New results on network error correction: capacities and upper bounds

Sukwon Kim, Tracey Ho, Michelle Effros
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA, 91125, USA
Email: {sukwon, tho, effros}@caltech.edu

Salman Avestimehr
Department of Electrical and Computer Engineering
Cornell University
Ithaca, NY, 14853, USA
Email: avestimehr@ece.cornell.edu

***Abstract*— In this paper, we present new results on network error correction with unequal link capacities. We consider network error correction codes that can correct arbitrary errors occurring on up to z links. We find the capacity of a two-node network with multiple feedback links and show how feedback links can be used to increase the error correction capacity. We propose a new cut-set upper bound for general acyclic networks, and show its tightness for a family of four-node acyclic networks when each backward link has enough capacity. For a more general family of zig-zag networks, we present conditions under which our upper bound is tight. Finally, we propose an approach for high-probability network error correction with a causal adversary.**

I. Introduction

Yeung and Cai introduced the network error-correction problem [1], [2] with unit link capacity. They generalized the Hamming bound, the Singleton bound, and the Gilbert-Varshamov bound from classical error correction coding to network coding. In [3], [4], classical notions of the Hamming weight, Hamming distance, minimum distance and various classical error control coding bounds were generalized with unit link capacity. In [5], [6], network error correction under probabilistic assumptions was studied. Network error correction for non-coherent network coding was developed in [7], [8]. In these previous works on network error correction, the authors assume unit link capacity.

Network error correction with unequal link capacities was studied in our previous work [9]. In the case with errors, there is a loss of generality in assuming that errors occur independently on the unit capacity edges. For any link l in the network with capacity r, r symbols can be transmitted on l. If an adversary controls this link, it can corrupt some or all of the symbols transmitted across the link. The capacity of a network consisting of parallel links with arbitrary capacities and a generalized Singleton upper bound for general networks were given in [9]. Also it was shown that linear coding is insufficient in general and that even for a single source and single sink network, it may be necessary for intermediate nodes to do linear coding or nonlinear operations. This is unlike the equal link capacity case, where coding only at the source and forwarding at intermediate nodes suffices for a single source and sink. The necessity of nonlinear network coding for the related problem of correcting adversarial node errors was independently and concurrently shown in [10], [11].

In this paper, we present the following new contributions.

- We find the capacity of a two-node network with multiple feedback links and show how feedback links can be used to increase the error correction capacity (Section III).
- We propose a new cut-set upper bound for general acyclic networks that tightens our previous bound (Section IV).
- We consider a four-node acyclic network as a simplified model of arbitrary acyclic network and show the tightness of our bound when each feedback link has enough capacity (Section V).
- We consider a more general family of zig-zag network and present a condition under which our bound is tight (Section VI).
- We propose an approach for high-probability network error correction with a causal adversary (Section VII).

II. Preliminaries

We consider communication network represented by a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Source node $s \in \mathcal{V}$ transmits information to the sink nodes $u \in \mathcal{U}$. We use $r(a,b)$ to denote the capacity of edge $(a,b) \in \mathcal{E}$. We assume that the code alphabet is equal to $GF(q)$ for some prime power q. We regard an error vector in each link $l \in \mathcal{E}$ as set of $r(l)$ symbols in $GF(q)$, where the output y_l of link l equals the modulo q sum of the input x_l to link l and the error e_l applied to link l. We say that there are τ error links in the network if $e_l \neq 0$ on τ links.

Definition 1: A network code is z-error link-correcting if it can correct any τ adversarial links for $\tau \leqslant z$. That is, if the total number of adversarial links in the network is at most z, then the source message can be recovered by all the sink nodes $u \in \mathcal{U}$.

Let (A, B) be a partition of $\mathcal{V}$, and define the cut for the partition (A, B) by

$$cut(A,B) = \{(a,b) \in \mathcal{E} : a \in A, b \in B\}.$$

$cut(A,B)$ is called a cut between two nodes a and b if $a \in A$ and $b \in B$. Let $CS(a,b)$ denote the set of cuts between a and b. The links in $cut(A,B)$ are called the forward links of the cut. The links (a,b) for which $a \in B$, $b \in A$ are called the

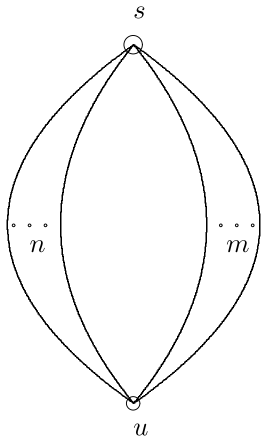

Fig. 1. Two-node network $\mathcal{G}$ with n forward links and m feedback links.

feedback links of the $cut(A, B)$. The capacity of a cut is the sum of the capacities of the forward links of the cut.

III. Two-node network with feedback links

A. Equal link capacities

In this section, we consider a two-node network $\mathcal{G}$ with n parallel unit capacity forward links and m feedback links with arbitrary capacities. We use C to denote the error-correction capacity in this two-node network with z adversarial links.

In following lemma, we show that information from feedback link can be used to increase the capacity.

Example 1: If $n = 3$ and $m = z = 1$, $C = 2$.

The strategy achieving rate 2 is as follows.

The source sends (a_i, b_i, a_i+b_i) in each time slot $i = 1, 2, ...$ on the three forward links. At each time step i, sink looks at its received symbol $(\tilde{a}_i, \tilde{b}_i, \tilde{c}_i)$. From any subset of two symbols, it gets a possible answer for a_i and b_i. If all three answers match, then this answer is correct and the adversary has not changed the symbols on forward links.

If for some i the answers are different, one of forward links is adversarial and feedback link is not. Then sink can send back $(\tilde{a}_i, \tilde{b}_i, \tilde{c}_i)$ to the source reliably. The source will identify the adversarial link and inform the sink using a repetition code on all three forward links. Since $n = 3 > 2 = 2z$, sink gets the location of adversarial link reliably. This happens only once, since from then on, the sink can just ignore adversarial link Therefore, we achieve rate 2 asymptotically.

Now we consider multiple feedback links and find the error-correction capacity in following lemma.

Lemma 1: If $n \leqslant 2z$, $C = 0$. Otherwise, $C = \min\{n - z, n - 2(z - m)\}$.

Proof: Case 1) $n \leqslant 2z$.

Suppose that all z adversarial links are among the forward links and $C > 0$. We show a contradiction. Since $C > 0$, there are two codewords $X = (x_1, .., x_n)$ and $Y = (y_1, .., y_n)$ that can be sent reliably. When X is sent along forward links and leftmost z links are adversarial, adversary changes X to $X' = (y_1, .., y_{\lfloor n/2 \rfloor}, x_{\lfloor n/2 \rfloor + 1}, .., x_n)$ so that first $\lfloor n/2 \rfloor$ bits of X' are the same as that of Y. Similarly, when Y is sent along forward links and rightmost z links are adversarial, adversary changes Y to $Y' = (y_1, .., y_{\lfloor n/2 \rfloor}, x_{\lfloor n/2 \rfloor + 1}, .., x_n)$ so that last $\lceil n/2 \rceil$ bits of Y' are the same as that of X. Then sink receives the same observations for the two codewords. Since information on feedback links is determined by what the sink receives, source also cannot get any different information from feedback links. Thus the two codewords cannot be distinguished and this contradicts $C > 0$.

Case 2) $n > 2z$.

We first show the converse. If the z adversarial links are all forward links, then the capacity is less than or equal to $n - z$. If all $m \leqslant z$ feedback links are adversarial, the remaining network is a two-node network composed of n unit capacity forward links with $z - m$ adversarial links whose capacity is $n - 2(z - m)$ from [2].

Now we describe the strategy for achievability as follows.

Case 2) - 1) $m \leqslant z/2$.

Step 1) In each time slot, the source s sends an $(n, n - 2(z - m))$ MDS code on the n forward links. Since $m \leqslant z/2$, $n - 2(z - m) \leqslant n - z$. Thus for any received n signals, there exist $n - 2(z - m)$ uncorrupted signals. If all $\binom{n}{n-2(z-m)}$ subsets of received symbols decode to the same message, this message is correct. Otherwise, the sink sends the n received signals to the source s on each feedback link using a repetition code.

Step 2) As in Example 1, based on the received information on each feedback link, the source tries to identify the bad forward links. Thus, for each feedback link, the source obtains a claim regarding the location of forward adversarial links which is correct if that feedback link is not adversarial.

Step 3) This step consists of m rounds, each composed of a finite number of time slots. In the ith round, the source sends the claim obtained from the ith feedback link together with what it received on that feedback link to the sink. This information can be sent reliably to the sink using a repetition code because $n - 2z > 0$. If what the source received matches what sink sent, the ith feedback link was not corrupted and the associated claim is correct. Using this claim, the sink can decode the message as well as identify at least one of the forward adversarial links. If all m feedback links were corrupted, the sink knows that there are only $z - m$ forward adversarial links and since we are using a $(n, n - 2(z - m))$ MDS code the message is correctly decodable at the sink.

Note that we only need to use above scheme the first $2m$ times the sink sees inconsistency at step 1. The reason is that from steps 1)-3), the sink either figures out that all feedback links are adversarial or identifies at least one forward adversarial link. If all feedback links are bad, they are ignored and the $(n, n - 2(z - m))$ MDS code gives us the correct output. If there are $k \leqslant 2m$ forward adversarial links, after the first k times the sink sees inconsistency at step 1, all forward adversarial links are identified subsequently and no further inconsistency is seen among the remaining forward links. Otherwise, when there are more than $2m$ adversarial links, the sink finds $2m$ forward adversarial links and ignores them. Then from [2], the rate $n-2m-2(z-2m)=n-2(z-m)$ can be achieved using the remaining forward links only.

Case 2) - 2) $m > z/2$.

In each time slot, the source s sends an $(n, n-z)$ MDS code on the n forward links. For any received n signals, there exist $n-z$ uncorrupted signals. If all $\binom{n}{n-z}$ subsets of received symbols decode to the same message, this message is correct. As in the case 2) - 1), from steps 2)-3), the sink either concludes that all feedback links are adversarial or identifies at least one forward adversarial link. If all m feedback links were corrupted, there are only $z-m<z/2$ bad forward links and subsequently only the forward links are used to achieve the rate $n-z$. Otherwise, the above scheme is used at most z times inconsistency is seen at step 1, after which the sink has identified all bad forward links and the remaining forward links suffice to achieve rate $n-z$. ■

B. Unequal link capacities

Here we generalize the above equal link capacities result to the unequal link capacities case.

Theorem 1: Consider a two-node network $\mathcal{G}$ with k forward links and m feedback links of arbitrary capacities. There are at most z adversarial links in this network. Let D_p denote the sum of the p smallest forward link capacities and n the sum of the forward link capacities. The error correction capacity is

$$C=\begin{cases} 0 & \text{if } k \leqslant 2z \\ \min\{D_{k-z}, D_{k-2(z-m)^+}\} & \text{if } k > 2z \end{cases}$$

Proof: We use the similar proof in Lemma 1 for the case $k \leqslant 2z$. Suppose that $C > 0$ and we show a contradiction. Since $C > 0$, there are two codewords X and Y that can be sent reliably. When X is sent along forward links and leftmost z links are adversarial, adversary changes X to X' so that the outputs of leftmost $\lfloor n/2 \rfloor$ links of X' are the same as that of Y. Similarly, when Y is sent along forward links and rightmost z links are adversarial, adversary changes Y to Y' so that the outputs of rightmost $\lceil n/2 \rceil$ links of Y' are the same as that of X. Then the two codewords cannot be distinguished and contradicts $C > 0$.

Consider the case $k \geqslant 2z$. We first show the converse. When sink knows z adversarial links are the z largest capacities forward links, the maximum achievable capacity is D_{k-z}. When all feedback links are adversarial, we can achieve at most $D_{k-2(z-m)^+}$.

For achievability, when $m \leqslant z/2$, source sends (n, D_{k-z}) MDS code to sink. When $m > z/2$, source sends $(n, D_{k-2(z-m)^+})$ MDS code to sink. By using the same strategy in the proof of Lemma 1, we can achieve the rate C.

■

IV. Upper bound

First we restate our previous generalized Singleton upper bound [9] below. Similar upper bound result was presented [10] for node problem of correcting adversarial node errors.

Lemma 2: [9, Lemma 2] (Generalized Singleton bound) Consider any z-error correcting network code with source alphabet X in acyclic network $\mathcal{G}$. Consider any set S consisting of $2z$ links on a source-sink cut Q such that none of the remaining links on Q are downstream of any link in S. Let M be the total capacity of the remaining links. Then

$$\log|X| \leqslant M \cdot \log q.$$

.

A subset of links in S is said to satisfy the *downstream condition* if none of the remaining links on Q are downstream of any link in S.

In this section, we give a tighter cut-set upper bound for general acyclic networks.

Given a $Q = cut(P, \mathcal{V} - P)$, let Q^R denote the set of feedback links of the cut. Given a set of $m \leqslant z$ feedback links $W \subset Q^R$ and a set of $k \leqslant z-m$ forward links $F \subset Q$, we use $N^{F,W}_{z,m,k}(Q)$ to denote the upper bound obtained from Lemma 2 with $z-m-k$ adversarial links on the cut Q after erasing W and F from the graph $\mathcal{G}$. Let

$$N_{z,k,m}(Q) = \min_{\{F\subset Q, |F|=k\leqslant z-m\}} \min_{\{W \subset Q^R, |W|=m\leqslant z\}} N^{F,W}_{z,k,m}(Q).$$

Then we define $N_z(Q)$ as follows.

$$N_z(Q) = \min_{0\leqslant k \leqslant z-m} \min_{0 \leqslant m \leqslant z} N_{z,k,m}(Q).$$

Lemma 3: Consider any z-error correcting network code with source alphabet X in acyclic network.

$$\log|X| \leqslant \min_{u\in\mathcal{U}} \min_{Q\in CS(s,u)} \{N_z(Q)\} \cdot \log q$$

Proof: For any cut $Q \in CS(s,u)$, the adversary can choose to erase a set $W \subset Q^R$ feedback links and a set $F \subset Q$ of forward links where $|W| = m \leqslant z$ and $|F| = k \leqslant z-m$. Applying Lemma 2 on Q after erasing W and F gives the upper bound $N^{F,W}_{z,k,m}(Q)$. By taking the minimum over all such cuts, we obtain the above bound. ■

The following examples illustrate how above upper bound tightens generalized Singleton bound. We first consider a four-node acyclic directed networks as shown in Fig. 2. In each example, there are sufficiently large number of large capacity links from S to B, and from A to U, respectively, such that information from S can be sent reliably to B and information from A can be sent reliably to U. There are feedback links with arbitrary capacities from A to B.

When we compute the generalized Singleton bound, for any cut Q, we choose and erase $2z$ links in the cut such that none of the remaining links in the cut are downstream of chosen $2z$ links. Then we sum the remaining link capacities and take the minimum over all cuts. Because of downstream condition, when the link capacities between S and A are much larger than the link capacities between B and U as shown in Fig. 2 (a), Singleton bound may not be tight. When $z = 2$, generalized Singleton bound gives upper bound 20. However, when adversary declares that he will use two forward links between S and A, we obtain the erasure bound 4.

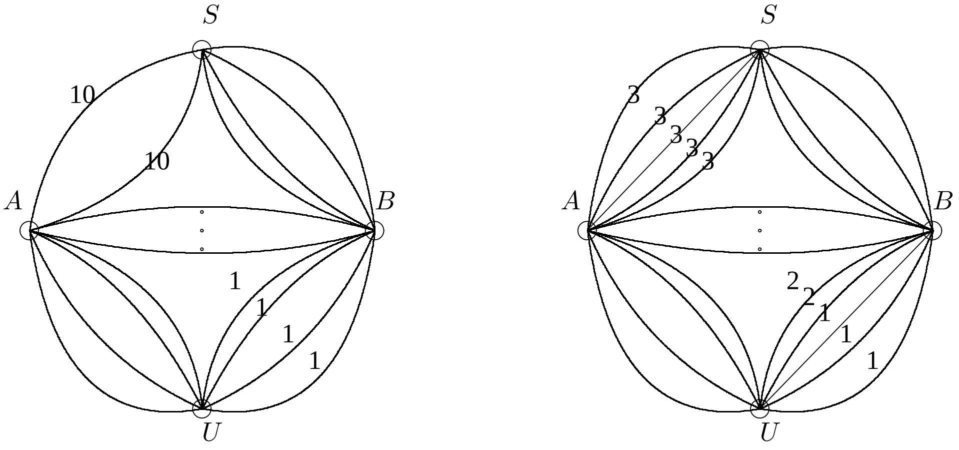

Fig. 2. Four node acyclic directed networks: There are sufficiently large number of large capacity links from S to B, and from A to U, respectively. (a) There are 2 links of capacity 10 from S to A and 4 unit capacity links from B to U. (b) There are 5 links of capacity 3 from S to A. There are 2 links of capacity 2 and 3 links of capacity 1 from B to U.

We consider the network in Fig. 2 (b). Suppose that $z = 2$. Applying generalized Singleton bound gives upper bound 16. If adversary declares that he will use one of forward link between S and A and sink knows it, we erase that link and apply generalized Singleton bound on the remaining network. Then our upper bound is improved 15. The intuition behind this example is that when adversary use $p \leqslant z$ large capacities links such that they are not in $2z$ downstream links, erasing those p links and applying generalized Singleton bound on remaining network with $(z - p)$ adversarial links can give tighter bound.

For the network in Fig. 3, when $z = 4$, min-cut is 37 and generalized Singleton bound gives upper bound 27. Suppose that adversary declares that he will use feedback link between C and D, and forward link with capacity 6 between S and A. By applying generalized Singleton bound on remaining network with two adversarial links, we obtain 37-6-(3+3+3+3)=19. The intuition behind this example is that the links between B and C and the links between D and U have the same topological order by erasing single feedback link between C and D. Since generalized Singleton bound is obtained by erasing $2z$ links on the cut such that none of the remaining links on the cut are downstream of any erased links, by erasing single feedback link between C and D, we can have tighter Singleton bound even with less number of adversarial links. Moreover, by erasing the link with capacity 6 which is the largest between S and A as we did in example in Fig. 2(b), we can also improve our upper bound.

Now we introduce another cut-set upper bound. For any cut $Q = (P, \mathcal{V} - P)$ and a set of nodes $A \subseteq \mathcal{V} - P$, let $F_A(Q) = \{(a, b) \in \mathcal{E} : a \in P, b \in A\} \subset Q$ and $W_A(Q) = \{(a, b) \in \mathcal{E} : a \in A, b \in P\} \subset Q^R$ to denote the set of all forward and feedback links incident to nodes in A, respectively. Let $|W_A(Q)| = m_A(Q)$.

Lemma 4: Suppose for a cut Q, there exists a set of nodes $A = \{v_1, .., v_t\} \subseteq \mathcal{V} - P$ such that $m_A(Q) \leqslant z$. For any $k \leqslant z - m_A(Q)$, first choose any set of k forward links $P_A(Q) \subseteq F_A(Q)$. Then choose a set of $z - k - m_A(Q)$ links $R_A(Q) \subset Q - P_A(Q)$ such that none of the remaining links on Q are downstream of links in $R_A(Q)$. Let $Z_A(Q) = P_A(Q) \cup R_A(Q)$ denote the set of chosen $z - m_A(Q)$ forward links. Similarly, for any set of nodes $B = \{j_1, .., j_r\} \subseteq \mathcal{V} - P - A$ such that $m_B(Q) \leqslant z$, we choose any set of $p \leqslant z - m_B(Q)$ forward links $P_B(Q) \subseteq F_B(Q)$ and a set of $z - p - m_B(Q)$ downstream links $R_B(Q) \subseteq Q - Z_A(Q) - P_B(Q)$. Let $Z_B(Q) = P_B(Q) \cup R_B(Q)$. Let M be the total capacity of the remaining links on $Q - Z_A(Q) - Z_B(Q)$. Then

$$\log |X| \leqslant M \cdot \log q.$$

Proof: We assume that $|X| > q^M$, and show that this leads to a contradiction. Let $K(Q)$ denote the number of links on the cut Q. Since $|X| > q^M$, from the definition of M, there exist two distinct codewords $x, x' \in X$ such that error-free outputs on the links in $Q - Z_A(Q) - Z_B(Q)$ are the same. Let $a = |Z_A(Q)|$ and $b = |Z_B(Q)|$. So we can write

$$O(x) = \{y_1, .., y_{K(Q)-a-b}, u_1, .., u_a, w_1, .., w_b\},$$

$$O(x') = \{y_1, .., y_{K(Q)-a-b}, u'_1, .., u'_a, w'_1, .., w'_b\},$$

where $(y_1, .., y_{K(Q)-a-b})$ denotes the error-free outputs on the links in $Q - Z_A(Q) - Z_B(Q)$, $(u_1, .., u_k)$ and $(u'_1, .., u'_k)$ denote the error-free outputs on the links in $P_A(Q)$ for x and x' respectively, and $(u_{k+1}, .., u_a)$ and $(u'_{k+1}, .., u'_a)$ denote the error-free outputs on the links in $R_A(Q)$ for x and x' respectively. Similarly, let $(w_1, .., w_p)$ and $(w'_1, .., w'_p)$ denote the error-free outputs on the links in $P_B(Q)$ for x and x' respectively, and let $(w_{p+1}, .., w_b)$ and $(w'_{p+1}, .., w'_b)$ denote the error-free outputs on the links in $R_B(Q)$ for x and x' respectively. We will show that it is possible for the adversary

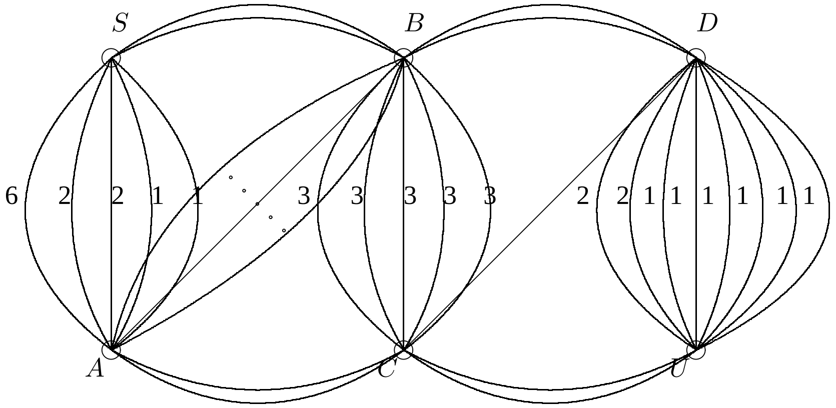

Fig. 3. Six node acyclic networks: There are sufficiently large number of large capacity links from S to B, from B to D, from A to C, and from C to U respectively. There are sufficiently large number of feedback links from A to B. There is one feedback link from C to D.

to produce exactly the same outputs at all the channels on Q when errors occur on at most z links. When codeword x is sent, we use $B_l(x)$ to denote the error-free output on feedback link l.

Assume the input of network is x. The adversary chooses feedback links set $W_A(Q)$ and forward links set $Z_A(Q)$ as z adversarial links. First adversary applies errors on $P_A(Q)$ to change the output from u_i to u'_i for $\forall 1 \leqslant i \leqslant k$ and causes each feedback link $l \in W_A(Q)$ to transmit $B_l(x)$. Since all feedback links in $W_A(Q)$ transmit the error-free output, when the output u_i on any link in $P_A(Q)$ is changed, the outputs of downstream links of it are not affected. Thus $(u_1, .., u_k)$ is changed to $(u'_1, .., u'_k)$ without affecting the outputs of any other links. Then jammer applies errors on $R_A(Q)$ to change the output from $(u_{k+1}, .., u_a)$ to $(u'_{k+1}, .., u'_a)$. Since the links in $R_A(Q)$ satisfy downstream condition, the outputs of any other links are not affected. Sink finally observes $\{y_1, .., y_{K(Q)-a-b}, u'_1, .., u'_a, w_1, .., w_b\}$.

When codeword x' is transmitted, the adversary chooses feedback links set $W_B(Q)$ and forward links set $Z_B(Q)$ as z adversarial links. Adversary applies errors on them to change $(w_1, .., w_b)$ to $(w'_1, .., w'_b)$ without affecting the outputs on other links as shown above. Then output is changed from $O(x')$ to $\{y_1, .., y_{K(Q)-a-b}, u'_1, .., u'_a, w_1, .., w_b\}$. Thus, sink node u cannot reliably distinguish between the codewords x and x', which gives a contradiction. ■

Given a cut Q, we consider all possible sets $(Z_A(Q), Z_B(Q))$ on the Q satisfying the condition on Lemma 4. We choose sets $(Z_A(Q)^*, Z_B(Q)^*)$ among them that have the maximum total link capacities and define $M_z(Q)$ to be the sum of the capacities of the links on Q which are not in $(Z_A(Q)^*, Z_B(Q)^*)$. This gives the upper bound

$$\log |X| \leqslant \min_{u \in \mathcal{U}} \min_{Q \in cut(s,u)} M_z(Q) \cdot \log q.$$

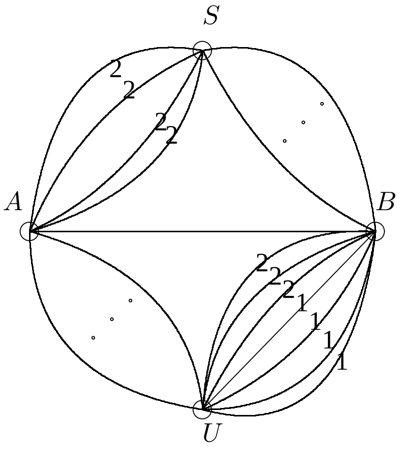

Fig. 4. Four node acyclic networks: There are 4 links of capacity 2 from S to A. There are 3 links of capacity 2 and 1 links of capacity 4 from B to U.

Following example shows that we can obtain tighter upper bound using Lemma 4. For example network in Fig. 4, when $z = 3$, Lemma 3 gives upper bound 9. However, Lemma 4 gives tighter upper bound 8.

Now we derive general cut-set upper bound that unifies Lemma 3 and Lemma 4. Given a cut Q, we choose the set of $m \leqslant z$ feedback links $W \subset Q^R$ and the set of $k \leqslant z - m$ forward links $F \subset Q$. We use $C^{F,W}_{z,m,k}(Q)$ to denote the upper bound obtained from Lemma 4 with $z - m - k$ adversarial links on the cut Q after erasing W and F from original graph

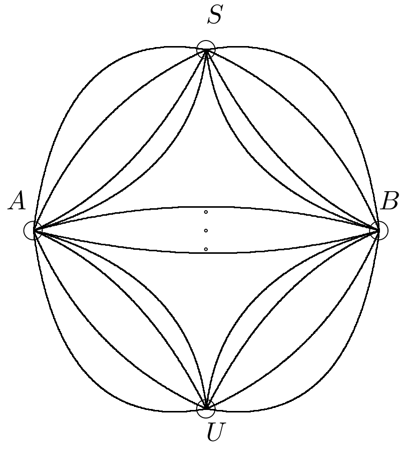

Fig. 5. Four node acyclic networks: this network consists of a links of arbitrary capacity from S to A, b links of arbitrary capacity from B to U, sufficiently large number of large capacity links from S to B, sufficiently large number of large capacity links from A to U. From A to B, there are m feedback links and each feedback link has enough capacity such that A can forward what it received from S to B.

$\mathcal{G}$. Let

$$C_{z,k,m}(Q) = \min_{\{F\subset Q, |F|=k\leqslant z-m\}} \min_{\{W\subset Q^R, |W|=m\leqslant z\}} C^{F,W}_{z,k,m}(Q).$$

Then we define $C_z(Q)$ as follows.

$$C_z(Q) = \min_{0\leqslant k\leqslant z-m} \min_{0\leqslant m\leqslant z} C_{z,k,m}(Q).$$

This gives the following upper bound.

Theorem 2: (General cut-set upper bound) Consider any z-error correcting network code with source alphabet X in acyclic network.

$$\log|X| \leqslant \min_{u\in\mathcal{U}} \min_{Q\in CS(s,u)} C_z(Q)\cdot\log q$$

Now we show that this general cut-set bound unifies Lemma 3 and Lemma 4. In Lemma 4, when $A = B = \emptyset$, the bound is the same as generalized Singleton bound. Thus, when we apply bound in Lemma 4 to compute $C^{F,W}_{z,m,k}(Q)$ after erasing W and F, choosing $A = B = \emptyset$ gives the bound in Lemma 3. It is also clear that $C^{F,W}_{z,m,k}(Q)$ is the same as bound in Lemma 4 when $F = W = \emptyset$.

V. Four node acyclic network

In this section, we show the tightness of the bound of Theorem 2 for the directed acyclic networks shown in Fig. 5. This network consists of a links of arbitrary capacities from source node S to A, m feedback links from A to B, b links of arbitrary capacities from B to sink U. There are sufficiently large number of large capacity links from S to B, and from A to U, respectively, such that information from S can be sent reliably to B and information from A can be sent reliably to U. We use K_1 and K_2 to denote the sum of link capacities between S and A, and B and U, respectively. In this network, there is only one finite capacity source-sink cut $cut(\{S,B\},\{A,U\})$ whose capacity is $K_1 + K_2 = C$. Each feedback link from A to B has capacity at least K_1. We use C_z to denote the upper bound obtained from Theorem 2.

Now we show that rate C_z is achievable in this network. W and $\hat{W}$ denote the symbols sent by S and received by A respectively on the links between S and A. W is sent reliably from S to B and $\hat{W}$ is sent reliably from A to U. We consider following strategy which will be used in both Lemma 5 and 6.

Strategy : At each time step, S and B together send a (C, C_z) MDS code to A and U across the $cut(\{S,B\},\{A,U\})$. A sends its codeword symbols $\hat{W}$ to B along each feedback link using a repetition code. For each feedback link l, let P_l denote the information received by B on l. B compares P_l with W which is received from S. If $P_l \neq W$, then B obtains a guess X_l identifying the locations of adversarial links between S and A assuming P_l is reliable. B sends the claim (X_l, P_l) to U along each link between B and U using repetition code. If $P_l = W$, B does not send anything. The above strategy is applied at each time step. We show that only a finite number of claims are sent altogether.

Lemma 5: When $b \geqslant 2z+1$, rate C_z is achievable.

Proof: Since $b \geqslant 2z+1$, any claim (X_l, P_l) can be sent reliably from B to U using a repetition code.

Case 1) sink receives some claim (X_i, P_i).

The sink compares P_i with $\hat{W}$ which is received from A reliably. If $P_i \neq \hat{W}$, then feedback link transmitting P_i is adversarial and the sink ignores it. Otherwise, P_i is reliable. Since the claim is sent, the sink knows that $P_i = \hat{W} \neq W$ and that guess X_i is correct. Thus the sink identifies at least one adversarial link between S and A, which is subsequently ignored.

Therefore, in this case, the sink remove one bad link whenever B sends claims. We show that it is possible to obtain correct solution after B sends claims $\min\{m, z\}$ times. If $m > z$, the sink can identify z adversarial links when B sends claims z times.

Assume that $m < z$. After B sends claims m times, there are at most $z - m$ remaining adversarial links on the cut and thus $(a+b-z+m)$ uncorrupted links. Now the sink check the consistency of outputs for any $(a+b-z+m)$ links on the cut. Suppose a set L composed of $(a+b-z+m)$ links on the cut gives the consistent output. This set includes at least $(a+b-2(z-m))$ uncorrupted links. From the definition of our bound in Lemma 3, when $m \leqslant z$, the sum of the $(a+b-2(z-m))$ link capacities is larger than or equal to C_z. Thus we obtain correct output with rate C_z from uncorrupted links. Since L gives the consistent output, we trust this output.

Case 2) no claims are sent.

In this case, we show that the correct output is achieved without using any claims. B does not sent any claim when it receives W from each feedback link. There are two possibilities.

a) all links between S and A and all feedback links are uncorrupted.

b) some links between S and A are corrupted and all feedback links are corrupted such that each feedback link transmits error-free output.

In a), each feedback link transmits W to B. In b), A sends $\hat{W} \neq W$ but each feedback link changes it to W so that B does not send any claims. We first consider all sets of $(a+b-z+m)$ links on the cut. There are $\binom{a+b}{a+b-z+m}$ such sets of links. From the definition of our bound, the sum of any $(a+b-z)$ forward links capacities are larger than or equal to C_z. Thus, for any set L of $(a+b-z+m)$ links, $\sum_{l \in L} r(l) \geqslant C_z$. For each such set L, the sink check the consistency of the output of rate C_z obtained from L. We also consider all sets of $(a+b-z)$ links such that each set includes all a links between S and A and any $b-z$ links between B and U. There are $\binom{b}{b-z}$ such sets. The sink also check the consistency of the output of rate C_z for each set.

Case 2) - 1) there is no set of $(a+b-z+m)$ link giving consistent output.

In this case, there are more than $z-m$ adversarial links on the cut. Thus b) cannot be happened and a) is true. Then there exists $a+b-z$ links set L that includes all a links between S and A and gives the consistent output. Since a) is true, at most z adversarial links are between B and U. Thus L includes a correct links between S and A and at least $b-2z$ correct links between B and U. From the definition of generalized Singleton bound, the sum of the capacities of a links between S and A and any $b-2z$ links between B and U are larger than or equal to C_z. Since L gives consistent output, this output should be correct.

Case 2) - 2) there is no set of $(a+b-z)$ links that include all a links between S and A and give the consistent output.

In this case, b) is true. Then there are at most $z-m$ adversarial links on the cut. We choose a set L composed of $(a+b-z+m)$ links on the cut which gives consistent output. Then L includes at least $(a+b-2(z-m))$ uncorrupted links. Since the sum of the $(a+b-2(z-m))$ link capacities is larger than or equal to C_z, we obtain correct output from $(a+b-2(z-m))$ uncorrupted links.

Case 2) - 3) There exist both $(a+b-z+m)$ links set L_1 giving consistent output and $(a+b-z)$ links set L_2 that include all a links between S and A and give the consistent output.

We show that L_1 and L_2 gives the same consistent output. $L_1 \cap L_2$ is obtained from the cut by erasing z links between B and U that L_2 does not include and $z-m$ links L_1 does not include. From the definition of our bound in Lemma 4, $\sum_{l \in L_1 \cap L_2} r(l) \geqslant C_z$. Thus L_1 and L_2 gives the same consistent output. Since at least one of a) and b) is true, this output is correct.

■

Lemma 6: When $b \leqslant 2z$, rate C_z is achievable.

Proof: When $b \leqslant 2z$, reliable transmission of claims from B to U is not guaranteed. First we show that any uncorrupted $(a+b-2z)$ links between S and A give the correct decoded output with rate C_z. From the definition of Singleton bound, after erasing $b \leqslant 2z$ links between B and U and any set of $2z-b$ links between S and A, the sum of the remaining link capacities are larger than or equal to C_z. Thus any uncorrupted $(a+b-2z)$ links between S and A give the correct message.

We consider any feedback link l. Based on information B received along l, B sends claim (X_l, P_l). Suppose that sink receives a set of distinct claims $G(l) = \{(X_{l1}, P_{l1}), .., (X_{lk}, P_{lk}), Y\}$ for l where Y denotes that no claims received. Assume that (X_{li}, P_{li}) is received on n_i links and Y is received on n_{k+1} links $(n_1 + .. + n_{k+1} = b)$. First we ignore any (X_{li}, P_{li}) claiming that there are more than $z-(b-n_i)$ adversarial links between S and A. Since X_{li} is shown on n_i links, believing X_{li} implies more than z adversarial links on the cut which is a contradiction. Thus, each of remaining claim (X_{lj}, P_{lj}) specifies a set L_j which is composed of at least $(a-(z-(b-n_i))) = a+b-z-n_i$ links between S and A claimed to be correct by (X_{lj}, P_{lj}). For each such claim, we check the consistency of the outputs of L_j. We first show that if there exist two different claims (X_{li}, P_{li}) and (X_{lj}, P_{lj}) both corresponding to consistent outputs, then those outputs should be the same. Since $|L_i| = a+b-z-n_i$, $|L_j| = a+b-z-n_j$, and $|L_i \cup L_j| \leqslant a$,

$$\begin{aligned} |L_i \cap L_j| &\geqslant (a+b-z-n_i) + (a+b-z-n_j) - a \\ &\geqslant a+b-2z. \end{aligned}$$

As we mentioned at the beginning of the proof, the sum of capacities of any $(a+b-2z)$ link between S and A are larger than or equal to C_z. Therefore (X_{li}, P_{li}) and (X_{lj}, P_{lj}) give the same consistent output.

Now we show that for any feedback link l, we can remove at least one bad link or obtain correct output using $G(l)$ except when only Y gives consistent output and it is shown on more than z links. We consider following cases.

Case 1) all claims are ignored or none of the remaining claims gives consistent output or all claims (X_{li}, P_{li}) that give consistent output satisfy that $P_{li} \neq \hat{W}$

In this case, there are only two possibilities.

a) feedback link l is adversarial.

b) all b links between B and U are adversarial.

If $b > z$, then feedback link is adversarial and we remove it. If $b \leqslant z$, the sink checks the consistency of outputs from each set of $(a+b-z)$ links between S and A. If no $(a+b-z)$ links set give consistency, there are more than $z-b$ adversarial links between S and A. Thus a) is true and we remove feedback link l. Otherwise, there exists set L of $(a+b-z)$ links giving consistency, which includes at least $(a+b-2z)$ uncorrupted links between S and A and sum of capacities of uncorrupted links are larger than or equal to C_z. Thus L gives correct output.

Case 2) there exists a claim (X_{li}, P_{li}) giving consistent output.

In this case, $P_{li} = \hat{W}$. We show that output obtained from (X_{li}, P_{li}) is correct. If there is at least one correct link showing (X_{li}, P_{li}), then feedback link l is also correct since $P_{li} = \hat{W}$

and this claim gives correct output. Thus (X_{li}, P_{li}) is wrong only when all n_i links showing this claim are adversarial, in which case, there are at most $z - n_i$ adversarial links between S and A. Then L_i includes at least $(a+b-z-n_i)-(z-n_i) = a + b - 2z$ correct links and give correct output.

Case 3) only Y gives consistent output and $n_{k+1} \leqslant z$.

First we check the consistency of outputs obtained from a links between S and A. If outputs are not consistent, Y is incorrect and we go to case 1). Assume that a links give consistent output.

If $n_{k+1} < b - z$, there are more than z adversarial links when we trust Y. Thus we remove links showing Y.

Assume that $b - z \leqslant n_{k+1} \leqslant z$.

If $b \leqslant z$, a links between S and A include at least $a - z \geqslant a + b - 2z$ uncorrupted links. Thus we obtain correct output from a links.

If $b > z$, Y is shown on $n_{k+1} \geqslant b - z$ links and $b - n_{k+1} \geqslant b - z$ links show claims different from Y. Thus there are at least $b - z$ adversarial links B and U. There are at most $2z - b$ adversarial links between S and A and at least $a + b - 2z$ uncorrupted links. Thus we also obtain correct output from a links.

From cases 1, 2, and 3, for any feedback link l, we can remove at least one bad link or obtain correct output using $G(l)$ except when only Y gives consistency and it is shown on more than z links. Thus the only remaining case is that only Y gives consistent output and $n_{k+1} > z$ for all feedback links. Then each feedback link transmits error-free output to B and sink knows it. There are following two possibilities.

a) all links between S and A and all feedback links are uncorrupted.

b) some links between S and A are corrupted and all feedback links are corrupted such that each feedback link transmits error-free output.

This case corresponds to the case 2 in Lemma 5. Therefore, we can obtain the correct output.

When we have correct output from some links, we add remaining links on the cut sequentially and choose the link that makes inconsistency. Then we detect at least one forward adversarial link and remove it. Therefore, after repeating our strategy at most m times, we obtain the correct output from MDS code. ■

VI. ZIG-ZAG NETWORK

In previous section, we have shown that our upper bound is tight in a four-node acyclic network. In this section, we consider a more general family of zig-zag networks. We present conditions under which our upper bound is tight.

We call zig-zag network shown in Fig. 6 a k-layer zig-zag network. There are sufficiently large number of large capacity links from A_i to A_{i+1} and from B_i to B_{i+1} for $\forall 0 \leqslant i \leqslant k$, respectively. ($S = B_0, U = A_{k+1}$). Thus, reliable transmission is possible from A_i to A_j, and from B_i to B_j for $\forall i < j$. We use F_i and W_i to denote the set of forward links and feedback links from B_{i-1} to A_i, and from A_i to B_i, respectively. Let $|F_i| = b_i$ and $|W_i| = m_i$. It is clear that the four-node network is 1-layer zig-zag network. Given a k-layer zig-zag network $\mathcal{G}$, we use C_z to denote the upper bound on $\mathcal{G}$ obtained from Theorem 2.

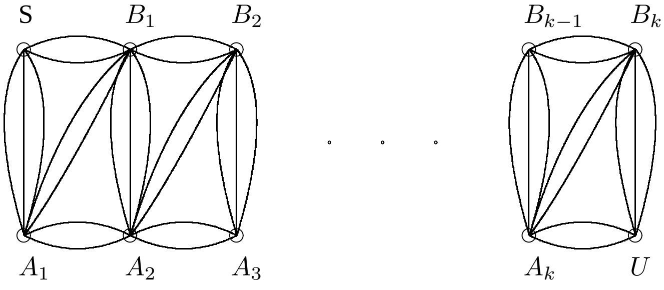

Fig. 6. k-layer zig-zag network: There are sufficiently large number of large capacity links from A_i to A_{i+1} and from B_i to B_{i+1} for $\forall 0 \leqslant i \leqslant k$, respectively. ($S = B_0$, $U = A_{k+1}$). We use F_i and W_i to denote the set of forward links and feedback links from B_{i-1} to A_i, and from A_i to B_i, respectively. $|F_i| = b_i$ and $|W_i| = m_i$.

Now we consider following strategy which is similar to that for a four-node network. We use C to denote the sum of all forward link capacities.

Strategy : At each time step, S and $(B_1, .., B_k)$ together send a (C, C_z) MDS code to $(A_1, .., A_k)$ and U across the cut. For $1 \leqslant i \leqslant k$, A_i sends its codeword symbols $\hat{W}$ to B_i along each feedback link using a repetition code. For each feedback link l, let P_l denote the information received by B_i along on l. B_i compares P_l with W which is received from S. If $P_l \neq W$, then B_i obtains a guess X_l identifying the locations of adversarial links between B_{i-1} and A_i assuming P_l is reliable. B_i sends claim (X_l, P_l) to A_{i+1} along each link using repetition code. If $P_l = W$, B_i does not send anything. For $\forall 2 \leqslant j \leqslant k$, A_j sends any received claim from B_{j-1} to the sink reliably. The above strategy is applied at each time step. We show that only a finite number of claims are sent altogether.

Lemma 7: Given a family of k-layers zig-zag networks such that $b_i \geqslant 2z + 1$ for $2 \leqslant i \leqslant k + 1$, rate C_z is achievable.

Proof: Since $b_i \geqslant 2z + 1$ for $2 \leqslant i \leqslant k + 1$, any claim (X_l, P_l) can be sent reliably from B_{i-1} to A_i using repetition code. Then A_i sends this claim reliably to sink U. In case 1, we show that at least one adversarial link is removed whenever sink receives some claim. We also show that correct output is always achievable when no claims are sent in case 2.

Case 1) sink receives some claim (X_l, P_l).

Assume that feedback link l is between A_j and B_j, and B_j sends this claim to A_{j+1}. In this case, we use the same strategy as in the case 1 in Lemma 5.

Case 2) no claims are sent to the sink.

In this case, there are following possibilities.

a) All forward links in (F_1,..,F_k) and feedback links in (W_1,..,W_k) are not corrupted.

b) For some $\{i_1, .., i_p\} \subseteq \{1, 2, .., k\}$ such that $m_{i_1} + .. + m_{i_p} \leqslant z$, all feedback links in $(W_{i_1}, .., W_{i_p})$ are corrupted and some forward links in $(F_{i_1}, .., F_{i_p})$ are corrupted. For $\forall j \notin \{i_1, .., i_p, k+1\}$, links in F_j and W_j are not corrupted.

Let $N = \{(i_1, .., i_p) | 1 \leqslant i_1 < .., < i_p \leqslant k, m_{i_1} + .. + m_{i_p} \leqslant z\} \cup \{\emptyset\}$. (Note that $\{\emptyset\}$ corresponds to the possibility in a)). From a) and b), there are $|N| + 1$ possibilities. Exactly only one of them is true. Now we describe how correct solution with rate C_z can be obtained. We check the consistency of the output for each possibility. For each $(i_1, .., i_p) \in N$, we check that there are $K - (z - (m_{i_1} + .. + m_{i_p}))$ forward links giving consistent output such that removed $(z - (m_{i_1} + .. + m_{i_p}))$ forward links are in $F_{i_1} \cup .. \cup F_{i_p} \cup F_{k+1}$. We use $G(i_1, .., i_p)$ to denote the the set of such forward links giving consistency. If there is no such $K - (z - (m_{i_1} + .. + m_{i_p}))$ forward links giving consistency, we remove $(i_1, .., i_p)$ from N and ignore corresponding possibilities.

Case 2) - 1) $|N| = 1$, i.e., only one element is remained in N.

Since exactly one of $|N| + 1$ possibilities is true, we should choose remained possibility and obtain a correct consistent output.

Case 2) - 2) $|N| > 1$.

We show that every remaining element in N gives the same consistent output. Suppose that $(i_1, .., i_p)$ and $(j_1, .., j_r)$ are remained in N. $G(i_1, .., i_p)$ gives $K - (z - (m_{i_1} + .. + m_{i_p}))$ forward links giving consistent output such that removed $(z - (m_{i_1} + .. + m_{i_p}))$ forward links are in $F_{i_1} \cup .. \cup F_{i_p} \cup F_{k+1}$. Similarly, $G(j_1, .., j_r)$ gives $K - (z - (m_{j_1} + .. + m_{j_r}))$ forward links giving consistent output such that removed $(z - (m_{j_1} + .. + m_{j_r}))$ forward links are in $F_{j_1} \cup .. \cup F_{j_r} \cup F_{k+1}$. In this case, from the definition of cut-set upper bound in Lemma 4, sum of the capacity of forward links assumed to be correct by both $G(i_1, .., i_p)$ and $G(j_1, .., j_r)$ are at least C_z. Since each guess gives the consistent output, these two guesses gives the same output. Since any two remained guesses in N gives the same consistent output, all remaining guesses give the same output.

■

Using above achievability result, we derive another condition under which our bound is tight.

Lemma 8: Given a family of k-layers zig-zag networks such that $m_t > z$ and $b_j \geqslant 2z + 1$ for $\forall j \geqslant t + 1$ for any $1 \leqslant t \leqslant k$, rate C_z is achievable.

Proof: We consider a reduced zig-zag network $\mathcal{G}'$ which is obtained from given a k-layer zig-zag network by erasing $m_1 + .. + m_{t-1}$ feedback links $W_1 \cup .. \cup W_{t-1}$. We use C'_z to denote the upper bound on $\mathcal{G}'$ from Theorem 2.

Step 1) We show that $C_z \leqslant C'_z$.

Suppose that C'_z is obtained from $\mathcal{G}'$ by choosing k forward links set F^*, m feedback links set W^*, and $A^* = \{A_{i_1}, .., A_{i_p}\} \subseteq \{A_t, A_{t+1} .., A_{k+1}\}$ and $B^* = \{A_{j_1}, .., A_{j_r}\} \subseteq \{A_t, A_{t+1}, .., A_{k+1}\} - A^*$ by applying Lemma 4 after erasing F^* and W^*. $P_{A^*} \subseteq F_{A_{i_1}} \cup .. \cup F_{A_{i_p}}$, $P_{B^*} \subseteq F_{A_{j_1}} \cup .. \cup F_{A_{j_r}}$, $Z_{A^*} = P_{A^*} \cup R_{A^*}$, and $Z_{B^*} = P_{B^*} \cup R_{B^*}$. Since $m_t > z$, from the definition of upper bound in Lemma 4, $A_t \notin A^*$ and $A_t \notin B^*$.

First we show that $W^* \subset W_{t+1} \cup .. \cup W_k$. Since $m_t > z$, from the downstream condition of our bound, erasing any feedback links in W_t does not give any chance to erase forward links in $F_1 \cup .. \cup F_t$. Since C'_z is optimal, $W^* \subset W_{t+1} \cup .. \cup W_k$. Then $Z_{A^*}, Z_{B^*} \subset F_{t+1} \cup .. \cup F_k$. Therefore, when we apply Lemma 4 on original graph $\mathcal{G}$ after erasing F^* and W^*, it is clear that choosing Z_{A^*} and Z_{B^*} gives the same upper bound on $\mathcal{G}$. Moreover, when we choose optimal nodes set $(A^*)'$ and $(B^*)'$ to apply Lemma 4 on $\mathcal{G}$, $(A^*)'$ and $(B^*)'$ can also contain nodes in $(A_1, .., A_{t-1})$ respectively, unlikely when we choose A^* and B^* on $\mathcal{G}'$. Therefore, $C_z \leqslant C'_z$.

Step 2) We show that rate C_z is achievable.

From our achievability results on the four-node network, rate C_z is achievable since $C_z \leqslant C'_z$. Thus, given a zig-zag network, we first remove all feedback links between A_i and B_i $(1 \leqslant i \leqslant k)$ and apply the same achievable strategy for four-node network.

From Step 1) and 2), we complete the proof. ■

VII. Network Error Correction with a Causal Adversary

In this section, we consider network error correction with a causal adversary. So far, network error correction was mainly studied for acyclic delay-free network with assumption that adversary has complete knowledge of network. Recently, the problem of codes against causal adversary was considered [12]. network error We add following two assumptions on our original problem.

1) Memory network: internal nodes in the network employ memory and can send information based on what it received after sufficient amount of time.

2) Causal adversary channels: In contrast to classical adversarial model in which adversary knows complete messages, the decisions of the jammer must be made in causal manner [12]. When source transmits codewords $(X_1, .., X_n)$, for each codeword X_i, the jammer's decision on whether to corrupt it or not (and on how to change it) must depend only on X_j for $j \leqslant i$.

By assuming above conditions, we can find the capacity of networks in previous sections. We first consider a two-node network consisting of $k \geqslant 2z+1$ forward links. Let D_p denote the sum of p smallest link capacities and K_1 denote the sum of all link capacities. We show that rate D_{k-z} is achievable by figuring out the locations of adversarial links correctly w.h.p.

Lemma 9: Given a two-node network, capacity D_{k-z} is achievable w.h.p.

Proof: It is clear that D_{k-z} is upper bound. For achievability, it is sufficient to show that sink can figure out the locations of adversarial links between S and A correctly w.h.p. Suppose that ϵ is arbitrarily small number.

We consider following strategy. For any $n > 2K_1/\epsilon$, we call n time slots a period. We use $(a_1^t, .., a_{K_1}^t)$ and $(\tilde{a}_1^t, .., \tilde{a}_{K_1}^t)$ to denote the information source sends and sink received at time slot t, respectively.

1) For $N > 2/\epsilon$, source sends $(a_1^t, .., a_{K_1}^t)$ and sink receives $(\tilde{a}_1^t, .., \tilde{a}_{K_1}^t)$ during first $N \times n$ time slots.

2) After $N \times n$ time slots, source chooses a n-dimensional row vector $(r_1, .., r_n)$ uniformly at random from $GF^n(q)$ and sends it to sink along each link. Since $k \geqslant 2z + 1$, this vector can be sent reliably.

3) For ith period $(1 \leqslant i \leqslant N)$, source sends $(\sum_{j=1}^n r_j a_1^{n(i-1)+j}, .., \sum_{j=1}^n r_j a_{K_1}^{n(i-1)+j})$ along each link. Note that $(r_1, .., r_n)$ are fixed over N periods.

4) Based on linear sums sent reliably, sink figures out the locations of adversarial links.

At step 3), source sends linear sum of each correct bit during n time slots. Since $k \geqslant 2z+1$, this linear sums are transmitted reliably to sink. $n + K_1 \cdot N$ bits for vector and linear sums are transmitted after $N \cdot m$ time slots. Since $N > 2/\epsilon$ and $n > 2K_1/\epsilon$, $(n + K_1 \cdot N)/(N \cdot n) \leqslant \epsilon$ and those transmissions are possible along each link with capacity ϵ. Now we show that sink can figure out the locations of adversarial links correctly with high probability. Sink knows correct $(r_1, .., r_n)$ and linear sums $(\sum_{j=1}^n r_j a_1^{n(i-1)+j}, .., \sum_{j=1}^n r_j a_{K_1}^{n(i-1)+j})$ for each of ith period. Without loss of generality, suppose that source sends $(a_1^t, .., a_h^t)$ to sink through some adversarial link at any time t. During ith period, sink figures out this link is not adversarial only if $(\sum_{j=1}^n r_j \tilde{a}_k^{n(i-1)+j} = \sum_{j=1}^n r_j a_k^{n(i-1)+j})$ for all $1 \leqslant k \leqslant h$. Thus, for any link transmitting h bits, given $(a_k^{n(i-1)+1}, .., a_k^{ni-1})$ and $(\tilde{a}_k^{n(i-1)+1}, .., \tilde{a}_k^{ni-1})$ for $1 \leqslant k \leqslant h$, the probability that sink figures out incorrectly is at most h/q. Thus, for every link, sink can figure out correctly with probability at least $1 - K_1/q$. ■

Corollary 1: For any zig-zag network with k forward links, rate D_{k-z} is achievable.

Proof: Since zig-zag network has only one cut with finite volume, ignoring all feedback links across the cut and applying Lemma 9 to the remaining network gives the result. ■

VIII. Conclusion and Future Work

In this paper, we consider network error correction with unequal link capacities and present new results on error correction capacities and upper bounds. We first characterize the capacity of a two-node network with multiple feedback links and show that feedback links can be used to increase the error correction capacity. We propose a new cut-set upper bound for general acyclic networks that tightens our previous upper bound. We consider a family of four-node acyclic networks and show that our bound is tight when each feedback link has enough capacity. For a more general family of zig-zag networks, we present conditions under which our upper bound is tight. Finally, we consider a network error correction with a causal adversary and propose a high-probability approach which can be used to achieve erasure capacity. Future work includes to characterize the capacity region when feedback link does not have enough capacity in the four-node acyclic network. We will also investigate more conditions in zig-zag network under which our upper bound is tight.

Acknowledgements

This work is partly supported by NSF grant CNS 0905615 and Caltech's Lee Center for Advanced Networking.

References

[1] R. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 19–36, 2006.

[2] N. Cai and R. Yeung, "Network error correction, part II: Lower bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 37–54, 2006.

[3] S. Yang, C. Ngai, and R. Yeung, "Construction of linear network codes that achieve a refined Singleton bound," in *Proc. ISIT*, vol. 7, 2007.

[4] S. Yang and R. Yeung, "Refined coding bounds for network error correction," *network*, vol. 1, no. y2, p. 8.

[5] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Medard, "Resilient network coding in the presence of byzantine adversaries," *benefits*, vol. 16, p. 6.

[6] D. Silva, F. Kschischang, and R. Kotter, "Capacity of random network coding under a probabilistic error model," in *24th Biennial Symposium on Communications, Kingston, ON, Canada*, 2008.

[7] R. Koetter and F. Kschischang, "Coding for errors and erasures in random network coding," *Arxiv preprint cs/0703061*, 2007.

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

[9] S. Kim, T. Ho, M. Effros, and S. Avestimehr, "Network error correction with unequal link capacities," in *Communication, Control, and Computing, 2009 47th Annual Allerton Conference on*.

[10] O. Kosut, L. Tong, and D. Tse, "Nonlinear network coding is necessary to combat general byzantine attacks," in *47th Annual Allerton Conference on Communication, Control, and Computing*, 2009.

[11] G. Liang, R. Agarwal, and N. Vaidya, "Non-Linear Network Coding against Byzantine Adversary: Part I."

[12] M. Langberg, S. Jaggi, and B. Dey, "Binary Causal-Adversary Channels," *Imprint*, 2009.