001.
- [18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1977.
- [19] P. Oswald and A. Shokrollahi, "Capacity-achieving sequences for the erasure channel," *IEEE Trans. Inform. Theory*, vol. 28, no. 12, pp. 3017 - 3028, Dec. 2002.
- [20] R. Palanki and J. S. Yedidia, "Rateless codes on noisy channels," in *Proc. IEEE Int. Symp. Inform. Theory*, Chicago, USA, page 37, June/July 2004.
- [21] S. Benedetto and G. Montorsi, "Unveiling turbo codes: some results on parallel concatenated cod-ing schemes," *IEEE Trans Inform. Theory*, vol. 42, no. 2, pp. 409 - 428, March 1996.
- [22] D. Divsalar, H. Jin, and R. McEliece, "Coding theorems for 'turbo-like' codes," in *Proc. 1998 Allerton Conf. Communication, Control and Computing*, Monticello, IL, pp. 201-210, Oct. 1998.
- [23] C. H. Hsu and A. Anastasopoulos, "Capacity-achieving codes with bounded graphical complexity on noisy channels," in *Proc. 43rd Allerton Conf. Communication, Control and Computing*, Monti-cello, IL, USA, pp. 1825-1834, Sep. 2005.
- [24] H. Pfister and I. Sason, "Accumulate-repeat-accumulate codes: Capacity-achieving ensembles of systematic codes for the erasure channel with bounded complexity," *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2088-2115, June 2007.
- [25] A. Shokrollahi, "New sequences of time erasure codes approaching channel capacity," in *Proc. 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer Verlag, pp. 65-76, 1999.
- [26] R. Courant and F. John, *Introduction to Calculus and Analysis*, Vol. 1. New York: Springer-Verlag, 1999.



**Xiaojun Yuan** (S'04-M'08) received the B.S. degree in electronic and information systems from Shanghai Jiaotong University, the M.S. degree in circuit and systems from Fudan University, and the Ph.D degree at City University of Hong Kong. He is now with the Department of Electronic Engineering, University of Hawaii at Manoa, Hawaii, USA.

His research interests include signal processing, coding theory, optimized communication system and network design.



**Rong Sun** received the B.E. degree in telecommunications engineering, the M.E. degree in communications and information systems and the Ph.D degree in communications and information systems from Xidian University, Xi'an, China, in 1998, 2001, and 2008, respectively. She is now with the School of Telecommunications Engineering, Xidian University.

Her research interests include wireless communications, channel coding design, and information theory.



**Li Ping** (S'87-M'91-SM'06) received his Ph.D degree at Glasgow University in 1990. He lectured at Department of Electronic Engineering, Melbourne University, from 1990 to 1992, and worked as a member of research staff at Telecom Australia Research Laboratories from 1993 to 1995. He has been with the Department of Electronic Engineering, City University of Hong Kong, since January 1996, where he is now a chair professor.

His research interests are communications systems and coding theory. Dr. Li Ping was awarded a British Telecom-Royal Society Fellowship in 1986, the IEE J J Thomson premium in 1993 and a Croucher Senior Research Fellowship in 2005.