This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2010 proceedings

Network Resources Optimization for Random Linear Network Coding

Kwang Taik Kim and Chan-Soo Hwang
Communication Lab., Samsung Advanced Institute of Technology, Samsung Electronics Co. Ltd., Yongin, Republic of Korea
Email: {kwangtaik.kim, cshwang}@samsung.com

***Abstract*—In a multisource multicast network using random linear network coding, only the *lower* bounds on the decoding probability, the probability that all receivers can decode all source processes, have been known. We obtained new topology-independent and topology-dependent *upper* bounds on the decoding probability by using a simple counting argument. These upper bounds and the best known lower bound on the decoding probability are used to optimize the finite field size governing the use of network resources by exploiting a trade-off between computational complexity and the decoding probability.**

I. Introduction

Computer networks today deliver information by using routing, where the intermediate nodes merely forward messages. However, the routing cannot achieve the multicast capacity, which is the smallest minimum cut to any receiver. On the other hand, Ahlswede *et al*. [1] in 2000 invented network coding where the intermediate nodes may mix messages arriving at the nodes into one or several output messages, and showed that, by using network coding, the source can multicast information at a rate approaching the multicast capacity as symbol size approaches infinity.

To derive more practical network coding schemes, Li *et al*. [9]; and Koetter and Médard [8] showed that linear network coding is sufficient for achieving the multicast capacity. Especially, Koetter and Médard introduced an algebraic framework for verifying the decodability of a network coding – They represented a network coding by a transfer matrix that describes the relationship between an input vector at sources and an output vector at receivers; and then showed that receivers can successfully decode the messages if the transfer matrix is nonsingular. To obtain the linear network coding vectors in practice, Ho *et al.* [7] introduced a random linear network coding where network nodes randomly, independently, and linearly mix incoming messages over a finite field to send them onto output links. To show the decodability of such a coding, they showed that the lower bound of the decoding probability, the probability that the transfer matrix is nonsingular, approaches 1 exponentially as the finite field size increases. Random linear network coding can be designed in a distributed way, thus opened up for a practical implementation of network coding in self-organizing networks, because the codes can be designed in a distributed way.

When network nodes suffer from battery limitations, one must optimize the operation of the network coding to minimize the power related cost. Two costs are related to power consumption: 1) The computational complexity for encoding/decoding, and 2) Transmission cost that is proportional to the message loss rate. One of the key parameters governing the total cost is the finite field size. If the finite field size is increased to improve the decoding performance, high computational complexity comes along as well. This trade-off motivates the work in this paper. First, we find new upper bounds on the decoding probability, because the best known lower bound alone provided by Balli *et al.* [2], [3] cannot yield the range of the optimal finite field size. Second, we optimize the finite field size by minimizing the cost function, which was obtained from the new upper bounds, the best known lower bound, and the computational complexity.

In Section II, we briefly summarize a basic model and an algebraic framework for random linear network coding in [7], [8]. In Section III-A, two upper bounds on the decoding probability are given. The two upper bounds are tight in a sense that they increase over extra links and nodes in the network in the same way as the exact decoding probability, unlike the lower bounds in [2], [3], [7]. Whereas the topology-independent upper bound is general enough to be applicable across all networks without considering specific network topology, similar to the lower bounds in [2], [3], [7], the topology-dependent upper bound depends on the network structure, and is tighter. In Section III-B, we optimize the use of network resources by exploiting a trade-off between the decoding probability and computational complexity at receivers over finite field size by using the best known lower bound in [2], [3] and the upper bounds developed in Section III-A. In Section IV, two proofs are given. We derive the topology-independent upper bound by allowing every node to access all source processes for their random linear network coding, while the other structure of the network remains the same. We establish the topology-dependent upper bound by using the property of cut-sets: Suppose that S source processes have been generated so far at source nodes in a cut containing upstream links. Then the random linear network coding can be decoded for multicast connection problem only if the number of information processes flowing onto a cut-set is at least S.

II. Basic Model and Algebraic Framework

This paper relies on the network coding model developed in [7], [8], which is briefly summarized in this section. A network is modeled using a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the

978-1-4244-6404-3/10/$26.00 ©2010 IEEE

set of vertices representing network nodes and $\mathcal{E}$ is the set of edges representing links. Each link $l \in \mathcal{E}$ delivers one bit of information per unit time from origin $o(l)$ to destination $d(l)$ without causing an error. A path is a sequence of links $(e_1, \cdots, e_k)$, where $d(e_i) = o(e_{i+1})$, $o(e_1) \neq d(e_k)$, and $d(e_i) \neq d(e_j)$,$\forall i \neq j$. Each source node $a(i)$ multicasts source processes X_i to receivers $b(i) = \{\beta_1, \ldots, \beta_d\}$ over the paths for all $i \in [1, r]$. Each source process is assumed to have an entropy rate of one bit per unit time.

Now let us summarize the algebraic network coding formulation in [7], [8]. Each information process in the network is a sequence of a $\log_2 q$-bit vector, which is an element of a finite field $\mathbb{F}_q$. The information process Y_j on a link j is a linear combination of inputs from incoming links $Y_l, d(l) = o(j)$ and source processes generated at the origin node $X_i, a(i) = o(j)$ as follows:

$$Y_j = \sum_{\{i:a(i)=o(j)\}} a_{i,j} X_i + \sum_{\{l:d(l)=o(j)\}} f_{l,j} Y_l.$$

The ith output process $Z_{\beta,i}$ at receiver node β is a linear combination of inputs from incoming links as follows:

$$Z_{\beta,i} = \sum_{\{l:d(l)=\beta\}} b_{\beta,i,l} Y_l.$$

The coefficients $\{a_{i,j}, f_{l,j}, b_{\beta,i,l}\}$ are collected to form matrices $\mathbf{A} \in \mathbb{F}_q^{r \times |\mathcal{E}|}, \mathbf{B}_\beta \in \mathbb{F}_q^{r \times |\mathcal{E}|}$, and $\mathbf{F} \in \mathbb{F}_q^{|\mathcal{E}| \times |\mathcal{E}|}$. The elements in the matrices are defined as $\mathbf{A}(i,j) = a_{i,j}, \mathbf{B}_\beta(i,l) = b_{\beta,i,l}$ and $\mathbf{F}(l,j) = f_{l,j}$. Then in acyclic graphs, the row vector of output processes $Z_\beta = [Z_{\beta,1}, \cdots, Z_{\beta,r}]$ at a receiver node β is given as follows:

$$Z_\beta = X\mathbf{A}(\mathbf{I} - \mathbf{F})^{-1}\mathbf{B}_\beta^T, \tag{1}$$

where $X = [X_1, \cdots, X_r]$ is a row vector of all source processes. Thus, if the transfer matrix $\mathbf{A}(\mathbf{I}-\mathbf{F})^{-1}\mathbf{B}_\beta^T$ has full rank r for each receiver node β, a receiver node can decode the message by a matrix inversion. It is shown in [7] that the transfer matrix $\mathbf{A}(\mathbf{I}-\mathbf{F})^{-1}\mathbf{B}_\beta^T$ is nonsingular if and only if its corresponding Edmonds matrix, defined in (2), is nonsingular:

$$\begin{bmatrix} \mathbf{A} & \mathbf{0}_{r\times r} \\ \mathbf{I}-\mathbf{F} & \mathbf{B}_\beta^T \end{bmatrix}. \tag{2}$$

Therefore, we will concentrate on the probability that the Edmonds matrix in (2) is nonsingular, instead of directly referring to the transfer function in (1).

For acyclic graphs, we number the links ancestrally, i.e., lower-numbered links upstream of higher-numbered links, so matrix $\mathbf{F}$ is upper triangular with zeros on the diagonal. A triple $(\mathbf{A}, \mathbf{F}, \mathbf{B})$, where

$$\mathbf{A} = \left[\begin{array}{c|c|c} \mathbf{A}_1 & & \\ \hline & \ddots & \\ \hline & & \mathbf{A}_{J-1} \end{array}\right], \quad \mathbf{F} = \left[\mathbf{F}_1 \mid \cdots \mid \mathbf{F}_{J-1}\right], \quad \text{and } \mathbf{B}^T = \left[\mathbf{B}_{\beta_1}^T \mid \cdots \mid \mathbf{B}_{\beta_d}^T\right]$$

specifies the behavior of the network, and represents a linear network code. More specifically, $r_j \times n_j$ matrix $\mathbf{A}_j$ describes how r_j source processes generated at node j are randomly mixed to send them onto the n_j output links of node j for $j = 1, \cdots, J-1$, where J is the total number of nodes in the network. Similarly, $|\mathcal{E}| \times n_j$ matrix $\mathbf{F}_j$ describes how m_j incoming processes, except the r_j newly generated source processes at node j, are randomly mixed to send them onto the n_j output links of node j for $j = 1, \cdots, J-1$.

We also consider a linearly correlated sources modeled as given linear combinations of underlying independent processes, each with an entropy rate of one bit per unit time. The jth column of the matrix $\mathbf{A}$ is a linear function $\sum_k \alpha_{k,j}\mathbf{x}_j^k$ of given column vectors $\mathbf{x}_j^k \in \mathbb{F}_q^r$, where $\mathbf{x}_j^k$ specifies the mapping from r underlying independent processes to the kth source process at $o(j)$.

III. Main Results

A. Upper Bounds on the Decoding Probability

This section has two main results. First, a topology-independent upper bound on the decoding probability is given:

Theorem 1. *Consider a multicast connection problem on an arbitrary network with r source processes, d receiver nodes, and ν_β terminal links at receiver node β; and a network code in which some of network code coefficients $\{a_{i,j}$ ($\alpha_{k,j}$ for linearly correlated sources$), f_{l,j}, b_{\beta,i,l}\}$ are chosen uniformly at random from a finite field $\mathbb{F}_q$ where $q > d$, and in which the remaining code coefficients, if any, are fixed. If there exists a solution to the network connection problem with the same values for the fixed code coefficients, the probability that the random network code is valid for the problem is at most*

$$\prod_{i=1}^{d}\prod_{k=1}^{r} \frac{1 - q^{r-\nu_{\beta_i}-k}}{1 - q^{-k}} \left(1 - \frac{1}{q^{r-k+1}}\right)^2. \tag{3}$$

Proof: See Section IV. ■

Observe that, if r decreases, or ν_{β_i} increases, i.e., there are redundant terminal links of the network, the topology-independent upper bound in (3) increases. This is consistent to the intuition that more redundancy should improve random linear network coding. On the other hand, since the upper bound in (3) is obtained by assuming all source processes are available at each node except the last node, it can be loose for networks whose source-sink minimum cut is small compared to the overall network size. These imply that (3) is tight enough to reflect the physical characteristics of the network whose source-sink minimum cut is relatively large compared to r. Moreover, it can be applicable across all networks with the same r, d, and ν_β, without going to the details of specific network topology.

Second, we provide a topology-dependent upper bound on the decoding probability:

Theorem 2. *Consider the same multicast connection problem on an arbitrary network as described in Theorem 1. In addition, let J denotes the number of nodes including source nodes and receiver nodes. If there exists a solution to the network connection problem with the same values for the fixed*

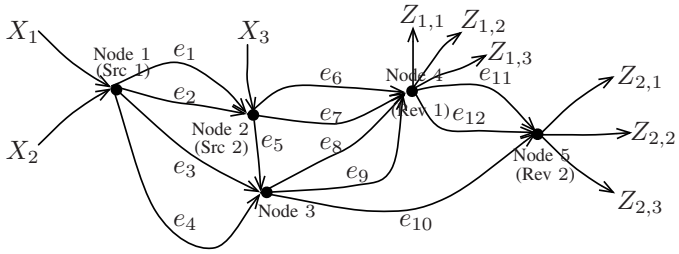

Fig. 1. Communication network with two source nodes and two receiver nodes.

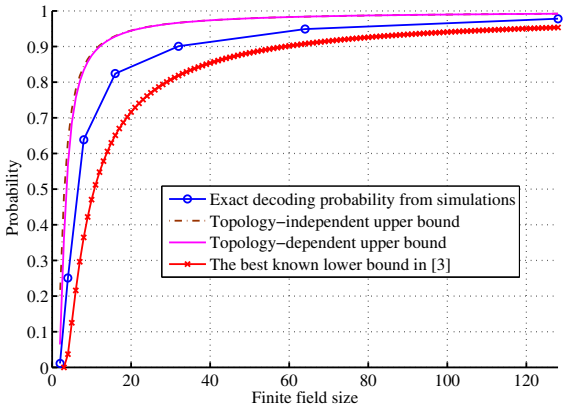

Fig. 2. The exact decoding probability, its topology-independent/dependent upper bounds, and its best known lower bound in [3].

code coefficients, the probability that the random network code is valid for the problem is at most (4), where $r = \sum_{j=1}^{J-1} r_j$, *and* m_j *is the number of incoming links at node* j.

Proof: See Section IV. ■

Unlike the topology-independent upper bound in (3), the topology-dependent upper bound in (4) depends not only on the amount of redundancy in the terminal links of the network, but also on a network wide notion of redundancy. We can show that the topology-dependent upper bound in (4) is tighter than the topology-independent upper bound in (3) by taking a ratio of (4) to (3).

Fig. 1 illustrates a communication network with two source nodes and two receiver nodes as an example. Fig. 2 shows the exact decoding probability obtained from simulations, its topology-independent, topology-dependent upper bounds, and the lower bound in [3]. We note that having more redundant links in a network increases the upper bounds on the decoding probability. This is consistent to the intuition that random linear network coding performs better, when there are more redundant nodes and links in the network. Contrarily, more redundancy decreases all the known lower bounds in [2], [3], [7]. Therefore, the upper bounds are especially useful in a large network with many links and nodes.

B. Network Resources Optimization

Two dominant costs incurred by random linear network coding are due to the decoding errors and computation complexity for intermediate processing and decoding at each receiver. The decoding error incurs retransmission that consumes more network resources. Thus, one needs to maximize the decoding probability, while minimizing the computational complexity.

The decoding probability improves with finite field size at the cost of increased computational complexity. Thus, the upper bounds and the best known lower bound on the decoding probability in [3] can be used to optimize the use of network resources by exploiting a trade-off between the decoding probability and computational complexity over finite field size.

The computational complexity is affected by the following: To recover the source processes, first, each receiver needs to evaluate the transfer matrix, $\mathbf{A}(\mathbf{I}-\mathbf{F})^{-1}\mathbf{B}_\beta^T$, in (1), which requires $\mathcal{O}\left(\left(|\mathcal{E}|^3 + r|\mathcal{E}|^2 + r^2|\mathcal{E}|\right)\log_2^2 q\right)$ binary operations, because typical algorithms for multiplications/inversions over a field of size $q = 2^n$ requires $\mathcal{O}(n^2)$ binary operations. Note that the fast implemented algorithms using Karatsuba method for multiplication in [6] require $\mathcal{O}(n^{log_2 3}) = \mathcal{O}(n^{1.585})$ binary operations. Second, each receiver needs to solve a system of the $r \times r$ linear equations, $Z_\beta = X\mathbf{A}(\mathbf{I}-\mathbf{F})^{-1}\mathbf{B}_\beta^T$, in (1), which requires $\mathcal{O}(r^3)$ operations over $\mathbb{F}_q$ if Gaussian elimination is used, while a successful parallel fast implemented algorithm using Strassen method in [6] requires $\mathcal{O}(r^{2.808})$ operations over $\mathbb{F}_q$.

This observation yields the cost function that increases with the number of required binary operations and decreases with the decoding probability. Since we have only the upper and lower bounds on the decoding probability, we design two cost functions with the upper and the lower bounds, respectively, as follows: Using the said fast algorithms, we have

$$\begin{aligned}\mathrm{Cost}_i(q) \;=\; & c_{i1}\left(|\mathcal{E}|^{2.808} + r|\mathcal{E}|^2 + r^2|\mathcal{E}| + r^{2.808}\right)(\log_2 q)^{1.585} \\ & + c_{i2}\,\Pr_i\left\{\exists T_\beta^{-1}\right\} \end{aligned} \tag{5}$$

$$\prod_{i=1}^{d}\left[\prod_{j=1}^{J-1}\left[\left\{\prod_{k_j=1}^{r_j}\frac{1-q^{r_j-n_j-k_j}}{1-q^{-k_j}}\left(1-\frac{1}{q^{r_j-k_j+1}}\right)\right\}\cdot\left[\sum_{r^\star_{f,j}=\min(m_j,n_j)-\sum_{i=1}^{j}(n_i-m_i-r_i)}^{\min(m_j,n_j)}\frac{q^{r^\star_{f,j}(m_j+n_j-r^\star_{f,j})}}{q^{m_jn_j}}\cdot\begin{cases}\displaystyle\prod_{k_j=1}^{r^\star_{f,j}}\frac{1-q^{r^\star_{f,j}-\max(m_j,n_j)-k_j}}{1-q^{-k_j}}\left(1-\frac{1}{q^{\min(m_j,n_j)-k_j+1}}\right), & r^\star_{f,j}\geq 1,\\ 1, & r^\star_{f,j}=0,\end{cases}\right]\right]\cdot\prod_{k=1}^{r}\frac{1-q^{r-\nu_{\beta_i}-k}}{1-q^{-k}}\left(1-\frac{1}{q^{r-k+1}}\right)\right] \tag{4}$$

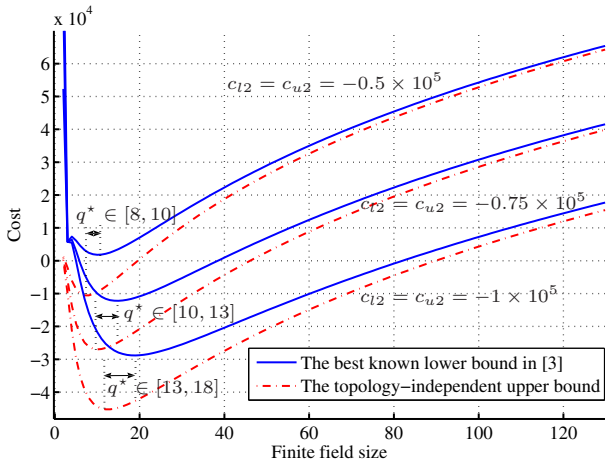

Fig. 3. Cost functions with the topology-independent upper bound and the best known lower bound in [3], and computational complexity over various weight coefficients c_{ij}'s.

for $i \in \{u, l\}$, where $\Pr_u\left\{\exists T_\beta^{-1}\right\}$ and $\Pr_l\left\{\exists T_\beta^{-1}\right\}$ represents the topology-independent upper bound in (3) and the best known lower bound on the decoding probability $\Pr_l\left\{\exists T_\beta^{-1}\right\} = \left(1 - \frac{d}{q-1}\right)^{J-d}$ in [3].

Lemma 1. *The functions $Cost_i(q)$'s in (5) are quasiconvex over the finite field size $q \geq 2$ for any $c_{i1} > 0$, $c_{i2} < 0$, and $i \in \{u, l\}$.*

Proof: The idea is to use Jensen's inequality for quasiconvex functions [4]. First, consider the cost function $\text{Cost}_u(q)$. Set $q_0 = \theta q_1 + (1-\theta)q_2$ and $0 \leq \theta \leq 1$. Since $c_{u1}\left(|\mathcal{E}|^{2.808} + r|\mathcal{E}|^2 + r^2|\mathcal{E}| + r^{2.808}\right)(\log_2 q)^{1.585}$ and $c_{u2}\prod_{i=1}^{d}\prod_{k=1}^{r}\frac{1-q^{r-\nu_{\beta_i}-k}}{1-q^{-k}}\left(1 - \frac{1}{q^{r-k+1}}\right)^2$ are monotonically increasing and decreasing functions over q for fixed $c_{i1} > 0$ and $c_{i2} < 0$, respectively, we have

$$\text{Cost}_u(q_0) \leq \max\left\{\text{Cost}_u(q_1), \text{Cost}_u(q_2)\right\} \tag{6}$$

for any $q_1, q_2 \in [2, \infty)$. It is straightforward to show that $\mathbf{dom}\ \text{Cost}_u(q) = [2, \infty)$ is convex. Thus, the above Jensen's inequality in (6) implies that $\text{Cost}_u(q)$ is a quasiconvex function over q [4]. In the same way, we can also show that $\text{Cost}_l(q)$ is a convex function. This proves the lemma. ■

Corollary 1. *A convex optimization problem $\min Cost_i(q)$ subject to $q \in [2, \infty)$, $i \in \{u, l\}$ has a unique solution.*

Proof: This is a direct consequence of Lemma 1. ■

From $\text{Cost}_u(q)$ and $\text{Cost}_l(q)$, we obtain the range of the optimal finite field size $q^\star$ rather than the exact optimal value $q^\star$. Note that, for simplicity, we use the topology-independent upper bound, while we can also replace it with the topology-dependent upper bound in (4) for (5).

Fig. 3 shows the cost functions with $c_{i1} = 1$ and different c_{i2}'s for the communication networks in Fig. 1, and the range of the optimal finite field size $q^\star$ providing the minimum cost, when each weight coefficients c_{ij} is given for $i = \{u, l\}$ and $j = 1, 2$. For example, in the case of $c_{11} = c_{21} = 1$ and $c_{u2} = c_{l2} = -0.5 \times 10^5$, the minimum value 8 of the range of $q^\star$ is obtained from the topology-independent upper bound on the decoding probability, whereas the maximum value 10 of the range of $q^\star$ from the best known lower bound. Thus, under the given constraints, the optimal finite field size $q^\star$ providing the minimum cost is some number between 8 and 10.

Fig. 3 describes that, if minimizing decoding error is more important than the computational complexity, finite field size q should be increased. On the other hand, if the computational complexity is more valuable than the decoding capability, the optimal finite field size $q^\star$ should be relatively small.

IV. Mathematical Development and Proofs

First, in order to prove Theorem 1 and 2, we need the following equality:

Lemma 2. *For $|s| < 1$,*

$$\prod_{m=0}^{r}\frac{1}{1-q^m s} = \sum_{n=0}^{\infty}\left(\prod_{k=1}^{r}\frac{1-q^{n+k}}{1-q^k}\right)s^n.$$

Proof: The Taylor expansion of an analytic function on the left hand side yields the desired equality. Due to the page limit, we omit the proof. ■

Next, we need the following lemma providing the number of all possible matrices with arbitrary rank, which will be very useful in the counting argument to find upper bounds on the decoding probability:

Lemma 3. *For $\nu \geq r \geq r^\star \in \mathbb{Z}_{++}$,*

$$\mathbf{card}\{\mathbf{B}_\beta^T \in \mathbb{F}_q^{\nu\times r} | \mathbf{rank}\mathbf{B}_\beta^T = r^\star\} = \prod_{k=1}^{r^\star}\frac{1-q^{\nu-r^\star+k}}{1-q^k}(q^r - q^{k-1}).$$

Proof: After two applications of rooted trees and a modified Motzkin triangle, we show the equality. Due to the page limit, we omit the proof. For a different proof, refer to [5]. ■

We are now ready to prove the first main result:

Proof of Theorem 1: An upper bound on the decoding probability can be obtained by assuming that all source processes are available at each node in a network except node J for its random linear network coding. Then, $\mathbf{A}$ is no longer a $r \times |\mathcal{E}|$ sparse matrix whose structure is constrained by the network. Instead $\mathbf{A}$ is a fully dense matrix denoted by $\mathbf{A}^\star$, every element of which is chosen independently and uniformly over $\mathbb{F}_q$, while the other structure, $\mathbf{F}$ and $\mathbf{B}_\beta$, of the network remains the same. Let us denote the modified Edmonds matrix by $\mathbf{T}_\beta^\star \in \mathbb{F}_q^{(r+|\mathcal{E}|)\times(r+|\mathcal{E}|)}$.

We begin by stating that

$$\Pr\left\{\exists \mathbf{T}_\beta^{-1}\right\} \leq \Pr\left\{\exists \mathbf{T}_\beta^{\star\,-1}\right\} = \frac{\mathbf{card}\left\{\mathbf{T}_\beta^\star \middle| \exists \mathbf{T}_\beta^{\star\,-1}\right\}}{\mathbf{card}\left\{\mathbf{T}_\beta^\star\right\}}. \tag{7}$$

In the case $\nu_\beta = 1, 2, \ldots, r-1$, the Edmonds matrix $\mathbf{T}_\beta^\star$ is singular for every possible code coefficient in $\mathbb{F}_q$. The

$$\mathbf{card}\left\{\mathbf{T}_\beta^\star \,\middle|\, \exists \mathbf{T}_\beta^{\star\,-1}\right\} = \mathbf{card}\left\{\mathbf{I}-\mathbf{F} \in \mathbb{F}_q^{|\mathcal{E}|\times|\mathcal{E}|}\right\} \cdot \mathbf{card}\left\{\mathbf{B}_\beta^T \in \mathbb{F}_q^{|\mathcal{E}|\times r} \,|\mathbf{rank}\mathbf{B}_\beta^T = r\right\} \cdot \mathbf{card}\left\{\mathbf{A}^\star \in \mathbb{F}_q^{r\times|\mathcal{E}|} \,\middle|\, \langle[\mathbf{A}^\star\ 0]\rangle \perp \mathbf{proj}_S\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle,\ \mathbf{rank}\mathbf{B}_\beta^T = r\right\} \tag{8}$$

singularity comes from the fact that we cannot generate r linearly independent columns of $\mathbf{B}_\beta^T$. Because all elements of $\mathbf{B}_\beta^T$ except $\nu_\beta r$ elements in ν_β r-dimensional row vector are fixed as zeros, the number ν_β of the incoming processes at receiver node β serves as an upper bound on $\mathbf{rank}\mathbf{B}_\beta^T$, which is strictly less than r, i.e., $\mathbf{rank}\mathbf{B}_\beta^T \le \nu_\beta < r$. We shall therefore consider the case $\nu_\beta = r, r+1, \ldots$.

Using the counting argument, the total number of all possible distinct Edmonds matrices $\mathbf{T}_\beta^\star$ is simply given by

$$\mathbf{card}\left\{\mathbf{T}_\beta^\star\right\} = q^{r|\mathcal{E}|} \cdot \mathbf{card}\{\mathbf{I}-\mathbf{F} \in \mathbb{F}_q^{|\mathcal{E}|\times|\mathcal{E}|}\} \cdot q^{r\nu_\beta}. \tag{9}$$

Next, we show that the total number $\mathbf{card}\left\{\mathbf{T}_\beta^\star \,\middle|\, \exists \mathbf{T}_\beta^{\star\,-1}\right\}$ of all possible distinct nonsingular Edmonds matrices $\mathbf{T}_\beta^\star$ is given by (8). We evaluate $\mathbf{card}\left\{\mathbf{T}_\beta^\star \,\middle|\, \exists \mathbf{T}_\beta^{\star\,-1}\right\}$ by generating each row sequentially from the last row to the first so that ith row is not a linear combination of the previously generated last $r+|\mathcal{E}|-i$ rows.

First, observe that $|\mathcal{E}| \times (r+|\mathcal{E}|)$ submatrix $\left[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T\right]$ always has $|\mathcal{E}|$ linearly independent rows regardless of the choice of code coefficients $\{f_{l,j}, b_{\beta,i,l} \in \mathbb{F}_q\}$, because $\mathbf{I}-\mathbf{F}$ is an upper triangular matrix with ones on the diagonal. However, $r \times (|\mathcal{E}|+r)$ submatrix $[\mathbf{A}^\star\ 0]$ does not necessarily have r linearly independent rows in the modified Edmonds matrix $\mathbf{T}_\beta^\star$ for some $\{a_{i,j}$ ($\alpha_{k,j}$ for linearly correlated sources), $f_{l,j}, b_{\beta,i,l} \in \mathbb{F}_q\}$ even if $[\mathbf{A}^\star\ 0]$ itself has r linearly independent rows, because some linear combinations of the rows of $\left[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T\right]$ can be expressed in the form $[\overbrace{\times\times\cdots\times}^{|\mathcal{E}|}\overbrace{0\cdots0}^{r}]$ that is the same form of the rows of $[\mathbf{A}^\star\ 0]$. This observation leads us to the following lemma:

Lemma 4. *$|\mathcal{E}| \times r$ tall matrix $\mathbf{B}_\beta^T$ has full column rank, i.e., $\mathbf{rank}\mathbf{B}_\beta^T = r$ in order for the modified Edmonds matrix $\mathbf{T}_\beta^\star$ to be nonsingular.*

Proof: The idea is to show that the following two inequalities are true:

$$\mathbf{rank}\mathbf{B}_\beta^T \le r, \text{ and } \mathbf{rank}\mathbf{B}_\beta^T \ge r.$$

The first inequality $\mathbf{rank}\mathbf{B}_\beta^T \le r$ comes from the fact that $|\mathcal{E}|\times r$ tall matrix $\mathbf{B}_\beta^T$ has at most r linearly independent rows.

The second inequality $\mathbf{rank}\mathbf{B}_\beta^T \ge r$ is a harder part. Set $\mathbf{rank}\mathbf{B}_\beta^T = r^\star$. Then $r^\star$ linearly independent rows of $\mathbf{B}_\beta^T$ can span the remaining $|\mathcal{E}|-r^\star$ rows of $\mathbf{B}_\beta^T$, i.e., $\mathbf{dim}\mathcal{N}(\mathbf{B}_\beta) = |\mathcal{E}|-r^\star$, where $\mathcal{N}(\mathbf{B}_\beta)$ is defined by the nullspace of matrix $\mathbf{B}_\beta$. Let S be a $|\mathcal{E}|$ dimensional subspace in $\mathbb{F}_q^{|\mathcal{E}|+r}$, the elements of which are in the form $[\overbrace{\times\times\cdots\times}^{|\mathcal{E}|}\overbrace{0\cdots0}^{r}]$. Then the projection of $\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle$ onto S results in a $|\mathcal{E}|-r^\star$ dimensional subspace in $\mathbb{F}_q^{|\mathcal{E}|+r}$, where $\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle$ is defined to be the rowspace of $[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]$, because $\mathbf{dim}\mathcal{N}(\mathbf{B}_\beta) = |\mathcal{E}|-r^\star$ and $|\mathcal{E}| \times (r+|\mathcal{E}|)$ submatrix $\left[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T\right]$ always has $|\mathcal{E}|$ linearly independent rows regardless of the choice of code coefficients $\{f_{l,j}, b_{\beta,i,l} \in \mathbb{F}_q\}$.

We now generate r linearly independent rows of $\mathbf{A}^\star$ sequentially so that not only are the rows of $\mathbf{A}^\star$ linearly independent, but also the projection of $\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle$ onto $\langle[\mathbf{A}^\star\ 0]\rangle$ results in a 0 dimensional subspace in $\mathbb{F}_q^{|\mathcal{E}|+r}$, that is,

$$\{0\} = \langle[\mathbf{A}^\star\ 0]\rangle \cap \mathbf{proj}_S\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle,$$

and the direct sum of two subspaces $\langle[\mathbf{A}^\star\ 0]\rangle$ and $\mathbf{proj}_S\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle$ is in S:

$$S \supset \langle[\mathbf{A}^\star\ 0]\rangle \oplus \mathbf{proj}_S\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle,$$

where $\mathbf{proj}_S$ is the projection

$$\mathbf{proj}_S : \mathbb{F}_q^{|\mathcal{E}|+r} \longrightarrow S$$

of $\mathbb{F}_q^{|\mathcal{E}|+r}$ onto S. This implies

$$|\mathcal{E}| \ge r + (|\mathcal{E}|-r^\star) \Longrightarrow r^\star \ge r,$$

which brings the desired result. ■

Thus the modified Edmonds matrix $\mathbf{T}_\beta^\star$ is nonsingular if and only if the following conditions are satisfied:

1) $\mathbf{B}_\beta^T$ has full column rank, i.e., $\mathbf{rank}\mathbf{B}_\beta^T = r$;
2) $\langle[\mathbf{A}^\star\ 0]\rangle \perp \mathbf{proj}_S\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle$.

The necessary and sufficient conditions on nonsingular matrix $\mathbf{T}_\beta^\star$ imply that the total number $\mathbf{card}\left\{\mathbf{T}_\beta^\star \,\middle|\, \exists \mathbf{T}_\beta^{\star\,-1}\right\}$ of all possible distinct nonsingular modified Edmonds matrices $\mathbf{T}_\beta^\star$ is given by multiplying the total numbers of all possible distinct matrices $\mathbf{I}-\mathbf{F}$, $\mathbf{B}_\beta^T$ with $\mathbf{rank}\mathbf{B}_\beta^T = r$, and $\mathbf{A}^\star$ satisfying the conditions together as can be seen in (8).

Finally, we are in a position to evaluate $\mathbf{card}\left\{\mathbf{T}_\beta^\star \,\middle|\, \exists \mathbf{T}_\beta^{\star\,-1}\right\}$ in (8) explicitly. First, we know from Lemma 3 that

$$\mathbf{card}\{\mathbf{B}_\beta^T \in \mathbb{F}_q^{|\mathcal{E}|\times r} | \mathbf{rank}\mathbf{B}_\beta^T = r\} = \mathbf{card}\{\mathbf{B}_\beta^T \in \mathbb{F}_q^{\nu_\beta\times r} | \mathbf{rank}\mathbf{B}_\beta^T = r\} \tag{10}$$

$$= \prod_{k=1}^{r} \frac{1-q^{\nu_\beta-r+k}}{1-q^k}(q^r - q^{k-1}), \tag{11}$$

where (10) is from the fact that elements of only ν_β rows of $\mathbf{B}_\beta^T$ are randomly chosen, while the others are rows of zeros.

Second, assuming that $\mathbf{B}_\beta^T$ has full rank, we now evaluate $\mathbf{card}\left\{\mathbf{A}^\star \in \mathbb{F}_q^{r\times|\mathcal{E}|} \,\middle|\, \langle[\mathbf{A}^\star\ 0]\rangle \perp \mathbf{proj}_S\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle\right\}$ by generating each row of $[\mathbf{A}^\star\ 0]$ sequentially from the last row to the first so that ith row is not a linear combination of the previously generated last $r-i$ rows in $[\mathbf{A}^\star\ 0]$ and the elements of $\mathbf{proj}_S\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle$. Since the first condition $\mathbf{rank}\mathbf{B}_\beta^T = r$

$$\mathbf{card}\left\{\mathbf{A}^\star \in \mathbb{F}_q^{r\times|\mathcal{E}|} \,\middle|\, \langle[\mathbf{A}^\star\ 0]\rangle \perp \mathbf{proj}_S\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle\right\} = \prod_{k=1}^{r}(q^{|\mathcal{E}|} - q^{k-1+|\mathcal{E}|-r}) \tag{12}$$

$$\prod_{\beta=1}^{d}\left[\Pr\left\{\mathbf{rank}\mathbf{B}_\beta^T=r\right\}\cdot\prod_{j=1}^{J-1}\left\{\begin{array}{l}\Pr\left\{\mathbf{rank}\mathbf{A}_j=r_j\right\}\cdot\\ \Pr\left\{\min(m_j,n_j)-\sum_{i=1}^{j}(n_i-m_i-r_i)\le\mathbf{rank}\mathbf{F}_j\le\min(m_j,n_j)\right\}\end{array}\right\}\right] \tag{13}$$

implies $\mathbf{dim}\left(\mathbf{proj}_S\langle[\mathbf{I}-\mathbf{F}\ \mathbf{B}_\beta^T]\rangle\right)=|\mathcal{E}|-r$, this process yields $q^{|\mathcal{E}|}-q^{k-1+|\mathcal{E}|-r}$ possible choices of such kth row in $[\mathbf{A}^\star\ 0]$, and thus (12).

Combining (7), (8), (9), (11), and (12) yields the desired probability. This proves the theorem. ■

Proof of Theorem 2: The trick of the proof is to use a necessary condition for the random linear network coding to be valid for the multicast connection problem.

Consider the network satisfying the min-cut max-flow bound, since Koetter and Médard [8] showed that there is a solution to the multicast connection problem if and only if the min-cut max-flow bound is satisfied. When a simple cut-set is deleted from a connected two-terminal network, the network falls into exactly two parts, a left part containing node 1 and a right part containing node J, where J is the total number of nodes in the network. In order for the random linear network coding to be valid in the multicast connection, the following conditions should be met: 1) r_j source processes must flow onto the output links of node j, that is, each $\mathbf{A}_j,\ j=1,\cdots,J-1$, has full rank, 2) r information processes must be extracted at receiver node β for $\beta=1,\cdots,d$, that is, $\mathbf{B}_\beta^T$ has full rank, and 3) when we change a simple cut-set by moving node j from the right part to the left part sequentially, node j must do random linear network coding in a way that at least $\sum_{i=1}^{j}r_i$ source processes must flow onto the simple cut-set changed by the move of node j for $j=1,\cdots,J-1$. More specifically, the simple cut-set bound determined by the move of node j must be greater than or equal to $\sum_{i=1}^{j}r_i$ source processes generating in the left part plus the number of information processes that collapses after passing through node j, that is,

$$\sum_{i=1}^{j}(n_i-m_i-r_i)-\{\min(m_j,n_j)-\mathbf{rank}\mathbf{F}_j\}\ge 0$$

for $1\le j\le J-1$. Thus a necessary condition for the random linear network coding to be valid is

1) $\mathbf{A}_j$ and $\mathbf{B}_\beta^T$ have full rank for $j=1,\cdots,J-1$, and $\beta=1,\cdots,d$, respectively,
2) $\min(m_j,n_j)-\sum_{i=1}^{j}(n_i-m_i-r_i)\le\mathbf{rank}\mathbf{F}_j\le\min(m_j,n_j),\ j=1,\cdots,J-1$.

Since all events are independent, the topology-dependent upper bound on the decoding probability is (13).

Lemma 3 and the fact that the elements of only m_j rows of F_j are randomly chosen, while the others are rows of zeros, yield

$$\Pr\left\{\mathbf{rank}\mathbf{B}_\beta^T=r\right\}=\prod_{k=1}^{r}\frac{1-q^{r-\nu_\beta-k}}{1-q^{-k}}\left(1-\frac{1}{q^{r-k+1}}\right), \tag{14}$$

$$\Pr\left\{\mathbf{rank}\mathbf{A}_j=r_j\right\}=\prod_{k_j=1}^{r_j}\frac{1-q^{r_j-n_j-k_j}}{1-q^{-k_j}}\left(1-\frac{1}{q^{r_j-k_j+1}}\right), \tag{15}$$

and (16). Plugging (14), (15), and (16) in (13) completes the proof. ■

V. Conclusion

In this paper, we obtained both the topology-independent and the topology-dependent upper bounds on the decoding probability of multisource multicast network using random linear network coding. The upper bounds are tighter than all the known lower bounds in a sense that both the upper bounds and the exact decoding probability increase over the number of redundant paths and nodes in a network, while all the known lower bounds decrease. For the optimal design of random linear network codes that minimizes the power related cost, we optimize the finite field size governing the computational complexity for encoding/decoding and the decoding probability at receivers. The left endpoint of the optimal finite field size range was given by the upper bounds on the decoding probability, while the right endpoint was given by the best known lower bound in [3]. Our result is useful for wireless networks, in which it is critical to optimize limited network resources such as power, time, bandwidth, computational capabilities of nodes, and number of nodes that are able to code.

One further research involves the development of tighter lower bound that increases over extra paths and nodes in a network. This can give a superior tool for a large network resources optimization.

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] H. Balli, X. Yan, and Z. Zhang, "Error correction capability of random network error correction codes," in Proc. *2007 IEEE Int. Symp. Information Theory*, pp. 1581–1585, Nice, France, Jun. 2007.

[3] H. Balli and Z. Zhang, "On the limiting behavior of random linear network codes," in Proc. *2009 Workshop on Network Coding, Theory and Applications*, Lausanne, France, Jun. 2009.

[4] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York: Cambridge University Press, 2004.

[5] S. D. Fisher and M. N. Alexander, "Matrices over a finite field," *Amer. Math. Monthly* 73, 639–641, 1966.

[6] J. Gathen and J. Gerhard, *Modern Computer Algebra*. New York: Cambridge University Press, 2003.

[7] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[8] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw*, vol. 11, no. 5, pp. 782 – 795, Oct. 2003.

[9] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

$$\begin{aligned}&\Pr\left\{\min(m_j,n_j)-\textstyle\sum_{i=1}^{j}(n_i-m_i-r_i)\le\mathbf{rank}\mathbf{F}_j\le\min(m_j,n_j),\ j=1,\cdots,J-1\right\}\\ &=\sum_{r_{f,j}^\star=\min(m_j,n_j)-\sum_{i=1}^{j}(n_i-m_i-r_i)}^{\min(m_j,n_j)}\frac{q^{r_{f,j}^\star(m_j+n_j-r_{f,j}^\star)}}{q^{m_jn_j}}\left\{\begin{array}{ll}\prod_{k_j=1}^{r_{f,j}^\star}\frac{1-q^{r_{f,j}^\star-\max(m_j,n_j)-k_j}}{1-q^{-k_j}}\left(1-\frac{1}{q^{\min(m_j,n_j)-k_j+1}}\right), & r_{f,j}^\star\ge 1,\\ 1, & r_{f,j}^\star=0.\end{array}\right.\end{aligned} \tag{16}$$