Rate Regions for Coherent and Noncoherent Multisource Network Error Correction

Svitlana Vyetrenko, Tracey Ho, Michelle Effros
California Institute of Technology
Email: {svitlana,tho,effros}@caltech.edu

Joerg Kliewer
New Mexico State University
Email: jkliewer@nmsu.edu

Elona Erez
Yale University
Email: elona.erez@yale.edu

Abstract—In this paper we derive capacity regions for network error correction with both known and unknown topologies (coherent and non-coherent network coding) under a multiple-source multicast transmission scenario. For the multiple-source non-multicast scenario, given any achievable network code for the error-free case, we construct a code with a reduced rate region for the case with errors.

I. INTRODUCTION

Network coding has emerged as a powerful technique to distribute information over networks. However, in unreliable or adversarial networks, due to error propagation in the network even a single error on a network link may lead to a corruption of many received packets at the destination nodes.

In the coherent case, there is centralized knowledge of the network topology and network code. Network error and erasure correction for this case has been addressed in [1] by generalizing classical coding theory to the network setting. In the non-coherent case, the network topology and/or network code are not known a priori; information transmission occurs via the space spanned by the received packets/vectors, since any generating set for the same space is equivalent to the receiver [2]. Error correction techniques for this case were recently proposed in [2] and [3] in the form of constant dimension and rank metric codes, respectively, where the codewords are defined as subspaces of some ambient space. Another approach that uses global coding vectors is given in [?]. These results primarily focus on the single source case. An extension to multiple sources in the noncoherent case has been recently addressed in [4], where an achievable rate region and practical coding schemes are given for two sources and a noncoherent multiple access channel model in the case without errors and erasures.

We find the network error correction capacity regions for multiple-source multicast for the coherent and noncoherent cases, in Sections III and IV respectively. For non-multicast, however, finding the capacity region of a general network even in the error-free case is an open problem. Thus, in Section V we consider the problem of constructing a network error correction code for the multiple-source non-multicast scenario from a given error-free network code.

II. NOTATION

Consider a network error correction problem on a directed acyclic graph $\mathcal{G}$ with n source nodes $\mathcal{S} = \{s_1, s_2, \ldots, s_n\}$ and a set of sink nodes $\mathcal{T}$. Each link has unit capacity, and there can be multiple parallel edges connecting a pair of nodes. Let r_i be the multicast transmission rate from s_i to each sink. For any non-empty subset $\mathcal{S}' \subseteq \mathcal{S}$, let $\mathcal{I}(\mathcal{S}')$ be the indices of the source nodes that belong to $\mathcal{S}'$. Let $m_{\mathcal{S}'}$ be the minimum cut capacity between any sink and $\mathcal{S}'$. For each $i, i = 1, \ldots, n$, let $\mathcal{C}_i$ be the code used by source i. Let $\mathcal{C}_{\mathcal{S}'}$ be the Cartesian product of the individual codes of the sources in $\mathcal{S}'$.

III. COHERENT MULTIPLE-SOURCE MULTICAST

Theorem 1 characterizes the network error correction capacity of centralized network coding over a known network $\mathcal{G}$ in a multiple-source multicast scenario.

Theorem 1. *Consider a multiple-source multicast network error correction problem on network $\mathcal{G}$ with known topology. For any arbitrary errors on up to z links, the capacity region is given by:*

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} r_i \le m_{\mathcal{S}'} - 2z \ \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{1}$$

Proof: Converse: Let $l_{i,j}, j = 1, \ldots, n_i$, be the outgoing links of each source $s_i, i = 1, \ldots, n$. Take any $\mathcal{S}' \subseteq \mathcal{S}$. We construct the graph $\mathcal{G}_{\mathcal{S}'}$ from $\mathcal{G}$ by adding a virtual super source node $w_{\mathcal{S}'}$, and n_i links $l'_{i,j}, j = 1, \ldots, n_i$, from $w_{\mathcal{S}'}$ to source s_i for each $i \in \mathcal{I}(\mathcal{S}')$. Note that the minimum cut capacity between $w_{\mathcal{S}'}$ and any sink is at least $m_{\mathcal{S}'}$. Any network code that multicasts rate r_i from each source $s_i, i \in \mathcal{I}(\mathcal{S}')$ over $\mathcal{G}$ corresponds to a network code that multicasts rate $\sum_{i \in \mathcal{I}(\mathcal{S}')} r_i$ from $w_{\mathcal{S}'}$ to all sinks over $\mathcal{G}_{\mathcal{S}'}$; the symbol on each link $l'_{i,j}$ is the same as that on link $l_{i,j}$, and the coding operations at all other nodes are identical for $\mathcal{G}$ and $\mathcal{G}_{\mathcal{S}'}$. The converse follows from applying the network Singleton bound [1] to $w_{\mathcal{S}'}$ for each $\mathcal{S}' \subseteq \mathcal{S}$.

Achievability: Construct the graph $\mathcal{G}_{\mathcal{S}}$ for the set of all source nodes $\mathcal{S}$ as in the proof of the converse. For the original n-source problem on $\mathcal{G}$, with high probability we can obtain a random linear network code $\mathcal{C}$ that can correct any $2z$ erasures iff the rate n−tuple $(r_1, r_2, \ldots, r_n)$ satisfies the cut set bound (1) [5]. This corresponds to a single-source network code $\mathcal{C}_{\mathcal{S}}$ on $\mathcal{G}_{\mathcal{S}}$ where the symbol on each link $l'_{i,j}$ is the same as that on link $l_{i,j}$, and the coding operations at all other nodes are identical for $\mathcal{G}$ and $\mathcal{G}_{\mathcal{S}}$.

For the single-source coherent case, the following are equivalent [6]:

1) a linear network code has network minimum distance at least $2z + 1$
2) the code corrects any error of weight at most z
3) the code corrects any erasure of weight at most $2z$.

This implies that $\mathcal{C}_{\mathcal{S}}$ has network minimum distance at least $2z + 1$, and so it can correct any z errors.

Note that a general single-source network code on $\mathcal{G}_{\mathcal{S}}$ would not correspond to a valid n-source network code on $\mathcal{G}_{\mathcal{S}}$, since for independent sources the set of source codewords in $\mathcal{C}_{\mathcal{S}}$ must be the Cartesian product of a set of codewords from $s_1, s_2, \ldots, s_n$. ∎

IV. NONCOHERENT MULTIPLE-SOURCE MULTICAST

Next we consider the multiple-source multicast capacity region in the non-coherent case where the network topology/transfer matrices are not known. Following the framework of constant-dimension noncoherent network coding in [2], let V be the vector space of length-K vectors over the finite field $\mathbb{F}_q$, representing the set of all possible values of packets transmitted and received in the network. Let $\mathcal{P}(V)$ denote the set of all subspaces of V. A code $\mathcal{C}$ consists of a nonempty subset of $\mathcal{P}(V)$, where each codeword $U \in \mathcal{C}$ is a subspace of constant dimension. The distance between two vector spaces U_1, U_2 is defined as

$$d(U_1, U_2) \doteq \dim(U_1) + \dim(U_2) - 2\dim(U_1 \cap U_2).$$

It is shown in [2] that d is a metric for $\mathcal{P}(V)$ and the triangle inequality holds. If U is the sent codeword and U' is the received codeword, then subspace minimum distance decoding is successful if and only if there is no codeword $\tilde{U} \neq U$ in $\mathcal{C}$ for which $d(\tilde{U}, U') \leq d(U, U')$. In [2] this approach is used to design codes of minimum distance D that correct up to a total of $\lfloor \frac{D-1}{2} \rfloor$ subspace errors (addition of vectors to the transmitted subspace) and erasures (deletion of vectors from the transmitted subspace).

Although the subspace coding approach is oblivious to the network topology, we study here the dependence of the achievable rates on the network topology and number of network errors. Network errors and erasures translate differently into subspace errors and erasures depending on the network code rate and network topology. Thus, to avoid confusion we will refer to subspace errors as additions and subspace erasures as deletions, and the terms errors and erasures will be reserved for network errors and erasures.

Theorem 2 gives the non-coherent capacity region. The code construction uses random linear network coding at intermediate nodes, single-source network error correction capacity-achieving codes at each source, and an overall global coding vector. The error analysis shows that decoding succeeds with high probability over the random network code. Note that straightforward distance arguments are not sufficient to show achievability, since a network error can potentially result in an addition plus a deletion, corresponding to a minimum distance requirement of $4z + 1$, which seems difficult to achieve in the multisource case.

Theorem 2. *Consider a multiple-source multicast network error correction problem on network $\mathcal{G}$ whose topology may be unknown. For any errors on up to z links, when random linear network coding in a sufficiently large finite field is performed, the capacity region is given by:*

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} r_i \leq m_{\mathcal{S}'} - 2z \; \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{2}$$

Proof: Converse. Follows from Theorem 1, since the noncoherent region is no larger than the coherent region.
Achievability.
1) Code construction: Consider any rate vector $(r_1, \ldots, r_n)$ such that

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} r_i < m_{\mathcal{S}'} - 2z \; \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{3}$$

Let each $\mathcal{C}_i$, $i = 1, \ldots, n$ be a code consisting of codewords that are k_i-dimensional linear subspaces. The codeword transmitted by source S_i is spanned by the packets transmitted by S_i. From the single source case, for each source $i = 1, \ldots, n$ we can construct a code $\mathcal{C}_i$ where

$$k_i > r_i + z \tag{4}$$

that corrects any z additions [7]. This implies that $\mathcal{C}_i$ has minimum distance greater than $2z$ [8], i.e. for any pair of distinct codewords $V_i, V_i' \in \mathcal{C}_i$

$$d(V_i, V_i') = \dim(V_i) + \dim(V_i') - 2\dim(V_i \cap V_i') > 2z.$$

Hence,

$$\dim(V_i \cap V_i') < k_i - z \; \forall V_i, V_i' \in \mathcal{C}_i. \tag{5}$$

By (3), scaling all source rates and link capacities by a sufficiently large integer if necessary, we can assume without loss of generality that we can choose k_i satisfying (4) as well as

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} k_i \leq m_{\mathcal{S}'} + (|\mathcal{S}'| - 2)z \; \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{6}$$

We can make vectors from one source linearly independent of vectors from all other sources by means of a length-$(\sum_{i \in \mathcal{I}(\mathcal{S})} k_i)$ global coding vector, which adds an overhead that becomes asymptotically negligible as packet length grows. This ensures that

$$\dim(V_i \cap V_j) = 0 \; \forall i \neq j, V_i \in \mathcal{C}_i, V_j \in \mathcal{C}_j. \tag{7}$$

2) Error analysis: Let $X \in \mathcal{C}_{\mathcal{S}}$ be the sent codeword, and let R be the subspace received at a sink. Consider any $\mathcal{S}' \subseteq \mathcal{S}$. Let $\overline{\mathcal{S}'} = \mathcal{S} \setminus \mathcal{S}'$. Let $X = V \oplus W$, where $V \in \mathcal{C}_{\mathcal{S}'}, W \in \mathcal{C}_{\overline{\mathcal{S}'}}$ and V is spanned by the codeword V_i from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$. We will show that with high probability over the random network code, there does not exist another codeword $Y = V' \oplus W$, such that V' is spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$, which could also have produced R under arbitrary errors on up to z links in the network.

Let $\mathcal{R}$ be the set of packets received by the sink, i.e. $R = \text{span}(\mathcal{R})$. Each of the packets in $\mathcal{R}$ can be expressed as $\mathbf{p} = \mathbf{u_p} + \mathbf{w_p}$, where $\mathbf{u_p}$ is a random linear combination

of zero or more packets from V and vectors transmitted on error links, and $\mathbf{w_p}$ is a random linear combination of zero or more packets from W.

Let $P = \text{span}\{\mathbf{u_p} : \mathbf{p} \in \mathcal{R}\}$. We next show that for random linear coding in a sufficiently large field, with high probability

$$\dim(P) - \dim(P \cap V') > z \qquad (8)$$

for all V' spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$.

Consider first the network with each source i in $\mathcal{S}'$ transmitting k_i linearly independent packets from V_i, sources in $\overline{\mathcal{S}'}$ silent, and no errors. From the maxflow-mincut bound, any rate vector $(h_1, \ldots, h_{|\mathcal{S}'|})$, such that

$$\sum_{i \in S''} h_i \leq m_{S''} \ \forall S'' \subseteq S'$$

can be achieved. Combining this with (6), we can see that in the error-free case, each $s_i \in \mathcal{S}'$ can transmit information to the sink at rate $k_i - \frac{(|\mathcal{S}'|-2)z}{|\mathcal{S}'|}$ for a total rate of

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z. \qquad (9)$$

With sources in $\overline{\mathcal{S}'}$ still silent, consider the addition of z unit-rate sources corresponding to the error links. The space spanned by the received packets corresponds to P. Consider any V' spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$.

Let Z be the space spanned by the error packets, and let $z' \leq z$ be the minimum cut between the error sources and the sink. Let $P = P_V \oplus P_Z$, where $P_Z = P \cap Z$ and P_V is a subspace of V. There exists a routing solution, which we distinguish by adding tildes in our notation, such that $\dim \tilde{P}_Z = z'$ and, from (9), $\dim \tilde{P} \geq \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z$, so

$$\dim(\tilde{P}_V) \geq \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z - z'. \qquad (10)$$

Note that, by (7), a packet from V_i is not in any $V_j' \in \mathcal{C}_j, j \neq i$, and hence is in V' if and only if it is in V_i'. Therefore, by (5)

$$\dim(\tilde{P}_V \cap V') \leq \sum_{i \in \mathcal{I}(\mathcal{S}')} \dim(V_i \cap V_i') < \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - |\mathcal{S}'|z.$$

Therefore, using (10) we have

$$\begin{aligned} \dim(\tilde{P}_V \cup V') &= \dim(\tilde{P}_V) + \dim(V') - \dim(\tilde{P}_V \cap V') \\ &> \dim(\tilde{P}_V) + \dim(V') + |\mathcal{S}'|z - \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i \\ &\geq \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z - z' + |\mathcal{S}'|z \\ &= \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i + 2z - z' \geq \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i + z. \end{aligned}$$

Then

$$\dim(\tilde{P} \cup V') > \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i + z.$$

For random linear coding in a sufficiently large field, with high probability by its generic nature

$$\dim(P \cup V') \geq \dim(\tilde{P} \cup V') > \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i + z,$$

and this also holds for any z or fewer errors, all sinks, and all V' spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$. Then, (8) follows by

$$\dim(P) - \dim(P \cap V') = \dim(P \cup V') - \dim(V').$$

By (7), if $\mathbf{w_p}$ is in W, then $\mathbf{u_p} + \mathbf{w_p}$ is in $V' \oplus W$ iff $\mathbf{u_p}$ is in V'. Hence, using (8),

$$\begin{aligned} \dim(R) - &\dim(R \cap (V' \oplus W)) \\ &\geq \dim(P) - \dim(P \cap V') > z. \end{aligned}$$

Thus, more than z additions are needed to produce R from $Y = V' \oplus W$. By the generic nature of random linear coding, with high probability this holds for any $\mathcal{S}'$. ∎

V. NON-MULTICAST

Consider a non-multicast problem with n independent sources and m sinks, where each source S_i, $i = 1, \ldots, n$, is demanded by a given set of sink nodes $\mathcal{T}_i$, and arbitrary coding across sessions is permitted. We give the following achievability result for the coherent case.

Theorem 3. *Given any linear network code $\mathcal{C}$ that achieves rate vector $\mathbf{r} = (r_1, r_2, \ldots, r_n)$ in the no-error case, where r_i is the information rate of source S_i, $i = 1, \ldots, n$, we can obtain a network code $\tilde{\mathcal{C}}$ that achieves rate vector $\tilde{\mathbf{r}} = (r_1 - 2z, r_2 - 2z, \ldots, r_n - 2z)$ under arbitrary errors on up to z links in the network.*

If the given linear network code $\mathcal{C}$ is a vector linear network code with vector length y, we can consider a modified network problem where each source is replaced with y co-located sources and each link with y parallel links joining the same nodes. The source rates and the number of errors are also scaled by y. Therefore, we may view the vector linear code $\mathcal{C}$ as a scalar linear code on the new network.

To prove Theorem 3, we first generalize the concept of network distance, introduced in [6] for multicast, to non-multicast as follows.

The Hamming weight of a vector $\mathbf{z}$ (the number of non-zero components of $\mathbf{z}$) is denoted by $w_H(\mathbf{z})$. As in [6], define a network erasure pattern ρ with Hamming weight $|\rho|$ as a set of channels in which an error may have occurred, whose location is known to all sink nodes. Abusing notation, we also use ρ to denote the set of vectors with nonzero entries corresponding to the erasure pattern ρ.

For any non-empty subset $\mathcal{S}' \subseteq \mathcal{S}$, let $A_{\mathcal{S}'}$ denote the transfer matrix mapping the length-$r_{\mathcal{S}'}$ vector $\mathbf{x}_{\mathcal{S}'}$ of source symbols of sources in $\mathcal{S}'$ to the corresponding incident outgoing links of the sources, where $r_{\mathcal{S}'} = \sum_{i \in \mathcal{S}'} r_i$. Let F_t be the transfer matrix from all links in the network to the incoming links of sink t. Let $Im(F_t)$ be the image of the map F_t. For any $t \in \mathcal{T}$, let $\mathcal{S}_t$ be the subset of sources demanded by sink node t, and $\overline{\mathcal{S}}_t$ the subset of sources not demanded by t. For any vector $\mathbf{y} \in Im(F_t)$ received at t, let

$$\Upsilon_t(\mathbf{y}) = \{\mathbf{z} : \exists \mathbf{x}_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}'}} \text{ s.t. } (\mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} + \mathbf{z})F_t = \mathbf{y}$$

1003

be the set of all error patterns that could result in $\mathbf{y}$ being observed at the sink. With this definition, we can, analogously to the multicast case in [6], develop the following definitions and results.

Definition 1. *For any sink node t, the network Hamming weight of a received vector $\mathbf{y} \in Im(F_t)$ is defined as*

$$W_t^{rec}(\mathbf{y}) = \min_{\mathbf{z} \in \Upsilon_t(\mathbf{y})} w_H(\mathbf{z}).$$

Definition 2. *For any sink node t, the network Hamming weight of a message vector $\mathbf{x}_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ is defined as*

$$W_t^{msg}(\mathbf{x}_{\mathcal{S}_t}) = W_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t).$$

Definition 3. *For any sink node t, the network Hamming distance between two received vectors $\mathbf{y}^1, \mathbf{y}^2 \in Im(F_t)$ is defined by*

$$D_t^{rec}(\mathbf{y}^1, \mathbf{y}^2) = W_t^{rec}(\mathbf{y}^1 - \mathbf{y}^2).$$

Definition 4. *For any sink node t, the network Hamming distance between two message vectors $\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2 \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$, is defined by*

$$D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2) = W_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1 - \mathbf{x}_{\mathcal{S}_t}^2).$$

Lemma 1. *For any sink node t, let $\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}^1 \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ be message vectors, $\mathbf{y}, \mathbf{y}^1 \in Im(F_t)$ be received vectors. Then we have*

$$
\begin{align}
D_t^{rec}(\mathbf{y}, \mathbf{y}^1) &= D_t^{rec}(\mathbf{y}^1, \mathbf{y}) \tag{11} \\
D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}^1) &= D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}) \tag{12} \\
D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}^1) &= D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{x}_{\mathcal{S}_t}^1 A_{\mathcal{S}_t} F_t) \tag{13}
\end{align}
$$

Proof: (11) and (12) follow from definitions of $W_t^{rec}(\mathbf{y})$, $W_t^{msg}(\mathbf{x}_{\mathcal{S}_t})$ and linearity of the code. To prove (13) note that:

$$
\begin{align}
D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}^1) &= W_t^{msg}(\mathbf{x}_{\mathcal{S}_t} - \mathbf{x}_{\mathcal{S}_t}^1) \\
&= W_t^{rec}((\mathbf{x}_{\mathcal{S}_t} - \mathbf{x}_{\mathcal{S}_t}^1) A_{\mathcal{S}_t} F_t) \\
&= D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{x}_{\mathcal{S}_t}^1 A_{\mathcal{S}_t} F_t).
\end{align}
$$

∎

Lemma 2 (Triangle inequality). *For any sink node t, let $\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2 \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ be message vectors, $\mathbf{y}, \mathbf{y}^1, \mathbf{y}^2 \in Im(F_t)$ be received vectors. Then we have:*

$$
\begin{align}
D_t^{rec}(\mathbf{y}_1, \mathbf{y}_2) &\le D_t^{rec}(\mathbf{y}_1, \mathbf{y}) + D_t^{rec}(\mathbf{y}, \mathbf{y}_2) \tag{14} \\
D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2) &\le D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}) + D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}^2) \tag{15}
\end{align}
$$

Proof: Consider $\mathbf{z}^1 \in \Upsilon_t(\mathbf{y}^1 - \mathbf{y})$ and $\mathbf{z}^2 \in \Upsilon_t(\mathbf{y} - \mathbf{y}^2)$ such that $D_t^{rec}(\mathbf{y}^1, \mathbf{y}) = w_H(\mathbf{z}^1)$ and $D_t^{rec}(\mathbf{y}, \mathbf{y}^2) = w_H(\mathbf{z}^2)$. By linearity of the code, $\mathbf{z}^1 + \mathbf{z}^2 \in \Upsilon_t(\mathbf{y}^1 - \mathbf{y}^2)$, therefore

$$
\begin{align}
D_t^{rec}(\mathbf{y}^1, \mathbf{y}^2) &= W_t^{rec}(\mathbf{y}^1 - \mathbf{y}^2) \\
&\le w_H(\mathbf{z}^1 + \mathbf{z}^2) \\
&\le w_H(\mathbf{z}^1) + w_H(\mathbf{z}^2) \\
&\le D_t^{rec}(\mathbf{y}^1, \mathbf{y}) + D_t^{rec}(\mathbf{y}, \mathbf{y}^2).
\end{align}
$$

(15) follows from (14) and (13):

$$
\begin{align}
&D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2) \\
&= D_t^{rec}(\mathbf{x}_{\mathcal{S}_t}^1 A_{\mathcal{S}_t} F_t, \mathbf{x}_{\mathcal{S}_t}^2 A_{\mathcal{S}_t} F_t) \\
&\le D_t^{rec}(\mathbf{x}_{\mathcal{S}_t}^1 A_{\mathcal{S}_t} F_t, \mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t) + D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{x}_{\mathcal{S}_t}^2 A_{\mathcal{S}_t} F_t) \\
&= D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}) + D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}^2).
\end{align}
$$

∎

Definition 5. *For each sink node t, the minimum distance of a network code is defined by:*

$$d_{\min,t} = \min\{D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2) : \mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2 \in \mathbb{F}_q^{r_{\mathcal{S}_t}}, \mathbf{x}_{\mathcal{S}_t}^1 \ne \mathbf{x}_{\mathcal{S}_t}^2\}$$

Definition 6. *The minimum distance of a network code is defined by:*

$$d_{min} = \min_{t \in \mathcal{T}} d_{\min,t}$$

Theorem 4. *For a sink node t, the following properties of a network code are equivalent:*

1) *the code has $d_{\min,t} \ge 2z + 1$;*
2) *any error $\mathbf{z}$ such that $w_H(\mathbf{z}) \le z$ can be corrected at t;*
3) *any erasure pattern ρ_t such that $|\rho_t| \le 2z$ can be corrected at t.*

Proof: $1 \Rightarrow 2$. For a message vector $\mathbf{x}_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ and an error vector $\mathbf{z}$, the received vector at t is given by

$$\mathbf{y}_t = \mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t + \mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z} F_t$$

for some $\mathbf{x}_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$. We will show that if $d_{\min,t} \ge 2z + 1$, the minimum distance decoding algorithm will always decode correctly for any message vector $\mathbf{x}_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ and any error vector $\mathbf{z}$ such that $w_H(\mathbf{z}) \le z$. By (14) for any $\mathbf{x}_{\mathcal{S}_t}' \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ such that $\mathbf{x}_{\mathcal{S}_t} \ne \mathbf{x}_{\mathcal{S}_t}'$ we have

$$
\begin{align}
&D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{x}_{\mathcal{S}_t}' A_{\mathcal{S}_t} F_t) \\
&\le D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{y}_t) + D_t^{rec}(\mathbf{x}_{\mathcal{S}_t}' A_{\mathcal{S}_t} F_t, \mathbf{y}_t). \tag{16}
\end{align}
$$

Note that

$$
\begin{align}
&D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{x}_{\mathcal{S}_t}' A_{\mathcal{S}_t} F_t) \\
&= D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}') \ge d_{\min,t} \ge 2z + 1 \tag{17} \\
&D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{y}_t) = W_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t - \mathbf{y}_t) \\
&= W_t^{rec}(\mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z} F_t) \le w_H(\mathbf{z}) \le z. \tag{18}
\end{align}
$$

Now using (16)-(18), we get

$$
\begin{align}
&D_t^{rec}(\mathbf{x}_{\mathcal{S}_t}' A_{\mathcal{S}_t} F_t, \mathbf{y}_t) \\
&\ge D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{x}_{\mathcal{S}_t}' A_{\mathcal{S}_t} F_t) - D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{y}_t). \\
&\ge z + 1 > D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{y}_t).
\end{align}
$$

Hence, the decoder outputs $\hat{\mathbf{x}} = \mathbf{x}_{\mathcal{S}_t}$ and $1 \Rightarrow 2$ follows.

$2 \Rightarrow 1$. We will prove this by contradiction. Assume that any error $\mathbf{z}$ with $w_H(\mathbf{z}) \le z$ can be corrected at t, but $d_{\min,t} \le 2z$. Take any $\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2 \in \mathbb{F}_q^{r_{\mathcal{S}_t}}, \mathbf{x}_{\mathcal{S}_t}^1 \ne \mathbf{x}_{\mathcal{S}_t}^2$ such that $W_t^{msg}((\mathbf{x}_{\mathcal{S}_t}^1 - \mathbf{x}_{\mathcal{S}_t}^2) A_{\mathcal{S}_t} F_t) = D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2) \le 2z$. Then by definition of $W_t^{msg}(.)$ there exist error vectors $\mathbf{z}$ and $\mathbf{x}_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$ such that

$$(\mathbf{x}_{\mathcal{S}_t}^1 - \mathbf{x}_{\mathcal{S}_t}^2) A_{\mathcal{S}_t} F_t = \mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z} F_t \tag{19}$$

with $w_H(\mathbf{z}) \le 2z$. Hence, we can find error vectors $\mathbf{z}^1$ and $\mathbf{z}^2$ such that $\mathbf{z} = \mathbf{z}^2 - \mathbf{z}^1$, $w_H(\mathbf{z}^1) \le z$ and $w_H(\mathbf{z}^2) \le z$. Also, by linearity of the code, we can find $\mathbf{x}_{\overline{\mathcal{S}}_t}^1, \mathbf{x}_{\overline{\mathcal{S}}_t}^2 \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$ such that $\mathbf{x}_{\overline{\mathcal{S}}_t} = \mathbf{x}_{\overline{\mathcal{S}}_t}^2 - \mathbf{x}_{\overline{\mathcal{S}}_t}^1$. Therefore, if $\mathbf{y}_t$ is received at t, by (19) we have two indistinguishable possibilities, a contradiction:

$$
\begin{align}
\mathbf{y}_t &= \mathbf{x}_{\mathcal{S}_t}^1 A_{\mathcal{S}_t} F_t + \mathbf{x}_{\overline{\mathcal{S}}_t}^1 A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z}^1 F_t \\
\mathbf{y}_t &= \mathbf{x}_{\mathcal{S}_t}^2 A_{\mathcal{S}_t} F_t + \mathbf{x}_{\overline{\mathcal{S}}_t}^2 A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z}^2 F_t.
\end{align}
$$

$1 \Rightarrow 3$. Let $d_{\min,t} \ge 2z + 1$ and $|\rho| \le 2z$. In order to prove the implication, we need to show that for any received vector

1004

$\mathbf{y}_t$, there is a unique message vector $\mathbf{x}_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ and some $\mathbf{x}_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$ and error $\mathbf{z} \in \rho$, such that

$$\mathbf{y}_t = \mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t + \mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z} F_t.$$

Call such $(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}_{\overline{\mathcal{S}}_t}, \mathbf{z})$ a solution of the decoding problem. Suppose the problem has two distinct solutions $(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\overline{\mathcal{S}}_t}^1, \mathbf{z}^1)$ and $(\mathbf{x}_{\mathcal{S}_t}^2, \mathbf{x}_{\overline{\mathcal{S}}_t}^2, \mathbf{z}^2)$. Then we have

$$\begin{aligned} D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2) &= W_t^{rec}((\mathbf{x}_{\mathcal{S}_t}^1 - \mathbf{x}_{\mathcal{S}_t}^2)A_{\mathcal{S}_t} F_t) \\ &= W_t^{rec}((\mathbf{x}_{\overline{\mathcal{S}}_t}^2 - \mathbf{x}_{\overline{\mathcal{S}}_t}^1)A_{\overline{\mathcal{S}}_t} F_t + (\mathbf{z}^2 - \mathbf{z}^1)F_t) \\ &\leq w_H(\mathbf{z}^2 - \mathbf{z}^1). \end{aligned}$$

Since both $\mathbf{z}^1, \mathbf{z}^2 \in \rho$, we have $D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2) \leq w_H(\mathbf{z}^2 - \mathbf{z}^1) \leq 2z$, which contradicts the fact that $d_{\min,t} \geq 2z + 1$.

$3 \Rightarrow 1$. Assume that any erasure pattern ρ with $|\rho| \leq 2z$ can be corrected at t, but $d_{\min,t} \leq 2z$. Take any $\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2 \in \mathbb{F}_q^{r_{\mathcal{S}_t}}, \mathbf{x}_{\mathcal{S}_t}^1 \neq \mathbf{x}_{\mathcal{S}_t}^2$ such that $W_t^{msg}((\mathbf{x}_{\mathcal{S}_t}^1 - \mathbf{x}_{\mathcal{S}_t}^2)A_{\mathcal{S}_t} F_t) = D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}^1, \mathbf{x}_{\mathcal{S}_t}^2) \leq 2z$. Therefore, by definition of $W_t^{msg}(.)$ there exist error vectors $\mathbf{z}$ and $\mathbf{x}_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$ such that

$$(\mathbf{x}_{\mathcal{S}_t}^1 - \mathbf{x}_{\mathcal{S}_t}^2)A_{\mathcal{S}_t} F_t = \mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z} F_t \qquad (20)$$

with $w_H(\mathbf{z}) \leq 2z$. Hence, we can choose error vectors $\mathbf{z}^1, \mathbf{z}^2 \in \rho$ such that $\mathbf{z} = \mathbf{z}^2 - \mathbf{z}^1$. Also, by linearity of the code, we can find $\mathbf{x}_{\overline{\mathcal{S}}_t}^1, \mathbf{x}_{\overline{\mathcal{S}}_t}^2 \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$ such that $\mathbf{x}_{\overline{\mathcal{S}}_t} = \mathbf{x}_{\overline{\mathcal{S}}_t}^2 - \mathbf{x}_{\overline{\mathcal{S}}_t}^1$. Therefore, if $\mathbf{y}_t$ is received at t, by (20) we have two indistinguishable possibilities

$$\begin{aligned} \mathbf{y}_t &= \mathbf{x}_{\mathcal{S}_t}^1 A_{\mathcal{S}_t} F_t + \mathbf{x}_{\overline{\mathcal{S}}_t}^1 A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z}^1 F_t \\ \mathbf{y}_t &= \mathbf{x}_{\mathcal{S}_t}^2 A_{\mathcal{S}_t} F_t + \mathbf{x}_{\overline{\mathcal{S}}_t}^2 A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z}^2 F_t. \end{aligned}$$

Hence, $3 \Rightarrow 1$ follows. ∎

Now we use Theorem 4 to prove Theorem 3:

Proof: The network code $\tilde{\mathcal{C}}$ is obtained by applying a random linear pre-code at each source S_i. That is, the length-$(r_i - 2z)$ vector of source symbols $\tilde{\mathbf{x}}_i$ is multiplied by R_i, an $(r_i - 2z) \times r_i$ matrix with entries chosen uniformly at random from $\mathbb{F}_q$, to form the input

$$\mathbf{x}_i = \tilde{\mathbf{x}}_i R_i \qquad (21)$$

to the original code. Let $\tilde{r}_{\mathcal{S}'} = \sum_{i \in \mathcal{S}'}(r_i - 2z) = r_{\mathcal{S}'} - 2|\mathcal{S}'|z$.

Consider any sink t. For any $\mathbf{x} \in \mathbb{F}_q^{\tilde{r}_{\mathcal{S}}}$, under the original code $\mathcal{C}$, in the absence of any errors or erasures, sink t receives

$$\mathbf{y}_t = \mathbf{x}M, \qquad (22)$$

where $M = A_{\mathcal{S}} F_t$, and applies a decoding matrix B to obtain its demanded source symbols $\mathbf{x}MB = \mathbf{x}_{\mathcal{S}_t}$.

Consider any network erasure pattern ρ with $|\rho| = 2z$, and any $\mathbf{z} \in \rho$. Let $\mathbf{s}$ be the length-$2z$ vector of nonzero symbols in $\mathbf{z}$, and let Q be the $2z \times |In_t|$ network transfer matrix from the symbols in $\mathbf{s}$ to the symbols on the sink's incoming links In_t. The vector received at t is

$$\mathbf{y}' = \mathbf{x}M + \mathbf{s}Q.$$

Sink t applies its original decoding matrix B to obtain

$$\mathbf{y}'B = \mathbf{x}MB + \mathbf{s}QB = \mathbf{x}_{\mathcal{S}_t} + \mathbf{s}QB. \qquad (23)$$

Let $a \leq 2z$ be the rank of QB, and let P be a submatrix of QB consisting of a linearly independent rows. Then $\mathbf{s}QB$ can be represented by $\mathbf{s}GP$, where $G \in \mathbb{F}_q^{2z \times a}$. Hence, (23) can be rewritten as

$$\mathbf{y}'B = \begin{pmatrix} \tilde{\mathbf{x}}_{\mathcal{S}_t} & \mathbf{s}' \end{pmatrix} \begin{pmatrix} R \\ P \end{pmatrix} \qquad (24)$$

where $\mathbf{s}'$ is a length-a vector of unknowns, and from (21), $R \in \mathbb{F}_q^{\tilde{r}_{\mathcal{S}_t} \times r_{\mathcal{S}_t}}$ is a block diagonal matrix with blocks $R_i, i \in \mathcal{S}_t$. Since each R_i has $2z$ fewer rows than columns and has all entries chosen uniformly at random from $\mathbb{F}_q$, the rows of R are linearly independent of the $a \leq 2z$ rows of P. Thus, $\begin{pmatrix} R \\ P \end{pmatrix}$ has full row rank and (24) can be solved for $\tilde{\mathbf{x}}_{\mathcal{S}_t}$.

Therefore, we can construct code $\tilde{\mathcal{C}}$ that achieves rate vector $\mathbf{r}_{2z} = (r_1 - 2z, r_2 - 2z, \ldots, r_n - 2z)$ under any network erasure pattern ρ with $|\rho| \leq 2z$. Now Theorem 4 implies that $\tilde{\mathcal{C}}$ has minimum distance $d_{min} \geq 2z + 1$ and that $\tilde{\mathcal{C}}$ can correct arbitrary errors on up to z links in the network. ∎

VI. CONCLUSIONS

We have derived network error correction capacity regions for multiple source multicast networks for both the coherent and the non-coherent case. For the non-multicast case where characterizing the capacity region is in general an open problem, we provided a technique for constructing a network error correction code for arbitrary errors in the network by using a given error-free network code as a starting point.

REFERENCES

[1] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 19–36, 2006.
[2] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54 (8), pp. 3579–3591, Aug. 2008.
[3] D.Silva and F.Kschischang, "Using rank-metric codes for error correction in random network coding," in *IEEE ISIT*, Jun. 2007.
[4] M. Siavoshani, C. Fragouli, and S. Diggavi, "Noncoherent multisource network coding," in *IEEE ISIT*, Jul. 2008.
[5] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *IEEE Transactions on Information Theory*, vol. 52, pp. 789–804, 2006.
[6] S. Yang and R. W. Yeung, "Characterizations of network error correction/detection and erasure correction," in *NetCod 2007*, Jan 2007.
[7] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient network coding in the presence of byzantine adversaries," in *Proc. IEEE INFOCOM 2007*, Anchorage, AK, May 2007.
[8] S. Vyetrenko, T. Ho, and E. Erez, "On noncoherent error and erasure correction," in *IEEE ISIT*, Jun. 2009.