

# Reliability of Broadcast Communications Under Sparse Random Linear Network Coding

Suzie Brown, Oliver Johnson and Andrea Tassi

**Abstract**—Ultra-reliable Point-to-Multipoint (PtM) communications are expected to become pivotal in networks offering future dependable services for smart cities. In this regard, sparse Random Linear Network Coding (RLNC) techniques have been widely employed to provide an efficient way to improve the reliability of broadcast and multicast data streams. This paper addresses the pressing concern of providing a tight approximation to the probability of a user recovering a data stream protected by this kind of coding technique. In particular, by exploiting the Stein–Chen method, we provide a novel and general performance framework applicable to any combination of system and service parameters, such as finite field sizes, lengths of the data stream and level of sparsity. The deviation of the proposed approximation from Monte Carlo simulations is negligible, improving significantly on the state of the art performance bounds.

**Index Terms**—Sparse random network coding, broadcast communication, multicast communications, Stein–Chen method.

## I. INTRODUCTION

In next-generation networks, reliable broadcast communication is expected to be critical. In particular, this holds true in future networks of self-driving vehicles where road-side base stations (BSs) will broadcast live sensor data [1]. For example in the 5G-PPP’s “bird’s eye” use case, live 3D Light Detection and Ranging (LiDAR) scans of vehicles engaging a traffic junction are broadcast to the incoming vehicles – enabling them to take an informed decision on how to safely drive through the junction [1]. In this kind of network, a key performance indicator is the *user delivery probability*, defined as the probability of a user successfully recovering the transmitted data stream.

Generally, modern communication systems enhance the reliability of Point-to-Multipoint (PtM) data streams by employing Application Level-Forward Error Correction (AL-FEC) techniques, which are usually based on Luby Transform (LT) or Raptor codes [2], [3]. These kinds of codes only operate to their capacity if large block lengths are employed, which could be a problem in the presence of delay-sensitive services [2]. For this reason, in our system model reliability of PtM data streams is ensured via the Random Linear Network Coding (RLNC) approach [4].

Copyright (c) 2015 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to [pubs-permissions@ieee.org](mailto:pubs-permissions@ieee.org).

This work is partially supported by the University of Bristol Faculty of Science, the School of Mathematics and the VENTURER Project, which is supported by Innovate UK under Grant Number 102202.

S. Brown and O. Johnson are with the School of Mathematics, University of Bristol, UK (e-mail: [sb13831.2013@my.bristol.ac.uk](mailto:sb13831.2013@my.bristol.ac.uk), [O.Johnson@bristol.ac.uk](mailto:O.Johnson@bristol.ac.uk)).

A. Tassi is with the Department of Electrical and Electronic Engineering, University of Bristol, UK (e-mail: [A.Tassi@bristol.ac.uk](mailto:A.Tassi@bristol.ac.uk)).

The RLNC approach requires the BS to split each PtM data stream into  $K$  source packets, which form a *source message*. A sequence of coded packets is obtained in a rateless fashion by linearly combining the source packets. A user recovers the PtM data stream as soon as it collects  $K$  linearly independent coded packets [4], [5]. A drawback of the RLNC approach is the computational complexity of the decoding phase, which is a function of  $K$  and the finite field size  $q$  considered during the encoding phase [6], [7]. Tassi *et al.* [8] observed that this complexity can be significantly reduced by adopting a *sparse implementation* of the RLNC approach, where the number of non-zero elements in the encoding matrix is smaller. However, as the encoding matrix becomes sparser, the number of coded packet transmissions needed by a user to recover the source message is likely to increase. To date, an exact expression for the user delivery probability as a function of the sparsity and number of coded packet transmissions is still unknown.

The key contribution of this paper is a tight approximation to the user delivery probability in a system where broadcast source messages are protected by sparse RLNC (see Section III). Our approximation is valid for any finite field size, sparsity level, and data stream length. As shown in Section IV, the deviation of the proposed model from simulation results is negligible. Our approximation enables service providers to increase the sparsity level (reducing the complexity of the decoding phase) while ensuring a target user delivery probability.

The lack of an exact performance model for sparse RLNC implementations is caused by the lack of an accurate expression for the probability of a sparse random matrix, generated over a finite field, being full rank [6], [8], [9]. Garrido *et al.* [6] proposed models based on absorbing Markov chains to characterize the user performance, in a particular implementation of sparse RLNC where the number of source packets employed to generate each coded packet is *fixed*. This assumption significantly simplifies the performance modeling issue, yet [6] mostly relies on Monte Carlo simulation to estimate, via a regression technique, the statistical correlation between the rows of full rank sparse matrices.

Unlike [6], this paper refers to a more general sparse RLNC scheme where a source packet participates in the generation of a coded packet with probability  $1 - p$ , for  $0 \leq p \leq 1$ . With regards to this general sparse RLNC formulation, Tassi *et al.* [8] proposed the first performance model valid for any finite field size, data stream length and probability  $p$ . In particular, the probability bound proved in [10, Theorem 6.3] allowed the authors [8] to derive a tractable but not tight performance bound. More recently, the theoretical framework proposed by A. Khan *et al.* [11] extended [10, Theorem 6.3] and can be

directly used to upper- and lower-bound the user delivery probability. However, again often these bounds are not tight.

In this paper, we address the limitations of the previous studies and provide the following contributions:

- We propose an accurate expression for the user delivery probability suitable for general sparse RLNC formulations and applicable to any combination of system parameters, which overcomes the lack of generality of the model proposed in [12] and [6]. In particular, with regards to [6], a new set of Monte Carlo simulations are required to re-derive a performance model as the field size, the number of source packets defining a source message or the number of source packets involved in the generation of each coded packet changes.
- Unlike most recent works [8], [11] which build upon [10, Theorem 6.3], we approximate the user delivery probability by employing a novel mathematical framework based on the Stein-Chern method. In fact, for  $K > 10$  and  $p \geq 0.7$ , [10, Theorem 6.3] notoriously is not a tight lower-bound to the probability of a sparse random matrix being full rank [8], with a subsequent impact on the estimation of the user delivery probability.
- Regardless of the field size and level of sparsity of the encoding matrix, our approximation of the user delivery probability is very close to simulated values. On the other hand, the state of the art upper- and lower-bound to the user delivery probability proposed in [11] significantly deviate from Monte Carlo simulations for a binary field, with the lower-bound performing better than the upper-bound. For larger field sizes, both our approximation and the upper-bound as per [11] to the user delivery probability tightly follow simulation results but, in this case, the lower-bound as per [11] significantly deviates from our Monte Carlo simulations. As such, unlike our approximation, neither the upper-bound nor lower-bound consistently give a tight approximation of the user delivery probability, regardless of the field size.

The rest of the paper is organized as follows. Section II presents the considered system model. Section III discusses the proposed performance characterization model for sparse RLNC implementations and states our novel approximate result in Theorem 3.1. The accuracy of the proposed performance model is considered using Monte Carlo simulation in Section IV. Finally, in Section V, we draw our conclusions.

## II. SYSTEM MODEL

We consider a system model where one transmitter broadcasts a stream of coded packets to multiple receiving nodes, over a channel with packet error probability equal to  $\epsilon$ . We assume that the transmission time of a coded packet is equal to one time step, and that the time needed to transmit  $N$  coded packets is equal to  $N$  time steps.

We say that a source message consists of  $K$  source packets  $\{\mathbf{s}_i\}_{i=1}^K$  where  $\mathbf{s}_i$  consists of  $L$  elements of a finite field  $\mathbb{F}_q$  of size  $q$ . A coded packet  $\mathbf{c}_j$  is also formed by  $L$  elements from  $\mathbb{F}_q$  and is defined as  $\mathbf{c}_j = \sum_{i=1}^K g_{i,j} \cdot \mathbf{s}_i$  where  $g_{i,j} \in \mathbb{F}_q$  is referred to as a coding coefficient. Provided that  $N$  coded packets have been broadcast by the transmitter, the input to

the broadcast channel can be expressed in matrix notation as  $[\mathbf{c}_1, \dots, \mathbf{c}_N] = [\mathbf{s}_1, \dots, \mathbf{s}_K] \cdot \mathbf{G}$ . The  $K \times N$  matrix  $\mathbf{G}$  is defined by elements  $g_{i,j}$ , i.e.,  $\mathbf{G} \in \mathbb{F}_q^{K \times N}$ . Coding coefficients are chosen at random over  $\mathbb{F}_q$ , in an identical and independent fashion according to the following probability law [8]:

$$\mathbb{P}(g_{i,j} = v) = \begin{cases} p & \text{if } v = 0 \\ \frac{1-p}{q-1} & \text{otherwise,} \end{cases} \quad (1)$$

where  $0 \leq p \leq 1$ . The greater the value of  $p$ , the more likely that a coding coefficient is equal to 0, so we observe that the average number of source packets actively participating in the generation of a coded packet is a function of  $p$ . The ‘classic’ RLNC scheme refers to  $p$  equal to  $1/q$  [8] (so the coding coefficients are uniform on  $\mathbb{F}_q$ ), ‘sparse’ RLNC schemes are characterized by  $p > 1/q$ .

Let  $\{\mathbf{c}_j\}_{j=1}^n$  be the set of coded packets that have been successfully received by a user, for  $0 \leq n \leq N$ . At the receiving end, each user populates a  $K \times n$  decoding matrix  $\mathbf{M}$  with the  $n$  columns of  $\mathbf{G}$  associated with the  $n$  coded packets that have been successfully received. Finally, relation  $[\mathbf{c}_1, \dots, \mathbf{c}_n] = [\mathbf{s}_1, \dots, \mathbf{s}_K] \cdot \mathbf{M}$  holds. The source message is recovered as soon as  $\mathbf{M}$  becomes full rank and hence,  $\mathbf{M}$  contains a  $K \times K$  invertible matrix.

## III. PERFORMANCE ANALYSIS

Based on [4], we observe that the probability of a user to recover a source message, i.e., the user delivery probability, as a function of  $\epsilon$  can be expressed as follows:

$$\mathbf{R}(\epsilon) = \sum_{n=K}^N \binom{N}{n} (1-\epsilon)^n \epsilon^{N-n} \mathbf{R}_{K,n}(p), \quad (2)$$

where  $\mathbf{R}_{K,n}(p)$  is the probability of a  $K \times n$  decoding matrix being full rank, as a function of  $p$ . In the case of classic RLNC, it is known that  $\mathbf{R}_{K,n}(p)|_{p=1/q} = \prod_{t=0}^{K-1} \left[1 - \frac{1}{q^{n-t}}\right]$  exactly [4]. For sparse RLNC schemes, an exact expression for  $\mathbf{R}_{K,n}(p)$  is still unknown but, as proposed in [11], it can be approximated by means of the following lower-bound

$$\mathbf{R}_{K,n}(p) \geq 1 - \min \left\{ \eta_{\max}(n); \sum_{t=1}^K \binom{K}{t} (q-1)^{t-1} \rho_t \right\} \quad (3)$$

and upper-bound

$$\mathbf{R}_{K,n}(p) \leq 1 - \max \left\{ \eta_{\min}(n); \sum_{t=1}^K \binom{K}{t} p^{nt} (1-p^n)^{K-t} \right\} \quad (4)$$

where  $\eta_{\max}(t) = 1 - \prod_{w=0}^{K-1} \left[1 - \left(\max \left\{ p, \frac{1-p}{q-1} \right\}\right)^{t-w}\right]$  and  $\eta_{\min}(t) = 1 - \prod_{w=0}^{K-1} \left[1 - \left(\min \left\{ p, \frac{1-p}{q-1} \right\}\right)^{t-w}\right]$ . From [10], it follows that  $\eta_{\max}(t)$  and  $\eta_{\min}(t)$  are the lower- and upper-bound to the probability, for  $t \leq K$ , of a  $K \times t$  being non-full rank, respectively. Finally, we write  $\rho_\ell$  for the probability that any set of  $\ell$  rows of a  $K \times n$  matrix sums to the zero vector

in  $\mathbb{F}_q$ , which can be expressed (directly following from [9, Eq. (5)]), for  $\ell = 1, \dots, K$  and  $n \geq K$ , as:

$$\rho_\ell \doteq \left[ \frac{1}{q} \left( 1 + (q-1) \left( 1 - \frac{q(1-p)}{q-1} \right)^\ell \right) \right]^n. \quad (5)$$

Both (3) and (4) are based on  $\eta_{\max}(t)$  and  $\eta_{\min}(t)$ , which essentially account for the event that some sets of rows form a non-full rank matrix. Overall,  $1 - \eta_{\max}(t)$  and  $1 - \eta_{\min}(t)$  give a notoriously not tight approximation of  $R_{K,t}(p)$ . This holds true especially for  $K > 10$  and  $p \geq 0.7$  [8]. In addition, the right-hand terms in the minimization of (3) and in the maximization of (4) represent the probability of having any set of rows that linearly combined sums to the zero vector and the probability of having any groups of rows that are equal to the zero vector, respectively. In both cases, these events are significantly different to the event that some submatrix in  $\mathbf{M}$  is not full rank – thus impacting on the tightness of (3) and (4). In the remainder of this section, we address this issue by providing a novel expression for  $R_{K,n}(p)$ , which tightly approximates the user delivery probability across a large range of system parameters.

#### A. Proposed Performance Model for Sparse RLNC

Therefore, we consider the key research question: *Given a  $K \times n$  decoding matrix  $\mathbf{M}$ , formed according to the probability model (1), what is the probability that  $\mathbf{M}$  has rank  $K$ ?* We remark that for  $n < K$ , the source message cannot be recovered, i.e.,  $R_{K,n}(p)$  is equal to 0. In the remainder of this section, we focus on the case where  $n \geq K$  and we wish to know whether the  $K$  rows of  $\mathbf{M}$  form a linearly independent set, i.e., the rank of  $\mathbf{M}$  is  $K$ . We give the following definition.

*Definition 3.1:* Write  $\mathcal{R} \doteq \{1, 2, \dots, \sum_{t=1}^K \binom{K}{t}\} = \{1, 2, \dots, 2^K - 1\}$  for a set of labels. For each  $r \in \mathcal{R}$ , we regard  $\mathcal{S}_r$  as a subset of the set of indices  $\{1, \dots, K\}$  composed of  $|\mathcal{S}_r|$  items.

It is immediate to prove that the following remark holds.

*Remark 3.1:* Matrix  $\mathbf{M}$  is full rank if and only if no linear combinations of any sets of rows indexed by a  $\mathcal{S}_r$  sums to the zero vector over the field  $\mathbb{F}_q$ . For  $q = 2$ , we can consider the collection of events

$$U_{\mathcal{S}_r} \doteq \left\{ \sum_{i \in \mathcal{S}_r} \mathbf{m}_i = \mathbf{0} \right\}, \quad \text{for } r \in \mathcal{R}, \quad (6)$$

where we write  $\mathbf{m}_i$  for the  $i$ -th row of  $\mathbf{M}$ , and where addition is understood to be over  $\mathbb{F}_2$ . We know that  $\mathbf{M}$  is full rank if and only if none of the events  $U_{\mathcal{S}_r}$  occur for any  $r \in \mathcal{R}$ .

*Example 3.1:* Consider the following matrix when  $q = 2$ :

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

In this case, rows 1 and 4 are identical, so  $U_{\{1,4\}}$  occurs. Further, rows 2,3 and 5 sum to zero over  $\mathbb{F}_2$ , so  $U_{\{2,3,5\}}$  also occurs. In addition, since both these sets of rows sum to zero, their union must also sum to zero, so  $U_{\{1,2,3,4,5\}}$  also occurs.

Example 3.1 illustrates why it is not sufficiently accurate to estimate the full-rank probability of  $\mathbf{M}$  by considering the expected number of events  $U_{\mathcal{S}_r}$  which occur, using the expression for the probability of each individual  $U_{\mathcal{S}}$ . This approach ignores the fact that such events are *positively correlated*. In general, given disjoint sets  $\mathcal{S}_1, \dots, \mathcal{S}_t$  such that  $U_{\mathcal{S}_1}, \dots, U_{\mathcal{S}_t}$  occur, then  $U_{\mathcal{S}}$  will occur for each of the  $2^t - 1$  sets  $\mathcal{S}$  formed as unions of the  $\mathcal{S}_i$

Our proposed performance framework builds upon a different set of statistical events, defined as follows.

*Definition 3.2:* Let  $V_{\mathcal{S}_r}$  be defined as follows

$$V_{\mathcal{S}_r} \doteq U_{\mathcal{S}_r} \cap \left( \bigcap_{\mathcal{T} \subset \mathcal{S}_r} U_{\mathcal{T}}^c \right), \quad \text{for } r \in \mathcal{R}, \quad (7)$$

which is the event that the rows indexed by  $\mathcal{S}_r$  sum to the zero vector in  $\mathbb{F}_2$  but that no collection of rows indexed by a proper subset of  $\mathcal{S}_r$  sums to the zero vector.

In general, from Definition 3.2, we have the following remark.

*Remark 3.2:* Matrix  $\mathbf{M}$  is full rank if and only if none of the events  $V_{\mathcal{S}_r}$  occurs, for  $r \in \mathcal{R}$ . This choice of events significantly mitigates the impact of the correlation among events observed in Example 3.1. There,  $V_{\{1,4\}}$  and  $V_{\{2,3,5\}}$  both occur (since no subset of them sums to zero), however  $V_{\{1,2,3,4,5\}}$  does not. This enables us to derive a tighter approximation of  $R_{K,n}(p)$ .

The proposed derivation of  $R_{K,n}(p)$  involves two approximation steps: (i) We approximate the probability of event  $V_{\mathcal{S}_r}$  happening for any set  $\mathcal{S}_r$  consisting of a given number of items, and (ii) Since results based on the Stein-Chen method [13], [14] show the sum of approximately independent zero-one variables with small probability of being one is close to Poisson, we approximate  $R_{K,n}(p)$  with a negative exponential function. Firstly, we consider the following quantities:

*Definition 3.3:* For each  $\ell = 1, \dots, K$ :

- 1) For each  $r \in \mathcal{R}$  such that the set  $\mathcal{S}_r$  has cardinality  $\ell$ , the event  $V_{\mathcal{S}_r}$  has the same probability  $\pi_\ell$  of happening, defined as

$$\pi_\ell \doteq \mathbb{P}[V_{\mathcal{S}_r}], \quad \ell = 1, \dots, K. \quad (8)$$

- 2) We define a further quantity  $\tilde{\pi}_\ell$  recursively as follows:

$$\tilde{\pi}_\ell \doteq \rho_\ell - \sum_{s=1}^{\ell-1} \binom{\ell-1}{s} \rho_s \tilde{\pi}_{\ell-s}, \quad (9)$$

where (since taking  $\ell = 1$  gives an empty sum)  $\tilde{\pi}_1 \doteq \rho_1$ .

*Lemma 3.1:* Term  $\pi_\ell$  (defined in (8)) can be approximated as  $\tilde{\pi}_\ell$  (defined in (9)).

*Proof:* See Appendix A. ■

We observe that an obvious way in which  $\mathbf{M}$  can fail to have full rank is that a particular row is identically zero. Indeed, considering this event gives an upper bound on  $R_{K,n}(p)$ , which for certain parameter values can be reasonably tight. For this reason, we condition out these events as follows:

$$R_{K,n}(p) = \mathbb{P}(\{\mathbf{M} \text{ has no zero rows}\} \cdot \mathbb{P}(\{\mathbf{M} \text{ is full rank}\} \mid \{\mathbf{M} \text{ has no zero rows}\})), \quad (10)$$

where we can write the first term of (10) directly as  $(1-p^n)^K$ .

From Lemma 3.1, we prove the following result.

*Theorem 3.1:* We approximate the second term of (10) as

$$\mathbb{P}(\mathbf{M} \text{ is full rank} \mid \mathbf{M} \text{ has no zero rows}) \simeq \exp(-\lambda), \quad (11)$$

where

$$\lambda \doteq \sum_{\ell=2}^K \lambda_{\ell}, \quad \text{for } \lambda_{\ell} \doteq \binom{K}{\ell} \frac{\tilde{\pi}_{\ell}}{(1-p^n)^{\ell}}, \quad (12)$$

so we approximate  $R_{K,n}(p)$  as follows:

$$R_{K,n}(p) \simeq (1-p^n)^K \exp(-\lambda). \quad (13)$$

*Proof:* See Appendix A. ■

The most computationally intensive part of calculating (13) is the derivation of  $\tilde{\pi}_{\ell}$ , which requires  $O(K^2)$  operations. However, since the expression of  $\tilde{\pi}_{\ell}$  is independent of  $K$ , it has to be computed only once to approximate  $R_{K,n}(p)$ . In addition, for  $K = 10, 20, 50$  and  $100$ , the average time needed to compute<sup>1</sup>  $\tilde{\pi}_1, \dots, \tilde{\pi}_K$  (normalized by  $K$ ) is equal to  $2.7 \cdot 10^{-3}$ s,  $7.7 \cdot 10^{-3}$ s,  $7.3 \cdot 10^{-2}$ s and  $4.3 \cdot 10^{-1}$ s, respectively. It is also key to note that Theorem 3.1 allows us to decouple the impact that any  $\ell \times n$  submatrix of  $\mathbf{M}$  has on the approximation of  $R_{K,n}(p)$  as in (13), for  $\ell = 2, \dots, K$ . As the following remark explains, this allows us to further approximate (13) by reducing the number of summation terms defining  $\lambda$  and hence, reducing the computational complexity of the approximation (13).

*Remark 3.3:* Consider the set of all the  $\ell \times n$  submatrices of  $\mathbf{M}$ , then  $\lambda_{\ell}$  approximates the probability that at least one of these submatrices is not full rank, assuming  $\mathbf{M}$  has no zero rows. For this reason, the approximation of  $R_{K,n}(p)$  given in (13) can be further approximated by referring to those submatrices of  $\mathbf{M}$  composed by up to  $m$  rows, for  $m = 2, \dots, K$ . As such, we define the  $m$ -th approximation order of (13) as follows:

$$R_{K,n}^{(m)}(p) \doteq (1-p^n)^K \exp\left(-\sum_{\ell=2}^m \lambda_{\ell}\right). \quad (14)$$

Let us consider the following approximation order optimization (AOO) problem<sup>2</sup>:

$$\text{AOO} \quad \min_{m \in \{2, \dots, K\}} m \quad (15)$$

$$\text{s.t. } e(m) \leq \tau \vee m \leq \hat{m} \quad (16)$$

where function  $e(m)$  is defined as  $R_{K,n}^{(m)}(p) - R_{K,n}^{(m+1)}(p)$ . The solution  $m^*$  to the AOO problem represents the smallest-order approximation of (13) associated with a target error value  $\tau \in [0, 1]$  or such that  $m^*$  is smaller than  $\hat{m}$ , for  $2 \leq \hat{m} \leq K$ .

*Remark 3.4:* From (12), it follows that term  $\sum_{\ell=2}^m \lambda_{\ell}$  is a non-decreasing function of  $m$ , i.e., relation  $R_{K,n}^{(m)}(p) \geq R_{K,n}^{(m+1)}(p) \geq R_{K,n}^{(K)}(p)$  holds. As such, for any given  $K$ ,  $n$  and  $p$ , the error function  $e(m)$  attains only one maximum, for

<sup>1</sup>Tests performed by running our benchmark code on one core of an Intel Xeon CPU E5-2650v4 operated at 2.20 GHz.

<sup>2</sup>For the sake of compactness, with a slight abuse of notation, we say that  $R_{K,n}^{(m)}(p)$  is always equal to  $R_{K,n}^{(K)}(p)$ , for any  $m > K$ .

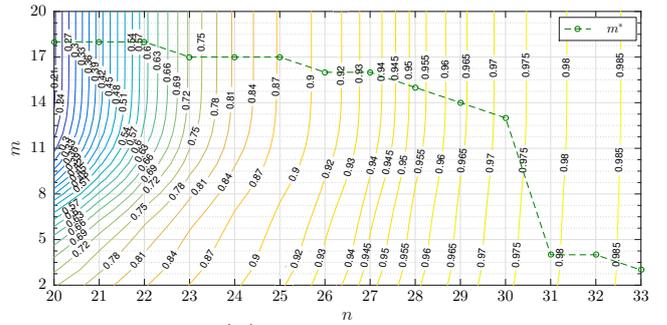


Fig. 1. Contour map of  $R_{K,n}^{(m)}$  as a function of  $n$  and  $m$ , for  $q = 2$ ,  $K = 20$  and  $p = 0.8$ . The values of  $m^*$  have been derived by referring to  $\tau = 10^{-4}$  and  $\hat{m} = K$ .

$m \in \{2, \dots, K\}$ . For this reason, the AOO problem can be solved iteratively evaluating  $R_{K,n}^{(m^*)}(p)$ , for  $m^* = 2, \dots, K$ , until  $e(m^*) \geq e(m^* + 1)$  and  $e(m^* + 1) \leq \tau$  or  $m^*$  is smaller than or equal to  $\hat{m}$ .

*Remark 3.5:* From Remark 3.2,  $\mathbf{M}$  is full rank if and only if none of the events  $V_{S_r}$  occurs, for  $r \in \mathcal{R}$ , and  $q = 2$ . However, for non-binary fields, the aforementioned statement captures a subsets of events when a random matrix is full rank. As such, we propose to use (13) to approximate  $R_{K,n}(p)$ , for  $q > 2$ .

#### IV. ANALYTICAL RESULTS

This section compares the approximation we proposed in Theorem 3.1 against the approximation (3) and (4). Both our simulator and the implementation of the proposed theoretical framework are available online [15].

Fig. 1 shows the relationship that exists between the order  $m$  of the approximation as in (14) and the number  $n$  of received coded packets in  $R_{K,n}^{(m)}$ , for  $q = 2$ , a source message composed by  $K = 20$  packets and  $p = 0.8$ . From (14), we remark that, for a given value of  $n$ ,  $R_{K,n}^{(m)}$  is a non-increasing function of  $m$ . This is directly related to the fact that small approximation orders account for submatrices of  $\mathbf{M}$  composed of a reduced number of rows. This can be intuitively explained by considering the extreme case where  $n$  is large compared to  $K$ . In this case, the probability of  $\mathbf{M}$  being full rank can be approximated by the probability of having a set of  $K$  (non-zero) rows of  $\mathbf{M}$  where no rows are identical – this corresponds to the case where  $m$  is set equal to 2.

The aforementioned facts are confirmed by Fig. 1. For instance, for  $n = 20$ , the value of  $R_{K,n}^{(m)}$  drops from 0.72 ( $m = 2$ ) to 0.21 ( $m = 14$ ) to remain almost unchanged for  $14 \leq m \leq 20$ . In particular, by solving the AOO problem for  $\tau = 10^{-4}$ ,  $\hat{m} = K$  and  $n = 20$ , we obtain an optimal value of  $m^*$  equal to 18 as per Remark 3.3. We also observe that the value of  $m^*$  appears to sharply decrease as  $n$  increases, which makes computationally convenient to approximate  $R_{K,n}$  with  $R_{K,n}^{(m^*)}$ . For instance, Fig. 1 shows that the error function  $e(m^*)$  takes values smaller than or equal to  $\tau = 10^{-4}$  for  $n = 31$  and  $m^* = 4$  – thus making it pointless to approximate  $R_{K,n}$  with an heuristic order equal to or greater than 5. In the remainder of this section, to highlight the accuracy of our approximation, we will refer to a value of  $\tau = 10^{-10}$  or  $\hat{m} \leq \lfloor 3K/4 \rfloor$ .

Fig. 2 compares the user delivery probability  $R(\epsilon)$  for  $K = 10, 20$  and  $50$  and  $q = 2$ . We compare the value for

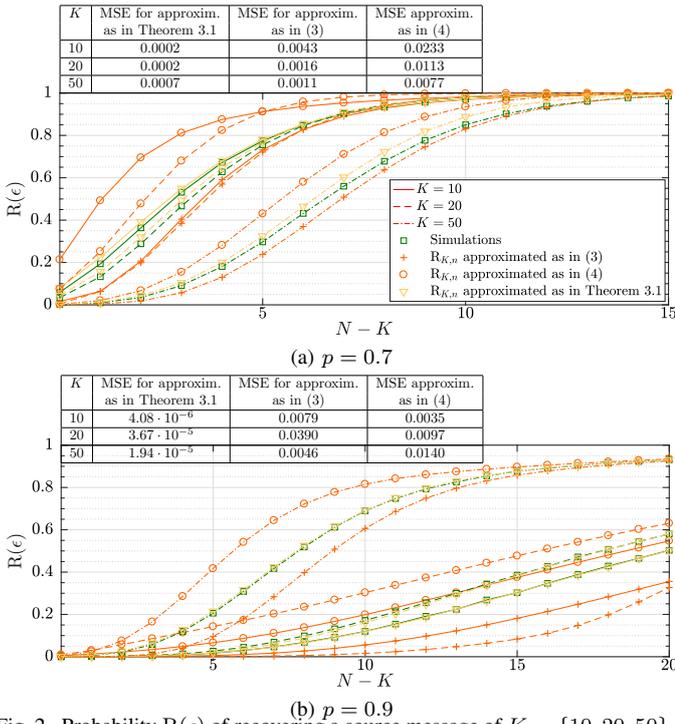


Fig. 2. Probability  $R(\epsilon)$  of recovering a source message of  $K = \{10, 20, 50\}$  source packets as a function of the number of coded packet transmissions  $N$ , for  $q = 2$  and  $\epsilon = 0.1$ . Tables shows the MSEs between simulation results and the cases where  $R_{K,n}$  is approximated as in (3), (4) and Theorem 3.1. Legend of both figures is reported in Fig. 2a.

$R(\epsilon)$  implied by (2), substituting the approximations to  $R_{K,n}$  given by (3), (4) and our proposal in (14) to the probability  $R(\epsilon)$  estimated by Monte Carlo simulations. Results are given as a function of  $N - K$ , which represents the transmission overhead, i.e., the number of coded packets in excess of  $K$  that are transmitted. Assuming that the time needed to transmit each coded packet is fixed and equal to one time slot, the goodput of the system can be immediately expressed as the bit length of the source message divided by the time duration of  $N$  time slots. For concreteness, we considered a value of packet error probability  $\epsilon = 0.1$ , which is the maximum transport block error probability regarded as acceptable in a Long Term Evolution-Advanced (LTE-A) system [4]. In particular, in the case where  $p = 0.7$ , Fig. 2a shows that the maximum gap between our proposed approximation (14) and simulation results is equal to  $3.1 \cdot 10^{-2}$ , which occurs for  $K = 20$ . Fig. 2b refers to the case when  $p = 0.9$  and shows that the gap between (14) and simulation results is negligible.

In contrast, both Fig. 2a and 2b show that approximating  $R_{K,n}$  using the state of the art (3) and (4) leads  $R(\epsilon)$  to significantly deviate from the simulation results. For instance, for  $p = 0.9$ ,  $K = 50$  and  $N - K = 7$ , the absolute deviation can be up to 0.14 and 0.22, in the case of (3) and (4), respectively. In general, the maximum Mean Squared Error (MSE) between simulations and our proposed approximation (14) is experienced for  $K = 50$  and  $p = 0.7$  and it is equal to  $7 \cdot 10^{-4}$ . That is smaller than the corresponding MSEs between simulation and approximations (3) and (4), which are equal to  $1.1 \cdot 10^{-3}$  and  $7.7 \cdot 10^{-3}$ , respectively (between 1.6 and 11 times smaller). In addition, Fig. 2b shows that, for  $p = 0.9$ , our proposal overlaps simulation results while the considered

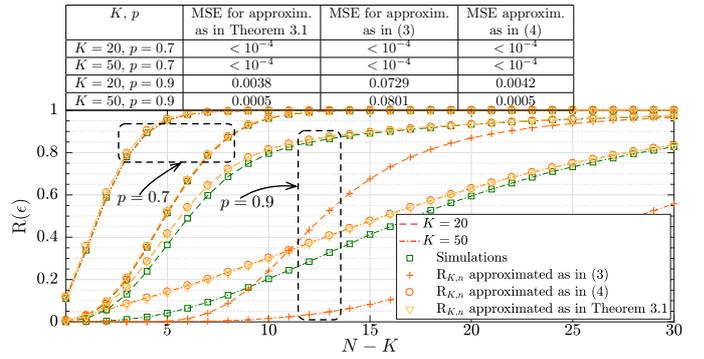


Fig. 3. Probability  $R(\epsilon)$  of recovering a source message of  $K = \{20, 50\}$  source packets as a function of the number of coded packet transmissions  $N$ , for  $p = \{0.7, 0.9\}$ ,  $q = 2^4$  and  $\epsilon = 0.1$ . Tables shows the MSE between simulation results and the cases where  $R_{K,n}$  is approximated as in (3), (4) and Theorem 3.1.

alternatives significantly deviate. In this case, the MSE of our approximation is between 237 times (for  $K = 50$ ) and 1063 times ( $K = 20$ ) smaller than in the case of (3) and, between 722 times ( $K = 50$ ) and 857 times (for  $K = 10$ ) smaller than in the case of (4).

Fig. 3 shows that for  $q = 2^4$ , our approximation either overlaps (for  $p = 0.7$ ) or marginally diverges from simulation results ( $p = 0.9$ ). In the latter case, we observe that the (absolute gap) never exceeds 0.11 and the maximum MSE is equal to  $3.8 \cdot 10^{-3}$ . Similar behavior is also exhibited by the case where  $R_{K,n}$  is approximated as in (3) or (4) and  $p = 0.7$ . However, as  $p$  increases to 0.9, the approximation based on (3) significantly deviates from simulation results even of a quantity larger than 0.51 ( $K = 20$  and  $N - K = 9$ ).

Generally, from Figs. 2 and 3 we observe that, for binary fields (with the only exception of  $K = 50$  and  $p = 0.9$ ), the approximation based on (3) is tighter than that based on (4). However, the exact opposite holds as both  $q$  and  $p$  increase. Our proposed approximation avoids this issue. In fact, our solution tightly approximates simulation results, for all the cases considered. These conclusions are also confirmed by Fig. 4, which shows the probability  $R(\epsilon)$  as a function of  $p$ , for  $q = \{2, 2^4\}$ ,  $K = \{20, 50\}$ .

As an immediate application of a tighter approximation of the user delivery probability, we can accurately estimate the average transmission overhead needed for a user to recover a source message (that is  $\sum_{t=K}^{\infty} t \cdot R_{|N=t}(\epsilon) - K$ ). In particular, Fig. 5 shows the average transmission overhead as a function of  $\epsilon$ , for  $K = 20, 50$  and 100 and,  $p = 0.7$  and 0.9. Direct proof of the quality of the proposed approximation is given by the fact that the deviation between theoretical and simulation results is negligible across the whole range of parameters – the maximum gap between theory and simulations is equal to 2 and occurs for  $K = 100$  and  $p = 0.9$ .

## V. CONCLUSION

This paper presented a novel approximated performance model for a sparse RLNC implementation. The proposed model exploits the Stein-Chen method to derive a tight approximation to the probability of a user recovering a source message. Analytical results show that the Mean Squared Error

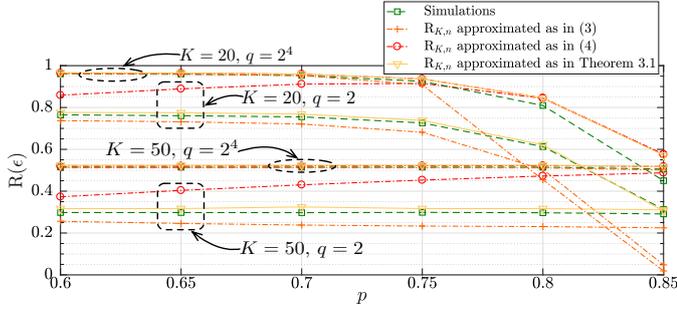


Fig. 4. Probability  $R(\epsilon)$  of recovering a source message of  $K = 20$  and  $50$  source packets for  $N = 25$  and  $55$ , respectively, as a function of  $p$  with  $q = \{2, 2^4\}$  and  $\epsilon = 0.1$ .

(MSE) between our approximation and simulation results, for  $q = 2$  and  $2^4$ , never exceeds  $7 \cdot 10^{-4}$  and  $3.8 \cdot 10^{-3}$ , respectively. On the other hand, the state of the art bounds are not always tight. For instance, when  $q = 2$  our proposal is between 1.5 and 1063 times closer in MSE to simulations.

#### APPENDIX A

*Proof of Lemma 3.1:* By symmetry it is enough to consider a subset of rows of the form  $\mathcal{S} = \{1, 2, \dots, \ell\}$ , where  $\ell \leq K$ . The key is to fix one row (say row 1) and to consider the smallest set of rows containing row 1 which sums to zero. Consider  $\mathcal{W}$ , a subset of  $\mathcal{S}$  with  $1 \in \mathcal{W}$ , and say that event  $T_{\mathcal{W}, \mathcal{S}}$  occurs when both: (i) the rows of  $\mathbf{M}$  with indices in  $\mathcal{S}$  add to zero and, (ii) rows with indices in  $\mathcal{W}$  add to zero, but no subset of these rows add to zero, i.e. event  $V_{\mathcal{W}}$  occurs see (7). By considering (i) and (ii) together,  $T_{\mathcal{W}, \mathcal{S}}$  occurs when the rows in both the sets  $\mathcal{S} \setminus \mathcal{W}$  and  $\mathcal{W}$  (but no subset of  $\mathcal{W}$ ) add to zero. In other words  $T_{\mathcal{W}, \mathcal{S}}$  equals  $U_{\mathcal{S} \setminus \mathcal{W}} \cap V_{\mathcal{W}}$ . Since rows in  $\mathbf{M}$  are statistically independent, for each  $\mathcal{W}$  of size  $(\ell - s)$ , the event  $T_{\mathcal{W}, \mathcal{S}}$  occurs with probability

$$\begin{aligned} \mathbb{P}(T_{\mathcal{W}, \mathcal{S}}) &= \mathbb{P}(U_{\mathcal{S} \setminus \mathcal{W}} \cap V_{\mathcal{W}}) \\ &= \mathbb{P}(U_{\mathcal{S} \setminus \mathcal{W}}) \mathbb{P}(V_{\mathcal{W}}) = \rho_s \pi_{\ell-s}. \end{aligned} \quad (17)$$

Furthermore, since  $U_{\mathcal{S}} = \bigcup_{\mathcal{W}} T_{\mathcal{W}, \mathcal{S}}$  for any  $\mathcal{S}$  we observe:

$$\begin{aligned} \rho_\ell &= \mathbb{P}(U_{\mathcal{S}}) = \mathbb{P}\left(\bigcup_{\mathcal{W}} T_{\mathcal{W}, \mathcal{S}}\right) \simeq \sum_{\mathcal{W}} \mathbb{P}(T_{\mathcal{W}, \mathcal{S}}) \\ &= \sum_{s=0}^{\ell-1} \binom{\ell-1}{s} \rho_s \tilde{\pi}_{\ell-s} = \sum_{s=1}^{\ell-1} \binom{\ell-1}{s} \rho_s \pi_{\ell-s} + \pi_\ell. \end{aligned} \quad (18)$$

This relation holds because (i) we assume events  $T_{\mathcal{W}, \mathcal{S}}$  are approximately disjoint (ii) there are  $\binom{\ell-1}{s}$  possible sets  $\mathcal{W}$  of size  $(\ell - s)$  containing 1. In Example 3.1, if  $\mathcal{S} = \{1, 2, 3, 4, 5\}$  then  $U_{\mathcal{S}}$  occurs as previously discussed, indeed so does  $T_{\mathcal{W}, \mathcal{S}}$  with  $\mathcal{W} = \{1, 4\}$ . This concludes the proof. ■

*Proof of Theorem 3.1:* We write  $\mathcal{R}^*$  for the collection of indices  $r$  such that  $|\mathcal{S}_r| \geq 2$  and define the random variable

$$W \doteq \sum_{r \in \mathcal{R}^*} \mathbb{I}(V_{\mathcal{S}_r} \mid \mathbf{M} \text{ has no zero rows}) \quad (19)$$

where indicator function  $\mathbb{I}(\cdot)$  equals 1 if a particular event has occurred, or 0 otherwise. Observe that  $\mathbb{P}(\mathbf{M} \text{ is full rank} \mid \{\mathbf{M} \text{ has no zero rows}\}) = \mathbb{P}(W = 0)$ .

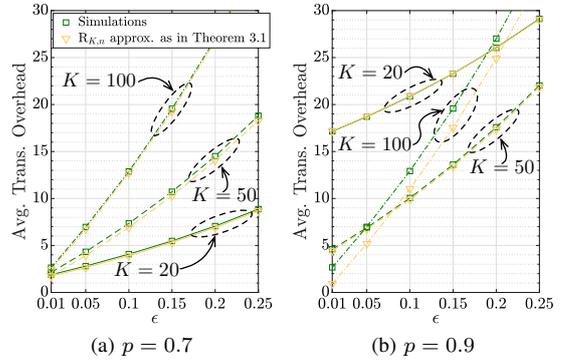


Fig. 5. Average transmission overhead as a function of  $\epsilon$ , for  $K = \{20, 50, 100\}$ ,  $q = 2$  and  $p = \{0.7, 0.9\}$ . Legend of both figures is reported in Fig. 5a.

By (8), if  $\mathcal{S}_r$  has  $\ell \geq 2$  elements, independence of the rows means that the probability

$$\begin{aligned} &\mathbb{P}(V_{\mathcal{S}_r} \mid \{\text{no zero rows in } \mathbf{M}\}) \\ &= \frac{\mathbb{P}(V_{\mathcal{S}_r} \cap \{\text{no zero rows in } \mathbf{M}\})}{(1 - p^n)^K} \\ &= \frac{\mathbb{P}(V_{\mathcal{S}_r}) \mathbb{P}(\{\text{no zero rows in } \mathcal{S}_r^c\})}{(1 - p^n)^K} \\ &\simeq \frac{\tilde{\pi}_\ell (1 - p^n)^{K-\ell}}{(1 - p^n)^K} = \frac{\tilde{\pi}_\ell}{(1 - p^n)^\ell}. \end{aligned} \quad (20)$$

Hence, by counting sets of different sizes in  $\mathcal{R}^*$ , we it follows that  $\mathbb{E}[W] = \lambda$ . Further,  $W$  is the sum of a large number of zero-one variables, each of which equals one with small probability, and where each random variable in the sum is independent of a large proportion of the other terms. These are the conditions under which  $W$  is close to Poisson, as shown by the Stein–Chen method [13], [14]. Approximation (13) follows because [13, Theorem 1] means that  $\mathbb{P}(W = 0) \simeq \exp(-\lambda)$ . ■

#### REFERENCES

- [1] “5G-PPP White Paper on Automotive Vertical Sector,” 5G Infrastructure Public Private Partnership, Tech. Rep., Oct. 2015. [Online]. Available: <https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf>
- [2] E. Magli, M. Wang, P. Frossard, and A. Markopoulou, “Network Coding Meets Multimedia: A Review,” *IEEE Trans. Multimedia*, vol. 15, no. 5, pp. 1195–1212, 2013.
- [3] P. Wang, G. Mao, Z. Lin, M. Ding, W. Liang, X. Ge, and Z. Lin, “Performance Analysis of Raptor Codes Under Maximum Likelihood Decoding,” *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 906–917, Mar. 2016.
- [4] A. Tassi, I. Chatzigeorgiou, and D. Vukobratović, “Resource-Allocation Frameworks for Network-Coded Layered Multimedia Multicast Services,” *IEEE J. Sel. Areas Commun.*, vol. 33, no. 2, pp. 141–155, Feb. 2015.
- [5] E. Tsimbalo, A. Tassi, and R. J. Piechocki, “Reliability of Multicast under Random Linear Network Coding,” Oct. 2017. [Online]. Available: <http://arxiv.org/abs/1709.05477>
- [6] P. Garrido, D. E. Lucani, and R. Agüero, “Markov Chain Model for the Decoding Probability of Sparse Network Coding,” *IEEE Trans. Commun.*, vol. 65, no. 4, pp. 1675–1685, Apr. 2017.
- [7] D. Andrén, L. Hellström, and K. Markström, “On the Complexity of Matrix Reduction Over Finite Fields,” *Advances in Applied Mathematics*, vol. 39, no. 4, pp. 428–452, 2007.
- [8] A. Tassi, I. Chatzigeorgiou, and D. E. Lucani, “Analysis and Optimization of Sparse Random Linear Network Coding for Reliable Multicast Services,” *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 285–299, Jan. 2016.
- [9] C. Cooper, “On the distribution of rank of a random matrix over a finite field,” *Random Struct. Alg.*, vol. 17, no. 3-4, pp. 197–212, 2000.
- [10] J. Blömer, R. Karp, and E. Welzl, “The Rank of Sparse Random Matrices Over Finite Fields,” *Random Struct. Alg.*, vol. 10, no. 4, pp. 407–419, 1997.

- [11] A. S. Khan and I. Chatzigeorgiou, "Improved Bounds on the Decoding Failure Probability of Network Coding Over Multi-Source Multi-Relay Networks," *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 2035–2038, Oct. 2016.
- [12] X. Li, W. H. Mow, and F.-L. Tsang, "Rank Distribution Analysis for Sparse Random Linear Network Coding," in *Proc. of NetCod 2011*, Beijing, China, CN, Jul. 2011, pp. 1–6.
- [13] R. Arratia, L. Goldstein, and L. Gordon, "Poisson approximation and the Chen-Stein method," *Statistical Science*, vol. 5, no. 4, pp. 403–424, 1990.
- [14] A. Barbour, L. Holst, and S. Janson, *Poisson Approximation*. Oxford: Clarendon Press, 1992.
- [15] "Proposed simulation framework and theoretical model." [Online]. Available: <https://github.com/andreatassi/SparseRLNC>