

UNIVERSITY OF CALIFORNIA, SAN DIEGO

**Linear Network Coding over Ring Alphabets**

A dissertation submitted in partial satisfaction of the  
requirements for the degree Doctor of Philosophy

in

Electrical Engineering  
(Communication Theory & Systems)

by

Joseph Michael Connelly

Committee in charge:

Professor Kenneth Zeger, Chair  
Professor Young-Han Kim  
Professor Daniel Rogalski  
Professor Paul Siegel  
Professor Lance Small

2018

Copyright

Joseph Michael Connelly, 2018

All rights reserved.

The dissertation of Joseph Michael Connelly is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

---

---

---

---

---

Chair

University of California, San Diego

2018

## TABLE OF CONTENTS

|  |      |
|--|------|
| Signature Page . . . . .                               | iii  |
| Table of Contents . . . . .                            | iv   |
| List of Figures . . . . .                              | vii  |
| Acknowledgements . . . . .                             | viii |
| Vita . . . . .   | ix   |
| Abstract of the Dissertation . . . . .                 | x    |
| Chapter 1 Introduction . . . . .                       | 1    |
| 1.1 Network Coding . . . . .                           | 1    |
| 1.2 Group, Ring, and Field Alphabets . . . . .         | 2    |
| 1.3 Scalar Linear Codes over Finite Fields . . . . .   | 5    |
| 1.4 Vector Linear Codes over Finite Fields . . . . .   | 7    |
| 1.5 Linear Network Coding over Finite Rings . . . . .  | 9    |
| 1.6 Overview . . . . .                                 | 10   |
| References . . . . .                                   | 11   |
| Chapter 2 Scalar Codes and Commutative Rings . . . . . | 13   |
| 2.1 Introduction . . . . .                             | 14   |
| 2.1.1 Network Model . . . . .                          | 14   |
| 2.1.2 Related Work . . . . .                           | 15   |
| 2.1.3 Our Contributions . . . . .                      | 17   |
| 2.2 Ring Dominance . . . . .                           | 20   |
| 2.2.1 Fundamental Ring Comparisons . . . . .           | 21   |
| 2.2.2 Minimizing Alphabet Size . . . . .               | 25   |
| 2.2.3 Direct Products of Rings . . . . .               | 26   |
| 2.2.4 The $n$ -Choose-Two Networks . . . . .           | 27   |
| 2.2.5 Rings of Size $p^2$ . . . . .                    | 30   |
| 2.3 Finite Field Dominance . . . . .                   | 31   |
| 2.3.1 Local Rings . . . . .                            | 33   |
| 2.3.2 Non-Power-of-Prime Size Rings . . . . .          | 35   |
| 2.4 Integer Partitions . . . . .                       | 37   |
| 2.4.1 Partition Division . . . . .                     | 38   |
| 2.4.2 Characterizing Maximal Partitions . . . . .      | 38   |
| 2.4.3 Maximal Partitions of Short Length . . . . .     | 41   |
| 2.5 Maximal Commutative Rings . . . . .                | 42   |
| 2.5.1 Multiple Maximal Rings of a Given Size . . . . . | 47   |
| 2.6 Open Questions . . . . .                           | 49   |
| References . . . . .                                   | 51   |

|           |   |     |
|-----------|---|-----|
| Chapter 3 | Vector Codes and Non-Commutative Rings . . . . .                    | 53  |
|           | 3.1 Introduction . . . . .  | 54  |
|           | 3.1.1 Linear Codes Over Modules . . . . .                           | 54  |
|           | 3.1.2 Our Contributions . . . . .                                   | 56  |
|           | 3.1.3 Comparisons of Modules . . . . .                              | 58  |
|           | 3.2 Commutative and Non-Commutative Rings . . . . .                 | 63  |
|           | 3.2.1 Modules and Vector Linear Codes . . . . .                     | 65  |
|           | 3.3 The Dim- $k$ Networks . . . . .                                 | 70  |
|           | 3.3.1 Insufficiency of Commutative Rings . . . . .                  | 76  |
|           | 3.4 Modules of the Same Size . . . . .                              | 79  |
|           | 3.4.1 Commutative Rings . . . . .                                   | 80  |
|           | 3.4.2 Non-Commutative Rings . . . . .                               | 82  |
|           | 3.5 Concluding Remarks . . . . .                                    | 85  |
|           | 3.5.1 Summary of Results . . . . .                                  | 86  |
|           | 3.5.2 Open Questions . . . . .                                      | 87  |
|           | 3.A Proofs of Lemmas 3.4.12, 3.4.13, and 3.4.14 . . . . .           | 88  |
|           | References . . . . .  | 92  |
| Chapter 4 | Capacity and Achievable Rate Regions . . . . .                      | 93  |
|           | 4.1 Introduction . . . . .  | 94  |
|           | 4.1.1 Modules, Linear Functions, and Tensor Products . . . . .      | 95  |
|           | 4.1.2 Network Coding Model . . . . .                                | 100 |
|           | 4.1.3 Linearity over Finite Rings and Modules . . . . .             | 101 |
|           | 4.1.4 Rate Regions, Capacity, and Solvability . . . . .             | 101 |
|           | 4.1.5 Related Work . . . . .  | 102 |
|           | 4.1.6 Main Results . . . . .  | 104 |
|           | 4.2 Fractional and Vector Codes over Modules . . . . .              | 105 |
|           | 4.2.1 Fractional Equivalent Network . . . . .                       | 106 |
|           | 4.2.2 Fractional Dominance . . . . .                                | 110 |
|           | 4.2.3 Matrix Rings over Fields . . . . .                            | 112 |
|           | 4.3 Linear Rate Regions over Fields . . . . .                       | 114 |
|           | 4.3.1 Comparing Linear Rate Regions over Different Fields . . . . . | 115 |
|           | 4.4 Linear Rate Regions over Rings . . . . .                        | 118 |
|           | 4.4.1 Comparing Linear Capacities over Different Rings . . . . .    | 119 |
|           | 4.4.2 Asymptotic Solvability . . . . .                              | 121 |
|           | 4.5 Concluding Remarks . . . . .                                    | 121 |
|           | References . . . . .  | 122 |
| Chapter 5 | A Class of Non-Linearly Solvable Networks . . . . .                 | 125 |
|           | 5.1 Introduction . . . . .  | 126 |
|           | 5.1.1 Network Coding Model . . . . .                                | 126 |
|           | 5.1.2 Previous Work . . . . .                                       | 128 |

|           |   |     |
|-----------|---|-----|
| 5.1.3     | Our Contributions   | 130 |
| 5.1.4     | Preliminaries   | 133 |
| 5.2       | Network $\mathcal{N}_0(m)$  | 134 |
| 5.3       | Network $\mathcal{N}_1(m)$  | 137 |
| 5.4       | Network $\mathcal{N}_2(m, w)$   | 141 |
| 5.5       | Network $\mathcal{N}_3(m_1, m_2)$                                     | 149 |
| 5.6       | Network $\mathcal{N}_4(m)$  | 157 |
| 5.6.1     | Solvability of $\mathcal{N}_4(m)$                                     | 159 |
| 5.6.2     | Linear Solvability of $\mathcal{N}_4(m)$                              | 162 |
| 5.6.3     | Capacity and Linear Capacity of $\mathcal{N}_4(m)$                    | 163 |
| 5.6.4     | Size of $\mathcal{N}_4(m)$  | 164 |
| 5.7       | Open Questions  | 167 |
| 5.A       | Capacity Proofs of $\mathcal{N}_1, \mathcal{N}_2$ and $\mathcal{N}_3$ | 168 |
| 5.A.1     | $\mathcal{N}_1$ Capacity Proof  | 168 |
| 5.A.2     | $\mathcal{N}_2$ Capacity Proof  | 175 |
| 5.A.3     | $\mathcal{N}_3$ Capacity Proof  | 178 |
|           | References  | 185 |
| Chapter 6 | Big Picture Discussion  | 187 |
| 6.1       | Can a Network be Linearly Solvable over Rings but not Fields?         | 187 |
| 6.2       | What is the “Best” Alphabet of a Given Size for Linear Coding?        | 188 |
| 6.3       | What is the “Best” Alphabet for Linear Coding on a Given Network?     | 188 |
| 6.4       | Over What Alphabet Sizes is a Given Network Solvable?                 | 188 |
| 6.5       | Can the Linear Capacity of a Network be Increased Using Rings?        | 189 |

## LIST OF FIGURES

|             |   |     |
|-------------|---|-----|
| Figure 1.1: | The Butterfly Network . . . . .   | 2   |
| Figure 1.2: | The $n$ -Choose-Two Network . . . . .   | 6   |
| Figure 1.3: | The $M$ Network . . . . .   | 7   |
| Figure 1.4: | The Diabolical Network . . . . .  | 8   |
| Figure 2.1: | A summary of the results in this chapter for a fixed network . . . . .            | 19  |
| Figure 2.2: | A summary of the results in this chapter for a fixed alphabet size . . . . .      | 19  |
| Figure 2.3: | The Char- $m$ Network . . . . .   | 22  |
| Figure 2.4: | The $n$ -Choose-Two Network . . . . .   | 28  |
| Figure 2.5: | The Two-Six Network . . . . .   | 29  |
| Figure 2.6: | The maximal partitions of $k = 1, 2, \dots, 30$ under partition division. . . . . | 50  |
| Figure 3.1: | The Fano Network . . . . .  | 60  |
| Figure 3.2: | The $n$ -Choose-Two Network . . . . .   | 68  |
| Figure 3.3: | The Dim- $k$ Network . . . . .  | 70  |
| Figure 3.4: | The $M$ Network . . . . .   | 78  |
| Figure 3.5: | A trivial network . . . . .   | 82  |
| Figure 4.1: | The Butterfly Network . . . . .   | 105 |
| Figure 4.2: | The $(k_x, k_y, n)$ -Butterfly Network . . . . .                                  | 107 |
| Figure 4.3: | The Char- $m$ Network . . . . .   | 115 |
| Figure 5.1: | Summary of the networks constructed in this chapter . . . . .                     | 132 |
| Figure 5.2: | A network building block . . . . .  | 135 |
| Figure 5.3: | The network $\mathcal{N}_0(m)$ . . . . .  | 136 |
| Figure 5.4: | The network $\mathcal{N}_1(m)$ . . . . .  | 138 |
| Figure 5.5: | The network $\mathcal{N}_2(m, w)$ . . . . .                                       | 142 |
| Figure 5.6: | The network $\mathcal{N}_3(m_1, m_2)$ . . . . .                                   | 150 |

## ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor, Ken Zeger, for his guidance, support, and inspiration. I am indebted to him for the many opportunities he has presented me with and for his efforts to help me become a better researcher. Ken's passion for research, teaching, and mathematics is highly contagious, and I hope to maintain a similar enthusiasm throughout my career. I am grateful to Young-Han Kim, Paul Siegel, Dan Rogalski, and Lance Small for serving on my committee and taking the time to read and edit this dissertation. I thank all of the friends I have made and those whom I have worked with at UCSD for making graduate school a memorable and rewarding experience. I am thankful to Richard Sahara and Marc Riedel for both inspiring and encouraging me to pursue graduate education. I also thank Jon Hamkins for his mentorship and help in making my time at JPL as enjoyable as it was.

My parents have provided me with the means and the encouragement to pursue my goals, no matter where they take me. I am thankful for their unconditional support throughout my life, particularly over the past 5 years. Finally, I thank my fiancée Allison Flickinger, for her patience and her willingness to put up with me through the highs and lows of writing this dissertation. This work would not have been possible were it not for her love and unwavering support.

The chapters of this dissertation consist of published and submitted journal articles. The dissertation author was the primary investigator and author of each of these papers.

- Chapter 2 is a reprint of the material as it appears in J. Connelly and K. Zeger, "Linear network coding over rings – Part I: Scalar codes and commutative alphabets," *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 274 – 291, January 2018.
- Chapter 3 is a reprint of the material as it appears in J. Connelly and K. Zeger, "Linear network coding over rings – Part II: Vector codes and non-commutative alphabets," *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 292 – 308, January 2018.
- Chapter 4 has been submitted for publication of the material J. Connelly and K. Zeger, "Linear capacity of networks over ring alphabets."
- Chapter 5 is a reprint of the material as it appears in J. Connelly and K. Zeger, "A class of non-linearly solvable networks," *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 201 – 229, January 2017.

This work was supported, in part, by the National Science Foundation.



## VITA

|             |   |
|-------------|---|
| 2013        | Bachelor of Electrical Engineering, University of Minnesota Twin Cities   |
| 2013        | Bachelor of Computer Engineering, University of Minnesota Twin Cities   |
| 2013 – 2018 | Teaching Assistant, University of California, San Diego   |
| 2014 – 2017 | Graduate Student Researcher, University of California, San Diego  |
| 2016        | Master of Science in Electrical Engineering (Communication Theory & Systems),<br>University of California, San Diego    |
| 2016        | Graduate Student Intern, NASA Jet Propulsion Laboratory   |
| 2017        | Associate Instructor, University of California, San Diego   |
| 2018        | Doctor of Philosophy in Electrical Engineering (Communication Theory & Systems),<br>University of California, San Diego |
| 2018 –      | Developmental Engineer, Air Force Research Labs, New Mexico   |

## PUBLICATIONS

- J. Connelly and K. Zeger, “A class of non-linearly solvable networks,” *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, pp. 1964–1968, Barcelona, Spain, July 10-15 2016.
- J. Connelly, “Repeat-PPM super-symbol synchronization,” *IPN Progress Report* vol. 42, no. 207, November 2016.
- J. Connelly and K. Zeger, “A class of non-linearly solvable networks,” *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 201 – 229, January 2017.
- J. Connelly and K. Zeger, “Linear network coding over rings – Part I: Scalar codes and commutative alphabets,” *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 274 – 291, January 2018.
- J. Connelly and K. Zeger, “Linear network coding over rings – Part II: Vector codes and non-commutative alphabets,” *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 292 – 308, January 2018.
- J. Connelly and K. Zeger, “Linear capacity of networks over ring alphabets,” submitted to *IEEE Transactions on Information Theory*, June 4, 2017, revised January 29, 2018.

ABSTRACT OF THE DISSERTATION

**Linear Network Coding over Ring Alphabets**

by

Joseph Michael Connelly

Doctor of Philosophy in Electrical Engineering  
(Communication Theory & Systems)

University of California, San Diego, 2018

Professor Kenneth Zeger, Chair

As connected devices play an ever-growing role in our society, there is a subsequent need for advances in multi-user communication systems. In a *network*, senders and receivers are connected via a series of intermediate users who share *information* represented as sequences of bits or elements of some other finite *alphabet*. By allowing users to transmit *functions* of their inputs, as opposed to simply *relaying* received data, the information throughput of a network can be increased. *Network codes* in which these functions are *linear* are suboptimal in general but are of practical interest due to their mathematical tractability and low implementation complexity. The study of linear network coding has primarily been limited to *finite field* alphabets. In this work, we consider linear network codes over more general algebraically-structured alphabets, namely *finite rings*. We contrast linear network codes over finite fields, commutative rings, and non-commutative rings, and we discuss cases where non-linear codes attain higher information rates than even very general linear codes. Our results show that finite fields are, in some sense, the best ring alphabets for linear network coding, but in certain instances, it may be advantageous to use linear coding over some other ring alphabet of the same size. Specifically, we prove results related to:

- (i) *network solvability*: whether or not a network's receivers can obtain their desired information using codes over a given alphabet. We characterize the commutative rings for which there exists a network that is linearly solvable over the ring but not over any other commutative ring of the same size. We show that these rings are, in some sense, the best commutative rings of a given size for linear network coding. We then present an infinite class of networks that are linearly solvable over certain non-commutative rings but not over any commutative rings. We also prove that *vector* linear codes over finite fields minimize the alphabet size needed for linear solvability, which is desirable from an implementation complexity standpoint.
- (ii) *network capacity*: how much information per channel use can be sent to the network's receivers in the limit of large block sizes for transmission. We show that the linear coding capacity of a given network cannot be increased by looking beyond finite fields to more general rings.

# Chapter 1

## Introduction

In the past decade, the world has become a more connected place, as cell phones, personal computers, and other smart devices have become increasingly ubiquitous. By 2021, the global Internet traffic is projected to double its 2017 levels, and the number of connected devices is expected to exceed the global population by a factor of three [4]. Alongside this growth in information volume, there is an ever-increasing demand for faster broadband speeds for applications such as video streaming and cloud computing. This growth in demand has produced a subsequent need for advances in multi-user communication systems, wherein senders and receivers are often not connected directly. Rather, information passes through intermediate users and relays in a *network*.

### 1.1 Network Coding

In 2000, Ahlswede et. al [1] published a seminal work proposing a mathematical model for information networks. They showed that, under this model, the information throughput of a network can be increased by allowing network nodes to transmit *functions* of their inputs, as opposed to simply relaying (*routing*) data. This paradigm shift gave rise to the field of network coding, which has since produced a rich collection of theoretical results and practical applications [2, 17]. Network coding has connections to a broad range of topics in engineering, mathematics, and computer science, and many problems in the field lie at the intersection of information theory, graph theory, complexity theory, and linear algebra. This dissertation explores a connection between abstract algebra and network coding theory.

Data in networks, such as sensor readings or multimedia, is typically represented as sequences of binary bits or as elements of some other finite set (e.g. ternary or, more generally,  $n$ -ary), called an *alphabet*. In order to more easily study and implement network codes, we can impose *algebraic structure* on the alphabet. That is, we introduce *operations*, such as addition and multiplication, on the alphabet, allowing us to describe edge and decoding functions in a network code in terms of these operations. There are generally multiple ways of assigning addition and multiplication operations to a given alphabet while still preserving certain arithmetic properties. In this dissertation, we compare classes of network codes with various algebraically-structured alphabets. Prior work has focused on alphabets with *finite field* structure; in what follows, we study the more general case where the alphabet is a *finite ring*. We broadly seek to answer the question of whether or not it is advantageous to use this more general class of network codes. We show that, while the information throughput of a network cannot be increased by using codes with finite ring alphabets instead of field alphabets, there can be other advantages to using these codes in certain instances.

### 1.2 Group, Ring, and Field Alphabets

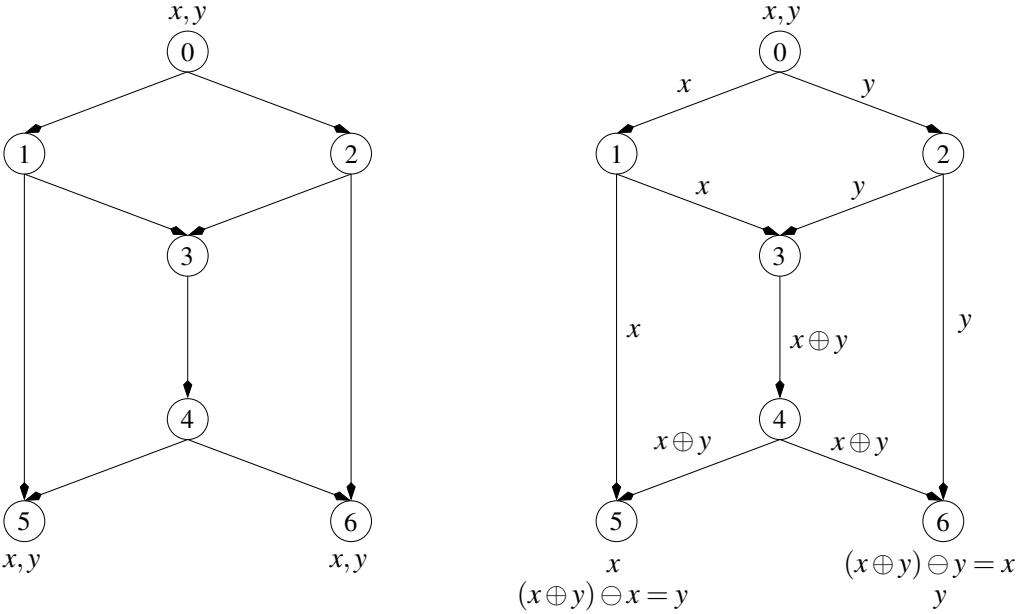


Figure 1.1: The Butterfly Network (left), and a solution for the Butterfly Network (right) over any finite group alphabet. There is a single source, node 0, which generates the messages  $x$  and  $y$ . Each of the receivers, nodes 5 and 6, demands both  $x$  and  $y$ . The Butterfly Network has no routing solutions when each edge is used at most once.

The overarching goal in network coding is for the *receivers* to recover their *demanded messages* while limiting the number of uses of the channels that connect the network's nodes. Such channels are modeled as directed edges that can carry *symbols* from the network alphabet. The *Butterfly Network*, given in Figure 1.1, is a classic example of a network that exhibits a throughput gain via network coding. When each edge of the Butterfly Network can carry at most one symbol, the source's messages cannot be relayed to both receivers using routing alone, regardless of the network alphabet. To see this, if (without loss of generality) node 0 transmits  $x$  to node 1 and  $y$  to node 2, then in order for  $x$  and  $y$  to get to nodes 6 and 5, respectively, the center edge must carry both symbols. However, we will see that using network coding, the receivers can recover their demands over any alphabet size using each edge exactly once. In order to describe such a network code, we introduce an algebraic structure with *addition* and *subtraction* operations.

**Definition 1.2.1.** An *Abelian group*  $(G, \oplus)$  is a set  $G$  with a binary operation  $\oplus : G \times G \rightarrow G$  such that

- $\oplus$  is associative and commutative,
- there is an *identity element*  $0 \in G$  such that  $0 \oplus g = g$  for all  $g \in G$ , and
- for each  $g \in G$ , there exists an *inverse*  $(-g) \in G$  such that  $g \oplus (-g) = 0$ .

We will write  $g \ominus h$  to mean  $g \oplus (-h)$ .

The binary alphabet  $\{0, 1\}$  together with the exclusive or (XOR) operation forms an Abelian group, where 0 is the identity element and 1 is its own inverse, i.e. addition and subtraction are both XOR, in this case. More generally, if  $n$  is a positive integer, then the  $n$ -ary alphabet  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  forms an Abelian group with  $n$  elements, where the operation is addition modulo  $n$  (i.e. taking the remainder of the sum when divided by  $n$ ), e.g.  $1 + 2 = 0$  modulo 3 and  $4 + 3 = 2$  modulo 5.

If an Abelian group structure  $(G, \oplus)$  is imposed on the alphabet in the Butterfly Network, then the network code given in Figure 1.1 allows each receiver to recover both  $x$  and  $y$  using each edge exactly once. This network coding *solution* requires only addition and subtraction operations and is valid for any Abelian group alphabet. This means that regardless of whether the network alphabet is binary, ternary, or  $n$ -ary, the receivers can recover their demands using this code.

In general, networks may require more complex coding operations in order to achieve solutions, and it may not be the case that a solution is attainable over every alphabet size. We can introduce a *multiplication* operation by considering network alphabets that have a *ring* structure. This will allow us to study classes of network codes much broader than those consisting only of addition and subtraction operations.

**Definition 1.2.2.** A ring  $(R, +, *)$  is a set  $R$  with binary operations  $+$  and  $*$  such that

- $(R, +)$  is an Abelian group with *additive identity* 0,
- $*$  is associative and distributive with respect to  $+$ , and
- there is a *multiplicative identity* element 1 in  $R$  such that  $1 * r = r * 1 = r$ , for all  $r \in R$

For brevity, we will often refer to a ring  $(R, +, *)$  as  $R$ . A ring is called *commutative* if the multiplication operation  $*$  is also commutative.

In other words, a ring is a collection of elements with addition, subtraction, and multiplication operations that behave as we might expect, except that  $a * b$  is not always equal to  $b * a$ . The set  $\mathbb{Z}_n$  together with addition and multiplication modulo  $n$  is a commutative ring with  $n$  elements. In particular, the addition and multiplication tables of  $\mathbb{Z}_4$  are given by

|   |   |   |   |   |
|---|---|---|---|---|
| + | 0 | 1 | 2 | 3 |
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

|   |   |   |   |   |
|---|---|---|---|---|
| * | 0 | 1 | 2 | 3 |
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

For each integer  $k \geq 2$ , the set of all  $k \times k$  matrices whose entries are from  $\mathbb{Z}_n$  together with matrix addition and multiplication modulo  $n$  is an example of a *non-commutative* ring, since matrix multiplication does not commute, in general, e.g.

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

There are generally multiple rings of a given size. For example, the ring of  $k \times k$  matrices with entries from  $\mathbb{Z}_n$  and the ring  $\mathbb{Z}_{n^{k^2}}$  both have  $n^{k^2}$  elements and are distinct, since the former is non-commutative and the latter is commutative. While our focus will be on rings with a finite number of elements, there exist rings with infinite cardinality, such as the set of integers  $\mathbb{Z}$  together with addition and multiplication.

Not every ring has a well-defined division operation for its non-zero elements. As an example, in the ring  $\mathbb{Z}_4$ , we have  $2 = 2 * 1 = 2 * 3$  and  $0 = 2 * 2 = 2 * 0$ , so the element 2 has no *multiplicative inverse*. That is, there is no element  $a \in \mathbb{Z}_4$  such that  $2a = 1$ , so there is no notion of “dividing by 2” in  $\mathbb{Z}_4$ . On the other hand, in the ring  $\mathbb{Z}_5$ , we have  $2 * 3 = 4 * 4 = 1$ , so  $2^{-1} = 3$ ,  $3^{-1} = 2$ , and  $4^{-1} = 4$ . It turns out whenever  $p$  is prime, every non-zero element of  $\mathbb{Z}_p$  has a multiplicative inverse.

**Definition 1.2.3.** A *field* is a commutative ring in which every non-zero element has a *multiplicative inverse*.

The sets of rational, real, and complex numbers together with their respective addition and multiplication operations are infinite-cardinality fields. Many results from linear algebra extend to fields with finite cardinality, making them attractive from a coding theory perspective. Unlike finite rings, a finite field must have prime-power size. When  $p$  is prime, there is a *unique* finite field with  $p^k$  elements, which we denote by  $\text{GF}(p^k)$ .<sup>1</sup> The rings  $\mathbb{Z}_p$  and  $\text{GF}(p)$  are *isomorphic*, but when  $k \geq 2$ , the ring  $\mathbb{Z}_{p^k}$  and the field  $\text{GF}(p^k)$  are distinct. For example,  $\text{GF}(4)$  has elements  $\{0, 1, \alpha, \alpha+1\}$  and addition and multiplication given by:

|            |            |            |            |            |
|------------|------------|------------|------------|------------|
| +          | 0          | 1          | $\alpha$   | $\alpha+1$ |
| 0          | 0          | 1          | $\alpha$   | $\alpha+1$ |
| 1          | 1          | 0          | $\alpha+1$ | $\alpha$   |
| $\alpha$   | $\alpha$   | $\alpha+1$ | 0          | 1          |
| $\alpha+1$ | $\alpha+1$ | $\alpha$   | 1          | 0          |

|            |   |            |            |            |
|------------|---|------------|------------|------------|
| *          | 0 | 1          | $\alpha$   | $\alpha+1$ |
| 0          | 0 | 0          | 0          | 0          |
| 1          | 0 | 1          | $\alpha$   | $\alpha+1$ |
| $\alpha$   | 0 | $\alpha$   | $\alpha+1$ | 1          |
| $\alpha+1$ | 0 | $\alpha+1$ | 1          | $\alpha$   |

Addition and multiplication in the field  $\text{GF}(4)$  differ from addition and multiplication in the ring  $\mathbb{Z}_4$ . In particular, every element of  $\text{GF}(4)$  added to itself is zero, whereas  $1 + 1 = 2$  in  $\mathbb{Z}_4$ , and there is no non-zero element of  $\text{GF}(4)$  whose square is zero, whereas  $2 * 2 = 0$  in  $\mathbb{Z}_4$ .

### 1.3 Scalar Linear Codes over Finite Fields

For each integer  $n \geq 2$ , the *n-Choose-Two Network*, given in Figure 1.2, is another example of a network that exhibits a network coding throughput gain under certain circumstances. Let  $\mathbb{F}$  be a finite field, and consider a code for the *n-Choose-Two Network* in which the messages  $x$  and  $y$  are from  $\mathbb{F}$  and each edge carries a single symbol from  $\mathbb{F}$  of the form:

$$\lambda_i = A_i x + B_i y$$

where the  $A_i$ 's and  $B_i$ 's are constants in  $\mathbb{F}$ . Such a code is *scalar linear over  $\mathbb{F}$* . In other words, *scalar linear codes over fields* consist of network out-edges carrying field elements which are linear combinations of their input field elements. It was shown in [21] that, for each finite field  $\mathbb{F}$ , there exists a scalar linear solution for the *n-Choose-Two Network* over  $\mathbb{F}$  if and only if  $|\mathbb{F}| \geq n - 1$ .

<sup>1</sup>“GF” stands for Galois Field, named after French mathematician Évariste Galois.



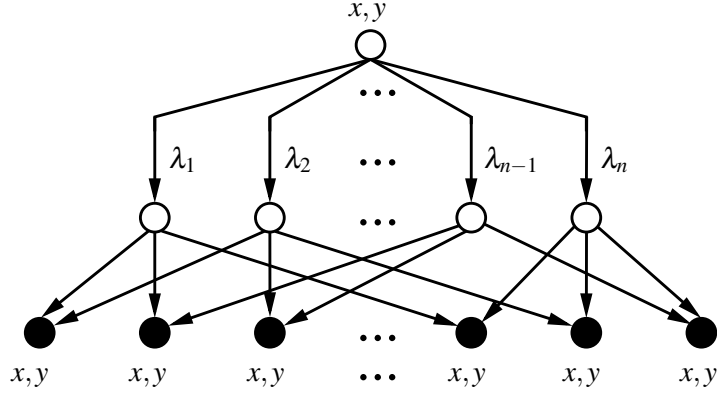


Figure 1.2: The  $n$ -Choose-Two Network is parameterized by an integer  $n \geq 2$ . There is a single source node that generates messages  $x$  and  $y$ , and there are  $\binom{n}{2}$  receivers, each of which gets a unique pair  $(\lambda_i, \lambda_j)$  of intermediate functions of  $x$  and  $y$ , from which they must recover  $x$  and  $y$ .

In particular, if  $\mathbb{F}$  is such that  $|\mathbb{F}| \geq n - 1$ , define a scalar linear code over  $\mathbb{F}$  such that

$$\lambda_1 = x, \quad \lambda_2 = y, \quad \lambda_i = x + B_i y \quad (i = 3, \dots, n),$$

where the  $B_i$ 's are distinct non-zero elements of  $\mathbb{F}$ . Such a choice for  $B_3, \dots, B_n$  is possible, since there are at least  $n - 2$  non-zero elements of  $\mathbb{F}$ . Then  $x$  and  $y$  can be recovered from each pair  $(\lambda_i, \lambda_j)$  by:

$$\begin{aligned} (\lambda_1, \lambda_2) &= (x, y) \\ \left( \lambda_1, \frac{\lambda_i - \lambda_1}{B_i} \right) &= (x, y) & (i = 3, \dots, n) \\ (\lambda_i - B_i \lambda_2, \lambda_2) &= (x, y) & (i = 3, \dots, n) \\ \left( \frac{B_i \lambda_j - B_j \lambda_i}{B_i - B_j}, \frac{\lambda_i - \lambda_j}{B_i - B_j} \right) &= (x, y) & (i, j = 3, \dots, n \text{ and } i \neq j). \end{aligned}$$

Division by  $B_i$  and  $(B_i - B_j)$  is well-defined in  $\mathbb{F}$ , since the  $B_i$ 's are non-zero and distinct, and every non-zero element of  $\mathbb{F}$  is invertible. Thus the code is a scalar linear solution over  $\mathbb{F}$ . Conversely, when  $|\mathbb{F}| < n - 1$ , it can be shown that there are not enough distinct linear combinations of  $x$  and  $y$  for  $x$  and  $y$  to be linearly recovered from each pair  $(\lambda_i, \lambda_j)$ .

Scalar linear codes over finite fields have been particularly attractive to study, in part because it is more feasible to analyze scalar linear functions, as opposed to arbitrary functions. There has been much work in developing algorithms for constructing scalar linear solutions for certain classes of networks [11, 12, 16]. The existence of scalar linear solutions over finite fields has also been connected to other topics in mathematics, such as finding roots of systems of polynomials [8, 14] and matroid theory [7, 19]. However, scalar linear codes over finite fields are far from sufficient in general.

## 1.4 Vector Linear Codes over Finite Fields

The *M Network*, defined in Figure 1.3, is an example of a network for which scalar linear codes over fields are insufficient. It was shown in [18] that the *M Network* has no scalar linear coding solutions over any finite field alphabet. However, by viewing each message and each edge symbol as a 2-dimensional vector over a field  $\mathbb{F}$  (i.e. the alphabet is  $\mathbb{F}^2$ ), we can describe a routing solution for the *M Network*.

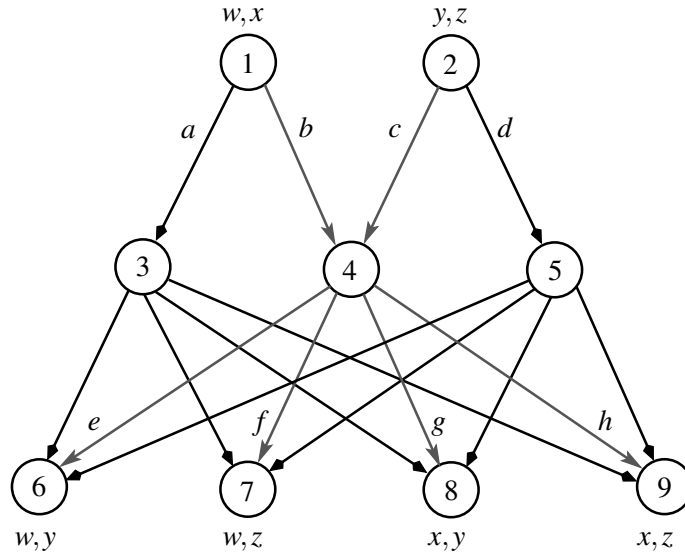


Figure 1.3: The *M Network*. The sources, nodes 1 and 2, generate messages  $w$ ,  $x$ ,  $y$ , and  $z$ , as indicated. Each receiver demands a unique pair of messages, one of which originates at node 1, the other of which originates at node 2.

Let  $x_1$  and  $x_2$  denote the components of the vector  $x \in \mathbb{F}^2$ , and define a code for the *M Network* over  $\mathbb{F}^2$  by:

$$(a_1, a_2) = (w_1, x_1) \quad (b_1, b_2) = (w_2, x_2) \quad (c_1, c_2) = (y_2, z_2) \quad (d_1, d_2) = (y_1, z_1)$$

and

$$\begin{aligned} (e_1, e_2) &= (b_1, c_1) & (f_1, f_2) &= (b_1, c_2) & (g_1, g_2) &= (b_2, c_1) & (h_1, h_2) &= (b_2, c_2) \\ &= (w_2, y_2) & &= (w_2, z_2) & &= (x_2, y_2) & &= (x_2, z_2) \end{aligned}$$

where each receiver can recover both components of each of its demands by:

$$\begin{array}{llll} 6: & (a_1, e_1) = (w_1, w_2) & 7: & (a_1, f_1) = (w_1, w_2) \\ & (d_1, e_2) = (y_1, y_2) & & (d_2, f_2) = (z_1, z_2) \\ 8: & & & (a_2, g_1) = (x_1, x_2) \\ & & & (d_1, g_2) = (y_1, y_2) \\ 9: & & & (a_2, h_1) = (x_1, x_2) \\ & & & (d_2, h_2) = (z_1, z_2) \end{array}$$

This solution uses routing operations on vectors and is a special case of the more general class of *vector linear codes*. This code provides a solution over any alphabet whose size is of the form  $p^{2n}$ , for some prime  $p$  and positive integer  $n$ , yet the *M Network* has no scalar linear solutions over any finite field.

In a *vector linear code over a field*, out-edges carry linear combinations of input vectors of field elements, where the coefficients are matrices of field elements, i.e. out-edges carry vectors of the form

$$M_1 x_1 + \dots + M_n x_n$$

where  $x_1, \dots, x_n$  are vectors from a field of a given dimension, representing the inputs to the node, and  $M_1, \dots, M_n$  are square matrices whose entries are constants from the field. Vector linear coding generalizes scalar linear coding and can attain linear solutions not possible with scalar coding [10, 18, 23]. In [9], the authors presented an algorithm for constructing vector linear solutions for certain classes of networks. Linear coding over finite fields has been the cornerstone of a large portion of network coding research during the last fifteen years [15]. However, vector linear codes over finite fields are known to not always be sufficient.

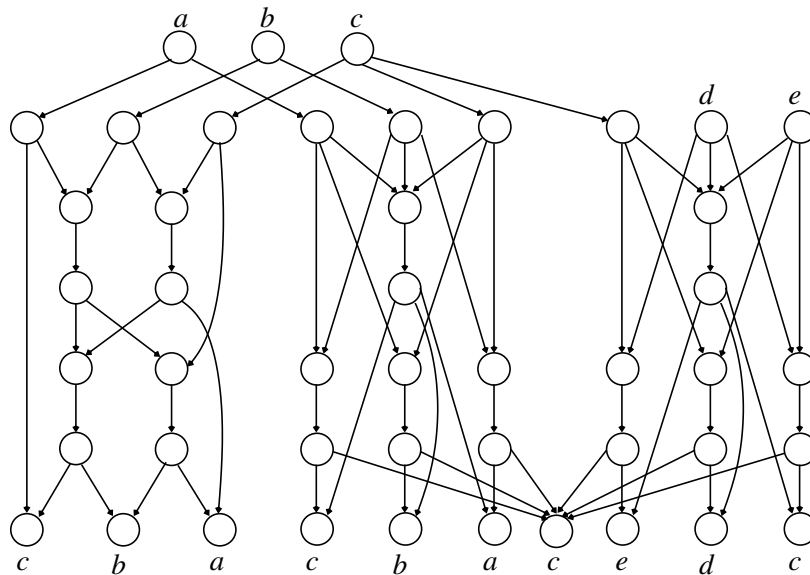


Figure 1.4: The Diabolical Network.

The *Diabolical Network*, given in Figure 1.4, is known [6] to have a non-linear solution over an alphabet of size 4, yet it has no linear solution over *any* finite field alphabet and any vector dimension.<sup>2</sup> In particular, for a linear code to be a solution for the left-hand side, we must have  $1 + 1 = 0$  in the field, but the right-hand side requires that  $1 + 1 \neq 0$  in the field. Other works have shown other advantages of non-linear codes, such as reducing the alphabet size needed for a solution (e.g. [5, 22]). Even though linear network codes over finite fields are suboptimal in general, they have been attractive to study for two primary reasons:

- (1) They can be less complex to implement in practice due to reduced storage and/or reduced computation compared to non-linear codes.

---

<sup>2</sup>The Diabolical Network was shown to not even have linear solutions over ring and module alphabets.

(2) They are more mathematically tractable to analyze compared to non-linear codes.

It is natural to ask whether there exists a class of network codes that still satisfy these desirable properties yet outperform linear codes over fields.

## 1.5 Linear Network Coding over Finite Rings

The definitions of scalar and vector linear codes over finite fields can easily be extended to more general finite ring alphabets, since computing a linear combination requires only addition and multiplication operations. A field is a special case of a ring, so a linear network code over a ring may be implemented analogously to a linear code over a field by performing addition and multiplication over the ring.<sup>3</sup> Since the founding of network coding in 2000, network codes whose edge functions are linear over fixed finite field alphabets have been studied extensively (e.g. [7–12, 14–16, 19, 22–24]). In contrast, very little is presently known about linear network coding over other ring alphabets. Non-field rings are known to be useful for other information-theoretic problems, such as error-correcting codes [3, Chapter 8] and cryptography [13], so it is reasonable to ask whether it is better in some sense to use linear network coding over a finite field alphabet or over some other ring alphabet of the same size.

If  $p$  is a prime, there is a unique finite field of size  $p^k$ , but the number of commutative rings of size  $p^k$  is on the order of  $p^{k^3}$  [20, Theorem 11.2]. This suggests that the class of codes that are linear with respect to *some* ring of size  $p^k$  is much broader than the class of codes that are linear with respect *the* field of size  $p^k$ . By considering a broader class of codes, one would expect to be able to attain more solutions. Additionally, linear network codes over rings may be of value by allowing for linear coding over non-power-of-prime alphabet sizes. Linear codes over rings appear to have many of the attractive properties of linear codes over finite fields, yet they also constitute a much broader class of network codes.

Many interesting questions regarding linear codes over rings exist: Can a network be linearly solvable over rings but not over fields? Can a network have no linear solutions over a given field yet be linearly solvable over some other ring of the same size? Is there a “best” ring alphabet of a given size to use for linear network coding? Is there a “best” ring alphabet to use for linear coding on a given network? Over what ring alphabets are particular networks (linearly) solvable? Can the linear capacity of a network over a finite field be increased by using some other ring of the same size as the field? Can linear codes over rings close the gap between linear codes over finite fields and non-linear codes? This dissertation addresses these and many related questions.

---

<sup>3</sup>Efficient implementations of ring arithmetic generally depend on the specific algebraic properties of the ring.

## 1.6 Overview

The results in this dissertation fall under the umbrella of two underlying network coding problems.

- (i) In the *network solvability* problem, one attempts to determine whether there exist network coding solutions over a given alphabet in which each edge carries at most one alphabet symbol.
- (ii) In the *network capacity* problem, one attempts to determine how much transmitted information per edge use can be sent to the network’s receivers in the limit of large block sizes for transmission.

The remainder of the dissertation consists of published and submitted journal papers on these topics and is organized as follows.

Chapter 2 studies network scalar linear solvability over commutative rings and makes comparisons to the well-studied special case where the alphabet is a field. We characterize the commutative rings for which there exists a network that is a scalar linearly solvable over the ring but not over any other commutative ring of the same size. We show that these rings are, in some sense, the “best” commutative rings of a given size. We also show that every finite field is such a ring, and, whenever  $p$  is prime, there is some network that is scalar linearly solvable over a commutative ring of size  $p^k$  but not the field of size  $p^k$  if and only if  $k \notin \{1, 2, 3, 4, 6\}$ . On the other hand, we show that if a network is scalar linearly solvable over some commutative ring, then the (unique) smallest such ring is a field. The results in this chapter imply that for scalar linear coding over commutative rings, fields can always be used when the alphabet size is flexible, but other rings may be needed when the alphabet size is fixed. Chapter 2 is a reprint of the material as it appears in J. Connelly and K. Zeger, “Linear network coding over rings – Part I: Scalar codes and commutative alphabets,” *IEEE Transactions on Information Theory*, January 2018.

Chapter 3 studies the more general setting of network vector linear solvability over (possibly non-commutative) rings. It is shown that vector linear solvability over some field is equivalent to scalar linear solvability over some ring.<sup>4</sup> We also present an infinite class of networks that are scalar linearly solvable over certain non-commutative rings but not over any commutative rings. Finally, we show that vector linear codes over fields minimize the alphabet size needed for linear solvability, which is desirable from an implementation complexity standpoint. The results in this chapter suggest that, in a sense, vector linear codes over prime fields are the best alphabets to use for linear network coding. Chapter 3 is a reprint of the material as it appears in J. Connelly and K. Zeger, “Linear network coding over rings – Part II: Vector codes and non-commutative alphabets,” *IEEE Transactions on Information Theory*, January 2018.

---

<sup>4</sup>In fact, vector linear solvability over some field is equivalent to linear solvability over some module. Linear codes over modules are an even broader class of codes that generalize both scalar and vector linear codes over rings.

Chapter 4 considers the network capacity problem using linear network codes. It is shown that a network's linear capacity cannot be improved by looking beyond finite field alphabets to more general ring alphabets. However, some rings can linearly attain higher rates for certain networks than can a given field. In particular, we show that for any finite ring and any finite field, there is some network with higher linear capacity over the ring if and only if the sizes of the field and ring are relatively prime. In other words, higher code rates *cannot* be attained by using linear codes over more general alphabets than finite fields. Chapter 4 is a reprint of the material as it appears in J. Connelly and K. Zeger, "Linear capacity of networks over ring alphabets," submitted to *IEEE Transactions on Information Theory*, June 2017, revised January 2018.

Chapter 5 considers both the network solvability and capacity problems for a particular class of networks with emphasis on non-linear coding. We present an infinite class of networks for which non-linear codes strictly outperform linear codes for both network solvability and capacity. These networks generalize the Diabolical Network from [6] and further demonstrate the insufficiency of linear network coding. Certain instances of these networks are shown to only be solvable over non-power-of-prime size alphabets. This contrasts greatly with linear solvability, since any linearly solvable network has a vector linear solution over a field (with prime-power alphabet size). Chapter 5 is a reprint of the material as it appears in "A class of non-linearly solvable networks," *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 201 – 229, January 2017.

## References

- [1] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.
- [2] R. Bassoli, H. Marques, J. Rodriguez, K. W. Shum and R. Tafazolli, "Network coding theory: A survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 1950–1978, 2013.
- [3] G. Bini and F. Flamini, *Finite Commutative Rings and Their Applications*, Kluwer Academic Publishers, 2002.
- [4] *Cisco Visual Networking Index: Forecast and Methodology, 2016–2021*, June 2017.
- [5] R. Dougherty, C. Freiling, and K. Zeger, "Linearity and solvability in multicast networks," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2243–2256, October 2004.
- [6] 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.
- [7] R. Dougherty, C. Freiling, and K. Zeger, "Networks, matroids, and non-Shannon information inequalities," *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 1949–1969, June 2007.

- [8] R. Dougherty, C. Freiling, and K. Zeger, “Linear network codes and systems of polynomial equations,” *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2303–2316, May 2008.
- [9] J.B. Ebrahimi and C. Fragouli, “Algebraic algorithms for vector network coding,” *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 996–1007, February 2011.
- [10] T. Etzion and A. Wachter-Zeh, “Vector network coding based on subspace codes outperforms scalar linear network coding,” *IEEE Transactions on Information Theory*, to appear.
- [11] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, “A random linear network coding approach to multicast,” *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, October 2006.
- [12] S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, “Polynomial time algorithms for multicast network code construction,” *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1973–1982, June 2005.
- [13] N. Koblitz, *Algebraic Aspects of Cryptography*, Springer-Verlag Berlin Heidelberg, 1998.
- [14] R. Koetter and M. Médard, “An algebraic approach to network coding,” *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, October 2003.
- [15] S.-Y.R. Li, Q. Sun, and S. Ziyu, “Linear network coding: theory and algorithms,” *Proceedings of the IEEE*, vol. 99, no. 3, pp. 372–387, March 2011.
- [16] S.-Y.R. Li, R.W. Yeung, and N. Cai, “Linear network coding,” *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, February 2003.
- [17] T. Matsuda, T. Noguchi, and T. Takine, “Survey of network coding and its applications,” *IEICE Transactions on Communications*, vol. 94, no. 3, pp. 698–717, March 2011.
- [18] M. Médard, M. Effros, T. Ho, and D. Karger, “On coding for non-multicast networks,” *Conference on Communication Control and Computing*, Monticello, IL, October 2003.
- [19] V. T. Muralidharan and S. Rajan, “Linear network coding, linear index coding, and representable discrete polymatroids,” *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 4096 – 4119, July 2016.
- [20] B. Poonen, “The moduli space of commutative algebras of finite rank,” *Journal of the European Mathematical Society*, vol. 10, no. 3, pp. 817–836, 2008.
- [21] A. Rasala Lehman and E. Lehman, “Complexity classification of network information flow problems,” *ACM-SIAM Symposium on Discrete algorithms*, 2004.
- [22] S. Riis, “Linear versus nonlinear boolean functions in network flow,” *Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March 2004.
- [23] Q. Sun, X. Yangy, K. Long, X. Yin, and Z. Li, “On vector linear solvability of multicast networks,” *IEEE Transactions on Communications* vol. 64, no. 12, pp. 5096–5107, December 2016.
- [24] R. W. Yeung, “Network coding: A historical perspective,” *Proceedings of the IEEE*, vol. 99, no. 3, pp. 366–371, March 2011.

# Chapter 2

## Scalar Codes and Commutative Rings

### Abstract

This chapter considers the setting of scalar linear network coding over finite commutative ring alphabets. We show that if a network has a scalar linear solution over some finite commutative ring, then the (unique) smallest such commutative ring is a field.

We also show that fixed-size commutative rings are quasi-ordered such that all scalar linearly solvable networks over any given ring are also scalar linearly solvable over any higher-ordered ring. We study commutative rings that are maximal with respect to this quasi-order, as they may be considered the best commutative rings of a given size. We prove that a commutative ring is maximal if and only if some network is scalar linearly solvable over the ring but not over any other commutative ring of the same size. Furthermore, we show that maximal commutative rings are direct products of certain fields specified by the integer partitions of the prime factor multiplicities of the ring's size. Finally, we prove there is a unique maximal commutative ring of size  $m$  if and only if each prime factor of  $m$  has multiplicity in  $\{1, 2, 3, 4, 6\}$ . As consequences, (i) every finite field is such a maximal ring, and (ii) for each prime  $p$ , some network is scalar linearly solvable over a commutative ring of size  $p^k$  but not over the field of the same size if and only if  $k \notin \{1, 2, 3, 4, 6\}$ .



## 2.1 Introduction

In this chapter, we focus on the case where the network coding alphabet is a commutative ring, and we make comparisons to the even more specialized (and more studied) case where the alphabet is a field. In Chapter 3, we study vector linear codes and non-commutative rings and specifically contrast the results with the results on scalar codes and commutative rings given in this present chapter.

Many networks evolve over time as nodes are added or deleted and as edge connections are formed or broken. Thus, it might be advantageous to choose a coding alphabet that makes as many networks as possible scalar linearly solvable over the chosen ring. If, for example, every network that is scalar linearly solvable over a particular ring is also scalar linearly solvable over a second ring, then, generally speaking, the second ring would be at least as good as the first ring. This notion of one ring being better than another ring is the core concept behind our study in this chapter. We seek out the best such rings, namely the ones that are maximal with respect to this induced ordering of rings of a given size. On the other hand, when a network is fixed, it is sometimes advantageous to select the smallest possible alphabet that yields a solution [22]. Two of the main results of this chapter are:

- (1) If  $p$  is prime and  $k \notin \{1, 2, 3, 4, 6\}$ , then there always exists some network that is not scalar linearly solvable over the finite field  $\text{GF}(p^k)$  yet is scalar linearly solvable over a different commutative ring of the same size. When  $k \in \{1, 2, 3, 4, 6\}$ , no such network exists.
- (2) If a network has a scalar linear solution over a commutative ring that is not a field, then it also has a scalar linear solution over a field of strictly smaller size.

### 2.1.1 Network Model

A *network* will refer to a finite, directed, acyclic multigraph, some of whose nodes are *sources* or *receivers*. Source nodes generate *messages*, each of which is an arbitrary element of a fixed, finite set of size at least 2, called an *alphabet*. The elements of an alphabet are called *symbols*. The *inputs* to a node are the messages, if any, originating at the node and the symbols on the incoming edges of the node. Each outgoing edge of a network node has associated with it an *edge function* that maps the node's inputs to the symbol carried by the edge, called the *edge symbol*. Each receiver node has *decoding functions* that map the receiver's inputs to an alphabet symbol in an attempt to recover the receiver's *demands*, which are the messages the receiver wishes to obtain. The *outputs* of a node are its demands, if any, and the symbols on the outgoing edges of the node. A network is *multicast* if there is a single source node and each receiver demands every message.

A *code over an alphabet*  $\mathcal{A}$  is an assignment of edge functions to all of the edges in a network and an assignment of decoding functions to all of the receiver nodes in the network such that messages and edge symbols are elements of  $\mathcal{A}$ . A *solution* is a code in which each receiver's decoding functions recover each of its demands from its inputs.

In particular, we will consider codes over alphabets that have addition and multiplication operations, namely finite rings. If  $\mathcal{A}$  is a ring alphabet, then a function  $f : \mathcal{A}^m \rightarrow \mathcal{A}$  is *linear over*  $\mathcal{A}$  if it can be written in the form  $f(x_1, \dots, x_m) = C_1 x_1 + \dots + C_m x_m$ , where  $C_1, \dots, C_m$  are constant values in  $\mathcal{A}$ . A code is *scalar linear over*  $\mathcal{A}$  if each edge function and each decoding function is linear over  $\mathcal{A}$ . In contrast, in a *k-dimensional vector linear code over*  $\mathcal{A}$ , messages and edge symbols are  $k$ -dimensional vectors over  $\mathcal{A}$  (i.e. the alphabet is  $\mathcal{A}^k$ ), and edge functions are linear combinations of input vectors, using  $k \times k$  matrices over  $\mathcal{A}$  as coefficients. Scalar linear codes are a special case of vector linear codes where  $k = 1$ .

We say a network is *solvable over*  $\mathcal{A}$  (respectively, *scalar linearly solvable over*  $\mathcal{A}$ ) if there exists a solution over  $\mathcal{A}$  (respectively, scalar linear solution over  $\mathcal{A}$ ), and we say a network is *solvable* if it is solvable over some alphabet.

### 2.1.2 Related Work

Ahlswede, Cai, Li, and Yeung [1] introduced network coding in 2000 and showed that it is possible to increase the information throughput of a network by allowing nodes to transmit functions of their inputs, as opposed to simply relaying their inputs. Li, Yeung, and Cai [26] showed that every solvable multicast network is scalar linearly solvable over every sufficiently large finite field, although it was shown in [8] that non-multicast networks may not have this property. Networks were demonstrated by Riis [30], Rasala Lehman and Lehman [29], and in [10] that are solvable non-linearly but not scalar linearly over the same alphabet size. It is not currently known whether there exists an algorithm that determines if a network is solvable; however, determining whether a network is scalar linearly solvable over a particular field has been studied extensively.

Koetter and Médard [21] showed that for every network, there exists a finite collection of polynomials, such that for every finite field  $\mathbb{F}$ , the network is scalar linearly solvable over  $\mathbb{F}$  if and only if the polynomials have a common root in  $\mathbb{F}$ . Conversely, it was shown in [9] that for every finite collection of polynomials, there exists a network, such that for every finite field  $\mathbb{F}$ , the polynomials have a common root in  $\mathbb{F}$  if and only if the network is scalar linearly solvable over  $\mathbb{F}$ . This connection between scalar linear solvability and polynomials stems from the connection between scalar linearly solvable networks and matroid theory. It was also shown in [11] that every network that is scalar linearly solvable over some field

is naturally associated with a representable matroid. Effros, El Rouayheb, and Langberg [14] showed that network coding and index coding are equivalent in a general setting, including with linear and non-linear codes.

The study of linear network codes over fields has led to efficient methods of constructing scalar linear solutions for networks that also minimize the field alphabet size. Ho et. al [18] described a random scalar linear coding technique where the probability that a code is a solution grows with the field size. Jaggi et. al [19] presented polynomial-time algorithms for designing scalar linear codes for multicast networks. Karimian, Borujeny, and Ardakani [20] showed there exists a class of non-multicast networks for which random scalar linear coding algorithms fail with high probability and presented a new approach to random scalar linear network coding for such networks. Rasala Lehman and Lehman [29] and Tavory, Feder, and Ron [35] independently showed that some solvable multicast networks asymptotically require finite field alphabets to be at least as large as twice the square root of the number of receiver nodes in order to achieve scalar linear solutions. Sun, Yin, Zi, and Long [33] and Sun, Li, and Li [34] both demonstrated classes of multicast networks that are scalar linearly solvable over certain fields but not every larger field.

Médard, Effros, Ho, and Karger [28] showed that there can exist a network that is vector linearly solvable over some field but not scalar linearly solvable over any field. Sun et. al [32] demonstrated that, while vector linear codes can outperform scalar linear codes in terms yielding solutions for general networks, there can exist multicast networks that are not  $k$ -dimensional vector linearly solvable over  $\text{GF}(2)$  yet have scalar linear solutions over some field alphabet whose size is less than  $2^k$ . Etzion and Wachter-Zeh [16] bounded the reduction in alphabet size needed for a vector linear solution to a multicast network as compared to a scalar linear solution. Ebrahimi and Fragouli [13] presented algorithms for constructing vector linear codes that achieve solutions not possible with scalar linear codes.

Convolutional network coding (e.g. [23, 24]) is a technique for linear coding for networks that may contain cycles, and the alphabets in such codes can be viewed as principal ideal domains (and more generally as discrete valuation rings), which are not necessarily finite. However, in our study, we focus on acyclic networks and finite coding alphabets. To our knowledge, outside of the context of the insufficiency of linear codes and convolutional coding, there has been little study of linear network codes over more general ring and module alphabets. We consider such linear codes and compare them to the well-studied case of linear codes over fields.

### 2.1.3 Our Contributions

Our main results show that for networks that use scalar linear codes over commutative rings, finite fields can always be used if the alphabet size is flexible, but if the alphabet size is fixed, then finite fields may not always be the best choice for every network. Figure 2.1 summarizes our main results for fixed networks, and Figure 2.2 summarizes our main results on the “best” commutative rings of a fixed size. We outline the remainder of the chapter in what follows.

We prove (in Theorem 2.2.10) that if a network has a scalar linear solution over some commutative ring, then the unique smallest-size commutative ring over which the network has a scalar linear solution is a field. Thus, for a given network, if the minimum alphabet size is desired for scalar linear network coding, it suffices to use finite fields. This result also shows that networks that are scalar linearly solvable over some commutative ring are also scalar linearly solvable over some field although not necessarily of the same size.

Section 2.2 introduces a “dominance” relation on finite rings, such that all networks that are scalar linearly solvable over a given ring are also scalar linearly solvable over any ring that dominates the given ring. We show that this relation is a quasi-order on the set of commutative rings of a given size.<sup>1</sup> We also demonstrate (in Theorem 2.2.19 and Corollary 2.3.3) non-isomorphic commutative rings of the same size that are equivalent with respect to dominance, and we show (in Theorem 2.2.20) that dominance is a total quasi-order of the commutative rings of size  $p^2$ .

Section 2.2.4 analyzes the scalar linear solvability of a class of multicast networks. We show (in Theorem 2.2.16) that for every finite field, there exists a multicast network that is scalar linearly solvable over the field but is not scalar linearly solvable over any other commutative ring of the same size. This demonstrates that every finite field is maximal with respect to the dominance. We also show (in Corollary 2.2.18) that there exists a solvable multicast network that is not scalar linearly solvable over any ring whose size is equal to  $2 \pmod{4}$ , which contrasts with the fact that every solvable multicast network is scalar linearly solvable over every sufficiently large field.

Section 2.3 compares various commutative rings with respect to dominance. We demonstrate (in Theorem 2.3.8) that some network is scalar linearly solvable over a commutative ring of size 32 but is not scalar linearly solvable over any other commutative ring of size 32, including the field  $\text{GF}(32)$ . We later prove (in Corollary 2.5.10) that 32 is the size of the smallest such commutative ring alphabet where this phenomenon can occur.

---

<sup>1</sup>Although the relation is defined on all finite rings, a maximal ring will always refer to a commutative ring which is maximal with respect to the quasi-order on the set of commutative rings of a given size.

We prove (in Theorem 2.3.9) that whenever a network is scalar linearly solvable over a commutative ring, the network must also be scalar linearly solvable over a field whose size divides the ring size. In fact, for each prime factor of the ring size, there is a corresponding such field whose characteristic equals the prime factor. As a consequence (in Corollary 2.3.11), whenever a network is scalar linearly solvable over a ring whose size is a product of distinct primes (i.e. “square free”), the network must also be scalar linearly solvable over each finite field whose size is a prime factor of the ring size. However, we demonstrate (in Corollary 2.3.12) that when the ring size is not square free, the particular ring may need to be examined in order to determine over which fields the network is scalar linearly solvable.

Section 2.4 introduces “partition rings” which are direct products of finite fields that are specified by integer partitions of the prime factor multiplicities of the ring size. We define a relation called “partition division” and show that it induces a quasi-order on the set of partitions of a given integer. We show that the maximal partitions under this quasi-order are precisely the partitions that do not divide any other partition of the same integer. We also provide a partial characterization of the maximal partitions. The results of this section are used in various proofs in Section 2.5.

Section 2.5 connects the relations of ring dominance and partition division. We prove (in Theorem 2.5.4) that, when restricting to commutative rings of a given size, the maximal commutative rings under dominance are precisely partition rings where each partition is maximal under partition division. We prove (in Theorem 2.5.8) that a finite commutative ring is maximal if and only if there exists a network that is scalar linearly solvable over the ring but is not scalar linearly solvable over any other commutative ring of the same size.

Finally, we prove (in Theorem 2.5.9) that if  $p$  is prime, then the field  $\text{GF}(p^k)$  is the unique maximal commutative ring of size  $p^k$  whenever  $k \in \{1, 2, 3, 4, 6\}$ , but if  $k = 5$  or  $k \geq 7$ , then there exist multiple maximal commutative rings of size  $p^k$ . This result is also generalized to commutative rings of non-power-of-prime sizes in Theorem 2.5.9. Since there can exist more than one maximal ring of a given size, there are instances where scalar linear solutions cannot be obtained using finite field alphabets of a given size but can be achieved using other commutative rings of the same size.

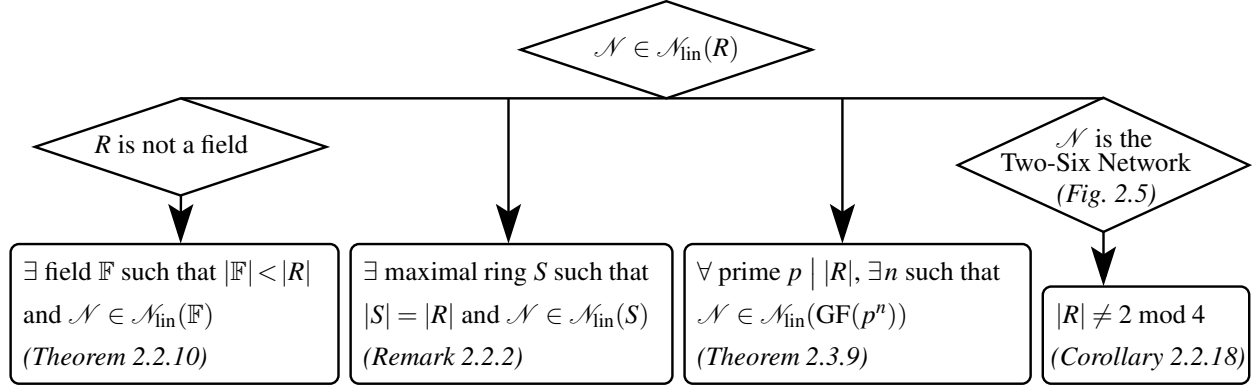


Figure 2.1:  $\mathcal{N}$  denotes an arbitrary network,  $R$  denotes an arbitrary finite commutative ring, and  $\mathcal{N}_{\text{lin}}(R)$  denotes the set of networks scalar linearly solvable over  $R$ . It follows from these results that finite fields minimize the alphabet size needed for a scalar linear solution over commutative rings, and the set of networks that are scalar linearly solvable over some commutative ring and the set of networks that are scalar linearly solvable over some field are equal.

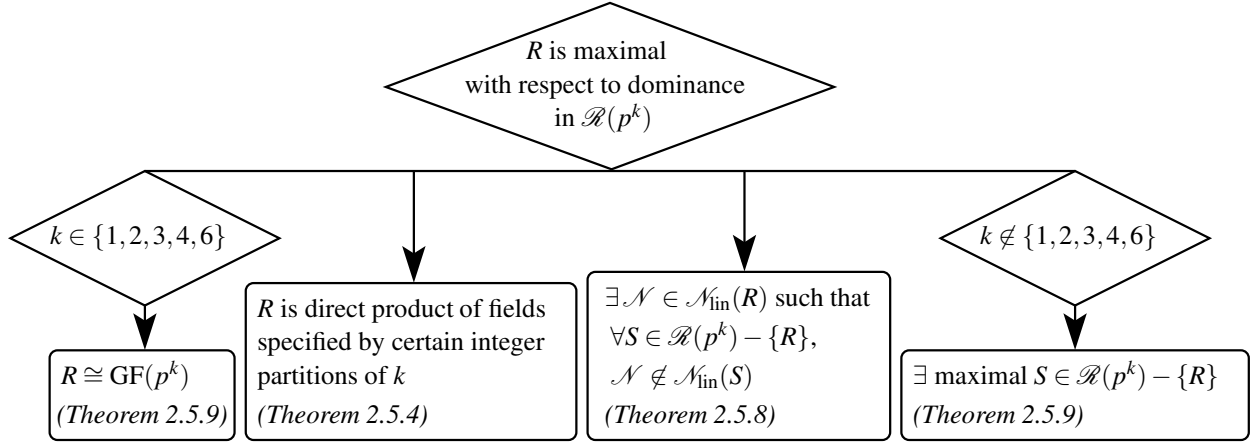


Figure 2.2: A ring  $S$  is *dominated* by a ring  $R$  if every network that is scalar linearly solvable over  $S$  is also scalar linearly solvable over  $R$ . This dominance induces a *quasi-order* on  $\mathcal{R}(p^k)$ , i.e. the set of commutative rings of size  $p^k$ . The rings which are *maximal* with respect to these quasi-orders are, in some sense, the best rings of a given size. The finite field  $\text{GF}(p^k)$  is always maximal (Theorem 2.2.16), but it follows from these results that, whenever  $k = 5$  or  $k \geq 7$ , there are other maximal rings of size  $p^k$ .  $\text{GF}(8) \times \text{GF}(4)$  is the smallest such maximal commutative ring (Corollary 2.5.10). In particular, it follows that there exist networks with scalar linear solutions over some ring of size  $p^k$  but not the field  $\text{GF}(p^k)$ , whenever  $k \notin \{1, 2, 3, 4, 6\}$ . The maximal rings of size  $p_1^{k_1} \cdots p_t^{k_t}$  (for distinct primes  $p_1, \dots, p_t$ ) are direct products of maximal rings of size  $p_1^{k_1}, \dots, p_t^{k_t}$  (Remark 2.5.5).

## 2.2 Ring Dominance

A *quasi-order*<sup>2</sup>  $\preceq$  on a set  $A$  is a subset of  $A \times A$  that is reflexive and transitive. We write  $x \preceq y$  to indicate that the pair  $(x, y)$  is in the relation. Each quasi-order induces an equivalence relation on  $A$  defined by  $x \equiv y$  if and only if  $x \preceq y$  and  $y \preceq x$ . We denote the equivalence class of  $x$  by  $[x]$ . Any quasi-order naturally extends to a partial order on the equivalence classes by defining  $[x] \preceq [y]$  if and only if  $x \preceq y$ . An element  $x \in A$  is said to be *maximal* with respect to the quasi-order if for all  $y \in A$ , we have  $y \preceq x$  whenever  $x \preceq y$ . The same definition of maximal applies with respect to the induced partial order on equivalence classes.

For each integer  $m \geq 2$  and each finite ring  $R$ ,

- $\mathcal{R}(m)$  denotes the set of commutative rings of size  $m$ , up to isomorphism,
- $\cong$  denotes ring isomorphism, and
- $\mathcal{N}_{\text{lin}}(R)$  denotes the set of all networks scalar linearly solvable over  $R$ .

**Definition 2.2.1.** For any two finite rings  $R$  and  $S$ , we say  $S$  is *dominated by*  $R$  (denoted  $S \preceq R$ ) if every network that is scalar linearly solvable over  $S$  is also scalar linearly solvable over  $R$ . Equivalently,  $S \preceq R$  if and only if  $\mathcal{N}_{\text{lin}}(S) \subseteq \mathcal{N}_{\text{lin}}(R)$ .

On the other hand,  $S$  is not dominated by  $R$  whenever there exists a network with a scalar linear solution over  $S$  but not over  $R$ . Intuitively, if a ring  $R$  dominates a ring  $S$  of the same size, it may be viewed as advantageous<sup>3</sup> to use  $R$  instead of  $S$  in a network coding implementation, since any network that is scalar linearly solvable over  $S$  is also scalar linearly solvable over  $R$ . If, additionally,  $\mathcal{N}_{\text{lin}}(S) \subset \mathcal{N}_{\text{lin}}(R)$  then even more networks are scalar linearly solvable over  $R$ . This dominance relation gives us a reasonable way of comparing rings with respect to linear network coding.

For each  $m \geq 2$ , it can be verified that the relation  $\preceq$  is a quasi-order on the set  $\mathcal{R}(m)$ . The induced equivalence relation on rings has the property that  $R \equiv S$  if and only if  $\mathcal{N}_{\text{lin}}(R) = \mathcal{N}_{\text{lin}}(S)$ . It turns out that the exact same set of networks can sometimes be scalar linearly solvable over non-isomorphic rings of the same size (as illustrated later, in Theorem 2.2.19 and Corollary 2.3.3), which means that the quasi-order  $\preceq$  is not anti-symmetric on  $\mathcal{R}(m)$ . This also means that  $\preceq$  is not generally a partial order.

<sup>2</sup>Also known as a *pre-order* (e.g. [31, Chapter 1]).

<sup>3</sup>There may be other advantages to using one ring over another, such as lower computational complexity arithmetic, ease of implementation, etc.

Throughout this chapter, whenever we refer to a finite commutative ring as being *maximal*, we mean the ring is maximal with respect to the relation  $\preceq$  on the set of commutative rings of the same size. A maximal commutative ring  $R$  has the desirable property that, for any commutative ring  $S$  of the same size, the set of networks that are scalar linearly solvable over  $R$  cannot be a proper subset of the set of networks that are scalar linearly solvable over  $S$ . Thus, in this sense, maximal rings may be considered the “best” commutative rings to use for network coding, and non-maximal rings are always “worse” than some maximal ring of the same size.

**Remark 2.2.2.** *Every commutative ring of size  $m$  is dominated by a maximal commutative ring of size  $m$ , since  $\mathcal{R}(m)$  is a finite quasi-order. Hence any network that is linearly solvable over some commutative ring of size  $m$  is linearly solvable over some maximal commutative ring of size  $m$ .*

### 2.2.1 Fundamental Ring Comparisons

We now prove results on ring dominance that will be used throughout the rest of the chapter.

For each integer  $m \geq 2$ , the *Char- $m$  Network* is given in Figure 2.3. This network was introduced as  $\mathcal{N}_2(m, 1)$  (with a slight relabeling of sources) in [4] and is a generalization of the Fano Network. We use this class of networks to demonstrate some interesting properties of scalar linear codes over rings. The following lemma was shown in [4, Lemma IV.6] in a slightly more general form.

**Lemma 2.2.3.** *For each finite ring  $R$  and integer  $m \geq 2$ , the Char- $m$  Network is scalar linearly solvable over  $R$  if and only if  $\text{char}(R) \mid m$ .*

In particular, if  $R$  is a finite ring such that  $\text{char}(R) \mid m$ , then  $m = 0$  in  $R$ , and the following scalar linear code over  $R$  is a solution for the Char- $m$  Network:

$$e_i = \sum_{\substack{j=0 \\ j \neq i}}^m x_j \quad \text{and} \quad e = \sum_{j=0}^m x_j$$

where  $i = 0, 1, \dots, m+1$ , and the receivers linearly recover their demands as follows

$$R_i : e - e_i = x_i \quad \text{and} \quad R_x : \sum_{i=1}^{m+1} e_i = x_0 + m \sum_{i=0}^{m+1} x_i = x_0 \quad [\text{from } \text{char}(R) \mid m].$$

On the other hand, if  $\text{char}(R) \nmid m$ , then  $m \neq 0$  in  $R$ , so this code is not a solution in this case, which agrees with Lemma 2.2.3.



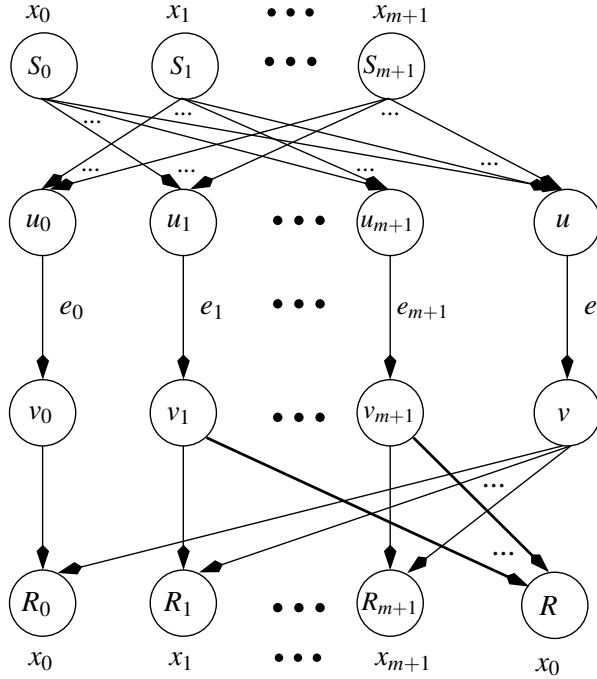


Figure 2.3: The Char- $m$  Network has source nodes  $S_0, S_1, \dots, S_{m+1}$  which generate the messages  $x_0, x_1, \dots, x_{m+1}$ , respectively. The node  $u$  has a single incoming edge from each source node, and the edge connecting nodes  $u$  and  $v$  carries the edge symbol  $e$ . For each  $i = 0, 1, \dots, m + 1$ , the node  $u_i$  has a single incoming edge from each source node, except  $S_i$ . The edge connecting nodes  $u_i$  and  $v_i$  carries the edge symbol  $e_i$ . The receiver  $R_i$  demands  $x_i$  and has an incoming edge from node  $v_i$  and an incoming edge from  $v$ . The receiver  $R$  demands  $x_0$  and has an incoming edge from each of the nodes  $v_1, \dots, v_{m+1}$ .

The following corollary demonstrates that rings whose sizes are powers of distinct primes cannot dominate one another. Our focus on comparing rings of the same size is driven in part from a practical standpoint, i.e. determining the “best” rings of a given size. However, the study of dominance is also more interesting when applied to rings whose sizes are powers of the same prime, particularly rings of the same size.

**Corollary 2.2.4.** *Let  $p$  and  $q$  be distinct primes, and let  $k$  and  $n$  be positive integers. No ring of size  $p^k$  is dominated by a ring of size  $q^n$ .*

*Proof.* The characteristic of any ring of size  $p^k$  must divide  $p^k$ , so by taking  $m = p^k$  in Lemma 2.2.3, the Char- $p^k$  Network is scalar linearly solvable over any ring of size  $p^k$ , but this network is not scalar linearly solvable over any ring of size  $q^n$ , since  $p$  and  $q$  are distinct primes. Hence, no ring of size  $p^k$  is dominated by a ring of size  $q^n$ . ■

The following lemma is also shown in Chapter 3 Corollary 3.1.7, where it follows from a more general result on linear codes over modules. However, we include the proof of Lemma 2.2.5 in this chapter for completeness.

A ring homomorphism is a mapping that preserves the additive and multiplicative structure of rings. Intuitively, a linear code consists of addition and multiplication operations, so taking the image of linear coding coefficients under the homomorphisms should preserve the structure of the code. In fact, this lemma shows that ring homomorphisms induce ring dominance.

**Lemma 2.2.5.** *Let  $R$  and  $S$  be finite rings. If  $\phi : S \rightarrow R$  is a homomorphism, then  $S$  is dominated by  $R$ .*

*Proof.* Let  $\mathcal{N}$  be a network that has a scalar linear solution over  $S$ . Suppose the inputs to a node in a scalar linear solution over  $S$  are  $x_1, \dots, x_m \in S$  and can be written in terms of the messages  $z_1, \dots, z_n \in S$  in the following way

$$x_i = \sum_{j=1}^n B_{i,j} z_j \quad (2.1)$$

where  $B_{i,1}, \dots, B_{i,n} \in S$  are constants. Then any output  $y \in S$  of the node is of the form

$$y = \sum_{i=1}^m C_i x_i \quad (2.2)$$

$$= \sum_{j=1}^n \left( \sum_{i=1}^m C_i B_{i,j} \right) z_j \quad \text{[from (2.1)]} \quad (2.3)$$

for some constants  $C_1, \dots, C_m \in S$ . Then (2.2) describes  $y$  in terms of the inputs to the node, and (2.3) describes  $y$  in terms of the messages of the network.

Form a scalar linear code for  $\mathcal{N}$  over  $R$  by replacing each coefficient  $C_i$  in (2.2) by  $\phi(C_i)$ . In other words, the coefficients in  $R$  that describe the linear combinations of the inputs at a node are the image under  $\phi$  of the corresponding coefficients in  $S$ . We will now show that the coefficients in  $R$  that describe the linear combinations of the messages at a node are the image under  $\phi$  of the corresponding coefficients in  $S$ .

Assume the corresponding inputs to the node in the linear code over  $R$  are  $x'_1, \dots, x'_m \in R$  and can be written in terms of the messages  $z'_1, \dots, z'_n \in R$  in the following way

$$x'_i = \sum_{j=1}^n \phi(B_{i,j}) z'_j. \quad (2.4)$$

i.e. the inputs to the node in the linear code over  $R$  are such that the coefficients are the image under  $\phi$  of the corresponding coefficients in  $S$ . Then, since homomorphisms preserve addition and multiplication, the

corresponding output  $y' \in R$  of the node is of the form

$$\begin{aligned}
y' &= \sum_{i=1}^m \phi(C_i) x'_i \\
&= \sum_{i=1}^m \phi(C_i) \sum_{j=1}^n \phi(B_{i,j}) z'_j && \text{[from (2.1)]} \\
&= \sum_{j=1}^n \sum_{i=1}^m \phi(C_i) \phi(B_{i,j}) z'_j \\
&= \sum_{j=1}^n \phi \left( \sum_{i=1}^m C_i B_{i,j} \right) z'_j && (2.5)
\end{aligned}$$

so the coefficients in  $R$  that describe the linear combinations of the messages at a node in (2.5) are the image under  $\phi$  of the corresponding coefficients in  $S$  in (2.3).

If a decoding function in the linear solution over  $S$  produces the message  $z_l$ , then in (2.3)

$$\sum_{i=1}^m C_i B_{i,j} = \begin{cases} 1 & \text{if } j = l \\ 0 & \text{if } j \neq l. \end{cases}$$

Since  $\phi$  is a homomorphism,  $\phi(1) = 1$  and  $\phi(0) = 0$ , so the corresponding coefficients in (2.5) are

$$\phi \left( \sum_{i=1}^m C_i B_{i,j} \right) = \begin{cases} 1 & \text{if } j = l \\ 0 & \text{if } j \neq l \end{cases}$$

so the decoding function in the linear code over  $R$  produces the message  $z'_l$ . Thus each receiver recovers its demands in the scalar linear code over  $R$ , so the code is, in fact, a solution for  $\mathcal{N}$ . Therefore  $S \preceq R$ . ■

The following corollary is a special case of Lemma 2.2.5, where  $S$  is a *subring* of  $R$ . A subring  $S$  of  $R$  is a subset of  $R$  that is closed under addition and multiplication and  $0, 1 \in S$ . A further special case, which will be used frequently throughout the rest of the chapter, is when  $R = \text{GF}(p^k)$  and  $S = \text{GF}(p^m)$  where  $p$  is prime and  $k, m$  are positive integers such that  $m$  divides  $k$  (e.g. see [3, Theorem 2.3.1]). We also remark that for finite rings  $R_1$  and  $R_2$ , the multiplicative identity of  $R_1 \times R_2$  is in neither  $R_1$  nor  $R_2$ , so while  $R_1$  and  $R_2$  are isomorphic to subsets of  $R_1 \times R_2$  that are closed under addition and multiplication, neither is a subring of  $R_1 \times R_2$ .

**Corollary 2.2.6.** *If  $S$  is a subring of a finite commutative ring  $R$ , then  $S$  is dominated by  $R$ .*

*Proof.* If  $S$  is a subring of  $R$ , then the identity mapping from  $S$  to  $R$  is an injective homomorphism, so by Lemma 2.2.5,  $S \preceq R$ . ■

In general, if a network is scalar linearly solvable over an alphabet  $\mathcal{A}$ , then it is also scalar linearly solvable over the alphabet  $\mathcal{A}^k$ , for any  $k \geq 2$ , by using a Cartesian product code.<sup>4</sup> In particular, if a network is scalar linearly solvable over the ring  $\mathbb{Z}_n$ , then it is also scalar linearly solvable over the direct product of rings  $\mathbb{Z}_n^k = \underbrace{\mathbb{Z}_n \times \cdots \times \mathbb{Z}_n}_{k \text{ times}}$ . Since  $\mathbb{Z}_n^k$  is not isomorphic to the product ring  $\mathbb{Z}_n^k$ , it does not immediately follow that a network scalar linearly solvable over  $\mathbb{Z}_n$  must also be scalar linearly solvable over  $\mathbb{Z}_n^k$ , and, in fact, the contrary is demonstrated below in Corollary 2.2.7.

**Corollary 2.2.7.** *Let  $m, n \geq 2$ . The ring  $\mathbb{Z}_m$  is dominated by the ring  $\mathbb{Z}_n$  if and only if  $n \mid m$ .*

*Proof.* Let  $\phi : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$  be defined such that  $\phi(a)$  is the unique integer in  $\{0, 1, \dots, n-1\}$  satisfying  $\phi(a) = a \bmod n$ . If  $n \mid m$ , then  $\phi$  is a surjective homomorphism, so by Lemma 2.2.5 we have  $\mathbb{Z}_m \preceq \mathbb{Z}_n$ . Conversely, if  $n \nmid m$ , then by Lemma 2.2.3, the Char- $m$  Network is scalar linearly solvable over  $\mathbb{Z}_m$  but not  $\mathbb{Z}_n$ , since  $\text{char}(\mathbb{Z}_m) = m \mid m$  and  $\text{char}(\mathbb{Z}_n) = n \nmid m$ , which implies  $\mathbb{Z}_m$  is not dominated by  $\mathbb{Z}_n$ . ■

If  $p$  is prime and  $k \geq 2$ , then by Corollary 2.2.7, we have  $\mathcal{N}_{\text{lin}}(\mathbb{Z}_{p^k}) \subset \mathcal{N}_{\text{lin}}(\mathbb{Z}_p)$ . In this sense, the larger ring alphabet  $\mathbb{Z}_{p^k}$  is strictly “worse” than the smaller field alphabet  $\mathbb{Z}_p$ . This contrasts significantly with finite fields, where, generally speaking, larger field alphabets are “better” than smaller field alphabets. In particular, it follows from Corollary 2.2.6 and Lemma 2.2.15 that  $\mathcal{N}_{\text{lin}}(\text{GF}(p)) \subset \mathcal{N}_{\text{lin}}(\text{GF}(p^k))$ .

## 2.2.2 Minimizing Alphabet Size

In this section, we prove our main result (Theorem 2.2.10) on minimizing the alphabet size needed for a scalar linear solution over a commutative ring. The following lemma is a standard result of algebra related to ideals of rings which will be used to show Corollary 2.2.9.

**Lemma 2.2.8.** [12, Theorem 7, p. 243]: *If  $I$  is a two-sided ideal of ring  $R$ , then the mapping  $\phi : R \rightarrow R/I$  given by  $\phi(x) = x + I$  is a surjective homomorphism.*

Corollary 2.2.9 demonstrates that rings with large ideals are “bad” in the sense that they are always dominated by a smaller ring. Intuitively, rings without ideals should minimize the ring-size needed for a scalar linear solution. We formalize this notion in Theorem 2.2.10.

**Corollary 2.2.9.** *If  $I$  is a proper ideal in a finite commutative ring  $R$ , then  $R$  is dominated by  $R/I$ .*

*Proof.* The quotient ring  $R/I$  is finite and commutative. By Lemma 2.2.8, there is a surjective homomorphism from  $R$  to  $R/I$ , so  $R \preceq R/I$  by Lemma 2.2.5. ■

---

<sup>4</sup>In fact, the network is solvable over any alphabet of size  $|\mathcal{A}|^k$  but linearity may not be preserved.

Theorem 2.2.10 next demonstrates that when attempting to find a minimum size commutative ring over which a network is scalar linearly solvable, it suffices to restrict attention to finite field alphabets.

**Theorem 2.2.10.** *If a network is scalar linearly solvable over a commutative ring, then the unique smallest such ring is a field.*

*Proof.* Let  $\mathcal{N}$  be a scalar linearly solvable network and let  $R$  be a smallest commutative ring over which  $\mathcal{N}$  is scalar linearly solvable. Suppose  $R$  is not a finite field, and let  $I$  be a maximal ideal<sup>5</sup> of  $R$ . Since  $\{0\}$  is an ideal in every ring,  $R$  must have at least one maximal (proper) ideal. Then  $R/I$  is a field (e.g. see [12, p. 254, Proposition 12]). By Lemma 2.2.8, there is a surjective homomorphism from  $R$  to  $R/I$ , but  $R/I$  is a field and  $R$  is not, so the rings cannot be isomorphic. Therefore,  $|R/I| < |R|$ . By Corollary 2.2.9,  $R \preceq R/I$ . Thus  $\mathcal{N}$  must also be scalar linearly solvable over  $R/I$ , which contradicts the assumption that  $R$  is a smallest commutative ring over which  $\mathcal{N}$  is scalar linearly solvable. ■

### 2.2.3 Direct Products of Rings

Sun, Yin, Li, and Long [33] presented a class of multicast networks, called *Swirl Networks*, parameterized by an integer  $\omega \geq 3$  that affects the number of independent messages generated by the source as well as the number of receivers and intermediate nodes. An interesting open question is for which  $p$  and  $k$  does there exist a multicast network that is scalar linearly solvable over some ring of size  $p^k$  but not over the field of the same size. Example 2.2.11 demonstrates a particular Swirl Network is such a multicast network for  $p = 2$  and  $k = 13$ .

**Example 2.2.11.** It was shown in [33, p. 6185] that the Swirl Network with  $\omega = 2^{13}$  is scalar linearly solvable over  $\text{GF}(2^9)$  and  $\text{GF}(2^4)$  but not over  $\text{GF}(2^{13})$ . By using a Cartesian product code, this Swirl Network is scalar linearly solvable over the ring  $\text{GF}(2^9) \times \text{GF}(2^4)$ .

The following lemma relates Cartesian product codes and the dominance relation.

**Lemma 2.2.12.** *A network is scalar linearly solvable over a finite direct product of finite rings if and only if the network is scalar linearly solvable over each ring in the product.*

---

<sup>5</sup>Whenever we refer to a maximal ideal, we will always mean maximal with respect to set inclusion.

*Proof.* Let  $R_1, \dots, R_m$  be finite rings. Any network that is scalar linearly solvable over each of the rings  $R_1, \dots, R_m$ , is clearly scalar linearly solvable over the product ring  $R_1 \times \dots \times R_m$  by using a Cartesian product code of the scalar linear solutions over each  $R_1, \dots, R_m$ . Conversely, for each  $j = 1, \dots, m$ , the projection mapping  $\phi_j : R_1 \times \dots \times R_m \rightarrow R_j$  defined by  $\phi_j(x_1, \dots, x_m) = x_j$  is a surjective homomorphism, so by Lemma 2.2.5,  $R_1 \times \dots \times R_m \preceq R_j$  and thus any network that is scalar linearly solvable over the product ring  $R_1 \times \dots \times R_m$  is also scalar linearly solvable over each ring  $R_1, \dots, R_m$ . ■

Lemma 2.2.13 demonstrates that if each ring in a collection of rings dominates at least one ring in a second collection of rings, then the direct product of the rings in the first collection dominates the direct product of the rings in the second collection.

**Lemma 2.2.13.** *If each of the finite rings  $S_1, \dots, S_n$  is dominated by at least one of the finite rings  $R_1, \dots, R_m$ , then  $S_1 \times \dots \times S_n$  is dominated by  $R_1 \times \dots \times R_m$ .*

*Proof.* Let  $\mathcal{N}$  be a network that is scalar linearly solvable over  $S_1 \times \dots \times S_n$ . Let  $i \in \{1, \dots, m\}$  and let  $j$  be such that  $S_j \preceq R_i$ . By Lemma 2.2.12,  $\mathcal{N}$  is scalar linearly solvable over  $S_j$ , so  $\mathcal{N}$  is scalar linearly solvable over  $R_i$ . Thus by Lemma 2.2.12, since  $i$  was chosen arbitrarily,  $\mathcal{N}$  is also scalar linearly solvable over  $R_1 \times \dots \times R_m$ . ■

The following remark notes that two rings of different sizes can each dominate the other.

**Remark 2.2.14.** *For each finite ring  $R$  and all positive integers  $m, n$ , the direct product rings  $\underbrace{R \times \dots \times R}_{n \text{ times}}$  and  $\underbrace{R \times \dots \times R}_{m \text{ times}}$  each dominate the other by Lemma 2.2.13.*

## 2.2.4 The $n$ -Choose-Two Networks

Figure 2.4 shows a multicast network studied by Rasala Lehman and Lehman [29], which we call the  $n$ -Choose-Two Network. This network will be used to illustrate various facts in what follows. The network has two messages  $x$  and  $y$ , intermediate edge symbols  $\lambda_1, \dots, \lambda_n$ , and  $\binom{n}{2}$  receivers. Each receiver receives a unique pair of symbols  $(\lambda_i, \lambda_j)$ , where  $i < j$ , and must decode both messages  $x$  and  $y$ . The following lemma was shown in [29], and it characterizes the finite fields over which a scalar linear solution to the  $n$ -Choose-Two Network exists and gives an alphabet-size condition necessary for solvability.

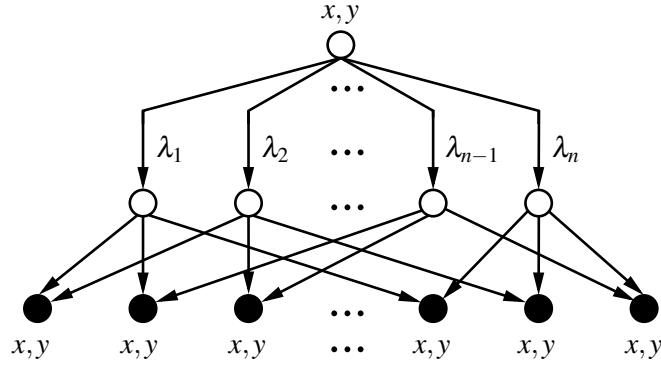


Figure 2.4: The  $n$ -Choose-Two Network is parameterized by an integer  $n \geq 2$ . The network's name indicates the number of receivers.

**Lemma 2.2.15.** [29, p. 144]: Let  $n \geq 3$ .

- (a) If the  $n$ -Choose-Two Network has a solution over an alphabet  $\mathcal{A}$ , then  $|\mathcal{A}| \geq n - 1$ .
- (b) The  $n$ -Choose-Two Network is scalar linearly solvable over a field  $\mathbb{F}$  if and only if  $|\mathbb{F}| \geq n - 1$ .

The following theorem demonstrates that for each finite field, there exists a multicast network that is scalar linearly solvable over the field but is not scalar linearly solvable over any other commutative ring of the same size. Theorem 2.2.16 additionally implies that  $\text{GF}(p^k)$  is not dominated by any other commutative ring of size  $p^k$ , which implies that  $\text{GF}(p^k)$  is maximal with respect to the quasi-order of commutative rings of size  $p^k$ .

**Theorem 2.2.16.** For each prime  $p$  and positive integer  $k$ , the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable over the field  $\text{GF}(p^k)$  but not over any other commutative ring of size  $p^k$ .

*Proof.* Lemma 2.2.15 (b) implies that the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p^k)$ . On the other hand, if the  $(p^k + 1)$ -Choose-Two Network network were scalar linearly solvable over a commutative ring  $R$  of size  $p^k$  that is not a field, then by Theorem 2.2.10, it would also be scalar linearly solvable over some field whose size is less than  $p^k$ , which would contradict Lemma 2.2.15. ■

The following theorem gives a necessary and sufficient condition on the alphabet sizes over which a scalar linear solution to the  $n$ -Choose-Two Network exists for at least one ring.

**Theorem 2.2.17.** *Let  $m = p_1^{k_1} \cdots p_t^{k_t}$  be the prime factorization of  $m \geq 2$ , and let  $n \geq 3$ . The  $n$ -Choose-Two Network is scalar linearly solvable over some ring of size  $m$  if and only if  $p_i^{k_i} \geq n - 1$  for each  $i$ .*

*Proof.* Assume  $p_i^{k_i} \geq n - 1$ . Then by Lemma 2.2.15 (b), the  $n$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p_i^{k_i})$ . So by Lemma 2.2.12, the  $n$ -Choose-Two Network is scalar linearly solvable over the product ring  $\text{GF}(p_1^{k_1}) \times \cdots \times \text{GF}(p_t^{k_t})$  which has cardinality  $m$ .

Conversely, suppose  $m = p_1^{k_1} \cdots p_t^{k_t}$  and the  $n$ -Choose-Two Network is scalar linearly solvable over a ring  $R$  of size  $m$ .  $R$  is isomorphic to a direct product of rings of size  $p_1^{k_1}, \dots, p_t^{k_t}$  (e.g. see [27, p. 2]). For each  $i = 1, \dots, t$ , let  $R_i$  be the ring of size  $p_i^{k_i}$ . Then by Lemma 2.2.12, the  $n$ -Choose-Two Network is scalar linearly solvable over each of  $R_1, \dots, R_t$ . Hence by Lemma 2.2.15 (a), we must have  $p_i^{k_i} \geq n - 1$  for all  $i$ . ■

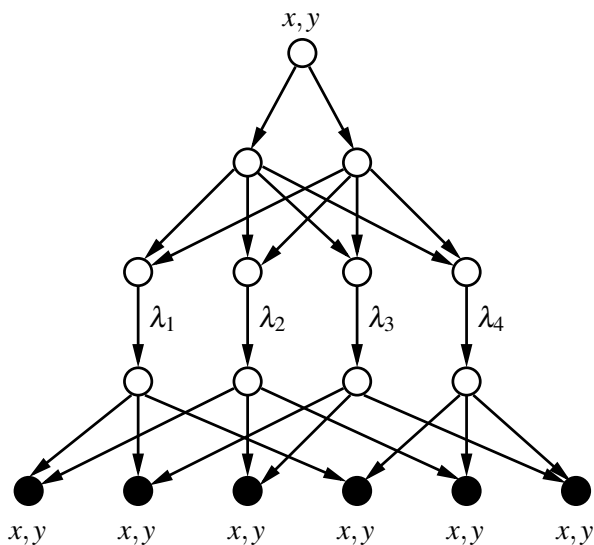


Figure 2.5: The Two-Six Network is a multicast network studied in [10]. Each of the receivers gets a unique pair of edge symbols  $(\lambda_i, \lambda_j)$ , where  $i < j$ . The network's name indicates the alphabet sizes over which the network is not solvable.

A variation of the 4-Choose-Two Network, called the *Two-Six Network*, is given in Figure 2.5. The Two-Six Network was used in [10] to show that a multicast network with a solution over a given alphabet size might not have a solution over all larger alphabet sizes. Corollary 2.2.18 gives conditions on the solvability and scalar linear solvability of the Two-Six Network. We use the fact that the Two-Six Network is equivalent in terms of solvability to the 4-Choose-Two Network.



**Corollary 2.2.18.** *For each  $m \geq 2$ , the Two-Six Network is:*

- (a) *Solvable over an alphabet of size  $m$  if and only if  $m \notin \{2, 6\}$ .*
- (b) *Scalar linearly solvable over some ring of size  $m$  if and only if  $m \not\equiv 2 \pmod{4}$ .*
- (c) *Scalar linearly solvable over all finite fields except  $\text{GF}(2)$ .*

*Proof.* Part (a) is [10, Lemma V.3]. Parts (b) and (c) follow immediately from Lemma 2.2.15 and Theorem 2.2.17, respectively, when  $n = 4$ . ■

The proof of Corollary 2.2.18 (a) (i.e. Lemma V.3 in [10]) made use of a theorem characterizing the orders for which orthogonal latin squares exist. Euler originally conjectured over 230 years ago that orthogonal latin squares existed for all orders not congruent to 2 mod 4. It turned out that Euler was incorrect, and it was shown in 1960 that orthogonal latin squares existed for all orders except 2 and 6. Interestingly, the Two-Six Network was shown in Corollary 2.2.18 to be solvable for all alphabet sizes except 2 and 6 and scalar linearly solvable over some ring of every size that is not congruent to 2 mod 4.

Li, Yeung, and Cai [26] showed that every solvable multicast network is scalar linearly solvable over every sufficiently large finite field. We observe that this property is not true for finite rings, as the Two-Six Network is a solvable multicast network and is not scalar linearly solvable over any ring whose size is 2 mod 4.

### 2.2.5 Rings of Size $p^2$

Remark 2.2.14 demonstrated that it is possible for the exact same set of networks to be scalar linearly solvable over two rings of different sizes. The following theorem shows that, for each prime  $p$ , this is also possible for two rings of size  $p^2$ , i.e. it is possible to have two non-isomorphic commutative rings of size  $p^2$ , such that the rings are equivalent under dominance.

**Theorem 2.2.19.** *For each prime  $p$ , the rings  $\text{GF}(p)[x]/\langle x^2 \rangle$  and  $\text{GF}(p) \times \text{GF}(p)$  are each dominated by the other but are not isomorphic.*

*Proof.* The rings are clearly not isomorphic since the only element of  $\text{GF}(p) \times \text{GF}(p)$  whose square is zero is zero itself, and in  $\text{GF}(p)[x]/\langle x^2 \rangle$ , the squares of both zero and  $x$  are zero. The field  $\text{GF}(p)$  is a

subring of  $\text{GF}(p)[x]/\langle x^2 \rangle$ , so by Corollary 2.2.6,  $\text{GF}(p) \preceq \text{GF}(p)[x]/\langle x^2 \rangle$ . On the other hand, the mapping  $\phi : \text{GF}(p)[x]/\langle x^2 \rangle \rightarrow \text{GF}(p)$  given by  $\phi(a + bx) = a$  is a surjective homomorphism, so by Lemma 2.2.5,  $\text{GF}(p)[x]/\langle x^2 \rangle \preceq \text{GF}(p)$ . Thus,  $\text{GF}(p) \equiv \text{GF}(p)[x]/\langle x^2 \rangle$  and by Lemma 2.2.12,  $\text{GF}(p) \times \text{GF}(p) \equiv \text{GF}(p)$ . ■

In the proof of the previous theorem it is shown that  $\text{GF}(p) \equiv \text{GF}(p)[x]/\langle x^2 \rangle$  which is another interesting example of rings of different sizes being equivalent under dominance. It is known [17, Theorem 2, p. 250] that, for each prime  $p$ , the only four commutative rings of size  $p^2$  are  $\text{GF}(p^2)$ ,  $\text{GF}(p) \times \text{GF}(p)$ ,  $\mathbb{Z}_{p^2}$ , and  $\text{GF}(p)[x]/\langle x^2 \rangle$ . The following theorem describes a chain of dominances between these rings and shows that dominance is a total quasi-order of the commutative rings of size  $p^2$ .

**Theorem 2.2.20.** *For each prime  $p$ , the four commutative rings of size  $p^2$  satisfy*

$$\mathcal{N}_{\text{lin}}(\mathbb{Z}_{p^2}) \subset \mathcal{N}_{\text{lin}}(\text{GF}(p)[x]/\langle x^2 \rangle) = \mathcal{N}_{\text{lin}}(\text{GF}(p) \times \text{GF}(p)) \subset \mathcal{N}_{\text{lin}}(\text{GF}(p^2)).$$

*Proof.* The field  $\text{GF}(p)$  is a subring of the field  $\text{GF}(p^2)$ , so by Corollary 2.2.6,  $\text{GF}(p) \preceq \text{GF}(p^2)$ . This, along with the fact the  $(p^2 + 1)$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p^2)$  but not  $\text{GF}(p)$  (via Lemma 2.2.15), implies  $\mathcal{N}_{\text{lin}}(\text{GF}(p)) \subset \mathcal{N}_{\text{lin}}(\text{GF}(p^2))$ . By Theorem 2.2.19 and Corollary 2.2.7, we also have  $\mathbb{Z}_{p^2} \preceq \text{GF}(p) \equiv \text{GF}(p) \times \text{GF}(p) \equiv \text{GF}(p)[x]/\langle x^2 \rangle$ . Additionally, by Lemma 2.2.3, the Char- $p$  Network is scalar linearly solvable over  $\text{GF}(p)$  but not  $\mathbb{Z}_{p^2}$ , thus proving the claim. ■

## 2.3 Finite Field Dominance

A ring  $R$  does not dominate the ring  $S$  whenever there exists a network that is scalar linearly solvable over  $S$  but not over  $R$ . The following lemma demonstrates a class of non-multicast networks that will be used in later proofs to show a given ring is not dominated by another given ring. Such networks are scalar linearly solvable only over certain fields.

**Lemma 2.3.1.** [9, Section VI, Example (7)]: *For any primes  $q_1, \dots, q_s$  and positive integers  $m_1, \dots, m_s$ , there exists a network that is scalar linearly solvable over the fields  $\text{GF}(q_1^{nm_1}), \dots, \text{GF}(q_s^{nm_s})$  for all  $n \geq 1$ , but not over any other fields.*

Note that the primes  $q_1, \dots, q_s$  in Lemma 2.3.1 need not be distinct. The following lemma will enable us to demonstrate certain networks that are scalar linearly solvable over some ring of prime power

size but not over the field of the same size. Lemma 2.3.2 will also be used in some of the proofs in Section 2.5.

**Lemma 2.3.2.** *Let  $p_1, \dots, p_r$  and  $q_1, \dots, q_s$  be primes, and let  $k_1, \dots, k_r$  and  $m_1, \dots, m_s$  be positive integers. The ring  $\text{GF}(q_1^{m_1}) \times \dots \times \text{GF}(q_s^{m_s})$  is dominated by the ring  $\text{GF}(p_1^{k_1}) \times \dots \times \text{GF}(p_r^{k_r})$  if and only if for each  $i \in \{1, \dots, r\}$  there exists  $j \in \{1, \dots, s\}$  such that  $q_j = p_i$  and  $m_j \mid k_i$ .*

*Proof.* If, for each  $i$ , there is a  $j$  such that  $q_j = p_i$  and  $m_j \mid k_i$ , then  $\text{GF}(q_j^{m_j})$  is a subring of  $\text{GF}(p_i^{k_i})$  so by Corollary 2.2.6,  $\text{GF}(q_j^{m_j}) \preceq \text{GF}(p_i^{k_i})$  and therefore, by Lemma 2.2.13,  $\text{GF}(q_1^{m_1}) \times \dots \times \text{GF}(q_s^{m_s}) \preceq \text{GF}(p_1^{k_1}) \times \dots \times \text{GF}(p_r^{k_r})$ .

To prove the converse, suppose to the contrary that there exists  $i \in \{1, \dots, r\}$  such that for all  $j \in \{1, \dots, s\}$ , either  $q_j \neq p_i$  or  $m_j \nmid k_i$ . By Lemma 2.3.1, there exists a network  $\mathcal{N}$  that is scalar linearly solvable precisely over those fields of size  $q_j^{m_j}$ , where  $j \in \{1, \dots, s\}$  and  $n \geq 1$ . Taking  $n = 1$  and applying Lemma 2.2.12, implies that  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(q_1^{m_1}) \times \dots \times \text{GF}(q_s^{m_s})$ . But  $\mathcal{N}$  can not be scalar linearly solvable over  $\text{GF}(p_i^{k_i})$ , since for all  $j \in \{1, \dots, s\}$ , either  $q_j \neq p_i$  or  $m_j \nmid k_i$ , so by Lemma 2.2.12,  $\mathcal{N}$  is not scalar linearly solvable over  $\text{GF}(p_1^{k_1}) \times \dots \times \text{GF}(p_r^{k_r})$ . Thus,  $\text{GF}(q_1^{m_1}) \times \dots \times \text{GF}(q_s^{m_s}) \not\preceq \text{GF}(p_1^{k_1}) \times \dots \times \text{GF}(p_r^{k_r})$ . ■

As in Theorem 2.2.19, the following corollary demonstrates that two non-isomorphic commutative rings of the same size may be equivalent with respect to the dominance relation  $\preceq$ . In this case, the rings are both direct products of fields.

**Corollary 2.3.3.** *For each  $k \geq 3$  and prime  $p$ , the rings  $\text{GF}(p^{k-1}) \times \text{GF}(p)$  and  $\text{GF}(p^{k-2}) \times \text{GF}(p) \times \text{GF}(p)$  each dominate the other.*

*Proof.* The result follows from Lemma 2.3.2 by taking  $r = 2, s = 3, p_1 = p_2 = q_1 = q_2 = q_3 = p, k_1 = k - 1, m_1 = k - 2$ , and  $k_2 = m_2 = m_3 = 1$  to get  $\text{GF}(p^{k-2}) \times \text{GF}(p) \times \text{GF}(p) \preceq \text{GF}(p^{k-1}) \times \text{GF}(p)$ , and by taking  $r = 3, s = 2, p_1 = p_2 = p_3 = q_1 = q_2 = p, k_1 = k - 2, m_1 = k - 1$ , and  $k_2 = k_3 = m_2 = 1$  to get  $\text{GF}(p^{k-1}) \times \text{GF}(p) \preceq \text{GF}(p^{k-2}) \times \text{GF}(p) \times \text{GF}(p)$ . ■

Example 2.3.4 next demonstrates a network that is scalar linearly solvable over a ring of size 32 but is not scalar linearly solvable over the field of size 32. It turns out that 32 is the smallest prime power alphabet size for which a network can have a scalar linear solution over a commutative ring but not over the field of the same size (see Corollary 2.5.10).

**Example 2.3.4.** Taking  $r = 1, s = 2, p_1 = q_1 = q_2 = 2$  and  $k_1 = 5, k_2 = 3, k_3 = 2$  in Lemma 2.3.2 shows that  $\text{GF}(8) \times \text{GF}(4)$  is not dominated by  $\text{GF}(32)$ . In particular, there exists a network that is scalar linearly solvable over the ring  $\text{GF}(8) \times \text{GF}(4)$  but not over the field  $\text{GF}(32)$ .

Theorem 2.2.16 and Examples 2.2.11 and 2.3.4 also demonstrate that dominance is not necessarily a total quasi-order of the commutative rings of a given size, as there can exist rings of the same size such that neither dominates the other.

### 2.3.1 Local Rings

A finite commutative ring is said to be *local* if it has a single maximal ideal (see [3, Definition 1.2.9]). Lemmas 2.3.5 and 2.3.6 are standard results from commutative ring theory.

**Lemma 2.3.5.** [3, Theorem 3.1.4]: *Every finite commutative ring is a direct product of local rings.*

**Lemma 2.3.6.** [3, Theorem 6.1.2 II]: *If  $R$  is a finite commutative local ring with maximal ideal  $I$ , then there exists a prime  $p$  and positive integers  $k$  and  $m$  such that*

- (i)  $|R| = p^k$
- (ii)  $R/I$  is a field of size  $p^m$  and  $m$  divides  $k$ .

All finite fields are local rings, since their unique maximal ideal is the trivial ring  $\{0\}$ . The ring  $\mathbb{Z}_n$  is local if and only if  $n$  is a prime power, since for any prime divisor  $p$  of  $n$ ,  $\langle p \rangle = \{ap : a \in \mathbb{Z}_n\}$  is a maximal ideal of  $\mathbb{Z}_n$ . However, not every ring of prime power size is local. For example,  $\text{GF}(2) \times \text{GF}(2)$  has distinct maximal ideals  $\{(0,0), (1,0)\}$  and  $\{(0,0), (0,1)\}$ . The following lemma connects the algebraic concept of local rings to the dominance relation of network coding.

**Lemma 2.3.7.** *Every finite commutative local ring is dominated by the finite field of the same size.*

*Proof.* Let  $R$  be a finite commutative local ring with maximal ideal  $I$ . By Lemma 2.3.6, there exist a prime  $p$  and positive integers  $k$  and  $m$  such that  $|R| = p^k$ ,  $m \mid k$ , and  $R/I \cong \text{GF}(p^m)$ . Thus, by Corollary 2.2.9, we have  $R \preceq \text{GF}(p^m)$ , and since  $m \mid k$ , we have  $\text{GF}(p^m) \preceq \text{GF}(p^k)$  by Lemma 2.3.2. The lemma then follows from the transitivity of  $\preceq$ . ■

Example 2.3.4 demonstrated that there exists a network that is scalar linearly solvable over the ring  $\text{GF}(8) \times \text{GF}(4)$  but not over the field  $\text{GF}(32)$ . The following theorem strengthens the result in Example 2.3.4 by additionally showing the network is not even scalar linearly solvable over any other commutative ring of size 32. This contrasts with Theorem 2.2.16, which demonstrates a network that is scalar linearly solvable over  $\text{GF}(32)$  but not over any other commutative ring of size 32.

**Theorem 2.3.8.** *There exists a network that is scalar linearly solvable over  $\text{GF}(8) \times \text{GF}(4)$  but not over any other commutative ring of size 32.*

*Proof.* By Lemma 2.3.1, there exists a network  $\mathcal{N}$  that is scalar linearly solvable precisely over all fields whose size is of the form  $2^{2n}$  or  $2^{3n}$ , where  $n \geq 1$ . Hence  $\mathcal{N}$  is scalar linearly solvable over both  $\text{GF}(4)$  and  $\text{GF}(8)$  but neither  $\text{GF}(2)$  nor  $\text{GF}(32)$ . By using a product code,  $\mathcal{N}$  is also scalar linearly solvable over the ring  $\text{GF}(8) \times \text{GF}(4)$  of size 32. We will now show that  $\mathcal{N}$  is not scalar linearly solvable over any other commutative ring of size 32.

By Lemmas 2.3.5 and 2.3.6 (i), every commutative ring  $R$  of size 32 satisfies exactly one of the following seven properties:

- (a)  $R$  is a local ring of size 32
- (b)  $R$  is a direct product of local rings of size 16 and 2
- (c)  $R$  is a direct product of local rings of size 8 and 4
- (d)  $R$  is a direct product of local rings of size 8, 2, and 2
- (e)  $R$  is a direct product of local rings of size 4, 4, and 2
- (f)  $R$  is a direct product of local rings of size 4, 2, 2, and 2
- (g)  $R$  is a direct product of five local rings of size 2.

By Lemma 2.3.7, any network that is scalar linearly solvable over a commutative local ring of size 32 is also scalar linearly solvable over  $\text{GF}(32)$ . This eliminates case (a). Similarly, any network that is scalar linearly solvable over a local ring of size 2 is also scalar linearly solvable over  $\text{GF}(2)$ . By Lemma 2.2.12, any network that is scalar linearly solvable over a direct product ring is also scalar linearly solvable over every ring in the direct product. This eliminates cases (b),(d),(e),(f),(g). Thus if  $\mathcal{N}$  is scalar linearly solvable over a commutative ring  $R$  of size 32,  $R$  must satisfy case (c).

Suppose  $S$  is a commutative local ring of size 8 with maximal ideal  $I$ . Then Lemma 2.3.6 (ii) implies  $S/I \cong \text{GF}(2^m)$  for some  $m \in \{1, 3\}$ . If  $m = 3$ , then  $S \cong \text{GF}(8)$ , and if  $m = 1$ , then by Corollary 2.2.9,  $S \preceq \text{GF}(2)$ . Similarly, a commutative local ring of size 4 is either isomorphic to  $\text{GF}(4)$  or is dominated by  $\text{GF}(2)$ . Thus if  $\mathcal{N}$  is scalar linearly solvable over a ring  $R$  satisfying case (c), then  $R \cong \text{GF}(8) \times \text{GF}(4)$ ; otherwise, by Lemma 2.2.12, a scalar linear solution over  $R$  would imply there exists a scalar linear solution over  $\text{GF}(2)$ . Thus  $\text{GF}(8) \times \text{GF}(4)$  is the only commutative ring of size 32 over which  $\mathcal{N}$  is scalar linearly solvable. ■

Theorem 2.3.8 demonstrates that  $\text{GF}(8) \times \text{GF}(4)$  is not dominated by any other commutative ring of size 32 (including  $\text{GF}(32)$ ) and thus is maximal. On the other hand, Theorem 2.2.16 demonstrates that  $\text{GF}(32)$  is not dominated by any other commutative ring of size 32 (including  $\text{GF}(8) \times \text{GF}(4)$ ) and thus is maximal. In Section 2.5, we characterize all maximal rings, and we show that all maximal rings have the property that there exists some network that is scalar linearly solvable over the maximal ring but not over any other commutative ring of the same size, which agrees with Theorems 2.3.8 and 2.2.16.

The network in the previous theorem is clearly also scalar linearly solvable over the fields  $\text{GF}(8)$  and  $\text{GF}(4)$ . So while  $\text{GF}(8) \times \text{GF}(4)$  is the only commutative ring of size 32 that the network is scalar linearly solvable over, it is not the smallest commutative ring the network is scalar linearly solvable over. This fact agrees with Theorem 2.2.10.

### 2.3.2 Non-Power-of-Prime Size Rings

Theorem 2.2.10 demonstrated that scalar linear solutions over commutative rings induce scalar linear solutions over finite fields. For a network that is scalar linearly solvable over a given commutative ring it is natural to ask over which fields is the network also scalar linearly solvable. In this section, we partially answer this question.

**Theorem 2.3.9.** *Suppose a network is scalar linearly solvable over some commutative ring whose size is divisible by the prime  $p$ . Then the network is scalar linearly solvable over some finite field of characteristic  $p$  whose size divides the size of the ring.*

*Proof.* Let the commutative ring be  $R$ . By Lemma 2.3.5, there exist commutative local rings  $R_1, \dots, R_n$  such that  $R \cong R_1 \times \dots \times R_n$ . So we have  $|R| = |R_1| \cdots |R_n|$  and since  $p$  divides  $|R|$ , there exists  $j \in \{1, \dots, n\}$  such that  $p$  divides  $|R_j|$ . By Lemma 2.3.6 (i), this implies  $|R_j| = p^m$  for some positive integer  $m$ . Therefore, by Lemma 2.3.7,  $R_j \preceq \text{GF}(p^m)$ . Since  $\mathcal{N}$  is scalar linearly solvable over  $R$ , by Lemma 2.2.12,  $\mathcal{N}$  must be scalar linearly solvable over  $R_j$ , and since  $R_j \preceq \text{GF}(p^m)$ ,  $\mathcal{N}$  must also be scalar linearly solvable over  $\text{GF}(p^m)$ . ■

Theorem 2.3.9 demonstrates that commutative rings of non-power-of-prime size are always dominated by some fields whose characteristics are the prime factors of the ring's size. Determining which fields dominate a particular ring appears to be a non-trivial problem, since it depends on the local decomposition of the ring. We address a select few cases.

The following result is a standard result of algebra and shows that for each square-free integer  $m$ , any ring (with identity) of size  $m$  must be isomorphic to a direct product of prime fields. As an example, the ring  $\mathbb{Z}_6$  is isomorphic to  $\text{GF}(3) \times \text{GF}(2)$ .

**Lemma 2.3.10.** [2, p. 457]: *Let  $p_1, \dots, p_n$  be distinct primes. The commutative ring  $\text{GF}(p_1) \times \dots \times \text{GF}(p_n)$  is the only ring of size  $p_1 \cdots p_n$ .*

The following corollary shows that if a network is scalar linearly solvable over a ring whose size is square-free, then it must also be scalar linearly solvable over the prime fields corresponding to its prime factors.

**Corollary 2.3.11.** *Let  $p_1, \dots, p_n$  be distinct primes. If a network is scalar linearly solvable over a ring of size  $p_1 \cdots p_n$ , then the network is scalar linearly solvable over each of the fields  $\text{GF}(p_1), \dots, \text{GF}(p_n)$ .*

*Proof.* By Lemma 2.3.10, the only ring of size  $p_1 \cdots p_n$  is  $\text{GF}(p_1) \times \dots \times \text{GF}(p_n)$ . By Lemma 2.2.12, any network that is scalar linearly solvable over this ring must also have a scalar linear solution over each of  $\text{GF}(p_1), \dots, \text{GF}(p_n)$ . ■

In general, one cannot specify in Theorem 2.3.9 which fields of characteristic  $p$  a particular network is scalar linearly solvable over without knowing the particular ring  $R$ . As an example, the following corollary illustrates that different networks that are scalar linearly solvable over different rings of size 12, may be scalar linearly solvable over different finite fields. Additionally, Corollary 2.3.12 demonstrates that Corollary 2.3.11 does not always hold when  $p_1, \dots, p_n$  are non-distinct primes.

**Corollary 2.3.12.** (i) *If a network is scalar linearly solvable over  $\text{GF}(4) \times \text{GF}(3)$ , then the network is scalar linearly solvable over  $\text{GF}(4)$  and  $\text{GF}(3)$  but not necessarily over  $\text{GF}(2)$ .* (ii) *If a network is scalar linearly solvable over  $\mathbb{Z}_{12}$ , then the network is scalar linearly solvable over  $\text{GF}(2)$  and  $\text{GF}(3)$ .*

*Proof.* Part (i) follows from Lemma 2.2.12 and the fact that the Two-Six Network is scalar linearly solvable over  $\text{GF}(4)$  and  $\text{GF}(3)$  but not over  $\text{GF}(2)$  (see Corollary 2.2.18). Part (ii) follows from Corollary 2.2.7. ■

## 2.4 Integer Partitions

This section focuses on using integer partitions to describe a particular class of commutative rings that are direct products of finite fields. These rings will then be used in Section 2.5 to characterize commutative rings that are maximal.

For any positive integer  $k$ , a *partition of  $k$  of length  $r$*  is a non-decreasing sequence of positive integers  $(a_1, \dots, a_r)$  whose sum is equal to  $k$ . The length  $r$  of a partition  $A$  is sometimes denoted  $|A|$ . Let  $\Pi(k)$  denote the set of all partitions of  $k$ .

**Definition 2.4.1.** For each prime  $p$ , and each partition  $A = (a_1, \dots, a_r)$  of  $k$ , define the direct product ring

$$R_{A,p} = \text{GF}(p^{a_1}) \times \cdots \times \text{GF}(p^{a_r}).$$

Let  $m \geq 2$  have prime factorization  $m = p_1^{k_1} \cdots p_t^{k_t}$ , and let  $R$  be a ring of size  $m$ . We call  $R$  a *partition ring* if for each  $i = 1, \dots, t$ , there exists  $A_i \in \Pi(k_i)$  such that

$$R \cong R_{A_1,p_1} \times \cdots \times R_{A_t,p_t}.$$

We will refer to  $A_1, \dots, A_t$  as the *partitions of  $R$* .

As an example, if  $m = 864 = 2^5 3^3$ , then  $R = \text{GF}(2^2) \times \text{GF}(2^2) \times \text{GF}(2^1) \times \text{GF}(3^2) \times \text{GF}(3^1)$  is a partition ring and the partitions of  $R$  are  $A_1 = (2, 2, 1)$  and  $A_2 = (2, 1)$ . Another partition ring of size 864 is  $R = \text{GF}(2^4) \times \text{GF}(2^1) \times \text{GF}(3^3)$  and the partitions of  $R$  are  $A_1 = (4, 1)$  and  $A_2 = (3)$ . As another special case, any field  $\text{GF}(p^k)$  is a partition ring whose partition is  $(k)$ . In later proofs, we will encounter direct products of fields not given in terms of partitions; however, Lemma 2.4.2 demonstrates that each such direct product is, in fact, a partition ring.

**Lemma 2.4.2.** *Every finite direct product of finite fields is a partition ring.*

*Proof.* Suppose  $q_1, \dots, q_s$  are (not necessarily distinct) prime numbers and  $n_1, \dots, n_s$  are positive integers and define the product ring  $R = \text{GF}(q_1^{n_1}) \times \cdots \times \text{GF}(q_s^{n_s})$ . Let  $p_1^{k_1} \cdots p_t^{k_t}$  denote the prime factorization of the ring size  $|R|$ , so that  $p_1^{k_1} \cdots p_t^{k_t} = q_1^{n_1} \cdots q_s^{n_s}$ . For each  $j \in \{1, \dots, s\}$ , we have  $q_j = p_i$  for some unique  $i \in \{1, \dots, t\}$ . Thus, for each  $i = 1, \dots, t$ , there exist positive integers  $r_i$  and  $a_{i,1} \geq \cdots \geq a_{i,r_i}$  such that  $a_{i,1} + \cdots + a_{i,r_i} = k_i$  and  $\text{GF}(q_1^{n_1}) \times \cdots \times \text{GF}(q_s^{n_s}) \cong \prod_{i=1}^t \prod_{j=1}^{r_i} \text{GF}(p_i^{a_{i,j}})$ . Let  $A_i = (a_{i,1}, \dots, a_{i,r_i})$ . Then for each  $i$ ,  $A_i$  is a partition of  $k_i$ , and  $R$  is isomorphic to the partition ring with partitions  $A_1, \dots, A_t$ . ■



### 2.4.1 Partition Division

**Definition 2.4.3.** Let  $A$  and  $B$  be partitions of  $k$ . We say that  $A$  *divides*  $B$  and write  $A \mid B$  if for each element  $b$  of  $B$ , there exists an element  $a$  of  $A$  such that  $a \mid b$ . We call the relation “ $\mid$ ” *partition division*.

For each positive integer  $k$ , it can be verified that the partition division relation is a quasi-order on the set  $\Pi(k)$ . Throughout this chapter, whenever we refer to a partition of an integer as being *maximal*, we mean the partition is maximal with respect to the relation  $\mid$  on the set of all partitions of the same integer. In particular, a partition  $B$  of  $k$  is maximal if and only if  $A \mid B$  whenever  $B \mid A$ , for all partitions  $A$  of  $k$ . Sometimes distinct partitions of the same integer each divide the other. For example, for each  $k \geq 3$ , the partitions  $(k-1, 1)$  and  $(k-2, 1, 1)$  of  $k$  divide one another. Hence partition division is not anti-symmetric on  $\Pi(k)$ .

Lemma 2.4.4 demonstrates the connection between partition division and dominance of partition rings. Lemma 2.4.4 is a special case of Lemma 2.3.2, where the direct products of finite fields are based on partition rings.

**Lemma 2.4.4.** Let  $m \geq 2$  have prime factorization  $m = p_1^{k_1} \cdots p_t^{k_t}$ , and for each  $i = 1, \dots, t$ , let  $A_i$  and  $B_i$  be partitions of  $k_i$ . Then  $\mathbf{R}_{A_1, p_1} \times \cdots \times \mathbf{R}_{A_t, p_t}$  is dominated by the ring  $\mathbf{R}_{B_1, p_1} \times \cdots \times \mathbf{R}_{B_t, p_t}$  if and only if  $A_i$  divides  $B_i$  for all  $i$ .

*Proof.* For each  $i \in \{1, \dots, t\}$ , let  $A_i = (a_{i,1}, \dots, a_{i,r_i})$  and  $B_i = (b_{i,1}, \dots, b_{i,s_i})$ . Then

$$\mathbf{R}_{A_1, p_1} \times \cdots \times \mathbf{R}_{A_t, p_t} \cong \prod_{i=1}^t \prod_{j=1}^{r_i} \text{GF}(p_i^{a_{i,j}}) \quad \text{and} \quad \mathbf{R}_{B_1, p_1} \times \cdots \times \mathbf{R}_{B_t, p_t} \cong \prod_{i=1}^t \prod_{j=1}^{s_i} \text{GF}(p_i^{b_{i,j}}).$$

By Lemma 2.3.2,

$$\prod_{i=1}^t \prod_{j=1}^{s_i} \text{GF}(p_i^{a_{i,j}}) \preceq \prod_{i=1}^t \prod_{j=1}^{r_i} \text{GF}(p_i^{b_{i,j}})$$

if and only if for each  $i \in \{1, \dots, t\}$  and each  $j \in \{1, \dots, r_i\}$ , there exists  $l \in \{1, \dots, s_i\}$  such that  $a_{i,l} \mid b_{i,j}$ .

However, the latter condition is precisely  $A_i \mid B_i$  for all  $i$ . ■

### 2.4.2 Characterizing Maximal Partitions

The following lemma shows that if a partition divides a partition that is not shorter than it, then it also divides a partition which is shorter. This property will be used to characterize maximal partitions in Theorems 2.4.6 and 2.4.9.

**Lemma 2.4.5.** *Let A and B be different partitions of k. If  $|A| \leq |B|$  and  $A \mid B$ , then there exists a partition C of k such that  $|C| < |A|$  and  $A \mid C$ .*

*Proof.* The proof uses induction on  $|B| - |A|$ . In this proof, when we refer to elements of an integer partition as being “distinct” we mean that the elements are in different positions in the partition but possibly equal in value, i.e. if  $i \neq j$ , then  $a_i$  and  $a_j$  are distinct elements of A, even when  $a_i = a_j$ .

- **Base case:**  $|B| - |A| = 0$ .

If no element of A divides multiple elements of B, then, since  $|A| = |B|$ , each element of A must divide exactly one element of B. Then there exists a permutation  $\sigma$  of  $\{1, \dots, |A|\}$  such that  $a_i$  divides  $b_{\sigma(i)}$ .

Then

$$\begin{aligned} \sum_{i=1}^{|A|} b_{\sigma(i)} &= \sum_{i=1}^{|A|} b_i && \text{[from } \sigma \text{ is a permutation]} \\ &= \sum_{i=1}^{|B|} b_i && \text{[from } |A| = |B|] \\ &= \sum_{i=1}^{|A|} a_i && \text{[from } A, B \in \Pi(k)] \end{aligned}$$

which implies  $a_i = b_{\sigma(i)}$  for all  $i$ . However, this contradicts the assumption that  $A \neq B$ .

So we may assume there exists an element  $a$  of A that divides some distinct elements  $b_i, b_j$  of B. Let C be the partition B with elements  $b_i$  and  $b_j$  removed and replaced by  $(b_i + b_j)$ . Then C is a partition of  $k$  that is shorter than A, and since  $a$  divides  $(b_i + b_j)$ , we have  $A \mid C$ .

- **Induction step:** Assume true whenever  $|B| - |A| < n$  (where  $n \geq 1$ ).

Suppose  $|B| - |A| = n$ .

- ▶ **Case:  $n = 1$**

Since  $|B| > |A|$  and  $A \mid B$ , there exists an element  $a$  of A that divides some distinct elements  $b_i, b_j$  of B. If there is a third distinct element  $b_l$  of B such that  $a \mid b_l$ , then let C be the partition B with elements  $b_i, b_j$ , and  $b_l$  removed and replaced by  $(b_i + b_j + b_l)$ . Then C is a partition of  $k$  that is shorter than A, and since  $a$  divides  $(b_i + b_j + b_l)$ , we have  $A \mid C$ .

If there is no such third distinct element  $b_l$ , then modify B by removing the elements  $b_i$  and  $b_j$  and adding an element  $(b_i + b_j)$ . The new B is a partition of  $k$  that is the same length as A, and since  $a$  divides  $(b_i + b_j)$ , we have  $A \mid B$ . Since  $a$  divides both  $b_i$  and  $b_j$ , we have  $a \neq b_i + b_j$ , and since  $(b_i + b_j)$  is the only element of B that  $a$  divides, the value  $a$  is not one of the elements of B. Hence  $B \neq A$ , which reduces to the base case  $n = 0$ .

► Case:  $n \geq 2$

Since  $|B| > |A|$  and  $A \mid B$ , there exists an element  $a$  of  $A$  that divides some distinct elements  $b_i, b_j$  of  $B$ . Modify the partition  $B$  by removing the elements  $b_i$  and  $b_j$  and adding the element  $(b_i + b_j)$ . The new  $B$  is a partition of  $k$  that is one shorter than before the modification, and since  $a$  divides  $(b_i + b_j)$ , we have  $A \mid B$ . This reduces to the case  $|B| - |A| = n - 1$ , which is true by the induction hypothesis. ■

**Theorem 2.4.6.** *No maximal partition of  $k$  can divide any other partition of  $k$ .*

*Proof.* Any partition  $A$  is maximal if and only if the equivalence class  $[A]$  is maximal (with respect to the induced partial order under partition division), so it suffices to show that if  $[A]$  is maximal, then  $[A] = \{A\}$ .

Let  $A$  be a maximal partition of  $k$  such that  $A$  is of minimal length among the partitions in  $[A]$ , and suppose  $B \in [A] - \{A\}$ . Then  $|A| \leq |B|$  and  $A \mid B$ , so by Lemma 2.4.5, there exists  $C \in \Pi(k)$  such that  $|C| < |A|$  and  $A \mid C$ . Since  $[A]$  is maximal, we must have  $C \mid A$ , which implies  $C \in [A]$ , but this violates the minimum length of  $A$  in  $[A]$ . Thus,  $[A] = \{A\}$ . ■

In theory, the maximal elements in a quasi-order could be equivalent to another maximal element, i.e. the corresponding equivalence class contains more than one element. However, Theorem 2.4.6 implies the maximal partitions of  $k$  are precisely the partitions of  $k$  that do not divide any other partition of  $k$ , i.e. each maximal partition is in a distinct equivalence class. This is a stronger maximality condition than the maximality induced by the quasi-order.

Lemma 2.4.7 demonstrates a property of maximal partitions that will be used in a later proof.

**Lemma 2.4.7.** *No element of a maximal partition of  $k$  is divisible by a different element of the partition.*

*Proof.* Let  $A = (a_1, \dots, a_r)$  be a partition of  $k$ . Assume there exist distinct  $i, j \in \{1, \dots, r\}$  such that  $a_i$  divides  $a_j$ . Then  $a_i$  divides  $(a_i + a_j)$ . Create a new partition  $B$  of  $k$  by removing the elements  $a_i$  and  $a_j$  of  $A$  and inserting a new element  $(a_i + a_j)$ . Then  $B \neq A$  and  $A \mid B$ , so by Theorem 2.4.6,  $A$  is not maximal. ■

The converse of Lemma 2.4.7 does not necessarily hold. For example, the partition  $(5, 3, 2)$  satisfies the latter condition of Lemma 2.4.7, but  $(5, 3, 2) \mid (10)$ , so  $(5, 3, 2)$  is not maximal.

### 2.4.3 Maximal Partitions of Short Length

The following results provide a partial characterization of the maximal partitions with respect to partition division.

**Remark 2.4.8.** For each  $k \geq 1$ , the partition  $(k)$  is maximal, since  $k$  does not divide any positive integer less than  $k$ .

Theorem 2.4.9 gives a complete characterization of the maximal partitions of length 2.

**Theorem 2.4.9.** Let  $k$  and  $m$  be positive integers such that  $m \leq k/2$ . The partition  $(k - m, m)$  of  $k$  is maximal if and only if  $m \nmid k$ .

*Proof.* Assume  $m \mid k$ . Then  $(k - m, m) \mid (k)$ , so by Theorem 2.4.6,  $(k - m, m)$  is not a maximal partition.

Now assume  $m \nmid k$ . Then  $k \neq 2m$ , so  $m < k/2$ , or equivalently  $k - m > k/2$ . Thus,  $(k - m) \nmid k$ , which means that  $(k - m, m)$  does not divide  $(k)$ . But  $(k)$  is the only partition of  $k$  shorter than the partition  $(k - m, m)$ , so by Lemma 2.4.5, the partition  $(k - m, m)$  cannot divide any other partition of  $k$  that is at least as long as  $(k - m, m)$ . Thus  $(k - m, m)$  is maximal. ■

We can have maximal partitions of length 3 or greater, such as  $(7, 6, 4)$ , although we do not know of a nice characterization of such partitions. In Table 2.6, we provide a computer generated list of all maximal partitions of  $k$ , for each  $k \leq 30$ .

**Theorem 2.4.10.** Let  $k$  be a positive integer. Then  $(k)$  is the unique maximal partition of  $k$  if and only if  $k \in \{1, 2, 3, 4, 6\}$ .

*Proof.* For each positive integer  $k$ , by Remark 2.4.8,  $(k)$  is a maximal partition. It is easily verified that the

following are all the partitions of  $k$ , for  $k \in \{1, 2, 3, 4, 6\}$ :

$$\begin{aligned}\Pi(1) &= \{(1)\} \\ \Pi(2) &= \{(2), (1, 1)\} \\ \Pi(3) &= \{(3), (2, 1), (1, 1, 1)\} \\ \Pi(4) &= \{(4), (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)\} \\ \Pi(6) &= \{(6), (5, 1), (4, 2), (4, 1, 1), (3, 3), \\ &\quad (3, 2, 1), (3, 1, 1, 1), (2, 2, 2), \\ &\quad (2, 2, 1, 1), (2, 1, 1, 1, 1), (1, 1, 1, 1, 1, 1)\}.\end{aligned}$$

For each  $k \in \{1, 2, 3, 4, 6\}$ , every partition of  $k$  has an element that divides  $k$ , so  $(k)$  is the only maximal partition for such  $k$ .

For each odd  $k \geq 5$ , we have

$$\gcd\left(\frac{k-1}{2}, k\right) = \gcd\left(\frac{k-1}{2}, k - 2\left(\frac{k-1}{2}\right)\right) = \gcd\left(\frac{k-1}{2}, 1\right) = 1 < \frac{k-1}{2}$$

so  $\frac{k-1}{2} \nmid k$ . Therefore  $(\frac{k+1}{2}, \frac{k-1}{2})$  is a maximal partition, by taking  $m = \frac{k-1}{2}$  in Theorem 2.4.9.

For each even  $k \geq 8$ , we have

$$\gcd\left(\frac{k}{2} - 1, k\right) = \gcd\left(\frac{k}{2} - 1, k - 2\left(\frac{k}{2} - 1\right)\right) = \gcd\left(\frac{k}{2} - 1, 2\right) \leq 2 < \frac{k}{2} - 1$$

so  $(\frac{k}{2} - 1) \nmid k$ . Therefore  $(\frac{k}{2} + 1, \frac{k}{2} - 1)$  is a maximal partition, by taking  $m = \frac{k}{2} - 1$  in Theorem 2.4.9.

Thus if  $k = 5$  or if  $k \geq 7$ , then there exist at least two maximal partitions of  $k$ . ■

## 2.5 Maximal Commutative Rings

In this section, we characterize the commutative rings which are maximal with respect to the quasi-order of commutative rings of a given size under dominance. In order to do, we make use of the results on partition division from Section 2.4.

**Corollary 2.5.1.** *If each of a partition ring's integer partitions is maximal, then the ring is not dominated by any other partition ring of the same size.*

*Proof.* Let  $m = p_1^{k_1} \cdots p_t^{k_t}$  be the prime factorization of  $m$ . For each  $i = 1, \dots, t$ , let  $A_i, B_i \in \Pi(k_i)$  be such that  $A_i$  is maximal. Suppose  $R_{A_1, p_1} \times \cdots \times R_{A_t, p_t} \preceq R_{B_1, p_1} \times \cdots \times R_{B_t, p_t}$ . Then by Lemma 2.4.4,  $A_i \mid B_i$  for all  $i$ . Since each  $A_i$  is maximal, by Theorem 2.4.6,  $B_i = A_i$ , for all  $i$ . Therefore the partition ring  $R_{A_1, p_1} \times \cdots \times R_{A_t, p_t}$  is isomorphic to the partition ring  $R_{B_1, p_1} \times \cdots \times R_{B_t, p_t}$ . ■

Lemma 2.5.2 extends Corollary 2.5.1 to show that partition rings, where each partition is maximal, are not dominated by any other (not necessarily partition) commutative ring of the same size.

**Lemma 2.5.2.** *If each of a partition ring's integer partitions is maximal, then the ring is not dominated by any other commutative ring of the same size.*

*Proof.* Let  $m = p_1^{k_1} \cdots p_t^{k_t}$  be the prime factorization of the size of the ring  $R = R_{A_1, p_1} \times \cdots \times R_{A_t, p_t}$ , where for each  $i = 1, \dots, t$ , the partition  $A_i = (a_{i,1}, \dots, a_{i,r_i})$  of  $k_i$  is maximal. Suppose  $R$  is dominated by a commutative ring  $S$  of size  $m$ . We will show that  $R$  and  $S$  are isomorphic rings.

By Lemma 2.3.5, the ring  $S$  can be written as a direct product of commutative local rings, and by Lemma 2.3.6 (i), the size of each such local ring has to be a power of one of the prime factors  $p_1, \dots, p_t$  of  $m$ . Specifically, for each  $i = 1, \dots, t$ , there exist local rings  $L_{i,1}, \dots, L_{i,s_i}$  such that each  $|L_{i,j}|$  is a power of  $p_i$  and

$$S \cong \prod_{i=1}^t \prod_{j=1}^{s_i} L_{i,j}. \quad (2.6)$$

For each  $i = 1, \dots, t$  and  $j = 1, \dots, s_i$ , Lemma 2.3.7 implies that  $L_{i,j} \preceq \text{GF}(|L_{i,j}|)$ . Then,

$$\begin{aligned} R_{A_1, p_1} \times \cdots \times R_{A_t, p_t} &\preceq \prod_{i=1}^t \prod_{j=1}^{s_i} L_{i,j} && \text{[from } R \preceq S, (2.6)\text{]} \\ &\preceq \prod_{i=1}^t \prod_{j=1}^{s_i} \text{GF}(|L_{i,j}|) && \text{[from Lemma 2.2.13]} \end{aligned} \quad (2.7)$$

and the right-hand-side of (2.7) is a partition ring of size  $m$ , by Lemma 2.4.2. Since each  $A_i$  is maximal, by Corollary 2.5.1 and (2.7), we have

$$\begin{aligned} \prod_{i=1}^t \prod_{j=1}^{s_i} \text{GF}(|L_{i,j}|) &\cong R_{A_1, p_1} \times \cdots \times R_{A_t, p_t} \\ &\cong \prod_{i=1}^t \prod_{j=1}^{r_i} \text{GF}(p_i^{a_{i,j}}). \end{aligned} \quad (2.8)$$

Therefore for each  $i = 1, \dots, t$ , we have  $s_i = r_i$ , and by (2.8), without loss of generality, we may assume  $|L_{i,j}| = p_i^{a_{i,j}}$ , for all  $j = 1, \dots, r_i$ .

For each  $i = 1, \dots, t$  and  $j = 1, \dots, r_i$ , let  $I_{i,j}$  be the maximal ideal of the local ring  $L_{i,j}$ . Then, by Lemma 2.3.6 (ii), for each  $i$  and  $j$ , there exists a positive integer  $b_{i,j}$  such that  $b_{i,j} \mid a_{i,j}$  and  $\text{GF}(p_i^{b_{i,j}})$  is isomorphic to  $L_{i,j}/I_{i,j}$ . Corollary 2.2.9 then implies

$$L_{i,j} \preceq \text{GF}(p_i^{b_{i,j}}) \quad (i = 1, \dots, t \text{ and } j = 1, \dots, r_i) \quad (2.9)$$

and therefore

$$\begin{aligned}
R &\cong \prod_{i=1}^t \prod_{j=1}^{r_i} \text{GF}(p_i^{a_{i,j}}) \\
&\preceq \prod_{i=1}^t \prod_{j=1}^{r_i} L_{i,j} && \text{[from } R \preceq S, (2.6)\text{]} \\
&\preceq \prod_{i=1}^t \prod_{j=1}^{r_i} \text{GF}(p_i^{b_{i,j}}) && \text{[from (2.9), Lemma 2.2.13].} \tag{2.10}
\end{aligned}$$

Lemma 2.3.2 and (2.10) imply that for each  $i \in \{1, \dots, t\}$  and  $j \in \{1, \dots, r_i\}$ , there exists  $l \in \{1, \dots, r_i\}$  such that  $a_{i,l} \mid b_{i,j}$ . We also have  $b_{i,j} \mid a_{i,j}$ , so  $a_{i,l} \mid a_{i,j}$ . Since  $A_i$  is maximal, by Lemma 2.4.7, this implies  $l = j$ . Thus  $b_{i,j} = a_{i,j}$ , for all  $i \in \{1, \dots, t\}$  and  $j \in \{1, \dots, r_i\}$ , and therefore  $L_{i,j}/I_{i,j} \cong \text{GF}(p_i^{a_{i,j}})$  for all  $i, j$ . However, we also have  $|L_{i,j}| = p_i^{a_{i,j}}$  for all  $i, j$ . So it must be the case that  $|I_{i,j}| = 1$ , and

$$L_{i,j} \cong \text{GF}(p_i^{a_{i,j}}) \quad (i = 1, \dots, t \text{ and } j = 1, \dots, r_i). \tag{2.11}$$

Thus,

$$\begin{aligned}
S &\cong \prod_{i=1}^t \prod_{j=1}^{r_i} \text{GF}(p_i^{a_{i,j}}) && \text{[from (2.6), (2.11)]} \\
&\cong \mathbf{R}_{A_1, p_1} \times \cdots \times \mathbf{R}_{A_t, p_t} \cong R.
\end{aligned}$$

■

Lemmas 2.5.2 and 2.5.3 will be used in the proof of Theorem 2.5.4 to show that the maximal commutative rings with respect to dominance are precisely partition rings where each partition is maximal.

**Lemma 2.5.3.** *Every finite commutative ring is dominated by some partition ring of the same size, all of whose partitions are maximal.*

*Proof.* Let  $R$  be a finite commutative ring. By Lemma 2.3.5, there exist commutative local rings  $R_1, \dots, R_n$  such that  $R \cong R_1 \times \cdots \times R_n$ . By Lemma 2.3.7, for each  $j = 1, \dots, n$ , we have  $R_j \preceq \text{GF}(|R_j|)$  so by Lemma 2.2.13, we have

$$R_1 \times \cdots \times R_n \preceq \text{GF}(|R_1|) \times \cdots \times \text{GF}(|R_n|). \tag{2.12}$$

Let  $m = p_1^{k_1} \cdots p_t^{k_t}$  denote the prime factorization of  $m$ . Then by Lemma 2.4.2, for each  $i = 1, \dots, t$ , there exists a partition  $B_i$  of  $k_i$  such that

$$\mathbf{R}_{B_1, p_1} \times \cdots \times \mathbf{R}_{B_t, p_t} \cong \text{GF}(|R_1|) \times \cdots \times \text{GF}(|R_n|). \tag{2.13}$$

Since  $\Pi(k_i)$  is a finite quasi-ordered set under partition division, for each  $i = 1, \dots, t$ , there exists maximal  $A_i \in \Pi(k_i)$  such that  $B_i \mid A_i$ . So we have

$$\begin{aligned} R &\preceq \mathbf{R}_{B_1, p_1} \times \cdots \times \mathbf{R}_{B_t, p_t} && \text{[from (2.12), (2.13)]} \\ &\preceq \mathbf{R}_{A_1, p_1} \times \cdots \times \mathbf{R}_{A_t, p_t} && \text{[from Lemma 2.4.4].} \end{aligned}$$

■

The following theorem characterizes maximal commutative rings.

**Theorem 2.5.4.** *A finite commutative ring is maximal if and only if it is a partition ring, each of whose integer partitions is maximal.*

*Proof.* If  $R$  is a partition ring such that each of its partitions is maximal, then by Lemma 2.5.2, no other commutative ring of the same size dominates  $R$ . Thus,  $R$  is maximal.

Conversely, assume commutative ring  $R$  is maximal. By Lemma 2.5.3,  $R$  is dominated by a partition ring  $S$  of the same size where each of its partitions is maximal. Since  $R$  is maximal, this implies  $S \preceq R$ . However, by Lemma 2.5.2, this implies  $S \cong R$ . Thus,  $R$  is a partition ring such that each of its partitions is maximal.

■

**Remark 2.5.5.** *Since the maximal rings of a given size are partition rings where each integer partition is maximal, the maximal rings of non-power-of-prime size are direct products of maximal rings of prime-power sizes.*

**Corollary 2.5.6.** *Let  $m \geq 2$  have prime factorization  $m = p_1^{k_1} \cdots p_t^{k_t}$ . Then  $\text{GF}(p_1^{k_1}) \times \cdots \times \text{GF}(p_t^{k_t})$  is a maximal ring of size  $m$ .*

*Proof.* This follows from Theorem 2.5.4 and Remark 2.4.8.

■

It was shown in Theorem 2.2.19 and Corollary 2.3.3 that non-isomorphic rings can be equivalent under dominance; however, Corollary 2.5.7 demonstrates that such equivalent rings cannot be maximal.



**Corollary 2.5.7.** *No maximal commutative ring is dominated by any other commutative ring of the same size.*

*Proof.* This follows immediately from Theorem 2.5.4 and Lemma 2.5.2 ■

We note that this is a stronger maximality than the maximality induced by the quasi-order, since in a quasi-order, maximal elements can be equivalent to other maximal elements.

Theorem 2.2.16 demonstrated that for each finite field, there exists a multicast network that is scalar linearly solvable over the field but not over any other commutative ring of the same size, and Theorem 2.3.8 demonstrated a network that is scalar linearly solvable over  $\text{GF}(8) \times \text{GF}(4)$  but not over any other commutative ring of size 32. The following theorem shows a similar property for every maximal commutative ring and provides an alternate characterization of maximal commutative rings than in Theorem 2.5.4.

**Theorem 2.5.8.** *A finite commutative ring is maximal if and only if there exists a network that is scalar linearly solvable over the ring but not over any other commutative ring of the same size.*

*Proof.* Let  $R$  be a maximal commutative ring of size  $m$ . By Corollary 2.5.7,  $R$  is not dominated by any other commutative ring of size  $m$ , so for each ring  $S$  of size  $m$  that is not isomorphic to  $R$ , there exists a network  $\mathcal{N}_S$  that is scalar linearly solvable over  $R$  but not  $S$ . Then the disjoint union of networks

$$\bigcup_{\substack{S \in \mathcal{R}(m) \\ S \neq R}} \mathcal{N}_S$$

is scalar linearly solvable over  $R$ , since each  $\mathcal{N}_S$  is scalar linearly solvable over  $R$ . However, for each  $S \in \mathcal{R}(m)$ , if  $S$  is not isomorphic to  $R$ , then  $\mathcal{N}_S$  is not scalar linearly solvable over  $S$ , so the disjoint union network is not scalar linearly solvable over  $S$ .

Conversely, if  $R$  is a finite commutative ring that is not maximal, then it is dominated by some other commutative ring  $S$  of the same size, so any network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $S$ . ■

An interesting open problem related to Theorem 2.5.8 is to characterize rings with the property that there exists a multicast network that is scalar linearly solvable over the ring but not over any other commutative ring of the same size. We showed (in Theorem 2.2.16) that such a multicast network exists

for every finite field, and we showed (in Example 2.2.11) that there exists a multicast network that is scalar linearly solvable over a ring of size  $2^{13}$  but not the field  $\text{GF}(2^{13})$ .

### 2.5.1 Multiple Maximal Rings of a Given Size

Theorem 2.5.9 demonstrates that in some cases, there is only one maximal commutative ring of a given size. If  $R$  is the only maximal ring of a given size, then by Lemma 2.5.3, any network with a scalar linear solution over some commutative ring of size  $|R|$  also has a scalar linear solution over  $R$ . Alternatively, since the set of commutative rings of size  $|R|$  is finite and quasi-ordered under dominance, each ring  $S \in \mathcal{R}(|R|)$  is dominated by some maximal ring, and if  $R$  is the only maximal ring of size  $|R|$ , then  $S$  is dominated by  $R$ . In this case,  $R$  can be thought of as the “best” commutative ring of size  $|R|$ , in terms of scalar linear solvability.

However, by Theorem 2.5.8, for each maximal ring, there exists a network which is scalar linearly solvable over the maximal ring but not over any other commutative ring of the same size. When there are multiple maximal rings of a given size, not every network with a scalar linear solution over some commutative ring of this size is scalar linearly solvable over every maximal ring. Thus there is no “best” commutative ring of this size.

**Theorem 2.5.9.** *Let  $m \geq 2$  have prime factorization  $m = p_1^{k_1} \cdots p_t^{k_t}$ . Then  $\text{GF}(p_1^{k_1}) \times \cdots \times \text{GF}(p_t^{k_t})$  is the only maximal ring of size  $m$  if and only if  $\{k_1, \dots, k_t\} \subseteq \{1, 2, 3, 4, 6\}$ .*

*Proof.* By Corollary 2.5.6,  $\text{GF}(p_1^{k_1}) \times \cdots \times \text{GF}(p_t^{k_t})$  is a maximal ring. Assume  $k_i \in \{1, 2, 3, 4, 6\}$  for all  $i$ . Then by Theorem 2.4.10,  $(k_i)$  is the only maximal partition of  $k_i$  for all  $i$ . Thus, by Theorem 2.5.4,  $\text{GF}(p_1^{k_1}) \times \cdots \times \text{GF}(p_t^{k_t})$  is the only maximal ring of size  $m$ .

Conversely, assume there exists  $j$  such that  $k_j = 5$  or  $k_j \geq 7$ . Then by Theorem 2.4.10, there exists a maximal partition  $B_j$  of  $k_j$  such that  $B_j \neq (k_j)$ . Then by Theorem 2.5.4,

$$\mathbb{R}_{B_j, p_j} \times \prod_{\substack{i=1 \\ i \neq j}}^t \text{GF}(p_i^{k_i}) \quad \text{and} \quad \text{GF}(p_1^{k_1}) \times \cdots \times \text{GF}(p_t^{k_t})$$

are distinct maximal rings of size  $m$ . ■

The bound in the following corollary can be achieved with equality, as illustrated in Example 2.3.4.

**Corollary 2.5.10.** *If a network is not scalar linearly solvable over a given finite field but is scalar linearly solvable over some commutative ring of the same size, then the size of the field is at least 32.*

*Proof.* It follows from Theorem 2.5.9 that for each  $k \in \{1, 2, 3, 4, 6\}$  and prime  $p$ , any network that is scalar linearly solvable over some commutative ring of size  $p^k$  must also be scalar linearly solvable over the field  $\text{GF}(p^k)$ . The claim follows from the fact  $p = 2$  and  $k = 5$  yield the minimum  $p^k$  that does not satisfy this condition. ■

In the following example, we list the maximal rings of various sizes.

**Example 2.5.11.** For each integer  $k \geq 1$  and prime  $p$ ,  $\text{GF}(p^k)$  is a maximal ring. The following are the other maximal commutative rings of size  $p^k$  for all  $k \leq 12$ :

$$p^5 : \text{GF}(p^3) \times \text{GF}(p^2)$$

$$p^7 : \text{GF}(p^5) \times \text{GF}(p^2) \text{ and } \text{GF}(p^4) \times \text{GF}(p^3)$$

$$p^8 : \text{GF}(p^5) \times \text{GF}(p^3)$$

$$p^9 : \text{GF}(p^7) \times \text{GF}(p^2) \text{ and } \text{GF}(p^5) \times \text{GF}(p^4)$$

$$p^{10} : \text{GF}(p^7) \times \text{GF}(p^3) \text{ and } \text{GF}(p^6) \times \text{GF}(p^4)$$

$$p^{11} : \text{GF}(p^9) \times \text{GF}(p^2), \text{GF}(p^8) \times \text{GF}(p^3), \text{GF}(p^7) \times \text{GF}(p^4), \text{ and } \text{GF}(p^6) \times \text{GF}(p^5)$$

$$p^{12} : \text{GF}(p^7) \times \text{GF}(p^5).$$

$\text{GF}(8) \times \text{GF}(4)$  is the smallest prime-power size maximal commutative ring that is not a finite field, and  $\text{GF}(128) \times \text{GF}(64) \times \text{GF}(16)$  has size  $2^{17}$  and is the smallest known<sup>6</sup> prime-power size maximal commutative ring consisting of a direct product of more than two fields.

Maximal commutative rings of non-power-of-prime size are direct products of maximal commutative rings of prime-power size (see Remark 2.5.5) and can be found using the maximal partitions of the prime factor multiplicities. For example, consider maximal rings of size  $777600 = 2^7 3^5 5^2$ . The maximal partitions of 7 are (7), (5, 2), and (4, 3); the maximal partitions of 5 are (5) and (3, 2); and the only maximal partition of 2 is (2). Hence the 6 maximal commutative rings of size 777600 are

---

<sup>6</sup> If there were a prime-power size maximal commutative ring, consisting of a direct product of more than two fields, and whose size were less than  $2^{17}$ , then there would exist a length-3 maximal partition of an integer less than 17. The enumeration of maximal partitions given in Table 2.6 implies such a partition does not exist.

$$\begin{aligned}
& \text{GF}(2^7) \times \text{GF}(3^5) \times \text{GF}(5^2) \\
& \text{GF}(2^5) \times \text{GF}(2^2) \times \text{GF}(3^5) \times \text{GF}(5^2) \\
& \text{GF}(2^4) \times \text{GF}(2^3) \times \text{GF}(3^5) \times \text{GF}(5^2) \\
& \text{GF}(2^7) \times \text{GF}(3^3) \times \text{GF}(3^2) \times \text{GF}(5^2) \\
& \text{GF}(2^5) \times \text{GF}(2^2) \times \text{GF}(3^3) \times \text{GF}(3^2) \times \text{GF}(5^2) \\
& \text{GF}(2^4) \times \text{GF}(2^3) \times \text{GF}(3^3) \times \text{GF}(3^2) \times \text{GF}(5^2).
\end{aligned}$$

Table 2.6 provides a list of the maximal partitions of  $k$  for  $k = 1, 2, \dots, 30$ , which can be used to find maximal commutative rings of size  $m = p_1^{k_1} \cdots p_t^{k_t}$ , where  $k_1, \dots, k_t \leq 30$ .

## 2.6 Open Questions

Some potentially interesting open questions related to scalar linear codes over commutative rings and partition division include:

- We have demonstrated there exist non-multicast networks with scalar linear solutions over commutative rings of size  $p^k$  but not  $\text{GF}(p^k)$  whenever  $k = 5$  or  $k \geq 7$ . For which  $p$  and  $k$  do there exist multicast networks with this property?
- Are there cleaner characterizations of maximal rings of a given size?
- Are there cleaner characterizations of maximal partitions of length 3 or greater?
- What is the asymptotic behavior of the number of maximal partitions (rings, respectively) of a given integer (size, respectively)?
- Can the quasi-order of (not necessarily commutative) rings of a given size under dominance be cleanly characterized? In particular, what are the maximal rings of a given size when the commutative restriction is removed? Non-commutative rings lack some of useful properties of commutative rings, such as local decomposition.

|  |
|--|
| (1)  |
| (2)  |
| (3)  |
| (4)  |
| (5) (3,2)  |
| (6)  |
| (7) (5,2) (4,3)  |
| (8) (5,3)  |
| (9) (7,2) (5,4)  |
| (10) (7,3) (6,4)   |
| (11) (9,2) (8,3) (7,4) (6,5)   |
| (12) (7,5)   |
| (13) (11,2) (10,3) (9,4) (8,5) (7,6)   |
| (14) (11,3) (10,4) (9,5) (8,6)   |
| (15) (13,2) (11,4) (9,6) (8,7)   |
| (16) (13,3) (11,5) (10,6) (9,7)  |
| (17) (15,2) (14,3) (13,4) (12,5) (11,6) (10,7) (9,8) (7,6,4)   |
| (18) (14,4) (13,5) (11,7) (10,8)   |
| (19) (17,2) (16,3) (15,4) (14,5) (13,6) (12,7) (11,8) (10,9) (9,6,4) (8,6,5)   |
| (20) (17,3) (14,6) (13,7) (12,8) (11,9)  |
| (21) (19,2) (17,4) (16,5) (15,6) (13,8) (12,9) (11,10) (11,6,4)  |
| (22) (19,3) (18,4) (17,5) (16,6) (15,7) (14,8) (13,9) (12,10) (9,8,5) (9,7,6)  |
| (23) (21,2) (20,3) (19,4) (18,5) (17,6) (16,7) (15,8) (14,9) (13,10) (13,6,4)<br>(12,11) (11,7,5) (10,9,4) (10,7,6) (9,8,6)  |
| (24) (19,5) (17,7) (15,9) (14,10) (13,11)  |
| (25) (23,2) (22,3) (21,4) (19,6) (18,7) (17,8) (16,9) (15,10) (15,6,4) (14,11) (13,12)<br>(11,10,4) (11,8,6) (10,9,6) (10,8,7)   |
| (26) (23,3) (22,4) (21,5) (20,6) (19,7) (18,8) (17,9) (16,10) (15,11) (14,12) (12,9,5)<br>(11,9,6) (11,8,7) (10,9,7)   |
| (27) (25,2) (23,4) (22,5) (21,6) (20,7) (19,8) (17,10) (17,6,4) (16,11) (15,12)<br>(14,13) (14,8,5) (13,10,4) (13,8,6) (12,8,7) (11,10,6)  |
| (28) (25,3) (23,5) (22,6) (20,8) (19,9) (18,10) (17,11) (16,12) (15,13) (13,9,6)<br>(12,11,5) (11,9,8)   |
| (29) (27,2) (26,3) (25,4) (24,5) (23,6) (22,7) (21,8) (20,9) (19,10) (19,6,4)<br>(18,11) (17,12) (16,13) (16,7,6) (15,14) (15,10,4) (15,8,6) (14,11,4)<br>(14,9,6) (13,11,5) (13,10,6) (13,9,7) (12,10,7) (12,9,8) (11,10,8) |
| (30) (26,4) (23,7) (22,8) (21,9) (19,11) (18,12) (17,13) (16,14) (13,9,8) (12,11,7)  |

Figure 2.6: The maximal partitions of  $k = 1, 2, \dots, 30$  under partition division.

## References

- [1] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, “Network information flow,” *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.
- [2] V. G. Antipkin and V. P. Elizarov, “Rings of order  $p^3$ ,” *Siberian Mathematical Journal*, vol. 23, no. 4, pp. 457–464, 1982.
- [3] G. Bini and F. Flamini, *Finite Commutative Rings and Their Applications*, Kluwer Academic Publishers, 2002.
- [4] J. Connelly and K. Zeger, “A class of non-linearly solvable networks,” *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 201–229, January 2017.
- [5] J. Connelly and K. Zeger, “Linear network coding over rings – Part II: Vector codes and non-commutative alphabets,” *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 292 – 308, January 2018.
- [6] B. Corbas and G. D. Williams, “Rings of order  $p^5$  part I. Nonlocal rings,” *Journal of Algebra*, vol. 231, no. 2, pp. 677–690, 2000.
- [7] B. Corbas and G. D. Williams, “Rings of order  $p^5$  part II. Local rings,” *Journal of Algebra*, vol. 231, no. 2, pp. 691–704, 2000.
- [8] 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.
- [9] R. Dougherty, C. Freiling, and K. Zeger, “Linear network codes and systems of polynomial equations,” *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2303–2316, May 2008.
- [10] R. Dougherty, C. Freiling, and K. Zeger, “Linearity and solvability in multicast networks,” *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2243–2256, October 2004.
- [11] R. Dougherty, C. Freiling, and K. Zeger, “Networks, matroids, and non-Shannon information inequalities,” *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 1949–1969, June 2007.
- [12] D. Dummit and R. Foote, *Abstract Algebra*, Third Edition, Hoboken, NJ, John Wiley and Sons Inc., 2004.
- [13] J.B. Ebrahimi and C. Fragouli, “Algebraic algorithms for vector network coding,” *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 996–1007, February 2011.
- [14] M. Effros, S. El Rouayheb, and M. Langberg, “An equivalence between network coding and index coding,” *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2478–2487, May 2015.
- [15] K.E. Eldridge, “Orders for finite noncommutative rings with unity,” *The American Mathematical Monthly*, vol. 75, no. 5, pp. 512–514, May 1968.
- [16] T. Etzion and A. Wachter-Zeh, “Vector network coding based on subspace codes outperforms scalar linear network coding,” arXiv:1604.03292v2 [cs.IT], May 13, 2016
- [17] B. Fine, “Classification of Finite Rings of Order  $p^2$ ,” *Mathematics Magazine* vol. 66, no. 4, pp. 248–252, October 1993.
- [18] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, “A random linear network coding approach to multicast,” *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, October 2006.
- [19] S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, “Polynomial time algorithms for multicast network code construction,” *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1973–1982, June 2005.

- [20] P. Karimian, R. Rafie Borujeny, and M. Ardakani, “On network coding for funnel networks,” *IEEE Communications Letters*, vol. 19, no. 11, pp. 1897–1900, November 2015.
- [21] R. Koetter and M. Médard, “An algebraic approach to network coding,” *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, October 2003.
- [22] M. Langberg, A. Sprintson and J. Bruck, “The encoding complexity of network coding,” *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2386–2397, June 2006.
- [23] S.-Y.R. Li and R.W. Yeung, “On convolutional network coding,” *IEEE International Symposium on Information Theory (ISIT 2006)*, pp. 1743–1747, July 2006.
- [24] S.-Y.R. Li, and Q. Sun, “Network coding theory via commutative algebra,” *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 403–415, January 2011.
- [25] S.-Y.R. Li, Q. Sun, and S. Ziyu, “Linear network coding: theory and algorithms,” *Proceedings of the IEEE*, vol. 99, no. 3, pp. 372–387, March 2011.
- [26] S.-Y.R. Li, R.W. Yeung, and N. Cai, “Linear network coding,” *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, February 2003.
- [27] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker Inc., 1974.
- [28] M. Médard, M. Effros, T. Ho, and D. Karger, “On coding for non-multicast networks,” *Conference on Communication Control and Computing*, Monticello, IL, October 2003.
- [29] A. Rasala Lehman and E. Lehman, “Complexity classification of network information flow problems,” *ACM-SIAM Symposium on Discrete algorithms*, 2004.
- [30] S. Riis, “Linear versus nonlinear boolean functions in network flow,” *Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March 2004.
- [31] J. Roitman, *Introduction to Modern Set Theory*, Virginia Commonwealth University Mathematics, 2011.
- [32] Q. Sun, X. Yangy, K. Long, X. Yin, and Z. Li, “On vector linear solvability of multicast networks,” *IEEE Transactions on Communications* vol. 64, no. 12, pp. 5096–5107, December 2016.
- [33] Q. Sun, X. Yin, Z. Li, and K. Long, “Multicast network coding and field sizes,” *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6182–6191, November 2015.
- [34] Q. Sun, S.-Y.R. Li, and Z. Li, “On base field of linear network coding,” *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7272–7282, December 2016.
- [35] A. Tavory, M. Feder, and D. Ron, “Bounds on linear codes for network multicast,” *Electronic Colloquium on Computational Complexity (ECCC)*, no. 33, pp. 1–9, 2003.

---

This chapter is a reprint of the material as it appears in J. Connelly and K. Zeger, “Linear network coding over rings – Part I: Scalar codes and commutative alphabets,” *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 274 – 291, January 2018. The dissertation author was the primary investigator of this paper. © IEEE. Reprinted with permission.

# Chapter 3

## Vector Codes and Non-Commutative Rings

### Abstract

In the previous chapter, we studied scalar linear network coding over finite commutative rings and made comparisons to the well-studied case of linear network coding over finite fields. Here, we consider the more general setting of vector linear network coding over finite (possibly non-commutative) rings and modules. We prove the following results regarding the linear solvability of directed acyclic networks over various finite alphabets.

For any network, the following are equivalent: (i) vector linear solvability over some field, (ii) scalar linear solvability over some ring, (iii) linear solvability over some module. Analogously, the following are equivalent: (a) scalar linear solvability over some field, (b) scalar linear solvability over some commutative ring, (c) linear solvability over some module whose ring is commutative. Whenever any network is linearly solvable over a module, a smallest such module arises in a vector linear solution over a field.

If a network is scalar linearly solvable over some non-commutative ring but not over any commutative ring, then such a non-commutative ring must have size at least 16, and for some networks, this bound is achieved. An infinite family of networks is given, each of which is scalar linearly solvable over some non-commutative ring but not over any commutative ring.

Whenever  $p$  is prime and  $1 \leq k \leq 6$ , if a network is scalar linearly solvable over some ring of size  $p^k$ , then it is also  $k$ -dimensional vector linearly solvable over the field  $\text{GF}(p)$ , but the converse does not necessarily hold. This result is extended to all  $k \geq 1$  when the ring is commutative.



## 3.1 Introduction

In Chapter 2, we studied scalar linear network codes over finite commutative rings. Equivalently, these are linear codes over modules where a finite commutative ring acts on its own additive group via multiplication in the ring. In particular, we compared the scalar linear solvability of directed acyclic networks over different types of commutative rings of the same size. We proved that networks that are scalar linearly solvable over some commutative ring are also scalar linearly solvable over some field of the same or smaller size. Additionally, we characterized all commutative rings with the property that there exists a network with a scalar linear solution over the ring but not over any other commutative ring of the same size.

Linear network codes can be advantageous due to their ease of implementation and mathematical tractability. These properties are due to the algebraic simplicity of linear maps and also to the structured nature of the alphabets used. Fields have the most algebraic constraints among alphabets used for linear network coding, e.g. associativity, distributivity, commutativity, invertibility. More generally, rings may lack commutativity and/or invertibility, thus providing a broader class of alphabets over which to achieve linear network solvability. We demonstrated in Chapter 2 that relaxing only the invertibility constraint (i.e. restricting to commutative rings) can lead to linear network solvability that would not otherwise be possible with fields of the same alphabet size.

In the present chapter, we additionally relax the commutativity constraint, and we study linear coding over general ring alphabets and, even more generally, over modules. Vector and scalar linear codes over rings and fields are special cases of linear codes over modules. We focus on the relationship between alphabet commutativity and the scalar and vector linear solvability of networks, and we compare the linear solvability of networks over different modules where the alphabet size is the same.

### 3.1.1 Linear Codes Over Modules

A module is a generalization of a vector space, where the scalars are from a ring, as opposed to a field, and the set of vectors may be some other Abelian group. As an example, if  $R$  is any ring and  $k$  is a positive integer, then the set of  $k$ -vectors over  $R$  with component-wise addition forms an Abelian group, and the ring  $R$  acts on this group by scalar multiplication in a similar way to scalar multiplication in a vector space. In the special case where  $R$  is a field, this module is, in fact, a vector space.

**Definition 3.1.1.** An  $R$ -module (specifically a left  $R$ -module) is an Abelian group<sup>1</sup>  $(G, \oplus)$  together with a ring  $(R, +, *)$  of *scalars* and an action  $\cdot : R \times G \rightarrow G$  such that for all  $r, s \in R$  and all  $g, h \in G$  the following hold:

$$r \cdot (g \oplus h) = (r \cdot g) \oplus (r \cdot h)$$

$$(r + s) \cdot g = (r \cdot g) \oplus (s \cdot g)$$

$$(r * s) \cdot g = r \cdot (s \cdot g)$$

$$1 \cdot g = g.$$

For brevity, we will sometimes refer to such an  $R$ -module as  ${}_R G$  or simply  $G$ . The *size of a module* will refer to  $|G|$ .

As an example, any Abelian group  $(G, \oplus)$  is a  $\mathbb{Z}$ -module with action given by

$$n \cdot g = \begin{cases} \underbrace{g \oplus \cdots \oplus g}_{n \text{ adds}} & n > 0 \\ (-n) \cdot (-g) & n < 0 \\ 0 & n = 0. \end{cases}$$

In this case, the ring of the module is, in fact, infinite. Since we study network codes over finite alphabets, we assume all groups are finite, but in theory, the ring of a module need not be finite.

For an  $R$ -module  $G$  and a positive integer  $k$ ,

- $M_k(R)$  will denote the ring of all  $k \times k$  matrices with entries in  $R$ , and
- $G^k$  will denote the Abelian group of all  $k$ -dimensional vectors with entries in  $G$  with vector addition.

Then  $G^k$  is an  $M_k(R)$ -module where the action is matrix-vector multiplication with multiplication of elements of  $R$  and elements of  $G$  given by the action of  ${}_R G$ . The special case where  $G$  is the additive group of  $R$  will be of particular interest, since this corresponds to matrices over  $R$  acting on vectors over  $R$ .

We will use the same models as in Chapter 2 (see Section 2.1.1) for networks, alphabets, etc., except we now study the generalized case of linear codes over modules, as opposed to restricting to linear codes over rings. An edge function on the out-edge of a network node is *linear with respect to the module*  ${}_R G$  if can be written in the form

$$f(x_1, \dots, x_m) = (C_1 \cdot x_1) \oplus \dots \oplus (C_m \cdot x_m) \quad (3.1)$$

where  $x_1, \dots, x_m \in G$  are the inputs of the node and  $C_1, \dots, C_m \in R$  are constants. That is, the messages and edge symbols are elements of the Abelian group  $G$ , and the linear edge and decoding functions are determined by coefficients of the ring  $R$ . A decoding function is linear with respect to  ${}_R G$  if it has a form analogous to (3.1), and a code is *linear over a module*  ${}_R G$  if all edge and decoding functions are linear with respect to  ${}_R G$ . The alphabet size in a linear code over a module is the size of the module, i.e.  $|G|$ .

For any ring  $R$ , we denote its additive (Abelian) group by  $(R, +)$ . The special case of a module where the finite ring  $R$  acts on its own additive group  $(R, +)$  by multiplication in  $R$  is denoted by  ${}_R R$ , and in this case, (3.1) is equivalent to the definition of a scalar linear code over a ring that we used in Chapter 2.

A network is *linearly solvable over a module*  ${}_R G$  if there exists a linear solution over  ${}_R G$ . We will focus on two special types of linear codes:

- (i) A *scalar linear code over a ring*  $R$  is a linear code over the module  ${}_R R$ . A network is *scalar linearly solvable over  $R$*  if it has a linear solution over the module  ${}_R R$ .
- (ii) A  *$k$ -dimensional vector linear code over a ring*  $R$  is a linear code over the module  ${}_{M_k(R)} R^k$ . A network is *vector linearly solvable over  $R$*  if it has a linear solution over the module  ${}_{M_k(R)} R^k$ , for some positive integer  $k$ .

When referring to a linear code or solution over a ring, we will always specify (in this chapter) scalar versus vector, or if neither is specified, then we are referring to a linear code over a module. Additionally, when referring to an  $R$ -module  $G$ , the ring  $R$  is not assumed to be finite, unless otherwise specified. However, when referring to a scalar or vector linear code over a ring  $R$ , the ring  $R$  is assumed to be finite.

We can similarly define a right  $R$ -module and a linear code over a right  $R$ -module. However, it can easily be shown that any linear code over a right module is equivalent to a particular linear code over a left module, so we restrict attention only to left modules.

### 3.1.2 Our Contributions

Our main results are succinctly summarized in Section 3.5, where we also provide concluding remarks and list some potentially interesting open questions. The remainder of the chapter is outlined as follows. In Section 3.1.3, we prove lemmas which are used in proofs later in the chapter.

Section 3.2 analyzes the linear solvability of networks over ring alphabets which are not necessarily commutative. In Theorem 2.2.10 of Chapter 2, we proved that whenever a network is scalar linearly solvable over some commutative ring, then the smallest commutative ring over which the network is scalar linearly solvable is a field (and thus the ring is unique) Here, we prove (in Theorem 3.2.5) that if a network is scalar linearly solvable over some (not necessarily commutative) ring, then a smallest such ring is a matrix ring over a field. It remains unknown, however, whether there can be more than one smallest (not necessarily commutative) ring over which a network is linearly solvable, since in general, there can exist multiple matrix rings over fields that are the same size. We demonstrate (in Corollaries 3.2.13 and 3.3.8) that for two infinite classes of networks studied in this chapter, the smallest size ring over which each network is linearly solvable is indeed unique.

We prove (in Theorem 3.2.10) that if a network is linearly solvable over some module, then a smallest such module (i.e. with a smallest associated Abelian group) corresponds to a vector linear solution over some finite field.<sup>2</sup> We prove (in Theorem 3.2.12), in contrast to the commutative ring case, that the minimum size module with respect to linear solvability is not necessarily unique. Thus, for a fixed network, vector linear codes over fields are “best” in a certain sense, as these codes can minimize the alphabet size needed for a linear solution.

We also show (in Corollary 3.2.14) that for all networks, the following properties are equivalent: (i) vector linear solvability over some field, (ii) scalar linear solvability over some ring, and (iii) linear solvability over some module. Similarly, we show (in Corollary 3.2.15) that for all networks, the following properties are equivalent: (a) scalar linear solvability over some field, (b) scalar linear solvability over some commutative ring, and (c) linear solvability over some module whose ring is commutative.

In Section 3.3, we present a family of networks that generalize the  $M$  Network of [8, 15], and we enumerate (in Theorem 3.3.6) the particular vector dimensions over which each of these networks has vector linear solutions. A similar result was obtained by Das and Rai in [5]. We prove (in Corollary 3.3.7) that these networks have scalar linear solutions over certain non-commutative matrix rings yet do not have scalar linear solutions over any commutative ring. We also show (in Theorem 3.3.10) that if a network is scalar linearly solvable over a non-commutative ring  $R$  and is not scalar linearly solvable over any commutative ring, then  $|R| \geq 16$ . This lower bound is shown to be achievable (in Corollary 3.3.7 and Example 3.3.9) by exhibiting a network which has a scalar linear solution over a non-commutative ring of size 16 but not over any commutative ring.

---

<sup>2</sup>For example, in a  $k$ -dimensional vector linear code over a field  $\mathbb{F}$ , the alphabet size of the module is  $|\mathbb{F}|^k$ .

Section 3.4 focuses on linear solvability of networks over different modules with the same alphabet size, specifically,  $k$ -dimensional vector codes over  $\text{GF}(p)$  and scalar codes over rings of size  $p^k$ . We prove (in Theorem 3.4.1) that for each prime power  $p^k$ , there exists a network with a linear solution over a module of size  $p^k$  but with no scalar linear solutions over any ring of size  $p^k$ . These particular networks have  $k$ -dimensional vector linear solutions over  $\text{GF}(p)$ . Using a result of Sun et. al [17], we also show (in Corollary 3.4.3) that there exists a class of multicast networks with similar properties.

On the other hand, we show (in Theorem 3.4.6) that any network with a scalar linear solution over a commutative ring of size  $p^k$  has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ . We prove a similar result (in Theorem 3.4.17) for general rings of size  $p^k$  when  $k \leq 6$ . In this sense,  $k$ -dimensional vector linear codes over  $\text{GF}(p)$  are better than any scalar linear code over a ring of size  $p^k$ . Additionally, we show (in Theorems 3.4.6 and 3.4.17) that these results generalize in naturally to rings of non-power-of-prime sizes.

### 3.1.3 Comparisons of Modules

If  $G$  is a  $\mathbb{Z}$ -module, then as a consequence of Lagrange's theorem of finite groups,  $(n|G|) \cdot g = 0$  for all  $g \in G$  and all  $n \in \mathbb{Z}$ . In other words, there are multiple elements of  $\mathbb{Z}$  that act on  $G$  in the same way. Modules in which every element of the ring acts on  $G$  in a different way will be frequently discussed in this chapter.

**Definition 3.1.2.** An  $R$ -module  $G$  is *faithful* if for each  $r \in R \setminus \{0\}$ , there exists  $g \in G$  such that  $r \cdot g \neq 0$ .

Equivalently,  $r \cdot g = 0$  for all  $g$  if and only if  $r = 0$ . For any finite ring  $R$  and positive integer  $k$ , the  $M_k(R)$ -module  $R^k$  is faithful, so vector and scalar linear codes over rings are special cases of linear codes over faithful modules. On the other hand, it can be verified that the ring  $\mathbb{Z}_6$  of integers mod 6, acts on the additive group  $(\mathbb{Z}_2, \oplus)$  of integers mod 2, where the action is multiplication modulo 2. For each  $a = 0, 1$ , we have  $0 = 2a = 4a \pmod{2}$  so the  $\mathbb{Z}_6$ -module  $(\mathbb{Z}_2, \oplus)$  is not faithful.

For a fixed ring  $R$ , there are generally multiple modules over  $R$ . For example, if  $R$  is a subring of  $S$ , then  $(S, +)$  is an  $R$ -module where the action is multiplication in  $S$ , and  $(R, +)$  is also an  $R$ -module where the action is multiplication in  $R$ . However, We note, however, that not every ring and group pair can form a module. For example, the additive group of  $\text{GF}(2)$  cannot be a  $\text{GF}(3)$ -module. If  $(\text{GF}(2), \oplus)$  were a  $\text{GF}(3)$ -module, then we would have  $0 = 0 \cdot 1 = (1 + 1 + 1) \cdot 1 = (1 \cdot 1) \oplus (1 \cdot 1) \oplus (1 \cdot 1) = 1 \oplus 1 \oplus 1 = 1$  but  $0 \neq 1$  in  $\text{GF}(2)$ . The following lemma shows that the linear solvability of a network over a faithful  $R$ -module is

determined entirely by the ring of scalars  $R$  and not by the module's underlying Abelian group.

**Lemma 3.1.3.** *Let  $R$  be a fixed ring. If a network is linearly solvable over some faithful  $R$ -module, then it is linearly solvable over every  $R$ -module.*

*Proof.* Let  $\mathcal{N}$  be a network that is linearly solvable over the faithful  $R$ -module  $(G, \oplus)$ . Any linear solution for  $\mathcal{N}$  over the  $R$ -module  $(G, \oplus)$  is a linear solution for  $\mathcal{N}$  over any other  $R$ -module.

To see this, let  $z_1, \dots, z_m \in G$  denote the messages of  $\mathcal{N}$ , and suppose a node in  $\mathcal{N}$  has inputs  $x_1, \dots, x_n \in G$  in a solution over  ${}_R G$ , where, for each  $i = 1, \dots, n$ ,

$$x_i = \bigoplus_{j=1}^m (B_{i,j} \cdot z_j)$$

for some  $B_{i,1}, \dots, B_{i,m} \in R$ . Then for each output  $y \in G$  of this node, there exist constants  $C_1, \dots, C_n \in R$  such that

$$y = \bigoplus_{i=1}^n (C_i \cdot x_i) = \bigoplus_{i=1}^n \bigoplus_{j=1}^m ((C_i B_{i,j}) \cdot z_j) = \bigoplus_{j=1}^m \left( \left( \sum_{i=1}^n C_i B_{i,j} \right) \cdot z_j \right).$$

Now let  $H$  be any  $R$ -module with action  $\odot$ , and suppose the corresponding inputs to the node in the linear code over  ${}_R H$  are  $x'_1, \dots, x'_n \in H$  and can be written in terms of the messages  $z'_1, \dots, z'_m \in H$  in the following way

$$x'_i = \bigoplus_{j=1}^m (B_{i,j} \odot z'_j).$$

Then the corresponding output  $y' \in R$  of the node is of the form

$$y' = \bigoplus_{i=1}^n (C_i \odot x'_i) = \bigoplus_{i=1}^n \bigoplus_{j=1}^m ((C_i B_{i,j}) \odot z'_j) = \bigoplus_{j=1}^m \left( \left( \sum_{i=1}^n C_i B_{i,j} \right) \odot z'_j \right).$$

so by induction, every edge and decoding function in the linear code over  ${}_R H$  is the same linear combination of the messages as in the linear solution over  ${}_R G$ .

$G$  is a faithful  $R$ -module, so 1 and 0 are the only elements of  $R$  such that  $1 \cdot g = g$  and  $0 \cdot g = 0$  for all  $g \in G$ . Hence it must be the case that decoding functions in the linear solution over  ${}_R G$  are of the form

$$(1 \cdot z_i) \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^n (0 \cdot z_j) = z_i.$$

so it must be the case that the corresponding decoding function in the linear code over  ${}_R H$  is

$$(1 \odot z'_i) \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^n (0 \odot z'_j) = z'_i.$$

Hence, each receiver can linearly recover its demands, so the linear code over  ${}_R H$  is, in fact, a solution. ■

In contrast to Lemma 3.1.3, if  $G$  is both an  $R$ -module and an  $S$ -module, then there may exist a network that is linearly solvable over  ${}_S G$  but not  ${}_R G$ . For example, consider the case where  $G = (\text{GF}(4), +)$ ,  $R = \text{GF}(2)$ , and  $S = \text{GF}(4)$ . Then  $\text{GF}(2)$  is a subfield of  $\text{GF}(4)$ , so  $G$  is both a faithful  $R$ -module and a faithful  $S$ -module. We demonstrate (in Corollary 3.2.13) a network that is scalar linearly solvable over  $\text{GF}(4)$  but not  $\text{GF}(2)$ , and by Lemma 3.1.3, this network is linearly solvable over  ${}_S G$  but not  ${}_R G$ .

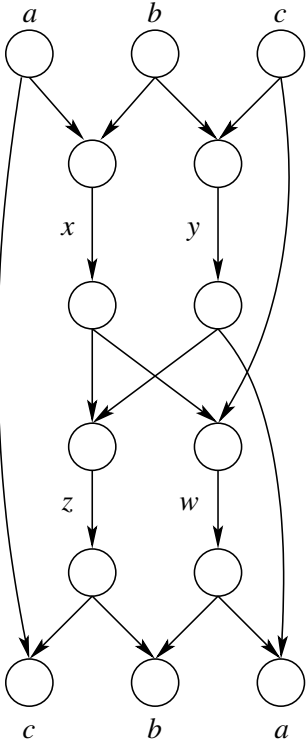


Figure 3.1: The Fano Network is constructed from the Fano matroid [8].

The *Fano Network* is given in Figure 3.1 and has been used to show numerous interesting properties of network coding. The following example illustrates the importance of the premise in Lemma 3.1.3 by demonstrating that the Fano Network has a linear solution over an unfaithful  $\mathbb{Z}_6$ -module yet has no linear solutions over another  $\mathbb{Z}_6$ -module.

**Example 3.1.4.** The Fano Network has a linear solution over the unfaithful  $\mathbb{Z}_6$ -module  $(\mathbb{Z}_2, \oplus)$  but not the faithful  $\mathbb{Z}_6$ -module  $(\mathbb{Z}_6, +)$ .

*Proof.* It was shown in [7, Corollary 11] that the Fano Network has solutions only over alphabets whose sizes are powers of 2, so in particular, the Fano Network has no linear solutions over the  $\mathbb{Z}_6$ -module  $(\mathbb{Z}_6, +)$ , since the alphabet size is 6 in this case.

Define a linear code for the Fano Network over the  $\mathbb{Z}_6$ -module  $(\mathbb{Z}_2, \oplus)$  as follows:

$$x = a \oplus b, \quad y = b \oplus c, \quad z = x \oplus y, \quad w = x \oplus c.$$

Each of the scalars in  $\mathbb{Z}_6$  is 1. Then, since  $g \oplus g = 0$  for all  $g \in \mathbb{Z}_2$ , we have

$$z \oplus a = c, \quad z \oplus w = b, \quad w \oplus y = a.$$

Thus each receiver is able to linearly recover its demands from its inputs, so the code over the  $\mathbb{Z}_6$ -module  $(\mathbb{Z}_2, \oplus)$  is a linear solution. ■

If we take the linear code given in Example 3.1.4 to be over the  $\mathbb{Z}_6$ -module  $(\mathbb{Z}_6, +)$ , i.e. the same linear combinations of inputs in a scalar linear code over  $\mathbb{Z}_6$ , then

$$x = a + b, \quad y = b + c, \quad z = x + y$$

and  $z + a = 2a + 2b + c \neq c$  so clearly this code is not a solution when taken over the  $\mathbb{Z}_6$ -module  $\mathbb{Z}_6$ , which agrees with the result from [7]. If  $R$  is any ring such that  $(\mathbb{Z}_2, \oplus)$  is an  $R$ -module, then the linear solution for the Fano Network in Example 3.1.4 is a linear solution over the  $R$ -module  $(\mathbb{Z}_2, \oplus)$ . For example, for each positive integer  $n$ ,  $(\mathbb{Z}_2, \oplus)$  is a  $\mathbb{Z}_{2n}$ -module where the action is multiplication modulo 2.

In fact, whenever  $n$  and  $m$  are positive integers, the ring  $\mathbb{Z}_{nm}$  acts on  $(\mathbb{Z}_m, +)$  by multiplication modulo  $m$ . Such a module is faithful when  $n = 1$  and is unfaithful otherwise. So if a network has a scalar linear solution over  $\mathbb{Z}_{nm}$ , which is equivalent to a linear solution over the faithful  $\mathbb{Z}_{nm}$ -module  $(\mathbb{Z}_{nm}, +)$ , then the network also has a linear solution over the (possibly unfaithful)  $\mathbb{Z}_{nm}$ -module  $(\mathbb{Z}_n, \oplus)$ . Although, as demonstrated in Example 3.1.4, the converse may not be true.

While these trivial examples may not seem particularly useful, Corollary 3.1.5 demonstrates an important special case of Lemma 3.1.3 which will be used frequently in later proofs. It demonstrates an equivalence between scalar linear solutions over matrix rings and vector linear solutions over rings.

**Corollary 3.1.5.** *Let  $R$  be a finite ring,  $k$  a positive integer, and  $\mathcal{N}$  a network. Then  $\mathcal{N}$  is scalar linearly solvable over the ring of  $k \times k$  matrices whose elements are from  $R$  if and only if  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $R$ .*

*Proof.* The “if” and the “only if” directions are each obtained by separately applying Lemma 3.1.3, since  $M_k(R)$  and  $R^k$  are faithful  $M_k(R)$ -modules with matrix-matrix multiplication and matrix-vector multiplication, respectively. ■



Note that in a  $k$ -dimensional vector linear code over a ring  $R$ , the alphabet size is  $|R|^k$ , whereas in a scalar linear solution over  $M_k(R)$ , the alphabet size is  $|R|^{k^2}$ . So any network that is scalar linearly solvable over the matrix ring  $M_k(R)$  is also linearly solvable over a smaller module alphabet. We will generalize this idea in Theorem 3.2.10.

**Lemma 3.1.6.** *If  $\phi : R \rightarrow S$  is a ring homomorphism and network  $\mathcal{N}$  is linearly solvable over some faithful  $R$ -module, then  $\mathcal{N}$  is linearly solvable over every  $S$ -module.*

*Proof.* Let  $H$  be an  $S$ -module and define a mapping  $\odot : R \times H \rightarrow H$  by  $r \odot h = \phi(r) \cdot h$ , where  $\cdot$  is the action of  $S$  on  $H$ . One can verify that  $H$  is an  $R$ -module under  $\odot$ . Now, let  $G$  be a faithful  $R$ -module, and suppose  $\mathcal{N}$  has a linear solution over  ${}_R G$ . By Lemma 3.1.3,  $\mathcal{N}$  is linearly solvable over  ${}_R H$ , so every output  $y' \in H$  in the solution over  ${}_R H$  is of the form

$$y' = (C_1 \odot x_1) \oplus \cdots \oplus (C_m \odot x_m) \quad (3.2)$$

where  $x_1, \dots, x_m \in H$  are the parent node's inputs and  $C_1, \dots, C_m \in R$  are constants.

Form a linear code for  $\mathcal{N}$  over  ${}_S H$  by replacing each coefficient  $C_i$  in (3.2) by  $\phi(C_i)$ . Let  $y \in H$  be the output in the code over  ${}_S H$  corresponding to  $y'$  in the code over  ${}_R H$ . Then

$$y = (\phi(C_1) \cdot x_1) \oplus \cdots \oplus (\phi(C_m) \cdot x_m) = (C_1 \odot x_1) \oplus \cdots \oplus (C_m \odot x_m) = y'.$$

By induction, whenever an edge function in the solution over  ${}_R H$  outputs the symbol  $y'$ , the corresponding edge function in the code over  ${}_S H$  will output the same symbol  $y'$ . Likewise, whenever  $x$  is an input to an edge function in the solution over  ${}_R H$ , the corresponding input of the corresponding edge function in the code over  ${}_S H$  will be the same symbol  $x$ . The same argument holds for the decoding functions in the code over  ${}_S H$ , so each receiver will correctly obtain its corresponding demands in the code over  ${}_S H$ . Hence, the code over  ${}_S H$  is a linear solution for  $\mathcal{N}$ . ■

Corollary 3.1.7 was also shown in Chapter 2 as Lemma 2.2.5. However, Corollary 3.1.7 can also be viewed as a special case of Lemma 3.1.6 where the modules are  ${}_R R$  and  ${}_S S$ .

**Corollary 3.1.7.** *Let  $R$  and  $S$  be finite rings. If there exists a ring homomorphism from  $R$  to  $S$ , then every network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $S$ .*

For finite rings  $R$  and  $S$ , special cases of Corollary 3.1.7 include:

- (1)  $R$  is a subring of  $S$ :

The identity mapping is an injective homomorphism from  $R$  to  $S$ , so any network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $S$ .

(2)  $R$  has a two-sided ideal  $I$ :

There is a surjective homomorphism from  $R$  to  $R/I$  (see Lemma 3.2.2), so any network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $R/I$ .

(3)  $\phi : R \times S \rightarrow R$  is the projection mapping:

$\phi$  is a surjective homomorphism, so any network that is scalar linearly solvable over  $R \times S$  is also scalar linearly solvable over  $R$  (and likewise over  $S$ ).

Cases (1), (2), and (3) agree with Corollaries 2.2.6 and 2.2.9 and Lemma 2.2.12, respectively.

## 3.2 Commutative and Non-Commutative Rings

In this section, we will focus on linear codes over modules whose ring acts on its own Abelian group, i.e. scalar linear codes over rings. As noted after Corollary 3.1.7, for any two-sided ideal  $I$  of a finite ring  $R$ , every network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $R/I$ , so in determining the smallest ring over which a network is scalar linearly solvable, it is natural to focus attention on rings without two-sided ideals.

A ring is *simple* if it has no proper two-sided ideals. That is, its only two-sided ideals are the ring itself and the trivial ideal  $\{0\}$ . The following lemmas give results related to simple rings and network linear solvability.

**Lemma 3.2.1.** *A finite ring is simple if and only if it is isomorphic to a matrix ring over a field.*

*Proof.* This is a corollary of the Artin-Wedderburn theorem (e.g. [13, p. 36, Theorem 3.10 (4)] and [14, p. 20, Theorem II.9]). ■

**Lemma 3.2.2.** [9, Theorem 7, p. 243]: *If  $I$  is a two-sided ideal of ring  $R$ , then the mapping  $\phi : R \rightarrow R/I$  given by  $\phi(x) = x + I$  is a surjective homomorphism.*

**Lemma 3.2.3.** *For each finite ring  $R$ , there exists a simple ring  $S$  such that the following hold:*

- (a) *there exists a surjective homomorphism from  $R$  to  $S$ ,*
- (b) *every network that is scalar linearly solvable over  $R$  is scalar linearly solvable over  $S$ , and*
- (c)  *$|S|$  divides  $|R|$ .*

*Proof.* If  $R$  is a simple ring, then each statement is trivially true by taking  $S = R$ , so we may assume  $R$  is not a simple ring. Thus,  $R$  has a proper maximal two-sided ideal  $I$ . Let  $S = R/I$ , and note that since  $I$  is maximal,  $S$  is simple. The mapping  $\phi : R \rightarrow R/I$  given by  $\phi(x) = x + I$  is a surjective homomorphism by

Lemma 3.2.2, which proves (a). Hence by Corollary 3.1.7, any network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $S$ , which proves (b). Since  $R$  is finite, we know that  $|R/I|$  divides  $|R|$ , which proves (c). ■

If  $R$  is a finite commutative ring and  $S$  is a simple ring satisfying (a)-(c) in Lemma 3.2.3, then  $S$  must also be commutative, since there is a surjective homomorphism from  $R$  to  $S$ . However, as we demonstrate in the following example, if  $R$  is non-commutative, then such an  $S$  is not necessarily non-commutative. Theorem 3.2.5 demonstrates that any smallest ring over which a network is scalar linearly solvable is simple.

**Example 3.2.4.** The following demonstrates: (i) a class of non-commutative rings for which the simple ring in Lemma 3.2.3 is non-commutative, and (ii) a class of non-commutative rings for which the simple ring in Lemma 3.2.3 is commutative.

- (i) For any positive integers  $k, n$ , and prime divisor  $p$  of  $n$ , there exists a surjective homomorphism from the non-commutative ring  $M_k(\mathbb{Z}_n)$  to the non-commutative simple ring  $M_k(\mathbb{Z}_p)$ , given by matrix-component-wise reduction mod  $p$ .
- (ii) For each field  $\mathbb{F}$  and integer  $k \geq 2$ , there exists a surjective homomorphism from the non-commutative ring of upper triangular  $k \times k$  matrices with entries in  $\mathbb{F}$  to the commutative simple ring  $\mathbb{F}$  (see the proof of Lemma 3.4.10).

**Theorem 3.2.5.** *If a network is scalar linearly solvable over a ring  $R$  but not over any smaller ring, then  $R$  is a matrix ring over a field.*

*Proof.* Suppose a network  $\mathcal{N}$  is scalar linearly solvable over a ring  $R$  that is not simple. By Lemma 3.2.3 (a) (b), there exists a simple ring  $S$  and a surjective homomorphism  $\phi : R \rightarrow S$ , such that  $\mathcal{N}$  is scalar linearly solvable over  $S$ . Since  $\phi$  is surjective,  $|R| \geq |S|$ , but since  $S$  is simple and  $R$  is not, the two rings cannot be isomorphic, so  $|R| \neq |S|$ , and therefore  $|R| > |S|$ . This proves that every smallest size ring over which  $\mathcal{N}$  is scalar linearly solvable must be simple, which implies that such a ring is a matrix ring over a field by Lemma 3.2.1. ■

In Theorem 2.2.10 of Chapter 2, we showed that the smallest-size commutative ring over which a network is scalar linearly solvable is unique. However, there may exist multiple simple rings of the same size. For example,  $\text{GF}(p^4)$  and  $M_2(\text{GF}(p))$  are non-isomorphic simple rings of size  $p^4$ . An interesting open

question is whether every network with a scalar linear solution over multiple simple rings of the same size also must have a scalar linear solution over some smaller simple ring. In other words, is the smallest ring  $R$  in Theorem 3.2.5 unique for a given network? We demonstrate (in Corollaries 3.2.13 and 3.3.8) that for two infinite classes of networks (one of which is a class of multicast networks) studied in this chapter, the smallest-size ring over which each network is scalar linearly solvable is unique.

### 3.2.1 Modules and Vector Linear Codes

In a linear network code over a module  ${}_R G$ , in principle, the ring  $R$  need not be finite (although representing linear code coefficients might be problematic). However, in a linear network code over a module, the alphabet is finite, so the Abelian group  $G$  must be finite.<sup>3</sup> The following lemma and corollary show that linear solutions over unfaithful modules (whose ring may be infinite) admit linear solutions over faithful modules (whose ring is finite).

**Lemma 3.2.6.** *Let  $G$  be an  $R$ -module. There exists a finite ring  $S$  such that  $G$  is a faithful  $S$ -module, and any network that is linearly solvable over  ${}_R G$  is linearly solvable over  ${}_S G$ .*

*Proof.* We use ideas from [6, p. 2750] here. Let  $J = \{r \in R : r \cdot g = 0, \forall g \in G\}$  which is easily verified to be a two-sided ideal of  $R$ . Let  $S = R/J$ . It can also be verified that  $G$  is an  $S$ -module with action  $\odot : S \times G \rightarrow G$  given by  $(r+J) \odot g = r \cdot g$ . If  $(r+J), (s+J) \in S$  are such that  $(r+J) \odot g = (s+J) \odot g$  for all  $g \in G$ , then  $(r-s) \cdot g = 0$ , which implies  $(r-s) \in J$ . Hence  $(r+J) = (s+J)$ , so the ring  $S$  acts faithfully on  $G$ . A faithful module requires different elements of the ring to yield different functions when acting on elements of the group. Since  $G$  is finite, the number of such functions must be finite, which implies the ring  $S$  must also be finite.

Suppose a network  $\mathcal{N}$  is linearly solvable over  ${}_R G$ . Every output  $y'$  in the solution over  ${}_R G$  is of the form

$$y' = (C_1 \cdot x_1) \oplus \cdots \oplus (C_m \cdot x_m) \quad (3.3)$$

where the  $x_i$ 's are the parent node's inputs and the  $C_i$ 's are constants from  $R$ . Form a linear code over  ${}_S G$  replacing each coefficient  $C_i$  in (3.3) by  $(C_i+J)$ . Let  $y$  be the edge symbol in the code over  ${}_S G$  corresponding to  $y'$  in the code over  ${}_R G$ . Then

$$y = ((C_1+J) \odot x_1) \oplus \cdots \oplus ((C_m+J) \odot x_m) = (C_1 \cdot x_1) \oplus \cdots \oplus (C_m \cdot x_m) = y'.$$

---

<sup>3</sup>We will call a module "finite" if and only if its Abelian group is finite.

Thus, whenever an edge function in the solution over  ${}_R G$  outputs the symbol  $y'$ , the corresponding edge function in the code over  ${}_S G$  will output the same symbol  $y'$ . Likewise, whenever  $x$  is an input to an edge function in the solution over  ${}_R G$ , the corresponding input of the corresponding edge function in the code over  ${}_S G$  will be the same symbol  $x$ . The same argument holds for the decoding functions in the code over  ${}_S G$ , so each receiver will correctly obtain its corresponding demands in the code over  ${}_S G$ . Hence, the code over  ${}_S G$  is a linear solution for  $\mathcal{N}$ . ■

**Corollary 3.2.7.** *Let  $G$  be an  $R$ -module such that  $R$  is commutative. There exists a finite commutative ring  $S$  such that  $G$  is a faithful  $S$ -module, and any network that is linearly solvable over  ${}_R G$  is linearly solvable over  ${}_S G$ .*

*Proof.* This proof is identical to the proof of Lemma 3.2.6. However, since  $R$  is commutative, the ring  $S = R/J$  is also commutative. ■

A *submodule* of an  $R$ -module  $G$  is a subgroup  $H$  of  $G$  such that  $H$  is closed when acted on by  $R$ . That is, both  $H$  and  $G$  are  $R$ -modules and  $H \subseteq G$ . Submodules are of particular interest, since by Lemma 3.1.3, if  $G$  and  $H$  are faithful  $R$ -modules, then the set of networks that are linearly solvable over  ${}_R G$  and the set of networks that are linearly solvable over  ${}_R H$  are equal, yet a linear code over  ${}_R H$  has a smaller alphabet if  $H$  is a proper submodule of  $G$ . As an example, let  $I$  be a two-sided ideal in the ring  $R$ . Then  $(I, +)$  is a subgroup of  $(R, +)$  that is closed under multiplication in  $R$ , so  ${}_R I$  is a submodule of the  $R$ -module  $R$ . As another example, for each finite field  $\mathbb{F}$  and integer  $k \geq 2$ , the  $M_k(\mathbb{F})$ -module  $\mathbb{F}^k$  is a proper submodule of the  $M_k(\mathbb{F})$ -module  $M_k(\mathbb{F})$ . Lemmas 3.2.8 and 3.2.9 show results related to submodules that will be used to prove Theorem 3.2.10.

**Lemma 3.2.8.** [13, Theorem 3.3 (2), p. 31]: *Let  $\mathbb{F}$  be a finite field and  $k$  a positive integer. Then  $\mathbb{F}^k$  is the only  $M_k(\mathbb{F})$ -module that has no proper submodules.*

By Lemma 3.1.3, for each ring  $R$ , if a network is linearly solvable over a faithful  $R$ -module, then it is linearly solvable over every  $R$ -module. When a network is solvable over the  $R$ -modules for a particular ring  $R$ , it may be desirable for linear network coding to determine the minimum-size  $R$ -modules. Lemma 3.2.9 considers this question for rings of matrices over a finite field.

**Lemma 3.2.9.** *Let  $\mathbb{F}$  be a finite field and  $k$  a positive integer. If  $G$  is a finite non-zero  $M_k(\mathbb{F})$ -module, then  $|\mathbb{F}|^k$  divides  $|G|$ .*

*Proof.* Since  $G$  is finite and non-zero,  $G$  contains a submodule with no proper submodules (possibly  $G$  itself). By Lemma 3.2.8,  $\mathbb{F}^k$  is the only  $M_k(\mathbb{F})$ -module with no proper submodules, so  $\mathbb{F}^k$  is a submodule of  $G$ . Hence by Lagrange's theorem of finite groups (e.g. [9, p. 89, Theorem 8]),  $|\mathbb{F}|^k$  divides  $|G|$ . ■

The following theorem is a generalization of Theorem 3.2.5, where we characterize smallest-size modules over which networks are linearly solvable. Theorem 3.2.10 demonstrates that if a network is linearly solvable over some module, then there exists a vector linear code over a field that minimizes the alphabet size needed for a linear solution.

**Theorem 3.2.10.** *Suppose a network  $\mathcal{N}$  is linearly solvable over an  $R$ -module  $G$ . Then the following hold:*

- (a) *There exists a finite field  $\mathbb{F}$  and positive integer  $k$  such that  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $\mathbb{F}$  and  $|\mathbb{F}|^k$  divides  $|G|$ .*
- (b) *If  $R$  is commutative, then there exists a finite field  $\mathbb{F}$  such that  $\mathcal{N}$  has a scalar linear solution over  $\mathbb{F}$  and  $|\mathbb{F}|$  divides  $|G|$ .*

*Proof.* If the ring  $R$  is infinite, then by Lemma 3.2.6,  $\mathcal{N}$  is linearly solvable over some faithful module with a finite ring. If  $R$  is commutative, then by Corollary 3.2.7,  $\mathcal{N}$  is linearly solvable over some faithful module with a finite commutative ring. So without loss of generality, assume  $R$  is finite and  $G$  is a faithful  $R$ -module. By Lemmas 3.2.1 and 3.2.3 (a), since  $R$  is finite, there exists a field  $\mathbb{F}$ , a positive integer  $k$ , and a surjective homomorphism  $\phi : R \rightarrow M_k(\mathbb{F})$ . By Lemma 3.1.6 any network that is linearly solvable over the faithful  $R$ -module  $G$  is also linearly solvable over every  $M_k(\mathbb{F})$ -module, so in particular,  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $\mathbb{F}$ . Since  $\phi$  is a homomorphism, any  $R$ -module is also an  $M_k(\mathbb{F})$ -module (see the proof of Lemma 3.1.6). Thus, both  $G$  and  $\mathbb{F}^k$  are  $M_k(\mathbb{F})$ -modules, so by Lemma 3.2.9, it must be the case that  $|\mathbb{F}|^k$  divides  $|G|$ .

If  $R$  is commutative, then, since  $\phi$  is a surjective homomorphism,  $M_k(\mathbb{F})$  must also be commutative, which implies  $k = 1$ . Hence  $\mathcal{N}$  has a scalar linear solution over  $\mathbb{F}$  and  $|\mathbb{F}|$  divides  $|G|$ . ■

Theorem 3.2.10 demonstrates that, in some sense, vector linear codes over finite fields are optimal for linear network coding, as they can minimize the alphabet size needed for a linear solution. In particular, if  $G$  is an  $R$ -module that yields a minimum-size linear solution for a network  $\mathcal{N}$ , then Theorem 3.2.10 implies there exists a field  $\mathbb{F}$  and an integer  $k$  such that  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $\mathbb{F}$

and  $|\mathbb{F}|^k \mid |G|$ . Since the linear code over  ${}_R G$  yields a minimum-size solution, we must have  $|G| = |\mathbb{F}|^k$ , so the  $M_k(\mathbb{F})$ -module  $\mathbb{F}^k$  also yields a minimum-size linear solution.

The following lemmas will be used to show (in Theorem 3.2.12) that a minimum-size module over which a network is linearly solvable is not necessarily unique. Lemma 3.2.11 is a result of Sun et. al [17], and similar results have been shown in, for example, [10].

**Lemma 3.2.11.** [17, Proposition 1]: *Let  $q$  be a prime power and  $k$  a positive integer. If a network has a scalar linear solution over  $\text{GF}(q^k)$ , then it has a  $k$ -dimensional vector linear solution over  $\text{GF}(q)$ .*

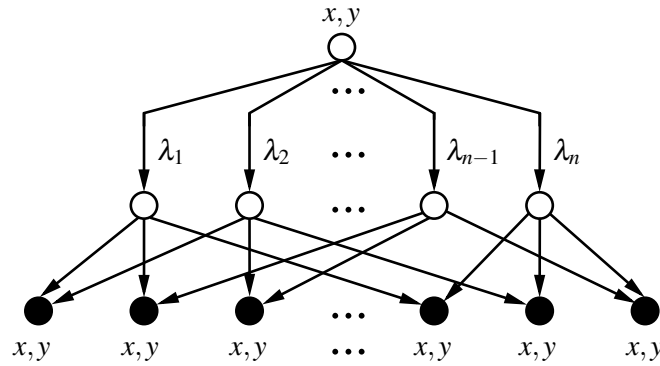


Figure 3.2: The  $n$ -Choose-Two Network is parameterized by an integer  $n \geq 2$ . The network’s name indicates the number of receivers.

For each integer  $n \geq 3$ , the  $n$ -Choose-Two Network is a multicast network given in Figure 3.2. These networks were described by Rasala Lehman and Lehman [16] and were further studied in Chapter 2. We make use of Lemma 2.2.15 from Chapter 2 in the proofs of the following two results. Lemma 2.2.15 is a result from [16] regarding the solvability of the  $n$ -Choose-Two Networks.

**Theorem 3.2.12.** *For each integer  $k \geq 2$  and prime  $p$ , the  $(p^k + 1)$ -Choose-Two Network is linearly solvable over at least two distinct modules of size  $p^k$  but not over any smaller modules.*

*Proof.* By Lemma 2.2.15, the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p^k)$  and is not solvable over any alphabet whose size is less than  $p^k$ . By Lemma 3.2.11, any network with a scalar linear solution over  $\text{GF}(p^k)$  has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ . Hence the  $(p^k + 1)$ -Choose-Two Network has a scalar linear solution over  $\text{GF}(p^k)$  and a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ , yet the network has no linear solution over any module whose size is less than  $p^k$ . ■

The following corollary generalizes Theorem 2.2.16 from Chapter 2, which showed the  $(p^k + 1)$ -Choose-Two Network is not scalar linearly solvable over any commutative ring of size  $p^k$  other than the field  $\text{GF}(p^k)$ . In fact, as a result of Corollary 3.2.13, the  $(p^k + 1)$ -Choose-Two Network is not scalar linearly solvable over any ring of size  $p^k$  other than the field.

**Corollary 3.2.13.** *For each integer  $k \geq 2$  and prime  $p$ , the unique smallest-size ring over which the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable is  $\text{GF}(p^k)$ .*

*Proof.* By Lemma 2.2.15, the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p^k)$  and is not solvable over any smaller alphabet. Suppose the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable over a ring  $R$  of size  $p^k$ . By Lemmas 3.2.1 and 3.2.3 (a) (b), there exists a field  $\mathbb{F}$ , a positive integer  $n$ , and a surjective homomorphism  $\phi : R \rightarrow M_n(\mathbb{F})$  such that the  $(p^k + 1)$ -Choose-Two Network is scalar linearly solvable over the ring  $M_n(\mathbb{F})$ . Since  $\phi$  is surjective,  $|R| = p^k \geq |\mathbb{F}|^{n^2}$ . By Corollary 3.1.5, the  $(p^k + 1)$ -Choose-Two Network has an  $n$ -dimensional vector linear solution over  $\mathbb{F}$ , so by Lemma 2.2.15 (a),  $|\mathbb{F}|^n \geq p^k = |R|$ . Hence  $|\mathbb{F}|^n \geq |R| \geq |\mathbb{F}|^{n^2}$  which implies  $n = 1$  and  $|\mathbb{F}| = |R| = p^k$ . Since  $\phi : R \rightarrow \mathbb{F}$  is a surjective homomorphism and we have  $R \cong \mathbb{F}$ , and since  $|R| = p^k$ , we have  $R \cong \text{GF}(p^k)$ . ■

The following corollaries summarize our results on the linear solvability of networks using scalar and linear vector codes over fields, scalar linear codes over rings, and linear codes over modules. Corollary 3.2.14 shows an equivalence between vector linear solvability over fields and linear solvability over rings and modules, while Corollary 3.2.15 shows an equivalence between scalar linear solvability over fields and linear solvability over commutative rings and modules.

**Corollary 3.2.14.** *For any network  $\mathcal{N}$ , the following three statements are equivalent:*

- (i)  $\mathcal{N}$  is vector linearly solvable over some finite field.
- (ii)  $\mathcal{N}$  is scalar linearly solvable over some ring.
- (iii)  $\mathcal{N}$  is linearly solvable over some module.

*Proof.* If a network has a  $k$ -dimensional vector linear solution over some field  $\mathbb{F}$ , then by Corollary 3.1.5 it has a scalar linear solution over the ring  $M_k(\mathbb{F})$ , hence (i) implies (ii). A scalar linear code over a ring is a special case of a linear code over a module, so (ii) implies (iii). By Theorem 3.2.10 (a), (iii) implies (i). ■



**Corollary 3.2.15.** For any network  $\mathcal{N}$ , the following three statements are equivalent:

- (i)  $\mathcal{N}$  is scalar linearly solvable over some finite field.
- (ii)  $\mathcal{N}$  is scalar linearly solvable over some commutative ring.
- (iii)  $\mathcal{N}$  is linearly solvable over some module whose ring is commutative.

*Proof.* A scalar linear code over a finite field is a special case of a scalar linear code over a commutative ring, hence (i) implies (ii). A scalar linear code over a commutative ring is a special case of a linear code over a module where the ring is commutative, so (ii) implies (iii). By Theorem 3.2.10 (b), (iii) implies (i). ■

### 3.3 The Dim- $k$ Networks

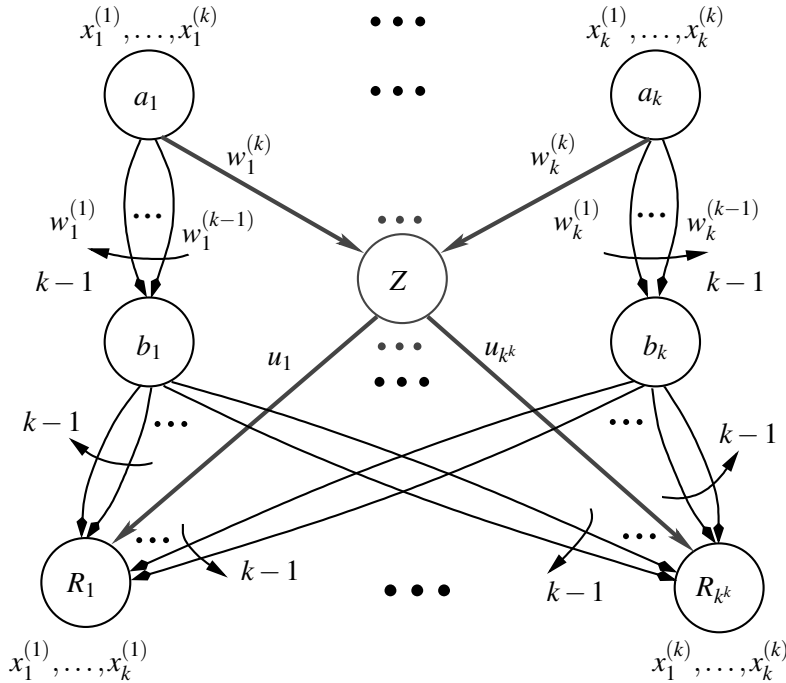


Figure 3.3: The Dim- $k$  Network. For each  $i = 1, \dots, k$ , the node  $a_i$  is a source node that generates messages  $x_i^{(1)}, \dots, x_i^{(k)}$ , and  $a_i$  has  $k-1$  parallel out-edges to node  $b_i$  and one out-edge to node  $Z$ . For each  $j = 1, \dots, k^k$ , the receiver  $R_j$  has  $k-1$  parallel in-edges from each of the nodes  $b_1, \dots, b_k$  and a single in-edge from node  $Z$ . Each receiver demands a single message from each source node and each set of  $k$  messages demanded by each receiver is unique; that is, for any  $i_1, \dots, i_k \in \{1, \dots, k\}$ , there is exactly one receiver which demands  $x_1^{(i_1)}, \dots, x_k^{(i_k)}$ .

For each integer  $k \geq 2$ , the *Dim- $k$  Network* is defined in Figure 3.3 and is referred to as such because it has vector linear solutions precisely over vector dimensions that are multiples of  $k$ . We prove this fact in Theorem 3.3.6. This infinite family of networks will be used to demonstrate several theorems related to commutative and non-commutative rings. The special case of  $k = 2$  corresponds to the *M Network* of [15], shown later in Figure 3.4. Das and Rai [5] presented a class of networks, called the *Generalized M Networks*, which are similar to the *Dim- $k$  Networks*. They independently proved a result analogous to Theorem 3.3.6, using a more general approach involving matroid theory. We include our proof of Theorem 3.3.6 for completeness.

**Remark 3.3.1.** *The Dim- $k$  Network has  $k^k + 2k + 1$  nodes and  $k^k(k^2 - k + 1) + k^2$  edges.*

A  *$k$ -dimensional vector routing code over an alphabet  $\mathcal{A}$*  is a code in which messages and edge symbols are elements of  $\mathcal{A}^k$  and edge and decoding functions copy certain input vector components to certain output vector components. A vector routing code over  $\mathcal{A}$  is, in fact, a special case of a vector linear code over  $\mathcal{A}$  where each row of each of the matrices  $C_1, \dots, C_m$  in (3.1) is either all zero or else has 1 one and  $k - 1$  zeros, and for each  $i \leq k$ , at most one of the matrices  $C_1, \dots, C_m$  has a non-zero  $i$ th row.

**Lemma 3.3.2.** *For each integer  $k \geq 2$  and alphabet  $\mathcal{A}$ , the Dim- $k$  Network has an  $k$ -dimensional vector routing solution over  $\mathcal{A}$ .*

*Proof.* Each message and edge symbol is an element of  $\mathcal{A}^k$ . Let  $[x]_i$  denote the  $i$ th component of  $x \in \mathcal{A}^k$ . Define a  $k$ -dimensional routing code over  $\mathcal{A}$  by

$$\left[ w_i^{(j)} \right]_l = \left[ x_i^{(l)} \right]_j \quad (i, j, l = 1, \dots, k).$$

That is, the  $l$ th component of the  $j$ th out-edge of the  $i$ th source node carries the  $j$ th component of the  $l$ th message originating at the  $i$ th source node.

For each  $i = 1, \dots, k$  and each  $j = 1, \dots, k^k$ , let the set of  $(k - 1)$  parallel edges from node  $b_i$  to receiver  $R_j$  carry the symbols  $w_i^{(1)}, \dots, w_i^{(k-1)}$ . Then each receiver gets the first  $(k - 1)$  components of every message from the edges originating at  $b_1, \dots, b_k$ , so in particular, each receiver can recover the first  $(k - 1)$  components of each of the messages it demands.

Node  $Z$  receives the  $k$ th component of each message, so each of its out-edges can carry any  $k$  of these components. Let  $j \in \{1, \dots, k^k\}$ , suppose  $x_1^{(i_1)}, \dots, x_k^{(i_k)}$  are the messages receiver  $R_j$  demands, and let

$$\left[ u_j \right]_l = \left[ w_l^{(k)} \right]_{i_l} = \left[ x_l^{(i_l)} \right]_k \quad (l = 1, \dots, k).$$

Then  $R_j$  can recover the  $k$ th component of each of the messages it demands. Since  $j$  was chosen arbitrarily, the code is an  $k$ -dimensional vector routing solution. ■

The following lemmas will be used in later proofs, and similar results have been noted in other works, such as [17, Proposition 5] and [10, Example VI.2].

**Lemma 3.3.3.** *Let  $R$  be a finite ring and let  $k_1, \dots, k_t$  be positive integers. If a network has  $k_1, \dots, k_t$ -dimensional vector linear solutions over  $R$ , then the network has a  $(k_1 + \dots + k_t)$ -dimensional vector linear solution over  $R$ .*

*Proof.* Assume a network has a  $k_i$ -dimensional vector linear solution over  $R$  for each  $i = 1, \dots, t$ . In the  $k_i$ -dimensional vector linear solution over  $R$ , every edge function is of the form  $y^{(i)} = C_1^{(i)} x_1^{(i)} + \dots + C_m^{(i)} x_m^{(i)}$ , where  $x_j^{(i)} \in R^{k_i}$  are the inputs to the node and  $C_j^{(i)}$  are  $k_i \times k_i$  matrices over  $R$ . For any such edge function, define a  $(k_1 + \dots + k_t)$ -dimensional vector linear edge function over  $R$  by letting

$$\begin{bmatrix} y^{(1)} \\ \vdots \\ y^{(t)} \end{bmatrix} = \sum_{j=1}^m \begin{bmatrix} C_j^{(1)} & \mathbf{0} \\ & \ddots \\ \mathbf{0} & C_j^{(t)} \end{bmatrix} \begin{bmatrix} x_j^{(1)} \\ \vdots \\ x_j^{(t)} \end{bmatrix}.$$

It is straightforward to see this provides a vector linear solution for the network. ■

Let  $X$  and  $Y$  be collections of discrete random variables over an alphabet  $\mathcal{A}$ , and let  $p_X$  be the probability mass function of  $X$ . We denote the (base  $|\mathcal{A}|$ ) *entropy* of  $X$  as

$$H(X) = - \sum_u p_X(u) \log_{|\mathcal{A}|} p_X(u)$$

and the *conditional entropy* of  $X$  given  $Y$  as  $H(X|Y) = H(X, Y) - H(Y)$ . The proof of Theorem 3.3.6 will make use of Lemmas 3.3.4 and 3.3.5 and the following basic information inequalities:

$$H(X|Y) \leq H(X) \tag{3.4}$$

$$\leq H(X, Y) \tag{3.5}$$

$$\leq H(X) + H(Y). \tag{3.6}$$

**Lemma 3.3.4.** *Let  $X, Y_1, \dots, Y_k$  be collections of discrete random variables. Then*

$$\sum_{i=1}^k H(X, Y_i) \geq (k-1)H(X) + H(X, Y_1, \dots, Y_k).$$

*Proof.*

$$\begin{aligned} \sum_{i=1}^k H(X, Y_i) &= kH(X) + \sum_{i=1}^k H(Y_i|X) \\ &\geq kH(X) + H(Y_1|X) + \sum_{i=2}^k H(Y_i|X, Y_1, \dots, Y_{i-1}) \\ &= (k-1)H(X) + H(X, Y_1, \dots, Y_k) \end{aligned}$$

where the inequality follows from (3.4). ■

**Lemma 3.3.5.** [8, Lemma V.9]: Let  $L : \mathbb{F}^m \rightarrow \mathbb{F}^n$  be a linear map, and let  $x$  be a uniformly distributed random variable on  $\mathbb{F}^m$ . Then  $L(x)$  is uniformly distributed on the range of  $L$ , and the base  $|\mathbb{F}|$  entropy of  $L(x)$  is  $H(L(x)) = \dim(\text{range}(L(x))) \cdot \log |\mathbb{F}|$ .

**Theorem 3.3.6.** For each integer  $k \geq 2$  and each field  $\mathbb{F}$ , the Dim- $k$  Network has an  $n$ -dimensional vector linear solution over  $\mathbb{F}$  if and only if  $k \mid n$ .

*Proof.* Suppose  $k \mid n$ . Then  $n = kt$  for some integer  $t \geq 1$ . By Lemma 3.3.2, the Dim- $k$  Network has a  $k$ -dimensional vector linear solution over  $\mathbb{F}$ , so by taking  $k_1 = \dots = k_t = k$  in Lemma 3.3.3, the Dim- $k$  Network has an  $n = kt$ -dimensional vector linear solution over  $\mathbb{F}$ .

Conversely, suppose that the Dim- $k$  Network has an  $n$ -dimensional vector linear solution over field  $\mathbb{F}$ . Then all messages  $x_i^{(j)}$  and edge symbols  $w_i^{(j)}$  are  $n$ -vectors over  $\mathbb{F}$ . For convenience of notation, let

$$\mathbf{x}_i = x_i^{(1)}, \dots, x_i^{(k)} \quad \text{and} \quad \mathbf{w}_i = w_i^{(1)}, \dots, w_i^{(k-1)}.$$

A linear solution must hold for any values the messages take on, so by viewing the message components as independent uniform random variables over  $\mathbb{F}$  and considering the entropy using logarithms base  $|\mathbb{F}|$ , we have

$$H(\mathbf{x}_1, \dots, \mathbf{x}_k) = \sum_{i,j=1}^k H(x_i^{(j)}). \quad (3.7)$$

For each  $i = 1, \dots, k$ , the edge symbols  $w_i^{(1)}, \dots, w_i^{(k-1)}$  are linear functions of  $x_i^{(1)}, \dots, x_i^{(k)}$ , so

$$H(\mathbf{w}_i | \mathbf{x}_i) = 0. \quad (3.8)$$

The receiver  $R_1$  demands the messages  $x_1^{(1)}, \dots, x_k^{(1)}$  and recovers its demands from its inputs, so

$$H(x_1^{(1)}, \dots, x_k^{(1)} | \mathbf{w}_1, \dots, \mathbf{w}_k, u_1) = 0. \quad (3.9)$$

For each  $i, j \in \{1, \dots, k\}$ , the edge symbol  $w_i^{(j)}$  is a linear function of only  $x_i^{(1)}, \dots, x_i^{(k)}$ , and the network's

messages are jointly independent, which implies

$$\begin{aligned}
\sum_{i=1}^k H(\mathbf{w}_i, x_i^{(1)}) &= H(x_1^{(1)}, \dots, x_k^{(1)}, \mathbf{w}_1, \dots, \mathbf{w}_k) && \text{[from ind.]} \\
&\leq H(u_1, x_1^{(1)}, \dots, x_k^{(1)}, \mathbf{w}_1, \dots, \mathbf{w}_k) && \text{[from (3.5)]} \\
&= H(u_1, \mathbf{w}_1, \dots, \mathbf{w}_k) && \text{[from (3.9)]} \\
&\leq H(u_1) + \sum_{i=1}^k \sum_{j=1}^{k-1} H(w_i^{(j)}) && \text{[from (3.6)]} \\
&\leq n(1 + k(k-1)).
\end{aligned}$$

By a similar argument, for any  $i_1, \dots, i_k \in \{1, \dots, k\}$ , there exists a receiver which demands the messages  $x_1^{(i_1)}, \dots, x_k^{(i_k)}$ , so

$$\sum_{j=1}^k H(\mathbf{w}_j, x_j^{(i_j)}) \leq n(k^2 - k + 1). \quad (3.10)$$

Since  $\{\mathbf{w}_1, w_1^{(k)}, \dots, \mathbf{w}_k, w_k^{(k)}\}$  is a cut-set for each receiver, we have

$$H(\mathbf{x}_1, \dots, \mathbf{x}_k | \mathbf{w}_1, w_1^{(k)}, \dots, \mathbf{w}_k, w_k^{(k)}) = 0. \quad (3.11)$$

Therefore,

$$\begin{aligned}
nk^2 &= H(\mathbf{x}_1, \dots, \mathbf{x}_k) && \text{[from (3.7)]} \\
&\leq H(\mathbf{x}_1, \dots, \mathbf{x}_k, \mathbf{w}_1, w_1^{(k)}, \dots, \mathbf{w}_k, w_k^{(k)}) && \text{[from (3.5)]} \\
&= H(\mathbf{w}_1, w_1^{(k)}, \dots, \mathbf{w}_k, w_k^{(k)}) && \text{[from (3.11)]} \\
&\leq \sum_{i=1}^k \sum_{j=1}^k H(w_i^{(j)}) && \text{[from (3.6)]} \\
&\leq nk^2 && (3.12)
\end{aligned}$$

which implies

$$\sum_{i=1}^k \sum_{j=1}^k H(w_i^{(j)}) = nk^2.$$

But, since  $H(w_i^{(j)}) \leq n$ , we get

$$H(w_i^{(j)}) = n \quad (i, j = 1, \dots, k).$$

This implies the bounds in (3.12) are tight, so

$$H\left(w_1^{(1)}, \dots, w_1^{(k)}, \dots, w_k^{(1)}, \dots, w_k^{(k)}\right) = \sum_{i=1}^k \sum_{j=1}^k H\left(w_i^{(j)}\right)$$

which implies  $w_1^{(1)}, \dots, w_1^{(k)}, \dots, w_k^{(1)}, \dots, w_k^{(k)}$  are independent. Thus,

$$H(\mathbf{w}_i) = n(k-1) \quad (i = 1, \dots, k). \quad (3.13)$$

For each  $j = 1, \dots, k$ , we have

$$\begin{aligned} \sum_{i=1}^k H\left(\mathbf{w}_j, x_j^{(i)}\right) &\geq (k-1)H(\mathbf{w}_j) + H(\mathbf{w}_j, \mathbf{x}_j) && \text{[from Lemma 3.3.4]} \\ &= n(k-1)(k-1) + H(\mathbf{x}_j) && \text{[from (3.8), (3.13)]} \\ &= n(k^2 - k + 1) && \text{[from (3.7)].} \end{aligned} \quad (3.14)$$

By fixing  $i_1 = 1$  and summing over all  $i_2, \dots, i_k$  in (3.10), we have

$$\begin{aligned} k^{k-1} n(k^2 - k + 1) &\stackrel{(a)}{\geq} \sum_{i_2, \dots, i_k=1}^k \left( H\left(\mathbf{w}_1, x_1^{(1)}\right) + \sum_{j=2}^k H\left(\mathbf{w}_j, x_j^{(i_j)}\right) \right) \\ &= k^{k-1} H\left(\mathbf{w}_1, x_1^{(1)}\right) + k^{k-2} \sum_{j=2}^k \sum_{i=1}^k H\left(\mathbf{w}_j, x_j^{(i)}\right) \\ &\stackrel{(b)}{\geq} k^{k-1} H\left(\mathbf{w}_1, x_1^{(1)}\right) + k^{k-2} \sum_{j=2}^k n(k^2 - k + 1) \\ &= k^{k-1} H\left(\mathbf{w}_1, x_1^{(1)}\right) + k^{k-2} n(k-1)(k^2 - k + 1) \end{aligned}$$

where (a) and (b) follow from (3.10) and (3.14), respectively. Solving for  $H(\mathbf{w}_1, x_1^{(1)})$  in the previous equation yields

$$H\left(\mathbf{w}_1, x_1^{(1)}\right) \leq n \left( \frac{k^2 - k + 1}{k} \right).$$

Similarly, for each  $i, j = 1, \dots, k$ , we have

$$H\left(\mathbf{w}_i, x_i^{(j)}\right) \leq n \left( \frac{k^2 - k + 1}{k} \right). \quad (3.15)$$

However, for each  $i = 1, \dots, k$  we also have

$$\begin{aligned} n(k^2 - k + 1) &\leq \sum_{j=1}^k H\left(\mathbf{w}_i, x_i^{(j)}\right) && \text{[from (3.14)]} \\ &\leq \sum_{j=1}^k n \left( \frac{k^2 - k + 1}{k} \right) && \text{[from (3.15)]} \\ &= n(k^2 - k + 1) \end{aligned}$$

and so for each  $i, j = 1, \dots, k$ ,

$$H(\mathbf{w}_i, x_i^{(j)}) = n \left( \frac{k^2 - k + 1}{k} \right).$$

The variables  $w_i^{(1)}, \dots, w_i^{(k-1)}, x_i^{(j)}$  are linear functions of the uniformly distributed messages, so by Lemma 3.3.5,  $H(\mathbf{w}_i, x_i^{(j)})$  (with logarithms in base  $|\mathbb{F}|$ ) is an integer. However,

$$\gcd(k, k^2 - k + 1) = \gcd(k, (k^2 - k + 1) - k(k - 1)) = \gcd(k, 1) = 1$$

so if  $n \left( \frac{k^2 - k + 1}{k} \right)$  is an integer, then we must have  $k \mid n$ . ■

### 3.3.1 Insufficiency of Commutative Rings

The following corollary demonstrates it is possible for a network to be scalar linearly solvable over a non-commutative ring but not over any commutative rings, which is, in fact, equivalent to a network being vector linearly solvable over some field but not scalar linearly solvable over any field, by Corollaries 3.2.14 and 3.2.15. This fact agrees with the result of Médard et. al [15], which demonstrate the  $M$  Network is vector linearly solvable over fields but not scalar linearly solvable over any field.

**Corollary 3.3.7.** *For all integers  $k \geq 2$ ,  $n \geq 1$ , and prime  $p$ , the Dim- $k$  Network has a scalar linear solution over a ring of size  $p^{nk^2}$  but has no scalar linear solution over any commutative ring.*

*Proof.* If the Dim- $k$  Network were scalar linearly solvable over a commutative ring, then Corollary 3.2.15 would imply the Dim- $k$  Network would also be scalar linearly solvable over some finite field. However, by Theorem 3.3.6, the Dim- $k$  Network is not scalar linearly solvable over any finite field.

By Theorem 3.3.6, the Dim- $k$  Network has a  $k$ -dimensional vector linear solution over  $\text{GF}(p^n)$ , so by Corollary 3.1.5 the Dim- $k$  Network has a linear solution over the ring  $M_k(\text{GF}(p^n))$ . ■

**Corollary 3.3.8.** *For each integer  $k \geq 2$ , the unique smallest-size ring over which the Dim- $k$  Network is scalar linearly solvable is the ring of all  $k \times k$  matrices over  $\text{GF}(2)$ .*

*Proof.* By taking  $p = 2$  in Corollary 3.3.7, the Dim- $k$  Network has a linear solution over  $M_k(\text{GF}(2))$ .

Suppose the Dim- $k$  Network is scalar linearly solvable over a ring  $R$  such that  $|R| \leq 2^{k^2}$ . By Lemmas 3.2.1 and 3.2.3 (a) (b) there exists a field  $\mathbb{F}$ , a positive integer  $n$ , and a surjective homomorphism

$\phi : R \rightarrow M_n(\mathbb{F})$  such that the Dim- $k$  Network is scalar linearly solvable over  $M_n(\mathbb{F})$ . By Corollary 3.1.5, this implies the Dim- $k$  Network has an  $n$ -dimensional vector linear solution over  $\mathbb{F}$ , which by Theorem 3.3.6, implies  $k$  divides  $n$ . Since  $\phi$  is surjective,  $|M_n(\mathbb{F})| \leq |R|$ . Hence we have

$$2^{k^2} \leq 2^{n^2} \leq |\mathbb{F}|^{n^2} = |M_n(\mathbb{F})| \leq |R| \leq 2^{k^2}.$$

Therefore  $n = k$  and  $\mathbb{F} = \text{GF}(2)$ . Since  $|R| = |M_n(\mathbb{F})|$  and  $\phi$  is a surjective homomorphism, we have  $R \cong M_k(\text{GF}(2))$ . ■

It is interesting to note that, while the smallest-size ring over which the Dim- $k$  Network is scalar linearly solvable has size  $2^{k^2}$ , the Dim- $k$  Network also has a  $k$ -dimensional vector linear solution over  $\text{GF}(2)$ , which has alphabet size  $2^k$ . This demonstrates that linear codes over modules can require smaller alphabet sizes than scalar linear codes over rings. This also agrees with Theorem 3.2.10, which showed that vector linear codes over fields minimize the alphabet size needed for a linear solution.

**Example 3.3.9.** Setting  $n = 1$  and  $p = k = 2$  in Corollary 3.3.7 results in the  $M$  Network (see Figure 3.4) having no scalar linear solution over any commutative ring but having a scalar linear solution over a non-commutative ring of size 16. The non-commutative ring  $M_2(\text{GF}(2))$  consists of all  $2 \times 2$  binary matrices under ordinary matrix addition and multiplication mod 2. Denote the 16 ring elements by:

$$R_{qrst} = \begin{bmatrix} q & r \\ s & t \end{bmatrix} \quad (q, r, s, t \in \{0, 1\}).$$

A scalar linear solution for the  $M$  Network over the non-commutative ring  $M_2(\text{GF}(2))$

(i.e. where  $A, B, C, D, E, F, G, H, W, X, Y, Z \in M_2(\text{GF}(2))$ ) is given by:

|  |  |
|--|--|
| Edge (1,3) : $A = R_{1000}W + R_{0010}X$ | Decode at node 6 : $W = R_{1000}A + R_{0010}E + R_{0000}D$ |
| Edge (1,4) : $B = R_{0100}W + R_{0001}X$ | $Y = R_{0000}A + R_{0001}E + R_{1000}D$                    |
| Edge (2,4) : $C = R_{0100}Y + R_{0001}Z$ | Decode at node 7 : $W = R_{1000}A + R_{0010}F + R_{0000}D$ |
| Edge (2,5) : $D = R_{1000}Y + R_{0010}Z$ | $Z = R_{0000}A + R_{0001}F + R_{0100}D$                    |
| Edge (4,6) : $E = R_{1000}B + R_{0010}C$ | Decode at node 8 : $X = R_{0100}A + R_{0010}G + R_{0000}D$ |
| Edge (4,7) : $F = R_{1000}B + R_{0001}C$ | $Y = R_{0000}A + R_{0001}G + R_{1000}D$                    |
| Edge (4,8) : $G = R_{0100}B + R_{0010}C$ | Decode at node 9 : $X = R_{0100}A + R_{0010}H + R_{0000}D$ |
| Edge (4,9) : $H = R_{0100}B + R_{0001}C$ | $Z = R_{0000}A + R_{0001}H + R_{0100}D,$                   |



where the out-edges of nodes with a single in-edge each carry the symbol on the in-edge, that is, each receiver directly receives the edge symbols  $A$  and  $D$  from the nodes 3 and 5, respectively.

We also note that if the messages and edge symbols of the  $M$  Network are 2-dimensional vectors over  $\text{GF}(2)$ , instead of  $2 \times 2$  binary matrices, then a small modification of the linear code described above provides the 2-dimensional vector linear solution over  $\text{GF}(2)$  given in [15]. This agrees with Corollary 3.1.5.

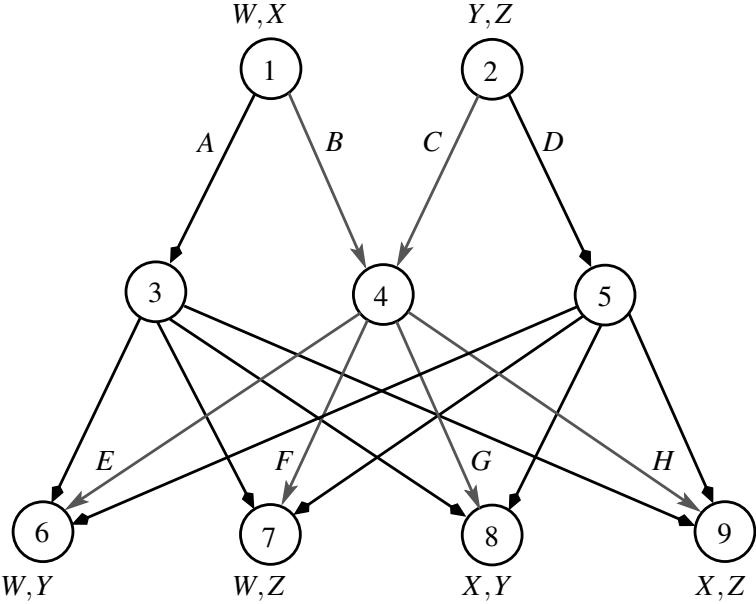


Figure 3.4: The  $M$  Network has a non-commutative scalar linear solution. The messages  $W, X, Y, Z$  take values in  $M_2(\text{GF}(2))$ . The variables  $A, B, C, D, E, F, G, H$  also take values in  $M_2(\text{GF}(2))$  and represent the symbols carried on the 8 indicated edges.

The bound in the following theorem is tight via Example 3.3.9.

**Theorem 3.3.10.** *If a network is scalar linearly solvable over some non-commutative ring  $R$ , but not over any commutative rings, then  $|R| \geq 16$ .*

*Proof.* Suppose network  $\mathcal{N}$  is scalar linearly solvable over some non-commutative ring  $R$  but not over any commutative ring. By Theorem 3.2.5, there exists a positive integer  $k$  and a field  $\mathbb{F}$  such that  $\mathcal{N}$  has a scalar linear solution over  $M_k(\mathbb{F})$  and  $|R| \geq |M_k(\mathbb{F})|$ . If  $k = 1$ , then  $\mathcal{N}$  is scalar linearly solvable over a field, which contradicts the assumption that  $\mathcal{N}$  is not scalar linearly solvable over any commutative ring. So  $k \geq 2$ , which implies  $|R| \geq |M_k(\mathbb{F})| = |\mathbb{F}|^{k^2} \geq |\mathbb{F}|^4 \geq 2^4 = 16$ . ■

Suppose  $R$  is a non-commutative ring of size  $p^n$ , for some prime  $p$ . It also follows from the proof of Theorem 3.3.10 that if a network  $\mathcal{N}$  is scalar linearly solvable over  $R$ , but not over any commutative ring, then  $n \geq 4$ . In fact, we later show in (Theorem 3.4.15) that whenever  $n \leq 3$ , any network with a scalar linear solution over some ring of size  $p^n$  must also have a scalar linear solution over the field  $\text{GF}(p^n)$ , which agrees with Theorem 3.3.10.

### 3.4 Modules of the Same Size

In Chapter 2, we compared the linear solvability of networks over different commutative rings of the same size, and we showed that in some cases, commutative rings of size  $p^k$  can attain scalar linear solutions when the field of size  $p^k$  cannot. In this section, we compare the linear solvability of networks over different modules of the same size. We particularly focus on comparing scalar linear codes over rings of size  $p^k$  and  $k$ -dimensional vector linear codes over  $\text{GF}(p)$ . The following theorem shows that a network can have a linear solution over a module with alphabet size  $p^k$  yet have no scalar linear solutions over any ring of size  $p^k$

**Theorem 3.4.1.** *For each integer  $k \geq 2$  and prime  $p$ , the Dim- $k$  Network has a  $k$ -dimensional vector linear solution over the field  $\text{GF}(p)$  but is not scalar linearly solvable over any ring of size  $p^k$ .*

*Proof.* By Theorem 3.3.6, the Dim- $k$  Network has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ . Let  $R$  be a ring of size  $p^k$  and suppose the Dim- $k$  Network has a scalar linear solution over  $R$ . By Lemmas 3.2.1 and 3.2.3 (b) (c), there exists a field  $\mathbb{F}$  and a positive integer  $n$  such that any network that is scalar linearly solvable over  $R$  is also scalar linearly solvable over  $M_n(\mathbb{F})$  and  $|\mathbb{F}|^{n^2}$  divides  $p^k$ . Hence  $\mathbb{F}$  is a field of characteristic  $p$  and  $n^2 \leq k$ .

Since the Dim- $k$  Network is scalar linearly solvable over  $R$ , the Dim- $k$  Network is scalar linearly solvable over the ring  $M_n(\mathbb{F})$ . By Corollary 3.1.5, this implies the Dim- $k$  Network has an  $n$ -dimensional vector linear solution over  $\mathbb{F}$ , which by Theorem 3.3.6 implies  $k \mid n$ . However, this contradicts the fact that  $n^2 \leq k$ . Thus, no such ring  $R$  exists. ■

While the Dim- $k$  Network is a non-multicast network, we note that a similar result can occur for multicast networks as well. The following result was shown by Sun et. al [17].

**Lemma 3.4.2.** [17, Theorem 4 and Corollary 11]: For each integer  $k \geq 2$  and prime  $p$ , there exists a multicast network with

- (a) a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ ,
- (b) no scalar linear solutions over any  $\text{GF}(q)$  with  $q \leq p^k$ , and
- (c) no  $n$ -dimensional vector linear solutions over any  $\text{GF}(q)$  with  $q^n < p^k$ .

We thank an anonymous reviewer for a helpful suggestion, which led to the following corollary.

**Corollary 3.4.3.** For each integer  $k \geq 2$  and prime  $p$ , there exists a multicast network that has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$  but is not scalar linearly solvable over any ring of size  $p^k$ .

*Proof.* Let  $\mathcal{N}$  denote the network constructed by Sun et. al [17] in Lemma 3.4.2 corresponding to  $p$  and  $k$ . Such a network has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ .

Since  $\mathcal{N}$  is vector linearly solvable, by Corollary 3.2.14, it must be scalar linearly solvable over some ring. Now suppose  $R$  is a minimum-size ring over which  $\mathcal{N}$  is scalar linearly solvable. By Theorem 3.2.5, there exists a prime-power  $q$  and an integer  $n$  such that  $R \cong M_n(\text{GF}(q))$ . By Corollary 3.1.5,  $\mathcal{N}$  has an  $n$ -dimensional vector linear solution over  $\text{GF}(q)$ , but by Lemma 3.4.2 (c), this implies  $q^n \geq p^k$ . If  $n \geq 2$ , then  $|R| = q^{n^2} > q^n \geq p^k$ . If  $n = 1$ , then  $\mathcal{N}$  has a scalar linear solution over  $\text{GF}(q)$ , which, by Lemma 3.4.2 (b), implies  $p^k < q = |R|$ . Thus the minimum size ring over which  $\mathcal{N}$  is scalar linearly solvable has cardinality greater than  $p^k$ , so in particular,  $\mathcal{N}$  is not scalar linearly solvable over any ring of size  $p^k$ . ■

### 3.4.1 Commutative Rings

Both a scalar linear code over a ring of size  $p^k$  and a  $k$ -dimensional vector linear code are linear codes over a module of size  $p^k$ . We have already seen (in Theorem 3.4.1) that there exists a network with a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$  yet with no scalar linear solutions over any ring of size  $p^k$ . The main result of this section (Theorem 3.4.6) will show that any network that is scalar linearly solvable over a commutative ring of size  $p^k$  must also have a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ . The following lemma was proved in Chapter 2 (in Lemmas 2.2.12 and 2.5.3) and will be used in what follows.

**Lemma 3.4.4.** For each prime  $p$  and positive integer  $k$ , if a network  $\mathcal{N}$  has a scalar linear solution over some commutative ring of size  $p^k$ , then there exists an integer partition  $(n_1, \dots, n_r)$  of  $k$  such that  $\mathcal{N}$  is scalar linearly solvable over each of the fields  $\text{GF}(p^{n_1}), \dots, \text{GF}(p^{n_r})$ .

**Lemma 3.4.5.** [14, Theorem I.1]: Every finite ring is isomorphic to a direct product of rings of prime power sizes.

**Theorem 3.4.6.** Let  $m$  be a positive integer with prime factorization  $m = p_1^{k_1} \cdots p_t^{k_t}$ . If a network  $\mathcal{N}$  has a scalar linear solution over some commutative ring of size  $m$ , then the following hold:

- (a) For each  $i = 1, \dots, t$ , network  $\mathcal{N}$  has a  $k_i$ -dimensional vector linear solution over  $\text{GF}(p_i)$ .
- (b) Network  $\mathcal{N}$  has a linear solution over the  $M_{k_1}(\text{GF}(p_1)) \times \cdots \times M_{k_t}(\text{GF}(p_t))$ -module  $\text{GF}(p_1)^{k_1} \times \cdots \times \text{GF}(p_t)^{k_t}$ .

*Proof.* Suppose  $\mathcal{N}$  is scalar linearly solvable over a commutative ring  $R$  of size  $m$ . By Lemma 3.4.5, there exist rings  $R_1, \dots, R_t$  such that  $R \cong R_1 \times \cdots \times R_t$  and  $|R_i| = p_i^{k_i}$  for all  $i$ .

Let  $i \in \{1, \dots, t\}$ . Since the projection mapping from  $R$  to  $R_i$  is a surjective homomorphism, by Corollary 3.1.7, network  $\mathcal{N}$  is scalar linearly solvable over  $R_i$ . Then by Lemma 3.4.4, there exists an integer partition  $(n_1, \dots, n_r)$  of  $k_i$  such that  $\mathcal{N}$  is scalar linearly solvable over each of the fields  $\text{GF}(p_i^{n_1}), \dots, \text{GF}(p_i^{n_r})$ . By Lemma 3.2.11, this implies that  $\mathcal{N}$  has an  $n_j$ -dimensional vector linear solution over  $\text{GF}(p_i)$  for each  $j = 1, \dots, r$ . However, by Lemma 3.3.3, this then implies that  $\mathcal{N}$  has a  $k_i = (n_1 + \cdots + n_r)$ -dimensional vector linear solution over  $\text{GF}(p_i)$ .

Hence, for all  $i \in \{1, \dots, t\}$ , a Cartesian product code formed from the  $k_i$ -dimensional vector linear solutions over  $\text{GF}(p_i)$  gives a linear solution to  $\mathcal{N}$  over the described module. ■

In Chapter 2, we showed (in Theorems 2.5.8 and 2.5.9) that with respect to ring domination for scalar linear coding, some ring sizes give rise to multiple maximal commutative rings whereas other ring sizes yield only a single unique maximal commutative ring. If there is just one maximal commutative ring of size  $m$ , then every network that is linearly solvable over some commutative ring of size  $m$  is also linearly solvable over the maximal ring. In contrast, if there are multiple maximal commutative rings of size  $m$ , then for any commutative ring  $R$  of size  $m$ , there is always a different commutative ring  $S$  also of size  $m$ , such that some network is scalar linearly solvable over  $S$  but not over  $R$ . Thus, in this sense, there is no “best” commutative ring of a given size.

However, by Theorem 3.4.6 (b), if a network has a linear solution over some commutative ring of size  $m = p_1^{k_1} \cdots p_t^{k_t}$ , then it has a linear solution over the  $M_{k_1}(\text{GF}(p_1)) \times \cdots \times M_{k_t}(\text{GF}(p_t))$ -module  $\text{GF}(p_1)^{k_1} \times \cdots \times \text{GF}(p_t)^{k_t}$ , which also has size  $m$ . In fact, we showed (in Theorem 3.4.1) that when  $m = p^k$ , the converse is not true. So in this sense,  $k$ -dimensional vector linear codes over  $\text{GF}(p)$  are strictly “better” than scalar linear codes over commutative rings of size  $p^k$ .

### 3.4.2 Non-Commutative Rings

This section generalizes the results of Theorem 3.4.6 to (not necessarily commutative) rings of size  $m$  with prime factor multiplicity less than or equal to 6. In order to do so, we first will prove some intermediate results and consider special cases.

The following lemma was proved in Chapter 2 (in Theorem 2.5.9) and will be used in what follows.

**Lemma 3.4.7.** *For each  $k \in \{1, 2, 3, 4, 6\}$  and prime  $p$ , if a network is scalar linearly solvable over some commutative ring of size  $p^k$ , then it is scalar linearly solvable over  $\text{GF}(p^k)$ .*

**Lemma 3.4.8.** [11, pp. 512–513]: *For each prime  $p$ , all rings of size  $p$  and of size  $p^2$  are commutative, and the ring of all upper-triangular  $2 \times 2$  matrices over  $\text{GF}(p)$  is the only non-commutative ring of size  $p^3$ .*

We remark that there exist rings of size  $p$  and  $p^2$  without identity. For example, the set  $\{0, 2, 4, 6\}$  with mod 8 addition and multiplication satisfies all of the properties of a ring except there is no multiplicative identity. However, such rings (sometimes called “rngs”) do not appear to be practical for linear network coding, as receivers must recover their demands from linear combinations of their inputs.

For example, consider the trivial network shown in Figure 3.5 consisting of a single message  $x$  emitted by a source directly connected by a single edge to a receiver demanding message  $x$ . The only possible linear functions that can be carried on the edge are of the form  $cx$  for some fixed  $c \in \{0, 2, 4, 6\}$ . However, no matter what the choice of  $c$  is, the messages 0 and 4 always get received as  $0 \pmod 8$ , so the receiver cannot uniquely determine  $x$  in general. Thus, there is no linear solution for the network over this ring (with no multiplicative identity). A similar issue arises for the set  $\{0, 2\}$  with mod 4 addition and multiplication, which also satisfies all of the properties of a ring except there is no multiplicative identity.

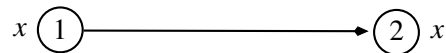


Figure 3.5: A trivial network with one message  $x$  that is demanded by the receiver.

**Lemma 3.4.9.** *For each prime  $p$ , if a network is scalar linearly solvable over some ring of size  $p^2$ , then it is a scalar linearly solvable over  $\text{GF}(p^2)$ .*

*Proof.* By Lemma 3.4.8, every ring of size  $p^2$  is commutative, and by Lemma 3.4.7, every network that is scalar linearly solvable over some commutative ring of size  $p^2$  has a scalar linear solution over  $\text{GF}(p^2)$ . ■

By Lemma 3.4.8, all rings of size 2, 3, 4, 5, or 7 are commutative, and by Lemma 3.4.5, any ring of size 6 is a direct product of rings of size 2 and 3, so any ring of size 6 must also be commutative. Hence, the smallest non-commutative ring is the ring of the 8 binary upper-triangular  $2 \times 2$  matrices. As a special case of the following lemma, any network that is scalar linearly solvable over this ring must also have a scalar linear solution over  $\text{GF}(2)$ .

**Lemma 3.4.10.** *For each finite field  $\mathbb{F}$  and integer  $k \geq 2$ , any network that is scalar linearly solvable over the ring of upper-triangular  $k \times k$  matrices over  $\mathbb{F}$  is also scalar linearly solvable over  $\mathbb{F}$ .*

*Proof.* Let  $R$  be the ring of upper-triangular  $k \times k$  matrices with entries in  $\mathbb{F}$  and let  $\phi : R \rightarrow \mathbb{F}$  be given by

$$\phi \left( \begin{bmatrix} a_{1,1} & \cdots & a_{1,k} \\ & \ddots & \vdots \\ \mathbf{0} & & a_{k,k} \end{bmatrix} \right) = a_{1,1}.$$

Then  $\phi$  is clearly surjective and preserves identities, and for any  $A, B \in R$ , we have  $\phi(A+B) = a_{1,1} + b_{1,1} = \phi(A) + \phi(B)$  and  $\phi(AB) = a_{1,1} b_{1,1} = \phi(A)\phi(B)$ . Thus  $\phi$  is a surjective homomorphism, so by Corollary 3.1.7, any network that is scalar linearly solvable over  $R$  is scalar linearly solvable over  $\mathbb{F}$ . ■

**Lemma 3.4.11.** *For each prime  $p$ , if a network is scalar linearly solvable over some ring of size  $p^3$ , then it is scalar linearly solvable over  $\text{GF}(p^3)$ .*

*Proof.* By Lemma 3.4.8, the only non-commutative ring of size  $p^3$  is the ring of upper triangular matrices with entries in  $\text{GF}(p)$ , and by Lemma 3.4.10, any network that is scalar linearly solvable over this ring is also scalar linearly solvable over  $\text{GF}(p)$ . Since  $\text{GF}(p)$  is a subring of  $\text{GF}(p^3)$ , any network that is scalar linearly solvable over  $\text{GF}(p)$  is scalar linearly solvable over  $\text{GF}(p^3)$ .

By Lemma 3.4.7, every network that is scalar linearly solvable over some commutative ring of size  $p^3$  has a scalar linear solution over  $\text{GF}(p^3)$ . ■

The following three lemmas are proved in the Appendix.

**Lemma 3.4.12.** *For each prime  $p$ , if a network is scalar linearly solvable over some ring of size  $p^4$ , then it is scalar linearly solvable over at least one of the rings  $\text{GF}(p^4)$  or  $M_2(\text{GF}(p))$ .*

**Lemma 3.4.13.** *For each prime  $p$ , if a network is scalar linearly solvable over some ring of size  $p^5$ , then it is scalar linearly solvable over at least one of the commutative rings  $\text{GF}(p^5)$  or  $\text{GF}(p^3) \times \text{GF}(p^2)$ .*

**Lemma 3.4.14.** *For each prime  $p$ , if a network is scalar linearly solvable over some ring of size  $p^6$ , then it is scalar linearly solvable over  $\text{GF}(p^6)$ .*

Theorem 3.4.15 is a generalization of Lemma 3.4.7 to scalar linear codes over non-commutative rings. Extending Theorem 3.4.15 to  $|R| = p^k$  for  $k \geq 7$  is left as an open problem.

**Theorem 3.4.15.** *Let  $p$  be a prime, and suppose  $\mathcal{N}$  is scalar linearly solvable over a ring  $R$ . Then  $\mathcal{N}$  is scalar linearly solvable over*

- (a) *the field  $\text{GF}(p^2)$ , when  $|R| = p^2$ .*
- (b) *the field  $\text{GF}(p^3)$ , when  $|R| = p^3$ .*
- (c) *at least one of the rings  $\text{GF}(p^4)$  or  $M_2(\text{GF}(p))$ , when  $|R| = p^4$ .*
- (d) *at least one of the commutative rings  $\text{GF}(p^5)$  or  $\text{GF}(p^3) \times \text{GF}(p^2)$ , when  $|R| = p^5$ .*
- (e) *the field  $\text{GF}(p^6)$ , when  $|R| = p^6$ .*

*Proof.* This follows immediately from Lemmas 3.4.9 and 3.4.11–3.4.14. ■

We also note that by Corollary 3.2.13, the  $(p^4 + 1)$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p^4)$  but not over  $M_2(\text{GF}(p))$ , and the  $(p^5 + 1)$ -Choose-Two Network is scalar linearly solvable over  $\text{GF}(p^5)$  but not over  $\text{GF}(p^3) \times \text{GF}(p^2)$ . By Corollary 3.3.7, the Dim-2 Network is scalar linearly solvable over  $M_2(\text{GF}(p))$  but not over  $\text{GF}(p^4)$ . We showed in Theorem 2.3.8 of Chapter 2 that there exists a network that is scalar linearly solvable over  $\text{GF}(p^3) \times \text{GF}(p^2)$  but not over  $\text{GF}(p^5)$ . Hence it is necessary to include both rings in (c) and (d) in Theorem 3.4.15.

**Corollary 3.4.16.** *Let  $p$  be a prime and  $k \in \{2, 3, 4, 5, 6\}$ , and suppose  $\mathcal{N}$  is scalar linearly solvable over a ring of size  $p^k$ . Then  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ .*

*Proof.* If  $k \in \{2, 3, 5, 6\}$ , then by Theorem 3.4.15,  $\mathcal{N}$  has a scalar linear solution over a commutative ring of size  $p^k$ , since fields and direct products of fields are commutative rings. So, by Theorem 3.4.6,  $\mathcal{N}$  has a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ .

Now suppose  $k = 4$ . If  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^4)$ , then by Lemma 3.2.11,  $\mathcal{N}$  has a 4-dimensional vector linear solution over  $\text{GF}(p)$ . If  $\mathcal{N}$  is not scalar linearly solvable over  $\text{GF}(p^4)$ , then

by Theorem 3.4.15 (c),  $\mathcal{N}$  must be scalar linearly solvable over  $M_2(\text{GF}(p))$ , so by Corollary 3.1.5,  $\mathcal{N}$  has a 2-dimensional vector linear solution over  $\text{GF}(p)$ , in which case  $\mathcal{N}$  also has a 4-dimensional vector linear solution over  $\text{GF}(p)$  by Lemma 3.3.3. ■

**Theorem 3.4.17.** *Let  $m$  be a positive integer with prime factorization  $m = p_1^{k_1} \cdots p_t^{k_t}$ . If a network  $\mathcal{N}$  has a scalar linear solution over a ring of size  $m$ , then, for each  $i = 1, \dots, t$  such that  $k_i \leq 6$ , network  $\mathcal{N}$  has a  $k_i$ -dimensional vector linear solution over  $\text{GF}(p_i)$ .*

*Proof.* Suppose  $\mathcal{N}$  is scalar linearly solvable over a ring  $R$  of size  $m$ . By Lemma 3.4.5, there exists rings  $R_1, \dots, R_t$  such that  $R \cong R_1 \times \cdots \times R_t$  and  $|R_i| = p_i^{k_i}$  for all  $i$ .

Now, let  $i \in \{1, \dots, t\}$  and suppose  $k_i \leq 6$ . The projection mapping from  $R$  to  $R_i$  is a surjective homomorphism, so by Corollary 3.1.7, network  $\mathcal{N}$  is scalar linearly solvable over  $R_i$ . Since  $\mathcal{N}$  is scalar linearly solvable over a ring of size  $p_i^{k_i}$  where  $k_i \leq 6$ , by Corollary 3.4.16,  $\mathcal{N}$  has a  $k_i$ -dimensional vector linear solution over  $\text{GF}(p_i)$ . ■

We leave as an open question whether the restriction that  $k_i \leq 6$  can be removed from the statement of Theorem 3.4.17. If this generalization is false, then for what primes  $p$  and positive integers  $k$  is the case that there exists a network with a scalar linear solution over a ring of size  $p^k$  but with no  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ ? If such a ring and such a network do exist, the ring must be non-commutative and  $k \geq 7$ .

### 3.5 Concluding Remarks

For each positive integer  $k$  and prime  $p$ , we have shown that the set of networks with scalar linear solutions over commutative rings of size  $p^k$  is properly contained in the set of networks with  $k$ -dimensional vector linear solutions over  $\text{GF}(p)$ . So in this sense,  $k$ -dimensional vector linear codes over  $\text{GF}(p)$  may be advantageous compared to scalar linear codes over commutative rings of the same size  $p^k$ . In addition, there are more  $k$ -dimensional linear functions over  $\text{GF}(p)$  than there over a commutative ring of size  $p^k$ . Vector linear codes over fields are also optimal in the sense that they minimize the alphabet size needed for a linear solution over a particular network. On the other hand, the complexity of implementing vector linear codes is generally higher than for scalar linear codes over commutative rings of the same size.



### 3.5.1 Summary of Results

We summarize our results on minimizing the alphabet size in linear network coding by:

- If a network is scalar linearly solvable over some commutative ring, then the (unique) smallest such commutative ring is a field (Theorem 2.2.10 of Chapter 2).
- If a network is scalar linearly solvable over some ring, then a smallest such ring is a matrix ring over field (Theorem 3.2.5). It is not known whether such a smallest ring is unique.
- If a network is linearly solvable over some module, then a smallest such module yields a vector linear solution over a field (Theorem 3.2.10). Such a module may not be unique (Theorem 3.2.12).

Additionally, we summarize our results on the linear solvability of networks over fields, rings, and modules in Corollaries 3.2.14 and 3.2.15.

We summarize our results on comparing alphabets of the same size by:

- A network can have no scalar linear solutions over a given field yet be scalar linearly solvable over a commutative ring of the same size (Theorem 2.3.8 of Chapter 2). Chapter 2 particularly focuses on commutative rings for which there exists a network that is scalar linearly solvable over the ring but not over any other commutative ring of the same size.
- A network can have no scalar linear solutions over any commutative ring yet be scalar linearly solvable over a non-commutative ring (Corollary 3.3.7). Such a non-commutative ring must have size at least 16 (Theorem 3.3.10), and for the  $M$  Network, this bound is achieved.
- When  $k \leq 6$ , any network with a scalar linear solution over a ring of size  $p^k$  has a  $k$ -dimensional vector linear solutions over  $\text{GF}(p)$  (Corollary 3.4.16). This extends to all positive integers  $k$  when the ring is commutative (Theorem 3.4.6).
- There exists a multicast network (Corollary 3.4.3) and a non-multicast network (Theorem 3.4.1) with  $k$ -dimensional vector linear solutions over  $\text{GF}(p)$  but with no scalar linear solutions over any ring of size  $p^k$ .

### 3.5.2 Open Questions

Some open questions related to linear solvability of networks over finite rings and modules include:

- Does there exist a network with a linear solution over some ring of size  $p^k$  but with no  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ ? We have shown that if such a network and such a ring exist, then the ring is non-commutative and  $k \geq 7$ .
- More generally, does there exist a network with a linear solution over some module of size  $p^k$  but with no  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ ?
- When a network has a scalar linear solution over a ring of a given size, over what other rings does the network have scalar linear solutions? In particular, how does Theorem 3.4.15 extend to rings of size  $p^k$  when  $k \geq 7$ ?
- Does there exist a network that is scalar linearly solvable over at least two rings of a given size but not over any smaller ring? I.e., is the smallest-size ring over which a network scalar linearly solvable unique?
- In Chapter 2, we characterized commutative rings with the property that there exists a network with a scalar linear solution over the ring but no other commutative ring of the same size? Is there a similar characterization when removing the commutative restriction?

### 3.A Proofs of Lemmas 3.4.12, 3.4.13, and 3.4.14

The main purpose of this Appendix is to prove Lemmas 3.4.12, 3.4.13, and 3.4.14, which are used in the proof of Theorem 3.4.15. It is an open question whether Theorem 3.4.17 can be extended to all finite rings. The techniques presented in this section may additionally be useful for examining such questions.

Recall that a finite ring is simple if it has no proper two-sided ideals. The *radical* of a ring  $R$  is the intersection of all its maximal left ideals. The radical of a ring is a two-sided ideal. A finite ring  $R$  with radical  $J$  is said to be:

- *local*<sup>4</sup> if  $R/J$  is a field.
- *semi-local* if  $R/J$  is simple, or equivalently  $R$  is isomorphic to a matrix ring over some local ring (e.g. [14, p. 162]).
- *semi-simple* if  $R$  is isomorphic to a direct product of simple rings (matrix rings over fields) or equivalently,  $J = \{0\}$  (e.g. [14, pp. 75, 128]).

The following lemma is a result on local rings that will be used in later proofs.

**Lemma 3.A.1.** *Let  $p$  be a prime,  $k$  a positive integer, and  $R$  a semi-local ring of size  $p^k$ . Then there exists a unique local ring  $S$  and positive integers  $r, s, t$  such that the following hold:*

- (a) [14, Theorem VIII.26]  $R \cong M_r(S)$
- (b) [1, Theorem 6.1.2]  $|S| = p^s$
- (c) [1, Theorem 6.1.2]  $\text{GF}(p^t) \cong S/J$ , where  $J$  is the radical of  $S$  and  $t \mid s$ .

As an example, let  $p$  be a prime and let  $r, s$  be positive integers. Then  $M_r(\mathbb{Z}_{p^s})$  is a semi-local ring, since  $\mathbb{Z}_{p^s}$  is a local ring. We also remark that in Lemma 3.A.1, if  $R$  is itself local, then  $S \cong R$ .

The following lemmas are results on semi-simple rings and the radicals of rings.

**Lemma 3.A.2.** [14, Proposition IV.6, Theorem VIII.4]: *Let  $R$  be a finite ring with radical  $J$ . Then there exist fields  $\mathbb{F}_1, \dots, \mathbb{F}_s$  and positive integers  $r_1, \dots, r_s$  such that  $R/J \cong M_{r_1}(\mathbb{F}_1) \times \dots \times M_{r_s}(\mathbb{F}_s)$ .*

**Lemma 3.A.3.** *Let  $R$  be a finite ring with radical  $J$ , and suppose*

$$R/J \cong M_{r_1}(\mathbb{F}_1) \times \dots \times M_{r_s}(\mathbb{F}_s)$$

*for some fields  $\mathbb{F}_1, \dots, \mathbb{F}_s$  and positive integers  $r_1, \dots, r_s$ . If a network is scalar linearly solvable over  $R$ , then it is also scalar linearly solvable over each of the rings  $M_{r_1}(\mathbb{F}_1), \dots, M_{r_s}(\mathbb{F}_s)$ .*

---

<sup>4</sup>If  $R$  is a local commutative ring, then  $R$  has a single maximal ideal, which corresponds to our definition of a commutative local ring in Chapter 2.

*Proof.* By Lemma 3.2.2, there exists a surjective homomorphism  $\phi : R \rightarrow R/J$ . Let  $i \in \{1, \dots, s\}$ . Then the projection mapping  $\psi_i : R/J \rightarrow M_{r_i}(\mathbb{F}_i)$  is a surjective homomorphism. Hence the composition of mappings  $\psi_i \circ \phi : R \rightarrow M_{r_i}(\mathbb{F}_i)$  is a surjective homomorphism. Thus by Corollary 3.1.7, any network with a scalar linear solution over  $R$  has a scalar linear solution over the ring  $M_{r_i}(\mathbb{F}_i)$ . ■

The following is an enumeration of semi-simple rings that we will reference in upcoming proofs. Semi-simple rings are direct products of rings of matrices over fields. There are a limited number of small-size matrix rings over fields, so the semi-simple rings of small sizes can be easily enumerated. For each prime  $p$ , it can be verified that the rings given in (3.16)–(3.48) are all of the semi-simple rings of sizes  $p, p^2, p^3, p^4, p^5$ , or  $p^6$  (up to isomorphism). In particular, these semi-simple rings must be direct products of the simple rings  $\text{GF}(p)$ ,  $\text{GF}(p^2)$ ,  $\text{GF}(p^3)$ ,  $\text{GF}(p^4)$ ,  $M_2(\text{GF}(p))$ ,  $\text{GF}(p^5)$ , and  $\text{GF}(p^6)$ .

- Size  $p$ :

$$\text{GF}(p) \tag{3.16}$$

- Size  $p^2$ :

$$\text{GF}(p^2) \tag{3.17}$$

$$\text{GF}(p) \times \text{GF}(p) \tag{3.18}$$

- Size  $p^3$ :

$$\text{GF}(p^3) \tag{3.19}$$

$$\text{GF}(p^2) \times \text{GF}(p) \tag{3.20}$$

$$\text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{3.21}$$

- Size  $p^4$ :

$$M_2(\text{GF}(p)) \tag{3.22}$$

$$\text{GF}(p^4) \tag{3.23}$$

$$\text{GF}(p^3) \times \text{GF}(p) \tag{3.24}$$

$$\text{GF}(p^2) \times \text{GF}(p^2) \tag{3.25}$$

$$\text{GF}(p^2) \times \text{GF}(p) \times \text{GF}(p) \tag{3.26}$$

$$\text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{3.27}$$

- Size  $p^5$ :

$$\text{GF}(p^5) \tag{3.28}$$

$$M_2(\text{GF}(p)) \times \text{GF}(p) \tag{3.29}$$

$$\text{GF}(p^4) \times \text{GF}(p) \tag{3.30}$$

$$\text{GF}(p^3) \times \text{GF}(p^2) \tag{3.31}$$

$$\text{GF}(p^3) \times \text{GF}(p) \times \text{GF}(p) \tag{3.32}$$

$$\text{GF}(p^2) \times \text{GF}(p^2) \times \text{GF}(p) \tag{3.33}$$

$$\text{GF}(p^2) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{3.34}$$

$$\text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{3.35}$$

- Size  $p^6$ :

$$\text{GF}(p^6) \tag{3.36}$$

$$\text{GF}(p^5) \times \text{GF}(p) \tag{3.37}$$

$$M_2(\text{GF}(p)) \times \text{GF}(p^2) \tag{3.38}$$

$$\text{GF}(p^4) \times \text{GF}(p^2) \tag{3.39}$$

$$M_2(\text{GF}(p)) \times \text{GF}(p) \times \text{GF}(p) \tag{3.40}$$

$$\text{GF}(p^4) \times \text{GF}(p) \times \text{GF}(p) \tag{3.41}$$

$$\text{GF}(p^3) \times \text{GF}(p^3) \tag{3.42}$$

$$\text{GF}(p^3) \times \text{GF}(p^2) \times \text{GF}(p) \tag{3.43}$$

$$\text{GF}(p^3) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{3.44}$$

$$\text{GF}(p^2) \times \text{GF}(p^2) \times \text{GF}(p^2) \tag{3.45}$$

$$\text{GF}(p^2) \times \text{GF}(p^2) \times \text{GF}(p) \times \text{GF}(p) \tag{3.46}$$

$$\text{GF}(p^2) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{3.47}$$

$$\text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \times \text{GF}(p) \tag{3.48}$$

We now prove Lemmas 3.4.12, 3.4.13, and 3.4.14.

**Proof of Lemma 3.4.12.** Let  $R$  be a ring of size  $p^4$  with radical  $J$ , and suppose  $\mathcal{N}$  is scalar linearly solvable over  $R$ . Then  $|R/J| \in \{p, p^2, p^3, p^4\}$ , so by Lemma 3.A.2,  $R/J$  is isomorphic to one of the rings in (3.16)–(3.27).

If  $R/J$  is isomorphic to any of these rings except those in (3.19) and (3.22), then by Lemma 3.A.3,  $\mathcal{N}$  is also scalar linearly solvable over at least one of  $\text{GF}(p)$ ,  $\text{GF}(p^2)$ , or  $\text{GF}(p^4)$ . Since  $\text{GF}(p)$  and  $\text{GF}(p^2)$  are both subrings of  $\text{GF}(p^4)$ , in these cases,  $\mathcal{N}$  is also scalar linearly solvable over  $\text{GF}(p^4)$ . On the other hand, if  $R/J$  is isomorphic to the ring in (3.22), then by Lemma 3.A.3,  $\mathcal{N}$  is also scalar linearly solvable over  $M_2(\text{GF}(p))$ . It follows from Lemma 3.A.1 that  $R/J$  is not isomorphic to the ring in (3.19). ■

**Proof of Lemma 3.4.13.** Let  $R$  be a ring of size  $p^5$  with radical  $J$ , and suppose  $\mathcal{N}$  is scalar linearly solvable over  $R$ . Then  $|R/J| \in \{p, p^2, p^3, p^4, p^5\}$ , so by Lemma 3.A.2,  $R/J$  must be isomorphic to one of the rings in (3.16)–(3.35).

If  $R/J$  is isomorphic to one of the rings in (3.22)–(3.27) (i.e.  $|R/J| = p^4$ ), then  $|J| = p$ . Since  $(J, +)$  is an  $R$ -module and  $\mathcal{N}$  has a linear solution over the faithful module  ${}_R R$ , by Lemma 3.1.3,  $\mathcal{N}$  has a linear solution over  ${}_R J$ . By Theorem 3.2.10, this implies  $\mathcal{N}$  has a scalar linear solution over  $\text{GF}(p)$ . Since  $\text{GF}(p)$  is a subring of  $\text{GF}(p^5)$ , in these cases,  $\mathcal{N}$  also has a scalar linear solution over  $\text{GF}(p^5)$ .

It follows from Lemma 3.A.1 that  $R/J$  is not isomorphic to either of the rings in (3.17) or (3.19). If  $R/J$  is isomorphic to the ring in (3.31), then by Lemma 3.A.3,  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^3) \times \text{GF}(p^2)$ . If  $R/J$  is isomorphic to any of the remaining cases, then by Lemma 3.A.3, network  $\mathcal{N}$  is scalar linearly solvable over either  $\text{GF}(p)$  or  $\text{GF}(p^5)$ . Since  $\text{GF}(p)$  is a subring of  $\text{GF}(p^5)$ , in these cases,  $\mathcal{N}$  also has a scalar linear solution over  $\text{GF}(p^5)$ . ■

**Proof of Lemma 3.4.14.** Let  $R$  be a ring of size  $p^6$  with radical  $J$ , and suppose  $\mathcal{N}$  is scalar linearly solvable over  $R$ . Then  $|R/J| \in \{p, p^2, p^3, p^4, p^5, p^6\}$ , so by Lemma 3.A.2,  $R/J$  must be isomorphic to one of the rings in (3.16)–(3.48). It follows from Lemma 3.A.1 that  $R/J$  is not isomorphic to any of the rings in (3.22), (3.23), or (3.28). If  $R/J$  is isomorphic to any of the remaining cases, then it follows from Lemma 3.A.3 that  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^n)$  for some  $n \in \{1, 2, 3, 6\}$ . Since  $n \mid 6$ ,  $\text{GF}(p^n)$  is a subring of  $\text{GF}(p^6)$ , which implies  $\mathcal{N}$  is scalar linearly solvable over  $\text{GF}(p^6)$ . ■

## References

- [1] G. Bini and F. Flamini, *Finite commutative rings and their applications*, Kluwer Academic Publishers, 2002.
- [2] J. Connelly and K. Zeger, “Linear network coding over rings – Part I: Scalar codes and commutative alphabets,” *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 274 – 291, January 2018.
- [3] B. Corbas and G. D. Williams, “Rings of order  $p^5$  part I. Nonlocal rings,” *Journal of Algebra*, vol. 231, no. 2, pp. 677–690, 2000.
- [4] B. Corbas and G. D. Williams, “Rings of order  $p^5$  part II. Local rings,” *Journal of Algebra*, vol. 231, no. 2, pp. 691–704, 2000.
- [5] N. Das and B.K. Rai, “On the message dimensions of vector linearly solvable networks,” *IEEE Communications Letters*, vol. 20, no. 9, pp. 1701–1704, June 2016.
- [6] 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.
- [7] R. Dougherty, C. Freiling, and K. Zeger, “Unachievability of network coding capacity,” *IEEE Transactions on Information Theory (joint issue with IEEE/ACM Transactions on Networking)*, vol. 52, no. 6, pp. 2365–2372, June 2006.
- [8] R. Dougherty, C. Freiling, and K. Zeger, “Networks, matroids, and non-Shannon information inequalities,” *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 1949–1969, June 2007.
- [9] D. Dummit and R. Foote, *Abstract Algebra*, Third Edition, Hoboken, NJ, John Wiley and Sons Inc., 2004.
- [10] J.B. Ebrahimi and C. Fragouli, “Algebraic algorithms for vector network coding,” *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 996–1007, February 2011.
- [11] K.E. Eldridge, “Orders for finite noncommutative rings with unity,” *The American Mathematical Monthly*, vol. 75, no. 5, pp. 512–514, May 1968.
- [12] B. Fine, “Classification of Finite Rings of Order  $p^2$ ,” *Mathematics Magazine*, vol. 66, no. 4, pp. 248–252, October 1993.
- [13] T.Y. Lam, *A First Course in Noncommutative Rings*, Second Edition, Springer Verlag New York Inc., 2001.
- [14] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker Inc., 1974.
- [15] M. Médard, M. Effros, T. Ho, and D. Karger, “On coding for non-multicast networks,” *Conference on Communication Control and Computing*, Monticello, IL, October 2003.
- [16] A. Rasala Lehman and E. Lehman, “Complexity classification of network information flow problems,” *ACM-SIAM Symposium on Discrete algorithms*, 2004.
- [17] Q. Sun, X. Yang, K. Long, X. Yin, and Z. Li, “On vector linear solvability of multicast networks,” *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 5096–5107, September 2016.

---

This chapter is a reprint of the material as it appears in J. Connelly and K. Zeger, “Linear network coding over rings – Part II: Vector codes and non-commutative alphabets,” *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 292 – 308, January 2018. The dissertation author was the primary investigator of this paper. © IEEE. Reprinted with permission.

# Chapter 4

## Capacity and Achievable Rate Regions

### Abstract

The rate of a network code is the ratio of the block size of the network's messages to that of its edge codewords. We compare the linear capacities and achievable rate regions of networks using finite field alphabets to the more general cases of arbitrary ring and module alphabets. For non-commutative rings, two-sided linearity is allowed. Specifically, we prove the following for directed acyclic networks:

- (i) The linear rate region and the linear capacity of any network over a finite field depend only on the characteristic of the field. Furthermore, any two fields with different characteristics yield different linear capacities for at least one network.
- (ii) Whenever the characteristic of a given finite field divides the size of a given finite ring, each network's linear rate region over the ring is contained in its linear rate region over the field. Thus, any network's linear capacity over a field is at least its linear capacity over any other ring of the same size. An analogous result also holds for linear network codes over module alphabets.
- (iii) Whenever the characteristic of a given finite field does not divide the size of a given finite ring, there is some network whose linear capacity over the ring is strictly greater than its linear capacity over the field. Thus, for any finite field, there always exist rings over which some networks have higher linear capacities than over the field.



## 4.1 Introduction

In network coding, solvability determines whether or not a network's receivers can adequately deduce from their inputs a specified subset of the network's message values. The solvability of directed acyclic networks follows a hierarchy of different types of network coding. For example, scalar linear coding over finite fields is known to be inferior to vector linear coding over finite fields [34], which in turn is known to be inferior to non-linear coding [11]. On the other hand, the capacity of a network reveals how much transmitted information per channel use (i.e. source messages per edge use) can be sent to the network's receiver nodes in the limit of large block sizes for transmission. It is also known that linear codes over finite fields cannot achieve the full capacity of some networks [11]. Thus, linear coding over finite fields is inferior to more general types of network coding in terms of both solvability and capacity. Nevertheless, linear codes over finite fields are attractive for both theoretical and practical reasons [30].

In certain cases, linear coding over finite ring alphabets can offer solvability advantages over finite field alphabets (see Chapters 2 and 3). An open question has been whether the linear capacity of a network over a finite field can be improved by using some other ring of the same size as the field. In other words, does the improvement in network solvability, from using more general rings than fields, also carry over to network capacity? In the present paper, we answer this question in the negative. That is, we prove that the linear capacity of a network cannot be improved by changing the network coding alphabet from a field to any other ring of the same size.

Another open question has been whether the linear capacity of a network over a finite field can depend on any aspect of the field other than its characteristic. Indeed it has been previously observed that the linear capacity of a network can vary as a function of the field (e.g. [14, 15]), but all known examples had linear capacities that only depended on the fields' characteristics. We also answer this question in the negative. That is, we prove that any two fields with the same characteristic will result in the same linear capacity for any given network. Furthermore, any two fields with different characteristics will result in different linear capacities for at least one network. We prove analogous (and more general) results for linearly achievable rate regions of networks over finite fields.

Unlike finite fields, finite rings need not have prime-power size, which may be advantageous in certain applications. An open question has been whether a network can increase its linearly achievable rate region by allowing the alphabet to be a ring of non-power-of-prime size. However, we again answer this question in the negative by showing that a network's linear rate region over a ring is contained in its linear rate region over any field whose characteristic divides the ring's size. This result follows from the fact that

every finite ring is isomorphic to some direct product of rings of prime-power sizes. As a consequence of this result, any network's linear capacity over a particular ring is at most its linear capacity over any field whose characteristic divides the ring's size. These results extend naturally to the more general case of linear network codes in which the alphabet has the structure of a finite module.

#### 4.1.1 Modules, Linear Functions, and Tensor Products

We focus on linear network codes over finite rings, but we prove many of our intermediate results in the broader context of linear network codes over modules. In this section, we define linear functions over modules, which generalize linear functions over rings. We then formally define linear network codes over rings and modules in Section 4.1.3.

**Definition 4.1.1.** A *left  $R$ -module* is an Abelian group  $(G, \oplus)$  together with a ring  $(R, +, *)$  of *scalars* and an action  $\cdot : R \times G \rightarrow G$  such that for all  $r, s \in R$  and all  $g, h \in G$  the following hold:

$$r \cdot (g \oplus h) = (r \cdot g) \oplus (r \cdot h)$$

$$(r + s) \cdot g = (r \cdot g) \oplus (s \cdot g)$$

$$(r * s) \cdot g = r \cdot (s \cdot g)$$

$$1 \cdot g = g.$$

From these properties, it also follows that  $0 \cdot g = 0$  and  $r \cdot 0 = 0$  for all  $g \in G$  and all  $r \in R$ . For brevity, we will sometimes refer to such an  $R$ -module as  ${}_R G$  or simply the  $R$ -module  $G$ . Since network coding alphabets are presumed to be finite, a module will always refer to a module in which  $G$  is finite. However, in principle, the ring need not be finite, so we make no assumptions about the cardinality of the ring in a module. Some important examples of modules include:

- The ring of integers  $\mathbb{Z}$  acts on any Abelian group  $G$  by repeated addition in  $G$ .
- Any ring  $R$  acts on its own additive group  $(R, +)$  by multiplication in  $R$ . We denote this module by  ${}_R R$ .
- Any ring  $R$  acts on the set of all  $t$ -vectors over  $R$ , denoted by  $R^t$ , by scalar multiplication. When  $R$  is a field, this module is a vector space.

- If  ${}_R G$  is a module, then the ring of all  $t \times t$  matrices with entries in  $R$ , denoted  $M_t(R)$ , acts on the group,  $G^t$ , of all  $t$ -vectors over  $G$  via matrix-vector multiplication where multiplication of elements of  $R$  with elements of  $G$  is given by the action of  ${}_R G$ . A special case of this module,  $M_t(R)G^t$ , occurs when  $G = (R, +)$ , in which case matrices over  $R$  act on vectors over  $R$  via matrix-vector multiplication over  $R$ .

If  $R$  is a ring, a function  $f : R^m \rightarrow R$  of the form

$$f(x_1, \dots, x_m) = a_1 x_1 + \dots + a_m x_m$$

where  $a_1, \dots, a_m \in R$ , is a (left) *one-sided linear function* with respect to both the ring  $R$  and the left module  ${}_R R$ .<sup>1</sup> A function  $f' : R^m \rightarrow R$  of the form

$$f'(x_1, \dots, x_m) = \sum_{i=1}^m \sum_{j=1}^{n_i} a_{i,j} x_i b_{i,j} \quad (4.1)$$

where  $a_{i,j}, b_{i,j} \in R$ , is a *two-sided linear function* with respect to  $R$ . When  $R$  is commutative, every two-sided linear function is also a one-sided linear function, since in a commutative ring,

$$\sum_{i=1}^m \sum_{j=1}^{n_i} a_{i,j} x_i b_{i,j} = \sum_{i=1}^m \left( \sum_{j=1}^{n_i} a_{i,j} b_{i,j} \right) x_i.$$

However, left and right multiplication are not necessarily the same in a non-commutative ring, so the class of two-sided linear functions is broader than the class of one-sided linear functions.

**Example 4.1.2.** Let  $R$  be the (non-commutative) ring of all  $2 \times 2$  matrices over a field. The function  $f : R \rightarrow R$  given by

$$\begin{aligned} f \left( \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix} \right) &= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} x_{1,1} & 0 \\ 0 & x_{2,2} \end{bmatrix} \end{aligned}$$

is a two-sided linear function over  $R$ . It can be verified that, for all  $A, B \in R$ , the function  $f(X)$  is not the function  $AXB$ . This also implies  $f(X)$  cannot be written as a (left or right) one-sided linear function.

<sup>1</sup> Every right one-sided linear function with respect to a ring or a right module can be written as a corresponding left one-sided linear function with respect to a left module with the same Abelian group. Hence, it suffices for us to exclusively use left one-sided linear functions.

By allowing for sums of terms multiplied by coefficients on both the left and the right, a broader class of functions can be attained than with a single term multiplied by coefficients on the left and the right. In the remainder of this section, we will show that two-sided linear functions over rings can be written as one-sided linear functions with respect to some module, i.e.  $f'$  in (4.1) can be written as

$$f'(x_1, \dots, x_m) = c_1 \cdot x_1 + \dots + c_m \cdot x_m$$

where  $c_1, \dots, c_m$  are elements of some other ring that acts on  $R$ . In order to do so, we exploit module tensor products. If  $G$  and  $H$  are each  $R$ -modules, then the tensor product of  $G$  and  $H$  is a third  $R$ -module that satisfies properties similar to the constructed vector space in the following example.

**Example 4.1.3.** Suppose  $\mathbb{F}$  is a field and  $U \subseteq \mathbb{F}^m$  and  $V \subseteq \mathbb{F}^n$  are vector spaces. For each  $u \in U$  and  $v \in V$ , define the  $mn$  vector  $(u, v)$  by

$$(u, v) = \begin{bmatrix} u_1 v_1 \\ \vdots \\ u_1 v_n \\ \vdots \\ u_m v_1 \\ \vdots \\ u_m v_n \end{bmatrix}.$$

It is easily verified that for all  $u, u' \in U$ , all  $v, v' \in V$ , and all  $\alpha \in \mathbb{F}$ ,

$$(u, v) + (u', v) = (u + u', v)$$

$$(u, v) + (u, v') = (u, v + v')$$

$$\alpha (u, v) = (\alpha u, v)$$

$$\alpha (u, v) = (u, \alpha v).$$

The subspace of  $\mathbb{F}^{mn}$  generated by all vectors of the form  $(u, v)$  for some  $u \in U$  and some  $v \in V$  is isomorphic to the tensor product of  $U$  and  $V$ . In general, this tensor product space differs from the direct product space  $U \times V \subseteq \mathbb{F}^{m+n}$  obtained by concatenating vectors from  $U$  with vectors from  $V$ . In fact, when  $U = \mathbb{F}^m$  and  $V = \mathbb{F}^n$ , the tensor product space is  $\mathbb{F}^{mn}$ , whereas the direct product space is  $\mathbb{F}^{m+n}$ .

If  $R$  is a ring and  $E$  is a set, the *free  $R$ -module generated by  $E$*  is denoted  $R^{(E)}$ . In this module, the group is the subset of the Cartesian product  $\prod_{e \in E} R$  consisting only of the elements that have finitely many non-zero components together with component-wise addition, and the ring  $R$  acts on  $R^{(E)}$  component-wise.

By mapping the element  $e \in E$  to the vector in  $R^{(E)}$  whose  $e$ th component is 1 and all other components are 0, we can view  $R^{(E)}$  as the set of all finite  $R$ -linear combinations of elements of  $E$ . In other words, every element of  $R^{(E)}$  can be uniquely written as  $\sum_{e \in E} a_e e$ , where only finitely many  $a_e \in R$  are non-zero, so the set  $E$  is a basis for  $R^{(E)}$ .

If  $G$  is an  $R$ -module and  $N$  is a subgroup of  $G$  that is closed under the action of  $R$ , then  $N$  is a *submodule* of  $G$ . The quotient group  $G/N$  is also an  $R$ -module (e.g. see [16, p. 348]). If  $E$  is a subset of  $G$ , then the *submodule generated by  $E$*  is

$$\{r_1 e_1 + \cdots + r_m e_m : r_1, \dots, r_m \in R, e_1, \dots, e_m \in E\}.$$

Now let  $R$  be a commutative ring, let  $G$  and  $H$  be  $R$ -modules, and let  $N$  be the submodule of  $R^{(G \times H)}$  generated by the set

$$\left\{ \begin{array}{l} (g, h) + (g', h) - (g + g', h), \\ (g, h) + (g, h') - (g, h + h'), \\ r(g, h) - (rg, h), \\ r(g, h) - (g, rh) \end{array} : g, g' \in G, h, h' \in H, r \in R \right\}.$$

The *tensor product module of  ${}_R G$  and  ${}_R H$* , denoted  $G \otimes_R H$ , is the quotient  $R$ -module  $R^{(E)}/N$ . In other words,  $G \otimes_R H$  is the set of equivalence classes of the congruence generated by the following relations on  $R^{(E)}$ :

$$(g, h) + (g', h) = (g + g', h)$$

$$(g, h) + (g, h') = (g, h + h')$$

$$r(g, h) = (rg, h)$$

$$r(g, h) = (g, rh).$$

The tensor product module is unique up to isomorphism (e.g. see [16, Sections 10.1 – 10.4] for more information on modules and tensor products) and exhibits similar properties to the tensor product of vector spaces. The elements of  $G \otimes_R H$  are called *tensors* and can be written (non-uniquely, in general) as sums of equivalence class representatives:  $(g_1, h_1) + \cdots + (g_m, h_m)$ , for some positive integer  $m$  and  $(g_1, h_1), \dots, (g_m, h_m) \in G \times H$ .

**Definition 4.1.4.** Let  $R$  and  $S$  be finite rings, and let  $\mathbb{Z}$  denote the ring of integers. The *tensor product ring*  $R \otimes S$  is the Abelian group  $R \otimes_{\mathbb{Z}} S$  together with multiplication given by

$$\left( \sum_{i=1}^m (r_i, s_i) \right) * \left( \sum_{j=1}^n (r'_j, s'_j) \right) = \sum_{i=1}^m \sum_{j=1}^n (r_i r'_j, s_i s'_j)$$

for all  $(\sum_{i=1}^m (r_i, s_i)), (\sum_{j=1}^n (r'_j, s'_j)) \in R \otimes_{\mathbb{Z}} S$ .

This tensor product ring is well defined and unique up to isomorphism (e.g. see [16, Chapter 10.4, Proposition 21]). As an example, if  $\mathbb{Z}_m$  and  $\mathbb{Z}_n$  denote the rings of integers modulo  $m$  and  $n$ , respectively, then we have  $\mathbb{Z}_m \otimes \mathbb{Z}_n \cong \mathbb{Z}_{\gcd(m,n)}$  (e.g. see [16, p. 369]). Specifically, if  $m = 4$  and  $n = 2$ , then the tensors in  $\mathbb{Z}_4 \otimes \mathbb{Z}_2$  are such that

$$(0,0) = (0,1) = (2,1) = (1,0) = (2,0) = (3,0) \quad \text{and} \quad (1,1) = (3,1)$$

and addition and multiplication are isomorphic to addition and multiplication in  $\mathbb{Z}_2$ .

We also comment that the *direct product ring*  $R \times S$  with component-wise addition and multiplication is generally not isomorphic to the tensor product ring  $R \otimes S$ . As an example, if  $m$  and  $n$  are relatively prime, then by the Chinese remainder theorem,  $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$  (e.g. see [16, p. 267]), whereas  $\mathbb{Z}_m \otimes \mathbb{Z}_n \cong \mathbb{Z}_1$  is the trivial ring.

For a finite ring  $R$ , the *opposite ring*, denoted  $R^{op}$ , is the additive group of  $R$  with multiplication taken in the opposite order, i.e.  $a *_{op} b = ba$ , for all  $a, b \in R$ . The tensor product ring  $R \otimes R^{op}$  acts on  $(R, +)$  via

$$\left( \sum_{i=1}^n (a_i, b_i) \right) \cdot r = \sum_{i=1}^n a_i r b_i$$

for all  $a_1, \dots, a_n, b_1, \dots, b_n, r \in R$ . In other words,  $R \otimes R^{op}$  acts on  $(R, +)$  by computing *two-sided* linear combinations of elements of  $(R, +)$ . We denote this module by  ${}_{R \otimes R^{op}} R$ . The properties of tensor addition and multiplication are natural in the context of this module. In particular, for all  $a, a', b, b', x \in R$ , and  $n \in \mathbb{Z}$ , we have

$$((a, b) + (a', b)) \cdot x = axb + a'xb = (a + a')xb = (a + a', b) \cdot x$$

$$((a, b) + (a, b')) \cdot x = axb + axb' = ax(b + b') = (a, b + b') \cdot x$$

$$n(a, b) \cdot x = n(axb) = (na)xb = (na, b) \cdot x$$

$$n(a, b) \cdot x = n(axb) = ax(nb) = (a, nb) \cdot x.$$

The two-sided linear function  $f'$  in (4.1) can now be written as

$$f'(x_1, \dots, x_m) = \sum_{i=1}^m \left( \sum_{j=1}^{n_i} (a_{i,j}, b_{i,j}) \right) \cdot x_i$$

which is a one-sided linear function with respect to the  $R \otimes R^{op}$ -module  $R$ . This shows that *one-sided* linearity over left modules generalizes *two-sided* linearity over rings.

**Example 4.1.5.** Let  $R$  be the (non-commutative) ring of all  $2 \times 2$  matrices over a field. The two-sided linear function  $f : R \rightarrow R$  from Example 4.1.2 can be written as a one-sided linear function over the  $R \otimes R^{op}$ -module  $R$  as

$$f \left( \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix} \right) = \left( \left( \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right) + \left( \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right) \right) \cdot \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix}.$$

### 4.1.2 Network Coding Model

A *network* will refer to a finite, directed, acyclic multigraph, some of whose nodes are *sources* or *receivers*. Source nodes generate *message vectors* whose components are arbitrary elements of a fixed, finite set of size at least 2, called an *alphabet*. The elements of an alphabet are called *symbols*. We will denote the cardinality of an alphabet  $\mathcal{A}$  by  $|\mathcal{A}|$ . The *inputs* to a node are the message vectors, if any, originating at the node and the symbols on the incoming edges of the node. Each outgoing edge of a network node has associated with it an *edge function* that maps the node's inputs to the vector of symbols carried by the edge, called the *edge vector*. Each receiver node has *decoding functions* that map the receiver's inputs to a vector of alphabet symbols in an attempt to recover the receiver's *demands*, which are the message vectors the receiver wishes to obtain.

In a network with  $m$  message vectors, a  $(k_1, \dots, k_m, n)$  *code over an alphabet*  $\mathcal{A}$  (also called a *fractional code*) is an assignment of edge functions to the edges in the network and an assignment of decoding functions to the receivers in the network such that the  $i$ th message vector is an element of  $\mathcal{A}^{k_i}$  and the edge vectors are elements of  $\mathcal{A}^n$ . The *rate vector* of a  $(k_1, \dots, k_m, n)$  network code is  $\mathbf{r} = (k_1/n, \dots, k_m/n)$ . A fractional code is a *solution* if each receiver recovers its demanded message vector from its inputs, and a rate vector  $\mathbf{r}$  is *achievable for a network* if the network has a fractional solution with rate vector  $\mathbf{r}$  over some alphabet.

### 4.1.3 Linearity over Finite Rings and Modules

A function  $f : G^s \rightarrow G^t$  is *linear with respect to the module*  ${}_R G$  if it can be written as a matrix-vector product,  $f(\mathbf{x}) = A\mathbf{x}$ , where

- $A$  is a  $t \times s$  matrix with elements from  $R$ ,
- multiplication of elements of  $R$  by elements of  $G$  is the action of the module.

A fractional code is *linear over the  $R$ -module*  $G$  if the message vectors and edge vectors have components from  $G$  and all edge functions and decoding functions are linear over the module. For each network node, the vector  $\mathbf{x} \in G^s$  is a concatenation of all the input vectors of the node. In other words, the network alphabet is  $G$ , and the outgoing edge vectors and decoded symbol vectors at a node are linear combinations of the node's vector inputs, where the coefficients describing the linear combination are from  $R$ . We use modules as a tool to prove results related to linear coding over rings, since linear network coding over modules generalizes linear network coding over rings and fields. The module approach is especially useful for non-commutative rings with two-sided linear codes.

If  $R$  is a finite ring, then a fractional linear code over the module  ${}_{R \otimes R^{op}} R$  is said to be a *fractional two-sided linear code over  $R$* . In particular, the network alphabet is  $R$ , and the outgoing edge vectors and decoded symbols carry linear combinations of the node's input components, where each input component in the combination is multiplied on the left and right by constants from  $R$ . If  $R$  is commutative, then then a fractional two-sided linear code over  $R$  is also a fractional linear code over the module  ${}_R R$ , since one-sided and two-sided linearity are equivalent in this case. A rate vector  $\mathbf{r}$  is *linearly achievable for a network over a finite ring  $R$*  if the network has a fractional two-sided linear solution over  $R$  with rate vector  $\mathbf{r}$ .

### 4.1.4 Rate Regions, Capacity, and Solvability

The *rate region* of a network  $\mathcal{N}$  is

$$\mathcal{R}(\mathcal{N}) = \{\mathbf{r} \in \mathbb{Q}^m : \mathbf{r} \text{ is achievable for } \mathcal{N}\},^2$$

the *capacity* (also known as the “uniform capacity” or the “symmetric capacity”) is

$$\mathcal{C}(\mathcal{N}) = \sup \{r \in \mathbb{Q} : (r, \dots, r) \text{ is achievable for } \mathcal{N}\},$$

---

<sup>2</sup>Some authors refer to the rate regions and linear rate regions of networks as “capacity regions” or “achievable rate regions” and sometimes define them as the convex hull or the topological closure of the set. We compare a network's linear rate regions over finite rings to its linear rate regions over finite fields, and our results immediately extend to these alternate definitions of rate regions.



the *linear rate region* with respect to a ring alphabet  $R$  is

$$\mathcal{R}_{lin}(\mathcal{N}, R) = \{\mathbf{r} \in \mathbb{Q}^m : \mathbf{r} \text{ is linearly achievable for } \mathcal{N} \text{ over } R\},$$

and the *linear capacity* with respect to a ring alphabet  $R$  is

$$\mathcal{C}_{lin}(\mathcal{N}, R) = \sup \{r \in \mathbb{Q} : (r, \dots, r) \text{ is linearly achievable for } \mathcal{N} \text{ over } R\}.$$

While the emphasis of this paper is on rate regions and capacities of networks, we define several solvability properties, as they will be useful in proving our main results. A  $(k_1, \dots, k_m, n)$  code, for which  $k_1 = \dots = k_m = n = t$ , is also called a *t-dimensional vector code*, i.e. the block size of every message and edge is  $t$ , and a 1-dimensional vector code is called a *scalar code*. A network is said to be

- *solvable* if it has a scalar solution over some alphabet,
- *scalar linearly solvable over  ${}_R G$*  if it has a scalar linear solution over the module  ${}_R G$ , and
- *vector linearly solvable over  ${}_R G$*  if it has a  $t$ -dimensional vector linear solution over the module  ${}_R G$ , for some  $t \geq 1$ .

Special cases of scalar and vector linear solvability over modules include scalar and vector linear solvability over rings, in which case the module is  ${}_{R \otimes R} R$  (or equivalently,  ${}_R R$ , if  $R$  is commutative). The all-one's vector is an achievable rate vector for any solvable network. We also comment that if a network has a  $t$ -dimensional vector solution over some alphabet  $\mathcal{A}$ , then it has a (possibly non-linear) scalar solution over the alphabet  $\mathcal{A}^t$ , so the network is solvable.

#### 4.1.5 Related Work

In 2000, Ahlswede, Cai, Li, and Yeung [1] showed that some networks can attain higher capacities by using linear coding at network nodes, rather than just using routing operations. Since then, many results on linear network coding over finite fields have been achieved. On the other hand, the theoretical potential and limitations of linear network coding over non-field alphabets has been much less understood.

Li, Yeung, and Cai [29] showed that when each of a network's receivers demands all of the messages (i.e. a *multicast* network), the linear capacity over any finite field is equal to the (nonlinear) capacity. Ho et. al [22] showed that for multicast networks, random fractional linear codes over finite fields achieve the network's capacity with probability approaching one as the block sizes increase. Jaggi et. al [25] developed polynomial-time algorithms for constructing capacity-achieving fractional linear codes over finite fields for

multicast networks. Algorithms for constructing fractional linear solutions over finite fields for other classes of networks have also been a subject of considerable interest (e.g. [17], [24], [40], and [45]).

It is known (e.g. [11]) that for general networks, fractional linear codes over finite fields do not necessarily attain the network's capacity. In fact, it was shown by Lovett [31] that, in general, fractional linear network codes over finite fields cannot even approximate the capacity to any constant factor. Blasiak, Kleinberg, and Lubetzky [2] demonstrated a class of networks whose capacities are larger than their linear capacities over any finite field by a factor that grows polynomially with the number of messages. Langberg and Sprintson [28] showed that, for general networks, constructing fractional solutions whose rates even approximate the capacity to any constant factor is NP-hard.

It was shown in [4] that the capacity of a network is independent of the coding alphabet. However, there are multiple examples in the literature (e.g. [7], [11], [15]) of networks whose linear capacity over a finite field can depend on the field alphabet, specifically by way of the characteristic of the field. Muralidharan and Rajan [35] demonstrated that a fractional linear solution over a finite field  $\mathbb{F}$  exists for a network if and only if the network is associated with a discrete polymatroid representable over  $\mathbb{F}$ . Linear rank inequalities of vector subspaces and linear information inequalities (e.g. [44]) are known to be closely related and have been shown to be useful in determining or bounding networks' linear capacities over finite fields (e.g. [14], [15], and [18]).

Chan and Grant [5] demonstrated a duality between entropy functions and rate regions of networks and provided an alternate proof that fractional linear codes over finite fields do not necessarily attain the capacity. The relationship between network rate regions and entropy functions has been further studied, for example, in [6], [21], [36], and [43]. It has also been shown (e.g. [13]) that non-Shannon information inequalities may be needed to determine the capacity of a network.

It was shown in [5] that fractional linear network codes over finite rings (and modules) are special cases of codes generated by Abelian groups. However, most other studies of linear capacity have generally been restricted to finite field alphabets. We will consider the case where the coding alphabet is viewed, more generally, as a finite ring. We showed in Chapters 2 and 3 that scalar linear network codes over finite rings can offer solvability advantages over scalar linear network codes over finite fields in certain cases. Some of the results from these chapters will be used in proofs in the present chapter.

### 4.1.6 Main Results

The remainder of the chapter is outlined as follows. In Section 4.2, we explore a connection between fractional linear codes and vector linear codes, which allows us to exploit network solvability results over modules from the previous chapters in order to achieve capacity results over rings. For a given network  $\mathcal{N}$  and rate vector  $\mathbf{r}$ , we show (in Lemma 4.2.2) there exists a network  $\mathcal{N}'$  that is vector linearly solvable over a given module if and only if the rate vector  $\mathbf{r}$  is linearly achievable for  $\mathcal{N}$  over the module. In Section 4.2.2, we order finite modules based on fractional solvability and show that under certain conditions, fractional linear solutions over a given module imply the existence of fractional linear solutions over other modules. The results in Sections 4.2.2 and 4.2.3 are used to show (in Lemma 4.2.14) that fractional linear solutions over modules imply the existence of fractional linear solutions over modules in which the ring of matrices over a field acts on vectors over the field.

In Section 4.3, we use the results relating solvability and fractional codes from Section 4.2 to show our main results on linear rate regions over fields. We prove (in Theorem 4.3.3) that for any two finite fields with different characteristics, there exists a network whose linear rate regions over the fields are not contained in one another. This indicates that some rate vectors may only be linearly achievable over certain fields, while other rate vectors may only be linearly achievable over other fields. Additionally, for any two finite fields with different characteristics, there exists a network whose linear capacities over the two fields are different (Corollary 4.3.2). We also show (in Theorem 4.3.4) that for any finite fields with the same characteristic, every network's linear rate regions over the fields are equal. In other words, the linear rate region of any network over a field depends only on the characteristic of the field. Consequently, the linear capacity of any network over a field depends only on the characteristic of the field as well (Corollary 4.3.5). This contrasts with linear solvability over fields, since scalar linear solvability can depend not only on the field's characteristic, but more specifically, on the precise cardinality of the field (e.g. see Chapter 2, [37], [39]).

In Section 4.4, we prove our main results on linear rate regions and linear capacities over finite rings. We show (in Theorem 4.4.2) that for any network, any finite field, and any finite ring whose size is divisible by the field's characteristic, the network's linear rate region over the ring is contained within the network's linear rate region over the field. Consequently, the network's linear capacity over the ring is at most its linear capacity over the field (Corollary 4.4.3). In this sense, it suffices to restrict attention to finite fields when choosing a coding alphabet from among all rings. In other words, the general class of rings does not provide any benefit over the restricted class of finite fields, in terms of achieving linear rate regions with

network coding. In order to prove Theorem 4.4.2, we show (in Theorem 4.4.1) that whenever a network has a fractional linear solution over some module with a given rate vector, the network has a fractional linear solution over some field with the same rate vector and potentially larger block sizes.

Even though Theorem 4.4.2 asserts non-field rings cannot provide an increase in linear capacity over fields for *all* networks, we show (in Corollary 4.4.4) that generally certain rings, smaller than a given field, can increase the linear capacity over at least *some* (but not all) networks. In fact, we show (in Theorem 4.4.5) that for any finite field and any finite ring, there exists a network with higher linear capacity over the ring than over the field if and only if the field's size and the ring's size are relatively prime. Finally, we show (in Corollary 4.4.6) that whenever a network has a fractional linear solution over some ring (or module) with a uniform rate arbitrarily close to 1, the network must also have a fractional linear solution over some field with the same uniform rate. This strengthens results in [11] by showing that the non-linearly solvable network presented in this paper additionally is not asymptotically linearly solvable over rings and modules.

## 4.2 Fractional and Vector Codes over Modules

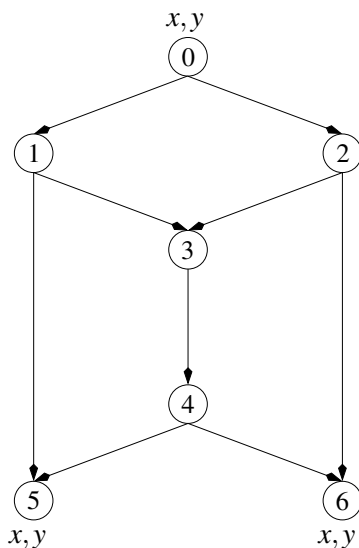


Figure 4.1: The Butterfly Network has a single source node 0, which generates message vectors  $x$  and  $y$ . Each of the receivers, nodes 5 and 6, demands both  $x$  and  $y$ . The linear rate region of the Butterfly Network is  $\{(r_x, r_y) \in \mathbb{Q}^2 : r_x, r_y \geq 0 \text{ and } r_x + r_y \leq 2\}$  over any ring.

Many techniques for upper bounding network linear capacities over finite fields (e.g. [11, 14]) exploit linear algebra results that sometimes do not extend to matrices over arbitrary rings. For example, it is known (e.g. see [20]) that the transpose of an invertible matrix over a non-commutative ring is not necessar-

ily invertible.<sup>3</sup> This suggests that directly computing network linear rate regions and linear capacities over finite rings and modules may be somewhat difficult.

One method for determining whether a network satisfies some solvability or capacity property is to transform the question into whether a certain related network satisfies a corresponding property (e.g. [26], [41], and [42]). Namely, in [41] and [42], the authors show that determining the rate region and linear rate region of a general network can be reduced to determining the rate region and linear rate region of a corresponding network where each message vector is demanded by exactly one receiver (i.e. a *multiple unicast* network). In [26], it is shown that determining whether a multiple unicast network has a solution with a given rate vector can be reduced to determining whether a corresponding unicast network with two message-receiver pairs has a solution with a corresponding rate vector.

We use a similar approach to relate the existence of fractional linear solutions over modules to scalar and vector linear solvability over modules. The results in this section allow us to more easily relate a network's linear rate region over a ring to the network's linear rate region over some field.

#### 4.2.1 Fractional Equivalent Network

For any network  $\mathcal{N}$  with  $m$  message vectors and integers  $k_1, \dots, k_m \geq 0$  and  $n \geq 1$ , the following defines a new network which is vector linearly solvable over a module  ${}_R G$  if and only if  $\mathcal{N}$  has a fractional linear solution over  ${}_R G$  whose rate vector is  $(k_1/n, \dots, k_m/n)$ . We prove this fact in Lemma 4.2.2. This network construction can be used to show many linear solvability properties extend to the existence of fractional linear solutions.

**Definition 4.2.1.** For any network  $\mathcal{N}$  with  $m$  message vectors and any integers  $k_1, \dots, k_m \geq 0$  and  $n \geq 1$ ,

let  $\mathcal{N}^{(k_1, \dots, k_m, n)}$  denote the network  $\mathcal{N}$  but with

- (i) each edge replaced with  $n$  parallel edges, and
- (ii) the  $i$ th message vector replaced with  $k_i$  message vectors.

The *Butterfly Network* is defined in Figure 4.1, and, for each  $k_x, k_y \geq 0$  and  $n \geq 1$ , the  $(k_x, k_y, n)$ -*Butterfly Network* is defined in Figure 4.2. These networks are consistent with Definition 4.2.1, if they are denoted by  $\mathcal{N}$  and  $\mathcal{N}^{(k_x, k_y, n)}$ , respectively.

<sup>3</sup>See [3] and [33] for more information on linear algebra over rings.

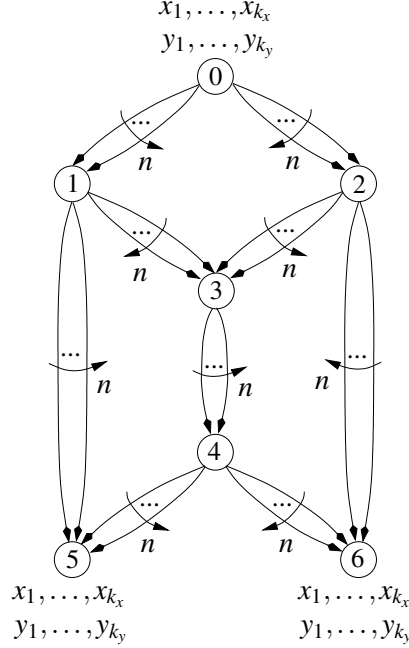


Figure 4.2: The  $(k_x, k_y, n)$ -Butterfly Network has a single source node, which generates message vectors  $x_1, \dots, x_{k_x}$  and  $y_1, \dots, y_{k_y}$ . Each receiver demands all of the message vectors. The  $(k_x, k_y, n)$ -Butterfly Network is vector linearly solvable over a given ring if and only if  $k_x + k_y \leq 2n$ .

**Lemma 4.2.2.** *Let  $\mathcal{N}$  be a network with  $m$  message vectors, let  $k_1, \dots, k_m \geq 0$  and  $n, t \geq 1$  be integers, let  ${}_R G$  be a module, and let  $\mathcal{N}^{(k_1, \dots, k_m, n)}$  denote the network in Definition 4.2.1 corresponding to  $\mathcal{N}$  and  $k_1, \dots, k_m$  and  $n$ . The network  $\mathcal{N}$  has a  $(tk_1, \dots, tk_m, tn)$  linear solution over  ${}_R G$  if and only if  $\mathcal{N}^{(k_1, \dots, k_m, n)}$  has a  $t$ -dimensional vector linear solution over  ${}_R G$ .*

*Proof.* In a  $(tk_1, \dots, tk_m, tn)$  linear code over module  ${}_R G$  for network  $\mathcal{N}$ , suppose a node generates the  $l_1$ th,  $\dots$ ,  $l_u$ th message vectors and has  $v$  incoming edges, where the  $i$ th message vector is an element of  $G^{tk_i}$  and the edge vectors are elements of  $G^{tn}$ . Then an edge function

$$f : \underbrace{G^{tk_{l_1}} \times \dots \times G^{tk_{l_u}}}_{u \text{ message vectors}} \times \underbrace{G^{tn} \times \dots \times G^{tn}}_{v \text{ edge vectors}} \longrightarrow G^{tn}$$

of an outgoing edge of the node is of the form  $f(\mathbf{x}) = A\mathbf{x}$  where  $A$  is a  $tn \times (tk_1 l_1 + \dots + tk_{l_u} + vtn)$  matrix with entries in  $R$  and  $\mathbf{x}$  is a vector over  $G$  formed by concatenating the input vectors of the node. Let  $A_1, \dots, A_n$  denote the  $t \times (tk_1 l_1 + \dots + tk_{l_u} + vtn)$  matrices such that  $A$  can be written in block form as

$$A = \begin{bmatrix} A_1 \\ \vdots \\ A_n \end{bmatrix}.$$

The corresponding node in  $\mathcal{N}^{(k_1, \dots, k_m, n)}$  generates  $k_{l_1} + \dots + k_{l_u}$  message vectors and has  $vn$  incoming edge vectors. Define the  $t$ -dimensional vector code for  $\mathcal{N}^{(k_1, \dots, k_m, n)}$  over  ${}_R G$  by letting the edge function of the  $i$ th parallel corresponding outgoing edge be the linear mapping

$$f_i : \underbrace{G^t \times \dots \times G^t}_{k_{l_1} + \dots + k_{l_u} \text{ message vectors}} \times \underbrace{G^t \times \dots \times G^t}_{vn \text{ edge vectors}} \longrightarrow G^t$$

given by  $f_i(\mathbf{x}) = A_i \mathbf{x}$ , where  $i = 1, \dots, n$ . The edge in the code for  $\mathcal{N}$  carries the same linear combination of its inputs as the  $n$  parallel edges in the code for  $\mathcal{N}^{(k_1, \dots, k_m, n)}$ .

Similarly, in a  $(tk_1, \dots, tk_m, tn)$  code for  $\mathcal{N}$ , suppose a receiver generates the  $l_1$ th,  $\dots$ ,  $l_u$ th message vectors, has  $v$  incoming edges, and demands  $x_j$ . Then the decoding function

$$d : \underbrace{G^{tk_1} \times \dots \times G^{tk_u}}_{u \text{ message vectors}} \times \underbrace{G^{tn} \times \dots \times G^{tn}}_{v \text{ edge vectors}} \longrightarrow G^{tk_j}$$

corresponding to  $x_j$  is of the form  $f(\mathbf{x}) = D\mathbf{x}$  where  $D$  is a  $tk_j \times (tk_1 l_1 + \dots + tk_{l_u} + vtn)$  matrix and  $\mathbf{x}$  is a vector over  $G$  formed by concatenating the input vectors of the node. Let  $D_1, \dots, D_{k_j}$  denote the  $t \times (tk_1 l_1 + \dots + tk_{l_u} + vtn)$  matrices such that  $D$  can be written in block form as

$$D = \begin{bmatrix} D_1 \\ \vdots \\ D_{k_j} \end{bmatrix}.$$

The corresponding node in  $\mathcal{N}^{(k_1, \dots, k_m, n)}$  generates  $k_{l_1} + \dots + k_{l_u}$  message vectors, has  $vn$  incoming edge vectors, and demands the  $k_j$  message vectors corresponding to  $x_j$ . Define the  $t$ -dimensional vector code for  $\mathcal{N}^{(k_1, \dots, k_m, n)}$  over  ${}_R G$  by letting the decoding function, corresponding to the  $i$ th such message vector, be the linear mapping

$$d_i : \underbrace{G^t \times \dots \times G^t}_{k_{l_1} + \dots + k_{l_u} \text{ message vectors}} \times \underbrace{G^t \times \dots \times G^t}_{vn \text{ edge vectors}} \longrightarrow G^t$$

given by  $d_i(\mathbf{x}) = D_i \mathbf{x}$ , where  $i = 1, \dots, k_j$ . If the function  $d$  correctly reproduces its demanded message vectors in the  $(tk_1, \dots, tk_m, tn)$  code for  $\mathcal{N}$ , then each of  $d_1, \dots, d_{k_j}$  correctly reproduces its demanded message vector in the  $t$ -dimensional code for  $\mathcal{N}^{(k_1, \dots, k_m, n)}$ . Hence, any  $(tk_1, \dots, tk_m, tn)$  linear solution over a module  ${}_R G$  for  $\mathcal{N}$  can be translated to a  $t$ -dimensional vector linear solution over  ${}_R G$  for  $\mathcal{N}^{(k_1, \dots, k_m, n)}$ .

A  $t$ -dimensional vector linear solution over the module  ${}_R G$  for  $\mathcal{N}^{(k_1, \dots, k_m, n)}$  can similarly be translated to a  $(tk_1, \dots, tk_m, tn)$  linear solution over  ${}_R G$  for  $\mathcal{N}$ . In particular, if  $f_1, \dots, f_n$  are the edge functions of the  $n$  parallel edges at a node in a  $t$ -dimensional vector linear solution for  $\mathcal{N}^{(k_1, \dots, k_m, n)}$ , then in the

$(tk_1, \dots, tk_m, tn)$  linear code over for  $\mathcal{N}$ , define the corresponding edge function to be

$$f(\mathbf{x}) = \begin{bmatrix} f_1(\mathbf{x}) \\ \vdots \\ f_n(\mathbf{x}) \end{bmatrix}.$$

Similarly, if  $d_1, \dots, d_{k_j}$  are the decoding functions at a node in a  $t$ -dimensional vector linear solution for  $\mathcal{N}^{(k_1, \dots, k_m, n)}$ , then in the  $(tk_1, \dots, tk_m, tn)$  linear code over for  $\mathcal{N}$ , define the corresponding decoding function  $d(\mathbf{x})$  to be the vector obtained by concatenating  $d_1(\mathbf{x}), \dots, d_{k_j}(\mathbf{x})$ . This  $(tk_1, \dots, tk_m, tn)$  linear code for  $\mathcal{N}$  over  ${}_R G$  is a solution, since the  $t$ -dimensional vector linear code for  $\mathcal{N}^{(k_1, \dots, k_m, n)}$  is a solution. ■

When  ${}_R G$  is a module and  $t$  is a positive integer,  $M_t({}_R G)$  denotes the module in which the ring of all  $t \times t$  matrices with entries in  $R$  acts on the set of all  $t$ -vectors over  $G$  with matrix-vector multiplication, where multiplication of elements of  $R$  with elements of  $G$  is given by the action of  ${}_R G$ . The following lemma shows an equivalence between fractional linear codes over modules and fractional linear codes over these vector modules.

**Lemma 4.2.3.** *Let  ${}_R G$  be a module, let  $\mathcal{N}$  be a network, and let  $k_1, \dots, k_m \geq 0$  and  $n, t \geq 1$  be integers. Network  $\mathcal{N}$  has a  $(k_1, \dots, k_m, n)$  linear solution over  $M_t({}_R G)$  if and only if  $\mathcal{N}$  has a  $(tk_1, \dots, tk_m, tn)$  linear solution over  ${}_R G$ .*

*Proof.* This lemma follows from the fact that a scalar linear solution over  $M_t({}_R G)$  is equivalent to a  $t$ -dimensional vector linear solution over  ${}_R G$ . In particular, in both a scalar linear code over  $M_t({}_R G)$  and a  $t$ -dimensional vector linear code over  ${}_R G$ , inputs to a node are  $t$ -vectors over  $G$  and outputs carry linear combinations of the inputs, where the coefficients that describe the linear combination are  $t \times t$  matrices over  $R$ . Any scalar linear solution over  $M_t({}_R G)$  can be translated to a  $t$ -dimensional vector linear solution over  ${}_R G$  and vice versa. This idea generalizes to fractional linear solutions:

$$\begin{aligned} &\mathcal{N} \text{ has a } (k_1, \dots, k_m, n) \text{ linear solution over } M_t({}_R G) \\ \iff &\mathcal{N}^{(k_1, \dots, k_m, n)} \text{ has a scalar linear solution over } M_t({}_R G) && \text{[from cap-Lemma 4.2.2]} \\ \iff &\mathcal{N}^{(k_1, \dots, k_m, n)} \text{ has a } t\text{-dimensional linear solution over } {}_R G \\ \iff &\mathcal{N} \text{ has a } (tk_1, \dots, tk_m, tn) \text{ linear solution over } {}_R G && \text{[from cap-Lemma 4.2.2]}. \end{aligned}$$

■



## 4.2.2 Fractional Dominance

**Definition 4.2.4.** Let  ${}_R G$  and  ${}_S H$  be modules. We say that

- (a)  ${}_S H$  *scalarly dominates*  ${}_R G$  if every network with a scalar linear solution over  ${}_R G$  also has a scalar linear solution over  ${}_S H$ ,
- (b)  ${}_S H$  *fractionally dominates*  ${}_R G$  if for each  $k_1, \dots, k_m \geq 0$  and  $n \geq 1$ , every network with a  $(k_1, \dots, k_m, n)$  linear solution over  ${}_R G$  also has a  $(k_1, \dots, k_m, n)$  linear solution over  ${}_S H$ .

**Remark 4.2.5.** Any left-sided fractional linear code over a ring can be viewed as a two-sided fractional linear code over the ring in which the inputs are multiplied on the right by the identity element, so the module  ${}_{R \otimes R^{op}} R$  fractionally dominates  ${}_R R$  for every finite ring  $R$ . Furthermore, if  $R$  is commutative, then any two-sided fractional linear code over  $R$  can equivalently be written as a left-sided fractional linear code over  $R$ , which implies  ${}_R R$  fractionally dominates  ${}_{R \otimes R^{op}} R$ .

We also comment that if  $R$  and  $S$  are finite rings such that  ${}_{S \otimes S^{op}} S$  fractionally dominates  ${}_{R \otimes R^{op}} R$ , then for each network  $\mathcal{N}$ , we have

$$\mathcal{R}_{lin}(\mathcal{N}, S) \supseteq \mathcal{R}_{lin}(\mathcal{N}, R) \quad \text{and} \quad \mathcal{C}_{lin}(\mathcal{N}, S) \supseteq \mathcal{C}_{lin}(\mathcal{N}, R).$$

The following lemma shows that scalar dominance and fractional dominance of modules are, in fact, equivalent. However, it is cleaner to prove results on scalar dominance, as the block sizes of the message vectors and edge vectors are all one, and we can use results from Chapter 3.

**Lemma 4.2.6.** Let  ${}_R G$  and  ${}_S H$  be modules.  ${}_S H$  scalarly dominates  ${}_R G$  if and only if  ${}_S H$  fractionally dominates  ${}_R G$ .

*Proof.* It follows immediately from the definition that  ${}_S H$  fractionally dominates  ${}_R G$  implies  ${}_S H$  scalarly dominates  ${}_R G$ . To prove the converse, suppose  ${}_S H$  scalarly dominates  ${}_R G$ . Let  $\mathcal{N}$  be a network with  $m$  message vectors, let  $k_1, \dots, k_m \geq 0$  and  $n \geq 1$  be integers, and let  $\mathcal{N}^{(k_1, \dots, k_m, n)}$  be the network in Definition 4.2.1 corresponding to  $\mathcal{N}$ ,  $k_1, \dots, k_m$ , and  $n$ . Then

$$\begin{aligned} & \mathcal{N} \text{ has a } (k_1, \dots, k_m, n) \text{ linear solution over } {}_R G \\ \implies & \mathcal{N}^{(k_1, \dots, k_m, n)} \text{ has a scalar linear solution over } {}_R G && \text{[from cap-Lemma 4.2.2]} \\ \implies & \mathcal{N}^{(k_1, \dots, k_m, n)} \text{ has a scalar linear solution over } {}_S H && \text{[from } S \text{ scalarly dominates } R\text{]} \\ \implies & \mathcal{N} \text{ has a } (k_1, \dots, k_m, n) \text{ linear solution over } {}_S H && \text{[from cap-Lemma 4.2.2]}. \end{aligned}$$

Hence, for any network, any fractional linear solution over  ${}_R G$  implies the existence of a fractional linear solution over  ${}_S H$  with the same block sizes. ■

**Definition 4.2.7.** An  $R$ -module  $G$  is *faithful* if for each  $r \in R \setminus \{0\}$ , there exists  $g \in G$  such that  $r \cdot g \neq 0$ .

Lemmas 4.2.8, 4.2.9, and 4.2.10 follow immediately from Lemma 4.2.6 and results from Chapter 3. Lemma 4.2.8 shows that, for a fixed ring  $R$ , fractional linear solutions over faithful  $R$ -modules induce fractional linear solutions over every other  $R$ -module. Lemma 4.2.9 shows that fractional linear solutions over non-faithful modules induce fractional linear solutions over some faithful module. Lemma 4.2.10 shows that ring homomorphisms also induce fractional dominance.

**Lemma 4.2.8.** *Lemma 3.1.3: Let  $R$  be a fixed ring, let  $G$  be a faithful  $R$ -module, and let  $H$  be an  $R$ -module. Then  ${}_R H$  fractionally dominates  ${}_R G$ .*

**Lemma 4.2.9.** *Lemma 3.2.6: Let  $G$  be an  $R$ -module. There exists a finite ring  $S$  such that  $G$  is a faithful  $S$ -module, and  ${}_S G$  fractionally dominates  ${}_R G$ .*

**Lemma 4.2.10.** *Lemma 3.1.6: Let  $\phi : R \rightarrow S$  be a ring homomorphism, let  $G$  be a faithful  $R$ -module, and let  $H$  be an  $S$ -module. Then  ${}_S H$  fractionally dominates  ${}_R G$ .*

By the fundamental theorem of finite Abelian groups, every finite Abelian group is isomorphic to a direct product of cyclic groups whose sizes are prime powers (with component-wise addition) [16, p. 161]. As an example,  $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ . The following lemma shows that if a finite Abelian group can be written as a direct product of Abelian groups  $G$  and  $H$  whose sizes are relatively prime, then whenever  $G \times H$  is an  $R$ -module for some ring  $R$ , the ring  $R$  acts on  $G \times H$  component-wise. This implies that  $G$  and  $H$  are also  $R$ -modules. Since fractional linear solutions over faithful  $R$ -modules induce fractional linear solutions over every other  $R$ -module, this is a useful tool for showing fractional dominance.

**Lemma 4.2.11.** *Let  $G$  and  $H$  be finite groups such that  $|G|$  and  $|H|$  are relatively prime, and let  $G \times H$  be some  $R$ -module. Then  $G$  and  $H$  are also  $R$ -modules.*

*Proof.* Let  $g \in G$  and  $r \in R$ , and suppose  $r \cdot (g, 0) = (g_r, h_r) \in G \times H$ . It follows from Lagrange's theorem of finite groups (e.g. [16, p. 45]) that  $|G|g = \underbrace{g \oplus \cdots \oplus g}_{|G| \text{ times}} = 0$ , so

$$(0, 0) = r \cdot (0, 0) = r \cdot (|G|g, 0) = |G|r \cdot (g, 0) = |G|(g_r, h_r) = (|G|g_r, |G|h_r) = (0, |G|h_r).$$

Since  $|G|$  and  $|H|$  are relatively prime, it follows from Cauchy's theorem of finite groups (e.g. [16, p. 93]) that  $H$  contains no non-identity elements whose order divides  $|G|$ , so it must be the case that  $h_r = 0$ .

Similarly, for each  $h \in H$  and each  $r \in R$ , there exists  $h_r \in H$  such that  $r \cdot (0, h) = (0, h_r)$ . This implies  $R$  acts on  $G \times H$  component-wise. In other words, if  $r \cdot (g, h) = (g_r, h_r)$ , then  $r \cdot (g, 0) = (g_r, 0)$  and  $r \cdot (0, h) = (0, h_r)$ . Thus the mapping  $\odot : R \times G \rightarrow G$  given by  $r \odot g = g_r$  satisfies the properties of an action, so  $G$  is an  $R$ -module with action  $\odot$ . It can similarly be shown  $H$  is an  $R$ -module. ■

We comment that Lemma 4.2.11 does not extend to finite groups whose sizes are not relatively prime. As an example, the field  $\text{GF}(4)$  acts on its own additive group  $(\text{GF}(4), +)$  by multiplication in the field. If the elements of  $\text{GF}(4)$  are represented as  $\{0, 1, \alpha, \alpha + 1\}$  where  $\alpha^2 = \alpha + 1$ , then for all  $(a_0 + \alpha a_1), (b_0 + \alpha b_1) \in \text{GF}(4)$

$$(a_0 + \alpha a_1)(b_0 + \alpha b_1) = a_0 b_0 + a_1 b_1 + \alpha(a_0 b_1 + a_1 b_0 + a_1 b_1).$$

The additive group of  $\text{GF}(4)$  is isomorphic to the set  $\text{GF}(2) \times \text{GF}(2)$  with component-wise addition in  $\text{GF}(2)$ , so  $\text{GF}(4)$  acts on  $\text{GF}(2) \times \text{GF}(2)$  by

$$(a_0 + \alpha a_1) \cdot (b_0, b_1) = (a_0 b_0 + a_1 b_1, a_0 b_1 + a_1 b_0 + a_1 b_1).$$

This action is not component-wise, since  $(1 + \alpha) \cdot (1, 0) = (1, 1)$  and  $\alpha \cdot (0, 1) = (1, 1)$ .

If  $\text{GF}(4)$  acts on  $\text{GF}(2)$ , then the action must be such that  $1 \cdot a = a$  and  $0 \cdot a = 0$  for all  $a \in \text{GF}(2)$  and  $x \cdot 0 = 0$  for all  $x \in \text{GF}(4)$ . If  $\alpha \cdot 1 = 1$ , then

$$0 = 1 + 1 = (\alpha \cdot 1) + (1 \cdot 1) = (\alpha + 1) \cdot 1 = (\alpha^2) \cdot 1 = \alpha \cdot (\alpha \cdot 1) = \alpha \cdot 1 = 1$$

which is a contradiction. If  $\alpha \cdot 1 = 0$ , then

$$1 = 0 + 1 = (\alpha \cdot 1) + (1 \cdot 1) = (\alpha + 1) \cdot 1 = (\alpha^2) \cdot 1 = \alpha \cdot (\alpha \cdot 1) = \alpha \cdot 0 = 0$$

which is a contradiction. Thus  $\text{GF}(2)$  cannot be a  $\text{GF}(4)$ -module, but as shown above,  $\text{GF}(2) \times \text{GF}(2)$  is a  $\text{GF}(4)$ -module.

### 4.2.3 Matrix Rings over Fields

If a ring  $R$  has a proper two-sided ideal  $I$ , then there is a surjective homomorphism from  $R$  to  $R/I$ . It is known (e.g. [32, p. 20]) that every finite ring with no proper two-sided ideals is isomorphic to some ring of matrices over a finite field. In fact, every finite ring  $R$  has a two-sided ideal  $I$  such that  $R/I$  is a matrix ring over a field. This implies the following lemma, which was more formally shown in Chapter 3.

**Lemma 4.2.12.** *Lemmas 3.2.1 and 3.2.3: Let  $R$  be a finite ring. There exists a positive integer  $t$ , a finite field  $\mathbb{F}$ , and a surjective homomorphism from  $R$  to  $M_t(\mathbb{F})$ .*

Lemmas 4.2.10 and 4.2.12 together imply that fractional linear solutions over modules induce fractional linear solutions over modules in which the ring is a matrix ring over a field. The following lemma proves a result on the cardinality of such modules.

**Lemma 4.2.13.** *Let  $\mathbb{F}$  be a finite field and  $t$  a positive integer. If  $G$  is a finite non-zero  $M_t(\mathbb{F})$ -module, then  $|\mathbb{F}|^t$  divides  $|G|$ .*

*Proof.* Since  $G$  is finite and non-zero,  $G$  contains a submodule with no proper submodules (possibly  $G$  itself). It is known (e.g. [27, Theorem 3.3 (2), p. 31]) that  $\mathbb{F}^t$  is the only  $M_t(\mathbb{F})$ -module with no proper submodules, so  $\mathbb{F}^t$  is a submodule of  $G$ . Hence by Lagrange's theorem of finite groups,  $|\mathbb{F}|^t$  divides  $|G|$ . ■

Lemma 4.2.14 shows that every module is fractionally dominated by a module whose group is the set of  $t$  vectors over some field and whose ring is the set of all  $t \times t$  matrices over the field. In network coding, arbitrarily large block sizes may be needed to achieve a solution with a particular rate. Das and Rai [10] showed that for each  $k, n \geq 1$  and each  $t \geq 2$ , there exists a network that has a  $(tk, \dots, tk, tn)$  linear solution over any finite field, yet the network has no  $(sk, \dots, sk, sn)$  linear solution over any finite field when  $s < t$ . It was also shown in Chapter 3 that for each  $t \geq 2$ , there exist networks with scalar linear solutions over certain rings but with no  $s$ -dimensional vector linear solutions over any field whenever  $s < t$ . This suggests that the quantity  $t$  in Lemma 4.2.14 may need to be arbitrarily large.

**Lemma 4.2.14.** *Let  ${}_R G$  be a module. For each prime  $p$  that divides  $|G|$ , there exists a finite field  $\mathbb{F}$  of characteristic  $p$  and a positive integer  $t$  such that  ${}_{M_t(\mathbb{F})} \mathbb{F}^t$  fractionally dominates  ${}_R G$ .*

*Proof.* By Lemma 4.2.9 there exists a finite ring  $S$  such that the faithful module  ${}_S G$  fractionally dominates  ${}_R G$ . By the fundamental theorem of finite Abelian groups, the group  $G$  is isomorphic to a direct product of Abelian groups whose sizes are prime powers, and since  $p \mid |G|$ , the size of at least one of these groups is a power of  $p$ . Let  $H$  be the direct product of all such groups whose sizes are powers of  $p$ . Then there exists a finite group  $G'$  such that  $G \cong G' \times H$  and  $|G'|$  and  $|H|$  are relatively prime. Hence by Lemma 4.2.11,  $H$  is also an  $S$ -module, and since  $G$  is a faithful  $S$ -module, by Lemma 4.2.8, the module  ${}_S H$  fractionally dominates  ${}_S G$ .

By Lemma 4.2.9, there exists a finite ring  $S'$  such that  $H$  is a faithful  $S'$ -module and  ${}_S H$  fractionally dominates  ${}_S H$ . By Lemma 4.2.12, there exists a positive integer  $t$ , a finite field  $\mathbb{F}$ , and a surjective homomorphism from  $S'$  to  $M_t(\mathbb{F})$ . By Lemma 4.2.10, the module  ${}_S H$  is fractionally dominated by every  $M_t(\mathbb{F})$ -module, and the ring  $M_t(\mathbb{F})$  acts on the of all  $t$ -vectors over  $\mathbb{F}$  by matrix-vector multiplication over  $\mathbb{F}$ , so  ${}_{M_t(\mathbb{F})} \mathbb{F}^t$  fractionally dominates  ${}_S H$ . The proof of Lemma 4.2.10 also implies  $H$  is an  $M_t(\mathbb{F})$ -module,

so Lemma 4.2.13 implies  $|\mathbb{F}|^t \mid |H|$ . Since  $|H|$  is a power of  $p$ , this implies  $\mathbb{F}$  is a field of characteristic  $p$ . Finally, by the transitivity of fractional dominance,  $M_t(\mathbb{F})\mathbb{F}^t$  fractionally dominates  ${}_R G$ . ■

Lemma 4.2.15 uses ideas similar to those in [38, Proposition 1] and [17], and we include a proof for completeness. This lemma, along with Lemma 4.2.3, implies that a fractional linear solution over any non-prime finite field induces a fractional linear solution over the corresponding prime field with the same rate vector. A fractional linear solution over a field  $\mathbb{F}$  is equivalent to a fractional linear solution over the faithful module  ${}_{\mathbb{F}}\mathbb{F}$ , since  $\text{GF}(\mathbb{F})$  is commutative.

**Lemma 4.2.15.** *Let  $q$  be a prime power and  $t$  a positive integer. Then  $M_t(\text{GF}(q))\text{GF}(q)^t$  fractionally dominates  ${}_{\text{GF}(q^t)}\text{GF}(q^t)$ .*

*Proof.* It is known (e.g. see [16, p. 531]) that every extension field  $\text{GF}(q^t)$  is isomorphic to a set of  $t \times t$  matrices over  $\text{GF}(q)$ . This implies there exists an injective homomorphism from  $\text{GF}(q^t)$  to  $M_t(\text{GF}(q))$ . By Lemma 4.2.10, any network with a fractional linear solution over  ${}_{\text{GF}(q^t)}\text{GF}(q^t)$  also has a fractional linear solution over any  $M_t(\text{GF}(q))$ -module. In particular,  $M_t(\text{GF}(q))\text{GF}(q)^t$  fractionally dominates  ${}_{\text{GF}(q^t)}\text{GF}(q^t)$ . ■

### 4.3 Linear Rate Regions over Fields

We define, for each integer  $m \geq 2$ , the *Char- $m$  Network* in Figure 4.3. The Char- $m$  Network is denoted by  $\mathcal{N}_2(m, 1)$  in [7], with a slight relabeling of sources, and Char- $m$  Network is known to be vector linearly solvable over a field if and only if the characteristic of the field divides  $m$ . When  $m = 2$ , this network exhibits solvability properties similar to those of the Fano network [13].

Let  $R$  be a finite ring whose characteristic divides  $m$ . Then  $m = 0$  in  $R$ , and the following scalar linear code:

$$e = \sum_{j=0}^{m+1} x_j \quad \text{and} \quad e_i = \sum_{\substack{j=0 \\ j \neq i}}^{m+1} x_j$$

over  $R$  is a solution for the Char- $m$  Network, where  $i = 0, 1, \dots, m+1$ , and the receivers linearly recover their demands as follows

$$\begin{aligned} R_i : e - e_i &= x_i \\ R : \sum_{i=1}^{m+1} e_i &= x_0 + m \sum_{i=0}^{m+1} x_i \\ &= x_0 \qquad \qquad \qquad [\text{from char}(R) \mid m]. \end{aligned}$$

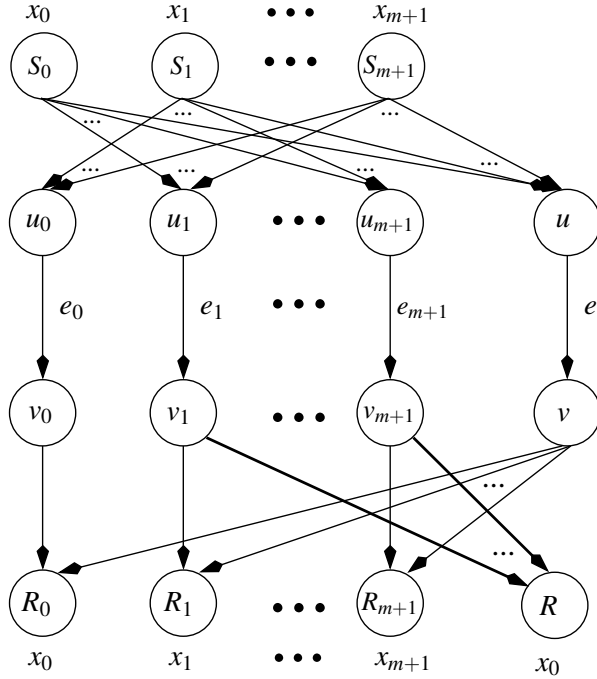


Figure 4.3: The Char- $m$  Network has source nodes  $S_0, S_1, \dots, S_{m+1}$  which generate message vectors  $x_0, x_1, \dots, x_{m+1}$ , respectively. Node  $u$  has a single incoming edge from each source node, and the edge connecting nodes  $u$  and  $v$  carries the edge vector  $e$ . For each  $i = 0, 1, \dots, m+1$ , node  $u_i$  has a single incoming edge from each source node, except  $S_i$ . The edge connecting nodes  $u_i$  and  $v_i$  carries edge vector  $e_i$ . The receiver  $R_i$  demands  $x_i$  and has an incoming edge from node  $v_i$  and an incoming edge from  $v$ . The receiver  $R$  demands  $x_0$  and has an incoming edge from each of nodes  $v_1, \dots, v_{m+1}$ .

This code relies on the fact  $m = 0$  in  $R$ , and it turns out the Char- $m$  Network has no scalar linear solutions over any ring whose characteristic does not divide  $m$  (see [7, Lemma IV.6]).

**Lemma 4.3.1.** [7, Lemma IV.7]: For each  $m \geq 2$  and each finite field  $\mathbb{F}$ , the linear capacity of the Char- $m$  Network is

- equal to 1, whenever  $\text{char}(\mathbb{F}) \mid m$ , and
- upper bounded by  $1 - \frac{1}{2m+3}$ , whenever  $\text{char}(\mathbb{F}) \nmid m$ .

### 4.3.1 Comparing Linear Rate Regions over Different Fields

It follows from Lemma 4.3.1 that certain fields may yield strictly larger linear capacities for some networks than other fields. In particular, whenever the characteristics of two finite fields are different, there exists some network whose linear capacities over the fields differ.

**Corollary 4.3.2.** *If  $\mathbb{F}$  and  $\mathbb{K}$  are finite fields with different characteristics, then there exist networks  $\mathcal{N}_1$  and  $\mathcal{N}_2$ , such that  $\mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{F}) > \mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{K})$  and  $\mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{K}) > \mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{F})$ .*

*Proof.* Suppose  $\text{char}(\mathbb{F}) = p \neq q = \text{char}(\mathbb{K})$  and let  $\mathcal{N}_1$  and  $\mathcal{N}_2$  be the Char- $p$  Network and the Char- $q$  Network, respectively. Then by Lemma 4.3.1,  $\mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{F}) = 1$  and  $\mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{K}) \leq 1 - \frac{1}{2p+3}$ . Similarly,  $\mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{K}) = 1$  and  $\mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{F}) \leq 1 - \frac{1}{2q+3}$ . ■

In [14], it was shown that for any finite fields  $\mathbb{F}$  and  $\mathbb{K}$  of even and odd characteristic, respectively: (i) the linear rate region of the non-Fano network over  $\mathbb{F}$  is a proper subset of its linear rate region over  $\mathbb{K}$ , and (ii) the linear rate region of the Fano network over  $\mathbb{K}$  is a proper subset of its linear rate region over  $\mathbb{F}$ . In these instances, it is strictly “better” to use an even/odd characteristic field instead of an odd/even characteristic field. However, the following theorem demonstrates that it may not always be the case that one field is necessarily “better” than the other for a particular network. In particular, for some networks, some rate vectors may only be linearly achievable over certain fields while other rate vectors may only be linearly achievable over other fields.

**Theorem 4.3.3.** *For any two finite fields with different characteristics, there exists a network whose linear rate regions over the fields do not contain one another.*

*Proof.* A disjoint union of networks refers to a new network whose nodes/edges/sources/receivers are the disjoint union of the nodes/edges/sources/receivers in the smaller networks. Let  $\mathbb{F}$  and  $\mathbb{K}$  be finite fields of characteristic  $p$  and  $q$ , for some distinct primes  $p$  and  $q$ . Let  $\mathcal{N}$  be the disjoint union of the Char- $p$  Network and the Char- $q$  Network. Whenever node (respectively, edge and message) labels are repeated, add an arbitrary additional level of labeling each node (respectively, edge and message) to avoid repeated labels. Then, by Lemma 4.3.1, the rate vector, in which the rates for the Char- $p$  Network are all one and the rates for the Char- $q$  Network are all zero, is linearly achievable over  $\mathbb{F}$  but not over  $\mathbb{K}$ . Similarly, the rate vector in which the rates for the Char- $q$  Network are all one and the rates for the Char- $p$  Network are all zero is linearly achievable over  $\mathbb{K}$  but not over  $\mathbb{F}$ . Thus the linear rate regions of  $\mathcal{N}$  over  $\mathbb{F}$  and  $\mathbb{K}$  do not contain one another. ■

We can use a similar network construction to show that there is not necessarily a particular finite field that can linearly achieve all linearly achievable rate vectors. In other words, there may not be a “best” field for a particular network. Let  $p$  and  $q$  be distinct primes, and let  $\mathcal{N}$  be the disjoint union of the Char- $p$

Network and the Char- $q$  Network. Then, by a similar argument to the proof of Theorem 4.3.3, there exists a rate vector that is only linearly achievable over fields of characteristic  $p$ , and there exists another rate vector that is only linearly achievable over fields of characteristic  $q$ . Thus there is no finite field which can linearly achieve both of these rate vectors. A similar result can be obtained by taking the disjoint union of the Fano and non-Fano networks.

Theorem 4.3.3 demonstrates that for any two finite fields of distinct characteristics, there always exists some network whose linear rate regions differ over the two fields. In the following theorem, we show that the linear rate region of a network over a field depends only on the characteristic of the field. This contrasts with the scalar linear solvability of networks over fields, since some networks can be scalar linearly solvable only over certain fields of a given characteristic.

**Theorem 4.3.4.** *Let  $\mathbb{F}$  and  $\mathbb{K}$  be finite fields. Then  $\text{char}(\mathbb{F}) = \text{char}(\mathbb{K})$  if and only if for each network  $\mathcal{N}$ , we have  $\mathcal{R}_{\text{lin}}(\mathcal{N}, \mathbb{F}) = \mathcal{R}_{\text{lin}}(\mathcal{N}, \mathbb{K})$ .*

*Proof.* Let  $r$  and  $s$  be positive integers,  $p$  a prime, and  $\mathcal{N}$  a network with  $m$  messages. Then  $\text{GF}(p)$  is a subfield  $\text{GF}(p^s)$ , which implies the identity mapping is an injective homomorphism from  $\text{GF}(p)$  to  $\text{GF}(p^s)$ . So

$$\begin{aligned} \mathcal{N} \text{ has a } (k_1, \dots, k_m, n) \text{ linear solution over } \text{GF}(p^r) \\ \implies \mathcal{N} \text{ has an } (rk_1, \dots, rk_m, rn) \text{ linear solution over } \text{GF}(p) & \quad [\text{from cap-Lemma 4.2.15}] \\ \implies \mathcal{N} \text{ has an } (rk_1, \dots, rk_m, rn) \text{ linear solution over } \text{GF}(p^s) & \quad [\text{from cap-Lemma 4.2.10}]. \end{aligned}$$

Both a  $(k_1, \dots, k_m, n)$  linear solution and a  $(rk_1, \dots, rk_m, rn)$  linear solution have the rate vector  $(k_1/n, \dots, k_m/n)$ . Hence any rate vector that is linearly attainable over  $\text{GF}(p^r)$  is also linearly attainable over  $\text{GF}(p^s)$  (with possibly larger vector sizes). Similarly, any rate vector that is linearly attainable over  $\text{GF}(p^s)$  is also linearly attainable over  $\text{GF}(p^r)$  (with possibly larger vector sizes). Hence if  $\text{char}(\mathbb{F}) = \text{char}(\mathbb{K})$ , then the linear rate regions of any network over  $\mathbb{F}$  and  $\mathbb{K}$  are equal. The reverse direction follows from Theorem 4.3.3. ■

Immediately following Definition 4.2.4, we showed that for any finite rings  $S$  and  $R$ ,

$$S \otimes_{S \otimes_{\mathbb{F}} S} S \text{ fractionally dominates } R \otimes_{R \otimes_{\mathbb{F}} R} R \implies \mathcal{R}_{\text{lin}}(\mathcal{N}, S) \supseteq \mathcal{R}_{\text{lin}}(\mathcal{N}, R) \text{ for every network } \mathcal{N}.$$



Theorem 4.3.4 can be used to show the converse is not necessarily true. There are numerous examples in the literature (e.g. see Lemma 2.3.2, [37], [39]) of networks that are scalar linearly solvable over  $\text{GF}(p^r)$  but not over  $\text{GF}(p^s)$ , for some prime  $p$  and some distinct positive integers  $r$  and  $s$ . In such cases,  $\text{GF}(p^s)$  does not fractionally dominates  $\text{GF}(p^r)$ ; however, by Theorem 4.3.4, any network's linear rate region over either field is the same, since both fields have characteristic  $p$ .

**Corollary 4.3.5.** *Let  $\mathbb{F}$  and  $\mathbb{K}$  be finite fields. Then  $\text{char}(\mathbb{F}) = \text{char}(\mathbb{K})$  if and only if for each network  $\mathcal{N}$ , we have  $\mathcal{C}_{\text{lin}}(\mathcal{N}, \mathbb{F}) = \mathcal{C}_{\text{lin}}(\mathcal{N}, \mathbb{K})$ .*

*Proof.* This corollary is an immediate consequence of Theorem 4.3.4 and Corollary 4.3.2. ■

## 4.4 Linear Rate Regions over Rings

The following theorem demonstrates that if a network has a fractional linear solution over some module and if  $p$  is a prime that divides the alphabet size (i.e. the size of the group), then the network must also have a fractional linear solution over every field of characteristic  $p$  with the same rate vector and possibly larger vector sizes.

**Theorem 4.4.1.** *Let  ${}_R G$  be a module and let  $\mathbb{F}$  be a finite field whose characteristic divides  $|G|$ . For each network  $\mathcal{N}$  and each  $k_1, \dots, k_m \geq 0$  and  $n \geq 1$  such that  $\mathcal{N}$  has a  $(k_1, \dots, k_m, n)$  linear solution over  ${}_R G$ , there exists a positive integer  $t$  such that  $\mathcal{N}$  has a  $(tk_1, \dots, tk_m, tn)$  linear solution over  $\mathbb{F}$ .*

*Proof.* Let  $p = \text{char}(\mathbb{F})$ . By Lemma 4.2.14, there exists a finite field  $\mathbb{K}$  of characteristic  $p$  and a positive integer  $s$  such that  ${}_{M_s(\mathbb{K})} \mathbb{K}^s$  fractionally dominates  ${}_R G$ . Lemma 4.2.3 implies a network  $\mathcal{N}$  with a  $(k_1, \dots, k_m, n)$  linear solution over  ${}_{M_s(\mathbb{K})} \mathbb{K}^s$  must also have an  $(sk_1, \dots, sk_m, sn)$  linear solution over  $\mathbb{K}$ . Since  $\mathbb{F}$  and  $\mathbb{K}$  both have characteristic  $p$ , and since the rate vector  $(k_1/n, \dots, k_m/n)$  is linearly achievable for  $\mathcal{N}$  over  $\mathbb{K}$ , by Theorem 4.3.4, the rate vector  $(k_1/n, \dots, k_m/n)$  is also linearly achievable for  $\mathcal{N}$  over  $\mathbb{F}$ . Hence there exists a positive integer  $t$  such that  $\mathcal{N}$  has a  $(tk_1, \dots, tk_m, tn)$  linear solution over  $\mathbb{F}$ . ■

We now prove one of our main results regarding linear rate regions over rings.

**Theorem 4.4.2.** *If  $R$  is a finite ring and  $\mathbb{F}$  is a finite field whose characteristic divides  $|R|$ , then the linear rate region of any network over  $R$  is contained in the network's linear rate region over  $\mathbb{F}$ .*

*Proof.* Let  $R$  be a finite ring, let  $\mathcal{N}$  be a network, and let  $\mathbb{F}$  finite field whose characteristic divides  $|R|$ . A fractional two-sided linear solution over  $R$  is a fractional linear solution over the module  ${}_{R\otimes R^{op}}R$ , so by Theorem 4.4.1, whenever  $\mathcal{N}$  has a fractional linear solution over  $R$  with a given rate vector,  $\mathcal{N}$  also has a fractional linear solution over  $\mathbb{F}$  with the same rate vector and possibly larger vector sizes. Hence,

$$\{\mathbf{r} \in \mathbb{Q}^m : \mathbf{r} \text{ is linearly achievable for } \mathcal{N} \text{ over } R\} \subseteq \{\mathbf{r} \in \mathbb{Q}^m : \mathbf{r} \text{ is linearly achievable for } \mathcal{N} \text{ over } \mathbb{F}\}.$$

■

**Corollary 4.4.3.** *If  $R$  is a finite ring and  $\mathbb{F}$  is a finite field whose characteristic divides  $|R|$ , then the linear capacity of any network over  $R$  at most its linear capacity over  $\mathbb{F}$ .*

In some cases, the containment in Theorem 4.4.2 (and the inequality in Corollary 4.4.3) is strict for some networks, while in other cases, there may be equality for all networks. As an example, by taking  $\mathbb{F} = \text{GF}(2)$  and  $R = \mathbb{Z}_6$  in Theorem 4.4.2, any network's linear rate region over  $\text{GF}(2)$  contains its linear rate region over  $\mathbb{Z}_6$ . However, the linear capacity of the Char-2 Network is 1 over the field  $\text{GF}(2)$  and is upper bounded by  $6/7$  over the field  $\text{GF}(3)$  (see Lemma 4.3.1). Since  $3 = \text{char}(\text{GF}(3))$ , which divides  $6 = |\mathbb{Z}_6|$ , by Theorem 4.4.2, the Char-2 Network's linear capacity over  $\mathbb{Z}_6$  is upper bounded by  $6/7$ . This demonstrates that the linear rate regions of  $R$  and  $\mathbb{F}$  are not necessarily equal for all networks.

As another example, by taking  $\mathbb{F} = \text{GF}(4)$  and  $R = \mathbb{Z}_2[X]/\langle X^2 \rangle$  in Theorem 4.4.2, any network's linear rate region over  $\text{GF}(4)$  contains its linear rate region over  $\mathbb{Z}_2[X]/\langle X^2 \rangle$ . The field  $\text{GF}(2)$  is isomorphic to a subring of  $\mathbb{Z}_2[X]/\langle X^2 \rangle$  (namely  $\mathbb{Z}_2$ ), so there is an injective homomorphism from  $\text{GF}(2)$  to  $\mathbb{Z}_2[X]/\langle X^2 \rangle$ , which by Lemma 4.2.10, implies any network's linear rate region over  $\mathbb{Z}_2[X]/\langle X^2 \rangle$  contains its linear rate region over  $\text{GF}(2)$ . However, by Theorem 4.3.4, any network's linear rate regions over  $\text{GF}(4)$  and  $\text{GF}(2)$  must be equal. Thus the linear rate regions of  $\text{GF}(4)$  and  $\mathbb{Z}_2[X]/\langle X^2 \rangle$  are equal for all networks. Precisely characterizing for which rings and fields the linear rate regions are equal for all networks remains an open problem.

#### 4.4.1 Comparing Linear Capacities over Different Rings

Determining the exact linear capacity and the linear rate region of the Char- $m$  Network over each finite ring (or even each finite field) is also presently an open problem. Another related open question is for which finite rings  $R$  and  $S$  does there exist a network  $\mathcal{N}$  such that  $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, S)$ . We have answered this second question in some select special cases:

- In Theorem 4.3.4, we showed that when  $R$  and  $S$  are finite fields, such a network exists if and only if the characteristics of  $R$  and  $S$  differ.
- In Theorem 4.4.2, we showed that when  $S$  is a field whose characteristic divides  $|R|$ , no such network exists. This includes the special case where  $|S| = |R|$ .

**Corollary 4.4.4.** *Let  $R$  and  $S$  be finite rings. If some prime factor of  $|S|$  is not a factor of  $|R|$ , then there exists a network  $\mathcal{N}$  such that  $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, S)$ .*

*Proof.* Let  $p$  divide  $|S|$  but not  $|R|$ , and let  $\mathcal{N}$  denote the Char- $|R|$  Network. Then,

$$\begin{aligned}
\mathcal{C}_{lin}(\mathcal{N}, S) &\leq \mathcal{C}_{lin}(\mathcal{N}, \text{GF}(p)) && \text{[from Theorem 4.4.2]} \\
&\leq 1 - \frac{1}{2|R|+3} && \text{[from } p \nmid |R| \text{ and Lemma 4.3.1]} \\
&< 1 \\
&\leq \mathcal{C}_{lin}(\mathcal{N}, R) && \text{[from } \text{char}(R) \mid |R|\text{]}
\end{aligned}$$

where the last inequality uses the fact that  $\mathcal{N}$  must be scalar linearly solvable over  $R$ , since the characteristic of  $R$  divides the size of  $R$ . ■

Corollary 4.4.4 implies that if the sizes of two rings do not share the same set of prime factors, then at least one of the rings induces a higher linear capacity than the other on some network. As an example, the Char-6 Network has a strictly larger linear capacity over the ring  $\mathbb{Z}_6$  than over the field  $\text{GF}(25)$  of larger size.

Corollary 4.4.4, in particular, implies that for *every* finite field and *every* ring, whose sizes are relatively prime, there is *some* network for which the linear capacity of the network over the ring is strictly larger than the linear capacity over the field. In contrast, Theorem 4.4.2 shows that for *every* ring and *every* network, there is *some* field for which the linear capacity of the network over the ring is less than or equal to the linear capacity over the field. These facts are succinctly summarized in the following theorem.

**Theorem 4.4.5.** *Let  $\mathbb{F}$  be a finite field and  $R$  be a finite ring. Then  $|\mathbb{F}|$  and  $|R|$  are relatively prime if and only if there exists a network  $\mathcal{N}$  such that  $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, \mathbb{F})$ .*

*Proof.* Let  $p = \text{char}(\mathbb{F})$ . Then  $|\mathbb{F}|$  and  $|R|$  are relatively prime if and only if  $p \nmid |R|$ .

If  $p \nmid |R|$ , then by Corollary 4.4.4, there exists a network  $\mathcal{N}$  such that  $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, \mathbb{F})$ .

The converse is a restatement of Corollary 4.4.3. ■

## 4.4.2 Asymptotic Solvability

We say that a network  $\mathcal{N}$  is *asymptotically solvable over*  $\mathcal{A}$  if for all  $\varepsilon \in (0, 1)$ , the rate vector  $(1 - \varepsilon, \dots, 1 - \varepsilon)$  is contained in the network's rate region. In other words, a uniform rate arbitrarily close to, or above, 1 is attainable. A network which is asymptotically solvable but is not solvable was demonstrated in [12], and non-linearly solvable networks were demonstrated in [7] and [11] that are not asymptotically linearly solvable over any finite field. The following corollary demonstrates that such networks are additionally not asymptotically linearly solvable over any module (or ring).

**Corollary 4.4.6.** *If a network is asymptotically linearly solvable over some module or ring, then it must be asymptotically linearly solvable over some finite field.*

*Proof.* Suppose a network  $\mathcal{N}$  is asymptotically linearly solvable over some module  ${}_R G$ . By Theorem 4.4.1, there exists a finite field  $\mathbb{F}$  such that any rate vector that is linearly achievable over  ${}_R G$  must also be linearly achievable over  $\mathbb{F}$ . Hence  $\mathcal{N}$  is also asymptotically linearly solvable over  $\mathbb{F}$ . This also implies any network that is asymptotically linearly solvable over some ring must also be asymptotically linearly solvable over some field, since a fractional linear code over a ring is a special case of a fractional linear code over a module. ■

## 4.5 Concluding Remarks

Linear network codes over finite rings (and modules) constitutes a much broader class of codes than linear network codes over finite fields. Linear codes over rings have many of the attractive properties of linear codes over fields, including implementation complexity and possibly mathematical tractability. We have demonstrated, however, that with respect to linear capacity and linear rate regions, this broader class of codes does *not* offer an improvement over linear codes over fields. This particularly contrasts with the network solvability problem where we demonstrated certain cases where a ring alphabet can offer scalar linear solutions when a field alphabet cannot.

## References

- [1] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, “Network information flow,” *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204 – 1216, July 2000.
- [2] A. Blasiak, R. Kleinberg, and E. Lubetzky, “Lexicographic products and the power of non-linear network coding,” *IEEE Symposium on Foundations of Computer Science (FOCS)*, Palm Springs, CA, pp. 609 – 618, 2011.
- [3] W. Brown, *Matrices over Commutative Rings*, Taylor & Francis, 1992.
- [4] 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.
- [5] T. Chan and A. Grant, “Dualities between entropy functions and network codes,” *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4470 – 4487, October 2008.
- [6] T. Chan and A. Grant, “Network coding capacity regions via entropy functions,” *IEEE Transactions on Information Theory*, vol. 60, no. 9, pp. 5347 – 5374, September 2014.
- [7] J. Connelly and K. Zeger, “A class of non-linearly solvable networks,” *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 201 – 229, January 2017.
- [8] J. Connelly and K. Zeger, “Linear network coding over rings – Part I: Scalar codes and commutative alphabets,” *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 274 – 291, January 2018.
- [9] J. Connelly and K. Zeger, “Linear network coding over rings – Part II: Vector codes and non-commutative alphabets,” *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 292 – 308, January 2018.
- [10] N. Das and B.K. Rai, “On achievability of an  $(r, l)$  fractional linear network code,” *IET Networks*, vol. 6, no. 3, pp. 54 – 61, May 2017.
- [11] 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.
- [12] R. Dougherty, C. Freiling, and K. Zeger, “Unachievability of network coding capacity,” *IEEE Transactions on Information Theory (joint issue with IEEE/ACM Transactions on Networking)*, vol. 52, no. 6, pp. 2365 – 2372, June 2006.
- [13] R. Dougherty, C. Freiling, and K. Zeger, “Networks, matroids, and non-Shannon information inequalities,” *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 1949 – 1969, June 2007.
- [14] R. Dougherty, C. Freiling, and K. Zeger, “Achievable rate regions for network coding,” *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2488 – 2509, May 2015.
- [15] R. Dougherty, E. Freiling, and K. Zeger, “Characteristic-dependent linear rank inequalities with applications to network coding,” *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2510 – 2530, May 2015.
- [16] D. Dummit and R. Foote, *Abstract Algebra*, Third Edition, Hoboken, NJ, John Wiley and Sons Inc., 2004.
- [17] J.B. Ebrahimi and C. Fragouli, “Algebraic algorithms for vector network coding,” *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 996 – 1007, February 2011.
- [18] A. Gómez, C. Mejía, and J. Montoya, “Network coding and the model theory of linear information inequalities,” *International Symposium on Network Coding*, Aalborg, Denmark, pp. 1 – 6, 2014.
- [19] P.A. Grillet, *Abstract Algebra*, Springer-Verlag New York, 2007.
- [20] R.N. Gupta, A. Khurana, D. Khurana, and T.Y. Lam, “Rings over which the transpose of every invertible matrix is invertible,” *Journal of Algebra*, vol. 322, no. 5, pp. 1627 – 1636, September 2009.

- [21] N. Harvey, R. Kleinberg, and A. Rasala Lehman, “On the capacity of information networks,” *IEEE Transactions on Information Theory (joint issue with IEEE/ACM Transactions on Networking)*, vol. 52, no. 6, pp. 2345 – 2364, June 2006.
- [22] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, “A random linear network coding approach to multicast,” *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413 – 4430, October 2006.
- [23] R. Horn and C. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, 1991.
- [24] S. Huang and A. Ramamoorthy, “On the multiple-unicast capacity of 3-source, 3-terminal directed acyclic networks,” *IEEE/ACM Transactions on Networking*, vol. 22, no. 1, pp. 285 – 299, February 2014.
- [25] S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, “Polynomial time algorithms for multicast network code construction,” *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1973 - 1982, June 2005.
- [26] S. Kamath, V. Anantharam, D. Tse, C.C. Wang, “The two-unicast problem,” to appear in *IEEE Transactions on Information Theory*.
- [27] T.Y. Lam, *A First Course in Noncommutative Rings*, Second Edition, Springer Verlag New York Inc., 2001.
- [28] M. Langberg and A. Sprintson, “On the hardness of approximating the network coding capacity,” *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1008 – 1014, February 2011.
- [29] S.-Y.R. Li, R.W. Yeung, and N. Cai, “Linear network coding,” *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371 – 381, February 2003.
- [30] S.-Y.R. Li, Q. Sun, and S. Ziyu, “Linear network coding: theory and algorithms,” *Proceedings of the IEEE*, vol. 99, no. 3, pp. 372–387, March 2011.
- [31] S. Lovett, “Linear codes cannot approximate the network capacity within any constant factor,” *Electronic Colloquium on Computational Complexity*, vol. 21, no. 141, pp. 1 – 19, 2014.
- [32] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker Inc., 1974.
- [33] B.R. McDonald, *Linear Algebra over Commutative Rings*, Taylor & Francis, 1984.
- [34] M. Médard, M. Effros, T. Ho, and D. Karger, “On coding for non-multicast networks,” *Conference on Communication Control and Computing*, Monticello, IL, October 2003.
- [35] V. T. Muralidharan and S. Rajan, “Linear network coding, linear index coding, and representable discrete polymatroids,” *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 4096 – 4119, July 2016.
- [36] L. Song, R.W. Yeung, and N. Cai, “Zero-error network coding for acyclic networks,” *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3129 – 3139, December 2003.
- [37] Q. Sun, S.-Y.R. Li, and Z. Li, “On base field of linear network coding,” *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7272 – 7282, December 2016.
- [38] Q. Sun, X. Yang, K. Long, X. Yin, and Z. Li, “On vector linear solvability of multicast networks,” *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 5096 – 5107, September 2016.
- [39] Q. Sun, X. Yin, Z. Li, and K. Long, “Multicast network coding and field sizes,” *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6182 – 6191, November 2015.
- [40] X. Xu, Y. Zeng, Y. L. Guan, and T. Ho, “An achievable region for double-unicast networks with linear network coding,” *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3621 – 3630, October 2014.

- [41] M. F. Wong, M. Langberg, and M. Effros, “On a capacity equivalence between multiple multicast and multiple unicast,” *Allerton Conference on Communication, Control, and Computing*, Monticello, IL, pp. 1537 – 1544, 2013.
- [42] M. F. Wong, M. Langberg, and M. Effros, “Linear capacity equivalence between multiple multicast and multiple unicast,” *IEEE International Symposium on Information Theory*, Honolulu, HI, pp. 2152 – 2156, 2014.
- [43] X. Yan, R.W. Yeung, and Z. Zhang, “An implicit characterization of the achievable rate region for acyclic multisource multisink network coding,” *IEEE Transactions on Information Theory*, vol. 58, no. 9, pp. 5625 – 5639, September 2012.
- [44] R.W. Yeung, “A framework for linear information inequalities,” *IEEE Transactions on Information Theory*, vol. 43, no. 6, pp. 1924 - 1934, November 1997.
- [45] W. Zeng, V. R. Cadambe, and M. Médard, “Alignment-based network coding for two-unicast-Z networks,” *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3183 – 3211, June 2016.

---

This chapter is a reprint of the material as it appears in J. Connelly and K. Zeger, “Linear capacity of networks over ring alphabets,” submitted to *IEEE Transactions on Information Theory*, June 2017, revised January 2018. The dissertation author was the primary investigator of this paper.

# Chapter 5

## A Class of Non-Linearly Solvable Networks

### Abstract

For each positive composite integer  $m$ , a network is constructed which is solvable over an alphabet of size  $m$  but is not solvable over any smaller alphabet. These networks have no linear solutions over any module alphabet and are not asymptotically linearly solvable over any finite-field alphabet. The networks' capacities are all shown to equal one, and their linear capacities are all shown to be bounded away from one for all finite-field alphabets. Additionally, if  $m$  is a non-power-of-prime composite number, then such a network is not solvable over any prime-power-size alphabet.



## 5.1 Introduction

In 2005, it was demonstrated in [7] that there can exist a solvable network which is not vector linearly solvable over any finite-field alphabet and any vector dimension. To date, the network given in [7] is the only known example of such a network published in the literature. In fact, the network given in [7] was shown to not be linearly solvable over very general algebraic types of alphabets, such as finite rings and modules, and it was shown not to even be asymptotically linearly solvable over finite-field alphabets. As a result, the network has been described as “diabolical” by Kschischang [19]<sup>1</sup> and Koetter [17].

The diabolical network has been utilized in numerous extensions and applications of network coding, such as by Krishnan and Rajan [18] for network error correction and by Rai and Dey [23] for multicasting the sum of messages, to construct networks with equivalent solvability properties, hence showing that linear codes are insufficient for each problem. El Rouayheb, Sprintson, and Georghiades [13] reduced the index coding problem to a network coding problem, thereby using the diabolical network to show that linear index codes are not necessarily sufficient. Blasiak, Kleinberg, and Lubetzky [2] used index codes to create networks where there is a polynomial separation between linear and non-linear network coding rates. Chan and Grant [5] showed a duality between entropy functions and network coding problems, which allowed for an alternative proof of the insufficiency of linear network codes.

There remain many open questions regarding non-linear network coding. In this chapter, we present a class of networks that generalize the diabolical network and show a number of other results related to non-linear network coding.

### 5.1.1 Network Coding Model

A *network* will refer to a finite, directed, acyclic multigraph, some of whose nodes are *sources* or *receivers*. Source nodes generate vectors of *messages*, where each of the messages is an arbitrary element of a fixed, finite set of size at least 2, called an *alphabet*. The elements of an alphabet are called *symbols*. The *inputs* to a node are the messages, if any, originating at the node and the symbols carried by the incoming edges of the node. Each outgoing edge of a network node carries a vector of alphabet symbols, called *edge symbols*. Each outgoing edge of a node has associated with it an *edge function* which maps the node’s inputs to the output vector carried by the edge. Each receiver node has *demands*, which are the message vectors the receiver wishes to obtain. Each receiver also has *decoding functions* which map the receiver’s inputs to vectors of alphabet symbols in an attempt to satisfy the receiver’s demands.

---

<sup>1</sup>The terminology was apparently attributed by F. Kschischang to M. Sudan.

A  $(k, n)$  fractional code over an alphabet  $\mathcal{A}$  (or, more briefly, a  $(k, n)$  code over  $\mathcal{A}$ ) is an assignment of edge functions to all of the edges in a network and an assignment of decoding functions to all of the receiver nodes in the network such that message vectors are elements of  $\mathcal{A}^k$  and edge vectors are elements of  $\mathcal{A}^n$ . A code is a *solution* if each receiver recovers each of its demands from its inputs. For linear network coding, we will focus attention on two specific types of  $(k, n)$  codes:

Case (1):  $k = n = 1$  and the network alphabet is a module.

Case (2): Any  $k, n$  and the network alphabet is a ring.

In a  $(1, 1)$  code over an  $R$ -module  $G$ , an edge or decoding function  $f : G^i \rightarrow G$  is *linear over the  $R$ -module  $G$*  if it can be written in the form  $f(x_1, \dots, x_i) = (C_1 \cdot x_1) \oplus \dots \oplus (C_i \cdot x_i)$ , where  $x_1, \dots, x_i \in G$  are the node's inputs,  $C_1, \dots, C_i \in R$  are constants,  $\oplus$  is the Abelian group operation, and  $\cdot$  is the action of the module. A  $(1, 1)$  code is said to be *linear over the  $R$ -module  $G$*  if each edge function and decoding function is linear over the  $R$ -module  $G$ . Note that for any  $R$ -module  $G$  and positive integer  $k$ , the set  $M_k(R)$  of  $k \times k$  matrices over  $R$  with matrix addition and multiplication defined in the usual way is a ring, and  $G^k$  is an  $M_k(R)$ -module. Hence a “vector linear code” over a module is, in fact, a  $(1, 1)$  linear code over a different module.

In a  $(k, n)$  code over a ring  $R$ , an edge function  $f : \underbrace{R^k \times \dots \times R^k}_i \times \underbrace{R^n \times \dots \times R^n}_j \rightarrow R^n$  is *linear over  $R$*  if it can be written in the form

$$f(x_1, \dots, x_i, y_1, \dots, y_j) = M_1 x_1 + \dots + M_i x_i + M'_1 y_1 + \dots + M'_j y_j \quad (5.1)$$

where  $x_1, \dots, x_i \in R^k$  are message vectors originating at the node,  $y_1, \dots, y_j \in R^n$  are edge vectors carried by the incoming edges to the node,  $M_1, \dots, M_i$  are  $n \times k$  matrices and  $M'_1, \dots, M'_j$  are  $n \times n$  matrices whose entries are constant in  $R$ , i.e. the edge symbol can be written as a linear combination of the node's inputs. Similarly, a decoding function is linear if it has a form analogous to (5.1). A  $(k, n)$  code is said to be *linear over the ring  $R$*  if each edge function and each decoding function is linear over  $R$ .

A  $(1, 1)$  linear code over a ring  $R$  (called a *scalar linear code over  $R$* ) is also a linear code over the  $R$ -module  $R$ , where  $R$  acts on its own Abelian group by multiplication in  $R$ . For each positive integer  $k$ , a  $(k, k)$  linear code over  $R$  (called a  *$k$ -dimensional vector linear code over  $R$* ) is also a linear code over the  $M_k(R)$ -module  $R^k$ . Hence scalar and vector linear codes over rings are special cases of linear codes over modules. When discussing linear codes over rings, we will always specify the dimension (e.g. scalar, vector, or  $(k, n)$ ), but a linear code over a module will always refer to a  $(1, 1)$  linear code.

A network is defined to be

- *solvable over  $\mathcal{A}$*  if there exists a  $(1, 1)$  solution over  $\mathcal{A}$ ,
- *asymptotically solvable over  $\mathcal{A}$*  if for any  $\varepsilon > 0$ , there exists a  $(k, n)$  solution over  $\mathcal{A}$  for some  $k$  and  $n$  satisfying  $k/n > 1 - \varepsilon$ ,
- *linearly solvable over the  $R$ -module  $G$*  if there exists a linear solution over the  $R$ -module  $G$ ,
- *scalar linearly solvable over the ring  $R$*  if there exists a  $(1, 1)$  linear solution over  $R$ ,
- *vector linearly solvable over the ring  $R$*  if there exists a  $(k, k)$  linear solution over  $R$ , for some  $k \geq 1$ .

We say that a network is *solvable* if it is solvable over some alphabet. A solvable network is able to communicate at rate  $k/n = 1$ , and an asymptotically solvable network is able to communicate at a rate arbitrarily close to 1. Since scalar and vector linear codes over rings are special cases of linear codes over modules, a network that is vector (or scalar) linearly solvable over some ring is also linearly solvable over some module. Conversely, a network with no linear solution over any module also has no vector linear solutions over any ring (or field). This paper focuses on solvable networks that are not linear solvable over any module.

The *capacity*<sup>2</sup> of a network is:

$$\sup\{k/n : \exists \text{ a } (k, n) \text{ solution over some } \mathcal{A}\}.$$

The *linear capacity* of a network with respect to a ring  $R$  is:

$$\sup\{k/n : \exists \text{ a } (k, n) \text{ linear solution over } R\}.$$

It was shown in [4] that the capacity of a network is independent of alphabet size, and it was noted that linear capacity can depend on alphabet size.

### 5.1.2 Previous Work

We now summarize some of the existing results regarding the solvability and linear solvability of *multicast networks* (in which each receiver demands all of the messages) and *general networks* (in which each receiver demands a subset of the messages). Network codes were first presented by Ahlswede, Ning, Li, and Yeung [1] as a method of improving the throughput of a network; they presented the butterfly network, a variant of which is scalar linearly solvable over every field but not solvable via routing. Li, Yeung, and Ning [20] showed that if a multicast network is solvable, then it is scalar linearly solvable over every sufficiently large finite-field alphabet. In addition, Riis [25] showed that every solvable multicast

---

<sup>2</sup>In the literature, this is sometimes referred to as the “coding capacity” (as opposed to the routing capacity). For brevity, we will simply use the term “capacity,” as we do not discuss routing capacity in this paper.

network has a binary vector linear solution in some dimension. Feder, Ron, and Tavorly [15] and Rasala Lehman and Lehman [24] both independently showed that some solvable multicast networks asymptotically require finite-field alphabets to be at least as large as twice the square root of the number of receiver nodes in order to have a scalar linear solution over the field.

Non-linear coding in multicast networks can offer advantages such as reducing the alphabet size required for solvability; Rasala Lehman and Lehman [24] presented a network which is solvable over a ternary alphabet but has no scalar linear solution over any field alphabet whose size is less than five, and Riis [25] and also [9] demonstrated general and multicast networks, respectively, which have scalar non-linear binary solutions but no scalar linear binary solutions. A multicast network was presented in [9] which is solvable precisely over those alphabets whose size is neither 2 nor 6, and Sun, Yin, Li, and Long [33] presented families of multicast networks which are scalar linearly solvable over certain finite-field alphabets but not over all larger finite-field alphabets.

Unlike multicast networks, general networks that are solvable do not necessarily have vector linear solutions over fields, as demonstrated in [7]. Médard, Effros, Ho, and Karger [21] showed that there can exist a network which is vector linearly solvable over some field but is not scalar linearly solvable over any field. Das and Rai [6] showed more generally that for each integer  $m \geq 2$  the following holds: there exists a network with  $k$ -dimensional vector linear solutions over an arbitrary field if and only if  $k$  is a multiple of  $m$ . Sun, Yang, Long, Yin, and Li [31] compared alphabet sizes using scalar and vector linear codes over fields, where the vector alphabet size is  $|\mathbb{F}|^k$ . They showed that in some cases, linear solutions may be obtained with vector alphabet sizes that are smaller than any possible scalar solution alphabet size. They also showed that in other cases, the opposite result may be true. Similarly, Etzion and Wachter-Zeh [14] showed that vector linear coding can significantly reduce the required vector alphabet size compared to scalar coding.

Shenvi and Dey [29] showed that for networks with two source-receiver pairs the following are equivalent: the network is solvable, the network is vector linearly solvable over some field, the network satisfies a simple cut condition. Cai and Han [3] showed that for a particular class of networks with three source-receiver pairs: the solvability can be determined in polynomial time, being solvable is equivalent to being scalar linearly solvable over some field, and finite-field alphabets of size 2 or 3 are sufficient to construct scalar linear solutions. In [11], the Fano and non-Fano networks were shown to be solvable precisely over power-of-two and odd alphabet sizes, respectively. For each integer  $m \geq 2$ , Rasala Lehman and Lehman [24] demonstrated a class of networks which are not solvable over any alphabet whose size is less than  $m$  and are solvable over all alphabets whose size is a prime power greater than or equal to  $m$ . For each integer  $m \geq 3$ , Yuan and Kan [34] demonstrated a class of networks which are not solvable over

any alphabet whose size is less than  $m$  and are solvable over all alphabets whose size is not divisible by  $2, 3, \dots, m - 1$ .

Koetter and Médard [16] showed for every finite field  $\mathbb{F}$  and every network, the network is scalar linearly solvable over  $\mathbb{F}$  if and only if a corresponding system of polynomials has a common root in  $\mathbb{F}$ , and in [8] it was shown that for every finite field  $\mathbb{F}$  and any system of polynomials, there exists a corresponding network which is scalar linearly solvable over  $\mathbb{F}$  if and only if the system of polynomials has a common root in  $\mathbb{F}$ . Subramanian and Thangaraj [30] showed an alternate method of deriving a system of polynomials which corresponds to the scalar linear solvability of a network, such that the degree of each polynomial equation is at most 2. Presently, there are no known algorithms for determining whether a general network is solvable.

While networks that are linearly solvable over some module are solvable, the converse need not be true. This paper demonstrates infinitely many such counterexamples. There remain numerous open questions regarding the existence of solvable networks which are not linearly solvable over any module. Are many/most solvable networks not linearly solvable? Can such networks be efficiently characterized? Can such networks be algorithmically recognized? We leave these questions for future research.

### 5.1.3 Our Contributions

In this paper, we present an infinite class of solvable networks which are not linearly solvable over any module alphabet. We denote each such network as  $\mathcal{N}_4$ , and we construct  $\mathcal{N}_4$  from several intermediate networks denoted by  $\mathcal{N}_1, \mathcal{N}_2$ , and  $\mathcal{N}_3$ , all of which are constructed from a fundamental network building block  $B$ . Specifically, for each positive composite number  $m$ , we describe how to construct a network  $\mathcal{N}_4$  which has a non-linear solution over an alphabet of size  $m$  yet has no linear solution over any module alphabet, including vector linear codes over rings and fields. In addition, such a network is not solvable over any alphabet whose size is less than  $m$ . The diabolical network in [7] was shown to be non-linearly solvable over an alphabet of size 4. The network in [7] was designed using matroid theory. Other connections between networks and matroids were investigated, for example, by [10, 13, 18, 22, 32, 35].

The inspiration for the construction of networks  $\mathcal{N}_1, \mathcal{N}_2$ , and  $\mathcal{N}_3$  in order to construct  $\mathcal{N}_4$  relates to specific solvability properties of each of these component networks. The  $\mathcal{N}_1$  networks are a generalization of the non-Fano network, the  $\mathcal{N}_2$  networks are a generalization of a modified Fano network that also have non-linear solutions in some cases, and the  $\mathcal{N}_3$  networks are a generalization of a modified non-Fano network that also have non-linear solutions in some cases. We construct all of these component networks from the same network building block  $B$ . As a result, we can more easily characterize the solvability and linear

solvability of the networks, since the solvability of this network building block was characterized in [34]. By combining the networks  $\mathcal{N}_1, \mathcal{N}_2$ , and  $\mathcal{N}_3$  with certain parameters, we construct non-linearly solvable networks.

We will now summarize the main results of this paper, which all appear in Section 5.6. The network  $\mathcal{N}_4$  is parameterized by an arbitrary integer  $m \geq 2$ . Theorem 5.6.4 shows that  $\mathcal{N}_4$  is solvable over an alphabet of size  $m$ . Theorem 5.6.5 shows, however, that  $\mathcal{N}_4$  is never solvable over alphabets smaller than  $m$ . Theorem 5.6.8 shows that when  $m$  is prime,  $\mathcal{N}_4$  has a scalar linear solution over a field of size  $m$ . In fact, for all non-prime integers  $m$ , the network  $\mathcal{N}_4$  has no linear solution, as demonstrated by Theorems 5.6.9 and 5.6.10. In particular, Theorem 5.6.9 shows that when  $m$  is composite, no linear solution for  $\mathcal{N}_4$  exists over any module, and Corollary 5.6.11 shows that in such case,  $\mathcal{N}_4$  is not even asymptotically linearly solvable over any finite-field alphabet. In the special case of  $m = 4$ , the demonstrated network  $\mathcal{N}_4$  exhibits properties similar to the network presented in [7]. We also demonstrate (in Corollary 5.6.6) that if  $m$  is a non-power-of-prime composite (e.g. 6), then  $\mathcal{N}_4$  is not solvable over any prime-power size alphabets.

The diabolical network was shown in [7] to have capacity equal to one, whereas its linear capacity is bounded away from one for any finite-field alphabet. Analogously, we show in Theorem 5.6.10 that for all  $m$ , the capacity of  $\mathcal{N}_4$  equals one, whereas for all composite  $m$ , its linear capacity over any finite-field alphabet is bounded away from one. Related capacity results are given for the constituent networks  $\mathcal{N}_0$  (in Lemma 5.2.4),  $\mathcal{N}_1$  (in Lemma 5.3.4),  $\mathcal{N}_2$  (in Lemma 5.4.7), and  $\mathcal{N}_3$  (in Lemma 5.5.8). We do not see a straightforward method to determine the linear capacity or asymptotic linear solvability over more general ring alphabets, as many of the linear algebra results used in this analysis do not extend to matrices over general rings.

The rest of the paper is organized as follows. Table 5.1 summarizes the networks created and the results in this paper. Section 5.1.4 provides mathematical background and definitions. Sections 5.2-5.5 present the building block networks which are used to construct the main class of networks. Section 5.6 details the properties and construction of the main class of networks. For each network family, we will discuss the solvability properties, the linear solvability properties, and the capacity. The Appendix contains the proofs of three of the lemmas in this paper. All other proofs are given in the main body of the paper. Section 5.7 poses some open questions regarding the solvability and capacity of general networks.

|  |                  |
|--|------------------|
| <b>Network</b> $\mathcal{N}_1(m)$  | Section 5.3      |
| · Consists of a block $B(m)$ together with source nodes and an additional receiver.  | Figure 5.4       |
| · $4m + 7$ nodes.  | Remark 5.3.1     |
| · If solvable over $\mathcal{A}$ , then $\gcd( \mathcal{A} , m) = 1$ .   | Lemma 5.3.2      |
| · Linearly solvable over standard $R$ -module $G$ iff $\gcd(\text{char}(R), m) = 1$ .  | Lemma 5.3.3      |
| <b>Network</b> $\mathcal{N}_2(m, w)$   | Section 5.4      |
| · Consists of $w$ blocks $B(m + 1)$ together with source nodes and an additional receiver.   | Figure 5.5       |
| · $4mw + 9w + 2$ nodes.  | Remark 5.4.1     |
| · If $w \geq 2$ , then non-linearly solvable over an alphabet of size $mw$ .   | Lemma 5.4.4      |
| · If solvable over $\mathcal{A}$ , then $\gcd( \mathcal{A} , m) \neq 1$ .  | Lemma 5.4.5      |
| · Linearly solvable over standard $R$ -module $G$ iff $\text{char}(R) \mid m$ .  | Lemma 5.4.6      |
| <b>Network</b> $\mathcal{N}_3(m_1, m_2)$   | Section 5.5      |
| · Consists of blocks $B(m_1)$ and $B(m_2)$ together with source nodes and an additional receiver.  | Figure 5.6       |
| · $4m_1 + 4m_2 + 12$ nodes.  | Remark 5.5.1     |
| · For each $s, t \geq 1$ relatively prime to $m_1$ , if $m_2 = sm_1^\alpha$ for some $\alpha \geq 1$ , then non-linearly solvable over an alphabet of size $tm_1^{\alpha+1}$ . | Corollary 5.5.7  |
| · If solvable over $\mathcal{A}$ , then $\gcd( \mathcal{A} , m_1) = 1$ or $ \mathcal{A}  \nmid m_2$ .  | Lemma 5.5.5      |
| · Linearly solvable over standard $R$ -module $G$ iff $\gcd(\text{char}(R), m_1, m_2) = 1$ .   | Lemma 5.5.6      |
| <b>Network</b> $\mathcal{N}_4(m)$  | Section 5.6      |
| · Consists of a disjoint union of various networks $\mathcal{N}_1, \mathcal{N}_2$ , and $\mathcal{N}_3$ .  | Equation (5.54)  |
| · Solvable over an alphabet of size $m$ .  | Theorem 5.6.4    |
| · If $ \mathcal{A}  < m$ , then not solvable over $\mathcal{A}$ .  | Theorem 5.6.5    |
| · If $m$ is not a prime power, then not solvable over any prime-power-size $\mathcal{A}$ .   | Corollary 5.6.6  |
| · If $m$ is prime, then scalar linearly solvable over $\text{GF}(m)$ .   | Theorem 5.6.8    |
| · If $m$ is composite, then: (1) not linearly solvable over any module.  | Theorem 5.6.9    |
| (2) not asymptotically linearly solvable over any finite field.  | Corollary 5.6.11 |
| · Number of nodes is $O\left(m^{\frac{\log m}{\log \log m}}\right)$ and $\Omega(m)$ .  | Theorem 5.6.12   |

Figure 5.1: Summary of the networks constructed in this chapter, where  $m, m_1, m_2$ , and  $w$  are integers such that  $m, m_1, m_2 \geq 2$  and  $w \geq 1$ .

### 5.1.4 Preliminaries

The following definitions regarding linear network codes over modules are from [7] and [12].

**Definition 5.1.1.** Let  $(R, +, *)$  be a ring with additive identity  $0_R$ . An  $R$ -module (specifically a left  $R$ -module) is an Abelian group  $(G, \oplus)$  with identity  $0_G$  and an action  $\cdot : R \times G \rightarrow G$  such that for all  $r, s \in R$  and all  $g, h \in G$  the following hold:

$$r \cdot (g \oplus h) = (r \cdot g) \oplus (r \cdot h)$$

$$(r + s) \cdot g = (r \cdot g) \oplus (s \cdot g)$$

$$(r * s) \cdot g = r \cdot (s \cdot g).$$

The ring multiplication symbol  $*$  will generally be omitted for brevity. If the ring  $R$  has a multiplicative identity  $1_R$ , then we also require  $1_R \cdot g = g$  for all  $g \in G$ . For brevity, we say that  $G$  is an  $R$ -module.  $\ominus$  will denote adding the inverse of an element (subtraction) within the group.

For any finite ring  $R$  with multiplicative identity, the *characteristic of  $R$*  is denoted  $\text{char}(R)$  and is the smallest positive integer  $m$  such that  $1_R$  added to itself  $m$  times equals  $0_R$ . The characteristic of a finite field is always a prime number. The following definition describes a class of modules which we will use to discuss linear solvability in this paper.

**Definition 5.1.2.** Let  $G$  be an  $R$ -module. We will say that  $G$  is a *standard  $R$ -module* if

1.  $R$  acts faithfully on  $G$ ; that is if  $r, s \in R$  are such that  $r \cdot g = s \cdot g$  for all  $g \in G$ , then  $r = s$ .
2.  $R$  has a multiplicative identity  $1_R$ .
3.  $R$  is finite.
4. If  $r \in R$  has a multiplicative left (respectively, right) inverse, then this element is a two-sided inverse, which will be denoted  $r^{-1}$ .

A finite commutative ring  $R$ , with a multiplicative identity, acting on itself is a standard  $R$ -module. For each positive integer  $k$ , the set  $M_k(R)$  of  $k \times k$  matrices over  $R$  with matrix addition and multiplication is a ring and  $R^k$  is a standard  $M_k(R)$ -module. Since fields are a special case of commutative rings, scalar and vector linear codes over fields are also special cases of linear codes over standard modules.



Lemma 5.1.3 was proved in a slightly different form in the proof of Theorem III.4 in [7].

**Lemma 5.1.3.** *If a network is not linearly solvable over any standard module, then it is not linearly solvable over any module.*

We say that a positive integer  $m$  is *invertible in  $R$*  if there exists  $m^{-1} \in R$  such that  $m^{-1}(m1_R) = 1_R$ , where  $(m1_R)$  denotes  $1_R$  added to itself  $m$  times. Specifically,

$$m^{-1} = \left( \underbrace{1_R + \cdots + 1_R}_{m \text{ adds}} \right)^{-1}.$$

Lemma 5.1.4 is relatively straightforward to show, and thus its proof is omitted. This lemma discusses properties of multiplicative inverses in rings and will be used in the proofs of Lemmas 5.3.3 and 5.5.6 to more easily characterize the classes of modules over which  $\mathcal{N}_1$  and  $\mathcal{N}_3$  are linearly solvable.

**Lemma 5.1.4.** *For each finite ring  $R$  with a multiplicative identity and each positive integer  $m$ , the integer  $m$  is invertible in  $R$  if and only if  $\text{char}(R)$  and  $m$  are relatively prime.*

The following definition was called Property  $P'$  by Yuan and Kan [34]. They used this property to characterize the solvability of classes of networks similar to  $\mathcal{N}_0$  and  $\mathcal{N}_1$ , and we will use it throughout this paper.

**Definition 5.1.5.** Let  $m \geq 2$ . A  $(1, 1)$  code for a network  $\mathcal{N}$  over an alphabet  $\mathcal{A}$ , containing messages  $x_0, x_1, \dots, x_m$  and edge symbols  $e_0, e_1, \dots, e_m$ , is said to have *Property  $P(m)$*  if there exists a binary operation  $\oplus : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$  and permutations  $\pi_0, \pi_1, \dots, \pi_m$  and  $\sigma_0, \sigma_1, \dots, \sigma_m$  of  $\mathcal{A}$ , such that  $(\mathcal{A}, \oplus)$  is an Abelian group and the edge symbols can be written as

$$e = \bigoplus_{j=0}^m \pi_j(x_j) \quad \text{and} \quad e_i = \sigma_i \left( \bigoplus_{\substack{j=0 \\ j \neq i}}^m \pi_j(x_j) \right) \quad (i = 0, 1, \dots, m)$$

## 5.2 Network $\mathcal{N}_0(m)$

For each  $m \geq 2$ , the network building block  $B(m)$  is defined in Figure 5.2 and is used to build network  $\mathcal{N}_0(m)$ , which is defined in Figure 5.3. For each  $i$ , the node  $v_i$  within  $B(m)$  has a single incoming edge from node  $u_i$ , so without loss of generality, we may assume both outgoing edges of  $v_i$  carry the

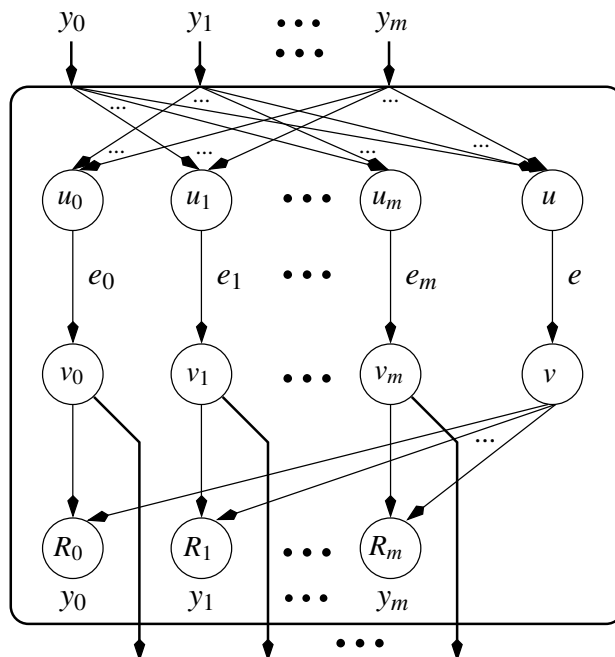


Figure 5.2: The network building block  $B(m)$  has message vector inputs  $y_0, y_1, \dots, y_m$  (from unspecified source nodes) and  $m + 1$  output edges. The node  $u$  receives each of the inputs and has a single outgoing edge to the node  $v$ , which carries the edge symbol  $e$ . For each  $i$ , the node  $u_i$  receives each of the inputs except  $y_i$  and has a single outgoing edge to the node  $v_i$ , which carries the edge symbol  $e_i$ . The receiver node  $R_i$  has an incoming edge from  $v_i$  and an incoming edge from  $v$  and demands the  $i$ th message vector  $y_i$ . The  $i$ th output edge of  $B(m)$  is an outgoing edge of node  $v_i$ .

symbol  $e_i$ . Similarly, we may assume each of the outgoing edges of the node  $v$  carries the symbol  $e$ . Lemma 5.2.2 demonstrates that for each  $m \geq 2$ , the  $(1, 1)$  solutions of network  $\mathcal{N}_0(m)$  are precisely those codes which satisfy Property  $P(m)$ , defined in Definition 5.1.5. In particular, the solution alphabets have to be permutations of Abelian groups.

**Remark 5.2.1.** *The network  $\mathcal{N}_0(m)$  has  $m + 1$  source nodes,  $2(m + 2)$  intermediate nodes, and  $m + 1$  receiver nodes, so the total number of nodes in  $\mathcal{N}_0(m)$  is  $4m + 6$ .*

Lemma 5.2.2 characterizes the solvability of  $\mathcal{N}_0(m)$  and will be used in the proofs of the solvability conditions of  $\mathcal{N}_1, \mathcal{N}_2$ , and  $\mathcal{N}_3$ . This lemma was proved in a slightly different form in [34, Proposition 3.2].

**Lemma 5.2.2.** *Let  $m \geq 2$ . A  $(1, 1)$  code over an alphabet  $\mathcal{A}$  is a solution for network  $\mathcal{N}_0(m)$  if and only if the code satisfies Property  $P(m)$ .*

The following result regarding the linear solvability of  $\mathcal{N}_0(m)$  will be used in later proofs.

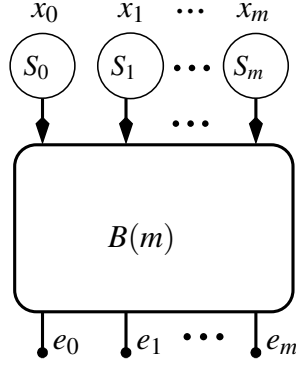


Figure 5.3: Network  $\mathcal{N}_0(m)$  consists of a block  $B(m)$  together with source nodes  $S_0, S_1, \dots, S_m$ , which generate message vectors  $x_0, x_1, \dots, x_m$ , respectively. The output edges of  $B(m)$  are unused.

**Lemma 5.2.3.** *Let  $m \geq 2$  and let  $G$  be a standard  $R$ -module. Suppose a linear solution for network  $\mathcal{N}_0(m)$  over  $G$  has edge symbols*

$$e = \bigoplus_{j=0}^m (c_j \cdot x_j) \quad \text{and} \quad e_i = \bigoplus_{\substack{j=0 \\ j \neq i}}^m (c_{i,j} \cdot x_j) \quad (i = 0, 1, \dots, m)$$

and decoding functions

$$R_i: x_i = (d_{i,e} \cdot e) \oplus (d_i \cdot e_i) \quad (i = 0, 1, \dots, m)$$

where  $c_{i,j}, c_j, d_{i,e}, d_i \in R$ . Then each  $c_{i,j}, c_j, d_{i,e}$ , and  $d_i$  is invertible in  $R$ , and

$$c_{i,j} = -d_i^{-1} d_{i,e} c_j \quad (i, j = 0, 1, \dots, m \text{ and } j \neq i).$$

*Proof.* Equating message components at the receiver  $R_i$  and using the fact  $G$  is a standard  $R$ -module, yields

$$1_R = d_{i,e} c_i \quad (i = 0, 1, \dots, m)$$

$$0_R = d_{i,e} c_j + d_i c_{i,j} \quad (i, j = 0, 1, \dots, m \text{ and } j \neq i)$$

which implies the following elements of  $R$  are invertible:

$$d_{i,e} \text{ and } c_i \quad (i = 0, 1, \dots, m)$$

$$d_i \text{ and } c_{i,j} \quad (i, j = 0, 1, \dots, m \text{ and } j \neq i).$$

The result then follows by solving for  $c_{i,j}$ . ■

Lemma 5.2.4 characterizes the capacity and linear capacity of  $\mathcal{N}_0$ , and this lemma will be used to upper bound the capacities of  $\mathcal{N}_1, \mathcal{N}_2$ , and  $\mathcal{N}_3$  in the proofs of Lemmas 5.3.4, 5.4.7, and 5.5.8, respectively.

**Lemma 5.2.4.** *The network  $\mathcal{N}_0(m)$  has capacity and linear capacity, for any finite-field, equal to 1.*

*Proof.* Let  $G$  be a standard  $R$ -module. The network  $\mathcal{N}_0(m)$  has the following linear solution over  $G$ :

$$e = \bigoplus_{j=0}^m x_j \quad \text{and} \quad e_i = \bigoplus_{\substack{j=0 \\ j \neq i}}^m x_j \quad (i = 0, 1, \dots, m)$$

and decoding at each receiver as follows:

$$R_i : e \ominus e_i = x_i \quad (i = 0, 1, \dots, m).$$

A scalar linear solution over a finite-field alphabet is a special case of a linear solution over a standard module. Therefore  $\mathcal{N}_0(m)$  is scalar linearly solvable over any finite-field alphabet, so the linear capacity of  $\mathcal{N}_0(m)$  for any finite-field alphabet is at least 1. The only path for message vector  $x_0$  to reach the receiver  $R_0$  is through the edge connecting nodes  $u$  and  $v$ , so its capacity is at most 1. Thus, both the capacity of  $\mathcal{N}_0(m)$  and its linear capacity for any finite-field alphabet are equal to 1. ■

### 5.3 Network $\mathcal{N}_1(m)$

For each  $m \geq 2$ , network  $\mathcal{N}_1(m)$  is defined in Figure 5.4. The special case  $m = 2$  corresponds to the non-Fano network from [10, 11], with a relabeling of messages and nodes. Lemmas 5.3.2, 5.3.3, and 5.3.4, respectively, demonstrate that network  $\mathcal{N}_1(m)$  is

1. solvable over  $\mathcal{A}$  only if  $|\mathcal{A}|$  is relatively prime to  $m$ ,
2. linearly solvable over standard  $R$ -module  $G$  if and only if  $\text{char}(R)$  is relatively prime to  $m$ ,
3. asymptotically linearly solvable over finite field  $\mathbb{F}$  if and only if  $\text{char}(\mathbb{F})$  does not divide  $m$ .

**Remark 5.3.1.** *Network  $\mathcal{N}_1(m)$  is a network  $\mathcal{N}_0(m)$  with one additional receiver node, so the total number of nodes in  $\mathcal{N}_1(m)$  is  $4m + 7$ .*

The following lemma also follows from [34, Proposition 4.1] and characterizes a condition on the alphabet size necessary for the solvability of  $\mathcal{N}_1(m)$ .

**Lemma 5.3.2.** *For each  $m \geq 2$ , if network  $\mathcal{N}_1(m)$  is solvable over alphabet  $\mathcal{A}$ , then  $m$  and  $|\mathcal{A}|$  are relatively prime.*

*Proof.* Assume  $\mathcal{N}_1(m)$  is solvable over  $\mathcal{A}$ . Network  $\mathcal{N}_1(m)$  consists of a network  $\mathcal{N}_0(m)$  with the additional receiver  $R_x$ , so by Lemma 5.2.2, the edge functions within  $B(m)$  must satisfy Property  $P(m)$ . Thus,

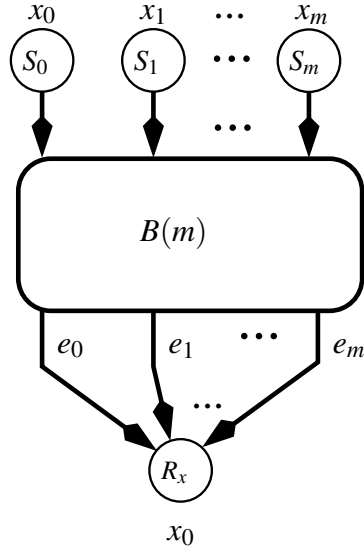


Figure 5.4: Network  $\mathcal{N}_1(m)$  consists of a block  $B(m)$  together with source nodes  $S_0, S_1, \dots, S_m$  and an additional receiver  $R_x$ . For each  $i$ , the source node  $S_i$  generates the message vector  $x_i$  and is the  $i$ th input to  $B(m)$ . The additional receiver  $R_x$  receives all of the output edges of  $B(m)$  and demands the message vector  $x_0$ .

there exists an Abelian group  $(\mathcal{A}, \oplus)$  and permutations  $\pi_0, \pi_1, \dots, \pi_m$  and  $\sigma_0, \sigma_1, \dots, \sigma_m$  of  $\mathcal{A}$ , such that the edges carry the symbols:

$$e_i = \sigma_i \left( \bigoplus_{\substack{j=0 \\ j \neq i}}^m \pi_j(x_j) \right) \quad (i = 0, 1, \dots, m) \quad (5.2)$$

$$e = \bigoplus_{j=0}^m \pi_j(x_j).$$

Now suppose to the contrary that  $m$  and  $|\mathcal{A}|$  share a prime factor  $p$ . By Cauchy's Theorem of Finite Groups [12, p. 93], there exists a nonzero element  $a$  in the group  $\mathcal{A}$  whose order is  $p$ . Since  $p \mid m$ , we have  $\underbrace{a \oplus \dots \oplus a}_{m \text{ adds}} = 0$ . Define two collections of messages as follows:

$$x_j = \pi_j^{-1}(0) \quad \text{and} \quad \hat{x}_j = \pi_j^{-1}(a) \quad (j = 0, 1, \dots, m)$$

Since  $a \neq 0$  and each  $\pi_j$  is bijective, it follows that  $x_j \neq \hat{x}_j$  for all  $j$ .

By Property  $P(m)$ , for each  $i = 0, 1, \dots, m$ , we have

$$e_i = \sigma_i \left( \underbrace{0 \oplus \dots \oplus 0}_{m \text{ adds}} \right) = \sigma_i(0) \quad [\text{from (5.2)}]$$

for the messages  $x_0, x_1, \dots, x_m$ , and

$$e_i = \sigma_i \left( \underbrace{a \oplus \dots \oplus a}_{m \text{ adds}} \right) = \sigma_i(0) \quad [\text{from (5.2)}]$$

for the messages  $\hat{x}_0, \hat{x}_1, \dots, \hat{x}_m$ . For both collections of messages, the edge symbols  $e_0, e_1, \dots, e_m$  are the same, and therefore the decoded value  $x_0$  at  $R_x$  must be the same. However, this contradicts the fact that  $x_0 \neq \hat{x}_0$ . ■

**Lemma 5.3.3.** *Let  $m \geq 2$ , and let  $G$  be a standard  $R$ -module. Then network  $\mathcal{N}_1(m)$  is linearly solvable over  $G$  if and only if  $\text{char}(R)$  is relatively prime to  $m$ .*

*Proof.* By Lemma 5.1.4,  $m$  is invertible in  $R$  if and only if  $\text{char}(R)$  is relatively prime to  $m$ , so it suffices to show that for each  $m$  and each standard  $R$ -module  $G$ , network  $\mathcal{N}_1(m)$  is linearly solvable over  $G$  if and only if  $m$  is invertible in  $R$ .

Assume network  $\mathcal{N}_1(m)$  is linearly solvable over the standard  $R$ -module  $G$ . The messages are drawn from  $G$ , and there exist  $c_{i,j}, c_j \in R$ , such that the edge symbols can be written as:

$$e_i = \bigoplus_{\substack{j=0 \\ j \neq i}}^m (c_{i,j} \cdot x_j) \quad (i = 0, 1, \dots, m) \quad (5.3)$$

$$e = \bigoplus_{j=0}^m (c_j \cdot x_j) \quad (5.4)$$

and there exist  $d_{i,e}, d_i, d_{x,i} \in R$ , such that each receiver can linearly recover its respective demands from its inputs by:

$$R_i : x_i = (d_{i,e} \cdot e) \oplus (d_i \cdot e_i) \quad (i = 0, 1, \dots, m) \quad (5.5)$$

$$R_x : x_0 = \bigoplus_{i=0}^m (d_{x,i} \cdot e_i). \quad (5.6)$$

Since  $\mathcal{N}_1(m)$  contains  $\mathcal{N}_0(m)$ , by Lemma 5.2.3 and (5.3) – (5.5), each  $c_i$  and each  $d_i$  is invertible in  $R$ , and

$$c_{i,j} = -d_i^{-1} d_{i,e} c_j \quad (i, j = 0, 1, \dots, m \text{ and } j \neq i). \quad (5.7)$$

Equating message components at  $R_x$  yields:

$$\begin{aligned} 1_R &= \sum_{i=1}^m d_{x,i} c_{i,0} && [\text{from (5.3), (5.6)}] \\ &= - \sum_{i=1}^m d_{x,i} d_i^{-1} d_{i,e} c_0 && [\text{from (5.7)}] \end{aligned} \quad (5.8)$$

and for each  $j = 1, 2, \dots, m$ ,

$$\begin{aligned}
0_R &= \sum_{\substack{i=0 \\ i \neq j}}^m d_{x,i} c_{i,j} && \text{[from (5.3), (5.6)]} \\
&= - \left( \sum_{\substack{i=0 \\ i \neq j}}^m d_{x,i} d_i^{-1} d_{i,e} \right) c_j && \text{[from (5.7)].} \\
&= \sum_{\substack{i=0 \\ i \neq j}}^m d_{x,i} d_i^{-1} d_{i,e} c_0. && \text{[from right multiplying by } -c_j^{-1} c_0 \text{].} \tag{5.9}
\end{aligned}$$

By summing (5.9) over  $j = 1, 2, \dots, m$  and subtracting (5.8), we get

$$\begin{aligned}
-1_R &= \sum_{j=0}^m \sum_{\substack{i=0 \\ i \neq j}}^m d_{x,i} d_i^{-1} d_{i,e} c_0 && \text{[from (5.8), (5.9)]} \\
&= m \sum_{i=0}^m d_{x,i} d_i^{-1} d_{i,e} c_0.
\end{aligned}$$

Therefore,  $m$  is invertible in  $R$ .

To prove the converse, let  $G$  be a standard  $R$ -module such that  $m$  is invertible in  $R$ . Define a linear code over  $G$  by:

$$\begin{aligned}
e_i &= \bigoplus_{\substack{j=0 \\ j \neq i}}^m x_j && (i = 0, 1, \dots, m) \\
e &= \bigoplus_{j=0}^m x_j.
\end{aligned}$$

Receiver  $R_i$  can linearly recover  $x_i$  from its received edge symbols  $e$  and  $e_i$  by:

$$R_i : e \ominus e_i = x_i \quad (i = 0, 1, \dots, m)$$

and receiver  $R_x$  can linearly recover  $x_0$  from its received edge symbols  $e_0, e_1, \dots, e_m$  by:

$$R_x : \left( m^{-1} \cdot \bigoplus_{i=0}^m e_i \right) \ominus e_0 = \left( m^{-1} \cdot \bigoplus_{i=0}^m \bigoplus_{\substack{j=0 \\ j \neq i}}^m x_j \right) \ominus \bigoplus_{j=1}^m x_j = \bigoplus_{j=0}^m x_j \ominus \bigoplus_{j=1}^m x_j = x_0.$$

Thus the code is a linear solution for  $\mathcal{N}_1(m)$ . ■

As an example of the previous lemma, for each  $q \geq 2$  relatively prime to  $m$ , network  $\mathcal{N}_1(m)$  has a scalar linear solution over the ring  $\mathbb{Z}_q$ , since  $\mathbb{Z}_q$  is a standard  $\mathbb{Z}_q$ -module and  $\text{char}(\mathbb{Z}_q) = q$ . It then follows from Lemma 5.3.2 that network  $\mathcal{N}_1(m)$  is solvable over  $\mathcal{A}$  if and only if  $|\mathcal{A}|$  is relatively prime to  $m$ . As another special case, the network  $\mathcal{N}_1(m)$  is vector linearly solvable over a field  $\mathbb{F}$  if and only if  $\text{char}(\mathbb{F}) \nmid m$ .

The following lemma characterizes the capacity and the linear capacity over finite-field alphabets of  $\mathcal{N}_1(m)$ , and its proof is contained in the Appendix.

**Lemma 5.3.4.** *For each  $m \geq 2$ , network  $\mathcal{N}_1(m)$  has:*

- (a) *capacity equal to 1,*
- (b) *linear capacity equal to 1 for any finite-field alphabet whose characteristic does not divide  $m$ ,*
- (c) *linear capacity equal to*

$$1 - \frac{1}{2m+2}$$

*for any field alphabet whose characteristic divides  $m$ .*

## 5.4 Network $\mathcal{N}_2(m, w)$

For each  $m \geq 2$  and  $w \geq 1$ , network  $\mathcal{N}_2(m, w)$  is defined in Figure 5.5. We note that  $\mathcal{N}_2(m, 1)$  and  $\mathcal{N}_1(m+1)$  have similar structure, but in network  $\mathcal{N}_1(m+1)$  each of the output edges of  $B(m+1)$  is connected to  $R_x$ , and in network  $\mathcal{N}_2(m, 1)$  all but one of the output edges of  $B(m+1)$  are connected to  $R_z$ . This disconnected edge causes the difference in solvability properties of the two networks. Lemmas 5.4.4, 5.4.5, 5.4.6, and 5.4.7 demonstrate that network  $\mathcal{N}_2(m, w)$  is:

1. non-linearly solvable over alphabet of size  $mw$ , if  $w \geq 2$ ,
2. solvable over  $\mathcal{A}$  only if  $|\mathcal{A}|$  is not relatively prime to  $m$ ,
3. linearly solvable over standard  $R$ -module  $G$  if and only if  $\text{char}(R)$  divides  $m$ ,
4. asymptotically linearly solvable over finite field  $\mathbb{F}$  if and only if  $\text{char}(\mathbb{F})$  divides  $m$ .

**Remark 5.4.1.** *For each  $m \geq 2$  and  $w \geq 1$ , network  $\mathcal{N}_2(m, w)$  has:  $w(m+1)+1$  source nodes,  $w(2m+6)$  intermediate nodes, and  $w(m+2)+1$  receiver nodes. So the total number of nodes in  $\mathcal{N}_2(m, w)$  is  $4mw+9w+2$ .*

For each positive integer  $m$ , we will view the ring  $\mathbb{Z}_m$  as the set  $\{0, 1, \dots, m-1\}$  together with addition and multiplication modulo  $m$ . This ring will be used to construct non-linear solutions in Lemmas 5.4.2, 5.4.4, 5.5.2, and 5.5.4.



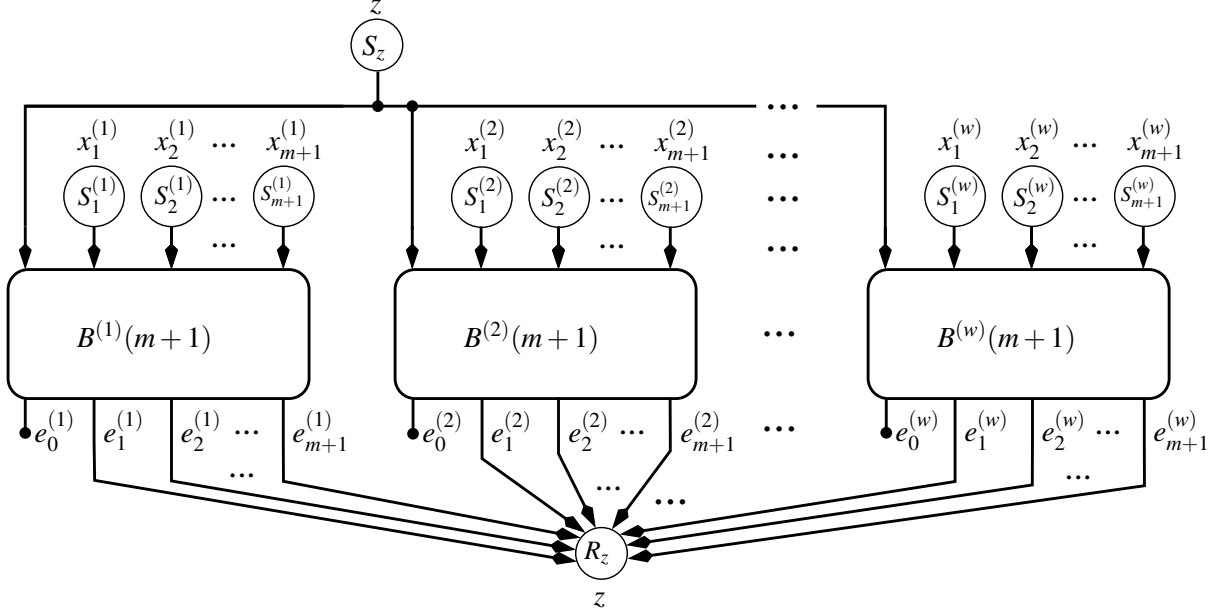


Figure 5.5: The network  $\mathcal{N}_2(m, w)$  is constructed from  $w$  blocks of  $B(m+1)$  together with  $w(m+1) + 1$  source nodes and an additional receiver  $R_z$ . The  $l$ th block is denoted  $B^{(l)}(m+1)$ , and the nodes and edge symbols within  $B^{(l)}(m+1)$  are denoted with a superscript  $l$ . For each  $l = 1, 2, \dots, w$ , the block  $B^{(l)}(m+1)$  has inputs from source nodes  $S_1^{(l)}, S_2^{(l)}, \dots, S_{m+1}^{(l)}$ , which generate message vectors  $x_1^{(l)}, x_2^{(l)}, \dots, x_{m+1}^{(l)}$ . The shared message vector  $z$  is generated by source node  $S_z$  and is the 0th input to each  $B^{(l)}(m+1)$ . Each of the output edges of  $B^{(l)}(m+1)$ , except the 0th, is an input to the shared receiver  $R_z$ , which demands the shared message vector  $z$ .

For each  $m, w \geq 2$  and each  $a \in \mathbb{Z}_{mw}$ , a receiver cannot uniquely determine the symbol  $a$  in  $\mathbb{Z}_{mw}$  from the symbol  $wa \in \mathbb{Z}_{mw}$  since the integer  $w$  is not invertible in  $\mathbb{Z}_{mw}$ . For example, if a receiver receives  $wa = 0$  in  $\mathbb{Z}_{mw}$ , then the symbol  $a$  could be any element in the set  $\{0, m, 2m, \dots, (w-1)m\}$ . The following lemma describes a technique for recovering the value of  $a$  via a decoding function  $\psi$  from the  $w$ -tuple  $w\pi_1(a), w\pi_2(a), \dots, w\pi_w(a)$ , where each  $\pi_i$  is a particular permutation of  $\mathbb{Z}_{mw}$ . This technique will then be used to show that network  $\mathcal{N}_2(m, w)$  is solvable over an alphabet of size  $mw$ .

**Lemma 5.4.2.** *For each  $m \geq 2$  and  $w \geq 1$ , there exists a mapping  $\psi : \mathbb{Z}_{mw}^w \rightarrow \mathbb{Z}_{mw}$  and permutations  $\pi_1, \pi_2, \dots, \pi_w$  of  $\mathbb{Z}_{mw}$  such that for all  $a \in \mathbb{Z}_{mw}$ , we have  $\psi(w\pi_1(a), w\pi_2(a), \dots, w\pi_w(a)) = a$ .*

*Proof.* If  $w = 1$ , let  $\psi$  and  $\pi_1$  be identity permutations. For each  $a \in \mathbb{Z}_{mw}$  we have  $\psi(w\pi_1(a)) = a$ .

Assume  $w > 1$ . By the Euclidean Division Theorem, for each integer  $y$ , there exist unique integers  $q_y, r_y$  such that  $y = q_y m + r_y$  and  $0 \leq r_y < m$ . We have  $wy = w(q_y m + r_y)$ , which implies

$$wy = wr_y \pmod{mw}. \quad (5.10)$$

For all integers  $x, y$  we have

$$\begin{aligned}
wx &= wy \pmod{mw} \\
\iff wr_x &= wr_y \pmod{mw} && \text{[from (5.10)]} \\
\iff r_x &= r_y && \text{[from } 0 \leq r_x, r_y < m\text{]}. \tag{5.11}
\end{aligned}$$

For each  $a = q_a m + r_a \in \mathbb{Z}_{mw}$  such that  $0 \leq r_a < m$ , let  $\hat{r}_a$  be the unique integer in  $\{0, 1, \dots, m-1\}$  such that  $\hat{r}_a = r_a + 1 \pmod{m}$ , and for each  $l = 1, 2, \dots, w-1$ , define permutations of  $\mathbb{Z}_{mw}$  as follows:

$$\pi_l(a) = \begin{cases} q_a m + \hat{r}_a & \text{if } q_a = l \\ q_a m + r_a & \text{otherwise} \end{cases} \tag{5.12}$$

$$\pi_w(a) = a = q_a m + r_a. \tag{5.13}$$

Note that for all  $l = 1, 2, \dots, w-1$ , the (non-linear) permutation  $\pi_l$  modifies the remainder  $r_a$  if  $q_a = l$  and otherwise acts as the identity permutation. Also,  $\pi_w$  is the identity permutation.

For each  $a \in \mathbb{Z}_{mw}$ , we will now show the mapping given by  $a \mapsto (w\pi_1(a), \dots, w\pi_w(a))$  is injective.

For each  $a, b \in \mathbb{Z}_{mw}$ , suppose

$$w\pi_l(a) = w\pi_l(b) \pmod{mw} \quad (l = 1, 2, \dots, w), \tag{5.14}$$

where  $a = q_a m + r_a$  and  $b = q_b m + r_b$ , with  $0 \leq r_a, r_b < m$  and  $0 \leq q_a, q_b < w$ . Then

$$w\pi_w(a) = w\pi_w(b) \pmod{mw} \quad \text{[from (5.14)]} \tag{5.15}$$

$$wr_a = wr_b \pmod{mw} \quad \text{[from (5.10), (5.13), (5.15)]}$$

$$\therefore r_a = r_b \quad \text{[from (5.11)]}. \tag{5.16}$$

Let  $\hat{r}_b$  be the unique integer in  $\{0, 1, \dots, m-1\}$  such that  $\hat{r}_b = r_b + 1 \pmod{m}$ . If  $q_a \neq q_b$ , then without loss of generality,  $q_b \neq 0$ , so

$$w\pi_{q_b}(a) = w\pi_{q_b}(b) \pmod{mw} \quad \text{[from (5.14)]} \tag{5.17}$$

$$\therefore wr_a = w\hat{r}_b \pmod{mw} \quad \text{[from (5.10), (5.12), (5.17)]}$$

$$\therefore r_a = r_a + 1 \pmod{m} \quad \text{[from (5.11), (5.16)],}$$

which is a contradiction, so we must have  $q_a = q_b$ . We have shown  $w\pi_l(a) = w\pi_l(b) \pmod{mw}$  for all  $l$  if and only if  $a = b$ . Thus  $a$  can be uniquely determined from the  $w$ -tuple  $(w\pi_1(a), w\pi_2(a), \dots, w\pi_w(a))$ , which implies the existence of the claimed mapping. ■

**Example 5.4.3.** The following table illustrates the permutations of  $\mathbb{Z}_{12}$  described in Lemma 5.4.2 for the case  $m = 4$  and  $w = 3$ .

| $a = \pi_3(a)$ | $\pi_2(a)$ | $\pi_1(a)$ | $3\pi_3(a)$ | $3\pi_2(a)$ | $3\pi_1(a)$ |
|----------------|------------|------------|-------------|-------------|-------------|
| 0              | 0          | 0          | 0           | 0           | 0           |
| 1              | 1          | 1          | 3           | 3           | 3           |
| 2              | 2          | 2          | 6           | 6           | 6           |
| 3              | 3          | 3          | 9           | 9           | 9           |
| 4              | 4          | 5          | 0           | 0           | 3           |
| 5              | 5          | 6          | 3           | 3           | 6           |
| 6              | 6          | 7          | 6           | 6           | 9           |
| 7              | 7          | 4          | 9           | 9           | 0           |
| 8              | 9          | 8          | 0           | 3           | 0           |
| 9              | 10         | 9          | 3           | 6           | 3           |
| 10             | 11         | 10         | 6           | 9           | 6           |
| 11             | 8          | 11         | 9           | 0           | 9           |

For each  $a \in \mathbb{Z}_{12}$ , the triple  $(3\pi_3(a), 3\pi_2(a), 3\pi_1(a)) \in \mathbb{Z}_{12}^3$  is distinct, so  $a$  can be uniquely determined from  $3\pi_3(a)$ ,  $3\pi_2(a)$ , and  $3\pi_1(a)$ .

The proof of Lemma 5.4.4 describes a (possibly non-linear) solution for  $\mathcal{N}_2(m, w)$ .

**Lemma 5.4.4.** For each  $m \geq 2$  and  $w \geq 1$ , network  $\mathcal{N}_2(m, w)$  is solvable over an alphabet of size  $mw$ .

*Proof.* Let  $\psi$  and  $\pi_1, \pi_2, \dots, \pi_w$  be the mapping and permutations, respectively, from Lemma 5.4.2. Define a  $(1, 1)$  code for network  $\mathcal{N}_2(m, w)$  over the ring  $\mathbb{Z}_{mw}$  for each  $l = 1, 2, \dots, w$  by:

$$\begin{aligned}
e_0^{(l)} &= \sum_{j=1}^{m+1} x_j^{(l)} \\
e_i^{(l)} &= \pi_l(z) + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} x_j^{(l)} && (i = 1, 2, \dots, m+1) \\
e^{(l)} &= \pi_l(z) + \sum_{j=1}^{m+1} x_j^{(l)}.
\end{aligned}$$

For each  $l = 1, 2, \dots, w$ , the receivers within each  $B^{(l)}(m+1)$  block can recover their respective demands as follows:

$$R_0^{(l)} : \pi_l^{-1}(e^{(l)} - e_0^{(l)}) = z \quad \text{and} \quad R_i^{(l)} : e^{(l)} - e_i^{(l)} = x_i^{(l)} \quad (i = 1, 2, \dots, m+1).$$

For each  $l = 1, 2, \dots, w$ , we have

$$\begin{aligned}
w \sum_{i=1}^{m+1} e_i^{(l)} &= w(m+1) \pi_l(z) + mw \sum_{j=1}^{m+1} x_j^{(l)} \\
&= w\pi_l(z) \quad [\text{from } mw = 0 \pmod{mw}].
\end{aligned} \tag{5.18}$$

Receiver  $R_z$  can recover  $z$  from its inputs as follows:

$$\begin{aligned}
R_z &: \psi \left( w \sum_{i=1}^{m+1} e_i^{(1)}, w \sum_{i=1}^{m+1} e_i^{(2)}, \dots, w \sum_{i=1}^{m+1} e_i^{(w)} \right) \\
&= \psi (w\pi_1(z), w\pi_2(z), \dots, w\pi_w(z)) \\
&= z \quad \text{[from (5.18) and Lemma 5.4.2].}
\end{aligned}$$

Thus the code described above is, in fact, a solution for the network  $\mathcal{N}_2(m, w)$ . ■

In the code given in the proof of Lemma 5.4.4, if  $w = 1$ , then  $\pi_1$  and  $\psi$  are identity permutations, so the code is linear. However if  $w > 1$ , then  $\pi_1, \pi_2, \dots, \pi_{w-1}$  are generally non-linear, so the code is non-linear.

**Lemma 5.4.5.** *For each  $m \geq 2$  and  $w \geq 1$ , if network  $\mathcal{N}_2(m, w)$  is solvable over alphabet  $\mathcal{A}$ , then  $m$  and  $|\mathcal{A}|$  are not relatively prime.*

*Proof.* Assume  $\mathcal{N}_2(m, w)$  is solvable over  $\mathcal{A}$ . For each  $l = 1, 2, \dots, w$ , the block  $B^{(l)}(m+1)$  together with source nodes  $S_z, S_1^{(l)}, S_2^{(l)}, \dots, S_{m+1}^{(l)}$  forms a copy of  $\mathcal{N}_0(m+1)$ , so by Lemma 5.2.2, the edge functions within block  $B^{(l)}(m+1)$  must satisfy Property  $P(m+1)$ . Thus, for each  $l$ , there exists an Abelian group  $(\mathcal{A}, \oplus_l)$ , with identity  $0_l \in \mathcal{A}$ , and permutations  $\pi_0^{(l)}, \pi_1^{(l)}, \dots, \pi_{m+1}^{(l)}$  and  $\sigma_0^{(l)}, \sigma_1^{(l)}, \dots, \sigma_{m+1}^{(l)}$  of  $\mathcal{A}$ , such that for each  $i = 1, \dots, m+1$ , the edges carry the symbols:

$$\begin{aligned}
e_0^{(l)} &= \sigma_0^{(l)} \left( \bigoplus_{j=1}^{m+1} \pi_j^{(l)} (x_j^{(l)}) \right) \\
e_i^{(l)} &= \sigma_i^{(l)} \left( \pi_0^{(l)}(z) \oplus_l \bigoplus_{\substack{j=1 \\ j \neq i}}^{m+1} \pi_j^{(l)} (x_j^{(l)}) \right) \\
e^{(l)} &= \pi_0^{(l)}(z) \oplus_l \bigoplus_{j=1}^{m+1} \pi_j^{(l)} (x_j^{(l)}),
\end{aligned} \tag{5.19}$$

where  $\bigoplus$  in each of the previous three equations denotes  $\oplus_l$ .

Now suppose to the contrary that  $m$  and  $|\mathcal{A}|$  are relatively prime. Then by Cauchy's Theorem, for each  $l = 1, 2, \dots, w$ , the group  $(\mathcal{A}, \oplus_l)$  contains no non-identity elements whose order divides  $m$ . That is, for each  $a \in \mathcal{A}$ , we have  $\underbrace{a \oplus_l \cdots \oplus_l a}_{m \text{ adds}} = 0_l$  if and only if  $a = 0_l$ . Let  $a, b \in \mathcal{A}$ . Then we have  $\underbrace{a \oplus_l \cdots \oplus_l a}_{m \text{ adds}} = \underbrace{b \oplus_l \cdots \oplus_l b}_{m \text{ adds}}$  if and only if:

$$\begin{aligned}
\underbrace{(a \oplus_l b) \oplus_l \cdots \oplus_l (a \oplus_l b)}_{m \text{ adds}} &= 0_l && \text{[from } (\mathcal{A}, \oplus_l) \text{ Abelian]} \\
\iff a = b &&& \text{[from } \gcd(m, |\mathcal{A}|) = 1 \text{].}
\end{aligned}$$

Thus, for each  $l$  the mapping  $a \mapsto \underbrace{a \oplus_l \cdots \oplus_l a}_{m \text{ adds}}$  is injective on the finite set  $\mathcal{A}$  and therefore is bijective, and its inverse  $\phi_l : \mathcal{A} \rightarrow \mathcal{A}$  satisfies

$$\underbrace{\phi_l(a) \oplus_l \cdots \oplus_l \phi_l(a)}_{m \text{ adds}} = a \quad (l = 1, 2, \dots, w). \quad (5.20)$$

For each  $a \in \mathcal{A}$  such that  $a \neq 0_1$  and each  $l = 2, \dots, w$ , let

$$f_l(a) = \pi_0^{(l)} \left( \pi_0^{(1)^{-1}}(0_1) \right) \ominus_l \pi_0^{(l)} \left( \pi_0^{(1)^{-1}}(a) \right). \quad (5.21)$$

Define two collections of messages as follows:

$$\begin{cases} x_j^{(1)} = \pi_j^{(1)^{-1}}(\phi_1(a)) \\ x_j^{(l)} = \pi_j^{(l)^{-1}}(0_l) \\ z = \pi_0^{(1)^{-1}}(0_1) \end{cases} \quad \text{and} \quad \begin{cases} \hat{x}_j^{(1)} = \pi_j^{(1)^{-1}}(0_1) \\ \hat{x}_j^{(l)} = \pi_j^{(l)^{-1}}(\phi_l(f_l(a))) \\ \hat{z} = \pi_0^{(1)^{-1}}(a), \end{cases}$$

where  $l = 2, \dots, w$  and  $j = 1, 2, \dots, m+1$ . Since  $a \neq 0_1$  and  $\pi_0^{(1)}$  is bijective, it follows that  $z \neq \hat{z}$ .

By Property  $P(m+1)$  and (5.19), for each  $i = 1, 2, \dots, m+1$  and each  $l = 2, \dots, w$ , we have:

$$\begin{aligned} e_i^{(1)} &= \sigma_i^{(1)} \left( \underbrace{\phi_1(a) \oplus_1 \cdots \oplus_1 \phi_1(a)}_{m \text{ adds}} \right) = \sigma_i^{(1)}(a) && \text{[from (5.20)]} \\ e_i^{(l)} &= \sigma_i^{(l)} \left( \pi_0^{(l)} \left( \pi_0^{(1)^{-1}}(0_1) \right) \right) \end{aligned}$$

for the messages  $x_j^{(l)}$ ,  $z$ , and

$$\begin{aligned} e_i^{(1)} &= \sigma_i^{(1)}(a) \\ e_i^{(l)} &= \sigma_i^{(l)} \left( \pi_0^{(l)} \left( \pi_0^{(1)^{-1}}(a) \right) \oplus_l \underbrace{\phi_l(f_l(a)) \oplus_l \cdots \oplus_l \phi_l(f_l(a))}_{m \text{ adds}} \right) \\ &= \sigma_i^{(l)} \left( \pi_0^{(l)} \left( \pi_0^{(1)^{-1}}(a) \right) \oplus_l f_l(a) \right) && \text{[from (5.20)]} \\ &= \sigma_i^{(l)} \left( \pi_0^{(l)} \left( \pi_0^{(1)^{-1}}(0_1) \right) \right) && \text{[from (5.21)]} \end{aligned}$$

for the messages  $\hat{x}_j^{(l)}$ ,  $\hat{z}$ . For both collections of messages, the edge symbols  $e_i^{(l)}$  are the same for all  $l = 1, 2, \dots, w$  and  $i = 1, 2, \dots, m+1$ , and therefore the decoded value  $z$  at  $R_z$  must be the same. However, this contradicts the fact that  $z \neq \hat{z}$ . ■

Lemmas 5.4.4 and 5.4.5 together provide a partial characterization of the alphabet sizes over which network  $\mathcal{N}_2$  is solvable. However, these conditions are sufficient for showing our main results. Lemma 5.4.6 characterizes a necessary and sufficient condition for the linear solvability of network  $\mathcal{N}_2(m, w)$  over standard modules.

**Lemma 5.4.6.** *Let  $m \geq 2$  and  $w \geq 1$ , and let  $G$  be a standard  $R$ -module. Then network  $\mathcal{N}_2(m, w)$  is linearly solvable over  $G$  if and only if  $\text{char}(R)$  divides  $m$ .*

*Proof.* For any ring  $R$  with multiplicative identity  $1_R$ , the characteristic of  $R$  divides  $m$  if and only if  $m = m 1_R = 0_R$ , so it suffices to show that for each  $m, w$  and each standard  $R$ -module  $G$ , network  $\mathcal{N}_2(m, w)$  is linearly solvable over  $G$  if and only if  $m = 0_R$ .

Assume network  $\mathcal{N}_2(m, w)$  is linearly solvable over the standard  $R$ -module  $G$ . The messages are drawn from  $G$ , and there exist  $c_{i,j}^{(l)}, c_j^{(l)} \in R$ , such that for each  $l = 1, 2, \dots, w$  and each  $i = 1, 2, \dots, m+1$ , the edge symbols can be written as:

$$e_0^{(l)} = \bigoplus_{j=1}^{m+1} \left( c_{0,j}^{(l)} \cdot x_j^{(l)} \right) \quad (5.22)$$

$$e_i^{(l)} = \left( c_{i,0}^{(l)} \cdot z \right) \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m+1} \left( c_{i,j}^{(l)} \cdot x_j^{(l)} \right) \quad (5.23)$$

$$e^{(l)} = \left( c_0^{(l)} \cdot z \right) \oplus \bigoplus_{j=1}^{m+1} \left( c_j^{(l)} \cdot x_j^{(l)} \right) \quad (5.24)$$

and there exist  $d_{i,e}^{(l)}, d_i^{(l)} \in R$ , such that each receiver within  $B^{(l)}(m+1)$  can linearly recover its respective demands from its received edge symbols by:

$$R_0^{(l)} : z = \left( d_{0,e}^{(l)} \cdot e^{(l)} \right) \oplus \left( d_0^{(l)} \cdot e_0^{(l)} \right) \quad (5.25)$$

$$R_i^{(l)} : x_i^{(l)} = \left( d_{i,e}^{(l)} \cdot e^{(l)} \right) \oplus \left( d_i^{(l)} \cdot e_i^{(l)} \right). \quad (5.26)$$

Since  $R_z$  linearly recovers  $z$  from its inputs, there exists  $d_{z,i}^{(l)} \in R$  such that

$$R_z : z = \bigoplus_{l=1}^w \bigoplus_{i=1}^{m+1} \left( d_{z,i}^{(l)} \cdot e_i^{(l)} \right). \quad (5.27)$$

For each  $l = 1, 2, \dots, w$ , the block  $B^{(l)}(m+1)$  together with source nodes  $S_z, S_1^{(l)}, S_2^{(l)}, \dots, S_{m+1}^{(l)}$  forms a copy of network  $\mathcal{N}_0(m+1)$ , so by Lemma 5.2.3 and (5.22) – (5.26), each  $c_i^{(l)}$  and each  $d_i^{(l)}$  is invertible in  $R$ , and for each distinct  $i, j \in \{0, 1, \dots, m+1\}$ , we have

$$c_{i,j}^{(l)} = -d_i^{(l)-1} d_{i,e}^{(l)} c_j^{(l)}. \quad (5.28)$$

Equating message components at  $R_z$  yields:

$$\begin{aligned} 1_R &= \sum_{l=1}^w \sum_{i=1}^{m+1} d_{z,i}^{(l)} c_{i,0}^{(l)} && \text{[from (5.23), (5.27)]} \\ &= - \sum_{l=1}^w \sum_{i=1}^{m+1} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} c_0^{(l)} && \text{[from (5.28)]} \end{aligned} \quad (5.29)$$

and for each  $l = 1, 2, \dots, w$  and each  $j = 1, 2, \dots, m+1$ ,

$$\begin{aligned}
0_R &= \sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)} c_{i,j}^{(l)} && \text{[from (5.23), (5.27)]} \\
&= - \left( \sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} \right) c_j^{(l)} && \text{[from (5.28)]} \\
&= \sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} c_0^{(l)} && \left[ \text{from right multiplying by } -c_j^{(l)-1} c_0^{(l)} \right] \tag{5.30}
\end{aligned}$$

and by summing (5.30) over  $j = 1, 2, \dots, m+1$ , we have

$$\begin{aligned}
0_R &= \sum_{j=1}^{m+1} \sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} c_0^{(l)} \\
&= m \sum_{i=1}^{m+1} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} c_0^{(l)}. \tag{5.31}
\end{aligned}$$

By summing (5.31) over  $l = 1, 2, \dots, w$ , we have

$$\begin{aligned}
0_R &= m \sum_{i=1}^w \sum_{i=1}^{m+1} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} c_0^{(l)} && \text{[from (5.31)]} \\
&= m && \text{[from (5.29)].}
\end{aligned}$$

To prove the converse, let  $G$  be a standard  $R$ -module such that  $m = 0_R$ . Define a linear code over  $G$  such that for each  $l = 1, 2, \dots, w$ , we have

$$\begin{aligned}
e_0^{(l)} &= \bigoplus_{j=1}^{m+1} x_j^{(l)} \\
e_i^{(l)} &= z \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m+1} x_j^{(l)} && (i = 1, 2, \dots, m+1) \\
e^{(l)} &= z \oplus \bigoplus_{j=1}^{m+1} x_j^{(l)}.
\end{aligned}$$

For each  $l = 1, 2, \dots, w$ , the receivers within each block  $B^{(l)}(m+1)$  can linearly recover their respective demands as follows:

$$R_0^{(l)} : e^{(l)} \ominus e_0^{(l)} = z \quad \text{and} \quad R_i^{(l)} : e^{(l)} \ominus e_i^{(l)} = x_i^{(l)} \quad (i = 1, 2, \dots, m+1).$$

Since  $m = 0_R$  in  $R$ , receiver  $R_z$  can linearly recover  $z$  as follows:

$$R_z : \bigoplus_{i=1}^{m+1} e_i^{(1)} = z \oplus (mz) \oplus \left( m \bigoplus_{j=1}^{m+1} x_j^{(1)} \right) = z.$$

Thus the code is a linear solution for  $\mathcal{N}_2(m, w)$ . ■

By Lemma 5.4.4, for every  $m, w \geq 2$ , network  $\mathcal{N}_2(m, w)$  is solvable over the ring  $\mathbb{Z}_{mw}$ , but the characteristic of  $\mathbb{Z}_{mw}$  is  $mw$ , which does not divide  $m$ , so by Lemma 5.4.6, the solution is necessarily non-linear. The following lemma provides a partial characterization of the linear capacity of  $\mathcal{N}_2(m, w)$  over finite-field alphabets.

**Lemma 5.4.7.** *For each  $m \geq 2$  and  $w \geq 1$ , network  $\mathcal{N}_2(m, w)$  has*

- (a) *capacity equal to 1,*
- (b) *linear capacity equal to 1 for any finite-field alphabet whose characteristic divides  $m$ ,*
- (c) *linear capacity upper bounded by  $1 - \frac{1}{2mw+2w+1}$  for any finite-field alphabet whose characteristic does not divide  $m$ .*

Improving these upper-bounds on the linear capacities and/or finding codes at these rates are left as open problems. The problems appear to be non-trivial, and such improvements are unrelated to the main results of this paper.

## 5.5 Network $\mathcal{N}_3(m_1, m_2)$

For each  $m_1, m_2 \geq 2$ , network  $\mathcal{N}_3(m_1, m_2)$  is defined in Figure 5.6. We note that  $\mathcal{N}_2(m, 2)$  and  $\mathcal{N}_3(m+1, m+1)$  have similar structure, with the exception of the disconnected output edge of each  $B(m+1)$  in  $\mathcal{N}_2(m, 2)$ . This disconnected edge causes the difference in solvability properties of the two networks. Corollary 5.5.7 and Lemmas 5.5.5, 5.5.6, and 5.5.8 demonstrate that network  $\mathcal{N}_3(m_1, m_2)$  is:

1. non-linearly solvable over an alphabet of size  $tm_1^{\alpha+1}$ , when  $m_2 = sm_1^\alpha$ , where  $\alpha, s, t \geq 1$  and  $s$  and  $t$  are relatively prime to  $m_1$ ,
2. solvable over alphabet  $\mathcal{A}$  only if  $|\mathcal{A}|$  is relatively prime to  $m_1$  or  $|\mathcal{A}|$  does not divide  $m_2$ ,
3. linearly solvable over standard  $R$ -module  $G$  if and only if  $\gcd(\text{char}(R), m_1, m_2) = 1$ ,
4. asymptotically linearly solvable over finite field  $\mathbb{F}$  if and only if  $\text{char}(\mathbb{F})$  is relatively prime to  $m_1$  or  $m_2$ .

**Remark 5.5.1.** *For each  $m_1, m_2 \geq 2$ , the network  $\mathcal{N}_3(m_1, m_2)$  has  $m_1 + m_2 + 1$  source nodes,  $2(m_1 + m_2 + 4)$  intermediate nodes, and  $m_1 + m_2 + 3$  receiver nodes, so the total number of nodes in  $\mathcal{N}_3(m_1, m_2)$  is  $4m_1 + 4m_2 + 12$ .*

The following lemmas demonstrate that  $\mathcal{N}_3(m_1, m_2)$  is non-linearly solvable when  $m_2 = sm_1^\alpha$ , where  $\alpha \geq 1$  and  $s$  is relatively prime to  $m_1$ . Consider the ring alphabet  $\mathbb{Z}_{m_1^{\alpha+1}}$ . For every  $a \in \mathbb{Z}_{m_1^{\alpha+1}}$ , a receiver cannot uniquely determine a symbol  $a$  from the symbols  $m_1a$  and  $sm_1^\alpha a$ , since the integer  $m_1$  is not invertible in  $\mathbb{Z}_{m_1^{\alpha+1}}$ . For example, if a receiver receives  $m_1a = sm_1^\alpha a = 0 \in \mathbb{Z}_{m_1^{\alpha+1}}$ , then the symbol  $a$  could be any



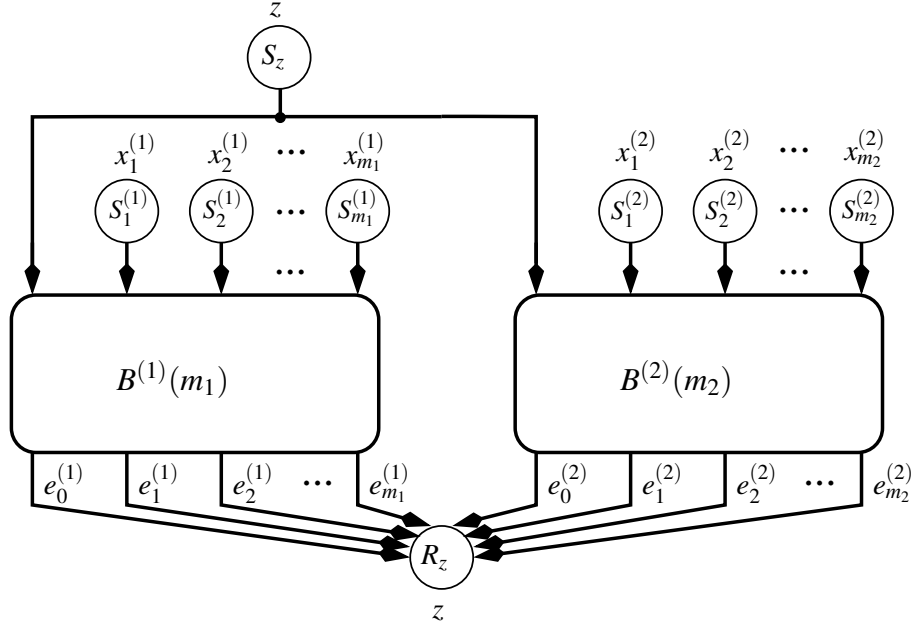


Figure 5.6: The network  $\mathcal{N}_3(m_1, m_2)$  is constructed from  $B(m_1)$  and  $B(m_2)$  blocks together with  $m_1 + m_2 + 1$  source nodes and an additional receiver  $R_z$ . The blocks are denoted  $B^{(1)}(m_1)$  and  $B^{(2)}(m_2)$  respectively, and for each  $l = 1, 2$ , the nodes and edge symbols in  $B^{(l)}(m_l)$  are denoted with a superscript  $l$ . Each  $B^{(l)}(m_l)$  block has inputs from source nodes  $S_1^{(l)}, S_2^{(l)}, \dots, S_{m_l}^{(l)}$ , which generate message vectors  $x_1^{(l)}, x_2^{(l)}, \dots, x_{m_l}^{(l)}$ . The shared message vector  $z$  is generated by source node  $S_z$  and is the 0th input to  $B^{(l)}(m_l)$ . The additional receiver  $R_z$  receives all of the output edges of  $B^{(1)}(m_1)$  and  $B^{(2)}(m_2)$  and demands the shared message vector  $z$ .

element in the set  $\{0, m_1^\alpha, 2m_1^\alpha, \dots, (m_1 - 1)m_1^\alpha\}$ . The following lemma describes a technique for recovering the value of  $a$  via a decoding function  $\psi$  from  $m_1\pi_1(a)$  and  $sm_1^\alpha\pi_2(a)$ , where  $\pi_1$  and  $\pi_2$  are particular permutations of  $\mathbb{Z}_{m_1^{\alpha+1}}$ . This technique will be used to show that, in some cases, network  $\mathcal{N}_3$  has non-linear solutions.

**Lemma 5.5.2.** *Let  $m \geq 2$  and  $\alpha, s \geq 1$  be integers such that  $s$  is relatively prime to  $m$ . Then there exist permutations  $\pi_1$  and  $\pi_2$  of  $\mathbb{Z}_{m^{\alpha+1}}$  and a mapping  $\psi: \mathbb{Z}_{m^{\alpha+1}}^2 \rightarrow \mathbb{Z}_{m^{\alpha+1}}$  such that for all  $a \in \mathbb{Z}_{m^{\alpha+1}}$ ,*

$$\psi(m\pi_1(a), sm^\alpha\pi_2(a)) = a.$$

*Proof.* Define permutations  $\pi_1, \pi_2$  of  $\mathbb{Z}_{m^{\alpha+1}}$  as follows. For each  $a \in \mathbb{Z}_{m^{\alpha+1}}$ , let  $\sum_{i=0}^{\alpha} m^i a_i$  denote the base  $m$  representation of  $a$ . We define

$$\pi_1(a) = m^\alpha a_0 + \sum_{i=1}^{\alpha} m^{i-1} a_i \tag{5.32}$$

$$\pi_2(a) = a = \sum_{i=0}^{\alpha} m^i a_i. \tag{5.33}$$

The (non-linear) permutation  $\pi_1$  performs a right-cyclic shift of the base- $m$  digits of  $a$ , and  $\pi_2$  is the identity permutation. For each  $a \in \mathbb{Z}_{m^{\alpha+1}}$ , we will show that the mapping given by  $a \mapsto (m\pi_1(a), sm^\alpha\pi_2(a))$  is injective. For each  $a, b \in \mathbb{Z}_{m^{\alpha+1}}$ , suppose

$$m\pi_1(a) = m\pi_1(b) \pmod{m^{\alpha+1}} \quad (5.34)$$

$$sm^\alpha\pi_2(a) = sm^\alpha\pi_2(b) \pmod{m^{\alpha+1}} \quad (5.35)$$

where  $a = \sum_{i=0}^{\alpha} m^i a_i$  and  $b = \sum_{i=0}^{\alpha} m^i b_i$ . Then we have

$$\sum_{i=1}^{\alpha} m^i a_i = \sum_{i=1}^{\alpha} m^i b_i \pmod{m^{\alpha+1}} \quad [\text{from (5.32), (5.34)}].$$

Therefore

$$\begin{aligned} a_i &= b_i & (i = 1, 2, \dots, \alpha) & \quad [\text{from } 0 \leq a_i, b_i < m] \\ sm^\alpha a_0 &= sm^\alpha b_0 & \pmod{m^{\alpha+1}} & \quad [\text{from (5.33), (5.35)}] \\ \therefore m^\alpha a_0 &= m^\alpha b_0 & \pmod{m^{\alpha+1}} & \quad [\text{from } \gcd(m, s) = 1] \\ \therefore a_0 &= b_0 & & \quad [\text{from } 0 \leq a_0, b_0 < m]. \end{aligned}$$

Thus  $a = b$ . We have shown that  $a = b$  if and only if  $m\pi_1(a) = m\pi_1(b)$  and  $sm^\alpha\pi_2(a) = sm^\alpha\pi_2(b)$ . Thus  $a$  can be uniquely determined from  $m\pi_1(a)$  and  $sm^\alpha\pi_2(a)$ . This implies the existence of the claimed mapping. ■

**Example 5.5.3.** The table below illustrates the permutations of  $\mathbb{Z}_8$  described in Lemma 5.5.2 for the case  $m = 2, s = 3$ , and  $\alpha = 2$ .

| $a = \pi_2(a)$ | $\pi_1(a)$ | $12\pi_2(a)$ | $2\pi_1(a)$ |
|----------------|------------|--------------|-------------|
| 0              | 0          | 0            | 0           |
| 1              | 4          | 4            | 0           |
| 2              | 1          | 0            | 2           |
| 3              | 5          | 4            | 2           |
| 4              | 2          | 0            | 4           |
| 5              | 6          | 4            | 4           |
| 6              | 3          | 0            | 6           |
| 7              | 7          | 4            | 6           |

For each  $a \in \mathbb{Z}_8$ , the pair  $(2\pi_1(a), 12\pi_2(a)) \in \mathbb{Z}_8^2$  is distinct. Hence  $a$  can uniquely be determined from  $2\pi_1(a)$  and  $12\pi_2(a)$ .

**Lemma 5.5.4.** Let  $m_1, m_2 \geq 2$  and  $\alpha, s \geq 1$  be integers such that  $m_2 = sm_1^\alpha$  and  $s$  is relatively prime to  $m_1$ . Then network  $\mathcal{N}_3(m_1, m_2)$  is solvable over an alphabet of size  $m_1^{\alpha+1}$ .

*Proof.* Let  $\pi_1, \pi_2$  and  $\psi$  be the permutations and mapping, respectively, from Lemma 5.5.2. Define a  $(1, 1)$  code for the network  $\mathcal{N}_3(m_1, m_2)$  over the ring  $\mathbb{Z}_{m_1^{\alpha+1}}$ , for each  $l = 1, 2$ , by:

$$\begin{aligned} e_0^{(l)} &= \sum_{j=1}^{m_l} x_j^{(l)} \\ e_i^{(l)} &= \pi_l(z) + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} x_j^{(l)} && (i = 1, 2, \dots, m_l) \\ e^{(l)} &= \pi_l(z) + \sum_{j=1}^{m_l} x_j^{(l)}. \end{aligned}$$

For each  $l = 1, 2$ , the receivers within the block  $B^{(l)}(m_l)$  can recover their respective demands as follows:

$$R_0^{(l)} : \pi_l^{-1} \left( e^{(l)} - e_0^{(l)} \right) = z \quad \text{and} \quad R_i^{(l)} : e^{(l)} - e_i^{(l)} = x_i^{(l)} \quad (i = 1, 2, \dots, m_l).$$

For each  $l = 1, 2$ , we have

$$-m_l e_0^{(l)} + \sum_{i=0}^{m_l} e_i^{(l)} = -m_l \sum_{j=1}^{m_l} x_j^{(l)} + m_l \pi_l(z) + m_l \sum_{j=1}^{m_l} x_j^{(l)} = m_l \pi_l(z). \quad (5.36)$$

The receiver  $R_z$  can recover  $z$  from its inputs as follows:

$$\begin{aligned} \psi \left( -m_1 e_0^{(1)} + \sum_{i=0}^{m_1} e_i^{(1)}, -m_2 e_0^{(2)} + \sum_{i=0}^{m_2} e_i^{(2)} \right) &= \psi(m_1 \pi_1(z), m_2 \pi_2(z)) && [\text{from (5.36)}] \\ &= \psi(m_1 \pi_1(z), sm_1^\alpha \pi_2(z)) && [\text{from } m_2 = sm_1^\alpha] \\ &= z && [\text{from Lemma 5.5.2}]. \end{aligned}$$

Thus the code described above is, in fact, a solution for the network  $\mathcal{N}_3(m_1, m_2)$ . ■

**Lemma 5.5.5.** *Let  $m_1, m_2 \geq 2$ . If network  $\mathcal{N}_3(m_1, m_2)$  is solvable over alphabet  $\mathcal{A}$  and  $|\mathcal{A}|$  divides  $m_2$ , then  $m_1$  and  $|\mathcal{A}|$  are relatively prime.*

*Proof.* Assume  $\mathcal{N}_3(m_1, m_2)$  is solvable over the alphabet  $\mathcal{A}$ . For each  $l = 1, 2$  the block  $B^{(l)}(m_l)$  together with the source nodes  $S_z, S_1^{(l)}, S_2^{(l)}, \dots, S_{m_l}^{(l)}$  forms a copy of  $\mathcal{N}_0(m_l)$ , so by Lemma 5.2.2, the edge functions within  $B^{(1)}(m_1)$  and  $B^{(2)}(m_2)$  must satisfy Property  $P(m_1)$  and Property  $P(m_2)$ , respectively. Thus there exist Abelian groups  $(\mathcal{A}, \oplus_1)$  and  $(\mathcal{A}, \oplus_2)$  with identity elements  $0_1$  and  $0_2$  for the left-hand side and right-hand side of the network, respectively, and permutations  $\pi_0^{(l)}, \pi_1^{(l)}, \dots, \pi_{m_l}^{(l)}$  and  $\sigma_0^{(l)}, \sigma_1^{(l)}, \dots, \sigma_{m_l}^{(l)}$  of  $\mathcal{A}$ , such

that for each  $l = 1, 2$  and each  $i = 1, 2, \dots, m_l$ , the edges carry the symbols:

$$e_0^{(l)} = \sigma_0^{(l)} \left( \bigoplus_{j=1}^{m_l} \pi_j^{(l)} (x_j^{(l)}) \right) \quad (5.37)$$

$$e_i^{(l)} = \sigma_i^{(l)} \left( \pi_0^{(l)}(z) \oplus_l \bigoplus_{\substack{j=1 \\ j \neq i}}^{m_l} \pi_j^{(l)} (x_j^{(l)}) \right) \quad (5.38)$$

$$e^{(l)} = \pi_0^{(l)}(z) \oplus_l \bigoplus_{j=1}^{m_l} \pi_j^{(l)} (x_j^{(l)})$$

where  $\bigoplus$  in each of the previous three equations denotes  $\oplus_l$ .

Now suppose to the contrary that  $m_1$  and  $|\mathcal{A}|$  are not relatively prime and  $|\mathcal{A}|$  divides  $m_2$ . Then, since  $(\mathcal{A}, \oplus_2)$  is a finite group, for all  $a \in \mathcal{A}$ , we have

$$\underbrace{a \oplus_2 \cdots \oplus_2 a}_{m_2 \text{ adds}} = 0_2 \quad [\text{from } |\mathcal{A}| \mid m_2]. \quad (5.39)$$

Since  $m_1$  and  $|\mathcal{A}|$  are not relatively prime,  $m_1$  and  $|\mathcal{A}|$  share a common factor  $p$ . Since  $p \mid |\mathcal{A}|$ , by Cauchy's Theorem, there exists  $a \in \mathcal{A} \setminus \{0_1\}$  such that the order of  $a$  is  $p$ , and since  $p$  divides  $m_1$  we have  $\underbrace{a \oplus_1 \cdots \oplus_1 a}_{m_1 \text{ adds}} = 0_1$ . Define two collections of messages as follows:

$$\begin{aligned} x_j^{(1)} &= \pi_j^{(1)-1}(0_1) & \text{and} & & \hat{x}_j^{(1)} &= \pi_j^{(1)-1}(a) & (j = 1, 2, \dots, m_1) \\ x_j^{(2)} &= \pi_j^{(2)-1} \left( \pi_0^{(2)} \left( \pi_0^{(1)-1}(0_1) \right) \right) & \text{and} & & \hat{x}_j^{(2)} &= \pi_j^{(2)-1} \left( \pi_0^{(2)} \left( \pi_0^{(1)-1}(a) \right) \right) & (j = 1, 2, \dots, m_2) \\ z &= \pi_0^{(1)-1}(0_1) & \text{and} & & \hat{z} &= \pi_0^{(1)-1}(a). \end{aligned}$$

Since  $a \neq 0_1$  and  $\pi_0^{(1)}$  is bijective, it follows that  $z \neq \hat{z}$ .

By Properties  $P(m_1)$  and  $P(m_2)$ , (5.37), (5.38), and (5.39) we have

$$\begin{aligned} e_i^{(1)} &= \sigma_i^{(1)} \left( \underbrace{0_1 \oplus_1 \cdots \oplus_1 0_1}_{m_1 \text{ adds}} \right) = \sigma_i^{(1)}(0_1) & (i = 0, 1, \dots, m_1) \\ e_i^{(2)} &= \sigma_i^{(2)} \left( \underbrace{\pi_0^{(2)} \left( \pi_0^{(1)-1}(0_1) \right) \oplus_2 \cdots \oplus_2 \pi_0^{(2)} \left( \pi_0^{(1)-1}(0_1) \right)}_{m_2 \text{ adds}} \right) = \sigma_i^{(2)}(0_2) & (i = 0, 1, \dots, m_2) \end{aligned}$$

for the messages  $x_j^{(l)}, z$ , and

$$e_i^{(1)} = \sigma_i^{(1)} \left( \underbrace{a \oplus_1 \cdots \oplus_1 a}_{m_1 \text{ adds}} \right) = \sigma_i^{(1)}(0_1) \quad (i = 0, 1, \dots, m_1)$$

$$e_i^{(2)} = \sigma_i^{(2)} \left( \underbrace{\pi_0^{(2)} \left( \pi_0^{(1)-1}(a) \right) \oplus_2 \cdots \oplus_2 \pi_0^{(2)} \left( \pi_0^{(1)-1}(a) \right)}_{m_2 \text{ adds}} \right) = \sigma_i^{(2)}(0_2) \quad (i = 0, 1, \dots, m_2)$$

for the messages  $\hat{x}_j^{(l)}, \hat{z}$ . For both collections of messages, the incoming edge symbols at  $R_z$  are the same, and therefore the decoded value  $z$  at  $R_z$  must be the same. However, this contradicts the fact that  $z \neq \hat{z}$ . ■

Lemmas 5.5.4 and 5.5.5 together provide a partial characterization of the alphabet sizes over which network  $\mathcal{N}_3$  is solvable. However, these conditions are sufficient for showing our main results. Lemma 5.5.6 characterizes a necessary and sufficient condition for the linear solvability of network  $\mathcal{N}_3(m_1, m_2)$  over standard modules.

**Lemma 5.5.6.** *Let  $m_1, m_2 \geq 2$ , and let  $G$  be a standard  $R$ -module. Then network  $\mathcal{N}_3(m_1, m_2)$  is linearly solvable over  $G$  if and only if  $\gcd(\text{char}(R), m_1, m_2) = 1$ .*

*Proof.* For any integers  $a, b, c \geq 1$ , we have  $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$ , so by Lemma 5.1.4 the integer  $\gcd(m_1, m_2)$  is invertible in the ring  $R$  if and only if  $\gcd(m_1, m_2, \text{char}(R)) = 1$ . Thus it suffices to show that for each  $m_1, m_2$  and each standard  $R$ -module  $G$ , network  $\mathcal{N}_3(m_1, m_2)$  is linearly solvable over  $G$  if and only if  $\gcd(m_1, m_2)$  is invertible in  $R$ .

Assume network  $\mathcal{N}_3(m_1, m_2)$  is linearly solvable over standard  $R$ -module  $G$ . The messages are drawn from  $G$ , and there exist  $c_{i,j}^{(l)}, c_j^{(l)} \in R$ , such that for each  $l = 1, 2$  and each  $i = 1, 2, \dots, m_l$ , the edge symbols can be written as:

$$e_0^{(l)} = \bigoplus_{j=1}^{m_l} \left( c_{0,j}^{(l)} \cdot x_j^{(l)} \right) \quad (5.40)$$

$$e_i^{(l)} = \left( c_{i,0}^{(l)} \cdot z \right) \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m_l} \left( c_{i,j}^{(l)} \cdot x_j^{(l)} \right) \quad (5.41)$$

$$e^{(l)} = \left( c_0^{(l)} \cdot z \right) \oplus \bigoplus_{j=1}^{m_l} \left( c_j^{(l)} \cdot x_j^{(l)} \right) \quad (5.42)$$

and there exist  $d_{i,e}^{(l)}, d_i^{(l)} \in R$ , such that each receiver within  $B^{(l)}(m_l)$  can linearly recover its respective

demand from its received edge symbols by:

$$R_0^{(l)} : z = \left( d_{0,e}^{(l)} \cdot e^{(l)} \right) \oplus \left( d_0^{(l)} \cdot e_0^{(l)} \right) \quad (5.43)$$

$$R_i^{(l)} : x_i^{(l)} = \left( d_{i,e}^{(l)} \cdot e^{(l)} \right) \oplus \left( d_i^{(l)} \cdot e_i^{(l)} \right). \quad (5.44)$$

Since  $R_z$  linearly recovers  $z$  from its inputs, there exists  $d_{z,i}^{(l)} \in R$  such that

$$R_z : z = \bigoplus_{l=1}^2 \bigoplus_{i=0}^{m_l} \left( d_{z,i}^{(l)} \cdot e_i^{(l)} \right). \quad (5.45)$$

For each  $l = 1, 2$  the block  $B^{(l)}(m_l)$  together with the source nodes  $S_z, S_1^{(l)}, S_2^{(l)}, \dots, S_{m_l}^{(l)}$  forms a copy of  $\mathcal{N}_0(m_l)$ , so by Lemma 5.2.3 and (5.40) – (5.44), each  $c_i^{(l)}$  and each  $d_i^{(l)}$  is invertible in  $R$ , and for each distinct  $i, j \in \{0, 1, \dots, m_l\}$ , we have

$$c_{i,j}^{(l)} = -d_i^{(l)-1} d_{i,e}^{(l)} c_j^{(l)}. \quad (5.46)$$

Equating message components at  $R_z$  yields:

$$\begin{aligned} 1_R &= \sum_{l=1}^2 \sum_{i=1}^{m_l} d_{z,i}^{(l)} c_{i,0}^{(l)} && \text{[from (5.40), (5.41), (5.45)]} \\ &= - \sum_{l=1}^2 \sum_{i=1}^{m_l} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} c_0^{(l)} && \text{[from (5.46)]} \end{aligned} \quad (5.47)$$

and for each  $l = 1, 2$  and each  $j = 1, 2, \dots, m_l$ , we have

$$\begin{aligned} 0_R &= \sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} c_{i,j}^{(l)} && \text{[from (5.40), (5.41), (5.45)]} \\ &= - \left( \sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} \right) c_j^{(l)} && \text{[from (5.46)]} \\ &= \sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} c_0^{(l)} && \left[ \text{from right multiplying by } c_j^{(l)-1} c_0^{(l)} \right] \end{aligned} \quad (5.48)$$

Summing (5.48) over  $l = 1, 2$  and  $j = 1, 2, \dots, m_l$  and subtracting (5.47), yields

$$\begin{aligned} -1_R &= \sum_{l=1}^2 \sum_{j=0}^{m_l} \sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} c_0^{(l)} \\ &= \sum_{l=1}^2 m_l \sum_{i=0}^{m_l} d_{z,i}^{(l)} d_i^{(l)-1} d_{i,e}^{(l)} c_0^{(l)}. \end{aligned} \quad (5.49)$$

Equation (5.49) implies there exist  $r_1, r_2 \in R$  such that

$$1_R = m_1 r_1 + m_2 r_2. \quad (5.50)$$

Since  $\gcd(m_1, m_2)$  can be factored out of both terms on the right-hand side of equation (5.50), the ring element  $\gcd(m_1, m_2)$  is invertible.

To prove the converse, let  $G$  be a standard  $R$ -module, such that  $\gcd(m_1, m_2)$  is invertible in  $R$ . Define a linear code over  $G$  for  $\mathcal{N}_3(m_1, m_2)$ , for each  $l = 1, 2$ , by:

$$\begin{aligned} e_0^{(l)} &= \bigoplus_{j=1}^{m_l} x_j^{(l)} \\ e_i^{(l)} &= z \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m_l} x_j^{(l)} && (i = 1, 2, \dots, m_l) \\ e^{(l)} &= z \oplus \bigoplus_{j=1}^{m_l} x_j^{(l)}. \end{aligned}$$

For each  $l = 1, 2$ , the receivers within  $B^{(l)}(m_l)$  can linearly recover their respective demands by:

$$\begin{aligned} R_0^{(l)} : e^{(l)} \ominus e_0^{(l)} &= z \\ R_i^{(l)} : e^{(l)} \ominus e_i^{(l)} &= x_i^{(l)} && (i = 1, 2, \dots, m_l). \end{aligned}$$

Let  $m'_1 = m_1/\gcd(m_1, m_2)$  and  $m'_2 = m_2/\gcd(m_1, m_2)$ . Then  $m'_1$  and  $m'_2$  are relatively prime, so there exist  $n_1, n_2 \in \mathbb{Z}$  such that  $n_1 m'_1 + n_2 m'_2 = 1$ . Thus in  $R$  we have  $(n_1 m'_1) 1_R + (n_2 m'_2) 1_R = 1_R$ .

Receiver  $R_z$  can linearly recover message  $z$  as follows:

$$\begin{aligned} R_z : & \bigoplus_{l=1}^2 \left( \left( n_l \gcd(m_1, m_2)^{-1} \right) \cdot \left( \bigoplus_{i=0}^{m_l} e_i^{(l)} \ominus (m_l e_0^{(l)}) \right) \right) \\ &= \bigoplus_{l=1}^2 \left( \left( n_l \gcd(m_1, m_2)^{-1} \right) \cdot (m_l z) \right) \\ &= (n_1 m'_1 z) \oplus (n_2 m'_2 z) = ((n_1 m'_1) 1_R + (n_2 m'_2) 1_R) z = z. \end{aligned}$$

Thus the code is a linear solution for  $\mathcal{N}_3(m_1, m_2)$ . ■

Corollary 5.5.7 uses Lemmas 5.5.4 and 5.5.6 to show that network  $\mathcal{N}_3$  is solvable over additional alphabet sizes.

**Corollary 5.5.7.** *Let  $m_1, m_2 \geq 2$  and  $\alpha, s, t \geq 1$  be integers such that  $m_2 = s m_1^\alpha$  and  $s$  and  $t$  are relatively prime to  $m_1$ . Then the network  $\mathcal{N}_3(m_1, m_2)$  is solvable over an alphabet of size  $t m_1^{\alpha+1}$ .*

*Proof.* By Lemma 5.5.4, the network  $\mathcal{N}_3(m_1, m_2)$  is solvable over an alphabet of size  $m_1^{\alpha+1}$ .  $\mathbb{Z}_t$  is a standard  $\mathbb{Z}_t$ -module and  $\text{char}(\mathbb{Z}_t) = t$  is relatively prime to  $m_1$ , so by Lemma 5.5.6, the network  $\mathcal{N}_3(m_1, m_2)$  is scalar linearly solvable over the ring  $\mathbb{Z}_t$ . By taking the Cartesian product code of these solutions, the network  $\mathcal{N}_3(m_1, m_2)$  is solvable over an alphabet of size  $t m_1^{\alpha+1}$ . ■

For each  $m_1 \geq 2$  and  $\alpha, s \geq 1$  such that  $s$  is relatively prime to  $m_1$ , let  $m_2 = m_1^\alpha s$ . By Lemma 5.5.4, network  $\mathcal{N}_3(m_1, m_2)$  is solvable over the ring  $\mathbb{Z}_{m_1^{\alpha+1}}$ , but in this case we have

$$\gcd\left(m_1, m_2, \text{char}\left(\mathbb{Z}_{m_1^{\alpha+1}}\right)\right) = \gcd\left(m_1, m_1^\alpha s, m_1^{\alpha+1}\right) = m_1 \neq 1.$$

So, by Lemma 5.5.6, the solution is necessarily non-linear.

Lemma 5.5.8 characterizes the linear capacity of  $\mathcal{N}_3(m_1, m_2)$  and is proved in the Appendix. Since the characteristic of any finite field is prime, the conditions of (b) and (c) of the following lemma are complements of one another.

**Lemma 5.5.8.** *For each  $m_1, m_2 \geq 2$ , network  $\mathcal{N}_3(m_1, m_2)$  has*

- (a) *capacity equal to 1,*
- (b) *linear capacity equal to 1 for any finite field whose characteristic is relatively prime to  $m_1$  or  $m_2$ ,*
- (c) *linear capacity equal to  $1 - \frac{1}{2m_1 + 2m_2 + 3}$  for any finite field whose characteristic divides  $m_1$  and  $m_2$ .*

## 5.6 Network $\mathcal{N}_4(m)$

A *disjoint union* of networks refers to a new network formed by combining existing networks with disjoint sets of nodes, edges, sources, and receivers. Specifically, the nodes/edges/sources/receivers in the resulting network are the disjoint union of the nodes/edges/sources/receivers in the smaller networks.

**Remark 5.6.1.** *The disjoint union of networks  $\mathcal{N}_1, \dots, \mathcal{N}_w$ , has a  $(k, n)$  solution over the alphabet  $\mathcal{A}$  if and only if each of  $\mathcal{N}_1, \dots, \mathcal{N}_w$  has a  $(k, n)$  solution over  $\mathcal{A}$ .*

For any integer  $m \geq 2$ , let  $\omega(m)$  denote the number of distinct prime factors of  $m$ . Denote the prime factorization of  $m$  by  $m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$  where  $\gamma_1, \dots, \gamma_{\omega(m)} \geq 1$  and  $p_1, \dots, p_{\omega(m)}$  are distinct primes. The following functions of  $m$  and its prime divisors will be used throughout this section. For each  $i = 1, \dots, \omega(m)$ , let

$$f(m) = p_1^{\gamma_1 - 1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)} - 1} \tag{5.51}$$

$$\mu(m, i) = \min \{ \alpha \geq 0 : p_i^\alpha \geq f(m) \} \tag{5.52}$$

$$g(m, i) = p_i^{\gamma_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega(m)} p_j^{\mu(m, j)}. \tag{5.53}$$



We construct network  $\mathcal{N}_4(m)$  from the following *disjoint union*<sup>3</sup> of networks:

$$\mathcal{N}_4(m) = \left( \bigcup_{\substack{\text{prime } q \\ q \nmid m \\ q < f(m)}} \mathcal{N}_1(q) \right) \cup \left( \bigcup_{i=1}^{\omega(m)} \mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i})) \right) \cup \left( \bigcup_{\substack{i=1 \\ \gamma_i > 1}}^{\omega(m)} \mathcal{N}_3(p_i, g(m, i)) \right). \quad (5.54)$$

**Theorem 5.6.2.** *For each  $m \geq 2$ , the network  $\mathcal{N}_4(m)$  is:*

1. *solvable over an alphabet of size  $m$ ,*
2. *not solvable over any alphabet whose size is less than  $m$ ,*
3. *not solvable over any prime-power-size alphabet, if  $m$  is not a prime power,*
4. *scalar linearly solvable over  $\text{GF}(m)$ , if  $m$  is prime,*
5. *neither linearly solvable over any module alphabet nor asymptotically linearly solvable over any finite-field alphabet if  $m$  is composite.*

*Proof.* The theorem follows immediately from Theorems 5.6.4, 5.6.5, 5.6.8, 5.6.9, and Corollaries 5.6.6 and 5.6.11. ■

**Example 5.6.3.** Consider the special cases of the square-free (i.e. not divisible by the square of any prime) integer 6, the prime power 27, and the integer 100 which is neither square-free nor a prime power.

- $m = 6 = 2^1 3^1$ . We have  $\gamma_1 = \gamma_2 = 1$  and  $f(m) = 2^{(1-1)} 3^{(1-1)} = 1$ , so  $\mathcal{N}_4(6)$  has neither  $\mathcal{N}_1$  nor  $\mathcal{N}_3$  components. Thus by (5.54), network  $\mathcal{N}_4(6)$  is the disjoint union of networks:

$$\mathcal{N}_2(2, 3) \cup \mathcal{N}_2(3, 2).$$

- $m = 27 = 3^3$ . We have  $f(27) = 3^{(3-1)} = 9$  and  $g(27, 1) = 3^{(3-1)} = 9$ , and the primes less than  $f(27)$  which do not divide 27 are 2, 5, and 7. Thus by (5.54), network  $\mathcal{N}_4(6)$  is the disjoint union of networks:

$$\mathcal{N}_1(2) \cup \mathcal{N}_1(5) \cup \mathcal{N}_1(7) \cup \mathcal{N}_2(27, 1) \cup \mathcal{N}_3(3, 9).$$

---

<sup>3</sup>When node (respectively, edge and message) labels are repeated (e.g.  $\mathcal{N}_1(m_1)$  and  $\mathcal{N}_1(m_2)$  both have receiver  $R_x$ ), add additional superscripts to each node (respectively, edge and message) to avoid repeated labels. Each disjoint network has a set of messages, nodes, and edges which is disjoint to every other network's set in the union. The messages, nodes, and edges are not directly referenced in this section, so the additional level of labeling is arbitrary so long as the networks are disjoint.

- $m = 100 = 2^2 5^2$ . We have  $f(100) = 2^{(2-1)} 5^{(2-1)} = 10$ . Then  $\mu(100, 1) = 4$ , since  $2^4 > f(100) > 2^3$ , and  $\mu(100, 2) = 2$ , since  $5^2 > f(100) > 5^1$ . So  $g(100, 1) = 2^1 5^2$  and  $g(100, 2) = 5^1 2^4$ , and the primes less than  $f(100)$  which do not divide 100 are 3 and 7. Thus by (5.54), network  $\mathcal{N}_4(100)$  is the disjoint union of networks:

$$\mathcal{N}_1(3) \cup \mathcal{N}_1(7) \cup \mathcal{N}_2(4, 25) \cup \mathcal{N}_2(25, 4) \cup \mathcal{N}_3(2, 50) \cup \mathcal{N}_3(5, 80).$$

We will use the networks described in Example 5.6.3 as running examples throughout this section and will refer back to these constructions.

### 5.6.1 Solvability of $\mathcal{N}_4(m)$

The following lemma shows that each disjoint component of  $\mathcal{N}_4(m)$  is solvable over an alphabet of size  $m$ , and therefore  $\mathcal{N}_4(m)$  is solvable over an alphabet of size  $m$ . The proofs of Theorems 5.6.4 and 5.6.5 make use of the functions  $f, \mu$ , and  $g$  defined in (5.51), (5.52), and (5.53), respectively.

**Theorem 5.6.4.** *For each  $m \geq 2$ , network  $\mathcal{N}_4(m)$  is solvable over an alphabet of size  $m$ .*

*Proof.* Let  $p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$  be the prime factorization of  $m$ . For each prime  $q < f(m)$  such that  $q \nmid m$ , by (5.54), network  $\mathcal{N}_4(m)$  contains a copy of  $\mathcal{N}_1(q)$ .  $\mathbb{Z}_m$  is a standard  $\mathbb{Z}_m$ -module and  $\text{char}(\mathbb{Z}_m) = m$  is relatively prime to  $q$ , so by Lemma 5.3.3, network  $\mathcal{N}_1(q)$  is scalar linearly solvable over the ring  $\mathbb{Z}_m$ . For each  $i = 1, \dots, \omega(m)$ , by (5.54), network  $\mathcal{N}_4(m)$  contains a copy of  $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$ . By Lemma 5.4.4, network  $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$  is solvable over an alphabet of size  $m$ . If  $\gamma_i > 1$ , then by (5.54), network  $\mathcal{N}_4(m)$  contains a copy of  $\mathcal{N}_3(p_i, g(m, i))$ . Also,  $p_i$  and  $m/p_i^{\gamma_i}$  are relatively prime, and by (5.53),  $g(m, i)$  is the product of  $p_i^{\gamma_i - 1}$  and a term which is relatively prime to  $p_i$ , so by Corollary 5.5.7, network  $\mathcal{N}_3(p_i, g(m, i))$  is solvable over an alphabet of size  $m$ . Thus each disjoint component of  $\mathcal{N}_4(m)$  is solvable over an alphabet of size  $m$ , so  $\mathcal{N}_4(m)$  is solvable over an alphabet of size  $m$ . ■

Each network  $\mathcal{N}_1, \mathcal{N}_2$ , and  $\mathcal{N}_3$  requires the alphabet size to meet some divisibility condition in order to have a solution over that alphabet. The following lemma shows that because of these conditions, there does not exist an alphabet whose size is less than  $m$  over which each component of  $\mathcal{N}_4(m)$  is solvable.

**Theorem 5.6.5.** For each  $m \geq 2$ , if network  $\mathcal{N}_4(m)$  is solvable over alphabet  $\mathcal{A}$ , then  $|\mathcal{A}| \geq m$ .

*Proof.* Assume to the contrary that  $\mathcal{N}_4(m)$  is solvable over an alphabet  $\mathcal{A}$  such that  $|\mathcal{A}| < m$ . Then each disjoint component of  $\mathcal{N}_4(m)$  must be solvable over  $\mathcal{A}$ . Let  $m$  have prime factorization  $m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$ . For each  $i = 1, \dots, \omega(m)$ , by (5.54), the network  $\mathcal{N}_4(m)$  contains a copy of  $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$ . Network  $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$  is solvable over  $\mathcal{A}$ , so by Lemma 5.4.5,  $p_i$  is not relatively prime to  $|\mathcal{A}|$ . Since  $p_i$  is prime, we have  $p_i \mid |\mathcal{A}|$ , and thus each of  $p_1, \dots, p_{\omega(m)}$  divides  $|\mathcal{A}|$ . Let

$$\delta = \frac{|\mathcal{A}|}{p_1 \cdots p_{\omega(m)}}.$$

If  $m = p_1 \cdots p_{\omega(m)}$  (i.e.  $m$  is square-free), then we contradict the assumption that  $|\mathcal{A}| < m$ . So we may assume  $m > p_1 \cdots p_{\omega(m)}$ , which implies  $\delta \geq 2$ . If  $\delta \geq f(m)$ , then

$$\begin{aligned} |\mathcal{A}| &= \delta p_1 \cdots p_{\omega(m)} \\ &\geq f(m) p_1 \cdots p_{\omega(m)} \\ &= p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}} = m \end{aligned} \quad [\text{from (5.51)}],$$

which again contradicts the assumption that  $|\mathcal{A}| < m$ , so we assume  $\delta < f(m)$ .

Consider the prime factorization of  $\delta$ . Let  $\{q_1, \dots, q_\rho\}$  denote the set of primes which are less than  $f(m)$  and do not divide  $m$ . Each prime less than  $f(m)$  either divides  $m$  and is in the set  $\{p_1, \dots, p_{\omega(m)}\}$  or it does not divide  $m$  and is in the set  $\{q_1, \dots, q_\rho\}$ . Thus  $\delta$  must be a product of  $q_1, \dots, q_\rho$  and  $p_1, \dots, p_{\omega(m)}$  terms, so there exist  $\alpha_1, \dots, \alpha_{\omega(m)} \geq 1$  and  $\beta_1, \dots, \beta_\rho \geq 0$  such that we can write  $|\mathcal{A}|$  as

$$|\mathcal{A}| = p_1^{\alpha_1} \cdots p_{\omega(m)}^{\alpha_{\omega(m)}} q_1^{\beta_1} \cdots q_\rho^{\beta_\rho}. \quad (5.55)$$

For each prime  $q < f(m)$  such that  $q \nmid m$ , by (5.54), the network  $\mathcal{N}_4(m)$  contains a copy of  $\mathcal{N}_1(q)$ . Network  $\mathcal{N}_1(q)$  is solvable over  $\mathcal{A}$ , so by Lemma 5.3.2, we have  $\gcd(q, |\mathcal{A}|) = 1$ . Thus in (5.55) we have  $\beta_1 = \cdots = \beta_\rho = 0$ .

For each  $i = 1, \dots, \omega(m)$  such that  $\gamma_i > 1$ , by (5.54), the network  $\mathcal{N}_4(m)$  contains a copy of  $\mathcal{N}_3(p_i, g(m, i))$ . Network  $\mathcal{N}_3(p_i, g(m, i))$  is solvable over  $\mathcal{A}$  and  $p_i \mid |\mathcal{A}|$ , so by Lemma 5.5.5,  $|\mathcal{A}|$  does not divide  $g(m, i)$ . Expressing  $|\mathcal{A}|$  and  $g(m, i)$  as their prime factorizations yields:

$$p_1^{\alpha_1} \cdots p_{\omega(m)}^{\alpha_{\omega(m)}} \nmid p_i^{\gamma_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega(m)} p_j^{\mu(m, j)} \quad [\text{from (5.53), (5.55)}].$$

This implies that for each  $i \in \{1, \dots, \omega(m)\}$  such that  $\gamma_i > 1$ , either  $\alpha_i \geq \gamma_i$  or  $\alpha_j \geq \mu(m, j) + 1$  for some  $j \neq i$ . If there exists  $j \in \{1, \dots, \omega(m)\}$  such that  $\alpha_j \geq \mu(m, j) + 1$ , then we have

$$\begin{aligned} |\mathcal{A}| &= p_1^{\alpha_1} \cdots p_{\omega(m)}^{\alpha_{\omega(m)}} && \text{[from (5.55)]} \\ &\geq p_j^{\alpha_j - 1} (p_1 \cdots p_{\omega(m)}) && \text{[from } \alpha_i \geq 1] \\ &\geq p_j^{\mu(m, j)} (p_1 \cdots p_{\omega(m)}) \geq f(m) (p_1 \cdots p_{\omega(m)}) = m && \text{[from (5.51), (5.52)],} \end{aligned}$$

which contradicts the assumption that  $|\mathcal{A}| < m$ . So it must be the case that  $\alpha_i \geq \gamma_i$ , for each  $i$  such that  $\gamma_i > 1$ . If  $\gamma_i = 1$ , then  $\alpha_i \geq 1 = \gamma_i$ . So we have  $\alpha_i \geq \gamma_i$  for all  $i$ , but this implies

$$\begin{aligned} |\mathcal{A}| &= p_1^{\alpha_1} \cdots p_{\omega(m)}^{\alpha_{\omega(m)}} && \text{[from (5.55)]} \\ &\geq p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}} = m, \end{aligned}$$

which again contradicts the assumption that  $|\mathcal{A}| < m$ . Thus there does not exist an alphabet  $\mathcal{A}$  whose size is less than  $m$  such that each disjoint component of  $\mathcal{N}_4(m)$  is solvable over  $\mathcal{A}$ . ■

Corollary 5.6.6 demonstrates that, in some cases, network  $\mathcal{N}_4(m)$  is not solvable over any prime-power size alphabets. In particular, such a solvable network is not solvable over any finite-field alphabet.

**Corollary 5.6.6.** *For each non-power-of-prime composite number  $m \geq 6$ , network  $\mathcal{N}_4(m)$  is not solvable over any prime-power-size alphabet.*

*Proof.* Let  $m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$ , and assume network  $\mathcal{N}_4(m)$  is solvable over the alphabet  $\mathcal{A}$ . It follows from the of the proof of Theorem 5.6.5 that each of  $p_1, \dots, p_{\omega(m)}$  must divide  $|\mathcal{A}|$ . If  $\omega(m) \geq 2$ , then network  $\mathcal{N}_4(m)$  is not solvable over any prime-power-size alphabet. ■

**Example 5.6.7.** We continue our example networks  $\mathcal{N}_4(6)$ ,  $\mathcal{N}_4(27)$ , and  $\mathcal{N}_4(100)$ .

- Suppose  $\mathcal{N}_4(6)$  is solvable over an alphabet  $\mathcal{A}$ . Since  $\mathcal{N}_2(2, 3)$  is solvable over  $\mathcal{A}$ , we have  $2 \mid |\mathcal{A}|$ . Similarly for  $\mathcal{N}_2(3, 2)$ , we have that  $3 \mid |\mathcal{A}|$ . Hence we have  $|\mathcal{A}| \geq 6$ .
- Suppose  $\mathcal{N}_4(27)$  is solvable over an alphabet  $\mathcal{A}$  whose size is less than 27. Then
  - $\mathcal{N}_2(27, 1)$  requires  $3 \mid |\mathcal{A}|$ , so  $|\mathcal{A}| \in \{3, 6, 9, 12, 15, 18, 21, 24\}$ .
  - $\mathcal{N}_1(2)$ ,  $\mathcal{N}_1(5)$ , and  $\mathcal{N}_1(7)$  require  $|\mathcal{A}|$  be relatively prime to 2, 5, and 7, so  $|\mathcal{A}| \notin \{6, 12, 15, 18, 21, 24\}$ .

- $\mathcal{N}_3(3, 9)$  requires  $|\mathcal{A}| \nmid 9$ , so  $|\mathcal{A}| \notin \{3, 9\}$ .

Therefore  $\mathcal{N}_4(27)$  is not solvable over any alphabet whose size is less than 27.

- Suppose  $\mathcal{N}_4(100)$  is solvable over an alphabet  $\mathcal{A}$  whose size is less than 100. Then
  - $\mathcal{N}_2(4, 25)$  and  $\mathcal{N}_2(25, 4)$  require  $10 \mid |\mathcal{A}|$ , so  $|\mathcal{A}| \in \{10, 20, 30, 40, 50, 60, 70, 80, 90\}$ .
  - $\mathcal{N}_1(3)$  and  $\mathcal{N}_1(7)$  require  $|\mathcal{A}|$  to be relatively prime to 3 and 7, so  $|\mathcal{A}| \notin \{30, 60, 70, 90\}$ .
  - $\mathcal{N}_3(2, 50)$  requires  $|\mathcal{A}| \nmid 50$ , so  $|\mathcal{A}| \notin \{10, 50\}$ .
  - $\mathcal{N}_3(5, 80)$  requires  $|\mathcal{A}| \nmid 80$ , so  $|\mathcal{A}| \notin \{10, 20, 40, 80\}$ .

Therefore  $\mathcal{N}_4(100)$  is not solvable over any alphabet whose size is less than 100.

### 5.6.2 Linear Solvability of $\mathcal{N}_4(m)$

The following theorems show that network  $\mathcal{N}_4(m)$  is linearly solvable if and only if  $m$  is prime.

**Theorem 5.6.8.** *For each prime  $p$ , the network  $\mathcal{N}_4(p)$  is scalar linearly solvable over  $\text{GF}(p)$ .*

*Proof.* If  $p$  is a prime number, then  $f(p) = 1$  and the power of  $p$  is one, so by (5.54), network  $\mathcal{N}_4(p)$  consists solely of a copy of network  $\mathcal{N}_2(p, 1)$ . By Lemma 5.4.6, network  $\mathcal{N}_2(p, 1)$  has a scalar linear solution over every finite-field alphabet with characteristic  $p$ . ■

**Theorem 5.6.9.** *For each composite number  $m$ , the network  $\mathcal{N}_4(m)$  is not linearly solvable over any module.*

*Proof.* Let  $G$  be a standard  $R$ -module, and assume a linear solution for  $\mathcal{N}_4(m)$  exists over  $G$ . Since  $\mathcal{N}_4(m)$  is linearly solvable over  $G$ , each disjoint component of  $\mathcal{N}_4(m)$  is linearly solvable over  $G$ . Suppose  $m$  is a composite number. Then  $m$  is a product of two or more (possibly distinct) primes. We will separately consider the cases of prime powers and non-power-of-prime composite numbers.

For each prime  $p$  and integer  $\gamma \geq 2$ , by (5.54), network  $\mathcal{N}_4(p^\gamma)$  contains copies of  $\mathcal{N}_2(p^\gamma, 1)$  and  $\mathcal{N}_3(p, p^{\gamma-1})$ . Since network  $\mathcal{N}_2(p^\gamma, 1)$  is linearly solvable over  $G$ , by Lemma 5.4.6, the characteristic of  $R$  divides  $p^\gamma$ . Since network  $\mathcal{N}_3(p, p^{\gamma-1})$  is linearly solvable over  $G$ , by Lemma 5.5.6, the characteristic of  $R$  is relatively prime to  $p$ . If the characteristic of  $R$  both divides  $p^\gamma$  and is relatively prime to  $p$ , then the

characteristic of  $R$  is 1, which only occurs in the trivial ring (of size one). Thus there is no standard module over which all components of network  $\mathcal{N}_4(p^\gamma)$  are linearly solvable.

Now suppose  $\omega(m) \geq 2$ . Then  $m$  has prime factorization  $m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$ , and by (5.54), network  $\mathcal{N}_4(m)$  contains copies of networks  $\mathcal{N}_2(p_1^{\gamma_1}, (m/p_1^{\gamma_1}))$  and  $\mathcal{N}_2(p_2^{\gamma_2}, (m/p_2^{\gamma_2}))$ . Both of these networks are linearly solvable over  $G$ , so by Lemma 5.4.6, the characteristic of  $R$  divides  $p_1^{\gamma_1}$  and  $p_2^{\gamma_2}$ . Since  $p_1 \neq p_2$ , the characteristic of  $R$  must be 1, which only occurs in the trivial ring. Thus there is no standard module over which all components of network  $\mathcal{N}_4(m)$  are linearly solvable.

If  $m$  is a composite number, then there are no linear solutions for  $\mathcal{N}_4(m)$  over any standard module, which, by Lemma 5.1.3 implies there are no linear solutions for  $\mathcal{N}_4(m)$  over any module. ■

### 5.6.3 Capacity and Linear Capacity of $\mathcal{N}_4(m)$

**Theorem 5.6.10.** *For each  $m \geq 2$  network  $\mathcal{N}_4(m)$  has:*

- (a) *capacity equal to 1,*
- (b) *linear capacity bounded away from 1 over all finite-field alphabets, if  $m$  is composite.*

*Proof.* For each  $m \geq 2$ , by Theorem 5.6.4, network  $\mathcal{N}_4(m)$  is solvable over an alphabet of size  $m$ , so its capacity is at least 1. Network  $\mathcal{N}_4(m)$  consists of disjoint copies of  $\mathcal{N}_1, \mathcal{N}_2$ , and  $\mathcal{N}_3$ , which each have capacity equal to 1, so the capacity of  $\mathcal{N}_4(m)$  is at most 1. Thus the capacity of  $\mathcal{N}_4(m)$  is equal to 1. For composite  $m$ , we will again separately consider the cases of prime powers and non-power-of-prime composite numbers.

For each prime  $p$  and integer  $\gamma \geq 2$ , by (5.54), network  $\mathcal{N}_4(p^\gamma)$  contains copies of  $\mathcal{N}_2(p^\gamma, 1)$  and  $\mathcal{N}_3(p, p^{\gamma-1})$ . By Lemma 5.4.7, network  $\mathcal{N}_2(p^\gamma, 1)$  has linear capacity upper bounded by  $1 - \frac{1}{2p^\gamma+3}$  for finite-field with characteristic other than  $p$ . By Lemma 5.5.8, network  $\mathcal{N}_3(p, p^{\gamma-1})$  has linear capacity equal to  $1 - \frac{1}{2p^{\gamma-1}+2p+3}$  for finite-field alphabets with characteristic  $p$ . Whether we select a finite-field alphabet with characteristic  $p$  or characteristic other than  $p$ , the linear capacity of  $\mathcal{N}_4(p^\gamma)$  is bounded away from 1, for fixed  $p$  and  $\gamma$ .

Now suppose  $\omega(m) \geq 2$ . Then  $m$  has prime factorization  $m = p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}}$ , and by (5.54), the network  $\mathcal{N}_4(m)$  contains copies of networks  $\mathcal{N}_2(p_1^{\gamma_1}, (m/p_1^{\gamma_1}))$  and  $\mathcal{N}_2(p_2^{\gamma_2}, (m/p_2^{\gamma_2}))$ . By Lemma 5.4.7, network  $\mathcal{N}_2(p_i^{\gamma_i}, (m/p_i^{\gamma_i}))$  has linear capacity upper bounded by  $1 - \frac{1}{2m+2(m/p_i^{\gamma_i})+1}$  for finite-field alphabets with characteristic other than  $p_i$ . Since  $p_1 \neq p_2$ , whether we select a finite-field alphabet with characteristic

$p_1, p_2$ , or neither  $p_1$  nor  $p_2$ , the linear capacity is bounded away from 1, for fixed  $m$ .

Thus for any fixed composite number  $m$ , the linear capacity of network  $\mathcal{N}_4(m)$  is bounded away from 1 over all finite-field alphabets. ■

Calculating the exact linear capacity of network  $\mathcal{N}_4$  over every finite field is left as an open problem.

**Corollary 5.6.11.** *For each composite  $m$ , network  $\mathcal{N}_4(m)$  is not asymptotically linearly solvable over any finite-field alphabet.*

*Proof.* This follows directly from the fact that for any fixed composite number  $m$ , by Theorem 5.6.10, the linear capacity of  $\mathcal{N}_4(m)$  is bounded away from one over all finite-field alphabets. ■

#### 5.6.4 Size of $\mathcal{N}_4(m)$

Depending on the prime divisors of  $m$ , the number of nodes in  $\mathcal{N}_4(m)$  can be dominated by nodes from  $\mathcal{N}_1$  networks,  $\mathcal{N}_2$  networks, or  $\mathcal{N}_3$  networks. The following theorem makes use of the functions  $f(m)$ ,  $\mu(m, i)$ , and  $g(m, i)$  defined in (5.51), (5.52), (5.53).

**Theorem 5.6.12.** *For each  $m \geq 2$ , the number of nodes in network  $\mathcal{N}_4(m)$  is asymptotically*

- (a)  $\Omega(m)$ ,
- (b)  $O(m)$  when  $m$  is prime,
- (c)  $O\left(\frac{m \log m}{\log \log m}\right)$ , when  $m$  is square-free,
- (d)  $O\left(\frac{m^2}{\log m}\right)$ , when  $m$  is a prime-power,
- (e)  $O\left(m^{\frac{\log m}{\log \log m}}\right)$ , when  $m$  is neither square-free nor a prime-power.

*Proof.* By Remark 5.3.1, the number of nodes in  $\mathcal{N}_1(q)$  is  $4q + 7$ . By Remark 5.4.1, the number of nodes in  $\mathcal{N}_2(m, w)$  is  $4mw + 9w + 2$ . By Remark 5.5.1, the number of nodes in  $\mathcal{N}_3(m_1, m_2)$  is  $4m_1 + 4m_2 + 12$ . By the construction of  $\mathcal{N}_4(m)$  given in (5.54), the total number of nodes in  $\mathcal{N}_4(m)$  is:

$$\left( \sum_{\substack{\text{prime } q \\ q \nmid m \\ q < f(m)}} (4q + 7) \right) + \left( \sum_{i=1}^{\omega(m)} (4m + 9(m/p_i^{\gamma_i}) + 2) \right) + \left( \sum_{\substack{i=1 \\ \gamma_i > 1}}^{\omega(m)} (4g(m, i) + 4p_i + 12) \right) \quad (5.56)$$

where the first, second, and third terms are the number of nodes from  $\mathcal{N}_1$ ,  $\mathcal{N}_2$ , and  $\mathcal{N}_3$  networks, respectively. In order to find upper and lower bounds on the total number of nodes in  $\mathcal{N}_4(m)$ , we will first find upper and lower bounds on the number of nodes from  $\mathcal{N}_1$ ,  $\mathcal{N}_2$ , and  $\mathcal{N}_3$  networks within  $\mathcal{N}_4(m)$ .

If  $m$  is a square-free number, then we have  $f(m) = 1$ , so in this case, there are no nodes in  $\mathcal{N}_4(m)$  from  $\mathcal{N}_1$  networks. Thus for general  $m$ , we have

$$\sum_{\substack{\text{prime } q \\ q \nmid m \\ q < f(m)}} (4q + 7) \geq 0 \quad (5.57)$$

$$\sum_{\substack{\text{prime } q \\ q \nmid m \\ q < f(m)}} (4q + 7) < \sum_{\substack{\text{prime } q \\ q \leq m}} (4q + 7) = O\left(\frac{m^2}{\log m}\right) \quad [\text{from [27, p. 257]}]. \quad (5.58)$$

The total number of nodes in  $\mathcal{N}_4(m)$  from  $\mathcal{N}_2$  networks is

$$\sum_{i=1}^{\omega(m)} (4m + 9(m/p_i^{\gamma_i}) + 2) > \sum_{i=1}^{\omega(m)} 4m = \Omega(\omega(m)m) \quad (5.59)$$

$$\sum_{i=1}^{\omega(m)} (4m + 9(m/p_i^{\gamma_i}) + 2) < \sum_{i=1}^{\omega(m)} (13m + 2) = O(\omega(m)m). \quad (5.60)$$

For each  $i = 1, \dots, \omega(m)$  we have

$$p_i^{\mu(m,i)} < p_i f(m) \quad [\text{from (5.52)}] \quad (5.61)$$

$$g(m, i) = p_i^{\gamma_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega(m)} p_j^{\mu(m,j)} \quad [\text{from (5.53)}]$$

$$< p_i^{\gamma_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega(m)} p_j f(m) \quad [\text{from (5.61)}]$$

$$< p_i^{\gamma_i} f(m)^{\omega(m)-1} \prod_{j=1}^{\omega(m)} p_j \\ = p_i^{\gamma_i} f(m)^{\omega(m)-2} m \quad [\text{from (5.51)}]. \quad (5.62)$$

If  $m$  is square-free, then  $\gamma_i = 1$  for all  $i$ , so in this case, there are no nodes in  $\mathcal{N}_4(m)$  from  $\mathcal{N}_3$  networks. Thus for general  $m$ , we have

$$\sum_{\substack{i=1 \\ \gamma_i > 1}}^{\omega(m)} (4g(m, i) + 4p_i + 12) \geq 0, \text{ and} \quad (5.63)$$



and

$$\begin{aligned}
\sum_{\substack{i=1 \\ \gamma_i > 1}}^{\omega(m)} (4g(m, i) + 4p_i + 12) &\leq \sum_{i=1}^{\omega(m)} 20g(m, i) && \text{[from (5.53)]} \\
&< 20m f(m)^{\omega(m)-2} \sum_{i=1}^{\omega(m)} p_i^{\gamma_i} && \text{[from (5.62)]} \\
&< 20m f(m)^{\omega(m)-2} \prod_{i=1}^{\omega(m)} p_i^{\gamma_i} && \text{[from } ab \geq a + b, \forall a, b \geq 2\text{]} \\
&= 20m^2 f(m)^{\omega(m)-2} \\
&< 20m^{\omega(m)} = O\left(m^{\omega(m)}\right) && \text{[from (5.51)].} \tag{5.64}
\end{aligned}$$

To prove part (a), consider the lower bounds of each term of (5.56). By equations (5.56), (5.57), (5.59), and (5.63), the total number of nodes in  $\mathcal{N}_4(m)$  is lower bounded by:

$$0 + \Omega(\omega(m)m) + 0 = \Omega(\omega(m)m) = \Omega(m),$$

where the final equality comes from the fact  $\omega(m) = \Omega(1)$ , since  $\omega(m) = 1$  when  $m$  is prime.

It follows from [26, Theorem 11] that

$$\omega(m) = O\left(\frac{\log m}{\log \log m}\right). \tag{5.65}$$

To prove parts (b)-(e), we will consider the upper bounds on the number of nodes of each term of (5.56). However, each term dominates in different cases, depending on the prime factors of  $m$ . To prove parts (b) and (c), consider a square-free integer  $m = p_1 \cdots p_{\omega(m)}$ . Since  $\gamma_i = 1$  for all  $i$ , we have  $f(m) = 1$ , so there are neither  $\mathcal{N}_1$  nor  $\mathcal{N}_3$  components in  $\mathcal{N}_4(m)$ . Thus there are 0 nodes from  $\mathcal{N}_1$  and  $\mathcal{N}_3$  components. Then by (5.56) and (5.60), the number of nodes in  $\mathcal{N}_4(m)$  is  $O(\omega(m)m)$ . If  $m$  is prime, then  $\omega(m) = 1$ , so we have the desired bound. If  $m$  is not prime, then the number of nodes is  $O(\omega(m)m)$ , which, along with (5.65), yields the desired bound.

To prove part (d), consider a prime power  $m = p^\gamma$ , where  $\gamma \geq 2$ . We have  $\omega(p^\gamma) = 1$ , so by (5.60), the number of nodes from  $\mathcal{N}_2$  components is  $O(m)$ , and, by (5.64), the number of nodes from  $\mathcal{N}_3$  components is  $O(m)$ . By (5.58), the number of nodes from  $\mathcal{N}_1$  components is  $O(m^2/\log m)$ . Thus the number of nodes in  $\mathcal{N}_4(m)$  is  $O(m^2/\log m)$ .

To prove part (e), consider  $m$  which is neither a prime power (so  $\omega(m) \geq 2$ ) nor square-free (so there are  $\mathcal{N}_3$  components in  $\mathcal{N}_4(m)$ ). By equations (5.56), (5.58), (5.60), and (5.64), The number of nodes in  $\mathcal{N}_4(m)$  is

$$O\left(\frac{m^2}{\log m}\right) + O(\omega(m)m) + O\left(m^{\omega(m)}\right) O\left(m^{\omega(m)}\right) \quad \text{[from } \omega(m) \geq 2\text{]},$$

which, along with (5.65), yields the desired bound. ■

**Example 5.6.13.** We continue our example networks  $\mathcal{N}_4(6)$ ,  $\mathcal{N}_4(27)$ , and  $\mathcal{N}_4(100)$ .

- $\mathcal{N}_4(6)$  has 97 nodes: 53 from  $\mathcal{N}_2(2,3)$  and 44 from  $\mathcal{N}_2(3,2)$ .
- $\mathcal{N}_4(27)$  has 256 nodes: 15 from  $\mathcal{N}_1(2)$ , 27 from  $\mathcal{N}_1(5)$ , 35 from  $\mathcal{N}_1(7)$ , 119 from  $\mathcal{N}_2(27,1)$ , and 60 from  $\mathcal{N}_3(3,9)$ .
- $\mathcal{N}_4(100)$  has 1691 nodes: 19 from  $\mathcal{N}_1(3)$ , 35 from  $\mathcal{N}_1(7)$ , 627 from  $\mathcal{N}_2(4,25)$ , 438 from  $\mathcal{N}_2(25,4)$ , 220 from  $\mathcal{N}_3(2,50)$ , and 352 from  $\mathcal{N}_3(5,80)$ .

## 5.7 Open Questions

Below are some remaining open questions regarding linear and non-linear network coding:

1. In [7] it was shown that there exists a network which is not linearly solvable over any module yet is non-linearly solvable over an alphabet of size 4. We have shown that for each composite number  $m$ , there exists a network which is not linearly solvable over any module yet is non-linearly solvable over an alphabet of size  $m$ . Do there exist networks which are not linearly solvable over any module but are non-linearly solvable over some alphabet of prime size?
2. There are examples [34], [24] in the literature of solvable networks which are not solvable over any alphabet whose size is less than some  $m$ . For each  $m \geq 2$ , we have demonstrated a network which is solvable over an alphabet of size  $m$  but is not solvable over any alphabet whose size is less than  $m$ . For each  $m \geq 2$  does there exist a network which is solvable over alphabet  $\mathcal{A}$  if and only if  $|\mathcal{A}| \geq m$ ? Which other “interesting” sets  $S \subset \mathbf{N}$  have the property that there exists a network which is solvable over  $\mathcal{A}$  if and only if  $|\mathcal{A}| \in S$ ?
3. It is not currently known whether there can exist an algorithm which determines whether a network is solvable. We have demonstrated a class of solvable networks with no linear solutions (i.e. diabolical networks). Can there exist an algorithm which detects whether a network is diabolical?
4. We partially characterized the linear capacities of  $\mathcal{N}_1$ ,  $\mathcal{N}_2$ , and  $\mathcal{N}_3$  over finite-field alphabets. However, the techniques we use do not extend more general ring alphabets. What techniques exist for upper bounding the linear capacities over ring alphabets?

## 5.A Capacity Proofs of $\mathcal{N}_1$ , $\mathcal{N}_2$ and $\mathcal{N}_3$

The following definition and lemmas will be used in the proofs of Lemmas 5.3.4, 5.4.7, and 5.5.8.

**Definition 5.A.1.** Let  $\mathbb{F}$  be a finite field and suppose  $a_1 \in \mathbb{F}^{s_1}, \dots, a_q \in \mathbb{F}^{s_q}$  and  $b_1 \in \mathbb{F}^{t_1}, \dots, b_r \in \mathbb{F}^{t_r}$  are functions of variables  $x_1, \dots, x_w$ . We write  $a_1, \dots, a_q \longrightarrow b_1, \dots, b_r$  to mean that there exist  $t_j \times s_i$  matrices  $M_{j,i}$  over  $\mathbb{F}$  such that for all choices of  $x_1, \dots, x_w$ , we have  $b_j = \sum_{i=1}^q M_{j,i} a_i$  for all  $j$ .

In other words, each of  $b_1, \dots, b_r$  can be written as a linear combination of  $a_1, \dots, a_q$ . In the context of network coding, the variables  $x_1, \dots, x_w$  will always be taken as the network messages. In what follows, the transitive relation  $\longrightarrow$  will be used to describe linear coding functions at network nodes.

Lemma 5.A.2 is known from linear algebra [28, p. 124] and will be used in later proofs. In particular, Lemmas 5.A.2, 5.A.3, and 5.A.4 will be used in bounding the linear capacities of  $\mathcal{N}_1, \mathcal{N}_2$ , and  $\mathcal{N}_3$ . Lemmas 5.A.3 and 5.A.4 were proved in slightly different form in [7, Lemma IV.2 and Theorem IV.4].

**Lemma 5.A.2.** *Let  $\mathbb{F}$  be a finite field. If  $A : \mathbb{F}^m \rightarrow \mathbb{F}^n$  and  $B : \mathbb{F}^k \rightarrow \mathbb{F}^m$  are linear maps, then*

$$\text{rank}(A) + \text{rank}(B) - m \leq \text{rank}(AB) \quad (5.66)$$

$$\leq \min(\text{rank}(A), \text{rank}(B)). \quad (5.67)$$

**Lemma 5.A.3.** *If  $A$  is an  $n \times k$  matrix of rank  $k$  over finite field  $\mathbb{F}$ , then there exists a nonsingular  $n \times n$  matrix  $B$  such that  $BA = \begin{bmatrix} I_k \\ 0 \end{bmatrix}$ .*

**Lemma 5.A.4.** *If  $A$  is an  $m \times n$  matrix of rank  $k$  over finite field  $\mathbb{F}$ , then there exists an  $(n-k) \times n$  matrix  $Q$  over  $\mathbb{F}$  of rank  $n-k$  such that for all  $x \in \mathbb{F}^n$  we have  $Ax, Qx \longrightarrow x$ .*

### 5.A.1 $\mathcal{N}_1$ Capacity Proof

*Proof of Lemma 5.3.4.* Since a scalar linear solution over a finite-field alphabet is a special case of a linear solution over a standard module, by Lemma 5.3.3,  $\mathcal{N}_1(m)$  is scalar linearly solvable over any finite-field alphabet whose characteristic does not divide  $m$ , so the network's linear capacity for such finite-field alphabets is at least 1. By Lemma 5.2.4, network  $\mathcal{N}_0(m)$  has capacity equal to 1, and since  $\mathcal{N}_1(m)$  contains  $\mathcal{N}_0(m)$ , the capacity of  $\mathcal{N}_1(m)$  is at most 1. Thus, both the capacity of  $\mathcal{N}_1(m)$  and its linear capacity for field alphabets whose characteristic does not divide  $m$  are equal to 1.

To prove part (c), consider a  $(k, n)$  fractional linear solution for  $\mathcal{N}_1(m)$  over a finite field  $\mathbb{F}$  whose characteristic divides  $m$ . Since  $\text{char}(\mathbb{F}) \mid m$ , we have  $m = 0$  in  $\mathbb{F}$ .

We have  $x_i \in \mathbb{F}^k$  and  $e, e_i \in \mathbb{F}^n$ , with  $n \geq k$ , since the capacity is one. There exist  $n \times k$  coding matrices  $M_j, M_{i,j}$  with entries in  $\mathbb{F}$ , such that the edge vectors can be written as:

$$e_i = \sum_{\substack{j=0 \\ j \neq i}}^m M_{i,j} x_j \quad (i = 0, 1, \dots, m) \quad (5.68)$$

$$e = \sum_{j=0}^m M_j x_j \quad (5.69)$$

and there exist  $k \times n$  decoding matrices  $D_{i,e}, D_i$  with entries in  $\mathbb{F}$ , such that each  $x_i$  can be linearly decoded at  $R_i$  from the two  $n$ -vectors  $e$  and  $e_i$  by:

$$R_i : x_i = D_{i,e} e + D_i e_i \quad (i = 0, 1, \dots, m). \quad (5.70)$$

Since receiver  $R_x$  linearly recovers  $x_0$  from  $e_0, e_1, \dots, e_m$ , we can write

$$e_0, e_1, \dots, e_m \longrightarrow x_0. \quad (5.71)$$

We also have

$$x_0, \sum_{j=1}^m M_j x_j \longrightarrow e \quad [\text{from (5.69)}]. \quad (5.72)$$

For each  $i = 0, 1, \dots, m$ , if we set  $x_i = 0$  in (5.70), then we get the following relationship among the remaining  $m$  message vectors (since  $e_i$  does not depend on  $x_i$ ):

$$0 = D_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j + D_i e_i \quad [\text{from (5.68), (5.69), (5.70)}], \quad (5.73)$$

and thus, for each  $i = 1, 2, \dots, m$ ,

$$e_i \longrightarrow D_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j \quad [\text{from (5.73)}] \quad (5.74)$$

$$\sum_{j=1}^m M_j x_j \longrightarrow D_0 e_0 \quad [\text{from (5.73)}]. \quad (5.75)$$

For each  $i = 1, 2, \dots, m$ , let  $Q_{i,e}$  be the matrix  $Q$  corresponding to when  $D_{i,e}$  is the matrix  $A$  in Lemma 5.A.4. Similarly, let  $Q_0$  be the matrix  $Q$  corresponding to taking  $A$  to be  $D_0$  in Lemma 5.A.4. Let  $L$  be the following list of  $2m + 1$  vector functions of  $x_0, x_1, \dots, x_m$ :

$$\begin{aligned} & Q_0 e_0, \\ & e_i, \quad (i = 1, 2, \dots, m) \\ & Q_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j \quad (i = 1, 2, \dots, m). \end{aligned}$$

For each  $i = 1, 2, \dots, m$ , we have

$$L \longrightarrow D_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j \quad [\text{from (5.74)}] \quad (5.76)$$

$$L \longrightarrow \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j \quad [\text{from Lemma 5.A.4, (5.76)}], \quad (5.77)$$

and

$$\begin{aligned} \left\{ \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j : i = 1, 2, \dots, m \right\} &\longrightarrow \sum_{i=1}^m \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j \\ &= m M_0 x_0 + (m-1) \sum_{j=1}^m M_j x_j \\ &= - \sum_{j=1}^m M_j x_j \quad [\text{from char}(\mathbb{F}) \mid m]. \end{aligned} \quad (5.78)$$

Thus we have

$$L \longrightarrow \sum_{j=1}^m M_j x_j \quad [\text{from (5.77), (5.78)}] \quad (5.79)$$

$$L \longrightarrow D_0 e_0 \quad [\text{from (5.75), (5.79)}] \quad (5.80)$$

$$L \longrightarrow e_0 \quad [\text{from Lemma 5.A.4, (5.80)}] \quad (5.81)$$

$$L \longrightarrow x_0 \quad [\text{from (5.71), (5.81)}] \quad (5.82)$$

$$L \longrightarrow e \quad [\text{from (5.79), (5.82), (5.72)}] \quad (5.83)$$

$$L \longrightarrow x_i \quad (i = 1, 2, \dots, m) \quad [\text{from (5.70), (5.83)}]. \quad (5.84)$$

We will now bound the number of independent entries in the list  $L$ . By equating message components in equation (5.70), for each  $i = 0, 1, \dots, m$ , we have:

$$I_k = D_{i,e} M_i \quad [\text{from (5.68), (5.69), (5.70)}]. \quad (5.85)$$

Since each  $D_{i,e}$  and  $M_i$  have dimensions  $k \times n$  and  $n \times k$ , respectively, and  $k \leq n$ , the rank of each matrix is at most  $k$ , but we also have

$$\begin{aligned} \min(\text{rank}(D_{i,e}), \text{rank}(M_i)) &\geq \text{rank}(D_{i,e} M_i) \quad [\text{from (5.67)}] \\ &= \text{rank}(I_k) = k \quad [\text{from (5.85)}], \end{aligned}$$

and so  $\text{rank}(D_{i,e}) = \text{rank}(M_i) = k$ , which, by Lemma 5.A.4, implies

$$\text{rank}(Q_{i,e}) = n - k \quad (i = 1, 2, \dots, m). \quad (5.86)$$

Since  $\text{rank}(M_0) = k$ , Lemma 5.A.3 implies there exists an  $n \times n$  nonsingular matrix  $W$  such that

$$WM_0 = \begin{bmatrix} I_k \\ 0_{(n-k) \times k} \end{bmatrix}. \quad (5.87)$$

Partition each of the  $k \times n$  matrices  $D_{i,e}W^{-1}$  into a  $k \times k$  block  $T_i$  to the left of a  $k \times (n-k)$  block  $U_i$ :

$$D_{i,e}W^{-1} = [T_i \quad U_i] \quad (5.88)$$

and then let  $V$  be the following  $n \times n$  matrix over  $\mathbb{F}$ :

$$V = \begin{bmatrix} I_k & U_0 \\ 0_{(n-k) \times k} & I_{n-k} \end{bmatrix}. \quad (5.89)$$

It is easy to verify that

$$V^{-1} = \begin{bmatrix} I_k & -U_0 \\ 0_{(n-k) \times k} & I_{n-k} \end{bmatrix}. \quad (5.90)$$

For each  $i = 0, 1, \dots, m$ , change the network encoding and decoding matrices from  $M_i$  and  $D_{i,e}$ , respectively, to

$$M'_i = VWM_i \quad (5.91)$$

$$D'_{i,e} = D_{i,e}W^{-1}V^{-1}. \quad (5.92)$$

We have

$$T_0 = D_{0,e}W^{-1}WM_0 = I_k \quad [\text{from (5.85), (5.87), (5.88)}] \quad (5.93)$$

$$M'_0 = \begin{bmatrix} I_k \\ 0 \end{bmatrix} \quad [\text{from (5.87), (5.89), (5.91)}]$$

$$D'_{0,e} = [I_k \quad 0] \quad [\text{from (5.88), (5.90), (5.92), (5.93)}]. \quad (5.94)$$

In this case,  $e' = \sum_{j=0}^m M'_j x_j$  and for each  $i = 0, 1, \dots, m$ , the message vectors can be recovered by:

$$D'_{i,e}e' + D_i e_i = D_{i,e}W^{-1}V^{-1} \sum_{j=0}^m VWM_j x_j + D_i e_i \quad [\text{from (5.91), (5.92)}]$$

$$= D_{i,e}e + D_i e_i = x_i \quad [\text{from (5.69), (5.70)}].$$

Thus, this linear code still provides a  $(k, n)$  solution.

Partition each of the matrices  $M_i$  into a  $k \times k$  block  $R_i$  on top of a  $(n - k) \times k$  block  $S_i$ :

$$M_i = \begin{bmatrix} R_i \\ S_i \end{bmatrix} \quad (5.95)$$

and let  $\rho = \text{rank}([R_1 \ \cdots \ R_m])$ , where  $[R_1 \ \cdots \ R_m]$  is the concatenation of the matrices  $R_i$  into a  $k \times mk$  matrix. Clearly  $\rho \leq k$ . We have

$$\begin{aligned} D_0 \sum_{j=1}^m M_{0,j} x_j &= D_0 e_0 && \text{[from (5.68)]} \\ &= -D_{0,e} \sum_{j=1}^m M_j x_j && \text{[from (5.73)]} \\ &= - \sum_{j=1}^m R_j x_j && \text{[from (5.94), (5.95)].} \end{aligned}$$

This gives us  $D_0 [M_{0,1} \ \cdots \ M_{0,m}] = -[R_1 \ \cdots \ R_m]$ , which implies

$$\begin{aligned} \text{rank}(D_0) &\geq \text{rank}([R_1 \ \cdots \ R_m]) = \rho && \text{[from (5.67)]} \\ \therefore \text{rank}(Q_0) &= n - \text{rank}(D_0) \leq n - \rho. && (5.96) \end{aligned}$$

Since the matrix  $[R_1 \ \cdots \ R_m]$  has rank  $\rho$ , there exists a  $k \times k$  permutation matrix  $P$  such that the first  $\rho$  rows of  $P [R_1 \ \cdots \ R_m]$  are linearly independent and the remaining  $k - \rho$  rows are linear combinations of those first  $\rho$  rows. Thus, there exists a  $(k - \rho) \times k$  matrix  $X$ , whose right-most  $k - \rho$  columns form  $I_{k-\rho}$ , and such that

$$XP [R_1 \ \cdots \ R_m] = 0_{(k-\rho) \times mk}. \quad (5.97)$$

$X$  and  $P$  are  $(k - \rho) \times k$  and  $k \times k$  respectively, thus the rank of  $X$  is at most  $(k - \rho)$  and the rank of  $P$  is at most  $k$ . Since the right-most columns of  $X$  form  $I_{k-\rho}$ , we have  $\text{rank}(X) = k - \rho$ , and since  $P$  is a permutation matrix, we have  $\text{rank}(P) = k$ . Since  $XP$  has dimensions  $(k - \rho) \times k$ , we have

$$\begin{aligned} k - \rho &\geq \text{rank}(XP) \\ &\geq \text{rank}(X) + \text{rank}(P) - k && \text{[from (5.66)]} \\ &= (k - \rho) + k - k = k - \rho \end{aligned}$$

and thus  $\text{rank}(XP) = k - \rho$ .

Define a  $(k - \rho) \times n$  matrix  $Y$  by concatenating the product  $XP$  with an all-zero matrix as follows:

$$Y = [XP \quad 0_{(k-\rho) \times (n-k)}].$$

For each  $i = 1, 2, \dots, m$  we have

$$YM_i = \begin{bmatrix} XP & 0_{(k-\rho) \times (n-k)} \end{bmatrix} \begin{bmatrix} R_i \\ S_i \end{bmatrix} = 0_{(k-\rho) \times k} \quad [\text{from (5.95), (5.97)}]. \quad (5.98)$$

Since, for each  $i = 1, 2, \dots, m$ , we have  $YM_i = 0_{(k-\rho) \times k}$  and by (5.85),  $D_{i,e}M_i = I_k$ , the rows of  $Y$  and the rows of  $D_{i,e}$  are linearly independent. (If  $v$  is a nontrivial linear combination of rows of  $D_{i,e}$ , then  $vM_i \neq 0$ ; if  $v'$  is a nontrivial linear combination of rows of  $Y$ , then  $v'M_i = 0$ , so  $v \neq v'$ ). Therefore, by Lemma 5.A.4, we may choose  $Q_{i,e}$  such that its first  $k - \rho$  rows are the rows of  $Y$ . By (5.86), each vector function  $Q_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j$  in the list  $L$  has dimension  $n - k$ , but the first  $k - \rho$  components of each such vector function can be written as

$$Y \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j = YM_0 x_0 \quad [\text{from (5.98)}]. \quad (5.99)$$

If we view the message vectors  $x_0, x_1, \dots, x_m$  as random variables, each of whose  $k$  components are independent and uniformly distributed over the field  $\mathbb{F}$ , then we have the following entropy (using logarithms with base  $|\mathbb{F}|$ ) upper bounds:

$$H(Q_0 e_0) \leq n - \rho \quad [\text{from (5.96)}] \quad (5.100)$$

$$H(e_1, \dots, e_m) \leq mn \quad [\text{from } e_i \in \mathbb{F}^n] \quad (5.101)$$

$$H \left( Q_{i,e} \sum_{\substack{j=0 \\ j \neq i}}^m M_j x_j : i = 1, 2, \dots, m \right) \leq m(n - k) - (m - 1)(k - \rho) \quad [\text{from (5.86), (5.99)}] \quad (5.102)$$

$$(5.103)$$

Therefore, the entropy of all of the vector functions in the list  $L$  is bounded by summing these bounds. So

$$\begin{aligned} (m+1)k &= H(x_0, x_1, \dots, x_m) && [\text{from } x_i \in \mathbb{F}^k] \\ &\leq H(L) && [\text{from (5.82), (5.84)}] \\ &\leq (2m+1)n - (m+1)k - (k-\rho)(m-2) && [\text{from (5.100), (5.101), (5.102)}] \\ &\leq (2m+1)n - (m+1)k && [\text{from } \rho \leq k \text{ and } m \geq 2] \\ \therefore \frac{k}{n} &\leq \frac{2m+1}{2m+2}. \end{aligned}$$

Thus the linear capacity of  $\mathcal{N}_1(m)$  for any finite-field alphabet whose characteristic divides  $m$  is upper bounded by  $1 - \frac{1}{2m+2}$ .



For each  $y \in \mathbb{F}^m$ , let  $[y]_i$  denote the  $i$ th component of  $y$ . To show the upper bound on the linear capacity is tight, consider a  $(2m+1, 2m+2)$  fractional linear code for  $\mathcal{N}_1(m)$  over any finite-field alphabet whose characteristic divides  $m$ , given by:

$$[e_0]_l = \begin{cases} \sum_{\substack{j=1 \\ j \neq l}}^m [x_j]_l & (l = 1, 2, \dots, m) \\ \sum_{j=1}^m [x_j]_l & (l = m+1, \dots, 2m+1) \\ \sum_{j=2}^m [x_j]_j & (l = 2m+2) \end{cases}$$

$$[e]_l = \begin{cases} \sum_{\substack{j=0 \\ j \neq l}}^m [x_j]_l & (l = 1, 2, \dots, m) \\ \sum_{j=0}^m [x_j]_l & (l = m+1, \dots, 2m+1) \\ [x_0]_{m+1} + \sum_{j=1}^m [x_j]_j & (l = 2m+2) \end{cases}$$

$$[e_i]_l = \begin{cases} \sum_{\substack{j=0 \\ j \neq i \\ j \neq l}}^m [x_j]_l & (l = 1, 2, \dots, m \text{ and } l \neq i) \\ [x_0]_{m+1} + \sum_{\substack{j=1 \\ j \neq i}}^m [x_j]_j & (l = i) \\ \sum_{\substack{j=0 \\ j \neq i}}^m [x_j]_l & (l = m+1, \dots, 2m+1) \\ [x_0]_{m+1+i} & (l = 2m+2). \end{cases} \quad (i = 1, 2, \dots, m)$$

For each  $l = 1, 2, \dots, m$ , we have

$$\sum_{\substack{i=0 \\ i \neq l}}^m [e_i]_l = \sum_{\substack{i=0 \\ i \neq l}}^m \sum_{\substack{j=0 \\ j \neq i \\ j \neq l}}^m [x_j]_l = (m-1) \sum_{\substack{j=0 \\ j \neq l}}^m [x_j]_l = - \sum_{\substack{j=0 \\ j \neq l}}^m [x_j]_l \quad [\text{from char}(\mathbb{F}) \mid m]. \quad (5.104)$$

For each  $i = 1, 2, \dots, m$ , the receivers can linearly recover their respective demands by:

$$R_0 : [e]_l - [e_0]_l = [x_0]_l \quad (l = 1, 2, \dots, 2m+1)$$

$$R_i : [e]_l - [e_i]_l = [x_i]_l \quad (l = 1, \dots, 2m+1 \text{ and } l \neq i)$$

$$[e]_{2m+2} - [e_i]_i = [x_i]_i$$

$$R_x : -[e_0]_l - \sum_{\substack{i=0 \\ i \neq l}}^m [e_i]_l = [x_0]_l \quad (l = 1, 2, \dots, m) \quad [\text{from (5.104)}]$$

$$[e_1]_1 - [e_0]_{2m+2} = [x_0]_{m+1}$$

$$[e_{l-m-1}]_{2m+2} = [x_0]_l \quad (l = m+2, \dots, 2m+1).$$

Thus, the code is in fact a solution for  $\mathcal{N}_1(m)$ . ■

### 5.A.2 $\mathcal{N}_2$ Capacity Proof

*Proof of Lemma 5.4.7.* Since a scalar linear solution over a finite field is a special case of a linear solution over a standard module, by Lemma 5.4.6,  $\mathcal{N}_2(m, w)$  is scalar linearly solvable over any finite field whose characteristic divides  $m$ , so the linear capacity for such fields alphabets is at least 1. By Lemma 5.2.4, network  $\mathcal{N}_0(m+1)$  has capacity equal to 1, and the block  $B^{(1)}(m+1)$  together with the source nodes  $S_z, S_1^{(1)}, S_2^{(1)}, \dots, S_{m+1}^{(1)}$  forms a copy of  $\mathcal{N}_0(m+1)$ , so the capacity of  $\mathcal{N}_2(m, w)$  is at most 1. Thus both the capacity of  $\mathcal{N}_2(m, w)$  and its linear capacity over any finite field whose characteristic divides  $m$  are 1.

To prove part (c), consider a  $(k, n)$  fractional linear solution for  $\mathcal{N}_2(m, w)$  over a finite field  $\mathbb{F}$  whose characteristic does not divide  $m$ . Since  $\text{char}(\mathbb{F}) \nmid m$ , the integer  $m$  is invertible in  $\mathbb{F}$ . We have  $x_j^{(l)}, z \in \mathbb{F}^k$  and  $e_i^{(l)}, e^{(l)} \in \mathbb{F}^n$ , with  $n \geq k$ , since the capacity is one. There exist  $n \times k$  coding matrices  $M_j^{(l)}, M_{i,j}^{(l)}$  over  $\mathbb{F}$ , such that for each  $l = 1, 2, \dots, w$  the edge vectors can be written as:

$$e_i^{(l)} = M_{i,0}^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_{i,j}^{(l)} x_j^{(l)} \quad (i = 1, 2, \dots, m+1) \quad (5.105)$$

$$e^{(l)} = M_0^{(l)} z + \sum_{j=1}^{m+1} M_j^{(l)} x_j^{(l)} \quad (5.106)$$

and there exist  $k \times n$  decoding matrices  $D_{i,e}^{(l)}$  and  $D_i^{(l)}$  over  $\mathbb{F}$ , such that for each  $l = 1, 2, \dots, w$ , the message vector  $x_i^{(l)}$  can be linearly decoded at  $R_i^{(l)}$  from the  $n$ -vectors  $e_i^{(l)}$  and  $e^{(l)}$  by:

$$R_i^{(l)} : x_i^{(l)} = D_{i,e}^{(l)} e^{(l)} + D_i^{(l)} e_i^{(l)} \quad (i = 1, 2, \dots, m+1). \quad (5.107)$$

Since receiver  $R_z$  linearly recovers  $z$  from its incoming edge vectors, we have

$$\left\{ e_i^{(l)} : \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right\} \longrightarrow z. \quad (5.108)$$

By (5.105) and (5.106), if we set  $x_i^{(l)} = 0$  in (5.107), then, since  $e_i^{(l)}$  does not depend on  $x_i^{(l)}$ , we get the following relationship among the remaining message vectors:

$$0 = D_{i,e}^{(l)} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) + D_i^{(l)} e_i^{(l)} \quad \left( \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right) \quad (5.109)$$

and therefore

$$e_i^{(l)} \longrightarrow D_{i,e}^{(l)} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) \quad \left( \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right) \quad [\text{from (5.109)}]. \quad (5.110)$$

For each  $l = 1, 2, \dots, w$  and each  $i = 1, 2, \dots, m+1$ , let  $Q_{i,e}^{(l)}$  be the matrix  $Q$  in Lemma 5.A.4 corresponding to when the matrix  $A$  is  $D_{i,e}^{(l)}$ , and let  $L^{(l)}$  be the following list of  $2(m+1)$  vector functions of the messages:

$$\begin{aligned} Q_{i,e}^{(l)} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) & \quad (i = 1, 2, \dots, m+1) \\ e_i^{(l)} & \quad (i = 1, 2, \dots, m+1). \end{aligned}$$

We have

$$L^{(l)} \longrightarrow D_{i,e}^{(l)} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) \quad \left( \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right) \quad [\text{from (5.110)}],$$

which, along with Lemma 5.A.4, implies

$$L^{(l)} \longrightarrow M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)}. \quad \left( \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right) \quad (5.111)$$

For each  $l = 1, 2, \dots, w$ , we also have

$$\begin{aligned}
& z, \left\{ M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} : i = 1, 2, \dots, m+1 \right\} \\
& \longrightarrow \sum_{i=1}^{m+1} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) - M_0^{(l)} z \\
& = (m+1) M_0^{(l)} z + m \sum_{j=1}^{m+1} M_j^{(l)} x_j^{(l)} - M_0^{(l)} z \\
& = m e^{(l)} \longrightarrow e^{(l)} \quad [\text{from (5.106) and } \text{char}(\mathbb{F}) \nmid m] \tag{5.112}
\end{aligned}$$

and

$$L^{(1)}, \dots, L^{(w)} \longrightarrow z \quad [\text{from (5.108)}] \tag{5.113}$$

$$L^{(l)}, z \longrightarrow e^{(l)} \quad (l = 1, 2, \dots, w) \quad [\text{from (5.111), (5.112)}] \tag{5.114}$$

$$L^{(l)}, z \longrightarrow x_i^{(l)} \quad \begin{pmatrix} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{pmatrix} \quad [\text{from (5.107), (5.114)}]. \tag{5.115}$$

Thus it follows from (5.113) and (5.115) that

$$L^{(1)}, \dots, L^{(w)} \longrightarrow z, \left\{ x_i^{(l)} : \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right\}. \tag{5.116}$$

We will now bound the number of independent entries in each list  $L^{(l)}$ .

By equating message components in equation (5.107), we have:

$$I_k = D_{i,e}^{(l)} M_i^{(l)} \quad \begin{pmatrix} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{pmatrix} \quad [\text{from (5.105), (5.106), (5.107)}] \tag{5.117}$$

Since each  $D_{i,e}^{(l)}$  is  $k \times n$  and  $k \leq n$ , the rank of each matrix is at most  $k$ , but we also have

$$\begin{aligned}
\text{rank} \left( D_{i,e}^{(l)} \right) & \geq \text{rank} \left( D_{i,e}^{(l)} M_i^{(l)} \right) && [\text{from (5.67)}] \\
& = \text{rank} (I_k) = k && [\text{from (5.117)}].
\end{aligned}$$

Hence  $\text{rank} \left( D_{i,e}^{(l)} \right) = k$ , which by Lemma (5.A.4), implies  $\text{rank} \left( Q_{i,e}^{(l)} \right) = n - k$ . Therefore each vector function

$$Q_{i,e}^{(l)} \begin{pmatrix} M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \\ (l = 1, 2, \dots, w) \\ (i = 1, 2, \dots, m+1) \end{pmatrix}$$

in the list  $L^{(l)}$  has dimension  $n - k$ .

If we view the message vectors as random variables, each of whose  $k$  components are independent and uniformly distributed over the field  $\mathbb{F}$ , then we have the following entropy (using logarithms base  $|\mathbb{F}|$ ) upper bounds:

$$H \left( Q_{i,e}^{(l)} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) : \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right) \leq w(m+1)(n-k) \quad (5.118)$$

$$H \left( e_i^{(l)} : \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right) \leq w(m+1)n. \quad (5.119)$$

Since each message is independent and uniformly distributed over  $\mathbb{F}$  and  $z, x_i^{(l)} \in \mathbb{F}^k$ , we have

$$\begin{aligned} (w(m+1)+1)k &= H \left( z, \left\{ x_i^{(l)} : \begin{array}{l} l = 1, 2, \dots, w \\ i = 1, 2, \dots, m+1 \end{array} \right\} \right) \\ &\leq H \left( L^{(1)}, \dots, L^{(w)} \right) && \text{[from (5.116)]} \\ &\leq w(m+1)n - w(m+1)k. && \text{[from (5.118), (5.119)]} \end{aligned}$$

which implies

$$\frac{k}{n} \leq \frac{2w(m+1)}{2w(m+1)+1}.$$

Thus the linear capacity of  $\mathcal{N}_2(m, w)$  for finite-field alphabets whose characteristic does not divide  $m$  is upper bounded by  $1 - \frac{1}{2mw+2w+1}$ . ■

### 5.A.3 $\mathcal{N}_3$ Capacity Proof

*Proof of Lemma 5.5.8.* By Lemma 5.5.6, the network  $\mathcal{N}_3(m_1, m_2)$  is scalar linearly solvable over any finite field whose characteristic is relatively prime to  $m_1$  or  $m_2$ , so the network's linear capacity for such fields is at least 1. By Lemma 5.2.4, network  $\mathcal{N}_0(m_1)$  has capacity equal to 1, the block  $B^{(1)}(m_1)$  together with the source nodes  $S_z, S_1^{(1)}, S_2^{(1)}, \dots, S_{m_1}^{(1)}$  forms a copy of  $\mathcal{N}_0(m_1)$ , so the capacity of  $\mathcal{N}_3(m_1, m_2)$  is at most 1. Thus both the capacity of  $\mathcal{N}_3(m_1, m_2)$  and its linear capacity over any finite field whose characteristic is relatively prime to  $m_1$  or  $m_2$  are 1.

To prove part (c), consider a  $(k, n)$  fractional linear solution for  $\mathcal{N}_3(m_1, m_2)$  over a finite field  $\mathbb{F}$  whose characteristic divides both  $m_1$  and  $m_2$ . Since  $\text{char}(\mathbb{F}) \mid m_1$  and  $\text{char}(\mathbb{F}) \mid m_2$ , we have  $m_1 = m_2 = 0$  in  $\mathbb{F}$ . We have  $x_j^{(l)}, z \in \mathbb{F}^k$  and  $e_i^{(l)}, e^{(l)} \in \mathbb{F}^n$ , with  $n \geq k$ , since the capacity is one. There exist  $n \times k$  coding

matrices  $M_j^{(l)}, M_{i,j}^{(l)}$  with entries in  $\mathbb{F}$ , such that for each  $l = 1, 2$  the edge vectors can be written as:

$$e_0^{(l)} = \sum_{j=1}^{m_l} M_{0,j}^{(l)} x_j^{(l)} \quad (5.120)$$

$$e_i^{(l)} = M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_{i,j}^{(l)} x_j^{(l)} \quad (i = 1, 2, \dots, m_l) \quad (5.121)$$

$$e^{(l)} = M_0^{(l)} z + \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \quad (5.122)$$

and there exist  $k \times n$  decoding matrices  $D_{i,e}^{(l)}, D_i^{(l)}$  with entries in  $\mathbb{F}$ , such that for each  $l = 1, 2$  the receivers within the block  $B^{(l)}(m_l)$  can recover their respective demands from their received edge vectors by:

$$R_0^{(l)} : z = D_{0,e}^{(l)} e^{(l)} + D_0^{(l)} e_0^{(l)} \quad (5.123)$$

$$R_i^{(l)} : x_i^{(l)} = D_{i,e}^{(l)} e^{(l)} + D_i^{(l)} e_i^{(l)} \quad (i = 1, 2, \dots, m_l). \quad (5.124)$$

For each  $l = 1, 2$ , by (5.120) and (5.122), if we set  $z = 0$  in (5.123), we have

$$\begin{aligned} 0 &= D_{0,e}^{(l)} \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} + D_0^{(l)} e_0^{(l)} \\ \therefore \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} &\longrightarrow D_0^{(l)} e_0^{(l)} \end{aligned} \quad (5.125)$$

and similarly, for each  $i = 1, 2, \dots, m_l$ , by (5.121) and (5.122), if we set  $x_i^{(l)} = 0$  in (5.124), we have

$$\begin{aligned} 0 &= D_{i,e}^{(l)} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \right) + D_i^{(l)} e_i^{(l)} \\ \therefore e_i^{(l)} &\longrightarrow D_{i,e}^{(l)} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \right). \end{aligned} \quad (5.126)$$

Since the receiver  $R_z$  recovers message vector  $z$  linearly from its incoming edge vectors, we have

$$\left\{ e_i^{(l)} : \begin{array}{l} l = 1, 2 \\ i = 0, 1, \dots, m_l \end{array} \right\} \longrightarrow z. \quad (5.127)$$

As in Lemma 5.3.4, for each  $l = 1, 2$  and  $i = 1, 2, \dots, m_l$ , let  $Q_0^{(l)}$  be the matrix  $Q$  in Lemma 5.A.4 corresponding to when  $D_0^{(l)}$  is the matrix  $A$  in the lemma, and let  $Q_{i,e}^{(l)}$  be the matrix  $Q$  corresponding to when  $D_{i,e}^{(l)}$  is the matrix  $A$ .

Let  $L^{(1)}$  and  $L^{(2)}$  be the lists from Lemma 5.3.4 (where  $z$  plays the role of  $x_0$ ), corresponding to the left-hand side and right-hand side of the network, respectively. Specifically, for each  $l = 1, 2$ , let  $L^{(l)}$  be the list

$$\begin{aligned} & \mathcal{Q}_0^{(l)} e_0^{(l)} \\ & e_i^{(l)} \quad (i = 1, 2, \dots, m_l) \\ & \mathcal{Q}_{i,e}^{(l)} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \right) \quad (i = 1, 2, \dots, m_l). \end{aligned}$$

For each  $l = 1, 2$ , we have

$$\begin{aligned} L^{(l)} & \longrightarrow D_{i,e}^{(l)} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \right) && \text{[from (5.126)]} \\ \therefore L^{(l)} & \longrightarrow M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} && \text{[from Lemma 5.A.4].} \end{aligned} \quad (5.128)$$

and

$$\begin{aligned} & \left\{ M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} : i = 1, 2, \dots, m_l \right\} \\ & \longrightarrow \sum_{i=1}^{m_l} \left( M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} M_j^{(l)} x_j^{(l)} \right) = m_l M_0^{(l)} z + (m_l - 1) \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \\ & = - \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \quad \text{[from } \text{char}(\mathbb{F}) \mid m_l], \end{aligned} \quad (5.129)$$

and so

$$L^{(l)} \longrightarrow \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \quad \text{[from (5.129), (5.128)]} \quad (5.130)$$

$$L^{(l)} \longrightarrow D_0^{(l)} e_0^{(l)} \quad \text{[from (5.125), (5.130)]} \quad (5.131)$$

$$L^{(l)} \longrightarrow e_0^{(l)} \quad \text{[from Lemma 5.A.4, (5.131)]} \quad (5.132)$$

$$z, \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \longrightarrow e^{(l)} \quad \text{[from (5.122)]} \quad (5.133)$$

$$L^{(l)}, z \longrightarrow e^{(l)} \quad \text{[from (5.130), (5.133)]} \quad (5.134)$$

Finally, we have

$$L^{(1)}, L^{(2)} \longrightarrow z \quad [\text{from (5.127), (5.132)}] \quad (5.135)$$

$$L^{(l)}, z \longrightarrow x_i^{(l)} \quad (l = 1, 2 \text{ and } i = 1, 2, \dots, m_l) \quad [\text{from (5.124), (5.134)}]. \quad (5.136)$$

Thus equations (5.135) and (5.136) imply

$$L^{(1)}, L^{(2)} \longrightarrow z, \left\{ x_i^{(l)} : \begin{array}{l} l = 1, 2 \\ i = 1, 2, \dots, m_l \end{array} \right\}. \quad (5.137)$$

We have  $L^{(l)}$  corresponding to the same set of vector functions (with a slight change of labeling) as the list  $L$  for  $\mathcal{N}_1(m_l)$  in Lemma 5.3.4. Thus the bound on the entropy of the list  $L$  in the proof of Lemma 5.3.4 can be used to bound the entropy of the list  $L^{(1)}, L^{(2)}$ . Since each message is independent and uniformly distributed over  $\mathbb{F}$  and  $z, x_i^{(l)} \in \mathbb{F}^k$ , we have

$$\begin{aligned} (m_1 + m_2 + 1)k &= H \left( z, \left\{ x_i^{(l)} : \begin{array}{l} l = 1, 2 \\ i = 1, 2, \dots, m_l \end{array} \right\} \right) \\ &\leq H(L_1, L_2) \quad [\text{from (5.137)}] \\ &\leq (2m_1 + 2m_2 + 2)n - (m_1 + m_2 + 2)k \quad [\text{from (5.100), (5.101), (5.102)}] \end{aligned}$$

which implies

$$\frac{k}{n} \leq \frac{2m_1 + 2m_2 + 2}{2m_1 + 2m_2 + 3}.$$

Thus the linear capacity of  $\mathcal{N}_3(m_1, m_2)$  for finite-field alphabets whose characteristic divides both  $m_1$  and  $m_2$  is upper bounded by  $1 - \frac{1}{2m_1 + 2m_2 + 3}$ .

Consider a  $(k, n) = (2m_1 + 2m_2 + 2, 2m_1 + 2m_2 + 3)$  fractional linear code for  $\mathcal{N}_3(m_1, m_2)$  over any finite-field alphabet whose characteristic divides both  $m_1$  and  $m_2$ , described below. Let the  $(k + 1)$ -dimensional edge vectors on the left-hand-side of the network be given by

$$[e^{(1)}]_l = \begin{cases} [z]_l + \sum_{\substack{j=1 \\ j \neq l}}^{m_1} [x_j^{(1)}]_l & (l = 1, 2, \dots, m_1) \\ [z]_l + \sum_{j=1}^{m_1} [x_j^{(1)}]_l & (l = m_1 + 1, \dots, k) \\ [z]_{m_1+1} + \sum_{j=1}^{m_1} [x_j^{(1)}]_j & (l = k + 1) \end{cases}$$



$$\begin{aligned}
[e_0^{(1)}]_l &= \begin{cases} \sum_{\substack{j=1 \\ j \neq l}}^{m_1} [x_j^{(1)}]_l & (l = 1, 2, \dots, m_1) \\ \sum_{j=1}^{m_1} [x_j^{(1)}]_l & (l = m_1 + 1, \dots, k) \\ \sum_{j=2}^{m_1} [x_j^{(1)}]_j & (l = k + 1) \end{cases} \\
[e_i^{(1)}]_l &= \begin{cases} [z]_l + \sum_{\substack{j=1 \\ j \neq i \\ j \neq l}}^{m_1} [x_j^{(1)}]_l & \left( \begin{array}{l} l = 1, 2, \dots, m_1 \\ \text{and } l \neq i \end{array} \right) \\ [z]_{m_1+1} + \sum_{\substack{j=1 \\ j \neq i}}^{m_1} [x_j^{(1)}]_j & (l = i) \\ [z]_l + \sum_{\substack{j=1 \\ j \neq i}}^{m_1} [x_j^{(1)}]_l & (l = m_1 + 1, \dots, k) \\ [z]_{m_1+i+1} & (l = k + 1). \end{cases} \quad (i = 1, 2, \dots, m_1)
\end{aligned}$$

For brevity, let  $\delta = 2m_1 + m_2 + 2 = k - m_2$ , and let the  $(k + 1)$ -dimensional edge vectors on the right-hand side of the network be given by

$$\begin{aligned}
[e^{(2)}]_l &= \begin{cases} [z]_l + \sum_{j=1}^{m_2} [x_j^{(2)}]_l & (l = 1, 2, \dots, \delta) \\ [z]_l + \sum_{\substack{j=1 \\ j \neq l - \delta}}^{m_2} [x_j^{(2)}]_l & (l = \delta + 1, \dots, k) \\ [z]_\delta + \sum_{j=1}^{m_2} [x_j^{(2)}]_{\delta+j} & (l = k + 1) \end{cases} \\
[e_0^{(2)}]_l &= \begin{cases} \sum_{j=1}^{m_2} [x_j^{(2)}]_l & (l = 1, 2, \dots, \delta) \\ \sum_{\substack{j=1 \\ j \neq l - \delta}}^{m_2} [x_j^{(2)}]_l & (l = \delta + 1, \dots, k) \\ \sum_{j=2}^{m_2} [x_j^{(2)}]_{\delta+j} & (l = k + 1) \end{cases}
\end{aligned}$$

$$[e_i^{(2)}]_l = \begin{cases} [z]_l + \sum_{\substack{j=1 \\ j \neq i}}^{m_2} [x_j^{(2)}]_l & (l = 1, 2, \dots, \delta) \\ [z]_\delta + \sum_{\substack{j=1 \\ j \neq i}}^{m_2} [x_j^{(2)}]_{\delta+j} & (l = \delta + i) \\ [z]_l + \sum_{\substack{j=1 \\ j \neq i \\ j \neq l-\delta}}^{m_2} [x_j^{(2)}]_l & \left( \begin{array}{l} l = \delta + 1, \dots, k \\ \text{and } l \neq \delta + i \end{array} \right) \\ [z]_{2m_1+1+i} & (l = k + 1). \end{cases} \quad (i = 1, 2, \dots, m_2)$$

For each  $i = 1, 2, \dots, m_1$ , the left-hand-side receivers can linearly recover their demands as follows:

$$R_0^{(1)} : [e^{(1)}]_l - [e_0^{(1)}]_l = [z]_l \quad (l = 1, 2, \dots, k)$$

$$R_i^{(1)} : [e^{(1)}]_{k+1} - [e_i^{(1)}]_i = [x_i^{(1)}]_i \\ [e^{(1)}]_l - [e_i^{(1)}]_l = [x_i^{(1)}]_l \quad \left( \begin{array}{l} l = 1, 2, \dots, k \\ \text{and } l \neq i \end{array} \right).$$

For each  $i = 1, 2, \dots, m_2$ , the right-hand-side receivers can linearly recover their demands as follows:

$$R_0^{(2)} : [e^{(2)}]_l - [e_0^{(2)}]_l = [z]_l \quad (l = 1, 2, \dots, k)$$

$$R_i^{(2)} : [e^{(2)}]_{k+1} - [e_i^{(2)}]_{\delta+i} = [x_i^{(2)}]_{\delta+i} \\ [e^{(2)}]_l - [e_i^{(2)}]_l = [x_i^{(2)}]_l \quad \left( \begin{array}{l} l = 1, 2, \dots, k \\ \text{and } l \neq \delta + i \end{array} \right).$$

For each  $l = 1, 2, \dots, m_1$ , we have

$$\sum_{\substack{i=1 \\ i \neq l}}^{m_1} [e_i^{(1)}]_l = (m_1 - 1)[z]_l + (m_1 - 2) \sum_{\substack{j=1 \\ j \neq l}}^{m_1} [x_j^{(1)}]_l \\ = -[z]_l - 2[e_0^{(1)}]_l \quad [\text{from char}(\mathbb{F}) \mid m_1]. \quad (5.138)$$

Similarly, for each  $l = \delta + 1, \dots, k$ , we have

$$\begin{aligned} \sum_{\substack{i=1 \\ i \neq l-\delta}}^{m_2} [e_i^{(2)}]_l &= (m_2 - 1) [z]_l + (m_2 - 2) \sum_{\substack{j=1 \\ j \neq l-\delta}}^{m_2} [x_j^{(2)}]_l \\ &= -[z]_l - 2[e_0^{(2)}]_l \end{aligned} \quad \text{[from char}(\mathbb{F}) \mid m_2]. \quad (5.139)$$

The shared receiver can recover  $z$  as follows:

$$R_z : -2[e_0^{(1)}]_l - \sum_{\substack{i=1 \\ i \neq l}}^{m_1} [e_i^{(1)}]_l = [z]_l \quad (l = 1, 2, \dots, m_1) \quad \text{[from (5.138)]}$$

$$[e_1^{(1)}]_1 - [e_0^{(1)}]_{k+1} = [z]_{m_1+1}$$

$$[e_{l-m_1-1}^{(1)}]_{k+1} = [z]_l \quad (l = m_1 + 2, \dots, 2m_1 + 1)$$

$$[e_{l-2m_1-1}^{(2)}]_{k+1} = [z]_l \quad (l = 2m_1 + 2, \dots, \delta - 1)$$

$$[e_1^{(2)}]_{\delta+1} - [e_0^{(2)}]_{k+1} = [z]_\delta$$

$$-2[e_0^{(2)}]_l - \sum_{\substack{i=1 \\ i \neq l-\delta}}^{m_2} [e_i^{(2)}]_l = [z]_l \quad (l = \delta + 1, \dots, k) \quad \text{[from (5.139)].}$$

Thus the code is, in fact, a linear solution for  $\mathcal{N}_3(m_1, m_2)$ . ■

## References

- [1] R. Ahlswede, C. Ning, S.-Y.R. Li, and R.W. Yeung, “Network information flow,” *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.
- [2] A. Blasiak, R. Kleinberg, and E. Lubetzky, “Lexicographic products and the power of non-linear network coding,” *IEEE Symposium on Foundations of Computer Science*, pp. 609–618, October 2011.
- [3] K. Cai and G. Han, “On the solvability of three-pair networks with common bottleneck links,” *IEEE Information Theory Workshop*, pp. 546–550, November 2–5, 2014.
- [4] 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.
- [5] T. Chan and A. Grant, “Dualities between entropy functions and network codes,” *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4470–4487, October 2008.
- [6] N. Das and B.K. Rai, “On the message dimensions of vector linearly solvable networks,” *IEEE Communications Letters*, vol. 20, no. 9, pp. 1701–1704, September 2016.
- [7] 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.
- [8] R. Dougherty, C. Freiling, and K. Zeger, “Linear network codes and systems of polynomial equations,” *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2303–2316, May 2008.
- [9] R. Dougherty, C. Freiling, and K. Zeger, “Linearity and solvability in multicast networks,” *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2243–2256, October 2004.
- [10] R. Dougherty, C. Freiling, and K. Zeger, “Networks, matroids, and non-Shannon information inequalities,” *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 1949–1969, June 2007.
- [11] R. Dougherty, C. Freiling, and K. Zeger, “Unachievability of network coding capacity,” *IEEE Transactions on Information Theory (joint issue with IEEE/ACM Transactions on Networking)*, vol. 52, no. 6, pp. 2365–2372, June 2006.
- [12] D. Dummit and R. Foote, *Abstract Algebra*, Third Edition, John Wiley and Sons Inc., 2004.
- [13] S. El Rouayheb, A. Sprintson, and C. Georghiades, “On the index coding problem and its relation to network coding and matroid theory,” *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3187–3195, July 2010.
- [14] T. Etzion and A. Wachter-Zeh, “Vector network coding based on subspace codes outperforms scalar linear network coding,” *IEEE International Symposium on Information Theory*, pp. 1949–1953, July 2016.
- [15] M. Feder, D. Ron, and A. Tavory, “Bounds on linear codes for network multicast,” *Electronic Colloquium on Computational Complexity*, pp. 1–9, 2003.
- [16] R. Koetter and M. Médard, “An algebraic approach to network coding,” *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, October 2003.
- [17] R. Koetter, Keynote presentation at *International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, March 31 – April 4, 2008, Berlin, Germany.
- [18] P. Krishnan and B.S. Rajan, “A matroidal framework for network-error correcting codes,” *IEEE Transactions on Information Theory*, vol. 61, no. 2, pp. 836–872, February 2015.
- [19] F. Kschischang, “An Introduction to Network Coding,” chapter 1 in: *Network Coding: Fundamentals and Applications*, M. Médard and A. Sprintson, editors, Academic Press, 2012.

- [20] S.-Y.R. Li, R.W. Yeung, and C. Ning, “Linear network coding,” *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, February 2003.
- [21] M. Médard, M. Effros, T. Ho, and D. Karger, “On coding for non-multicast networks,” *Conference on Communication Control and Computing*, Monticello, IL, October 2003.
- [22] V. Muralidharan and B. Rajan, “Linear network coding, linear index coding and representable discrete polymatroids,” *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 4096–4119, July 2016.
- [23] B.K. Rai and B.K. Dey, “On network coding for sum-networks”, *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 50–63, January 2012.
- [24] A. Rasala Lehman and E. Lehman, “Complexity classification of network information flow problems,” *ACM-SIAM Symposium on Discrete algorithms*, 2004.
- [25] S. Riis, “Linear versus nonlinear boolean functions in network flow,” *Conference on Information Sciences and Systems*, Princeton, NJ, March 2004.
- [26] G. Robin, “Estimation de la fonction de Tchebychef  $\theta$  sur le  $k$ -ième nombre premier et grandes valeurs de la fonction  $\omega(n)$  nombre de diviseurs premiers de  $n$ ” (in French), *Acta Arithmetica*, vol. 42, no. 4, pp. 367–389, 1983.
- [27] J. Sándor, D.S. Mitrinovic, and B. Crstici, *Handbook of Number Theory I*, Springer, 2006.
- [28] I. Satake, *Linear Algebra*. New York: Marcel Dekker, 1975.
- [29] S. Shenvi and B.K. Dey, “A simple necessary and sufficient condition for the double unicast problem,” *IEEE International Conference on Communications*, pp. 1–5, May 2010.
- [30] A. T. Subramanian and A. Thangaraj, “Path gain algebraic formulation for the scalar linear network coding problem,” *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4520–4531, September 2010.
- [31] Q. Sun, X. Yang, K. Long, X. Yin, and Z. Li, “On vector linear solvability of multicast networks,” *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 5096–5107, December 2016.
- [32] Q. T. Sun, S.-Y.R. Li, and C. Chan, “Matroidal characterization of optimal linear network codes over cyclic networks,” *IEEE Communications Letters*, vol. 17, no. 10, pp. 1992–1995, October 2013.
- [33] Q. Sun, X. Yin, Z. Li, and K. Long, “Multicast network coding and field sizes,” *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6182–6191, November 2015.
- [34] C. Yuan and H. Kan, “A characterization of solvability for a class of networks,” *Science China Information Sciences*, vol. 55, no. 4, pp. 747–754, April 2012.
- [35] C. Yuan, H. Kan, X. Wang, and H. Imai, “A construction method of matroidal networks,” *Science China Information Sciences* vol. 55, no. 11, pp. 2445-2453, 2012.

---

This chapter is a reprint of the material as it appears in “A class of non-linearly solvable networks,” *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 201 – 229, January 2017. The dissertation author was the primary investigator of this paper. © IEEE. Reprinted with permission.

# Chapter 6

## Big Picture Discussion

There are many open problems related to network coding theory, and in this chapter, we briefly discuss how the results in this dissertation fit into the bigger picture of network coding theory. We also comment on some potential directions for future work.

### 6.1 Can a Network be Linearly Solvable over Rings but not Fields?

It is known that not all solvable networks are linearly solvable over fields (or even rings or modules), so it is natural to ask whether rings can ever attain solvability when fields cannot. In Section 3.2.1, we established that vector linear solvability over some field is equivalent to linear solvability over some module (which generalizes both scalar and vector linear solvability over rings). We also showed that scalar linear solvability over some field is equivalent to scalar linear solvability over some commutative ring. Hence it is possible for a network to be scalar linearly solvable over some ring yet not over any field, but such a network will also have a vector linear solution over some field. In this sense, allowing for a broader class of linear codes does not make more networks “linearly solvable.”

In Sections 2.5.1 and 3.3.1, we additionally studied cases where networks do not have scalar linear solutions over a given field, yet do have a scalar linear solution over some other ring of the same size. We showed that, for each prime  $p$ , there exists such a ring of size  $p^k$  if and only if  $k \notin \{1, 2, 3, 6\}$ . Some examples of such rings include: when  $k = 4$ , the matrix ring  $M_2(\text{GF}(p))$ ; when  $k \geq 5$  is odd, the direct product ring  $\text{GF}(p^{(k+1)/2}) \times \text{GF}(p^{(k-1)/2})$ ; and when  $k \geq 8$  is even, the direct product ring  $\text{GF}(p^{(k/2)+1}) \times \text{GF}(p^{(k/2)-1})$ .

## 6.2 What is the “Best” Alphabet of a Given Size for Linear Coding?

Many networks evolve over time, as nodes and connections are added and removed, so it may be desirable to choose the alphabet that makes the most networks linearly solvable over the alphabet. Particularly, does there exist a module  $G$  of a given size such that: any network that is linearly solvable over *some* module of size  $|G|$  also is linearly solvable over  $G$  itself. If there exists such a module, then this module would be, in a sense, the “best” alphabet of a given size for linear network coding.

In Section 3.4, we demonstrated several classes of modules that are “dominated” by vector linear codes over prime fields. For example, if  $k \leq 6$ , then any network with a scalar linear solution over *some* ring of size  $p^k$  must also have a  $k$ -dimensional vector linear solution over  $\text{GF}(p)$ . We showed this result extends to all  $k \geq 2$  when the ring is commutative. This suggests that vector linear codes over prime fields *may* be the best candidate for linear coding when the alphabet size is fixed. However, it remains to be seen whether there can exist networks that are linearly solvable only over other modules of size  $p^k$ .

## 6.3 What is the “Best” Alphabet for Linear Coding on a Given Network?

Implementing a network code requires computation at intermediate nodes, and the time and space complexities of implementing a code are generally proportional to the size of the alphabet. In this sense, it is desirable to minimize the size of the network coding alphabet. We showed in Section 3.2.1 that vector linear solutions over finite fields yield the smallest alphabet sizes over which a given network can be linearly solvable (even when allowing for module alphabets). However, the field and the vector dimension are not always unique.

Of all of the ring and module alphabets to use for linear network coding, vector linear codes over prime fields appear to be among the best. On the other hand, we have also demonstrated an infinite class of networks that require non-linear codes to be solvable, and while vector linear codes over fields are desirable, it is also important to understand their limitations.

## 6.4 Over What Alphabet Sizes is a Given Network Solvable?

The role between the size of the alphabet and the solvability of networks is a promising direction for future research. Determining whether a network has a (possibly non-linear) solution over a given alphabet size is decidable, but it is a difficult problem, in general. The exact alphabet sizes over which a given network is solvable is only known for a handful of specific example networks. In Chapter 5, we demonstrated an

infinite class of networks that require non-power-of-prime alphabet sizes (and non-linear codes) to attain solutions. This particularly contrasts with linear network coding, since any network with a linear solution over a ring or module must have a vector linear solution over a finite field alphabet (with prime-power alphabet size). Another interesting direction for future research is studying structured non-linear codes, i.e. codes that are tractable (to an extent) yet outperform linear codes, such as codes in which edges carry polynomial functions of the inputs. A fundamental open question in network coding is whether or not solvability is decidable, and there remains much to discover about the solvability of general networks, particularly solvable networks that are not linearly solvable.

## **6.5 Can the Linear Capacity of a Network be Increased Using Rings?**

There are now numerous examples in the literature of networks whose linear capacities over finite fields are strictly less than their capacities. However, we have shown that linear codes over rings and modules offer no improvement over linear codes over fields with respect to the capacities of networks. Particularly, we showed in Section 4.4 that any network's linear capacity over a ring alphabet is upper bounded by its linear capacity over any finite field whose characteristic divides the ring's size. This fact also implies any two fields with the same characteristic will have the same linear capacities on every network.

Linear network coding over rings and modules offers some specific advantages over fields, but it does not close the gap between linear network coding over fields and non-linear network codes. Whether there exists a class of low-complexity codes that can do so remains to be seen. A fundamental open question in network coding is whether or not capacity is computable, and there remains much potential for future work in the area of non-linear network capacities.