| Title | A graph theoretical approach to network encoding complexity |
| :---: | :--- |
| Author（s） | Xu，EL；Shang，W；Han，G |
| Citation | The 2012 International Symposium on Information Theory and its <br> Applications（ISITA），Honolulu，HI．，28－31 October 2012．In ISITA <br> Proceedings，2012，p．396－400 |
| Issued Date | 2012 |
| URL | http：／／hdl．handle．net／10722／160280 |
| Rights | International Symposium on Information Theory and Its <br> Applications Proceedings．Copyright © IEEE． |

# A Graph Theoretical Approach to Network Encoding Complexity 

Easton Li Xu<br>The University of Hong Kong<br>email: xuli@hku.hk

Weiping Shang<br>Zhengzhou University<br>email: shangwp@zzu.edu.cn

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


#### Abstract

For an acyclic directed network with multiple pairs of sources and sinks and a group of edge-disjoint paths connecting each pair of source and sink, it is known that the number of mergings among different groups of edge-disjoint paths is closely related to network encoding complexity. Using this connection, we derive exact values of and bounds on 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) $e \in \bigcap_{i=1}^{k} \beta_{i}$,
2) there are at least two distinct edges $f, g \in E$ such that $f, g$ are immediately ahead of $e$ on some $\beta_{i}, \beta_{j}$, $i \neq j$, respectively.
We call the maximal subpath that starts with $e$ and is shared by all $\beta_{i}$ 's merged subpath (or simply merging) by all $\beta_{i}$ 's at $e$; see Figure 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 $v$.

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 $\alpha_{i}=\left\{\alpha_{i, 1}, \alpha_{i, 2}, \ldots, \alpha_{i, c_{i}}\right\}$ 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 $\alpha_{i}$ 's, denoted by $|G|_{\mathcal{M}}\left(\alpha_{1}, \alpha_{2}, \ldots, \alpha_{l}\right)$. In this paper, we count the number of mergings without multiplicity: all the mergings at the same edge will be counted as one merging.

The motivation for considerations of the number of mergings is more or less obvious in transportation networks: mergings among different groups of transportation paths can cause congestions, which may either decrease the whole network throughput or incur


Fig. 1. Paths $\beta_{1}, \beta_{2}$ merge at edge $A \rightarrow B$ and at merged subpath (or merging) $A \rightarrow B \rightarrow C \rightarrow D$, and paths $\beta_{1}, \beta_{2}, \beta_{3}$ merge at edge $B \rightarrow C$ and at merged subpath (or merging) $B \rightarrow C$.
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 three examples in network coding theory. Here, we remark that all computer networks considered in this paper have unit capacity on each link, and by encoding complexity, we refer to the number of encoding operations needed (as opposed to the time needed to perform encoding operations).

The first example is the "butterfly network" [5], as depicted in Figure 2(a). For the purpose of transmitting messages $a, b$ simultaneously from the sender $S$ to the receivers $R_{1}, R_{2}$, network encoding has to be done at node $C$. Another way to interpret the necessity of network coding at $C$ (for the simultaneous transmission to $R_{1}$ and $R_{2}$ ) is as follows: If the 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 the 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 $a, b$ from $S$ to $R_{2}$. For the simultaneous transmission to $R_{1}$ and $R_{2}$, merging by these two groups of Menger's paths at $C \rightarrow D$ becomes a "bottleneck", therefore network coding at $C$ is required to avoid possible congestions.
The second example is a variant of the classic butterfly network (see Example 17.2 of [13]; cf. the two-way channel in Page 519 of [1]) with two senders and two receivers, where the sender $S_{1}$ is attached to the receiver $R_{2}$ to form a group and the sender $S_{2}$ is attached to the receiver $R_{1}$ to form the other group. As depicted in Figure 2(b), the two groups wish to exchange messages $a$ and $b$ through the network. Similarly as in the first
example, the edge $A \rightarrow B$ is where the Menger's paths $S_{1} \rightarrow A \rightarrow B \rightarrow R_{1}$ and $S_{2} \rightarrow A \rightarrow B \rightarrow R_{2}$ merge with each other, which is a bottleneck for the simultaneous transmission of messages $a, b$. The simultaneous transmission is achievable if upon receiving the messages $a$ and $b$, network encoding is performed at the node $A$ and the newly derived message $a+b$ is sent over the channel $A B$.

The third example is concerned with two sessions of unicast in a network [7]. As shown in Figure 2(c), the sender $S_{1}$ is to transmit message $a$ to the receiver $R_{1}$ using Menger's path $S_{1} \rightarrow A \rightarrow B \rightarrow E \rightarrow F \rightarrow C \rightarrow$ $D \rightarrow R_{1}$. And the sender $S_{2}$ is to transmit message $b$ to the receiver $R_{2}$ 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 bottlenecks for simultaneous transmission of messages $a$ and $b$, network coding at these bottlenecks, as shown in Figure 2(c), 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 when all sources in $G$ are identical, we define $M^{*}(G)$ as the minimum of $|G|_{\mathcal{M}}\left(\alpha_{1}, \alpha_{2}, \ldots, \alpha_{l}\right)$ over all possible Menger's path sets $\alpha_{1}, \alpha_{2}, \ldots, \alpha_{l}$, and $\mathcal{M}^{*}\left(c_{1}, c_{2}, \ldots, c_{l}\right)$ as the supremum of $M^{*}(G)$ over all possible $G$ (with min-cuts $c_{1}, c_{2}, \ldots, c_{l}$ defined as above). It is clear that $M^{*}(G)$ is the least number of network encoding operations required for a given $G$, and $\mathcal{M}^{*}\left(c_{1}, c_{2}, \ldots, c_{l}\right)$ is the largest such number among all such $G$. For multicast networks (generalizations of the first example), $\mathcal{M}^{*}$ is in fact an upper bound on network coding complexity. As for $\mathcal{M}^{*}$, the authors of [2] used the idea of "subtree decomposition" to first prove that

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

It was first shown in [4] that $\mathcal{M}^{*}\left(c_{1}, c_{2}\right)$ is finite for all $c_{1}, c_{2}$ (see Theorem 22 in [4]), and subsequently $\mathcal{M}^{*}\left(c_{1}, c_{2}, \ldots, c_{l}\right)$ is finite for all $c_{1}, c_{2}, \ldots, c_{l}$. Some exact values of and bounds on $\mathcal{M}^{*}$ with special parameters are derived using a "line graph" approach in [12].

For the case when all sources in $G$ are distinct, $M(G)$ is defined as the minimum of $|G|_{\mathcal{M}}\left(\alpha_{1}, \alpha_{2}, \ldots, \alpha_{l}\right)$ over all possible Menger's path sets $\alpha_{i}$ 's, and $\mathcal{M}\left(c_{1}, c_{2}, \ldots, c_{l}\right)$ is defined as the supremum of $M(G)$ over all possible $G$. Again, the encoding idea for the second example can be easily generalized to networks,


Fig. 2. (a) Network coding on the butterfly network (b) Network coding on a variant of the butterfly network (c) Network coding on two sessions of unicast
where each receiver is attached to all senders except its associated one. It is clear that the number of mergings is a tight upper bound for the number of network encoding operations required. For networks with several unicast sessions, the authors of [7] gave an upper bound on the encoding complexity in a network with two unicast sessions. It is easy to see that for networks with multiple unicast sessions (straightforward generalizations of the third example), $\mathcal{M}$ with appropriate parameters can serve as an upper bound on network encoding complexity. It was first conjectured that $\mathcal{M}\left(c_{1}, c_{2}, \ldots, c_{l}\right)$ is finite in [8]. More specifically the authors proved that (see Lemma 10 in [8]) if $\mathcal{M}\left(c_{1}, c_{2}\right)$ is finite for all $c_{1}, c_{2}$, then $\mathcal{M}\left(c_{1}, c_{2}, \ldots, c_{l}\right)$ is finite as well. Here, we remark that we have rephrased the work in [2], [4], [8], since all of them are done using different languages from ours.

In [3], we have shown that for any $c_{1}, c_{2}, \ldots, c_{l}$, $\mathcal{M}^{*}\left(c_{1}, c_{2}, \ldots, c_{l}\right), \mathcal{M}\left(c_{1}, c_{2}, \ldots, c_{l}\right)$ are both finite, and we further studied the behaviors of $\mathcal{M}^{*}, \mathcal{M}$ as functions of the min-cuts. One novel aspect of our approach is that paths, rather than vertices and edges, are treated as "elementary" objects, which can be transformed to different paths through reroutings. The effectiveness of this approach is evidenced by our work [10], where exact values of bounds on $\mathcal{M}^{*}$ and $\mathcal{M}$ for certain parameters are derived.

The contribution of this paper can be summarized as follows:

- novel methods are used to derive the exact values of some $\mathcal{M}^{*}$ with two parameters (see Theorem III.1) and the exact values of some $\mathcal{M}$ with more than two parameters (see Theorems III.2, III.3, III.4, III.5).
- through a nontrivial refinement of the arguments in [10], we get tighter upper bounds on $\mathcal{M}^{*}$ and $\mathcal{M}$ (see Theorems IV.1, IV.2) and scaling law (see Theorems IV.3).
- we obtain inequality relationships between $\mathcal{M}^{*}$ and $\mathcal{M}$ (see Theorem V.1, V.2), and between $\mathcal{M}^{*}$ with two parameters and multiple parameters (see Theorem V.3), which may serve as a first step to understand the connections between single-source and multiple-source networks, and between two-
sink and multiple-sink networks, respectively.
- our constructive proofs reveal the topological structure of some worst case networks (in terms of the number of network encoding operations), which may shed some light on the implementation of efficient network coding strategies.
- the problems in this paper are of mathematical interest as well, which is evidenced by Theorem III.3, a dual result to the classical Turan's theorem [9].
Many proofs are shortened or omitted in this manuscript due to the space limit; we refer to [11] for more illustrative examples and detailed proofs.

In this paper, say $G$ is a $\left(c_{1}, c_{2}, \ldots, c_{l}\right)$-graph if every edge in $G$ belongs to some $\alpha_{i}$-path; or, in loose terms, all $\alpha_{i}$ 's "cover" the whole $G$. For a $\left(c_{1}, c_{2}, \ldots, c_{l}\right)$ graph, the number of mergings is equal to the number of vertices with in-degree at least 2 . It is clear that to compute $\mathcal{M}\left(c_{1}, c_{2}, \ldots, c_{l}\right)\left(\mathcal{M}^{*}\left(c_{1}, c_{2}, \ldots, c_{l}\right)\right)$, it is enough to consider all the $\left(c_{1}, c_{2}, \ldots, c_{l}\right)$-graphs with distinct (identical) sources. For a $\left(c_{1}, c_{2}, \ldots, c_{l}\right)$-graph $G$, we say $\alpha_{i}$ is reroutable if there exists a different set of Menger's paths $\alpha_{i}^{\prime}$ from $S_{i}$ to $R_{i}$, and we say $G$ is reroutable, if some $\alpha_{i}$ is reroutable. Note that for a non-reroutable $G$, the choice of $\alpha_{i}$ 's is unique, so we often write $|G|_{\mathcal{M}}\left(\alpha_{1}, \alpha_{2}, \ldots, \alpha_{l}\right)$ as $|G|_{\mathcal{M}}$ for notational simplicity.

## II. AA-SEQUENCES

Consider a non-reroutable $(m, n)$-graph $G$ with two sources $S_{1}, S_{2}$ (either distinct or identical), two distinct sinks $R_{1}, R_{2}$, a set of Menger's paths $\phi=$ $\left\{\phi_{1}, \phi_{2}, \ldots, \phi_{m}\right\}$ from $S_{1}$ to $R_{1}$, and a set of Menger's paths $\psi=\left\{\psi_{1}, \psi_{2}, \ldots, \psi_{n}\right\}$ from $S_{2}$ to $R_{2}$.

For the case when $S_{1}$ and $S_{2}$ are distinct, consider the following procedure on $G$. For each $i$, starting from $S_{1}$, go along path $\phi_{i}$ until we reach a merged subpath (or more precisely, the terminal vertex of a merged subpath), we then go against the associated $\psi$ path (corresponding to the merged subpath just visited) until we reach another merged subpath, we then go along the associated $\phi$-path, ... Continue this procedure (of alternately going along $\phi$-paths or going against $\psi$-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 merged subpaths visited, such a procedure produces a $\phi_{i}$-AA-sequence [10]. Apparently, there are $m \phi$-AAsequences. $\psi$-AA-sequences can be defined in a similar procedure as above except that we have to start from $R_{2}$ and go against $\psi$-path first. Apparently, there are $n$ $\psi$-AA-sequences.

The length of an AA-sequence $\pi$, denoted by $L(\pi)$, is defined to be the number of terminal vertices of merged subpaths visited during the procedure. Since each such
terminal vertex in an AA-sequence is associated with a path pair, equivalently, the length of an AA-sequence can be also defined as the number of the associated path pairs.

For the case when $S_{1}$ and $S_{2}$ are identical, by Proposition 3.6 in [3], we restrict our attention to the case when $m=n$. For the purpose of computing $\mathcal{M}^{*}(n, n)$, by the proof of Proposition 3.6 in [3], we can assume that paths $\phi_{i}$ and $\psi_{i}$ share a starting subpath (a maximal shared subpath by $\phi_{i}$ and $\psi_{i}$ starting from the source) for $i=1,2, \ldots, m$. Then, $\psi$-AA-sequences and their lengths can be similarly defined as in the case when $S_{1}$ and $S_{2}$ are distinct, except that we have to replace "merged subpath" by "merged subpath or starting subpath". (Here, let us note that the procedure of defining $\phi$ -AA-sequences does NOT carry over.) It can be checked that the existence of $m$ starting subpaths implies that any $\psi$-AA-sequence is of positive length and will always terminate at $R_{1}$.

Regarding the lengths of AA-sequences, we have the following lemmas.
Lemma II. 1 ([10]). For a non-reroutable graph $G$, the shortest $\phi-A A$-sequence ( $\psi-A A$-sequence) is of length at most 1.

And it can be readily verified that
Lemma II.2. For a non-reroutable graph $G$, any path pair occurs at most once in any given $A A$-sequence.

It turns out that the number of mergings is related to the lengths of AA-sequences.

Lemma II.3. For a non-reroutable $(m, n)$-graph $G$ with distinct sources,

$$
|G|_{\mathcal{M}}=\frac{1}{2} \sum_{\pi} L(\pi)
$$

for a non-reroutable $(n, n)$-graph $G$ with identical sources and $n$ starting subpaths,

$$
|G|_{\mathcal{M}}=\frac{1}{2}\left(\sum_{\pi} L(\pi)-n\right)
$$

where the two summations above are over all possible $A A$-sequences $\pi$.

## III. Exact Values

For $\mathcal{M}^{*}$ or $\mathcal{M}$ with two parameters, it has been known that $\mathcal{M}(1, n)=n, \mathcal{M}(2, n)=3 n-1, \mathcal{M}(3,3)=13$, $\mathcal{M}^{*}(2,2)=1, \mathcal{M}^{*}(3,3)=4$ (see [3], [10]). Computer simulations [10] suggest that $\mathcal{M}^{*}(4,4)=9$, the following theorem establishes this result with a rigorous proof.
Theorem III.1.

$$
\mathcal{M}^{*}(4,4)=9
$$

Proof: We can construct a non-reroutable (4,4)graph with 9 mergings. To prove the upper bound direction, consider a non-reroutable $(4,4)$-graph $G$ has one source $S$, two sinks $R_{1}, R_{2}$. Let $\phi=\left\{\phi_{1}, \phi_{2}, \phi_{3}, \phi_{4}\right\}$ and $\psi=\left\{\psi_{1}, \psi_{2}, \psi_{3}, \psi_{4}\right\}$ denote the set of Menger's paths from $S$ to $R_{1}$ and $R_{2}$, respectively. We assume that $\phi_{i}$ and $\psi_{i}$ share a starting subpath for $i=1,2,3,4$, and furthermore, $\psi_{1}, \phi_{4}$ do not merge with any other paths, and every other $\phi$-path or $\psi$-path merges at least once.

By Lemma II.1, the shortest $\psi$-AA-sequence is of length 1 ; and by Lemma II.2, the longest $\psi$-AA-sequence is of length at most 9 , and any other $\psi$-AA-sequence is of length at most 7 . We then deduce, by Lemma II.3, that

$$
|G|_{\mathcal{M}} \leq(9+7+7+1-4) / 2=10
$$

By contradiction, we can conclude that $|G|_{\mathcal{M}}$ cannot be 10 , whose proof is omitted.

The following theorem gives the exact value for $\mathcal{M}$ with three special-valued parameters.

## Theorem III.2.

$$
\mathcal{M}(1,2, n)= \begin{cases}4 n & \text { if } n=2,3 \\ 4 n+1 & \text { if } n=1 \text { or } n \geq 4\end{cases}
$$

The following theorem is, in a sense, a "dual" version of the classical Turan's theorem [9], and can be proven using similar ideas.

## Theorem III.3.

$$
\mathcal{M}(\underbrace{1,1, \ldots, 1}_{k})=\left\lfloor\frac{k^{2}}{4}\right\rfloor
$$

Proof: For the " $\geq$ " direction, by Proposition 2.12 of [3], we deduce that

$$
\mathcal{M}(\underbrace{1,1, \ldots, 1}_{k}) \geq \sum_{i \leq\lfloor k / 2\rfloor, j \geq\lfloor k / 2\rfloor+1} \mathcal{M}(1,1)=\left\lfloor\frac{k^{2}}{4}\right\rfloor
$$

To prove the " $\leq$ " direction, consider a non-reroutable $(\underbrace{1,1, \ldots, 1}_{k})$-graph $G$ with distinct sources and sets of Menger's paths $\left\{\beta_{1}\right\},\left\{\beta_{2}\right\}, \ldots,\left\{\beta_{k}\right\}$. It is easy to check that due to non-reroutability of $G$, any two $\beta$ paths can merge with each other at most once. Without loss of generality, assume that $\beta_{k}$ only merges with $\beta_{1}, \beta_{2}, \ldots, \beta_{j}$; and any other path $\beta_{i}, i \neq k$, merges at most $j$ times. Again, due to non-reroutability of $G$, there are no non- $\beta_{k}$-involved mergings among paths $\beta_{1}, \beta_{2}, \ldots, \beta_{j}$, where we say a merging at edge $e$ is $\beta_{k^{-}}$ involved if $e$ belongs to $\beta_{k}$. It then follows that any non-$\beta_{k}$-involved merging in $G$ must be associated with one of paths from $\beta_{j+1}, \ldots, \beta_{k-1}$, each of which merges at most $j$ times. We then conclude that

$$
|G|_{\mathcal{M}} \leq j+(k-j-1) j=(k-j) j \leq\left\lfloor\frac{k^{2}}{4}\right\rfloor
$$

We have also proven the following theorem.

## Theorem III.4.

$$
\mathcal{M}(\underbrace{1, \ldots, 1}_{k}, 2)= \begin{cases}3 k-1 & \text { if } k \leq 6 \\ \left\lfloor\frac{k^{2}}{4}\right\rfloor+k+2 & \text { if } k>6 .\end{cases}
$$

## Theorem III.5.

$$
\mathcal{M}(\underbrace{1,1, \ldots, 1}_{k}, n)=n k+\left\lfloor\frac{k^{2}}{4}\right\rfloor \text { for } n \geq \frac{3 k-1}{4} .
$$

## IV. Bounds

It has been established in [10] that

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

$2 m n-m-n+1 \leq \mathcal{M}(m, n) \leq m n(m+n-2) / 2+1$.
The following two theorems give tighter upper bounds on $\mathcal{M}^{*}(n, n)$ and $\mathcal{M}(m, n)$, respectively. Here, we remind the reader that, by Proposition 3.6 in [3], $\mathcal{M}^{*}(m, n)=$ $\mathcal{M}^{*}(n, n)$ for any $m \geq n$.

## Theorem IV.1.

$$
\mathcal{M}^{*}(n, n) \leq\left\lceil\frac{n}{2}\right\rceil\left(n^{2}-4 n+5\right)
$$

Proof: Consider any $(n, n)$-graph $G$ with one source $S$, sinks $R_{1}, R_{2}$, a set of Menger's paths $\phi=$ $\left\{\phi_{1}, \phi_{2}, \ldots, \phi_{n}\right\}$ from $S$ to $R_{1}$, a set of Menger's paths $\psi=\left\{\psi_{1}, \psi_{2}, \ldots, \psi_{n}\right\}$ from $S$ to $R_{2}$. We assume that, for $1 \leq i \leq n$, paths $\phi_{i}$ and $\psi_{i}$ share a starting subpath, and paths $\phi_{n}$ and $\psi_{1}$ do not merge with any other paths, directly flowing to the sinks (then, necessarily, each $\psi$-AA-sequence is of positive length, and by Lemma II.1, the shortest $\psi$-AA-sequence is of length 1 ). We say that the path pair $\left(\phi_{i}, \psi_{j}\right)$ is matched if $i=j$, otherwise, unmatched. Apparently, each starting subpath corresponds to a matched path pair; and among the set of all path pairs, each of which corresponds some merging in $G$, there are at most $(n-2)$ matched and at most $\left(n^{2}-3 n+3\right)$ unmatched.

We then consider the following two cases (note that they may not be mutually exclusive):

Case 1: there exists a shortest $\psi$-AA-sequence associated with a matched path pair. By Lemma II. 2 and the fact that each starting subpath corresponds to a matched path pair, there are at most $\left\lfloor\frac{n-1}{2}\right\rfloor$ mergings corresponding to this path pair, at most $\left\lfloor\frac{n-2}{2}\right\rfloor$ corresponding to any other matched, and at most $\left\lfloor\frac{n-1}{2}\right\rfloor$ mergings corresponding to any unmatched. So, the number of mergings is upper bounded by

$$
\begin{equation*}
\left\lfloor\frac{n-1}{2}\right\rfloor+(n-3)\left\lfloor\frac{n-2}{2}\right\rfloor+\left(n^{2}-3 n+3\right)\left\lfloor\frac{n-1}{2}\right\rfloor . \tag{1}
\end{equation*}
$$

Case 2: there exists a shortest $\psi$-AA-sequence associated with an unmatched path pair. Similarly as in Case 1, there are at most $\left\lfloor\frac{n}{2}\right\rfloor$ mergings corresponding to this
path pair, at most $\left\lfloor\frac{n-1}{2}\right\rfloor$ mergings corresponding to any other unmatched, and at most $\left\lfloor\frac{n-2}{2}\right\rfloor$ mergings corresponding to any matched. So, the number of mergings is upper bounded by

$$
\begin{equation*}
\left\lfloor\frac{n}{2}\right\rfloor+(n-2)\left\lfloor\frac{n-2}{2}\right\rfloor+\left(n^{2}-3 n+2\right)\left\lfloor\frac{n-1}{2}\right\rfloor \tag{2}
\end{equation*}
$$

Then $\mathcal{M}^{*}(n, n) \leq \max \{(1),(2)\}$. Straightforward computations then lead to the theorem.

Following the same spirit, we can prove the following theorem.
Theorem IV.2.

$$
\mathcal{M}(m, n) \leq(m+n-1)+(m n-2)\left\lfloor\frac{m+n-2}{2}\right\rfloor .
$$

It has been shown in [3] that for any $k$, there exists $C_{k}$ such that $\mathcal{M}(k, n) \leq C_{k} n$ for all $n$, where $C_{k}$ can be rather loose. The following result refines the above result for the case $k=3$.

## Theorem IV.3.

$$
\mathcal{M}(3, n) \leq 14 n
$$

## V. InEQUALITIES

We will establish some inequalities in this section.

## Theorem V.1.

$$
\mathcal{M}(n, n) \geq 2 \mathcal{M}^{*}(n, n)+n
$$

Proof: For $j=1,2$, we assume that a nonreroutable $(n, n)$-graph $G^{(j)}$ has one source $S^{(j)}$, two sinks $R_{1}^{(j)}, R_{2}^{(j)}$ with $\mathcal{M}^{*}(n, n)$ mergings. Let $\phi^{(j)}=$ $\left\{\phi_{1}^{(j)}, \phi_{2}^{(j)}, \ldots, \phi_{n}^{(j)}\right\}$ denote the set of Menger's paths from $S^{(j)}$ to $R_{1}^{(j)}$ and $\psi^{(j)}=\left\{\psi_{1}^{(j)}, \psi_{2}^{(j)}, \ldots, \psi_{n}^{(j)}\right\}$ denote the set of Menger's paths from $S^{(j)}$ to $R_{2}^{(j)}$. We assume that, for $1 \leq i \leq n$, paths $\phi_{i}^{(j)}$ and $\psi_{i}^{(j)}$ share a starting subpath.

Now, consider the following procedure of concatenating graphs $G^{(1)}$ and $G^{(2)}$ (see Figure 3 for an example where we concatenate two (3, 3)-graphs):

1) reverse the direction of each edge in $G^{(2)}$ to obtain a new graph $\widehat{G}^{(2)}$ (for $1 \leq i \leq n$, path $\phi_{i}^{(2)}$ in $G^{(2)}$ becomes path $\hat{\phi}_{i}^{(2)}$ in $\widehat{G}^{(2)}$ and path $\psi_{i}^{(2)}$ in $G^{(2)}$ becomes path $\hat{\psi}_{i}^{(2)}$ in $\widehat{G}^{(2)}$ );
2) split $S^{(1)}$ into $n$ copies $S_{1}^{(1)}, S_{2}^{(1)}, \ldots, S_{n}^{(1)}$ in $G^{(1)}$ such that paths $\phi_{i}^{(1)}$ and $\psi_{i}^{(1)}$ have the same starting point $S_{i}^{(1)}$; split $S^{(2)}$ into $n$ copies $S_{1}^{(2)}, S_{2}^{(2)}, \ldots, S_{n}^{(2)}$ in $\widehat{G}^{(2)}$ such that paths $\hat{\phi}_{i}^{(2)}$ and $\hat{\psi}_{i}^{(2)}$ have the same ending point $S_{i}^{(2)}$;
3) for $1 \leq i \leq n$, identify $S_{i}^{(1)}$ and $S_{i}^{(2)}$.

It can be verified that such procedure produces a non-reroutable $(n, n)$-graph with two distinct sources $R_{1}^{(2)}, R_{2}^{(2)}$, two sinks $R_{1}^{(1)}, R_{2}^{(1)}$, a set of Menger's paths


Fig. 3. Concatenation of two $(3,3)$-graphs
$\left\{\hat{\phi}_{1}^{(2)} \circ \phi_{1}^{(1)}, \hat{\phi}_{2}^{(2)} \circ \phi_{2}^{(1)}, \ldots, \hat{\phi}_{n}^{(2)} \circ \phi_{n}^{(1)}\right\}$ from $R_{1}^{(2)}$ to $R_{1}^{(1)}$ and a set of Menger's paths $\left\{\hat{\psi}_{1}^{(2)} \circ \psi_{1}^{(1)}, \hat{\psi}_{2}^{(2)} \circ\right.$ $\left.\psi_{2}^{(1)}, \ldots, \hat{\psi}_{n}^{(2)} \circ \psi_{n}^{(1)}\right\}$ from $R_{2}^{(2)}$ to $R_{2}^{(1)}$, where" "०" means "concatenated with". The theorem then immediately follows.

The following two theorems follow from more or less the same "concatenation" approach.

## Theorem V.2.

$\mathcal{M}(n, n) \geq \mathcal{M}^{*}(n+1, n+1)+\mathcal{M}^{*}(n-1, n-1)+(n-1)$.
Theorem V.3. For $n_{1} \leq n_{2} \leq \cdots \leq n_{k}$,

$$
\mathcal{M}^{*}\left(n_{1}, n_{2}, \ldots, n_{k}\right) \geq \sum_{i=1}^{k-1} \mathcal{M}^{*}\left(n_{i}, n_{i}\right)
$$

## REFERENCES

[1] T.M. Cover and J.A. Thomas. Elements of Information Theory, 2nd ed., New York: Wiley-Interscience, 2006.
[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. 10, 1927, pp. 96-115.
[7] W. Song, K. Cai, R. Feng and R. Wang, "Encoding Complexity for Intersession Network Coding with Two Simple Multicast Sessions," arXiv: 1007.2928.
[8] A. Tavory, M. Feder and D. Ron, "Bounds on Linear Codes for Network Multicast," Electron. Colloq. on Comput. Complexity, Rep. 33, 2003.
[9] P. Turan, "Eine Extremalaufgabe aus der Graphentheorie," Mat. Fiz. Lapok, vol. 48, 1941, pp. 436-452.
[10] L. Xu and G. Han, "Bounds and Exact Values in Network Encoding Complexity with Two Sinks," Proc. 49th Annu. Allerton Conf. on Commun., Control and Comput., 2011, pp. 1462-1469.
[11] L. Xu, W. Shang and G. Han, "A Graph Theoretical Approach to Network Encoding Complexity," arXiv: 1202.0747.
[12] S. Yang, "On the Structure of Multicast Networks," preprint, available at http://staff.ie.cuhk.edu.hk/־shyang/pub/reduced.pdf.
[13] R. W. Yeung, Information Theory and Network Coding, New York: Springer-Verlag, 2008.

