Network Coding Fundamentals

Network Coding Fundamentals

Christina Fragouli

École Polytechnique Fédérale de Lausanne (EPFL)
Switzerland
christina.fragouli@epfl.ch

Emina Soljanin

Bell Laboratories, Alcatel-Lucent
USA
emina@research.bell-labs.com

the essence of knowledge

Boston – Delft

Foundations and Trends® in Networking

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is C. Fragouli and E. Soljanin, Network Coding Fundamentals, Foundation and Trends® in Networking, vol 2, no 1, pp 1–133, 2007

Printed on acid-free paper

ISBN: 978-1-60198-032-8

Foundations and Trends® in Networking
Volume 2 Issue 1, 2007

Editorial Scope

Foundations and Trends® in Networking will publish survey and tutorial articles in the following topics:

- Ad Hoc Wireless Networks
- Sensor Networks
- Optical Networks
- Local Area Networks
- Satellite and Hybrid Networks
- Cellular Networks
- Internet and Web Services
- Protocols and Cross-Layer Design
- Network Coding
- Energy-Efficiency Incentives/Pricing/Utility-based
- Games (co-operative or not)
- Security
- Scalability
- Topology
- Control/Graph-theoretic models
- Dynamics and Asymptotic Behavior of Networks

Information for Librarians
Foundations and Trends® in Networking, 2007, Volume 2, 4 issues. ISSN paper version 1554-057X. ISSN online version 1554-0588. Also available as a combined paper and online subscription.

Foundations and Trends® in
Networking
Vol. 2, No. 1 (2007) 1–133

DOI: 10.1561/1300000003

Network Coding Fundamentals

Christina Fragouli[1] and Emina Soljanin[2]

[1] *École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, christina.fragouli@epfl.ch*
[2] *Bell Laboratories, Alcatel-Lucent, USA, emina@research.bell-labs.com*

Abstract

Network coding is an elegant and novel technique introduced at the turn of the millennium to improve network throughput and performance. It is expected to be a critical technology for networks of the future. This tutorial addresses the first most natural questions one would ask about this new technique: how network coding works and what are its benefits, how network codes are designed and how much it costs to deploy networks implementing such codes, and finally, whether there are methods to deal with cycles and delay that are present in all real networks. A companion issue deals primarily with applications of network coding.

Contents

1
Introduction

Networked systems arise in various communication contexts such as phone networks, the public Internet, peer-to-peer networks, ad-hoc wireless networks, and sensor networks. Such systems are becoming central to our way of life. During the past half a century, there has been a significant body of research effort devoted to the operation and management of networks. A pivotal, inherent premise behind the operation of all communication networks today lies in the way information is treated. Whether it is packets in the Internet, or signals in a phone network, if they originate from different sources, they are transported much in the same manner as cars on a transportation network of highways, or fluids through a network of pipes. Namely, independent information streams are kept separate. Today, routing, data storage, error control, and generally all network functions operate on this principle.

Only recently, with the advent of network coding, the simple but important observation was made that in communication networks, we can allow nodes to not only forward but also process the incoming independent information flows. At the network layer, for example, intermediate nodes can perform binary addition of independent bitstreams, whereas, at the physical layer of optical networks, intermediate nodes can superimpose incoming optical signals. In other words, data streams that are independently produced and consumed do not necessarily need to be kept separate when they are transported throughout the network: there are ways to combine and later extract independent information. Combining independent data streams allows to better tailor the information flow to the network environment and accommodate the demands of specific traffic patterns. This shift in paradigm is expected to revolutionize the way we manage, operate, and understand organization in networks, as well as to have a deep impact on a wide range of areas such as reliable delivery, resource sharing, efficient flow control, network monitoring, and security.

This new paradigm emerged at the turn of the millennium, and immediately attracted a very significant interest in both Electrical Engineering and Computer Science research communities. This is an idea whose time has come; the computational processing is becoming cheaper according to Moore's law, and therefore the bottleneck has shifted to network bandwidth for support of ever-growing demand in applications. Network coding utilizes cheap computational power to dramatically increase network throughput. The interest in this area continues to increase as we become aware of new applications of these ideas in both the theory and practice of networks, and discover new connections with many diverse areas (see Figure 1.1).

Throughout this tutorial we will discuss both theoretical results as well as practical aspects of network coding. We do not claim to exhaustively represent and reference all current work in network coding; the presented subjects are the problems and areas that are closer to our interests and offer our perspective on the subject. However, we did attempt the following goals:

(1) to offer an introduction to basic concepts and results in network coding, and
(2) to review the state of the art in a number of topics and point out open research directions.

We start from the main theorem in network coding, and proceed to discuss network code design techniques, benefits, complexity require-

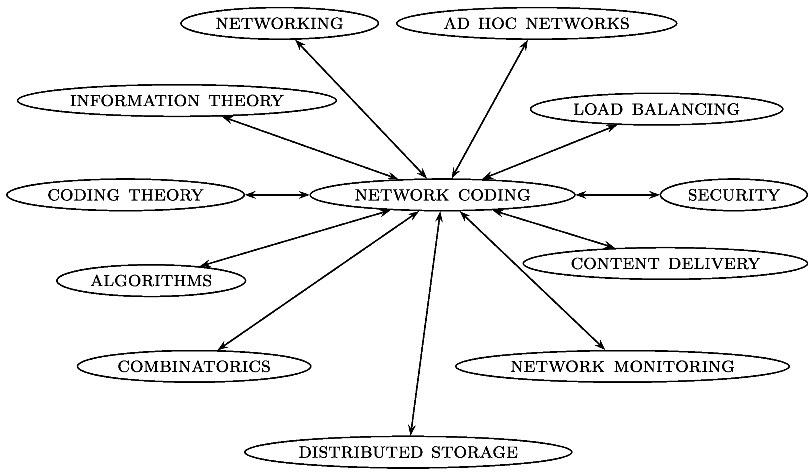

Fig. 1.1 Connections with other disciplines.

ments, and methods to deal with cycles and delay. A companion volume is concerned with application areas of network coding, which include wireless and peer-to-peer networks.

In order to provide a meaningful selection of literature for the novice reader, we reference a limited number of papers representing the topics we cover. We refer a more interested reader to the webpage www.networkcoding.info for a detailed literature listing. An excellent tutorial focused on the information theoretic aspects of network coding is provided in [49].

1.1 Introductory Examples

The following simple examples illustrate the basic concepts in network coding and give a preliminary idea of expected benefits and challenges.

1.1.1 Benefits

Network coding promises to offer benefits along very diverse dimensions of communication networks, such as throughput, wireless resources, security, complexity, and resilience to link failures.

Throughput

The first demonstrated benefits of network coding were in terms of throughput when multicasting. We discuss throughput benefits in Chapter 4.

Example 1.1. Figure 1.2 depicts a communication network represented as a directed graph where vertices correspond to terminals and edges correspond to channels. This example is commonly known in the network coding literature as the butterfly network. Assume that we have slotted time, and that through each channel we can send one bit per time slot. We have two sources S_1 and S_2, and two receivers R_1 and R_2. Each source produces one bit per time slot which we denote by x_1 and x_2, respectively (unit rate sources).

If receiver R_1 uses all the network resources by itself, it could receive both sources. Indeed, we could route the bit x_1 from source S_1 along the path $\{AD\}$ and the bit x_2 from source S_2 along the path $\{BC, CE, ED\}$, as depicted in Figure 1.2(a). Similarly, if the second receiver R_2 uses all the network resources by itself, it could also receive both sources. We can route the bit x_1 from source S_1 along the path $\{AC, CE, EF\}$, and the bit x_2 from source S_2 along the path $\{BF\}$ as depicted in Figure 1.2(b).

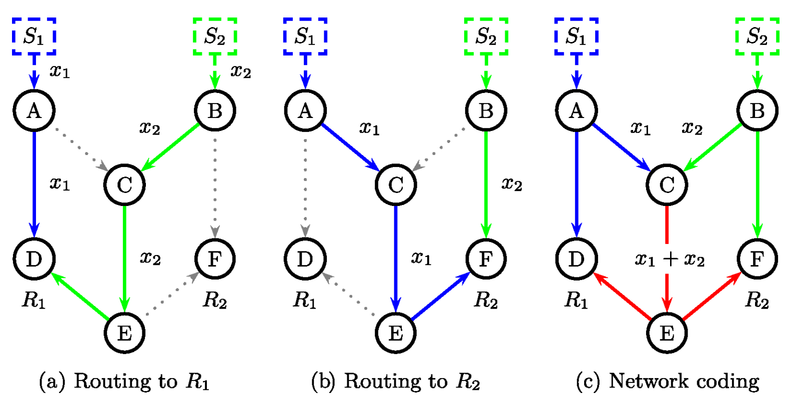

Fig. 1.2 The Butterfly Network. Sources S_1 and S_2 multicast their information to receivers R_1 and R_2.

Now assume that both receivers want to simultaneously receive the information from both sources. That is, we are interested in multicasting. We then have a "contention" for the use of edge CE, arising from the fact that through this edge we can only send one bit per time slot. However, we would like to simultaneously send bit x_1 to reach receiver R_2 and bit x_2 to reach receiver R_1.

Traditionally, information flow was treated like fluid through pipes, and independent information flows were kept separate. Applying this approach we would have to make a decision at edge CE: either use it to send bit x_1, or use it to send bit x_2. If for example we decide to send bit x_1, then receiver R_1 will only receive x_1, while receiver R_2 will receive both x_1 and x_2.

The simple but important observation made in the seminal work by Ahlswede *et al.* is that we can allow intermediate nodes in the network to process their incoming information streams, and not just forward them. In particular, node C can take bits x_1 and x_2 and `xor` them to create a third bit $x_3 = x_1 + x_2$ which it can then send through edge CE (the `xor` operation corresponds to addition over the binary field). R_1 receives $\{x_1,\, x_1 + x_2\}$, and can solve this system of equations to retrieve x_1 and x_2. Similarly, R_2 receives $\{x_2,\, x_1 + x_2\}$, and can solve this system of equations to retrieve x_1 and x_2.

The previous example shows that if we allow intermediate node in the network to combine information streams and extract the information at the receivers, we can increase the throughput when multicasting. This observation is generalized to the main theorem for multicasting in Chapter 2.

Wireless Resources

In a wireless environment, network coding can be used to offer benefits in terms of battery life, wireless bandwidth, and delay.

Example 1.2. Consider a wireless ad-hoc network, where devices A and C would like to exchange the binary files x_1 and x_2 using device B as a relay. We assume that time is slotted, and that a device can

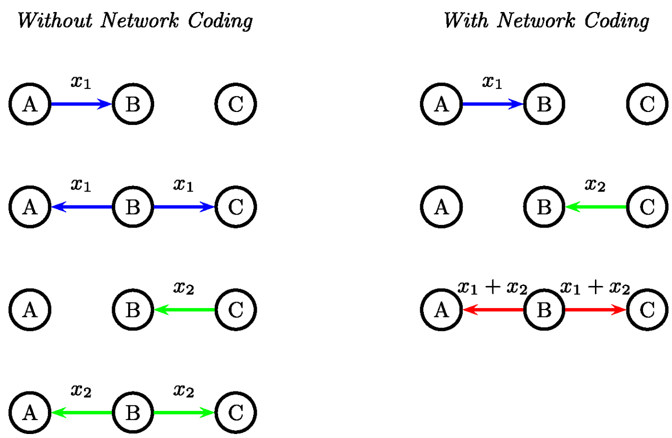

Fig. 1.3 Nodes A and C exchange information via relay B. The network coding approach uses one broadcast transmission less.

either transmit or receive a file during a timeslot (half-duplex communication). Figure 1.3 depicts on the left the standard approach: nodes A and C send their files to the relay B, who in turn forwards each file to the corresponding destination.

The network coding approach takes advantage of the natural capability of wireless channels for broadcasting to give benefits in terms of resource utilization, as illustrated in Figure 1.3. In particular, node C receives both files x_1 and x_2, and bitwise `xor`s them to create the file $x_1 + x_2$, which it then broadcasts to both receivers using a common transmission. Node A has x_1 and can thus decode x_2. Node C has x_2 and can thus decode x_1.

This approach offers benefits in terms of energy efficiency (node B transmits once instead of twice), delay (the transmission is concluded after three instead of four timeslots), wireless bandwidth (the wireless channel is occupied for a smaller amount of time), and interference (if there are other wireless nodes attempting to communicate in the neighborhood).

The benefits in the previous example arise from that broadcast transmissions are made maximally useful to all their receivers. Network coding for wireless is examined in the second part of this review. As we will discuss there, $x_1 + x_2$ is nothing but some type of binning or hashing for the pair (x_1, x_2) that the relay needs to transmit. Binning is not a new idea in wireless communications. The new element is that we can efficiently implement such ideas in practice, using simple algebraic operations.

Security

Sending linear combinations of packets instead of uncoded data offers a natural way to take advantage of multipath diversity for security against wiretapping attacks. Thus systems that only require protection against such simple attacks, can get it "for free" without additional security mechanisms.

Example 1.3. Consider node A that sends information to node D through two paths ABD and ACD in Figure 1.4. Assume that an adversary (Calvin) can wiretap a single path, and does not have access to the complementary path. If the independent symbols x_1 and x_2 are sent uncoded, Calvin can intercept one of them. If instead linear combinations (over some finite field) of the symbols are sent through the different routes, Calvin cannot decode any part of the data. If for example he retrieves $x_1 + x_2$, the probability of his guessing correctly x_1 equals 50%, the same as random guessing.

Similar ideas can also help to identify malicious traffic and to protect against Byzantine attacks, as we will discuss in the second part of this review.

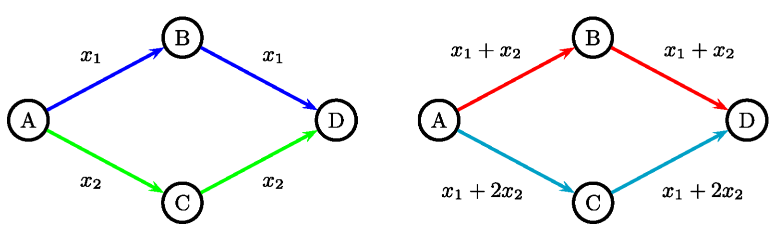

Fig. 1.4 Mixing information streams offers a natural protection against wiretapping.

1.1.2 Challenges

The deployment of network coding is challenged by a number of issues that will also be discussed in more detail throughout the review. Here we briefly outline some major concerns.

Complexity

Employing network coding requires nodes in the network to have additional functionalities.

Example 1.4. In Example 1.2, Figure 1.3, node B has additional memory requirements (needs to store file x_1 instead of immediately broadcasting it), and has to perform operations over finite fields (bitwise `xor` x_1 and x_2). Moreover, nodes A and C need to also keep their own information stored, and then solve a system of linear equations.

An important question in network coding research today is assessing the complexity requirements of network coding, and investigating tradeoffs between complexity and performance. We discuss such questions in Chapter 7.

Security

Networks where security is an important requirement, such as networks for banking transactions, need to guarantee protection against sophisticated attacks. The current mechanisms in place are designed around the assumption that the only eligible entities to tamper with the data are the source and the destination. Network coding on the other hand requires intermediate routers to perform operations on the data packets. Thus deployment of network coding in such networks would require to put in place mechanisms that allow network coding operations without affecting the authenticity of the data. Initial efforts toward this goal are discussed in the second part of the review.

Integration with Existing Infrastructure

As communication networks evolve toward an ubiquitous infrastructure, a challenging task is to incorporate the emerging technologies such as network coding, into the existing network architecture. Ideally, we would like to be able to profit from the leveraged functionalities network coding can offer, without incurring dramatic changes in the existing equipment and software. A related open question is, how could network coding be integrated in current networking protocols. Making this possible is also an area of current research.

References

[1] A. Agarwal and M. Charikar, "On the advantage of network coding for improving network throughput," *IEEE Information Theory Workshop*, San Antonio, Texas, 2004.

[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, pp. 1204–1216, July 2000.

[3] A. H. Ali, J. W. P. Hirschfeld, and H. Kaneta, "On the size of arcs in projective spaces," *IEEE Transaction on Information Theory*, vol. 41, pp. 1649–1656, September 1995.

[4] M. Ball, T. L. Magnanti, C. L. Monma, and G. L. Nemhauser, "Network Models," in *Handbooks in Operations Research and Management Science*, North Holland, 1994.

[5] J. Bang-Jensen, A. Frank, and B. Jackson, "Preserving and increasing local edge-connectivity in mixed graphs," *SIAM Journal on Discrete Mathematics*, vol. 8, pp. 155–178, 1995.

[6] Á. M. Barbero and Ø. Ytrehus, "Heuristic algorithms for small field multicast encoding," *2006 IEEE International Symposium Information Theory (ISIT'06)*, Chengdu, China, October 2006.

[7] A. M. Barbero and Ø. Ytrehus, "Cycle-logical treatment for cyclopathic networks," *Joint special issue of the IEEE Transactions on Information Theory and the IEEE/ACM Transaction on Networking*, vol. 52, pp. 2795–2804, June 2006.

[8] B. Bollobás, *Modern Graph Theory*. Springer-Verlag, 2002.

[9] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*. Amsterdam: North-Holland, 1979.

[10] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, March 2004.

[11] J. Cannons, R. Dougherty, C. Freiling, and K. Zeger, "Network routing capacity," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 777–788, March 2006.

[12] J. Cannons and K. Zeger, "Network coding capacity with a constrained number of coding nodes," *Allerton Conference on Communication, Control, and Computing Allerton Park*, Illinois, September 2006.

[13] Y. Cassuto and J. Bruck, "Network coding for non-uniform demands," *2005 IEEE International Symposium Information Theory (ISIT 2005)*, Adelaide, Australia, September 2005.

[14] C. Chekuri, C. Fragouli, and E. Soljanin, "On achievable information rates in single-source non-uniform demand networks," *IEEE International Symposium on Information Theory*, July 2006.

[15] C. Chekuri, C. Fragouli, and E. Soljanin, "On average throughput benefits and alphabet size for network coding," *Joint Special Issue of the IEEE Transactions on Information Theory and the IEEE/ACM Transactions on Networking*, vol. 52, pp. 2410–2424, June 2006.

[16] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," *Allerton Conference on Communication, Control, and Computing*, Monticello, IL, October 2003.

[17] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, New York, 1991.

[18] R. Diestel, *Graph Theory*. Springer-Verlag, 2000.

[19] R. Dougherty, C. Freiling, and K. Zeger, "Insufficiency of linear coding in network information flow," *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2745–2759, August 2005.

[20] P. Elias, A. Feinstein, and C. E. Shannon, "Note on maximum flow through a network," *IRE Transaction on Information Theory*, vol. 2, pp. 117–119, 1956.

[21] E. Erez and M. Feder, "Convolutional network codes," *IEEE International Symposium on Information Theory (ISIT)*, Chicago 2004.

[22] L. R. Ford Jr. and D. R. Fulkerson, "Maximal flow through a network," *Canadian Journal of Mathematics*, vol. 8, pp. 399–404, 1956.

[23] C. Fragouli and E. Soljanin, "A connection between network coding and convolutional codes," *IEEE International Conference on Communications (ICC)*, vol. 2, pp. 661–666, June 2004.

[24] C. Fragouli and E. Soljanin, "Information flow decomposition for network coding," *IEEE Transactions on Information Theory*, vol. 52, pp. 829–848, March 2006.

[25] N. Harvey, "Deterministic network coding by matrix completion," MS Thesis, 2005.

[26] T. Ho, R. Kötter, M. Médard, M. Effros, J. Shi, and D. Karger, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, pp. 4413–4430, October 2006.

[27] T. Ho, B. Leong, R. Kötter, and M. Médard, "Distributed Asynchronous Algorithms for Multicast Network Coding," *1st Workshop on Network Coding*, WiOpt 2005.

[28] S. Jaggi, Y. Cassuto, and M. Effros, "Low complexity encoding for network codes," in *Proceedings of 2006 IEEE International Symposium Information Theory (ISIT'06)*, Seattle, USA, July 2006.

[29] S. Jaggi, P. A. Chou, and K. Jain, "Low complexity algebraic network multicast codes," presented at *ISIT 2003*, Yokohama, Japan.

[30] S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Transaction on Information Theory*, vol. 51, no. 6, no. 6, pp. 1973–1982, 2005.

[31] M. Kim, C. W. Ahn, M. Médard, and M. Effros, "On minimizing network coding resources: An evolutionary approach," *Network Coding Workshop*, 2006.

[32] R. Kötter and M. Médard, "Beyond routing: An algebraic approach to network coding," *IEEE/ACM Transaction on Networking*, vol. 11, pp. 782–796, October 2003.

[33] G. Kramer and S. Savari, "Cut sets and information flow in networks of two-way channels," in *Proceedings of 2004 IEEE International Symposium Information Theory (ISIT 2004)*, Chicago, USA, June 27–July 2 2004.

[34] M. Langberg, A. Sprintson, and J. Bruck, "The encoding complexity of network coding," *Joint special issue of the IEEE Transactions on Information Theory and the IEEE/ACM Transaction on Networking*, vol. 52, pp. 2386–2397, 2006.

[35] A. R. Lehman and E. Lehman, "Complexity classification of network information flow problems," *SODA*, 2004.

[36] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, pp. 371–381, February 2003.

[37] Z. Li, B. Li, and L. C. Lau, "On achieving optimal multicast throughput in undirected networks," in *Joint Special Issue on Networking and Information Theory, IEEE Transactions on Information Theory (IT) and IEEE/ACM Transactions on Networking (TON)*, vol. 52, June 2006.

[38] D. S. Lun, N. Ratnakar, M. Médard, R. Kötter, D. R. Karger, T. Ho, E. Ahmed, and F. Zhao, "Minimum-cost multicast over coded packet networks," *IEEE Transactions on Information Theory*, vol. 52, pp. 2608–2623, June 2006.

[39] R. J. McEliece, "The algebraic theory of convolutional codes," in *Handbook of Coding Theory*, (V. Pless and W. C. Huffman, eds.), North Holland, October 1998.

[40] K. Menger, "Zur allgemeinen Kurventheorie," *Fundamenta Mathematicae*, vol. 10, pp. 95–115, 1927.

[41] A. Rasala-Lehman and E. Lehman, "Complexity classification of network information flow problems," *SODA*, pp. 142–150, 2004.

[42] S. Riis, "Linear versus nonlinear boolean functions in network flow," in *Proceedings of 38th Annual Conference on Information Sciences and Systems (CISS'04)*, Princeton, NJ, March 2004.

[43] P. Sanders, S. Egner, and L. Tolhuizen, "Polynomial time algorithms for network information flow," in *Proceedings of 15th ACM Symposium on Parallel Algorithms and Architectures*, 2003.

[44] A. Schrijver, *Theory of Linear and Integer Programming*. John Wiley & Sons, June 1998.

[45] J. T. Schwartz, "Fast probabilistic algorithms for verification of polynomial identities," *Journal of the ACM*, vol. 27, pp. 701–717, 1980.

[46] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*. Cambridge Univ. Press, Second Edition, September 2003.

[47] Y. Wu, P. A. Chou, and K. Jain, "A comparison of network coding and tree packing," *ISIT 2004*, 2004.

[48] R. W. Yeung, "Multilevel diversity coding with distortion," *IEEE Transaction on Information Theory*, vol. 41, pp. 412–422, 1995.

[49] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, "Network coding theory: A tutorial," *Foundation and Trends in Communications and Information Theory*, vol. 2, pp. 241–381, 2006.

[50] L. Zosin and S. Khuller, "On directed Steiner trees," in *Proceedings of the 13th Annual ACM/SIAM Symposium on Discrete Algorithms (SODA)*, pp. 59–63, 2002.