Performance Analysis of Raptor Codes under Maximum Likelihood Decoding

Peng Wang, *Student Member, IEEE,* Guoqiang Mao, *Senior Member, IEEE,*
Zihuai Lin, *Senior Member, IEEE,* Ming Ding, *Member, IEEE,*
Weifa Liang, *Senior Member, IEEE,* Xiaohu Ge, *Senior Member, IEEE,*
and Zhiyun Lin, *Senior Member, IEEE*

***Abstract*—In this paper, we analyze the maximum likelihood decoding performance of Raptor codes with a systematic low-density generator-matrix code as the pre-code. By investigating the rank of the product of two random coefficient matrices, we derive upper and lower bounds on the decoding failure probability. The accuracy of our analysis is validated through simulations. Results of extensive Monte Carlo simulations demonstrate that for Raptor codes with different degree distributions and pre-codes, the bounds obtained in this paper are of high accuracy. The derived bounds can be used to design near-optimum Raptor codes with short and moderate lengths.**

***Index Terms*—Raptor codes; asymptotic analysis; maximum likelihood (ML) decoding; decoding failure probability.**

I. Introduction

Rateless codes have been increasingly used in many telecommunication systems [1], [2], [3], [4], including cellular networks and satellite communication systems. Recent work has shown that, by employing rateless codes, wireless transmission efficiency and reliability can be dramatically improved [5], [6].

Rateless codes are a class of *forward error correction* (FEC) codes with special properties, which were initially designed for the *binary erasure channel* (BEC). Compared with conventional FEC codes with a fixed code rate, rateless codes have a number of advantages. Firstly, similar as *low-density parity-check* (LDPC) codes, rateless codes can be implemented with far less complex encoding and decoding algorithms, which are attractive for implementation. Secondly, as suggested by the name, rateless codes are suitable for any code rate. They can automatically adapt to instantaneous channel states and do not require feedback channels [1], [3], [5]. This is because they can generate a potentially limitless stream of coded symbols, and all source symbols can be correctly decoded when there are a sufficient number of successfully received coded symbols. Hence, rateless codes are desirable for certain channels, such as erasure multicast or broadcast channels, whose real-time channel erasure probability is very difficult to capture or estimate. Furthermore, they have the potential to replace the conventional *automatic repeat request* (ARQ) mechanism as a new mechanism of transmission control protocol [7].

Among the well-known rateless codes, two codes stand out. One is the *Luby transform* (LT) codes [3], which are the first class of practical digital fountain codes with an average decoding cost in the order of $O(k\log(k))$ where k is the number of source symbols. The other is the Raptor codes [1], which are the first class of fountain codes with linear time encoding and decoding complexities. Raptor codes are concatenated codes, which combine a traditional FEC code with an LT code to relax the condition that all input (source) symbols need to be recovered in an LT decoder. Note that Raptor codes have already been standardized in *the 3rd Generation Partnership Project* (3GPP) [4] to efficiently disseminate data over a broadcast/multicast network to provide multimedia broadcast and multicast services.

Despite the successful application of Raptor codes in 3GPP, our understanding of Raptor codes is still incomplete due to a lack of complete theoretical analysis on their decoding error performance. Without analytical results, the optimization of the degree distribution and other parameters of Raptor codes would be extremely difficult.

In this paper, we investigate the performance of Raptor codes by theoretically analyzing their decoding failure probability under *maximum likelihood* (ML) decoding. The decoding failure probability is the probability that not all source symbols can be decoded by ML decoding from a given number of successfully received coded symbols. We consider a Raptor code ensemble with a systematic (n, k, η) *low-density generator matrix* (LDGM) code as the pre-code. In the case of the erasure channel, ML decoding is equivalent to solving a consistent system of m linear equations in k unknowns

This research is supported by Australian Research Council (ARC) Discovery projects DP110100538 and DP120102030 and Chinese National Science Foundation project 61428102. Zihuai Lin's research is supported by the Australian Research Council (ARC) Discovery project DP120100405.

Peng Wang is with the School of Electrical and Information Engineering, The University of Sydney, Australia and National ICT Australia (NICTA) Sydney (e-mail: wpwd1986@hotmail.com).

Guoqiang Mao is with the School of Computing and Communications, The University of Technology Sydney. He is also with Data61 Australia, Beijing University of Posts and Telecommunications and Huazhong University of Science and Technology. (e-mail: g.mao@ieee.org).

Zihuai Lin is with the School of Electrical and Information Engineering, The University of Sydney, Australia (e-mail: zihuai.lin@sydney.edu.au).

Ming Ding is with the National ICT Australia (NICTA) (e-mail: Ming.Ding@nicta.com.au).

Weifa Liang is with the Research School of Computer Science, The Australian National University, Australia (e-mail: wliang@cs.anu.edu.au).

Xiaohu Ge (corresponding author) is with the School of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China (email: xhge@mail.hust.edu.cn).

Zhiyun Lin is with the College of Electrical Engineering, Zhejiang University, China (email: linz@zju.edu.cn).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2016.2522403, IEEE Transactions on Communications

by means of *Gaussian elimination* (GE). In this paper, we investigate the decoding failure probability of Raptor codes by theoretically analyzing the rank of the product of two random coefficient matrices and deriving tight analytical bounds. The tightness of the bounds is confirmed by extensive Monte Carlo simulations. More specifically, the contributions of this paper are summarized in the following:

- Firstly, this paper provides analytical results (i.e. an upper bound and a lower bound) on the decoding failure performance of Raptor codes, using a systematic LDGM code as the pre-code and assuming ML decoding.
- Furthermore, simulations are conducted to validate the accuracy of the proposed bounds. That is, Raptor codes with different degree distributions and pre-codes are evaluated to verify the claims on the accuracy of the derived upper and lower bounds.

The rest of the paper is organized as follows. Section II reviews the related work. In Section III, a brief review of the encoding and decoding process of Raptor codes is given. In Section IV, a performance analysis of Raptor code is conducted by deriving an upper bound and a lower bound on the probability that not all source symbols can be successfully decoded by a receiver with a given number of successfully received coded symbols. Section V validates the analytical results through simulations, followed by concluding remarks in Section VI.

II. Related Work

In this section, we review related work on the analysis of the performance of Raptor codes.

In general, there are two inter-related metrics to measure the performance of Raptor codes. One is the bit error probability and the other is the decoding failure probability. To analyze the bit error probability of Raptor codes, Rahnavard et al. [7] proposed a method to compute the upper and the lower bounds on the bit error probability of Raptor codes under ML decoding over the *binary erasure channels* (BEC). Despite the advances in [7], their work can be further improved in the following aspects. Firstly, the authors in [7] used a stochastic parity-check codes, i.e. (n, k, η) LDPC code, as the pre-code of Raptor codes. All entries of the parity check matrix are assumed to be *independent and identically distributed* (i.i.d) Bernoulli random variables [7]. Contrary to this assumption, in 3GPP standard [4], the pre-code of the standardized Raptor codes is a systematic LDGM code. The use of the systematic LDGM code as the pre-code is to guarantee that the parity check matrix is a full-rank matrix. Secondly, Rahnavard et al. assumed that the erasures on intermediate bit level are independent. As explained in [8, Ch. 6.2.1], this assumption would only hold if a very long interleaver was used. Using an interleaver in this setup, however, is not reasonable. In [9], the authors derived the upper and the lower bounds on the bit error probability of Raptor codes over Rayleigh fading channels assuming ML decoding.

In [1], Shokrollahi analyzed the decoding failure probability of Raptor codes with a finite length assuming *belief propagation* (BP) decoding. The analysis relies on the computation of the failure probability of the LT codes under BP decoding, which was derived in [10]. ML decoding, on the other hand, is more computationally demanding than BP decoding for codes with a large length. The analysis of the decoding failure probability assuming ML decoding is however both important and significant, because it provides a benchmark on the optimum system performance that can be used to gauge the performance of other decoding schemes. Furthermore, in [8] a pseudo upper bound on the performance of Raptor codes under ML decoding was derived, under the assumption that the number of erasures correctable by the pre-code is small. This approximation is accurate only when the rate of the pre-code is sufficiently high. For the more general case, the decoding failure probability of Raptor codes still remains an open problem. In [11] it is shown that the rank profile of the constraint matrix of a Raptor code depends on the rank profile of the pre-code parity check matrix and the generator matrix of the LT code. The rank profile of the Raptor code cannot be determined if the rank profile of an LT code with a general degree distribution is unknown. In our previous work [6], we analyzed the rank profile of an LT code with a general degree distribution.

In this paper, we present theoretical analysis on the decoding failure probability of Raptor codes under ML decoding. We consider a Raptor code ensemble with a systematic (n, k, η) LDGM code as the pre-code to guarantee that the parity check matrix is a full-rank matrix. Furthermore, we take into account the fact that the residual erasure events after LT decoding are not independent, thereby deriving tighter bounds.

III. Background of Raptor Codes

This section is provided to familiarize the readers with the basic idea of Raptor codes, their encoding and decoding algorithms.

The encoding process of a Raptor code [1] is carried out in two phases: a) encode k source symbols with a (n, k) error correction code, which is referred to as the pre-code $\mathcal{C}$, to form n intermediate symbols; b) encode the n intermediate symbols with an LT code. Each coded symbol is generated by the following encoding rules of LT codes [3]. Firstly, a positive integer d (often referred to as the "degree" of coded symbols) is drawn from the set of integers $\{1, ..., n\}$ according to a probability distribution $\mathbf{\Omega} = (\Omega_1, ..., \Omega_n)$, where Ω_d is the probability that d is selected and $\sum_{d=1}^{k} \Omega_d = 1$. Then, d distinct intermediate symbols are selected randomly and independently from the n intermediate symbols to form the coded symbol to be transmitted using the XOR operation, where each intermediate symbol is selected with equal probability. A Raptor code with parameters $(k, \mathcal{C}, \mathbf{\Omega})$ is an LT code with distribution $\mathbf{\Omega} = (\Omega_1, ..., \Omega_n)$ on n symbols which are the output symbols of the pre-code $\mathcal{C}$.

An illustration of a Raptor code is given in Fig. 1. In practice, the parity check matrix of the pre-code of Raptor codes is a deterministic matrix. For example, in 3GPP standard [4], the parity check matrix of the pre-code of the standardized Raptor codes is a systematic deterministic matrix. Using a systematic deterministic matrix as the pre-code ensures that the parity

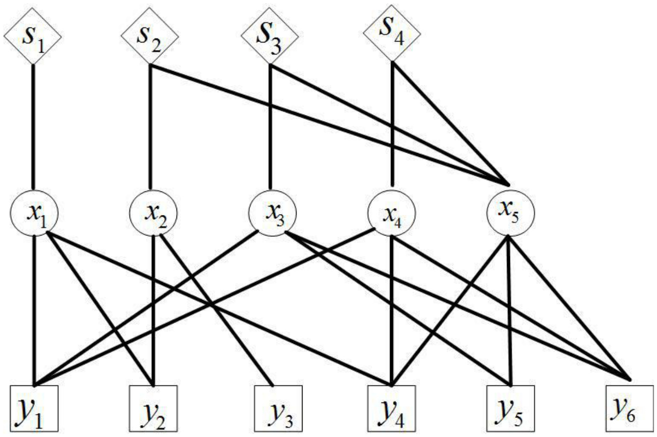


Figure 1. Two-stage structure of a Raptor code with a systematic pre-code.

check matrix of the pre-code is a full-rank matrix. However, it is difficult to obtain tractable analytical results of decoding performance for such Raptor codes. Therefore, in this paper we adopt a Raptor code ensemble with a semi-random (n, k, η) LDGM code as the pre-code for analytical tractability while ensuring that the parity check matrix of the pre-code is a full-rank matrix. The generator matrix of the pre-code, denoted by $\mathbf{G}_{n\times k}^{\text{pre}}$, can be written as $\mathbf{G}_{n\times k}^{\text{pre}} = [\mathbf{I}_k|\mathbf{P}_{k\times(n-k)}]^T$, where $\mathbf{I}_k$ is an identity matrix of size k, and $\mathbf{P}_{k\times(n-k)}$ is a k by $(n-k)$ matrix whose entries are i.i.d. Bernoulli random variables with parameter η. Such a code is denoted as an (n, k, η) LDGM code. Furthermore, we can obtain the parity check matrix of this LDGM code as $\mathbf{H}_{(n-k)\times n} = [\mathbf{P}_{(n-k)\times k}|\mathbf{I}_{(n-k)}]_{(n-k)\times n}$.

Let m, $(m \geq k)$, be the number of coded symbols that have already been successfully received by a receiver and $\gamma = \frac{m}{k}$, $(\gamma \geq 1)$ be the overhead of reception. When a coded symbol is received by a receiver, we use a $1 \times k$ binary row vector $\mathbf{g}_i^{\text{LT}}\mathbf{G}^{\text{pre}}$ to represent the coding information contained in the coded symbol, where $\mathbf{G}^{\text{LT}}$ is a $k\gamma \times n$ binary matrix, $\mathbf{g}_i^{\text{LT}}$ is the i^{th} row vector of $\mathbf{G}^{\text{LT}}$ and $\mathbf{G}^{\text{pre}}$ is a $n \times k$ binary matrix. Let $[\mathbf{G}]_{i,j}$ be the entry in the i^{th} row and the j^{th} column of the matrix $\mathbf{G}$. Particularly, $\left[\mathbf{g}_i^{LT}\right]_{1,j}$ is 1 if the coded symbol is a result of the XOR operation on the j^{th} intermediate symbol (and other intermediate symbols); otherwise $\left[\mathbf{g}_i^{LT}\right]_{1,j}$ equals 0. For $[\mathbf{G}^{\text{pre}}]_{i,j}$, it is 1 if the i^{th} intermediate symbol is a result of the XOR operation on the j^{th} source symbol (and other source symbols); otherwise $[\mathbf{G}^{\text{pre}}]_{i,j}$ equals 0. Therefore, a random row vector in this paper refers to the row vector of a randomly chosen coded symbol where the coded symbol is generated using the Raptor encoding process described above. Recall that $\mathbf{s} = (s_1, s_2, ..., s_k)$ represents the k source symbols to be transmitted. The coded symbol can be expressed as: $y_i = \mathbf{g}_i^{\text{LT}}\mathbf{G}^{\text{pre}}\mathbf{s}^T$, where "$\mathbf{s}^T$" is the transpose of $\mathbf{s}$.

Raptor codes can be decoded using a variety of decoding algorithms. A commonly used decoding algorithm for Raptor codes is the so-called "LT process" [3], but it is well known that the LT process is unable to decode all source symbols which can be possibly recovered from the received coded symbols. For example, the LT process relies on the existence of at least one degree-one coded symbol to be received in order to start the decoding process. For Raptor codes with limited lengths, ML decoding algorithm [12] has been proposed to replace the LT process. The performance of ML decoding is the same as the Gaussian elimination. One way to apply the Gaussian elimination on Raptor codes is to solve a system of linear equations given in the following.

$$\mathbf{G}_{k\gamma\times n}^{\text{LT}}\mathbf{G}_{n\times k}^{\text{pre}}\mathbf{s}_{k\times 1}^T \quad = \quad \mathbf{y}_{k\gamma\times 1},$$

where $\mathbf{y}_{k\gamma\times 1} = (y_1, y_2, ..., y_{k\gamma})^T$. Then we can obtain the following Lemma.

Lemma 1. *A receiver can recover all k source symbols from the $k\gamma$ coded symbols under ML decoding if and only if $(\mathbf{G}_{k\gamma\times n}^{LT}\mathbf{G}_{n\times k}^{pre})_{k\gamma\times k}$ is a full-rank matrix, i.e. its rank equals k [1].*

Note that in this paper, all algebraic operations and the associated analysis are conducted in a binary field $GF(2)$.

IV. Performance Analysis of Raptor Codes

Denote by $A_{k\gamma}^k$ the event that a receiver can successfully decode all k source symbols conditioned on the event that the receiver has successfully received $k\gamma$ coded symbols. Obviously the event that $(\mathbf{G}_{k\gamma\times n}^{\text{LT}}\mathbf{G}_{n\times k}^{\text{pre}})_{k\gamma\times k}$ is a full-rank matrix is equivalent to the event $A_{k\gamma}^k$. Let $\overline{A_{\gamma k}^k}$ be the complement of event $A_{k\gamma}^k$. The main results of this paper are summarized in Theorems 2 and 3.

In this section, we shall analyze the probability $\Pr\left[\overline{A_{\gamma k}^k}\right]$. The analysis of decoding failure probability $P_{k,n,\gamma}^{DF} = \Pr\left[\overline{A_{\gamma k}^k}\right]$ is conducted by analyzing the probability that the rank of $(\mathbf{G}_{k\gamma\times n}^{\text{LT}}\mathbf{G}_{n\times k}^{\text{pre}})_{k\gamma\times k}$ is not k.

A. Upper Bound on the Decoding Failure Probability of Raptor Codes

In this subsection, we will derive an upper bound on the decoding failure probability of Raptor codes with a systematic (n, k, η) LDGM code as the pre-code. The upper bound is formally stated in the following theorem.

Theorem 2. *When a receiver successfully receives $k\gamma$ coded symbols generated using the Raptor code $(k, \mathcal{C}, \Omega(x))$, where $\mathcal{C}$ is an (n, k, η) LDGM code, and the coded symbols received at the receiver are decoded using ML decoding, the probability that not all k source symbols can be successfully decoded by a receiver with the $k\gamma, (k\gamma \geq k)$, received coded symbols, denoted by $P_{k,n,\gamma}^{DF}$, is upper bounded by*

$$P_{k,n,\gamma}^{DF} \quad \leq \quad \sum_{i=1}^{k} \binom{k}{i} \sum_{r=i}^{n-k+i} \left(J\left(r\right)\right)^{k\gamma} D\left(i, r\right), \tag{1}$$

where

$$J(r) \quad = \quad \sum_{d=1}^{n} \Omega_d \frac{\sum_{s=0,2,...,2\left\lfloor \frac{d}{2} \right\rfloor} \binom{r}{s}\binom{n-r}{d-s}}{\binom{n}{d}} \tag{2}$$

and

$$D(i,r) = \tbinom{n-k}{r-i}\left[\frac{1+(1-2\eta)^i}{2}\right]^{n-k-r+i} \times \left[\frac{1-(1-2\eta)^i}{2}\right]^{r-i} \quad (3)$$

and Ω_d is the degree distribution of LT codes.

Proof: See Appendix A. ■

B. Lower Bound on the Decoding Failure Probability of Raptor Codes

In addition to the upper bound in the previous subsection, in the following paragraphs, we derive a lower bound on the decoding failure probability of Raptor codes which is formally stated in the following theorem.

Theorem 3. *When a receiver successfully receives $k\gamma$ coded symbols generated using the Raptor code $(k, \mathcal{C}, \Omega(x))$, where $\mathcal{C}$ is an (n, k, η) LDGM code, and the coded symbols received at the receiver are decoded using ML decoding, the probability that not all k source symbols can be successfully decoded by a receiver with the $k\gamma, (k\gamma \geq k)$, received coded symbols, denoted by $P^{DF}_{k,n,\gamma}$, is lower bounded by:*

$$\begin{aligned} &P^{DF}_{k,n,\gamma} \\ \geq\ & \sum_{i=1}^{k}\tbinom{k}{i} \sum_{r=i}^{n-k+i} (J(r))^{k\gamma} D(i,r) \\ & -\frac{1}{2}\sum_{i=1}^{k}\tbinom{k}{i} \sum_{w_0=0}^{i} \sum_{w_1=i-w_0} \sum_{w_2=0}^{k-i} \mathbf{1}(w_0+w_2)\mathbf{1}(w_1+w_2) \\ & \times \tbinom{i}{w_0}\tbinom{k-i}{w_2}\{ \sum_{r_0=w_0}^{n-k+w_0} \sum_{r_1=w_1}^{n-k+w_1} \sum_{r_0=w_2}^{n-k+w_2} D(w_0,r_0)D(w_1,r_1) \\ & \times D(w_2,r_2)[J(r_0)J(r_1)J(r_2) + \overline{J}(r_0)\overline{J}(r_1)\overline{J}(r_2)]\}^{k\gamma}, \quad (4) \end{aligned}$$

where $\mathbf{1}(x)$ is an indicator function, $\mathbf{1}(x) = 0$ if $x = 0$ and $\mathbf{1}(x) = 1$ otherwise, $\overline{J}(\cdot) = 1 - J(\cdot)$, $D(w_0, r_0)$ is defined in Eq. (3) and $J(r_0)$ is defined in Eq. (2).

Proof: See Appendix B. ■

C. A Special Case of the Derived Bounds

When we apply a special degree distribution - a binomial degree distribution [13] with $\Omega_d = \frac{\binom{n}{d}}{(2^n-1)}, 1 \leq d \leq n$, Eq. (1) can be further simplified into a much less (computationally) complex expression, for which Theorem 2 can be restated as the following Corollary.

Corollary 4. *When a receiver successfully receives $k\gamma$ coded symbols generated using the Raptor code $(k, \mathcal{C}, \Omega(x))$ where $\mathcal{C}$ is an (n, k, η) LDGM code, $\Omega(x) = \sum_{d=1}^{n} \frac{\binom{n}{d}x^d}{(2^n-1)}$, and the coded symbols received at the receiver are decoded using ML decoding, the probability that not all k source symbols can be successfully decoded by a receiver with the $k\gamma, (k\gamma \geq k)$, received coded symbols, denoted by $P^{DF}_{k,n,\gamma}$, satisfies*

$$P^{DF}_{k,n,\gamma} \quad \leq \quad (2^k-1)(\frac{(2^{n-1}-1)}{(2^n-1)})^{k\gamma}. \quad (5)$$

Proof: See Appendix C. ■

For Theorem 3, we can simplify the lower bound into a less (computationally) complex expression as well. This is summarized in the following Corollary.

Corollary 5. *When a receiver successfully receives $k\gamma$ coded symbols generated using the Raptor code $(k, \mathcal{C}, \Omega(x))$ where $\mathcal{C}$ is an (n, k, η) LDGM code, $\Omega(x) = \sum_{d=1}^{n} \frac{\binom{n}{d}x^d}{(2^n-1)}$, and the coded symbols received at the receiver are decoded using ML decoding, the probability that not all k source symbols can be successfully decoded by a receiver with the $k\gamma, (k\gamma \geq k)$, received coded symbols, denoted by $P^{DF}_{k,n,\gamma}$, satisfies*

$$\begin{aligned} &P^{DF}_{k,n,\gamma} \\ \geq\ & (2^k-1)\left[\frac{(2^{n-1}-1)}{(2^n-1)}\right]^{k\gamma} - (2^k-1)(2^{k-1}-1) \\ & \times \left\{\left[\frac{(2^{n-1}-1)}{(2^n-1)}\right]^3 + \left[1-\frac{(2^{n-1}-1)}{(2^n-1)}\right]^3\right\}^{k\gamma}. \quad (6) \end{aligned}$$

Proof: See Appendix D. ■

Compared with the general expressions in Theorems 2 and 3, the simplified expressions in Corollaries 4 and 5 allow us to easily observe the relationship between the decoding failure probability and the parameters of the encoding rules, i.e., k, n and γ. Additionally, the computation complexity of the derived upper bound can be reduced from $O(\frac{1}{2}n^2k(n-k))$ to $O(1)$. As for the lower bound, the computation complexity can be reduced from $O(\frac{1}{8}n^6k^3(n-k)^3)$ to $O(1)$.

V. Simulation Results

In this section, we shall validate the accuracy of the analytical results and the tightness of the proposed bounds, using MATLAB simulations. Each point shown in the figures is the average result obtained from 10^6 simulations. For clarity, the simulation parameters adopted in this section are summarized in Table I.

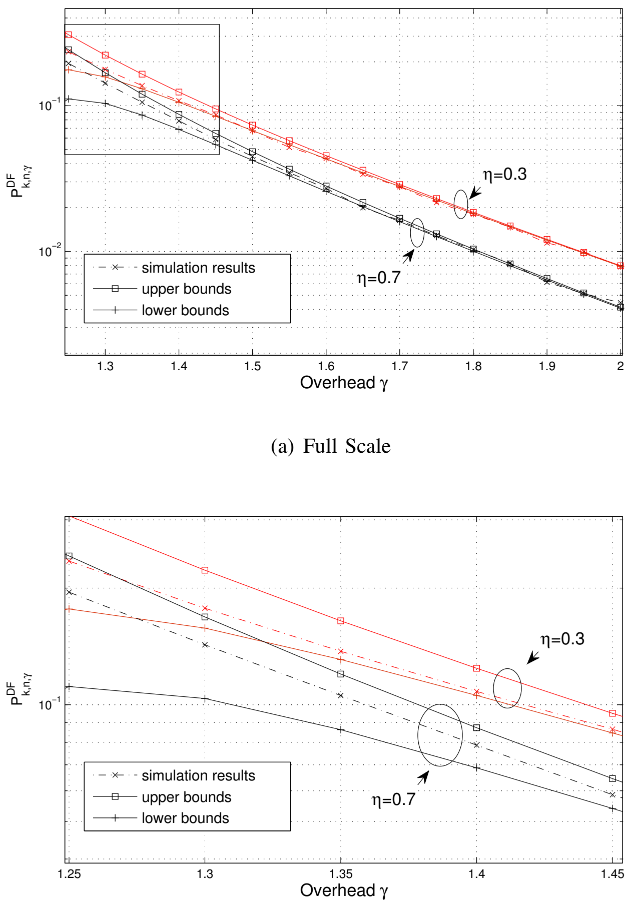
Table I
Simulation parameters

Rateless codes encoding parameters	
Number of source symbols k	$20, 40, 70$ and 100
Number of intermediate symbols n	$21, 42, 73$ and 105
Parameter for Bernoulli random variables η	0.3, 0.7
Pre-code $\mathcal{C}$	(n, k, η) LDGM code
Degree distributions	
Standard degree distribution	$\Omega^{3GPP}(x)$
Binomial degree distribution	$\Omega_d = \frac{\binom{n}{d}}{(2^n-1)}, 1 \leq d \leq n$
Ideal soliton degree distribution	$\Omega_d = \frac{1}{d(d-1)}, 2 \leq d \leq n$ and $\Omega_1 = \frac{1}{n}$

A. Verification of the Derived Bounds

In this subsection, the number of source symbols is set to be $k = 20$ and the degree distribution of Raptor codes follows the widely used ideal soliton degree distribution [3]. Besides, the pre-code $\mathcal{C}$ is assumed to be $(21, 20, 0.3)$ and $(21, 20, 0.7)$ LDGM codes respectively.

In Fig. 2(a) and 2(b), both analytical and simulation results are presented on $P^{DF}_{k,n,\gamma}$, the probability that not all $k = 20$



(a) Full Scale

(b) Zoom of the rectangular box in (a)

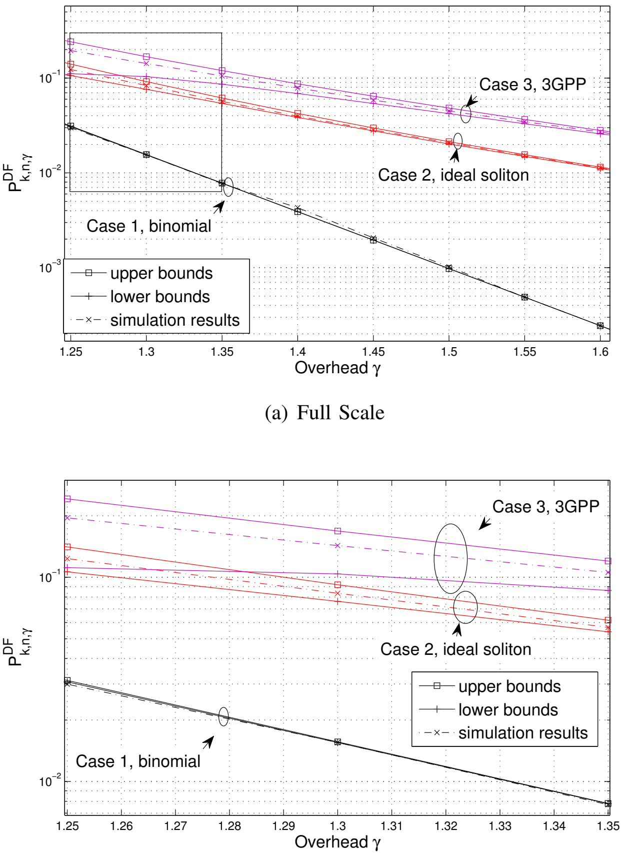
Figure 2. The decoding failure probabilities of Raptor codes with ideal soliton degree distribution and (n, k, η) LDGM codes as the pre-code versus overhead γ. Parameter for Bernoulli random variables η is set as 0.3 and 0.7.

source symbols can be successfully decoded by a receiver, for different values of the reception overhead $\gamma = m/k$. As shown in Fig. 2(a) and 2(b), our analytical results, i.e., the upper bound and the lower bound, match the simulation results very well. This validates the accuracy of the analysis. However, when the overhead γ is small, there is still a gap between the upper (lower) bound and simulation results in Fig. 2(a) and 2(b). The gap between the exact value and the upper bound is caused by the approximation used in Eq. (1), and the gap between the exact value and the lower bound is caused by Eq. (4).

B. Investigation of the Impact of Degree Distribution on the Decoding Failure Probability

In this subsection, we investigate the performance for different distributions of LT codes when we fix the pre-code $\mathcal{C}$ to be $(21, 20, 0.7)$. The investigated degree distributions are divided into three cases.

- Case 1 uses the binomial degree distribution [13].
- Case 2 investigates the widely used ideal soliton degree distribution [3].



(a) Full Scale

(b) Zoom of the rectangular box in (a)

Figure 3. The decoding failure probabilities of Raptor codes with $(n, k, 0.7)$ LDGM codes as the pre-code and different degree distributions versus overhead γ. The degree distributions of Raptor codes are chosen as ideal soliton degree distribution [3], the standardized degree distribution in 3GPP [4, Annex B] and binomial degree distribution [13].

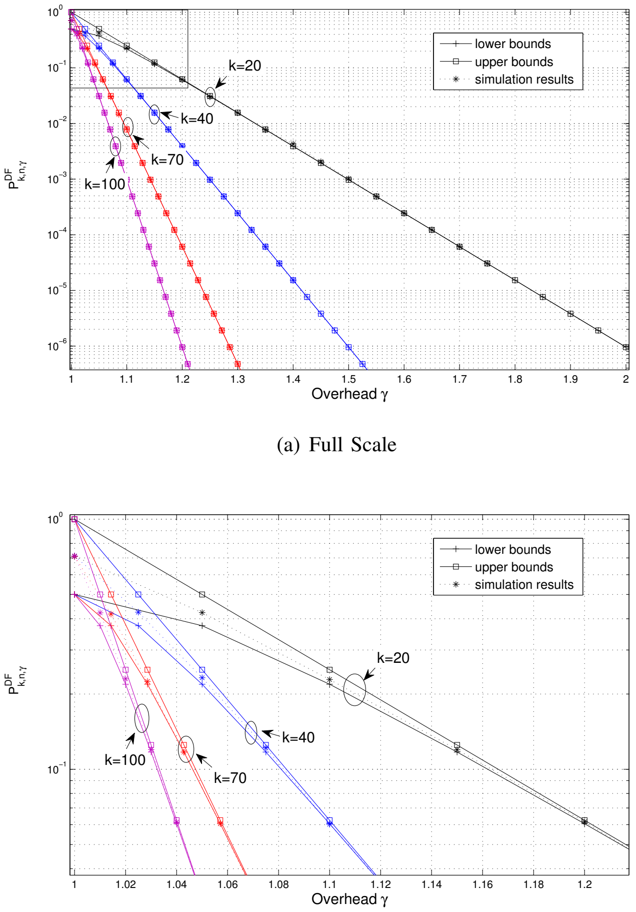
- Case 3 is the standardized degree distribution in 3GPP [4, Annex B]:

$$\begin{aligned}\Omega^{3GPP}(x) \;=\;& 0.0099x + 0.4663x^2 + 0.2144x^3 \\ & + 0.1152x^4 + 0.1131x^{10} + 0.0811x^{11}.\end{aligned}$$

As shown in Fig. 3(a) and 3(b), for different degree distributions, our analytical bounds agree very well with the simulation results. The performance of Raptor codes with the binomial degree distribution outperforms those obtained with the other three degree distributions. Furthermore, the decoding failure probability of Raptor codes with the binomial degree distribution in Corollaries 4 and 5 are less computationally demanding compared with those in Theorems 2 and 3. Therefore, we will use Raptor codes with the binomial degree distribution in the following simulations.

C. Investigation of the Impact of k on the Decoding Failure Probability of Raptor Codes

When the number of source symbols k varies from 20 to 100, our analytical results still match the simulation results very well. As shown in Fig. 4(a) and 4(b), at a larger value of the source symbols, a less reception overhead $\gamma = m/k$



(a) Full Scale

(b) Zoom of the rectangular box in (a)

Figure 4. The decoding failure probabilities of Raptor codes with the binomial degree distribution and $(n, k, 0.7)$ LDGM codes as the pre-code at different values of the overhead γ. The number of source symbols k is set to be 20, 40, 70 and 100 respectively.

is required to achieve the same performance on the decoding failure probability.

VI. Conclusion

In this paper we studied the performance of finite-length Raptor codes with a systematic LDGM code as the pre-code, and derived an upper bound and a lower bound on the decoding failure probability of Raptor codes under ML decoding. Due to the concatenated coding structure of Raptor codes, we analyzed the rank behavior of the product of two random matrices to obtain the decoding failure probability. Furthermore, by considering a special degree distribution, i.e. the binomial degree distribution, we derived the simplified upper and lower bounds. On the basis of the results presented in the paper, we shall explore the optimum degree distribution and optimal parameter setting of Raptor codes in different channels as our future work.

Acknowledgment

The authors would like to thank all the anonymous reviewers for their helpful comments and constructive suggestions to improve early drafts of this paper.

Appendix A
Proof of Theorem 2

In this appendix, we prove Theorem 2.

According to the property of the matrix product [14, Eq. (4.5.1)], we have

$$\begin{aligned} & rank(\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}) \\ = \; & rank(\mathbf{G}^{\text{pre}}_{n\times k}) - \dim\{N(\mathbf{G}^{\text{LT}}_{k\gamma\times n}) \cap R(\mathbf{G}^{\text{pre}}_{n\times k})\}, \quad (7) \end{aligned}$$

where $N(\bullet)$ is the right-hand null space of a matrix, $R(\bullet)$ is the column vector space generated by a matrix and $\dim\{\mathcal{V}\}$ represents the number of vectors in any basis for a vector space $\mathcal{V}$. It follows from the definition of $\mathbf{G}^{\text{pre}}_{n\times k}$ given earlier that the rank of $\mathbf{G}^{\text{pre}}_{n\times k}$ is k. It can then be readily obtained that

$$\begin{aligned} P^{DF}_{k,n,\gamma} &= \Pr[rank(\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}) \neq k] \\ &= \Pr[\dim\{N(\mathbf{G}^{\text{LT}}_{k\gamma\times n}) \cap R(\mathbf{G}^{\text{pre}}_{n\times k})\} \neq 0]. \quad (8) \end{aligned}$$

For convenience, let $W_{k\gamma,n,k}$ be the event that $\dim\{N(\mathbf{G}^{\text{LT}}_{k\gamma\times n}) \cap R(\mathbf{G}^{\text{pre}}_{n\times k})\} \neq 0$. Now we need to analyze $P^{DF}_{k,n,\gamma} = \Pr[W_{k\gamma,n,k}]$. Provided that $\mathbf{G}^{\text{pre}}_{n\times k}$ is the generator matrix of a systematic (n, k, η) LDGM code, the event $\dim\{N(\mathbf{G}^{\text{LT}}_{k\gamma\times n}) \cap R(\mathbf{G}^{\text{pre}}_{n\times k})\} \neq 0$, denoted by $W_{k\gamma,n,k}$, is equivalent to the event that at least one column vector from $R(\mathbf{G}^{\text{pre}}_{n\times k})$ is in $N(\mathbf{G}^{\text{LT}}_{k\gamma\times n})$, i.e., $\cup_{\mathbf{x}\in R(\mathbf{G}^{\text{pre}}_{n\times k})} \mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x} = \mathbf{0}$, where $\mathbf{x}$ is a column vector of $R(\mathbf{G}^{\text{pre}}_{n\times k})$. It can be readily shown that

$$\begin{aligned} \Pr[W_{k\gamma,n,k}] &= \Pr\left[\cup_{\mathbf{x}\in R(\mathbf{G}^{\text{pre}}_{n\times k})} \mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x} = \mathbf{0}\right] \\ &\leq \sum_{\mathbf{x}\in R(\mathbf{G}^{\text{pre}}_{n\times k})} \Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x} = \mathbf{0}\right]. \quad (9) \end{aligned}$$

The column vector space $R(\mathbf{G}^{\text{pre}}_{n\times k})$ is partitioned into k subspace $(\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_k)$ and $\mathcal{V}_i$ is the subspace that contains all the column vectors which are summation of i column vectors of $\mathbf{G}^{\text{pre}}_{n\times k}$. We denote ÎŞ$_i$ as the set of indices of the column vectors in $\mathcal{V}_i$ and there are $\binom{k}{i}$ elements in ÎŞ$_i$. Let $\mathbf{x}^i_a$ be the $a^{th}, a \in$ ÎŞ$_i$ column vector in $\mathcal{V}_i$. It can be shown that

$$\sum_{\mathbf{x}\in R(\mathbf{G}^{\text{pre}}_{n\times k})} \Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x} = \mathbf{0}] = \sum_{i=1}^{k} \sum_{a\in \text{ÎŞ}_i} \Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a = \mathbf{0}].(10)$$

Observe that $\mathbf{x}^i_a = \mathbf{G}^a_{n\times i}\mathbf{1}_i$ where $\mathbf{G}^a_{n\times i}$ is the matrix formed by i column vectors selected from k column vectors of $\mathbf{G}^{\text{pre}}_{n\times k}$ and $\mathbf{1}_i$ represent a $i \times 1$ all one column vector. Let $\left|\mathbf{x}^i_a\right|$ be the weight of column vector $\mathbf{x}^i_a$, using the law of total probability, we have

$$\begin{aligned} & \Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a = \mathbf{0}] \\ = \; & \sum_{r=0}^{n} \Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a = \mathbf{0} \middle| \left|\mathbf{x}^i_a\right| = r\right] \Pr\left[\left|\mathbf{x}^i_a\right| = r\right]. (11) \end{aligned}$$

Firstly, we need to calculate $\Pr\left[\left|\mathbf{x}^i_a\right| = r\right]$. Provided $\mathbf{G}^{\text{pre}}_{n\times k} = [\mathbf{I}_k|\mathbf{P}_{k\times(n-k)}]^T$, in the first k entries of $\mathbf{G}^a_{n\times i}\mathbf{1}_i$ there are i

ones. If $\left|\mathbf{x}_a^i\right| = r$, then there are $r-i$ ones in the last $n-k$ entries of $\mathbf{G}_{n\times i}^a \mathbf{1}_i$, .i.e, $\mathbf{P}_{(n-k)\times i}^a \mathbf{1}_i$. Hence we can obtain that

$$\Pr\left[\left|\mathbf{x}_a^i\right| = r\right] \;=\; \Pr\left[\left|\mathbf{P}_{(n-k)\times i}^a \mathbf{1}_i\right| = (r-i)\right], \quad (12)$$

and $i \le r \le n-k+i$. The rows of $\mathbf{P}_{(n-k)\times i}^a$, i.e., $\mathbf{p}_j, 1 \le j \le (n-k)$, are random binary row vectors, which are generated independently. Each entry of $\mathbf{P}_{(n-k)\times i}^a$ is i.i.d. Bernoulli random variable with parameter η. Therefore, $\Pr[\mathbf{p}_j \mathbf{1}_i = 0] = \Pr[\mathbf{p}_{k,k\neq j} \mathbf{1}_i = 0]$. The event that the j^{th} entry in $\mathbf{x}_a^i$ is zero is equivalent to the event that there are even number of ones in row vector $\mathbf{p}_j$. Thus we have

$$\begin{aligned}\Pr[\mathbf{p}_j \mathbf{1}_i = 0] &= \Pr\left[|\mathbf{p}_j| \text{ is even }\right] \\ &= \sum_{s=0,2,\ldots,2\left\lfloor \frac{i}{2}\right\rfloor} \tbinom{i}{s}\eta^s(1-\eta)^{(i-s)} \\ &= \frac{\left[(\eta+(1-\eta))^i + (-\eta+(1-\eta))^i\right]}{2} \\ &= \frac{1+(1-2\eta)^i}{2}. \qquad (13)\end{aligned}$$

There are $\binom{n-k}{r-i}$ possible *combinations* for $r-i$ ones in the last $n-k$ entries. It follows that

$$\begin{aligned}&\Pr\left[\left|\mathbf{P}_{(n-k)\times i}^a \mathbf{1}_i\right| = (r-i)\right] \\ =\;& \tbinom{n-k}{r-i}\{\Pr[\mathbf{p}_j\mathbf{1}_i = 0]\}^{n-k-r+i} \\ &\times\{1-\Pr[\mathbf{p}_j\mathbf{1}_i = 0]\}^{r-i}. \qquad (14)\end{aligned}$$

Combining Eq. (12), (13) and (14), we can obtain that

$$\begin{aligned}&D(i,r) = \Pr\left[\left|\mathbf{x}_a^i\right| = r\right] \\ =\;& \tbinom{n-k}{r-i}\left[\frac{1+(1-2\eta)^i}{2}\right]^{n-k-r+i} \\ &\times\left[\frac{1-(1-2\eta)^i}{2}\right]^{r-i}. \qquad (15)\end{aligned}$$

For $\mathbf{x}_a^i, \mathbf{x}_{b,b\neq a}^i \in \mathcal{V}_i$, $\mathbf{P}_{(n-k)\times i}^a$ and $\mathbf{P}_{(n-k)\times i}^b$ have the same probability to form the same matrix formation. So we can obtain that $\Pr\left[\left|\mathbf{P}_{(n-k)\times i}^a \mathbf{1}_i\right| = (r-i)\right] = \Pr\left[\left|\mathbf{P}_{(n-k)\times i}^b \mathbf{1}_i\right| = (r-i)\right]$, which in turn leads to the conclusion that $\Pr\left[\left|\mathbf{x}_a^i\right| = r\right] = \Pr\left[\left|\mathbf{x}_b^i\right| = r\right]$. Now, we calculate $\Pr\left[\mathbf{G}_{k\gamma\times n}^{LT}\mathbf{x}_a^i = 0 \mid \left|\mathbf{x}_a^i\right| = r\right]$. The rows of $\mathbf{G}_{\gamma k\times n}^{\mathrm{LT}}$, i.e., $\mathbf{g}_j^{\mathrm{LT}}, 1 \le j \le k\gamma$, are random binary row vectors, which are generated independently. We have

$$\begin{aligned}&\Pr\left[\mathbf{G}_{k\gamma\times n}^{\mathrm{LT}}\mathbf{x}_a^i = \mathbf{0}\middle|\, \left|\mathbf{x}_a^i\right| = r\right] \\ =&\left\{\Pr\left[\mathbf{g}_j^{\mathrm{LT}}\mathbf{x}_a^i = 0\middle|\, \left|\mathbf{x}_a^i\right| = r\right]\right\}^{k\gamma}. \qquad (16)\end{aligned}$$

The degree of $\mathbf{g}_j^{\mathrm{LT}}$, i.e. the number of non-zero elements of $\mathbf{g}_j^{\mathrm{LT}}$, is chosen according to the pre-defined degree distribution $\mathbf{\Omega} = (\Omega_1, \ldots, \Omega_n)$ and each non-zero element is then placed randomly and uniformly into $\mathbf{g}_j^{\mathrm{LT}}$. It can be readily obtain that

$$\begin{aligned}&\Pr\left[\mathbf{g}_j^{\mathrm{LT}}\mathbf{x}_a^i = 0\middle|\, \left|\mathbf{x}_a^i\right| = r\right] \\ =\;& \sum_{d=1}^{n}\Omega_d \Pr\left[\mathbf{g}_j^{\mathrm{LT}}\mathbf{x}_a^i = 0\middle|\, \left|\mathbf{x}_a^i\right| = r, \left|\mathbf{g}_j^{\mathrm{LT}}\right| = d\right]. \quad (17)\end{aligned}$$

Let $\mathbf{r}_j^i = (\mathbf{g}_{j1}^{\mathrm{LT}}\mathbf{x}_{a1}^i, \mathbf{g}_{j2}^{\mathrm{LT}}\mathbf{x}_{a2}^i, \ldots, \mathbf{g}_{jn}^{\mathrm{LT}}\mathbf{x}_{an}^i)$, where $\mathbf{g}_{jk}^{\mathrm{LT}}$ is $\left[\mathbf{g}_j^{\mathrm{LT}}\right]_{1,k}$ and $\mathbf{x}_{ak}^i$ is $\left[\mathbf{x}_a^i\right]_{k,1}$. Then, we can obtain that

$$\begin{aligned}&\Pr\left[\mathbf{g}_j^{\mathrm{LT}}\mathbf{x}_a^i = 0\middle|\, \left|\mathbf{x}_a^i\right| = r, \left|\mathbf{g}_j^{\mathrm{LT}}\right| = d\right] \\ =\;& \Pr\left[\left|\mathbf{r}_j^i\right| \text{ is even } \middle|\, \left|\mathbf{x}_a^i\right| = r, \left|\mathbf{g}_j^{\mathrm{LT}}\right| = d\right] \\ =\;& \frac{\sum_{s=0,2,\ldots,2\left\lfloor\frac{d}{2}\right\rfloor}\binom{r}{s}\binom{n-r}{d-s}}{\binom{n}{d}}. \qquad (18)\end{aligned}$$

Combining Eq. (17) and (18), we can obtain that

$$\begin{aligned}J(r) &= \Pr\left[\mathbf{g}_j^{\mathrm{LT}}\mathbf{x}_a^i = 0\middle|\, \left|\mathbf{x}_a^i\right| = r\right] \\ &= \sum_{d=1}^{n}\Omega_d\frac{\sum_{s=0,2,\ldots,2\left\lfloor\frac{d}{2}\right\rfloor}\binom{r}{s}\binom{n-r}{d-s}}{\binom{n}{d}}. \qquad (19)\end{aligned}$$

Incorporating Eq. (16) into (19), it can be established that

$$\Pr\left[\mathbf{G}_{k\gamma\times n}^{\mathrm{LT}}\mathbf{x}_a^i = \mathbf{0}\middle|\, \left|\mathbf{x}_a^i\right| = r\right] \;=\; [J(r)]^{k\gamma}. \quad (20)$$

We can obtain that $\Pr[\mathbf{G}_{k\gamma\times n}^{\mathrm{LT}}\mathbf{x}_a^i = \mathbf{0} \mid \left|\mathbf{x}_a^i\right| = r]$ is only determined by the weight of $\mathbf{x}_a^i$ rather than which i column vectors is chosen from $\mathbf{G}_{n\times k}^{\mathrm{pre}}$ to obtain the summation $\mathbf{x}_a^i$. So we can conclude that $\Pr[\mathbf{G}_{k\gamma\times n}^{\mathrm{LT}}\mathbf{x}_a^i = \mathbf{0}] = \Pr[\mathbf{G}_{k\gamma\times n}^{\mathrm{LT}}\mathbf{x}_b^i = \mathbf{0}]$. Recall that there are $\binom{k}{i}$ indices in ÎŞ_i. Combining Eq. (15), (20), (11) and Eq. (10), yields the following results

$$\begin{aligned}&P_{k,n,\gamma}^{DF} = \Pr[W_{k\gamma,n,k}] \\ \le\;& \sum_{i=1}^{k}\sum_{a\in\text{ÎŞ}_i}\Pr\left[\mathbf{G}_{k\gamma\times n}^{\mathrm{LT}}\mathbf{x}_a^i = \mathbf{0}\right] \\ =\;& \sum_{i=1}^{k}\tbinom{k}{i}\sum_{r=i}^{n-k+i}\tbinom{n-k}{r-i}\left[\sum_{d=1}^{n}\Omega_d\frac{\sum_{s=0,2,\ldots,2\left\lfloor\frac{d}{2}\right\rfloor}\binom{r}{s}\binom{n-r}{d-s}}{\binom{n}{d}}\right]^{k\gamma} \\ \times\;& \left[\frac{1+(1-2\eta)^i}{2}\right]^{n-k-r+i}\left[\frac{1-(1-2\eta)^i}{2}\right]^{r-i}, \qquad (21)\end{aligned}$$

which proves the theorem.

Appendix B
PROOF OF THEOREM 3

Similar as that in [7, Lemma 10], by using the Bonferroni inequality [15], we can obtain a lower bound of $\Pr[W_{k\gamma,n,k}]$ as

$$\begin{aligned}&P_{k,n,\gamma}^{DF} = \Pr[W_{k\gamma,n,k}] \\ =\;& \Pr[\cup_{\mathbf{x}\in R(\mathbf{G}_{n\times k}^{\mathrm{pre}})}\mathbf{G}_{k\gamma\times n}^{\mathrm{LT}}\mathbf{x} = \mathbf{0}] \\ \overset{(a)}{\ge}\;& \sum_{\mathbf{x}\in R(\mathbf{G}_{n\times k}^{\mathrm{pre}})}\Pr[\mathbf{G}_{k\gamma\times n}^{\mathrm{LT}}\mathbf{x} = \mathbf{0}] \\ &-\frac{1}{2}\sum_{\mathbf{x},\mathbf{y}\in R(\mathbf{G}_{n\times k}^{\mathrm{pre}}),\mathbf{x}\neq\mathbf{y}}\Pr[\mathbf{G}_{k\gamma\times n}^{\mathrm{LT}}\mathbf{x} = \mathbf{0}\cap\mathbf{G}_{k\gamma\times n}^{\mathrm{LT}}\mathbf{y} = \mathbf{0}], (22)\end{aligned}$$

where $\mathbf{x} = \mathbf{G}_{n\times k}^{\mathrm{pre}}\mathbf{a}, \mathbf{a} \in GF(2)^k$ and $\mathbf{y} = \mathbf{G}_{n\times k}^{\mathrm{pre}}\mathbf{b}, \mathbf{b} \in GF(2)^k\backslash\mathbf{a}$. The first term can be calculated by using Theorem 2. Recall that $\mathcal{V}_i$ is a subspace that contain all the column vectors which are summation of i column vectors of $\mathbf{G}_{n\times k}^{\mathrm{pre}}$, ÎŞ_i is the set of indices of the column vectors in $\mathcal{V}_i$ and $\mathbf{x}_a^i$

represents the $a^{th}, a \in \hat{\text{I}}\text{Ş}_i$ column vectors in $\mathcal{V}_i$. It can be readily shown that

$$\sum_{\mathbf{x},\mathbf{y}\in R(\mathbf{G}^{\text{pre}}_{n\times k}),\mathbf{x}\neq\mathbf{y}} \Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}=\mathbf{0}\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y}=\mathbf{0}]$$
$$=\sum_{\mathbf{x}\in R(\mathbf{G}^{\text{pre}}_{n\times k})}\ \sum_{\mathbf{y}\in R(\mathbf{G}^{\text{pre}}_{n\times k})\backslash\mathbf{x}} \Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}=\mathbf{0}\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y}=\mathbf{0}]$$
$$=\sum_{i=1}^{k}\sum_{a\in\hat{\text{I}}\text{Ş}_i}\ \sum_{\mathbf{y}\in R(\mathbf{G}^{\text{pre}}_{n\times k})\backslash\mathbf{x}^i_a} \Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a=\mathbf{0}\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y}=\mathbf{0}],\tag{23}$$

where $\mathbf{x}^i_a=\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{a}, |\mathbf{a}|=i$. Recall that $\mathbf{y}=\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{b}, \mathbf{b}\in GF(2)^k$. We define three binary vectors $\mathbf{z}_0$, $\mathbf{z}_1$, and $\mathbf{z}_2\in GF(2)^k$ such that for $t=1,...,k, \mathbf{z}_0(t)=1$ if and only if $\mathbf{a}(t)=1$ and $\mathbf{b}(t)=1$, $\mathbf{z}_1(t)=1$ if and only if $\mathbf{a}(t)=1$ and $\mathbf{b}(t)=0$, and $\mathbf{z}_2(t)=1$ if and only if $\mathbf{a}(t)=0$ and $\mathbf{b}(t)=1$. Let w_0, w_1 and w_2 be the weights of vectors $\mathbf{z}_0$, $\mathbf{z}_1$, and $\mathbf{z}_2$, respectively. For $\mathbf{x}^i_a$, we have $\mathbf{z}_0+\mathbf{z}_1=\mathbf{a}$ and $\mathbf{z}_0+\mathbf{z}_2=\mathbf{b}$. Hence we can obtain

$$\begin{aligned}&\Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a=\mathbf{0}\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y}=\mathbf{0}\right]\\ =\ &\Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_0=\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_1\right.\\ &\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_1=\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_2\\ &\left.\Big|\,|\mathbf{z}_0|=w_0\cap|\mathbf{z}_1|=w_1\cap|\mathbf{z}_2|=w_2\right].\end{aligned}\tag{24}$$

Let $I_{\mathbf{z}}=\{i_{\mathbf{z}1},i_{\mathbf{z}2},...,i_{\mathbf{z}\tau}\}$ be the set of indices such that $t\in I_{\mathbf{z}}$ for $\mathbf{z}(t)=1$, we can obtain the sets of indices of vectors $\mathbf{z}_0$, $\mathbf{z}_1$, and $\mathbf{z}_2$ as $I_{\mathbf{z}_0}$, $I_{\mathbf{z}_1}$ and $I_{\mathbf{z}_2}$. Corresponding to the three sets $I_{\mathbf{z}_0}$, $I_{\mathbf{z}_1}$ and $I_{\mathbf{z}_2}$, each column of the matrix $\mathbf{G}^{pre}_{n\times k}$, $\mathbf{g}^{pre}_i, 1\leq i\leq k$, can be divided into four mutually exclusive parts, $\mathbf{g}_{\mathbf{z}_0}$, $\mathbf{g}_{\mathbf{z}_1}$, $\mathbf{g}_{\mathbf{z}_2}$ and $\cup_{1\leq i\leq k}\mathbf{g}^{pre}_i\backslash(\mathbf{g}_{\mathbf{z}_0}\cup\mathbf{g}_{\mathbf{z}_1}\cup\mathbf{g}_{\mathbf{z}_2})$, i.e., $\mathbf{g}_{\mathbf{z}_0}\cap\mathbf{g}_{\mathbf{z}_1}=\{0\}$. Let $\mathbf{g}_{\mathbf{z}_0}$ be the subset of $\cup_{1\leq i\leq k}\mathbf{g}^{pre}_i$ such that all the elements of this subset are selected from $\cup_{1\leq i\leq k}\mathbf{g}^{pre}_i$ according to the indices in set $I_{\mathbf{z}_0}$ and $\mathbf{G}^{pre}_{\mathbf{z}_0}$ be the matrix whose columns are elements of $\mathbf{g}_{\mathbf{z}_0}$. The length of $\mathbf{g}_{\mathbf{z}_0}$ is w_0. The same operation is applied to the formation of $\mathbf{g}_{\mathbf{z}_1}$ and $\mathbf{g}_{\mathbf{z}_2}$, in which the elements are selected according to the indices in set $I_{\mathbf{z}_1}$ and $I_{\mathbf{z}_2}$, and have lengths w_1 and w_2, respectively. Let $\mathbf{x}^{w_0}=\mathbf{G}^{pre}_{\mathbf{z}_0}\mathbf{1}_{w_0}$, $\mathbf{x}^{w_1}=\mathbf{G}^{pre}_{\mathbf{z}_1}\mathbf{1}_{w_1}$ and $\mathbf{x}^{w_2}=\mathbf{G}^{pre}_{\mathbf{z}_2}\mathbf{1}_{w_2}$. Equivalently, Eq. (30) can be rewritten as,

$$\begin{aligned}&\Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_0=\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_1\right.\\ &\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_1=\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_2\\ &\left.\Big|\,|\mathbf{z}_0|=w_0\cap|\mathbf{z}_1|=w_1\cap|\mathbf{z}_2|=w_2\right]\\ =&\Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^{w_0}=\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^{w_1}\right.\\ &\left.\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^{w_1}=\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^{w_2}\right].\end{aligned}\tag{25}$$

Recall that the rows of $\mathbf{G}^{\text{LT}}_{k\gamma\times n}$, i.e., $\mathbf{g}^{\text{LT}}_j, 1\leq j\leq k\gamma$, are random binary row vectors, which are generated independently. We have

$$\begin{aligned}&\Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^{w_0}=\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^{w_1}\right.\\ &\left.\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^{w_1}=\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^{w_2}\right]\\ =&\left\{\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}\right.\right.\\ &\left.\left.\cap\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}=\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_2}\right]\right\}^{k\gamma}.\end{aligned}\tag{26}$$

According to the law of total probability, we have

$$\begin{aligned}&\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}\right.\\ &\left.\cap\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}=\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_2}\right]\\ =&\sum_{r_0=w_0}^{n-k+w_0}\ \sum_{r_1=w_1}^{n-k+w_1}\ \sum_{r_0=w_2}^{n-k+w_2}\Pr[|\mathbf{x}^{w_0}|=r_0]\\ \times&\Pr[|\mathbf{x}^{w_1}|=r_1]\Pr[|\mathbf{x}^{w_2}|=r_2]\\ \times&\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}\right.\\ &\cap\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}=\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_2}\\ &\left.\Big|\,|\mathbf{x}^{w_0}|=r_0\cap|\mathbf{x}^{w_1}|=r_1\cap|\mathbf{x}^{w_2}|=r_2\right]\end{aligned}\tag{27}$$

For $\Pr[|\mathbf{x}^{w_0}|=r_0]$, this can be calculated by using Eq. (15). Because all algebraic operations are conducted in a binary field, $\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}$ can only be 1 or 0. Eq. (27) can be further written as :

$$\begin{aligned}&\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}\cap\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}=\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_2}\right.\\ &\left.\Big|\,|\mathbf{x}^{w_0}|=r_0\cap|\mathbf{x}^{w_1}|=r_1\cap|\mathbf{x}^{w_2}|=r_2\right]\\ =&\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=0\cap\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}=0\cap\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_2}=0\right.\\ &\left.\Big|\,|\mathbf{x}^{w_0}|=r_0\cap|\mathbf{x}^{w_1}|=r_1\cap|\mathbf{x}^{w_2}|=r_2\right]\\ +&\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=1\cap\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}=1\cap\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_2}=1\right.\\ &\left.\Big|\,|\mathbf{x}^{w_0}|=r_0\cap|\mathbf{x}^{w_1}|=r_1\cap|\mathbf{x}^{w_2}|=r_2\right].\end{aligned}\tag{28}$$

Recall that $\mathbf{x}^{w_0}=\mathbf{G}^{\text{pre}}_{\mathbf{z}_0}\mathbf{1}_{w_0}$, $\mathbf{x}^{w_1}=\mathbf{G}^{\text{pre}}_{\mathbf{z}_1}\mathbf{1}_{w_1}$, $\mathbf{x}^{w_2}=\mathbf{G}^{\text{pre}}_{\mathbf{z}_2}\mathbf{1}_{w_2}$ and the columns of $\mathbf{G}^{\text{pre}}_{\mathbf{z}_0}$, $\mathbf{G}^{\text{pre}}_{\mathbf{z}_1}$, $\mathbf{G}^{\text{pre}}_{\mathbf{z}_2}$ are mutually exclusive to each other. So event that $|\mathbf{x}^{w_0}|=r_0$ is independent of event that $|\mathbf{x}^{w_1}|=r_1$ or $|\mathbf{x}^{w_2}|=r_2$ and the event that $\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=1$ is independent of event that $\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}=1$ or $\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_2}=1$. Conditioned on $|\mathbf{x}^{w_0}|=r_0, |\mathbf{x}^{w_1}|=r_1, |\mathbf{x}^{w_2}|=r_2$, the first part in Eq. (28) can be expressed as:

$$\begin{aligned}&\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=0\cap\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}=0\cap\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_2}=0\right.\\ &\left.\Big|\,|\mathbf{x}^{w_0}|=r_0\cap|\mathbf{x}^{w_1}|=r_1\cap|\mathbf{x}^{w_2}|=r_2\right]\\ =&\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=0\Big|\,|\mathbf{x}^{w_0}|=r_0\right]\\ &\times\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_1}=0\Big|\,|\mathbf{x}^{w_1}|=r_1\right]\\ &\times\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_2}=0\Big|\,|\mathbf{x}^{w_2}|=r_2\right].\end{aligned}\tag{29}$$

Based on the *previous* analysis, we know that $\Pr[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=0\Big|\,|\mathbf{x}^{w_0}|=r_0]$ only relates to parameter r_0. Let $D(w_0,r_0)=\Pr[|\mathbf{x}^{w_0}|=r_0]$ and $J(r_0)=\Pr[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=0|\,|\mathbf{x}^{w_0}|=r_0]$. For $J(r_0)$, it can be calculated by using Eq. (17) and (18). Based on the previous analysis,, we know that $J(r_0)$ only relates to parameter r_0 and $D(w_0,r_0)$ is affected by parameter r_0 and w_0. Hence for the same parameters w_0, w_1 and w_2, Eq. (25) has the same result. Because $\mathbf{x}^i_a\neq\mathbf{y}$, we can obtain that $w_1+w_2\neq 0$ and $w_0+w_2\neq 0$. For $\mathbf{x}^i_a$, when $|\mathbf{z}_0|=w_0$, we have $w_1=i-w_0$ and there are $\binom{i}{w_0}$ possible combinations of $\mathbf{z}_0$. For $\mathbf{z}_2$, there are $\binom{k-i}{w_2}$ possible combination of $\mathbf{z}_2$ when $|\mathbf{z}_2|=w_2$. Inserting Eq. (25), (27), (27), (28) and (29) into

(24), we can obtain:

$$\sum_{\mathbf{y}\in R(\mathbf{G}^{\text{pre}}_{n\times k})\backslash\mathbf{x}^i_a} \Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a=\mathbf{0}\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y}=\mathbf{0}]$$
$$=\sum_{w_0=0}^{i}\sum_{w_1=i-w_0}\sum_{w_2=0}^{k-i}\mathbf{1}(w_0+w_2)\mathbf{1}(w_1+w_2)\tbinom{i}{w_0}\tbinom{k-i}{w_2}$$
$$\times\{\sum_{r_0=w_0}^{n-k+w_0}\sum_{r_1=w_1}^{n-k+w_1}\sum_{r_0=w_2}^{n-k+w_2}D(w_0,r_0)D(w_1,r_1)D(w_2,r_2)$$
$$[J(r_0)J(r_1)J(r_2)+\overline{J}(r_0)\overline{J}(r_1)\overline{J}(r_2)]\}^{\gamma k}, \qquad (30)$$

where $\mathbf{1}(x):=\begin{cases}0 & \text{if } x=0\\ 1 & otherwise\end{cases}$.

For $\mathbf{x}^i_a,\mathbf{x}^i_{b,b\neq a}\in\mathcal{V}_i$, the probability $\sum_{\mathbf{x}^i_a\neq\mathbf{y}}\Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a=\mathbf{0}\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y}=\mathbf{0}\right]$ is affected by parameter i. So we can obtain that $\sum_{\mathbf{x}^i_a\neq\mathbf{y}}\Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a=\mathbf{0}\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y}=\mathbf{0}]=\sum_{\mathbf{x}^i_b\neq\mathbf{y}}\Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_b=\mathbf{0}\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y}=\mathbf{0}]$. Recall that there are $\tbinom{k}{i}$ indices in $\hat{\text{IŞ}}^i$. We can get that

$$\sum_{\mathbf{x},\mathbf{y}\in R(\mathbf{G}^{\text{pre}}_{n\times k}),\mathbf{x}\neq\mathbf{y}}\Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}=\mathbf{0}\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y}=\mathbf{0}]$$
$$=\sum_{i=1}^{k}\sum_{a\in\hat{\text{IŞ}}_i}\sum_{\mathbf{y}\in R(\mathbf{G}^{\text{pre}}_{n\times k})\backslash\mathbf{x}^i_a}\Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a=\mathbf{0}\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y}=\mathbf{0}]$$
$$=\sum_{i=1}^{k}\tbinom{k}{i}\sum_{w_0=0}^{i}\sum_{w_1=i-w_0}\sum_{w_2=0}^{k-i}\mathbf{1}(w_0+w_2)\mathbf{1}(w_1+w_2)$$
$$\times\tbinom{i}{w_0}\tbinom{k-i}{w_2}\{\sum_{r_0=w_0}^{n-k+w_0}\sum_{r_1=w_1}^{n-k+w_1}\sum_{r_0=w_2}^{n-k+w_2}D(w_0,r_0)D(w_1,r_1)$$
$$\times D(w_2,r_2)[J(r_0)J(r_1)J(r_2)+\overline{J}(r_0)\overline{J}(r_1)\overline{J}(r_2)]\}^{k\gamma}. \qquad (31)$$

This completes the proof of Theorem 3.

Appendix C
Proof of Corollary 4

When the binomial degree distribution (the expurgated standard random ensemble) [8], [13], i.e., $\Omega_d=\frac{\binom{n}{d}}{(2^n-1)}, 1\leq d\leq n$, is inserted into Eq. (17), we can obtain that

$$\Pr[\mathbf{g}^{\text{LT}}_j\mathbf{x}^i_a=0\mid\left|\mathbf{x}^i_a\right|=r]$$
$$=\ (2^n-1)^{-1}\sum_{d=1}^{n}\sum_{s=0,2,\ldots,2\left\lfloor\frac{d}{2}\right\rfloor}\tbinom{r}{s}\tbinom{n-r}{d-s}. \qquad (32)$$

Similar to [13, Lemma 2], when the upper limit of the inner summation is changed from $2\left\lfloor\frac{d}{2}\right\rfloor$ to $2\left\lfloor\frac{n}{2}\right\rfloor$, it will not affect the result of Eq. (32). This is because $\tbinom{n-r}{d-s}$ with $s>2\left\lfloor\frac{d}{2}\right\rfloor$ equals 0.

$$\Pr[\mathbf{g}^{\text{LT}}_j\mathbf{x}^i_a=0\mid\left|\mathbf{x}^i_a\right|=r]$$
$$=\ (2^n-1)^{-1}\sum_{d=1}^{n}\sum_{s=0,2,\ldots,2\left\lfloor\frac{n}{2}\right\rfloor}\tbinom{r}{s}\tbinom{n-r}{d-s}$$
$$\overset{a}{=}\ (2^n-1)^{-1}\sum_{s=0,2,\ldots,2\left\lfloor\frac{n}{2}\right\rfloor}\tbinom{r}{s}\sum_{d=1}^{n}\tbinom{n-r}{d-s}. \qquad (33)$$

The reason why the order of the two summations in Eq. (33) can be exchanged is because the inner summation variable s is now independent of the outer summation variable d. Note that $1\leq d\leq n$. Now we want to change the lower limit of the inner summation of Eq. (33) from 1 to 0 without affecting its result.

$$\Pr\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^i_a=0\mid\left|\mathbf{x}^i_a\right|=r\right]$$
$$=(2^n-1)^{-1}\{\sum_{s=0,2,\ldots,2\left\lfloor\frac{n}{2}\right\rfloor}\tbinom{r}{s}[\sum_{d=0}^{n}\tbinom{n-r}{d-s}-\tbinom{n-r}{d-s}_{d=0}]\}$$
$$\overset{b}{=}(2^n-1)^{-1}[\sum_{s=0,2,\ldots,2\left\lfloor\frac{n}{2}\right\rfloor}\tbinom{r}{s}\sum_{d=0}^{n}\tbinom{n-r}{d-s}-\tbinom{r}{s}\tbinom{n-r}{d-s}_{s=d=0}].(34)$$

Step (b) is because the term $\tbinom{n-r}{d-s}_{d=0}$ equals 0 for $s\neq 0$. Hence, only the case $s=0$ needs to be considered. The terms $\tbinom{n-r}{d-s}$ restricts d to $s\leq d\leq n-r+s$, such that

$$\sum_{d=0}^{n}\tbinom{n-r}{d-s}\ =\ \sum_{d=s}^{n-r+s}\tbinom{n-r}{d-s}=\sum_{d=0}^{n-r}\tbinom{n-r}{d}=2^{n-r}. \qquad (35)$$

Combining this term with the last expression for $\Pr[\mathbf{g}^{LT}_j\mathbf{x}^i_a=0\mid\left|\mathbf{x}^i_a\right|=r]$ yields

$$\left[\mathbf{g}^{\text{LT}}_j\mathbf{x}^i_a=0\mid\left|\mathbf{x}^i_a\right|=r\right]$$
$$=\ (2^n-1)^{-1}\left(2^{n-r}\sum_{s=0,2,\ldots,2\left\lfloor\frac{n}{2}\right\rfloor}\tbinom{r}{s}-1\right)$$
$$=\ (2^n-1)^{-1}(2^{n-r}2^{r-1}-1) \qquad (36)$$
$$=\ \frac{(2^{n-1}-1)}{(2^n-1)}, \qquad (37)$$

where we have used identity $\sum_{s\text{ even}}\tbinom{r}{s}=2^{r-1}$. We can observe that $\Pr[\mathbf{g}^{\text{LT}}_j\mathbf{x}^i_a=0\mid\left|\mathbf{x}^i_a\right|=r]$ is independent from the weight of $\mathbf{x}^i_a$, hence $\Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a=0|\left|\mathbf{x}^i_a\right|=r]=\Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}^i_a=0]$. Combining Eq. (16), (37), (10) and (8), we can obtain that

$$P^{DF}_{k,n,\gamma}=\Pr[W_{k\gamma,n,k}]$$
$$=\ \Pr\left[\cup_{\mathbf{x}\in R(\mathbf{G}^{\text{pre}}_{n\times k})}\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}=0\right]$$
$$\leq\ \sum_{\mathbf{x}\in R(\mathbf{G}^{\text{pre}}_{n\times k})}\Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}=0\right]$$
$$=\ (2^k-1)\Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}=0||\mathbf{x}|=r\right]$$
$$=\ (2^k-1)(\frac{(2^{n-1}-1)}{(2^n-1)})^{k\gamma}. \qquad (38)$$

The proof of Corollary 4 is completed.

Appendix D
Proof of Corollary 5

When the binomial degree distribution is inserted into Eq. (13), by using the result of Eq. (37), we can obtain that

$$J(r_0)\ =\ \Pr[\mathbf{g}^{\text{LT}}_j\mathbf{x}^{w_0}=0||\mathbf{x}^{w_0}|=r_0]$$
$$=\ \frac{(2^{n-1}-1)}{(2^n-1)}. \qquad (39)$$

Insert Eq. (39) into Eq. (25), we can obtain that

$$\begin{aligned} &\Pr\left[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_0 = \mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_1\right. \\ &\cap\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_1 = \mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{G}^{\text{pre}}_{n\times k}\mathbf{z}_2 \\ &\left.\mid |\mathbf{z}_0| = w_0 \cap |\mathbf{z}_1| = w_1 \cap |\mathbf{z}_2| = w_2\right] \\ = &\sum_{r_0=w_0}^{n-k+w_0}\sum_{r_1=w_1}^{n-k+w_1}\sum_{r_0=w_2}^{n-k+w_2} D(w_0,r_0)D(w_1,r_1)D(w_2,r_2) \\ \times &\{[\frac{(2^{n-1}-1)}{(2^n-1)}]^3 + [1-\frac{(2^{n-1}-1)}{(2^n-1)}]^3\}^{k\gamma} \\ = &\{[\frac{(2^{n-1}-1)}{(2^n-1)}]^3 + [1-\frac{(2^{n-1}-1)}{(2^n-1)}]^3\}^{k\gamma}. \end{aligned} \tag{40}$$

Incorporating Eq. (40) into Eq. (30), we can obtain that

$$\begin{aligned} &\sum_{\mathbf{x}_a^i\neq\mathbf{y}} \Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x}_a^i = 0 \cap \mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y} = 0] \\ = &\sum_{w_0=0}^{i}\sum_{w_1=i-w_0}\sum_{w_2=0}^{k-i} \mathbf{1}(w_0+w_2)\mathbf{1}(w_1+w_2)\tbinom{i}{w_0}\tbinom{k-i}{w_2} \\ \times &\{[\frac{(2^{n-1}-1)}{(2^n-1)}]^3 + [1-\frac{(2^{n-1}-1)}{(2^n-1)}]^3\}^{k\gamma} \\ = &(2^k-2)\{[\frac{(2^{n-1}-1)}{(2^n-1)}]^3 + [1-\frac{(2^{n-1}-1)}{(2^n-1)}]^3\}^{k\gamma}. \end{aligned} \tag{41}$$

Combining Eq. (41), (23) and (22), we can obtain that

$$\begin{aligned} &P^{DF}_{k,n,\gamma} = \Pr[W_{k\gamma,n,k}] \\ \geq &\sum_{\mathbf{x}\in R(\mathbf{G}^{\text{pre}}_{n\times k})} \Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x} = 0] \\ &-\frac{1}{2}\sum_{\mathbf{x},\mathbf{y}\in R(\mathbf{G}^{\text{pre}}_{n\times k}),\mathbf{x}\neq\mathbf{y}} \Pr[\mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{x} = 0 \cap \mathbf{G}^{\text{LT}}_{k\gamma\times n}\mathbf{y} = 0] \\ = &(2^k-1)(\frac{(2^{n-1}-1)}{(2^n-1)})^{k\gamma} - \frac{1}{2}\sum_{i=1}^{k}\tbinom{k}{i}(2^k-2) \\ &\times\{[\frac{(2^{n-1}-1)}{(2^n-1)}]^3 + [1-\frac{(2^{n-1}-1)}{(2^n-1)}]^3\}^{k\gamma} \\ = &(2^k-1)\left[\frac{(2^{n-1}-1)}{(2^n-1)}\right]^{k\gamma} - (2^k-1)(2^{k-1}-1) \\ &\times\left\{\left[\frac{(2^{n-1}-1)}{(2^n-1)}\right]^3 + \left[1-\frac{(2^{n-1}-1)}{(2^n-1)}\right]^3\right\}^{k\gamma}. \end{aligned} \tag{42}$$

The proof of Corollary 5 is completed.

References

[1] A. Shokrollahi, "Raptor codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2551-2567, 2006.

[2] J. W. Byers, M. Luby, M. Mitzenmacher, and A. Rege., "A digital fountain approach to reliable distribution of bulk data," SIGCOMM Comput. Commun. Rev., vol. 28, no. 4, pp. 56-67, 1998.

[3] M. Luby, "LT codes," in *Proceedings of the 43rd IEEE FOCS*, pp. 271-280, 2002.

[4] "3GPP TS 26.346 v6.1.0 (2005-06) Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service; Protocols and Codecs," Tech. Rep.

[5] H. D. T. Nguyen, T. Le-Nam, and H. Een-Kee, "On transmission efficiency for wireless broadcast using network coding and fountain codes," *IEEE Communications Letters*, vol. 15, no. 5, pp. 569-571, 2011.

[6] P. Wang, G. Mao, Z. Lin, X. Ge, and B. Anderson, "Network coding based wireless broadcast with performance guarantee," *IEEE Trans. Wireless Communications*, vol. 14, no. 1, pp. 532-544, 2014.

[7] N. Rahnavard, B. Vellambi, and F. Fekri, "Rateless codes with unequal error protection property," *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1521-1532, April 2007.

[8] B. Schotsch, "Rateless coding in the finite length regime," Ph.D. dissertation, Inst. of Commun. Systems and Data Proc., RWTH Aachen, Aachen, Germany, Jul 2014.

[9] J. Yue, Z. Lin, B. Vucetic, G. Mao, and T. Aulin, "Performance analysis of distributed raptor codes in wireless sensor networks," *IEEE Trans. Communications*, vol. 61, no. 10, pp. 4357-4368, 2013.

[10] R. Karp, M. Luby, and A. Shokrollahi, "Finite length analysis of LT codes," in *Proceedings of IEEE ISIT*, p. 39, 2004.

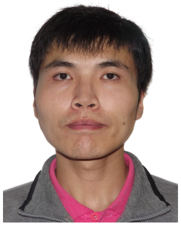
[11] A. Shokrollahi and M. Luby, "Raptor codes," Found. and Trends on Commun. and Inf. Theory, vol. 6, pp. 213-322, Mar. 2009.

[12] A. Shokrollahi, S. Lassen, and R. Karp, "Systems and processes for decoding chain reaction codes through inactivation," US Patent 6,856,263. [Online]. Available: http://www.google.com/patents/US6856263, Feb. 15 2005.

[13] B. Schotsch, H. Schepker, and P. Vary, "The performance of short random linear fountain codes under maximum likelihood decoding," in *Proceedings of IEEE ICC*, pp. 1-5, June 2011.

[14] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*. Siam, 2000.

[15] L. Comtet, *Advanced Combinatorics*. Reidel, 1974.

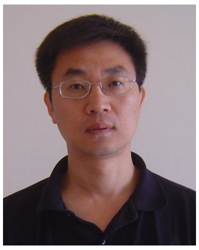


Peng Wang received the B.Sc. degree in applied electronics from Beijing University of Aeronautics and Astronautics, Beijing, China, in 2009, and the M.Eng. degree in telecommunications in 2012 from the Australian National University, Canberra, ACT, Australia. He is currently working towards the PhD degree in Engineering at The University of Sydney.

He is also with the Sydney Research Laboratory, National ICT Australia. His research interests include wireless broadcast networks, heterogeneous networks, graph theory, and its application in networking, channel/network coding, 5G cellular systems, etc.

Guoqiang Mao(S'98-M'02-SM'08) received PhD in telecommunications engineering in 2002 from Edith Cowan University. He was with the School of Electrical and Information Engineering, the University of Sydney between 2002 and 2014. He joined the University of Technology Sydney in February 2014 as Professor of Wireless Networking and Director of Center for Real-time Information Networks. The Center is among the largest university research centers in Australia in the field of wireless communications and networking. He has published more than 150 papers in international conferences and journals, which have been cited more than 3500 times. He is an editor of the IEEE Transactions on Wireless Communications (since 2014), IEEE Transactions on Vehicular Technology (since 2010) and received "Top Editor" award for outstanding contributions to the IEEE Transactions on Vehicular Technology in 2011 and 2014. He is a co-chair of IEEE Intelligent Transport Systems Society Technical Committee on Communication Networks. He has served as a chair, co-chair and TPC member in a large number of international conferences. His research interest includes intelligent transport systems, applied graph theory and its applications in telecommunications, wireless sensor networks, wireless localization techniques and network performance analysis.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2016.2522403, IEEE Transactions on Communications



Zihuai Lin received the Ph.D. degree in Electrical Engineering from Chalmers University of Technology, Sweden, in 2006. Prior to this he has held positions at Ericsson Research, Stockholm, Sweden. Following Ph.D. graduation, he worked as a Research Associate Professor at Aalborg University, Denmark and currently at the School of Electrical and Information Engineering, the University of Sydney, Australia. His research interests include graph theory, source/channel/network coding, coded modulation, MIMO, OFDMA, SC-FDMA, radio resource management, cooperative communications, small-cell networks, 5G cellular systems, etc.

Ming Ding received the B.S. and M.S. degrees (with first class Hons.) in electronics engineering from Shanghai Jiao Tong University (SJTU), Shanghai, China, and the Doctor of Philosophy (Ph.D.) degree in signal and information processing from SJTU, in 2004, 2007, and 2011, respectively. From September 2007 to September 2011, he pursued the Ph.D. degree at SJTU while at the same time working as a Researcher/Senior Researcher Sharp Laboratories of China (SLC). After achieving the Ph.D. degree, he continued working with SLC as a Senior Researcher/Principal Researcher until September 2014, when he joined National Information and Communications Technology Australia (NICTA). In September 2015, Commonwealth Scientific and Industrial Research Organization (CSIRO) and NICTA joined forces to create Data61, where he continued as a Researcher in this new R&D center located in Sydney, N.S.W., Australia. He has authored more than 30 papers in IEEE journals and conferences, all in recognized venues, and about 20 3GPP standardization contributions, as well as a Springer book Multi-point Cooperative Communication Systems: Theory and Applications. Also, as the first inventor, he holds fifteen CN, seven JP, three US, two KR patents and co-authored another 100+ patent applications on 4G/5G technologies. His research interests include B3G, 4G, and 5G wireless communication networks, synchronization, MIMO technology, cooperative communications, heterogeneous networks, device-to-device communications, and modelling of wireless communication systems. He served as the Algorithm Design Director and Programming Director for a system-level simulator of future telecommunication networks in SLC for more than 7 years. He is or has been Guest Editor/Co-Chair/TPC member of several IEEE top-tier journals/conferences, e.g., the IEEE Journal on Selected Areas in Communications, the IEEE Communications Magazine, and the IEEE Globecom Workshops. For his inventions and publications, he was the recipient of the President's Award of SLC in 2012, and served as one of the key members in the 4G/5G standardization team when it was awarded in 2014 as Sharp Company Best Team: LTE 1014 Standardization Patent Portfolio.

Weifa Liang (M'99–SM'01) received the PhD degree from the Australian National University in 1998, the ME degree from the University of Science and Technology of China in 1989, and the BSc degree from Wuhan University, China in 1984, all in computer science. He is currently a Full Professor in the Research School of Computer Science at the Australian National University. His research interests include design and analysis of routing protocols for Software-Defined Networks (SDNs), wireless ad hoc and sensor networks, cloud computing amd mobile cloud computing, design and analysis of parallel and distributed algorithms, combinatorial optimization, and graph theory. He is a senior member of the IEEE.

Xiaohu Ge (M'09-SM'11) is a full Professor with the School of Electronic Information and Communications at Huazhong University of Science and Technology (HUST), China. He is an adjunct professor at the University of Technology Sydney (UTS), Australia. He received his PhD degree in Communication and Information Engineering from HUST in 2003. He has worked at HUST since Nov. 2005. Prior to that, he worked as a researcher at Ajou University (Korea) and Politecnico Di Torino (Italy) from Jan. 2004 to Oct. 2005. He was a visiting researcher at Heriot-Watt University, Edinburgh, UK from June to August 2010. His research interests are in the area of mobile communications, traffic modeling in wireless networks, green communications, and interference modeling in wireless communications. He has published about 100 papers in refereed journals and conference proceedings and has been granted about 15 patents in China. He received the Best Paper Awards from IEEE Globecom 2010. He is leading several projects funded by NSFC, China MOST, and industries. He is taking part in several international joint projects, such as the EU FP7-PEOPLE-IRSES: project acronym S2EuNet (grant no. 247083), project acronym WiNDOW (grant no. 318992) and project acronym CROWN (grant no. 610524).

Dr. Ge is a Senior Member of the China Institute of Communications and a member of the National Natural Science Foundation of China and the Chinese Ministry of Science and Technology Peer Review College. He has been actively involved in organizing more the ten international conferences since 2005. He served as the general Chair for the 2015 IEEE International Conference on Green Computing and Communications (IEEE GreenCom). He serves as an Associate Editor for the IEEE ACCESS, Wireless Communications and Mobile Computing Journal (Wiley) and the International Journal of Communication Systems (Wiley), etc. Moreover, he served as the guest editor for IEEE Communications Magazine Special Issue on 5G Wireless Communication Systems.

Zhiyun Lin (SM'10) received his bachelor degree in Electrical Engineering from Yanshan University, China, in 1998, master degree in Electrical Engineering from Zhejiang University, China, in 2001, and PhD degree in Electrical and Computer Engineering from the University of Toronto, Canada, 2005.

He was a Postdoctoral Research Associate in the Department of Electrical and Computer Engineering, University of Toronto, Canada, from 2005 to 2007. He joined the College of Electrical Engineering, Zhejiang University, China, in 2007. Currently, he is a Professor of Systems Control in the same department. He is also affiliated with the State Key Laboratory of Industrial Control Technology at Zhejiang University. He held visiting professor positions at several universities including The Australian National University (Australia), University of Cagliari (Italy), University of Newcastle (Australia), University of Technology Sydney (Australia), and Yale University (USA).

His research interests focus on distributed control, estimation and optimization, coordinated and cooperative control of multi-agent systems, hybrid and switched system theory, and locomotion control of biped robots. He is currently an associate editor for Hybrid systems: Nonlinear Analysis and International Journal of Wireless and Mobile Networking.