場 明 物 通



The HKU Scholars Hub

The University of Hong Kong 香港大学学術庫

Title	Bounds and exact values in network encoding complexity with two sinks
Author(s)	Xu, L; Han, G
Citation	The 49th Allerton Conference on Communication, Control and Computing, Monticello, Illinois, USA, 28-30 September 2011. In Annual Allerton Conference on Communication, Control and Computing Proceedings, 2011, p. 1462-1469
Issued Date	2011
URL	http://hdl.handle.net/10722/158882
Rights	Annual Allerton Conference on Communication, Control and Computing Proceedings. Copyright © IEEE.

Bounds and Exact Values in Network Encoding Complexity with Two Sinks

Li Xu The University of Hong Kong email: xuli@hku.hk

Abstract—For an acyclic directed network with multiple pairs of sources and sinks and a set of Menger's paths connecting each pair of source and sink, it is well known that the number of mergings among these Menger's paths is closely related to network encoding complexity. In this paper, we focus on networks with two distinct sinks and we derive bounds on and exact values of two functions relevant to encoding complexity for such networks.

I. INTRODUCTION

Let G(V, E) denote an acyclic directed graph, where V denotes the set of all the vertices (or points) in G and E denotes the set of all the edges in G. In this paper, a *path* in G is treated as a set of concatenated edges. For k paths $\beta_1, \beta_2, \ldots, \beta_k$ in G(V, E), we say these paths *merge* [3] at an edge $e \in E$ if

- 1) $e \in \bigcap_{i=1}^k \beta_i$,
- there are at least two distinct edges f, g ∈ E such that f, g are immediately ahead of e on some β_i, β_j, i ≠ j, respectively.

We call *e* together with the subsequent concatenated edges shared by all β_i 's (until they branch off) *merged subpath* (or simply *merging*) by all β_i 's at *e*; see Fig. 1 for a quick example.

For any two vertices $u, v \in V$, we call any set consisting of the maximum number of pairwise edge-disjoint directed paths from u to v a set of *Menger's paths* from u to v. By Menger's theorem [6], the cardinality of Menger's paths from u to v is equal to the min-cut between u and v. Here, we remark that Ford-Fulkerson algorithm [1] can find the mincut and a set of Menger's paths from u to v in polynomial time.

Assume that G(V, E) has l sources S_1, S_2, \ldots, S_l and l distinct sinks R_1, R_2, \ldots, R_l . For $i = 1, 2, \ldots, l$, let c_i denote the min-cut between S_i and R_i , and let $\alpha_i = \{\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,c_i}\}$ denote a set of Menger's paths from S_i to R_i . We are interested in the number of mergings among paths from different α_i 's, denoted by $|G|_{\mathcal{M}}(\alpha_1, \alpha_2, \ldots, \alpha_l)$. The motivation for such consideration is more or less obvious in transportation networks: mergings among different groups of transportation paths can cause congestion, which may either decrease the whole network throughput or incur unnecessary cost. The connection between the number of mergings and the encoding complexity in computer networks, however, is a bit more subtle, which can be best illustrated by the following two examples in network coding theory (for a brief introduction to this theory, see [10]).

The first example is the famous "butterfly network" [5]. As depicted in Fig. 2(a), for the purpose of transmitting

Guangyue Han The University of Hong Kong email: ghan@hku.hk



Fig. 1. Paths β_1, β_2 merge at edge $A \to B$ and at merged subpath (or merging) $A \to B \to C \to D$, and paths $\beta_1, \beta_2, \beta_3$ merge at edge $B \to C$.

messages a, b simultaneously from S to R_1, R_2 , network encoding has to be done at node C. Another way to interpret the necessity of network coding at C (for simultaneous transmission to R_1 and R_2) is as follows: If transmission to R_2 is ignored, Menger's paths $S \rightarrow A \rightarrow R_1$ and $S \rightarrow B \rightarrow C \rightarrow D \rightarrow R_1$ can be used to transmit messages a, b from S to R_1 ; if transmission to R_1 is ignored, Menger's paths $S \rightarrow B \rightarrow R_2$ and $S \rightarrow A \rightarrow C \rightarrow D \rightarrow R_2$ to transmit messages a, b to R_2 . For simultaneous transmission to R_1 and R_2 , merging by these two groups of Menger's paths at $C \rightarrow D$ becomes a "bottle neck", therefore network coding at C is required to avoid the possible congestion.

The second example is concerned with two sessions of unicast in a network [8]. As shown in Fig. 2(b), S_1 is to transmit message a to R_1 using Menger's path $S_1 \rightarrow A \rightarrow$ $B \rightarrow E \rightarrow F \rightarrow C \rightarrow D \rightarrow R_1$. And S_2 is to transmit message b to R_2 using two Menger's paths $S_2 \rightarrow A \rightarrow$ $B \rightarrow C \rightarrow D \rightarrow R_2$ and $S_2 \rightarrow E \rightarrow F \rightarrow R_2$. Since mergings $A \rightarrow B$, $C \rightarrow D$ and $E \rightarrow F$ become bottle necks for simultaneous transmission of messages a and b, network coding at these bottle necks, as shown in Fig. 2(b), is performed to ensure the simultaneous message transmission.

Generally speaking, for a network with multiple groups of Menger's paths, each of which is used to transmit a set of messages to a particular sink, network encoding is needed at mergings by different groups of Menger's paths. As a result, the number of mergings is the number of network encoding operations required in the network. So, we are interested in the number of mergings among different groups of Menger's paths in such networks.

For the case where all sources in G are in fact identical, $M^*(G)$ is defined as the minimum number of mergings over all possible Menger's path sets α_i 's, i = 1, 2, ..., l, and $\mathcal{M}^*(c_1, c_2, ..., c_l)$ is defined as the supremum of $M^*(G)$ over all possible choices of such G. It is clear that $M^*(G)$ is the least number of network encoding operations required



Fig. 2. (a) Network coding on the butterfly network (b) Network coding on two sessions of unicast

for a given G, and $\mathcal{M}^*(c_1, c_2, \ldots, c_l)$ is the largest such number among all such G. As for \mathcal{M}^* , the authors of [2] use the idea of "subtree decomposition" to first prove that

$$\mathcal{M}^*(\underbrace{2,2,\ldots,2}_l) = l-1$$

Although their idea seems to be difficult to generalize to other parameters, it does allow us to gain deeper understanding about the topological structure of the graphs achieving l-1 mergings for this special case. It was first shown in [4] that $\mathcal{M}^*(c_1, c_2)$ is finite for all c_1, c_2 (see Theorem 22 in [4]), and subsequently $\mathcal{M}^*(c_1, c_2, \ldots, c_l)$ is finite for all c_1, c_2, \ldots, c_l .

For the case where all sources in G are distinct, M(G)is defined as the minimum number of mergings over all possible Menger's path sets α_i 's, i = 1, 2, ..., n, and $\mathcal{M}(c_1, c_2, \ldots, c_l)$ is defined as the supremum of M(G) over all possible choices of such G. In [8], a tight upper bound for the encoding complexity of a network with two unicast sessions is given, as a result of a more general treatment (to networks with two multicast sessions) by the authors. It is easy to see that for networks with multiple unicast sessions, \mathcal{M} with appropriate parameters can serve as an upper bound on network encoding complexity. It was first conjectured that $\mathcal{M}(c_1, c_2, \ldots, c_l)$ is finite in [9]. More specifically the authors proved that (see Lemma 10 in [9]) if $\mathcal{M}(c_1, c_2)$ is finite for all c_1, c_2 , then $\mathcal{M}(c_1, c_2, \ldots, c_l)$ is finite as well. Here, we remark that we have rephrased the work in [2], [4], [9], since all of them are done using very different languages from ours.

In [3], we have shown that for any c_1, c_2, \ldots, c_l , $\mathcal{M}(c_1, c_2, \ldots, c_l)$, $\mathcal{M}^*(c_1, c_2, \ldots, c_l)$ are both finite, and we further studied the behaviors of $\mathcal{M}, \mathcal{M}^*$ as functions of the min-cuts. In this paper, we focus our attention on the case when l = 2. More specifically, we give tighter bounds on $\mathcal{M}(c_1, c_2)$ and $\mathcal{M}^*(c_1, c_2)$, and exact values of them for certain special parameters c_1, c_2 .

To be consistent, we adopt the notational convention in [3]. For a path γ in G, let $a(\gamma), b(\gamma)$ denote the starting point and the ending point of γ , respectively; let $\gamma[s, t]$ denote the subpath of γ with the starting point s and the ending point t. For two distinct paths γ, π in G, we say γ is *smaller* than π (or, π is *larger* than γ) if there is a directed path from $b(\gamma)$ to $a(\pi)$; if γ, π and the connecting path from $b(\gamma)$ to $a(\pi)$ are subpaths of path β , we say γ is *smaller* than π on β . Note that this definition also applies to the case when paths degenerate to vertices/edges; in other words, in the definition, γ, π or the connecting path from $b(\gamma)$ to $a(\pi)$ can be vertices/edges in G, which can be viewed as degenerated paths. If $b(\gamma) = a(\pi)$, we use $\gamma \circ \pi$ to denote the path obtained by concatenating γ and π subsequently.

We say α_i is *reroutable* if there exists a different set of Menger's paths α'_i from S_i to R_i . And we say G is *reroutable* (with respect to $\alpha_1, \alpha_2, \ldots, \alpha_l$) if some $\alpha_i, i = 1, 2, \ldots, l$, is reroutable, otherwise G is said to be *non-reroutable*. Note that for a non-reroutable G, since the choice of α_i 's is unique, so we often write $|G|_{\mathcal{M}}(\alpha_1, \alpha_2, \ldots, \alpha_l)$ as $|G|_{\mathcal{M}}$ for notational simplicity. For the case l = 2, G is said to be a (c_1, c_2) -graph if every edge in G belongs to certain path in α_1 or α_2 (or, in loose terms, α_1 and α_2 "cover" the whole G).

For any m, n, consider the following procedure to "draw" an (m, n)-graph: for "fixed" edge-disjoint paths $\psi_1, \psi_2, \ldots, \psi_n$ from S_2 to R_2 , we extend edge-disjoint paths $\phi_1, \phi_2, \ldots, \phi_m$ from S_1 to merge with ψ -paths until we reach R_1 . More specifically, the procedure of extending ϕ -paths is done step by step, and for each step, we choose to extend one of the ϕ -paths to merge with one of the ψ -paths. Thus for each step, we have mn "strokes" to choose from the following set

$$\{(\phi_1,\psi_1),(\phi_1,\psi_2),\ldots,(\phi_m,\psi_{n-1}),(\phi_m,\psi_n)\},\$$

where (ϕ_i, ψ_j) means further extending path ϕ_i to merge with path ψ_j , while ensuring the new merged subpath is larger than any existing merged subpaths on path ψ_j . Apparently, the procedure, and thus the graph, is uniquely determined by the sequence of strokes (see Example 3), which will be referred to as a *merging sequence* of this (m, n)-graph. It is also easy to see that any (m, n)-graph can be generated by some merging sequence.

Example 1.1: Consider the following two graphs in Fig. 3 (here and hereafter, all the mergings are represented by solid dots instead). Listing the elements in the merging sequence, graph (a) can be described by $[(\phi_1, \psi_2), (\phi_2, \psi_1)]$, or alternatively $[(\phi_2, \psi_1), (\phi_1, \psi_2)]$. When the context is clear, we often omit ϕ, ψ in the merging sequence for notational simplicity. For example, graph (b) can be described by a merging sequence [(1, 1), (2, 1), (2, 2), (3, 2)]. Note that it cannot be described by [(1, 1), (2, 1), (3, 2), (2, 2)], since (3, 2) (or, more precisely, the merging corresponding to (3, 2)) is larger than (2, 2) on ψ_2 .

II. BOUNDS

A. An upper bound on $\mathcal{M}(m, n)$

Consider a non-reroutable (m, n)-graph G with two sources S_1, S_2 , two sinks R_1, R_2 , a set of Menger's paths $\phi = \{\phi_1, \phi_2, \dots, \phi_m\}$ from S_1 to R_1 , and a set of Menger's paths $\psi = \{\psi_1, \psi_2, \dots, \psi_n\}$ from S_2 to R_2 .



Fig. 3. Two examples of merging sequences

Consider the following procedure on G. Starting from S_1 , go along path ϕ_i until we reach a merged subpath, we then go against the associated ψ -path (corresponding to the merged subpath just visited) until we reach another merged subpath, we then go along the associated ϕ -path, ... Continue this procedure (of alternately going along ϕ -paths or going against ψ -paths until we reach a merged subpath) in the same manner as above, then the fact that G is non-reroutable and acyclic guarantees that eventually we will reach R_1 or S_2 . By sequentially listing all the terminal vertices of any merged subpaths visited, such a procedure produces a ϕ_i -AA-sequence. Apparently, there are $m \phi$ -AA-sequences.

Similarly, consider the following procedure on G. Starting from R_2 , go against path ψ_j until we reach a merged subpath, we then go along the associated ϕ -path (corresponding to the merged subpath just visited) until we reach another merged subpath, we then go against the associated ψ -path, ... Continue this procedure in the same manner, again, eventually, we are guaranteed to reach R_1 or S_2 . By sequentially listing all the terminal vertices of any merged subpaths visited, such a procedure produces a ψ_j -AA-sequence. Apparently, there are $n \psi$ -AA-sequences.

The *length* of an AA-sequence is defined to be the number of merged subpaths visited during the procedure. Then one checks that the number of mergings in G is half the sum of the lengths of all AA-sequences.

Example 2.1: Consider the graph in Fig. 4. Let " \Rightarrow " and " \Leftarrow " denote "going along" and "going against", respectively. By sequentially listing the terminal vertices of merged subpaths visited during the procedure, two ϕ -AA-sequences can be represented by $S_1 \Rightarrow a(\gamma_1) \Leftarrow S_2$ and $S_1 \Rightarrow a(\gamma_2) \Leftarrow b(\gamma_1) \Rightarrow a(\gamma_5) \Leftarrow b(\gamma_4) \Rightarrow R_1$. Similarly, two ψ -AA-sequences can be represented by $R_2 \Leftarrow b(\gamma_3) \Rightarrow R_1$ and $R_2 \Leftarrow b(\gamma_5) \Rightarrow a(\gamma_3) \Leftarrow b(\gamma_2) \Rightarrow a(\gamma_4) \Leftarrow S_2$.

One also checks that the number of mergings in G is 5, which is half of (1 + 4 + 1 + 4), the sum of lengths of all AA-sequences.

Lemma 2.2: 1. The shortest ϕ -AA-sequence (or ψ -AA-



Fig. 4. An example of AA-sequences

sequence) has length at most 1.

2. The longest ϕ -AA-sequence (or ψ -AA-sequence) has length at most mn.

Proof: **1.** Suppose, by contradiction, that the shortest ϕ -AA-sequence has length at least 2. Pick any ϕ -path, say ϕ_{i_0} . Assume that ϕ_{i_0} first merges with ψ_{j_0} at merged subpath γ_{i_0,j_0} . Since the ϕ_{i_0} -AA-sequence has length at least 2, there exists a ϕ -path, say ϕ_{i_1} , such that ϕ_{i_1} has a merged subpath, say ξ_{i_1,j_0} , smaller than γ_{i_0,j_0} on ψ_{j_0} . Now assume that ϕ_{i_1} first merges with ψ_{j_1} at merged subpath γ_{i_1,j_1} , then similarly there exists a ϕ -path, say ξ_{i_2,j_1} , smaller than γ_{i_1,j_1} on ψ_{j_1} . Continue this procedure in the similar manner to obtain ψ_{j_2} , γ_{i_2,j_2} , ϕ_{i_3} , ξ_{i_3,j_2} , ψ_{j_3} , γ_{i_3,j_3} , ϕ_{i_4} , ξ_{i_4,j_3} , ... Apparently, there exists k < l such that $i_l = i_k$. One then checks that

$$\phi_{i_k}[a(\gamma_{i_k,j_k}), a(\xi_{i_l,j_{l-1}})] \circ \psi_{j_{l-1}}[a(\xi_{i_l,j_{l-1}}), a(\gamma_{i_{l-1},j_{l-1}})]$$

$$p\phi_{i_{l-1}}[a(\gamma_{i_{l-1},j_{l-1}}), a(\xi_{i_{l-1},j_{l-2}})] \circ \psi_{j_{l-2}}[a(\xi_{i_{l-1},j_{l-2}}), a(\gamma_{i_{l-2},j_{l-2}})]$$

$$p\circ \cdots \circ \phi_{i_{k+1}}[a(\gamma_{i_{k+1},j_{k+1}}), a(\xi_{i_{k+1},j_k})] \circ \psi_{j_k}[a(\xi_{i_{k+1},j_k}), a(\gamma_{i_k,j_k})]$$

constitutes a cycle, which contradicts the assumption that G is acyclic.

A parallel argument can be applied to the shortest ψ -AA-sequence.

2. By contradiction, suppose that a ϕ -AA-sequence has no less than mn+1 mergings. Then by the pigeonhole principle, at least two of the mergings are associated with the same pair of ϕ -path and ψ -path. As in the proof of Lemma 2.7 in [3], one can check that G is reroutable, which is a contradiction.

A parallel argument can be applied to the longest ψ -AA-sequence.

Improving the upper bound mn(m+n)/2 derived in [3], the following theorem immediately follows from the fact that the number of mergings in G is half the sum of the lengths of all AA-sequences that

Theorem 2.3:

$$\mathcal{M}(m,n) \le mn(m+n-2)/2 + 1.$$

B. An upper bound on $\mathcal{M}^*(m,m)$

Consider two non-reroutable (m, m)-graph $G^{(1)}, G^{(2)}$. For j = 1, 2, assume that $G^{(j)}$ has one source $S^{(j)}$, two sinks $R_1^{(j)}, R_2^{(j)}$. Let $\phi^{(j)} = \{\phi_1^{(j)}, \phi_2^{(j)}, \ldots, \phi_m^{(j)}\}$ denote the set of Menger's paths from $S^{(j)}$ to $R_1^{(j)}$ and $\psi^{(j)} = \{\psi_1^{(j)}, \psi_2^{(j)}, \ldots, \psi_m^{(j)}\}$ denote the set of Menger's paths from $S^{(j)}$ to $R_2^{(j)}$. Without loss of generality (see Proposition 3.6 of [3]), we assume that, for $1 \le i \le m$, paths $\phi_i^{(j)}$ and $\psi_i^{(j)}$ share a subpath starting from $S^{(j)}$.

Now, consider the following procedure of concatenating $G^{(1)}$ and $G^{(2)}$:

- 1) reverse the direction of each edge in $G^{(1)}$ to obtain a new graph $\hat{G}^{(1)}$ (for $1 \leq i \leq m$, path $\phi_i^{(1)}$ in $G^{(1)}$ becomes path $\hat{\phi}_i^{(1)}$ in $\hat{G}^{(1)}$ and path $\psi_i^{(1)}$ in $G^{(1)}$ becomes path $\hat{\psi}_i^{(1)}$ in $\hat{G}^{(1)}$);
- 2) split $S^{(1)}$ into m copies $S_1^{(1)}, S_2^{(1)}, \ldots, S_m^{(1)}$ in $\hat{G}^{(1)}$ such that paths $\hat{\phi}_i^{(1)}$ and $\hat{\psi}_i^{(1)}$ have the same ending point $S_i^{(1)}$; split $S^{(2)}$ into m copies $S_1^{(2)}, S_2^{(2)}, \ldots, S_m^{(2)}$ in $G^{(2)}$ such that paths $\phi_i^{(2)}$ and $\psi_i^{(2)}$ have the same starting point $S_i^{(2)}$;
- 3) for $1 \le i \le m$, identify $S_i^{(1)}$ and $S_i^{(2)}$.

Obviously, such procedure produces a (m, m)-graph with two distinct sources $R_1^{(1)}, R_2^{(1)}$, two distinct sinks $R_1^{(2)}, R_2^{(2)}$, a set of Menger's paths $\{\hat{\phi}_1^{(1)} \circ \phi_1^{(2)}, \hat{\phi}_2^{(1)} \circ \phi_2^{(2)}, \dots, \hat{\phi}_m^{(1)} \circ \phi_m^{(2)}\}$ from $R_1^{(1)}$ to $R_1^{(2)}$ and a set of Menger's paths $\{\hat{\psi}_1^{(1)} \circ \psi_1^{(2)}, \hat{\psi}_2^{(1)} \circ \psi_2^{(2)}, \dots, \hat{\psi}_m^{(1)} \circ \psi_m^{(2)}\}$ from $R_2^{(1)}$ to $R_2^{(2)}$; see Fig. 5 for an example. We then have the following lemma, whose proof is omitted due to the space limit.

Lemma 2.4: The concatenated graph as above is a non-reroutable (m, m)-graph with the number of mergings equal to $|G^{(1)}|_{\mathcal{M}} + |G^{(2)}|_{\mathcal{M}} + m$.

This following theorem then immediately follows.

Theorem 2.5:

$$\mathcal{M}(m,m) \ge 2\mathcal{M}^*(m,m) + m.$$

It follows from Theorem 2.3 and 2.5 that

Theorem 2.6:

$$\mathcal{M}^*(m,m) \le (m-1)^2(m+1)/2$$

Here, we remind the reader that, by Proposition 3.6 in [3], $\mathcal{M}^*(m,n) = \mathcal{M}^*(m,m)$ for any $m \leq n$.

C. A lower bound on $\mathcal{M}^*(m,m)$

In this section, we will construct a non-reroutable (m, m)graph $\mathcal{F}(m, m)$ with one source S, two sinks R_1, R_2 , a set of Menger's paths $\phi = \{\phi_0, \phi_1, \dots, \phi_{m-1}\}$ from S to R_1 , a set of Menger's paths $\psi = \{\psi_0, \psi_1, \dots, \psi_{m-1}\}$ from S to R_2 and $(m-1)^2$ mergings for any positive integer m, thus giving a lower bound on $\mathcal{M}^*(m, m)$.

The graph $\mathcal{F}(m,m)$ can be described as follows: for each $0 \leq i \leq m-1$, paths ϕ_i and ψ_i share a maximal subpath starting from S, say Q_i . After Q_{m-1} , path ϕ_{m-1} does not merge any more, directly "flowing" to R_1 ; after Q_0 , path ψ_0 does not merge any more, directly "flowing" to R_2 . Then the rest of the graph can be determined how paths



Fig. 5. Concatenation of two (3, 3)-graphs

 $\phi_0, \phi_1, \dots, \phi_{m-2}$ merge with $\psi_1, \psi_2, \dots, \psi_{m-1}$. In more detail, for a given m, we define

$$U = \{U_{i,j} = i(2m - i - 2) + j : 0 \le i \le m - 2, \\ 1 \le j \le m - i - 1\}$$

and

$$V = \{V_{i,j} = i(2m - i - 3) + (m - 1) + j : 0 \le i \le m - 3, \\ 1 \le j \le m - i - 2\}.$$

It can be checked that all $U_{i,j}$'s, $V_{i,j}$'s are distinct and

$$U \cup V = \{1, 2, \dots, (m-1)^2\}.$$

Now we define a mapping $f : \{1, 2, ..., (m-1)^2\} \mapsto \{(i, j) : 0 \le i, j \le m-1\}$ by

$$f(k) = \begin{cases} (i,j) & \text{if } k = U_{i,j} \\ (m-1-j,m-1-i) & \text{if } k = V_{i,j} \end{cases}$$

Then a merging sequence of the rest of the graph can be defined as

$$\Omega = [\Omega_k : \Omega_k = f(k), 1 \le k \le (m-1)^2].$$

For example, $\mathcal{F}(4,4)$, as illustrated in Fig. 6, is determined by the merging sequence

$$\Omega = [(0,1), (0,2), (0,3), (2,3), (1,3), (1,1), (1,2), (2,2), (2,1)].$$

Now, we prove that

Lemma 2.7: $\mathcal{F}(m,m)$ is non-reroutable.

Proof: Let z = m - 1. Recall that for each $i = 0, 1, \ldots, z$, the maximal subpath shared (starting from S) by ϕ_i and ψ_i is labeled as Q_i . And for each $i, j = 0, 1, \ldots, z$, label each merging (i, j) in the merging sequence as $P_{i,j}$ (it can be easily checked that no two mergings share the same label).

We only prove that there is only one possible set of Menger's paths from S to R_1 . The uniqueness of Menger's



Fig. 6. Graph $\mathcal{F}(4,4)$ with 9 mergings

path set from S to R_2 can be established using a parallel argument.

Let α_1 be an arbitrary yet fixed set of Menger's paths from S to R_1 . It suffices to prove that α_1 is non-reroutable. Note that each path in α_1 must end with either $Q_z \to R_1$ or $P_{i,z-i} \to R_1$, $i = 0, 1, \ldots, z-1$ (here and hereafter, slightly abusing the notations " \to " and " \leftarrow ", for paths (or vertices) A_1, A_2, \ldots, A_k , we use $A_1 \to A_2 \to \cdots \to A_k$ or $A_k \leftarrow \cdots \leftarrow A_2 \leftarrow A_1$ to denote the unique path consisting of A_1, A_2, \ldots, A_k and the unique path from A_i to A_{i+1} for all i). In α_1 , label the Menger's path ending with $P_{i,z-i} \to$ R_1 as the *i*-th Menger's path for $0 \le i \le z-1$, and the Menger's path ending with $Q_z \to R_1$ as the *z*-th one.

It is obvious that in $\mathcal{F}(m,m)$, there is only one path ending with $Q_z \to R_1$, which implies that the z-th Menger's path in α_1 is "fixed" (as $S \to Q_z \to R_1$); or, more rigorously, for any set of Menger's paths α'_1 , the z-th Menger's path in α'_1 is the same as the z-th one in α_1 . So, for the purpose of choosing other Menger's paths, all the edges on $S \to Q_z \to R_1$ are "occupied". It then follows that, in α_1 , $P_{0,z}$ must "come" from $P_{0,z-1}$; more precisely, in $\alpha_1, P_{0,z-1}$ is smaller than $P_{0,z}$ on the 0-th path and there is no other merging between them on this path. Now, all the edges on $P_{0,z-1} \to P_{0,z} \to R_1$ are occupied.

Inductively, only considering unoccupied edges, one can check that for $0 \leq i \leq z-2$, $P_{i,z-i}$ must come from $P_{i,z-i-1}$; in other words, for $0 \leq i \leq z-2$, the *i*-th Menger's path must end with $P_{i,z-i-1} \rightarrow P_{i,z-i} \rightarrow R_1$. It then follows that the (z-1)-th Menger's path must come from $P_{z-1,2} \leftarrow P_{z-1,3} \leftarrow \cdots \leftarrow P_{z-1,z} \leftarrow Q_{z-1}$; so, the (z-1)-th Menger's path is fixed as $S \rightarrow Q_{z-1} \rightarrow P_{z-1,z} \rightarrow P_{z-1,z} \rightarrow P_{z-1,z} \rightarrow P_{z-1,z} \rightarrow P_{z-1,z} \rightarrow P_{z-1,z}$.

We now proceed by induction on j, j = z-2, z-3, ..., 1. Suppose that, for $j + 1 \le i \le z$, the *i*-th Menger's path is already fixed (and hence the edges on these paths are all occupied), and for $0 \le i \le j$, the *i*-th Menger's path ends with $P_{i,j-i+1} \rightarrow P_{i,j-i+2} \rightarrow \cdots \rightarrow P_{i,z-i} \rightarrow R_1$ (so, the edges on these paths are all occupied). Only considering the unoccupied edges, one checks that for $0 \le i \le j - 1$, $P_{i,j-i+1}$ must come from $P_{i,j-i}$. It then follows that the *j*-th Menger's path, which ends with $P_{j,1} \to P_{j,2} \to \cdots \to$ $P_{j,z-j} \to R_1$, must come from $P_{j,z-j+1} \leftarrow P_{j,z-j+2} \leftarrow$ $\cdots \leftarrow P_{j,z} \leftarrow Q_j$. So, the *j*-th Menger's path can now be fixed as $S \to Q_j \to P_{j,z} \to P_{j,z-1} \to \cdots \to P_{j,z-j+1} \to$ $P_{j,1} \to P_{j,2} \to \cdots \to P_{j,z-j} \to R_1$. Now, for $j \le i \le z$, the *i*-th Menger's path is fixed, and for $0 \le i \le j-1$, the *i*-th Menger's path must end with $P_{i,j-i} \to P_{i,j-i+1} \to \cdots \to$ $P_{i,z-i} \to R_1$.

It follows from the above inductive argument that for $1 \leq i \leq z$, the *i*-th Menger's path is fixed, and the 0-th Menger's path must end with $P_{0,1} \rightarrow P_{0,2} \rightarrow \cdots \rightarrow P_{0,z} \rightarrow R_1$. One then checks that the $P_{0,1}$ must come from Q_0 , which implies that the 0-th Menger's path is fixed as $S \rightarrow Q_0 \rightarrow P_{0,1} \rightarrow P_{0,2} \rightarrow \cdots \rightarrow P_{0,z} \rightarrow R_1$. The proof of uniqueness of Menger's path set from S to R_1 is then complete. The above lemma then immediately implies that

Theorem 2.8:

$$\mathcal{M}^*(m,m) \ge (m-1)^2$$

D. A lower bound on $\mathcal{M}(m,n)$

Consider the following (m,m)-graph $\mathcal{E}(m,m)$ with sources S_1, S_2 , sinks R_1, R_2 , a set of Menger's paths $\phi = \{\phi_1, \phi_2, \ldots, \phi_m\}$ from S_1 to R_1 , a set of Menger's paths $\psi = \{\psi_1, \psi_2, \ldots, \psi_m\}$ from S_2 to R_2 , and a merging sequence $\Omega = [\Omega_k : 1 \le k \le 2m^2 - 3m + 2]$, where

$$\Omega_k = \begin{cases} ([j-i]_m, i+1) & \text{if } k = 2i(m-1)+j \\ & \text{for } (0 \le i \le m-1, 1 \le j \le m-1) \\ & \text{or } (i = m-1, j = m) \\ (m-i, [i-j+2]_m) & \text{if } k = (2i+1)(m-1)+j \\ & \text{for } 0 \le i \le m-2, 1 \le j \le m-1 \end{cases}$$

where, for any integer t, $[t]_m$ denotes the least positive residue of t modulo m. For a quick example, see $\mathcal{E}(3,3)$ in Fig. 7(a), whose merging sequence is

$$\begin{split} \Omega = & [(1,1),(2,1),(3,1),(3,3),(3,2),(1,2),(2,2),(2,1),\\ & (2,3),(3,3),(1,3)]. \end{split}$$

Then, one can check (proof omitted here due to the space limit)

Lemma 2.9: $\mathcal{E}(m,m)$ is non-reroutable.

Consider a non-reroutable (k, m)-graph $\mathcal{H}(k, m)$ with sources S'_1, S'_2 , sinks R'_1, R'_2 , a set of Menger's paths $\phi' = \{\phi'_1, \phi'_2, \ldots, \phi'_k\}$ from S'_1 to R'_1 , a set of Menger's paths $\psi' = \{\psi'_1, \psi'_2, \ldots, \psi'_m\}$ from S'_2 to R'_2 . For a fixed merging sequence of $\mathcal{H}(k, m)$, assume, without loss of generality, that the first element is (ϕ'_1, ψ'_m) . Next, we will "concatenate" $\mathcal{E}(m,m)$ and $\mathcal{H}(k,m)$ to obtain a new graph. In the following, by *splitting* a set of Menger's paths $\phi = \{\phi_1, \phi_2, \ldots, \phi_m\}$ from S_1 to R_1 , we mean splitting S_1 into m copies $S_1^{(1)}, S_1^{(2)}, \ldots, S_1^{(m)}$, and R_1 into $R_1^{(1)}, R_1^{(2)}, \ldots, R_1^{(m)}$ such that each newly obtained ϕ_i has starting point $S_1^{(i)}$ and ending point $R_1^{(i)}$; see Fig. 7(b) for an example.



Fig. 7. (a) Graph $\mathcal{E}(3,3)$ with 11 mergings (b) Split ϕ -paths in $\mathcal{E}(3,3)$

The concatenating procedure can be described as follows:

- 1) split ϕ, ψ, ϕ' and ψ' ;
- delete all edges on φ₁ and all edges on ψ_m, each of which is larger than (φ₁, ψ_m) to obtain new φ₁ and ψ_m;
- delete all edges on φ'₁ and all edges on ψ'_m, each of which is smaller than (φ'₁, ψ'_m) to obtain new φ'₁ and ψ'_m;
- concatenate φ₁ and φ'₁ to obtain φ₁ ∘ φ'₁ (so, necessarily, ψ_m and ψ'_m are concatenated and we obtain ψ_m ∘ ψ'_m);
- 5) for i = 1, 2, ..., m-1, concatenate ψ_i and ψ'_i to obtain $\psi_i \circ \psi'_i$;
- 6) identify all the starting points of ψ_i ∘ ψ'_i, for i = 1, 2, ..., m, and then all the ending points; identify all the starting points of φ₁ ∘ φ'₁, φ₂, φ₃, ..., φ_m, φ'₂, φ'₃, ..., φ'_k, and then all the ending points.

For example, in Fig. 8, we concatenate $\mathcal{E}(2,2)$ and a nonreroutable (2,2)-graph to obtain a (3,2)-graph. We have the following lemma, whose proof is omitted due to the space limit.

Lemma 2.10: The concatenated graph as above is a nonreroutable (k+m-1,m)-graph with the number of mergings equal to $|\mathcal{E}(m,m)|_{\mathcal{M}} + |\mathcal{H}(k,m)|_{\mathcal{M}} - 1$.

We are now ready for the following theorem, which gives us a lower bound on $\mathcal{M}(m, n)$.

Theorem 2.11:

$$\mathcal{M}(m,n) \ge 2mn - m - n + 1.$$

Proof: Without loss of generality, assume that $m \le n$. For $1 \le m' \le m$ and $1 \le n' \le n$, we will iteratively construct a sequence of non-reroutable (m', n')-graphs with 2m'n' - m' - n' + 1 mergings, which immediately implies the theorem.

First, for any k, $\mathcal{L}(1, k)$, a non-reroutable (1, k)-graph can be given by specifying its mergings sequence

$$\Omega = [(1,1), (1,2), \dots, (1,k)]$$

Next, consider the case $2 \le m \le n$. Assume that for any $m' \le n'$ such that $m' \le m$, $n' \le n$, however $(m', n') \ne m$



Fig. 8. Concatenation of $\mathcal{E}(2,2)$ and a non-reroutable (2,2)-graph

(m, n), we have constructed a non-reroutable (m', n')-graph, which is effectively a non-reroutable (n', m')-graph as well. We obtain a new (m, n)-graph through the following procedure:

- 1) if m = n, concatenate $\mathcal{E}(m,m)$ and an already constructed non-reroutable (1,m)-graph.
- 2) if m < n, concatenate $\mathcal{E}(m,m)$ and an already constructed non-reroutable (n m + 1, m)-graph.

For the first case, according to Lemma 2.10, the obtained graph is non-reroutable (m, m)-graph with the number of mergings

$$(2m^2 - 3m + 2) + m - 1 = 2m^2 - 2m + 1$$

Similarly, for the second case, the obtained graph is a non-reroutable (m, n)-graph with the number of mergings

 $(2m^2 - 3m + 2) + (2(n - m + 1)m - (n - m + 1) - m + 1) - 1$ = 2mn - m - n + 1.

We then have established the theorem.

Example 2.12: To construct a non-reroutable (4, 6)-graph with 39 mergings, one can concatenate $\mathcal{E}(4, 4)$ and a non-reroutable (3, 4)-graph, which can be obtained by concatenating $\mathcal{E}(3, 3)$ and a non-reroutable (2, 3)-graph. The latter can be obtained by concatenating $\mathcal{E}(2, 2)$ and a non-reroutable (2, 2)-graph. Finally, a non-reroutable (2, 2)-graph can be obtained by concatenating $\mathcal{E}(2, 2)$ and $\mathcal{L}(1, 2)$. One readily checks that the number of mergings in the eventually obtained graph is

$$\begin{aligned} |\mathcal{E}(4,4)|_{\mathcal{M}} + |\mathcal{E}(3,3)|_{\mathcal{M}} + |\mathcal{E}(2,2)|_{\mathcal{M}} + |\mathcal{E}(2,2)|_{\mathcal{M}} + |\mathcal{L}(1,2)|_{\mathcal{M}} - 4 \\ = 22 + 11 + 4 + 4 + 2 - 4 = 39. \end{aligned}$$

Remark 2.13: It has been established in [4] that

$$m(m-1)/2 \le \mathcal{M}^*(m,m) \le m^3.$$

Summarizing all the four bounds we obtain, we have

 $(m-1)^2 \le \mathcal{M}^*(m,m) \le (m-1)^2(m+1)/2,$ $2mn - m - n + 1 \le \mathcal{M}(m,n) \le mn(m+n-2)/2 + 1.$

III. EXACT VALUES

In this section, we give exact values of \mathcal{M} and \mathcal{M}^* for certain special parameters.

Theorem 3.1:

$$\mathcal{M}(3,3) = 13.$$

Sketch of the proof: Consider any non-reroutable (3,3)-graph. Using an exhaustive approach, one checks the longest AA-sequence in this graph has length at most 7. So, by Lemma 2.2, we have

$$\mathcal{M}(3,3) \le (7+7+1+7+7+1)/2 = 15.$$

It follows from Theorem 2.11 that $\mathcal{M}(3,3) \geq 13$, and we can obtain a non-reroutable (3,3)-graph with 13 mergings by concatenating $\mathcal{E}(3,3)$ and $\mathcal{L}(1,3)$.

We next show $\mathcal{M}(3,3)$ cannot be 15 or 14. Note that any non-reroutable graph having 15 mergings implies that its (ϕ -AA-sequence; ψ -AA-sequence) have lengths (7, 7, 1; 7, 7, 1), respectively, while 14 mergings implies that its (ϕ -AA-sequences; ψ -AA-sequences) have lengths (7, 6, 1; 7, 6, 1), (7, 7, 1; 7, 5, 1) or (7, 7, 1; 6, 6, 1), respectively. We call such implications *the AA-sequence requirements*. The idea is that we can first preprocess to eliminate many cases by checking if the AA-sequence requirements are satisfied, then we can exhaustively investigate all the remaining cases to prove $\mathcal{M}(3,3)$ cannot be equal to 14 or 15. The detailed proof is rather tedious and lengthy, and thus omitted.

Remark 3.2: Through exhaustive searching, we are able to compute exact values of \mathcal{M} and \mathcal{M}^* with some small parameters: $\mathcal{M}^*(4,4) = 9$, $\mathcal{M}^*(5,5) = 16$, $\mathcal{M}^*(6,6) = 27$, $\mathcal{M}(3,4) = 18$, $\mathcal{M}(3,5) = 23$, $\mathcal{M}(3,6) = 28$, $\mathcal{M}(4,4) = 27$.

Theorem 3.3:

$$\mathcal{M}(m,2) = 3m - 1.$$

Proof: We first show that $\mathcal{M}(m, 2) \geq 3m - 1$. Consider the following (m, 2)-graph specified by the following merging sequence (for a simple example, see Fig. 9(a)): $\Omega = [\Omega_k : 1 \leq k \leq 3m - 1]$, where

$$\Omega_k = \begin{cases} (1, [i]_2) & \text{if } k = 3i-2 \quad \text{for } 1 \le i \le m \\ (i+1, [i]_2) & \text{if } k = 3i-1 \quad \text{for } 1 \le i \le m-1 \\ (i+1, [i+1]_2) & \text{if } k = 3i \quad \text{for } 1 \le i \le m-1 \\ (1, [m+1]_2) & \text{if } k = 3m-1 \end{cases}$$

One checks that the above graph is non-reroutable with 3m-1 mergings, which implies that $\mathcal{M}(m,2) \geq 3m-1$.

Next, we show that $\mathcal{M}(m, 2) \leq 3m - 1$. Consider a non-reroutable (m, 2)-graph G with two sets of Menger's paths

$$\phi = \{\phi_1, \phi_2, \dots, \phi_m\}, \quad \psi = \{\psi_1, \psi_2\}.$$

Define

$$\Psi = \{(\lambda,\mu): \text{merging } \lambda \text{ is smaller than merging } \mu \text{ on }$$

some ϕ -path and there is no other merging between them on this path}.

Note that for any $(\lambda, \mu) \in \Psi$, λ, μ must belong to different ψ -paths. We say $(\lambda, \mu) \in \Psi$ is of *type I*, if λ belongs to



Fig. 9. (a) A non-reroutable (3, 2)-graph with 8 mergings (b) An example of (5, 2)-graph

 ψ_1 , and $(\lambda, \mu) \in \Psi$ is of *type II*, if λ belongs to ψ_2 . For any two different elements $(\lambda_1, \mu_1), (\lambda_2, \mu_2) \in \Psi$. We say $(\lambda_1, \mu_1) \prec (\lambda_2, \mu_2)$ if either (they are of the same type and λ_1 is smaller than λ_2) or (they are of different types and λ_1 is smaller than μ_2). One then checks that the relationship defined by \prec is a strict total order.

Letting r denote the number of elements in Ψ , we define

$$\Theta = (\Theta_1, \Theta_2, \dots, \Theta_r)$$

to be the sequence of the ordered (by \prec) elements in Ψ . Now we consecutively partition Θ into t "medium-blocks" B_1, B_2, \ldots, B_t , and further consecutively partition each B_i into g_i "mini-blocks" $B_{i,1}, B_{i,2}, \ldots, B_{i,g_i}$ such that

- for any i, j, the elements in $B_{i,j}$ are of the same type.
- for any $i, j, B_{i,j}$ is *linked* to $B_{i,j+1}$ in the following sense: let (λ_1, μ_1) denote the element with the largest second component in $B_{i,j}$ and let (λ_2, μ_2) denote the element with the smallest first component in $B_{i,j+1}$, then $\mu_1 = \lambda_2$.
- for any i, B_{i,g_i} is not linked to $B_{i+1,1}$.

A mini-block is said to be a *singleton* if it has only one element. We then have the following lemma.

Lemma 3.4: Between any two "adjacent" singletons (meaning there is no singleton between these two singletons) in a medium-block, there must exist a mini-block containing at least three elements.

Letting g denote the number of mini-blocks in Θ and r_i denote the number of elements in medium-block B_i for any i, we then have

$$g = g_1 + g_2 + \dots + g_t,$$

 $r = r_1 + r_2 + \dots + r_t.$

Suppose there are k singletons in Θ , then by Lemma 3.4, we can find (k-1) mini-blocks, each of which has at least three elements. Hence, for $1 \le i \le t$,

$$r_i \ge 1 \cdot k + 3 \cdot (k-1) + 2 \cdot [g_i - k - (k-1)] = 2g_i - 1, \quad (1)$$

which implies

$$r = \sum_{i=1}^{t} r_i \ge \sum_{i=1}^{t} (2g_i - 1) = 2g - t.$$
 (2)

For any two linked mini-blocks $B_{i,j}$ and $B_{i,j+1}$, let (λ_1, μ_1) denote the element with the largest second component in $B_{i,j}$, and let (λ_2, μ_2) denote the element with the smallest first component in $B_{i,j+1}$. By the definition (of two mini-blocks being linked), $\mu_1 = \lambda_2$, which means $B_{i,j}$ and $B_{i,j+1}$ share a common merging. Together with the fact that each element in Ψ is a pair of mergings, this further implies that the number of mergings in G is

$$|G|_{\mathcal{M}} = 2r - (g - t). \tag{3}$$

Notice that λ_1, μ_1, μ_2 belong to the same ϕ -path, and furthermore, there exists only one ϕ -path passing by both an element (more precisely, passing by both its mergings) in $B_{i,j}$ and an element in $B_{i,j+1}$. So, m, the number of ϕ -paths in G can be computed as

$$m = r - (g - t). \tag{4}$$

It then follows from (2), (3), (4) and the fact $t \ge 1$ that

$$m = r - g + t \ge (2g - t) - g + t = g$$
(5)

and furthermore

$$|G|_{\mathcal{M}} = 2r - g + t = 2m + g - t \le 2m + m - 1 = 3m - 1,$$
 (6)

which establishes the theorem.

Example 3.5: Consider the graph in Fig. 9(b) and assume the context is as in the proof of Theorem 3.3. Then we have,

$$\Psi = \{ (A, J), (B, K), (L, C), (K, D), (F, M), (E, N) \}.$$

Among all the elements in Ψ , (A, J), (B, K), (F, M) and (E, N) are of type I, and (L, C), (K, D) are of type II. It is easy to check that

$$\Theta = ((A, J), (B, K), (K, D), (L, C), (E, N), (F, M)),$$

which is partitioned into three mini-blocks ((A, J), (B, K)), ((K, D), (L, C)) and ((E, N), (F, M)). The first mini-block is linked to the second one, but the second one is not linked to the third, so Θ is partitioned into two medium-blocks:

$$((A, J), (B, K), (K, D), (L, C))$$
 and $((E, N), (F, M))$.

Remark 3.6: The result in Theorem 3.3 in fact has already been proved in [3] using a different approach. The proof in this paper, however, is more intrinsic in the sense that it reveals in greater depth the topological structure of non-reroutable (m, 2)-graphs achieving 3m - 1 mergings, and further helps to determine the number of such graphs.

Assume a non-reroutable (m, 2)-graph G has 3m - 1 mergings. One then checks that in the proof of Theorem 3.3, equalities hold for (6). It then follows that

- t = 1, namely, there is only one medium-block in Θ ; and
- equalities hold necessarily for (5), (2) and eventually (1), which further implies that between two adjacent

singletons, only one mini-block has three elements and any other mini-block has two elements.

Furthermore, one checks that

- for a mini-block with two elements $((\lambda_1, \mu_1), (\lambda_2, \mu_2))$, μ_2 is smaller than μ_1 ; and
- for a mini-block with three elements $((\lambda_1, \mu_1), (\lambda_2, \mu_2), (\lambda_3, \mu_3))$, either $(\mu_2$ is smaller than μ_3 and μ_3 is smaller than μ_1) or $(\mu_3$ is smaller than μ_1 and μ_1 is smaller than μ_2).

Assume that G is "reduced" in the sense that, other than S_1, S_2, R_1, R_2 , each vertex in G is a terminal vertex of some merging. The properties above allow us to count how many reduced non-reroutable (m, 2)-graphs (up to graph isomorphism) can achieve 3m - 1 mergings: suppose that there are k ($1 \le k \le \lfloor \frac{m+1}{2} \rfloor$) singletons in G, then necessarily, there are (k-1) three element mini-blocks and (m-2k+1) two element mini-blocks in Θ . It can be checked that the number of ways for these m mini-blocks to form a Θ for some (m, 2)-graph is $\binom{m}{2k-1}2^{k-1}$. This implies that the number of (m, 2)-graph, whose Θ consists of k singletons, (k-1) three element mini-blocks and (m-2k+1) two element mini-blocks is $\binom{m}{2k-1}2^{k-1}$. Through a computation summing over all feasible k, the number of reduced non-reroutable (m, 2)-graphs with 3m - 1 mergings can be computed as

$$\sum_{k=1}^{\frac{m+1}{2}} \binom{m}{2k-1} 2^{k-1} = \frac{1}{2\sqrt{2}} [(1+\sqrt{2})^m - (1-\sqrt{2})^m] = P_m,$$

where P_m is the *m*-th Pell number [7].

REFERENCES

- L. R. Ford, Jr. and D. R. Fulkerson, "Maximal Flow Through a Network," *Canadian J. of Math.*, vol. 8, Feb. 1956, pp. 399-404.
- [2] C. Fragouli and E. Soljanin, "Information Flow Decomposition for Network Coding," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, Mar. 2006, pp. 829-848.
- [3] G. Han, Menger's Paths with Minimum Mergings, arXiv: 0805.4059.
- [4] M. Langberg, A. Sprintson and J. Bruck, "The Encoding Complexity of Network Coding," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, Jun. 2006, pp. 2386-2397.
- [5] S.-Y. R. Li, R. W. Yeung and N. Cai, "Linear Network Coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, Feb. 2003, pp. 371-381.
 [6] K. Menger, "Zur allgemeinen Kurventhoerie," *Fundamenta Math.*, vol.
- [6] K. Menger, "Zur allgemeinen Kurventhoerie," Fundamenta Math., vol. 10, 1927, pp. 96-115.
- [7] C. Serkland, "Generating Identities for Pell Triples," *Fibonacci Quart.*, vol. 12, no. 2, Apr. 1974, pp. 121-128.
- [8] W. Song, K. Cai, R. Feng and R. Wang, Encoding Complexity for Intersession Network Coding with Two Simple Multicast Sessions, arXiv: 1007.2928.
- [9] A. Tavory, M. Feder and D. Ron, "Bounds on Linear Codes for Network Multicast," Electron. Colloq. on Computational Complexity, Rep. 33, 2003.
- [10] R. W. Yeung, S.-Y. R. Li, N. Cai and Z. Zhang, Network Coding Theory (Foundations and Trends in Communications and Information Theory), Now Publishers Inc., 2006.