On Noncoherent Correction of Network Errors and Erasures with Random Locations

Svitlana Vyetrenko
California Institute of Technology
Pasadena, CA 91125, USA
Email: svitlana@caltech.edu

Tracey Ho
California Institute of Technology
Pasadena, CA 91125, USA
Email: tho@caltech.edu

Elona Erez
Yale University
New Haven, CT 06511, USA
Email: elona.erez@yale.edu

Abstract—**We consider the problem of correcting errors and erasures with network coding. Unlike existing works which consider performance limits for worst-case locations of given numbers of errors and erasures, we consider the performance of given (not necessarily optimal) coding and forwarding strategies for given (not necessarily worst-case) models of error and erasure locations. Our approach characterizes decoding success in terms of the rank of certain matrices corresponding to useful and erroneous information received at the sink nodes. We use this approach to analyze random coding and forwarding strategies on a family of simple networks with random error and erasure locations, and show that the relative performance of the strategies depends on the erasure and error probabilities.**

I. Introduction

Most existing results on multicast network error correction apply to worst-case error and erasure locations, e.g. [2], [9], for which random linear network coding achieves capacity. On the other hand we may consider non-worst-case scenarios where links may fail randomly, or an adversary may only succeed probabilistically in attempts to compromise network nodes. In this paper we investigate the performance of linear coding and routing strategies in networks with non-worst-case error/erasure locations. In this case random linear coding at every node is not always optimal, since it improves erasure resilience at the expense of error propagation.

We consider decentralized strategies, which we analyze by bringing topology considerations into the non-coherent subspace coding framework of [6]. For a given realization of error and erasure locations, successful decoding can be characterized in terms of the rank of certain matrices that correspond to useful and erroneous information received at the sink node. We analytically derive the probability of successful decoding for random coding and routing strategies on a family of simple network subgraphs consisting of multiple multihop paths with random error and erasure locations, and show how the relative performance of these strategies depends on the information rate, minimum cut capacity, and the error and erasure probabilities. Simulation experiments on randomly generated hypergraphs representing wireless networks show similar trends.

II. Noncoherent coding for errors and erasures

We first develop the analytical framework we need by extending the noncoherent network coding framework in [6]. We consider single-source multicast over an acyclic network $\mathcal{G} = (\mathcal{N}, \mathcal{L})$ with source $\mathcal{S}$ and a set of sink nodes $\mathcal{T}$. A link $l \in \mathcal{L}$ may be subject to an erasure, in which case no packet is received on l, or an error, in which case a packet of arbitrary value is received on l.

Following [6], we consider constant-dimension noncoherent network coding, defined as follows. 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 R. To transmit codeword $U \in \mathcal{C}$, the source transmits a set of packets whose corresponding vectors span U. The sink receives the subspace $U' = \mathcal{H}_k(U) \oplus E$, where $\mathcal{H}_k$ projects U onto a k-dimensional subspace of U, and E is the subspace spanned by the error packets. Let $t = \dim(E)$, and let $\rho = (R-k)_+$. In [6], t and ρ are referred to as the number of errors and erasures respectively. The concept of subspace errors and erasures is distinct from that of network errors and erasures. As will be seen later, the network topology and coding strategy determine what subspace errors and erasures result from given network errors and erasures. Thus, to avoid confusion, we refer to t as the number of additions, and ρ as the number of deletions. The distance between two spaces U_1, U_2 is defined as

$$d(U_1, U_2) \doteq \dim(U_1 + U_2) - \dim(U_1 \cap U_2). \qquad (1)$$

It is shown in [6] that d is a metric for $\mathcal{P}(V)$. Subspace minimum distance decoding is successful if and only if there is no codeword $\tilde{U} \neq U$ in $\mathcal{C}$ for which $d(\tilde{U}, U') \leq d(U, U')$.

Let $\Delta \doteq \underset{U_1,U_2 \in \mathcal{C}: U_1 \neq U_2}{min} d(U_1, U_2)$ be the minimum distance of $\mathcal{C}$. In [6] the following result is shown:

Theorem 1. *The transmitted subspace $U \in \mathcal{C}$ can be successfully recovered from the received subspace U' if*

$$2(t + \rho) < \Delta. \qquad (2)$$

Let r denote the code rate of $\mathcal{C}$. Theorem 2 gives a converse to this result for $r > (R - \Delta/2)/R$ and any $\mathcal{H}_k$. Concurrent independent work [8][1] gives a converse pertaining to the

[1] We thank an anonymous referee for pointing us to this work.

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

case where $\mathcal{H}_k$ is adversarially chosen subject to a minimum rank constraint. However, in our problem $\mathcal{H}_k$ depends on the coding/routing strategy employed.

Lemma 1. *Let $\mathcal{C}$ have minimum distance Δ. If $2t \geq \Delta$, then decoding is unsuccessful for some value of the transmitted subspace and the error packets.*

Proof: Consider $U, \tilde{U} \in \mathcal{C}$ such that $d(U, \tilde{U}) = \Delta$. If U is sent and E is chosen as a subspace of $\tilde{U} \cap U^c$, then $d(\tilde{U}, U') \leq d(U, U')$ for received subspace $U' = U \oplus E$. ■

Note that for constant dimension codes, Δ is even and that for given R and Δ, we have $r \leq (R - \Delta/2 + 1)/R$.

Theorem 2. *Let $\mathcal{C}$ have dimension R, minimum distance Δ and code rate $r > (R - \Delta/2)/R$. If $2(t + \rho) \geq \Delta$, then decoding is unsuccessful for some value of the transmitted subspace and the error packets.*

Proof: We only need to consider the case of $2(t+\rho) = \Delta$ by the information processing inequality. The sink receives the subspace $\mathcal{H}_k(U) \oplus E$ with $t = \dim(E)$ and $\rho = (R - k)_+$ such that $2(t+\rho) = \Delta$. Suppose that instead of adding E, we subject $\mathcal{H}_k(U)$ to a further t deletions resulting in the subspace $\mathcal{H}_{k'}(\mathcal{H}_k(U))$, where $k' = k - t$. Since there are altogether $\Delta/2$ deletions and $r > (R - \Delta/2)/R$, the mincut bound is violated [3], so for some $U \in \mathcal{C}$ there exists some $\tilde{U} \neq U$ in $\mathcal{C}$ such that $d(\tilde{U}, \mathcal{H}_{k'}(\mathcal{H}_k(U))) \leq d(U, \mathcal{H}_{k'}(\mathcal{H}_k(U)))$, which implies $\mathcal{H}_{k'}(\mathcal{H}_k(U))$ is also a subspace of $\tilde{U}$. Then $\tilde{U} + \mathcal{H}_k(U)$ has dimension at most $R + t$. If E is chosen as a subspace of $\tilde{U} \cap U^c$, then

$$\begin{aligned}
&d(\tilde{U}, \mathcal{H}_k(U) \oplus E) \\
&= \dim(\tilde{U} + (\mathcal{H}_k(U) \oplus E)) - \dim(\tilde{U} \cap (\mathcal{H}_k(U) \oplus E)) \\
&\leq \dim(\tilde{U} + \mathcal{H}_k(U)) - \dim(\mathcal{H}_{k'}(\mathcal{H}_k(U)) \oplus E) \\
&\leq R + t - (k' + t) = R - k'; \\
&d(U, \mathcal{H}_k(U) \oplus E) \\
&= \dim(U + (\mathcal{H}_k(U) \oplus E)) - \dim(U \cap (\mathcal{H}_k(U) \oplus E)) \\
&= \dim(U \oplus E) - \dim(\mathcal{H}_k(U)) = R + t - k = R - k'.
\end{aligned}$$

Thus, decoding is unsuccessful. ■

Lemma 2. *For any given set of adversarial links and any given network code, putting a linearly independent adversarial error on each adversarial link results in the lowest probability of successful decoding.*

Lemma 2 implies that we can henceforth consider the case where each adversarial link is associated with a linearly independent error.

Let $\mathbb{F}_q^{m \times n}$ denote the set of all $m \times n$ matrices over finite field $\mathbb{F}_q$. Let $\mathcal{C}$ be a subspace code with codeword dimension R, minimum distance Δ and code rate greater than $(R - \Delta/2)/R$. Let matrix $W \in \mathbb{F}_q^{R \times K}$ represent the transmitted codeword. Let ν be the number of incoming links of a sink $t \in \mathcal{T}$. Let $Q \in \mathbb{F}_q^{\nu \times R}$ be the network transfer matrix from the source packets to the packets received at t [5].

Let L denote the number of links in $\mathcal{G}$. An error on a link is modeled as addition of an arbitrary error packet to the packet being transmitted at that link. Let $Z \in \mathbb{F}_q^{L \times K}$ denote the error matrix whose ith row corresponds to the error packet that is injected on the ith link of $\mathcal{G}$. Let $B \in \mathbb{F}_q^{\nu \times L}$ be the transfer matrix from the error packets to the packets received at t.

Let $Y \in \mathbb{F}_q^{\nu \times K}$ be the matrix whose rows correspond to the packets received at t. Then

$$Y = QW + BZ \tag{3}$$

and the decodability condition given in Theorems 1 and 2 can be translated to our setting as follows:

Theorem 3. *For a given $\mathcal{C}$, let $y = \frac{\Delta}{2}$. Let the transmitted matrix W and the error matrix Z have linearly independent rows. Then decoding at $t \in \mathcal{T}$ is guaranteed to succeed iff*

$$R - \mathit{rank}(QW + BZ) + 2\mathit{rank}(BZ) < y. \tag{4}$$

III. Single path subgraph

We apply results in Sec. II to study error and erasure performance of coding and routing strategies on networks with randomly located errors and erasures. We analyze the probability that the error and erasure locations are such that not all error values can be corrected.

We first consider a simple building block network consisting of a simple multihop path with source $\mathcal{S}$ and sink $\mathcal{T}$(see Fig. 1(a)). Let the network consist of M hops. Let R, $\mathcal{C}$, Δ, y, W, L and Z be defined as in the previous section. Let C be the number of parallel links on each hop of $\mathcal{G}_M$. Let $S \in \mathbb{F}_q^{C \times R}$ be the source coding matrix and let $A \in \mathbb{F}_q^{C \times C}$ be the transfer matrix from all links in the network to the packets received at $\mathcal{T}$. Let $B \in \mathbb{F}_q^{C \times L}$ be the transfer matrix from error packets to the packets received at $\mathcal{T}$. According to (3), we can write

$$Y = ASW + BZ. \tag{5}$$

Enumerate all nodes of $\mathcal{G}_M$ with node 0 corresponding to $\mathcal{S}$ and node M corresponding to $\mathcal{T}$. Assume that the jth hop refers to the transmission from the $(j-1)$th to the jth node.

Consider the jth hop of the single path multihop network. In our model three mutually exclusive events can occur at the jth hop for any j: an erasure can occur on exactly one of the C links with probability p; an error can occur on exactly one of the C links with probability s; no errors and erasures occur at the jth hop with probability $(1 - p - s)$. When an error or erasure occurs, any one of the C links has probability $\frac{1}{C}$ of being the affected link.

To solve the problem we are going to adopt the algebraic coding model given in (3). Choosing different network coding strategies at the non-source nodes corresponds to modifying A (and, consequently, B) in (3). In this paper we compare performance of random linear coding at the source paired with two different strategies at non-source nodes:

1) **Forwarding with random replication (FRR)**
   - Each node forwards all received packets to the outgoing links.
   - In case of a link erasure, the node replaces the erased packet with a copy of any one of the successfully received packets.
2) **Random linear coding (RLC)**

- Each node creates random linear combinations of all received packets and sends them to the outgoing links.
- In case of a link erasure, the node replaces the erased packet by creating a random linear combination of the successfully received packets.

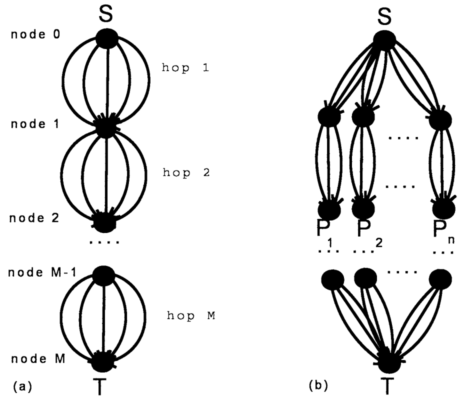

Fig. 1. Schematic depiction of: (a) single path subgraph; (b) multiple path subgraph

Let I be the $C \times C$ identity matrix. Define $A_j \in \mathbb{F}_q^{C\times C}$ as a random matrix with entries from $\mathbb{F}_q$ for RLC, and as $A_j \doteq I$ for FRR. If no erasure occurs, define $E_j \in \mathbb{F}_q^{C\times C}$ as $E_j \doteq I$. If an erasure occurs on link i, define $E_j \in \mathbb{F}_q^{C\times C}$ as I with the ith row equal to the unit vector with 1 in the kth position if link k was replicated for FRR, and I with the ith row equal to the zero vector for RLC. If no error occurs, define $D_j \in \mathbb{F}_q^{C\times C}$ as $D_j \doteq I$. If an error occurs on the ith link, define $D_j \in \mathbb{F}_q^{C\times C}$ as I with the ith row equal to the zero vector. Define $D_j^* \in \mathbb{F}_q^{C\times C}$ as $D_j^* \doteq I - D_j$.

Define

$$F_j = \begin{cases} D_j & \text{if an error occurs at the } j\text{th hop,} \\ E_j & \text{if an erasure occurs at the } j\text{th hop,} \\ I & \text{if neither error, nor erasure occur at the } j\text{th hop.} \end{cases}$$

Therefore, for both coding strategies we rewrite A and B in (5) as

$$\begin{aligned} A &= F_M A_M F_{M-1} A_{M-1} \dots F_2 A_2 F_1 A_1 \\ B &= \begin{pmatrix} F_M A_M .. F_2 A_2 D_1^* & F_M A_M .. F_3 A_3 D_2^* & .. & D_M^* \end{pmatrix} \end{aligned}$$

A. Random linear coding

Let $\mathcal{P}$ denote the probability of successful decoding. Let A and D be the random variables representing the number of dimension additions/deletions to/from $rowspace(W)$ in $\mathcal{G}_M$ respectively. Then according to Theorems 1 and 2, $\mathcal{P}$ can be computed as

$$\mathcal{P} = \text{Prob}\left(\mathsf{A} + \mathsf{D} \leq y - 1\right). \tag{6}$$

Let Y^j denote the subspace spanned by received packets at the jth node of $\mathcal{G}_M$. Let a_j and d_j be the number of dimension additions/deletions to/from $rowspace(W)$ present in Y^j respectively. Let us say that the jth node of $\mathcal{G}_M$ is in state i if, after random linear coding is performed at the jth node, we have $a_j + d_j = i$. Let $P_{i,k}^j$ denote the probability that given that the $(j-1)$th node of $\mathcal{G}_M$ is in state i, the jth node of $\mathcal{G}_M$ will be in state k after the data transmission from the $(j-1)$th to the jth hop.

Lemma 3. *When RLC is performed at every node of $\mathcal{G}_M$, for every node $j = 1, \dots, M$ we have:*

if $0 \leq i < C - R$
$P_{i,i}^j = 1 - s, P_{i,i+1}^j = s, P_{i,k}^j = 0$ *for* $k \neq i, i+1$
if $i = C - R + 2m, m = 0, \dots, R-1$
$P_{i,i}^j = 1 - p - s, P_{i,i+1}^j = p, P_{i,i+2}^j = s, P_{i,k}^j = 0$ *for* $k \neq i, i+1, i+2$
if $i = C - R + 2m + 1, m = 0, \dots, R-1$
$P_{i,i}^j = 1 - s, P_{i,i+1}^j = s, P_{i,k}^j = 0$ *for* $k \neq i, i+1$
if $i = C + R$
$P_{i,i-1}^j = p, P_{i,i}^j = 1 - p, P_{i,k}^j = 0$ *for* $k \neq i-1, i$

Lemma 3 implies that when RLC is performed, the system can be modeled as a Markov chain, that has a probability transition matrix with entries P_{ik}^j for $i, k = 0 \dots C + R$. Moreover, $\mathcal{P}$ can be computed using the distribution of this Markov chain after M transitions.

B. Forwarding with random replication

Lemma 4. *In case of FRR with RLC performed at S we have*
$$rank(ASW + BZ) = rank(ASW) + rank(BZ)$$
$$rank(ASW) = min(R, rank(A))$$
$$rank(BZ) = rank(F_M \dots F_2 D_1^* Z_1) + \dots + rank(D_M^* Z_M).$$

Using Theorem 3 and Lemma 4, $\mathcal{P}$ can be computed as:

$$\begin{aligned} \mathcal{P} &= \text{Prob}\left(R - \text{rank}(ASW + BZ) + 2\text{rank}(BZ) \leq y - 1\right) \qquad (7) \\ &= \sum_{f,l,z \in \mathcal{I}} \text{Prob}\left(\text{rank}(ASW) = l - z, \text{rank}(BZ) = z, \text{rank}(A) = f\right) \\ &= \sum_{f,l,z \in \mathcal{I}} \text{Prob}\left(\text{rank}(BZ) = z | \text{rank}(A) = f\right) \text{Prob}\left(\text{rank}(A) = f\right), \end{aligned}$$

$$\mathcal{I} = \{f, z, l : 0 \leq f \leq C, 0 \leq z \leq y-1, R+2z-(y-1) \leq l \leq C\}.$$

Now we can compute (7) by deriving explicit expressions for probability distributions $\text{Prob}\left(\text{rank}(BZ) = z | \text{rank}(A) = f\right)$ and $\text{Prob}\left(\text{rank}(A) = f\right)$. Lemmas 5,6 and 7 provide auxiliary results that our further derivation relies on.

Lemma 5. *If D_1 is the identity matrix with a randomly chosen row substituted by a zero row, then*

$$Prob\left(rank(F_j \dots F_2 D_1) = f | rank(F_j \dots F_2) = f + 1\right) = \frac{f+1}{C}.$$

Lemma 6. *If D_1 is the identity matrix with a randomly chosen row substituted by a zero row, then*

$$\begin{aligned} rank(F_j \dots F_2) &= f, rank(F_j \dots F_2 D_1) = f \Rightarrow rank(F_j \dots F_2 D_1^*) = 0 \\ rank(F_j \dots F_2) &= f + 1, rank(F_j \dots F_2 D_1) = f \Rightarrow rank(F_j \dots F_2 D_1^*) = 1 \end{aligned}$$

Lemma 7. *If E_1 is the identity matrix with a randomly chosen row substituted by a zero row, then*

$$Prob\left(rank(F_j \dots F_2 E_1) = f | \, rank(F_j \dots F_2) = f + 1\right) = \frac{f(f+1)}{C(C-1)}.$$

1) Derivation of $Prob\,(rank(A) = f)$: Denote $\text{Prob}\,(\text{rank}(F_jF_{j-1}\dots F_2F_1) = f)$ by $\phi_j(f)$. Let N_j be the number of error/erasure occurrences out of j hops. If $N_j = l$, suppose that all errors and/or erasures occurred on $i_1, i_2 \dots i_l$th hops. Compute $\phi_j(f)$ by conditioning on N_j:

$$\begin{aligned}
\phi_j(f) &= \sum_{l=C-f}^{j} \text{Prob}\,(\text{rank}(E_{i_l}\dots E_{i_1}) = f)\,\frac{j!}{l!(j-l)!}p^l(1-p-s)^{j-l} \\
&+ \sum_{l=C-f}^{j}\sum_{m=1}^{l} \text{Prob}\,(\text{rank}(F_{i_l}\dots F_{i_1}) = f,\ \text{errors on } m \text{ hops}) \\
&\times \frac{j!}{(l-m)!m!(j-l)!}p^{l-m}s^m(1-p-s)^{j-l},
\end{aligned}$$

where the first term corresponds to the case when only erasures occurred on all hops i_g, $g = 1\dots l$ and the second term corresponds to the case when both errors and erasures occurred on all hops i_g, $g = 1\dots l$.

Denote $\text{Prob}\,(\text{rank}(E_{i_l}\dots E_{i_2}E_{i_1}) = f)$ by $h_l(f)$. We can compute $h_l(f)$ by conditioning on $\text{rank}(E_{i_l}\dots E_{i_2})$ and Lemma 7. For $l \geq 2$

$$h_l(f) = \left(1 - \frac{f(f-1)}{C(C-1)}\right)h_{l-1}(f) + \frac{f(f+1)}{C(C-1)}h_{l-1}(f+1)$$

with the base case

$$h_1(f) = \begin{cases} 1, & f = C-1; \\ 0, & \text{otherwise.} \end{cases}$$

Denote $\text{Prob}\,\left(\text{rank}(F_{i_l}F_{i_{l-1}}\dots F_{i_2}F_{i_1}) = f,\ \text{errors on } m \text{ hops}\right)$ by $g_l(f,m)$. We can compute $g_l(f,m)$ by conditioning on F_{i_1}, $\text{rank}(F_{i_l}F_{i_{l-1}}\dots F_{i_2})$ and Lemmas 5 and 7. For $m \geq 2$

$$\begin{aligned}
g_l(f,m) &= \left(\frac{C-f}{C}g_{l-1}(f,m-1) + \frac{f+1}{C}g_{l-1}(f+1,m-1)\right)\frac{m}{l} \\
&+ \left((1-\frac{f(f-1)}{C(C-1)})g_{l-1}(f,m) + \frac{f(f+1)}{C(C-1)}g_{l-1}(f+1,m)\right)\frac{l-m}{l}
\end{aligned}$$

and for $m = 1$

$$\begin{aligned}
g_l(f,1) &= \left(\frac{C-f}{C}h_{l-1}(f) + \frac{f+1}{C}h_{l-1}(f+1)\right)\frac{1}{l} \\
&+ \left((1-\frac{f(f-1)}{C(C-1)})g_{l-1}(f,1) + \frac{f(f+1)}{C(C-1)}g_{l-1}(f+1,1)\right)\frac{l-1}{l}
\end{aligned}$$

with the base case

$$g_1(f,1) = \begin{cases} 1, & f = C-1; \\ 0, & \text{otherwise.} \end{cases}$$

2) Derivation of $Prob\,(rank(BZ) = z|\,rank(A) = f)$: Denote $F_M\dots F_{M-j+2}D^*_{M-j+1}Z_{M-j+1} + \dots + F_MD^*_{M-1}Z_{M-1} + D^*_MZ_M$ by B^jZ^j and $F_M\dots F_{M-j+2}F_{M-j+1}$ by A^j. Let $\psi_j(f,z) = \text{Prob}\,\left(\text{rank}(B^jZ^j) = z|\text{rank}(A^j) = f\right)$. We can compute $\psi_j(f,z)$ by conditioning on F_{M-j+1}, $\text{rank}(A^{j+1})$ and using Lemmas 5,6 and 7.

$$\begin{aligned}
&\psi_j(f,z) \\
= \ &\text{Prob}(\text{rank}(B^jZ^j) = z|F_{M-j+1} = D_{M-j+1}, \text{rank}(A^j) = f) \\
\times \ &\text{Prob}(F_{M-j+1} = D_{M-j+1}|\text{rank}(A^j) = f) \\
+ \ &\text{Prob}(\text{rank}(B^jZ^j) = z|F_{M-j+1} = E_{M-j+1}, \text{rank}(A^j) = f) \\
\times \ &\text{Prob}(F_{M-j+1} = E_{M-j+1}|\text{rank}(A^j) = f) \\
+ \ &\text{Prob}(\text{rank}(B^jZ^j) = z|F_{M-j+1} = I, \text{rank}(A^j) = f) \\
\times \ &\text{Prob}(F_{M-j+1} = I|\text{rank}(A^j) = f) \qquad (8)
\end{aligned}$$

with $\psi_1(f,z) = 0$ for any $f \leq C-2$,

$$\psi_1(C,z) = \begin{cases} 1, & z = 0; \\ 0, & \text{otherwise;} \end{cases}$$

$$\psi_1(C-1,z) = \begin{cases} \frac{p}{p+s}, & z = 0; \\ \frac{s}{p+s}, & z = 1; \\ 0, & \text{otherwise.} \end{cases}$$

$$\begin{aligned}
1.\quad &\text{Prob}(\text{rank}(B^jZ^j) = z|F_{M-j+1} = D_{M-j+1}, \text{rank}(A^j) = f) \\
= \quad &\psi_{j-1}(f,z)b_1 + \psi_{j-1}(f+1,z-1)b_2, \\
2.\quad &\text{Prob}(F_{M-j+1} = D_{M-j+1}|\text{rank}(A^j) = f) \\
= \quad &\frac{q\left(\frac{f+1}{C}\phi_{j-1}(f+1) + \frac{f}{C}\phi_{j-1}(f)\right)}{\phi_j(f)}, \\
3.\quad &\text{Prob}(\text{rank}(B^jZ^j) = z|F_{M-j+1} = E_{M-j+1}, \text{rank}(A^j) = f) \\
= \quad &\psi_{j-1}(f,z)b'_1 + \psi_{j-1}(f+1,z)b'_2, \\
4.\quad &\text{Prob}(F_{M-j+1} = E_{M-j+1}|\text{rank}(A^j) = f) \\
= \quad &\frac{p\left(\frac{f(f+1)}{C(C-1)}\phi_{j-1}(f+1) + \left(1 - \frac{f(f-1)}{C(C-1)}\right)\phi_{j-1}(f)\right)}{\phi_j(f)}, \\
5.\quad &\text{Prob}(\text{rank}(B^jZ^j) = z|F_{M-j+1} = I, \text{rank}(A^j) = f) = \psi_{j-1}(f,z), \\
6.\quad &\text{Prob}(F_{M-j+1} = I|\text{rank}(A^j) = f) = \frac{(1-p-q)\phi_{j-1}(f)}{\phi_j(f)},
\end{aligned}$$

where b_1, b_2, b'_1, b'_2 can be computed as:

$$\begin{aligned}
b_1 &= \frac{\frac{C-f}{C}\phi_{j-1}(f)}{\frac{C-f}{C}\phi_{j-1}(f) + \frac{f+1}{C}\phi_{j-1}(f+1)}, \\
b_2 &= \frac{\frac{f+1}{C}\phi_{j-1}(f+1)}{\frac{C-f}{C}\phi_{j-1}(f) + \frac{f+1}{C}\phi_{j-1}(f+1)}, \\
b'_1 &= \frac{\left(1 - \frac{f(f-1)}{C(C-1)}\right)\phi_{j-1}(f)}{\left(1 - \frac{f(f-1)}{C(C-1)}\right)\phi_{j-1}(f) + \frac{f(f+1)}{C(C-1)}\phi_{j-1}(f+1)}, \\
b'_2 &= \frac{\frac{f(f+1)}{C(C-1)}\phi_{j-1}(f+1)}{\left(1 - \frac{f(f-1)}{C(C-1)}\right)\phi_{j-1}(f) + \frac{f(f+1)}{C(C-1)}\phi_{j-1}(f+1)}.
\end{aligned}$$

IV. Multiple path subgraph

Consider a multiple path subgraph $\mathcal{G}_n$ (see Fig. 1(b)) with source $\mathcal{S}$ and sink $\mathcal{T}$. Let $\mathcal{P} = \{P_1, P_2 \dots P_n\}$ be the set of edge-disjoint paths from $\mathcal{S}$ to $\mathcal{T}$. Let M_i be the number of hops on each path P_i. Let C_i be the number of parallel links on each hop of P_i. Let $C = \sum_{i=1}^n C_i$. For the case of multiple path subgraph, assume that $R \geq max_{1\leq i\leq n}C_i$. Let $R_i \leq C_i$ be the rank of information packets that are transmitted on each P_i. We assume that $\sum_{i=1}^n R_i \geq R$.

Let $A^i \in \mathbb{F}_q^{C_i\times C_i}$ and $B^i \in \mathbb{F}_q^{C_i\times C_iM_i}$ be the linear transformations applied by the network on each P_i to information and error packets respectively. For the multiple path network model that we defined, matrices A and B have the block-diagonal structure with A^i and B^i on the main diagonal.

Lemma 8. *For any given set of error and erasure locations and any given network code, the probability of successful decoding for $\mathcal{G}_n$ is maximized when R_i is chosen to be equal to C_i on each P_i.*

By Lemma 8 it is sufficient to consider $R_i = C_i$ for each P_i since it results in the highest probability of successful decoding.

A. Random linear coding

Let A and D be random variables representing the number of dimension additions/deletions to/from rowspace(W) in $\mathcal{G}_n$ respectively. Let A_i and D_i be random variables, that stand for the number of dimension additions/deletions to/from $rowspace(W)$ on each P_i respectively. Let a, d, a_i and d_i be the values that A, D, A_i and D_i can take.

Lemma 9. *If RLC is performed on all paths of $\mathcal{G}_n$ and $R_i = C_i\ \forall i$, we have $a = \sum_{i=1}^{n} a_i$ and $d = max(\sum_{i=1}^{n} d_i - (C-R), 0)$.*

Now we can rewrite (6) as:

$$\begin{aligned}\mathcal{P} &= \text{Prob}\left(\mathsf{A}+\mathsf{D} \le y-1\right)\\ &= \sum_{\substack{a_i,\, d_i\, :\\ \sum a_i + \max(\sum d_i - (C-R),0) \le y-1,\\ d_i = a_i \text{ or } d_i = a_i+1}} \prod_{j=1}^{n} \text{Prob}\left(P_j \text{ in state } a_j + d_j \text{ after } M_j \text{ hops}\right),\end{aligned}$$

where the last equality follows from Lemmas 3,9 and the independence between $\mathsf{A}_i, \mathsf{D}_i$ and $\mathsf{A}_j, \mathsf{D}_j$ for $i \neq j$. We can then use the derivation for a single path subgraph to evaluate Prob $(P_i$ in state $a_i + d_i$ after M_i hops) for each P_i.

B. Forwarding with random replication

Using the fact that the quantities rank(A^i) and rank(B^iZ^i) associated with each P_i are independent of the corresponding quantities for P_j for $i \neq j$, we can write $\mathcal{P}$ as:

$$\mathcal{P} = \sum_{f_i, z_i \in \mathcal{I}} \prod_{j=1}^{n} \text{Prob}\left(\text{rank}(B^jZ^j) = z_j, \text{rank}(A^j) = f_j\right),$$

where $\mathcal{I} = \{f_i, z_i : 0 \le f_i \le C_i, \sum f_i = f; 0 \le z_i \le y-1, \sum z_i = z; R + 2z - (y-1) \le \min(f,R) + z \le C\}$. We then apply the derivation for a single path case by setting $A = A^i$, $B = B^i$, $Z = Z^i$, $i = 1 \ldots n$.

V. Comparison

Fig. 2 shows the probabilities of successful decoding computed analytically for both strategies. Fig. 3 depicts average probability of successful decoding curves obtained by running 500 experiments over 20 randomly generated one-source one-sink hypergraphs with 20 nodes. In our experiment, we assumed that each non-source node could become adversarial with probability s and each hyperarc could fail with probability p. In both Fig. 2 and Fig. 3, all curves are sketched against p for a fixed s when RLC is done at the source. Note that both analytical and experimental results suggest that RLC is more beneficial than FRR when information is transmitted at a higher rate.

Acknowledgement

This material is partly funded by subcontract #069153 issued by BAE Systems National Security Solutions, Inc. and supported by the Defense Advanced Research Projects Agency (DARPA) and the Space and Naval Warfare System Center (SPAWARSYSCEN), San Diego under Contract No. N66001-08-C-2013, by AFOSR under Grant 5710001972, and by Caltech's Lee Center for Advanced Networking.

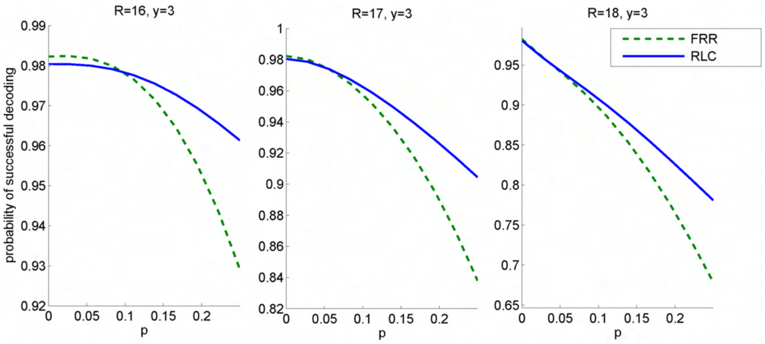

Fig. 2. $n = 4$, $M = 3$, $R_i = C_i = 5, i = 1 \ldots 4$, $s = 0.05$.

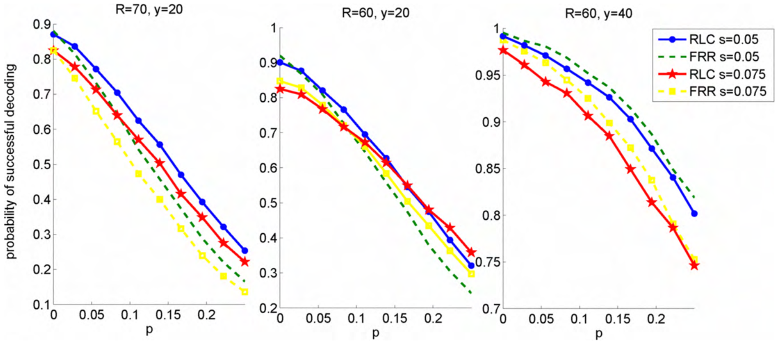

Fig. 3. Average over randomly generated hypergraphs with mincut capacity equal to 100.

References

[1] H. Balli, X. Yan, Z. Zhang, "Error correction capability of random network error correction codes", *IEEE ISIT 2007*.

[2] S.Jaggi, M.Langberg, S.Katti, T.Ho, D.Katabi, M.Medard, "Resilient network coding in the presence of Byzantine adversaries", *IEEE Trans. Inf. Theory, Special Issue on Inf. Theor. Security*, Vol. 54, No. 6, pp. 2596-2603, Jun. 2008.

[3] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, M. Effros, "Capacity of wireless erasure networks", *IEEE Trans. Inf. Theory*, vol. 52, pp. 789-804, 2006.

[4] T.Ho, M.Médard, R.Koetter, D.Karger, M.Effros, J.Shi, B.Leong, "A random linear network coding approach to multicast", *IEEE Trans. Inf. Theory*, vol. 52, pp. 4413-4430, Oct. 2006.

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

[6] R.Koetter, F.Kschischang, "Coding for the errors and erasures in random network coding", *IEEE Trans. Inf. Theory*, vol. 54, pp. 3579-3591, Aug. 2008.

[7] D.Silva, F.Kschischang, R.Koetter, "A rank-metric approach to error control in random network coding", *IEEE Trans. on Inf. Theory*, vol. 54, no. 9, pp. 3951-3967, 2008.

[8] D. Silva,F. R. Kschischang, "On Metrics for Error Correction in Network Coding," submitted to *IEEE Trans. Inform. Theory*, 2008.

[9] S.Yang, R.Yeung, "Refined coding bounds for network error correction", *IEEE ITW on Inf. Theory for Wireless Netw.*, Jul. 2007.

[10] Z.Zhang, "Linear error correction codes in packet networks", *IEEE Trans. Inf. Theory*, vol.54, pp.209-218, Jan. 2008.