A Class of Non-Linearly Solvable Networks

Joseph Connelly, *Student Member, IEEE*, and Kenneth Zeger, *Fellow, IEEE*

***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 alphabets and are not asymptotically linearly solvable over any finite-field alphabets. 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. In addition, if m is a non-power-of-prime composite number, then such a network is not solvable over any prime-power-size alphabet.**

***Index Terms*— Capacity, linear coding, network solvability, network coding.**

I. Introduction

A NETWORK will refer to a finite, directed, acyclic multigraph, some of whose nodes are *sources* or *receivers*. Source nodes generate k-dimensional vectors of *messages*, where each of the k 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 n alphabet symbols, called *edge symbols*. If a node has at most n input symbols, then we will assume, without loss of generality, that each of its out-edges carries all n of such 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 k-dimensional message vectors the receiver wishes to obtain. Each receiver also has *decoding functions* which map the receiver's inputs to k-dimensional vectors of alphabet symbols in an attempt to satisfy the receiver's demands.

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 (k, n) *solution over* $\mathcal{A}$ is a (k, n) code over $\mathcal{A}$ such that each receiver recovers all k components of each of its demands from its inputs.

Manuscript received January 14, 2016; accepted September 23, 2016. Date of publication October 19, 2016; date of current version December 20, 2016. This work was supported by the National Science Foundation. This paper was presented at the 2016 IEEE International Symposium on Information Theory. Communicated by S. Jaggi, Associate Editor for Coding Techniques.

The authors are with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA 92093 USA (e-mail: j2connelly@ucsd.edu; zeger@ucsd.edu).

Digital Object Identifier 10.1109/TIT.2016.2618379

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 $f : G^i \to G$ is *linear over the R-module G* if it can be written in the form

$$f(x_1, \ldots, x_i) = (M_1 \cdot x_1) \oplus \cdots \oplus (M_i \cdot x_i)$$

where $x_1, \ldots, x_i \in G$ are the node's inputs, $M_1, \ldots, M_i \in R$ 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) fractional code over a ring R, an edge function

$$f : \underbrace{R^k \times \cdots \times R^k}_{i \text{ message vectors}} \times \underbrace{R^n \times \cdots \times R^n}_{j \text{ in-edges}} \longrightarrow R^n$$

is *linear over* R if it can be written in the form

$$f(x_1, \ldots, x_i, y_1, \ldots, y_j) = M_1 x_1 + \cdots + M_i x_i + M'_1 y_1 + \cdots + M'_j y_j \qquad (1)$$

where $x_1, \ldots, x_i \in R^k$ are message vectors originating at the node, $y_1, \ldots, y_j \in R^n$ are edge vectors carried by the incoming edges to the node, $M_1, \ldots, M_i$ are $n \times k$ matrices and $M'_1, \ldots, M'_j$ 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 (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 (also called a *scalar linear code over* R) is 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 (also called a *k-dimensional vector linear code over* R) is 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.

0018-9448 © 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

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 $\epsilon > 0$, there exists a (k, n) solution over $\mathcal{A}$ for some k and n satisfying $k/n > 1 - \epsilon$,
- *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 linearly solvable over any module.

The *capacity*[1] 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 alphabet 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.

A. Previous Work

One decade ago, 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][2] 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 *et al.* [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 *et al.* [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.

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 *et al.* [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 *et al.* [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 network has a binary vector linear solution in some dimension. Feder *et al.* [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 *et al.* [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 *et al.* [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 *et al.* [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

[1] 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.

[2] The terminology was apparently attributed by F. Kschischang to M. Sudan.

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 $2, 3, \ldots, m-1$.

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.

B. 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], and [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 VI. The network $\mathcal{N}_4$ is parameterized by an arbitrary integer $m \geq 2$. Theorem VI.4 shows that $\mathcal{N}_4$ is solvable over an alphabet of size m. Theorem VI.5 shows, however, that $\mathcal{N}_4$ is never solvable over alphabets smaller than m. Theorem VI.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 VI.9 and VI.10. In particular, Theorem VI.9 shows that when m is composite, no linear solution for $\mathcal{N}_4$ exists over any module, and Corollary VI.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 VI.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 VI.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 II.4), $\mathcal{N}_1$ (in Lemma III.4), $\mathcal{N}_2$ (in Lemma IV.7), and $\mathcal{N}_3$ (in Lemma V.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 I summarizes the networks created and the results in this paper. Section I-C provides mathematical background and definitions. Sections II-V present the building block networks which are used to construct the main class of networks. Section VI 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 all but two of the lemmas in this paper. All other proofs are given in the main body of the paper.

TABLE I

SUMMARY OF THE NETWORKS CONSTRUCTED IN THIS PAPER, WHERE m, m_1, m_2, AND w ARE INTEGERS SUCH THAT $m, m_1, m_2 \geq 2$ AND $w \geq 1$

Network $\mathcal{N}_0(m)$	Section II
· Consists of a block $B(m)$ together with source nodes.	Figure 2
· $4m + 6$ nodes.	Remark II.1
· If a $(1, 1)$ code over $\mathcal{A}$ is a solution, then the code has an Abelian group structure.	Lemma II.2
Network $\mathcal{N}_1(m)$	Section III
· Consists of a block $B(m)$ together with source nodes and an additional receiver.	Figure 3
· $4m + 7$ nodes.	Remark III.1
· If solvable over $\mathcal{A}$, then $\gcd(\lvert\mathcal{A}\rvert, m) = 1$.	Lemma III.2
· Linearly solvable over standard R-module G iff $\gcd(\mathsf{char}(R), m) = 1$.	Lemma III.3
· Asymptotically linearly solvable over finite field $\mathbb{F}$ iff $\mathsf{char}(\mathbb{F}) \nmid m$.	Lemma III.4
Network $\mathcal{N}_2(m, w)$	Section IV
· Consists of w blocks $B(m + 1)$ together with source nodes and an additional receiver.	Figure 4
· $4mw + 9w + 2$ nodes.	Remark IV.1
· If $w \geq 2$, then non-linearly solvable over an alphabet of size mw.	Lemma IV.4
· If solvable over $\mathcal{A}$, then $\gcd(\lvert\mathcal{A}\rvert, m) \neq 1$.	Lemma IV.5
· Linearly solvable over standard R-module G iff $\mathsf{char}(R) \,\big|\, m$.	Lemma IV.6
· Asymptotically linearly solvable over finite field $\mathbb{F}$ iff $\mathsf{char}(\mathbb{F}) \,\big|\, m$.	Lemma IV.7
Network $\mathcal{N}_3(m_1, m_2)$	Section V
· Consists of blocks $B(m_1)$ and $B(m_2)$ together with source nodes and an additional receiver.	Figure 5
· $4m_1 + 4m_2 + 12$ nodes.	Remark V.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 V.7
· If solvable over $\mathcal{A}$, then $\gcd(\lvert\mathcal{A}\rvert, m_1) = 1$ or $\lvert\mathcal{A}\rvert \nmid m_2$.	Lemma V.5
· Linearly solvable over standard R-module G iff $\gcd(\mathsf{char}(R), m_1, m_2) = 1$.	Lemma V.6
· Asymptotically linearly solvable over finite field $\mathbb{F}$ iff $\mathsf{char}(\mathbb{F})$ is relatively prime to m_1 or m_2.	Lemma V.8
Network $\mathcal{N}_4(m)$	Section VI
· Consists of a disjoint union of various networks $\mathcal{N}_1, \mathcal{N}_2$, and $\mathcal{N}_3$.	Equation (7)
· Solvable over an alphabet of size m.	Theorem VI.4
· If $\lvert\mathcal{A}\rvert < m$, then not solvable over $\mathcal{A}$.	Theorem VI.5
· If m is not a prime power, then not solvable over any prime-power-size $\mathcal{A}$.	Corollary VI.6
· If m is prime, then scalar linearly solvable over $\mathrm{GF}(m)$.	Theorem VI.8
· If m is composite, then: (1) not linearly solvable over any module.	Theorem VI.9
(2) not asymptotically linearly solvable over any finite field.	Corollary VI.11
· Number of nodes is $O\left(m^{\frac{\log m}{\log\log m}}\right)$ and $\Omega(m)$.	Theorem VI.12

Section VII poses some open questions regarding the solvability and capacity of general networks.

C. Preliminaries

The following definitions and results regarding linear network codes over modules are from [7] and [12].

Definition I.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

$$\cdot : R \times G \to G$$

such that for all $r, s \in R$ and all $g, h \in G$ the following hold:

$$\begin{aligned} r \cdot (g \oplus h) &= (r \cdot g) \oplus (r \cdot h) \\ (r + s) \cdot g &= (r \cdot g) \oplus (s \cdot g) \\ (r * s) \cdot g &= r \cdot (s \cdot g). \end{aligned}$$

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 $\mathsf{char}(R)$ 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 use to discuss linear solvability in this paper.

Definition I.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. In particular, a field is a special case of a commutative ring, so a vector (or scalar) linear code over

field is, in fact, a special case of a linear code over a standard module.

Lemma I.3 was proved in a slightly different form in the proof of [7, Th. III.4].

Lemma I.3: If a network is not linearly solvable over any standard module, then it is not linearly solvable over any module.

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 I.4: Let $m \geq 2$. A $(1, 1)$ code for a network $\mathcal{N}$ over an alphabet $\mathcal{A}$, containing messages $x_0, x_1, \ldots, x_m$ and edge symbols $e_0, e_1, \ldots, e_m, e$, is said to have *Property* $P(m)$ if there exists a binary operation

$$\oplus: \ \mathcal{A} \times \mathcal{A} \to \mathcal{A}$$

and permutations $\pi_0, \pi_1, \ldots, \pi_m$ and $\sigma_0, \sigma_1, \ldots, \sigma_m$ of $\mathcal{A}$, such that $(\mathcal{A}, \oplus)$ is an Abelian group and the edge symbols can be written as

$$e_i = \sigma_i \left(\bigoplus_{\substack{j=0 \\ j \neq i}}^{m} \pi_j(x_j) \right) \quad (i = 0, 1, \ldots, m)$$

$$e = \bigoplus_{j=0}^{m} \pi_j(x_j).$$

II. Network $\mathcal{N}_0(m)$

For each $m \geq 2$, the network building block $B(m)$ is defined in Figure 1 and is used to build network $\mathcal{N}_0(m)$, which is defined in Figure 2. 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 symbol e_i. Similarly, we may assume each of the outgoing edges of the node v carries the symbol e. Lemma II.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 I.4. In particular, the solution alphabets have to be permutations of Abelian groups.

Remark II.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 II.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 II.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.

Lemma II.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

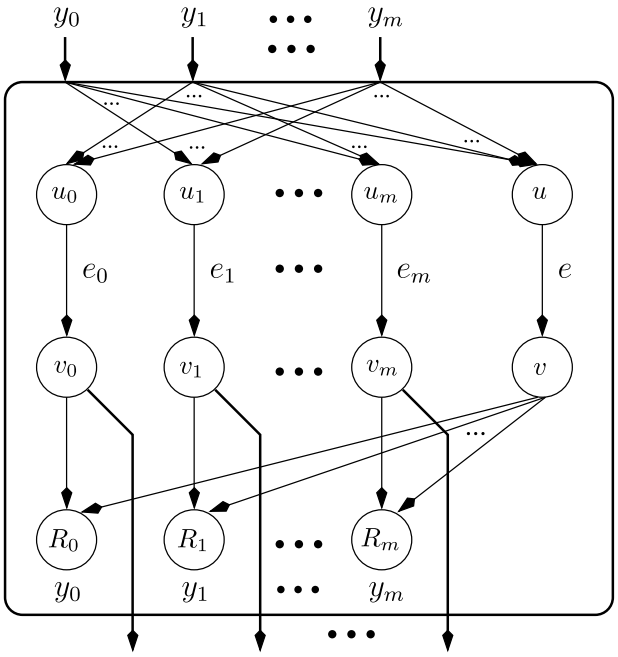

Fig. 1. The network building block $B(m)$ has message vector inputs $y_0, y_1, \ldots, y_m$ (from unspecified source nodes) and $m+1$ output edges. The node u receives each of the inputs and has a single outgoing edge to the node v, which carries the edge symbol e. For each i, the node u_i receives each 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 ith message vector y_i. The ith output edge of $B(m)$ is an outgoing edge of node v_i.

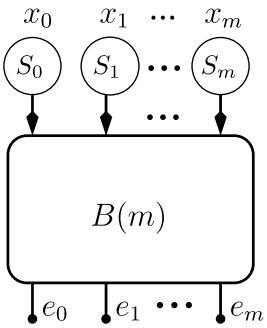

Fig. 2. The network $\mathcal{N}_0(m)$ consists of a block $B(m)$ together with source nodes $S_0, S_1, \ldots, S_m$, which generate message vectors $x_0, x_1, \ldots, x_m$, respectively. The output edges of $B(m)$ are unused.

symbols

$$e_i = \bigoplus_{\substack{j=0 \\ j \neq i}}^{m} (c_{i,j} \cdot x_j) \quad (i = 0, 1, \ldots, m)$$

$$e = \bigoplus_{j=0}^{m} (c_j \cdot x_j)$$

and decoding functions

$$R_i: \ x_i = (d_{i,e} \cdot e) \oplus (d_i \cdot e_i) \quad (i = 0, 1, \ldots, m)$$

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

$$c_{i,j} = -d_i^{-1} d_{i,e} c_j \qquad (i, j = 0, 1, \ldots, m \text{ and } j \neq i).$$

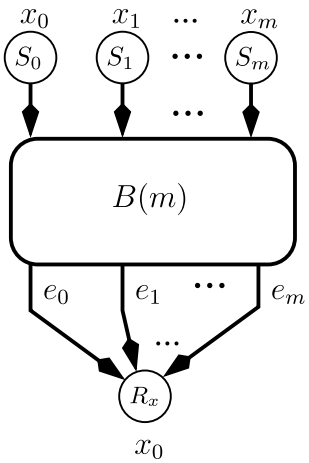

Fig. 3. The network $\mathcal{N}_1(m)$ is constructed from a $B(m)$ block together with source nodes $S_0, S_1, \ldots, S_m$ and an additional receiver R_x. For each i, the source node S_i generates the message vector x_i and is the ith input to $B(m)$. The additional receiver R_x receives all of the output edges of $B(m)$ and demands the message vector x_0.

Lemma II.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 III.4, IV.7, and V.8, respectively.

Lemma II.4: The network $\mathcal{N}_0(m)$ has capacity and linear capacity, for any finite-field alphabet, equal to 1.

III. Network $\mathcal{N}_1(m)$

For each $m \geq 2$, network $\mathcal{N}_1(m)$ is defined in Figure 3. The special case $m = 2$ corresponds to the non-Fano network from [10] and [11], with a relabeling of messages and nodes. Lemmas III.2, III.3, and III.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 $\mathsf{char}(R)$ is relatively prime to m,
3) asymptotically linearly solvable over finite field $\mathbb{F}$ if and only if $\mathsf{char}(\mathbb{F})$ does not divide m.

Remark III.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 $4m + 7$.

A. Solvability of $\mathcal{N}_1(m)$

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 III.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.

B. Linear Solvability of $\mathcal{N}_1(m)$

Lemma III.3 presents a necessary and sufficient condition for the linear solvability of $\mathcal{N}_1(m)$ over standard modules.

Lemma III.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 $\mathsf{char}(R)$ is relatively prime to m.

For example, for each $q \geq 2$ relatively prime to m, network $\mathcal{N}_1(m)$ has a scalar linear solution over the ring $\mathbf{Z}_q$, since $\mathbf{Z}_q$ is a standard $\mathbf{Z}_q$-module and $\mathsf{char}(\mathbf{Z}_q) = q$. It then follows from Lemma III.2 that network $\mathcal{N}_1(m)$ is solvable over $\mathcal{A}$ if and only if $|\mathcal{A}|$ is relatively prime to m.

C. Capacity and Linear Capacity of $\mathcal{N}_1(m)$

The following lemma characterizes the capacity and the linear capacity over finite-field alphabets of $\mathcal{N}_1(m)$.

Lemma III.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.

IV. 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 4. 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 IV.4, IV.5, IV.6, and IV.7 demonstrate that network $\mathcal{N}_2(m, w)$ is:

1) non-linearly solvable over an 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 $\mathsf{char}(R)$ divides m,
4) asymptotically linearly solvable over finite field $\mathbb{F}$ if and only if $\mathsf{char}(\mathbb{F})$ divides m.

Remark IV.1: For each $m \geq 2$ and $w \geq 1$, the network $\mathcal{N}_2(m, w)$ has:

$$\begin{aligned} &w(m+1)+1 \quad \text{source nodes,} \\ &w(2m+6) \quad \text{intermediate nodes,} \\ &w(m+2)+1 \quad \text{receiver nodes,} \end{aligned}$$

so the total number of nodes in $\mathcal{N}_2(m, w)$ is $4mw + 9w + 2$.

A. Solvability of $\mathcal{N}_2(m, w)$

For each positive integer m, we will view the ring $\mathbf{Z}_m$ as the set $\{0, 1, \ldots, m-1\}$ together with addition and multiplication modulo m. This ring will be used to construct non-linear solutions in Lemmas IV.2, IV.4, V.2, and V.4.

For each $m, w \geq 2$ and each $a \in \mathbf{Z}_{mw}$, a receiver cannot uniquely determine the symbol a in $\mathbf{Z}_{mw}$ from the symbol $wa \in \mathbf{Z}_{mw}$ since the integer w is not invertible in $\mathbf{Z}_{mw}$.

For example, if a receiver receives $wa = 0$ in $\mathbf{Z}_{mw}$, then the symbol a could be any element in the set

$$\{0, m, 2m, \ldots, (w-1)m\}.$$

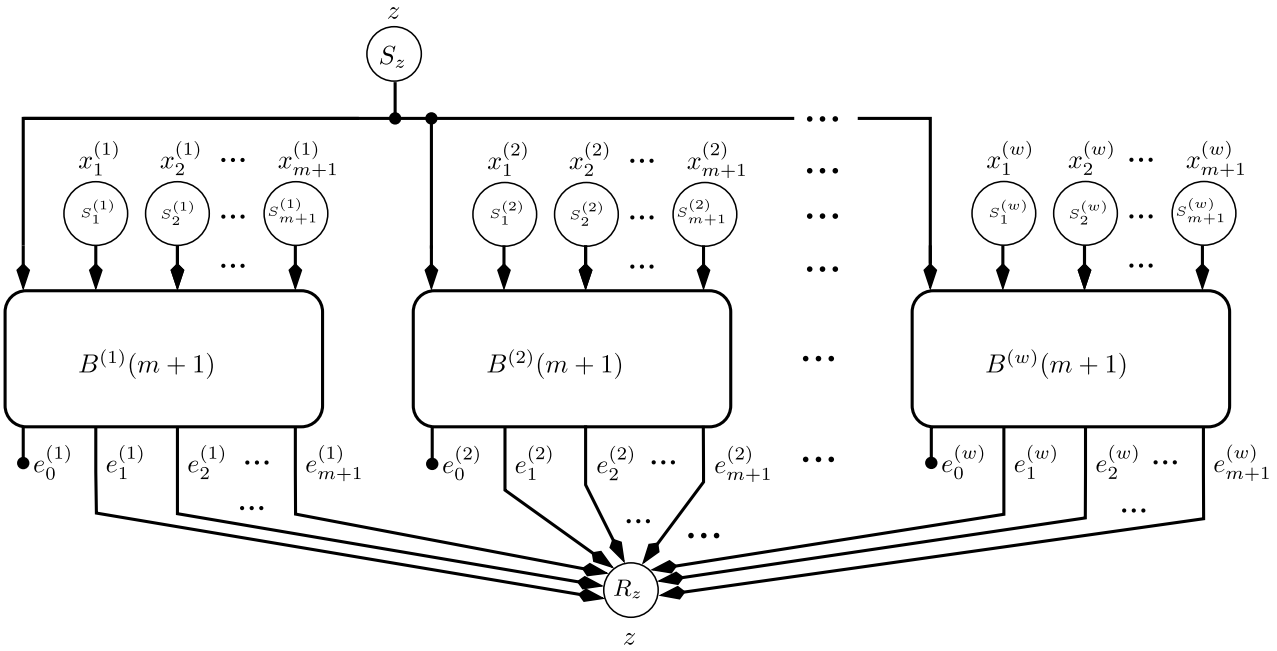

Fig. 4. The network $\mathcal{N}_2(m, w)$ is constructed from w blocks of $B(m+1)$ together with $w(m+1)+1$ source nodes and an additional receiver R_z. The lth block is denoted $B^{(l)}(m+1)$, and the nodes and edge symbols within $B^{(l)}(m+1)$ are denoted with a superscript l. For each $l = 1, 2, \ldots, w$, the block $B^{(l)}(m+1)$ has inputs from source nodes $S_1^{(l)}, S_2^{(l)}, \ldots, S_{m+1}^{(l)}$, which generate message vectors $x_1^{(l)}, x_2^{(l)}, \ldots, x_{m+1}^{(l)}$. 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.

The following lemma describes a technique for recovering the value of a via a decoding function ψ from the w-tuple

$$w\pi_1(a), w\pi_2(a), \ldots, w\pi_w(a),$$

where each π_i is a particular permutation of $\mathbf{Z}_{mw}$. This technique will then be used to show that network $\mathcal{N}_2(m, w)$ is solvable over an alphabet of size mw.

Lemma IV.2: For each $m \geq 2$ and $w \geq 1$, there exists a mapping $\psi : \mathbf{Z}_{mw}^w \to \mathbf{Z}_{mw}$ and permutations $\pi_1, \pi_2, \ldots, \pi_w$ of $\mathbf{Z}_{mw}$ such that for all $a \in \mathbf{Z}_{mw}$,

$$\psi\left(w\pi_1(a), w\pi_2(a), \ldots, w\pi_w(a)\right) = a.$$

Lemma IV.2 will be used in the proof of Lemma IV.4 to show that the receiver R_z can recover z from its inputs.

Example IV.3: The following table illustrates the permutations of $\mathbf{Z}_{12}$ described in Lemma IV.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 $a \in \mathbf{Z}_{12}$, the triple

$$(3\pi_3(a),\ 3\pi_2(a),\ 3\pi_1(a)) \in \mathbf{Z}_{12}^3$$

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 IV.4 describes a (possibly non-linear) solution for $\mathcal{N}_2(m, w)$ over the ring $\mathbf{Z}_{mw}$.

Lemma IV.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 ψ and $\pi_1, \pi_2, \ldots, \pi_w$ be the mapping and permutations, respectively, from Lemma IV.2. Define a $(1, 1)$ code for network $\mathcal{N}_2(m, w)$ over the ring $\mathbf{Z}_{mw}$ for each $l = 1, 2, \ldots, w$ by:

$$e_0^{(l)} = \sum_{j=1}^{m+1} x_j^{(l)}$$

$$e_i^{(l)} = \pi_l(z) + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} x_j^{(l)} \quad (i = 1, 2, \ldots, m+1)$$

$$e^{(l)} = \pi_l(z) + \sum_{j=1}^{m+1} x_j^{(l)}.$$

For each $l = 1, 2, \ldots, w$, the receivers within each $B^{(l)}(m+1)$ block can recover their respective demands as follows:

$$R_0^{(l)} : \pi_l^{-1}\left(e^{(l)} - e_0^{(l)}\right) = z$$

$$R_i^{(l)} : e^{(l)} - e_i^{(l)} = x_i^{(l)} \quad (i = 1, 2, \ldots, m+1).$$

For each $l = 1, 2, \ldots, w$, we have

$$w \sum_{i=1}^{m+1} e_i^{(l)} = w(m+1)\,\pi_l(z) + mw \sum_{j=1}^{m+1} x_j^{(l)}$$
$$= w\pi_l(z) \qquad [\text{from } mw = 0 \bmod mw]\,. \quad (2)$$

Receiver R_z can recover z from its inputs as follows:

$$R_z : \psi\left(w \sum_{i=1}^{m+1} e_i^{(1)},\ w \sum_{i=1}^{m+1} e_i^{(2)},\ \ldots,\ w \sum_{i=1}^{m+1} e_i^{(w)}\right)$$
$$= \psi\left(w\pi_1(z),\ w\pi_2(z),\ \ldots,\ w\pi_w(z)\right)$$
$$= z \qquad [\text{from (2) and Lemma IV.2}]\,.$$

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 IV.4, if $w = 1$, then π_1 and ψ are identity permutations, so the code is linear. However if $w > 1$, then $\pi_1, \pi_2, \ldots, \pi_{w-1}$ are generally non-linear, so the code is non-linear.

Lemma IV.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.

Lemmas IV.4 and IV.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.

B. Linear Solvability of $\mathcal{N}_2(m, w)$

Lemma IV.6 characterizes a necessary and sufficient condition for the linear solvability of network $\mathcal{N}_2(m, w)$ over standard modules.

Lemma IV.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 $\mathsf{char}(R)$ divides m.

By Lemma IV.4, for every $m, w \geq 2$, network $\mathcal{N}_2(m, w)$ is solvable over the ring $\mathbf{Z}_{mw}$, but $\mathsf{char}(\mathbf{Z}_{mw}) = mw \nmid m$ so by Lemma IV.6, the solution is necessarily non-linear.

C. Capacity and Linear Capacity of $\mathcal{N}_2(m, w)$

The following lemma provides a partial characterization of the linear capacity of $\mathcal{N}_2(m, w)$ over finite-field alphabets.

Lemma IV.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.

V. 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. 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 V.7 and Lemmas V.5, V.6, and V.8 demonstrate that network $\mathcal{N}_3(m_1, m_2)$ is:

1) non-linearly solvable over an alphabet of size $tm_1^{\alpha+1}$, if $m_2 = sm_1^{\alpha}$, 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 $\mathsf{gcd}(\mathsf{char}(R), m_1, m_2) = 1$,
4) asymptotically linearly solvable over finite field $\mathbb{F}$ if and only if $\mathsf{char}(\mathbb{F})$ is relatively prime to m_1 or m_2.

Remark V.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 $4m_1 + 4m_2 + 12$.

A. Solvability of $\mathcal{N}_3(m_1, m_2)$

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 $\mathbf{Z}_{m_1^{\alpha+1}}$. For every $a \in \mathbf{Z}_{m_1^{\alpha+1}}$, a receiver cannot uniquely determine a symbol a from the symbols $m_1 a$ and $sm_1^{\alpha} a$, since the integer m_1 is not invertible in $\mathbf{Z}_{m_1^{\alpha+1}}$. For example, if a receiver receives

$$m_1 a = sm_1^{\alpha} a = 0 \in \mathbf{Z}_{m_1^{\alpha+1}},$$

then the symbol a could be any element in the set

$$\{0, m_1^{\alpha}, 2m_1^{\alpha}, \ldots, (m_1 - 1)m_1^{\alpha}\}.$$

The following lemma describes a technique for recovering the value of a via a decoding function ψ from $m_1\pi_1(a)$ and $sm_1^{\alpha}\pi_2(a)$, where π_1 and π_2 are particular permutations of $\mathbf{Z}_{m_1^{\alpha+1}}$. This technique will be used to show that, in some cases, network $\mathcal{N}_3$ has non-linear solutions.

Lemma V.2: Let $m \geq 2$ and $\alpha, s \geq 1$ be integers such that s is relatively prime to m. Then there exist permutations π_1 and π_2 of $\mathbf{Z}_{m^{\alpha+1}}$ and a mapping $\psi : \mathbf{Z}_{m^{\alpha+1}}^2 \to \mathbf{Z}_{m^{\alpha+1}}$ such that for all $a \in \mathbf{Z}_{m^{\alpha+1}}$,

$$\psi\left(m\pi_1(a),\ sm^{\alpha}\pi_2(a)\right) = a.$$

Lemma V.2 will be used in the proof of Lemma V.4 to show that the receiver R_z can recover z from its inputs.

Example V.3: The table below illustrates the permutations of $\mathbf{Z}_8$ described in Lemma V.2 for the case $m = 2$, $s = 3$, and $\alpha = 2$.

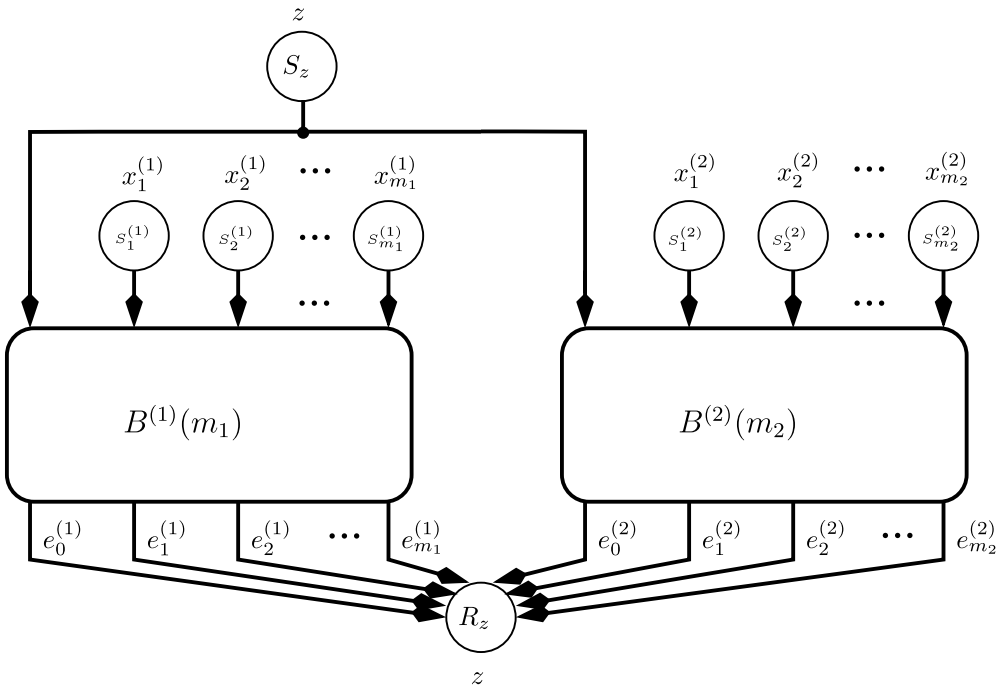

Fig. 5. The network $\mathcal{N}_3(m_1, m_2)$ is constructed from $B(m_1)$ and $B(m_2)$ blocks together with $m_1 + m_2 + 1$ source nodes and an additional receiver R_z. The blocks are denoted $B^{(1)}(m_1)$ and $B^{(2)}(m_2)$ respectively, and for each $l = 1, 2$, the nodes and edge symbols in $B^{(l)}(m_l)$ are denoted with a superscript l. Each $B^{(l)}(m_l)$ block has inputs from source nodes $S_1^{(l)}, S_2^{(l)}, \ldots, S_{m_l}^{(l)}$, which generate message vectors $x_1^{(l)}, x_2^{(l)}, \ldots, x_{m_l}^{(l)}$. 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.

$a = \pi_2(a)$	$\pi_1(a)$	$12\pi_2(a)$	$2\pi_1(a)$
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 $a \in \mathbf{Z}_8$, the pair $(2\pi_1(a), 12\pi_2(a)) \in \mathbf{Z}_8^2$ is distinct. Hence a can uniquely be determined from $2\pi_1(a)$ and $12\pi_2(a)$.

Lemma V.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 π_1, π_2 and ψ be the permutations and mapping, respectively, from Lemma V.2. Define a $(1, 1)$ code for the network $\mathcal{N}_3(m_1, m_2)$ over the ring $\mathbf{Z}_{m_1^{\alpha+1}}$, for each $l = 1, 2$, by:

$$
\begin{aligned}
e_0^{(l)} &= \sum_{j=1}^{m_l} x_j^{(l)} \\
e_i^{(l)} &= \pi_l(z) + \sum_{\substack{j=1 \\ j \neq i}}^{m_l} x_j^{(l)} \quad (i = 1, 2, \ldots, m_l) \\
e^{(l)} &= \pi_l(z) + \sum_{j=1}^{m_l} x_j^{(l)}.
\end{aligned}
$$

For each $l = 1, 2$, the receivers within the block $B^{(l)}(m_l)$ can recover their respective demands as follows:

$$
\begin{aligned}
R_0^{(l)} &: \pi_l^{-1}\left(e^{(l)} - e_0^{(l)}\right) = z \\
R_i^{(l)} &: e^{(l)} - e_i^{(l)} = x_i^{(l)} \quad (i = 1, 2, \ldots, m_l).
\end{aligned}
$$

For each $l = 1, 2$, we have

$$
\begin{aligned}
&-m_l e_0^{(l)} + \sum_{i=0}^{m_l} e_i^{(l)} \\
&\quad = -m_l \sum_{j=1}^{m_l} x_j^{(l)} + m_l \pi_l(z) + m_l \sum_{j=1}^{m_l} x_j^{(l)} \\
&\quad = m_l \pi_l(z). \qquad (3)
\end{aligned}
$$

The receiver R_z can recover z from its inputs as follows:

$$
\begin{aligned}
&\psi\left(-m_1 e_0^{(1)} + \sum_{i=0}^{m_1} e_i^{(1)},\ -m_2 e_0^{(2)} + \sum_{i=0}^{m_2} e_i^{(2)}\right) \\
&\quad = \psi\left(m_1\pi_1(z),\ m_2\pi_2(z)\right) && \text{[from (3)]} \\
&\quad = \psi\left(m_1\pi_1(z),\ sm_1^\alpha \pi_2(z)\right) && \left[\text{from } m_2 = sm_1^\alpha\right] \\
&\quad = z && \text{[from Lemma V.2]}.
\end{aligned}
$$

Thus the code described above is, in fact, a solution for the network $\mathcal{N}_3(m_1, m_2)$. ■

In the code given in the proof of Lemma V.4, the permutation π_1 is non-linear, so the code is non-linear.

Lemma V.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.

Lemmas V.4 and V.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.

B. Linear Solvability of $\mathcal{N}_3(m_1, m_2)$

Lemma V.6 characterizes a necessary and sufficient condition for the linear solvability of network $\mathcal{N}_3(m_1, m_2)$ over standard modules.

Lemma V.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 $\mathsf{gcd}(\mathsf{char}(R), m_1, m_2) = 1$.

Corollary V.7 uses Lemmas V.4 and V.6 to show that network $\mathcal{N}_3$ is solvable over additional alphabet sizes.

Corollary V.7: Let $m_1, m_2 \geq 2$ and $\alpha, s, t \geq 1$ be integers such that $m_2 = sm_1^\alpha$ 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 $tm_1^{\alpha+1}$.

Proof: By Lemma V.4, the network $\mathcal{N}_3(m_1, m_2)$ is solvable over an alphabet of size $m_1^{\alpha+1}$. $\mathbf{Z}_t$ is a standard $\mathbf{Z}_t$-module and $\mathsf{char}(\mathbf{Z}_t) = t$ is relatively prime to m_1, so by Lemma V.6, the network $\mathcal{N}_3(m_1, m_2)$ is scalar linearly solvable over the ring $\mathbf{Z}_t$. 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 $tm_1^{\alpha+1}$. ∎

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 V.4, network $\mathcal{N}_3(m_1, m_2)$ is solvable over the ring $\mathbf{Z}_{m_1^{\alpha+1}}$, but in this case we have

$$\begin{aligned}\mathsf{gcd}\left(m_1, m_2, \mathsf{char}\left(\mathbf{Z}_{m_1^{\alpha+1}}\right)\right) &= \mathsf{gcd}\left(m_1, m_1^\alpha s, m_1^{\alpha+1}\right)\\ &= m_1 \neq 1.\end{aligned}$$

So, by Lemma V.6, the solution is necessarily non-linear. This also implies that the Cartesian product code in Corollary V.7 is necessarily non-linear.

C. Capacity and Linear Capacity of $\mathcal{N}_3(m_1, m_2)$

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 V.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 alphabet 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 alphabet whose characteristic divides m_1 and m_2.

VI. 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 VI.1: The *disjoint union* of networks $\mathcal{N}_1, \ldots, \mathcal{N}_w$, has a (k, n) solution over the alphabet $\mathcal{A}$ if and only if each of $\mathcal{N}_1, \ldots, \mathcal{N}_w$ 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 $\gamma_1, \ldots, \gamma_{\omega(m)} \geq 1$ and $p_1, \ldots, p_{\omega(m)}$ are distinct primes. The following functions of m and its prime divisors will be used throughout this section. For each $i = 1, \ldots, \omega(m)$, let

$$f(m) = p_1^{\gamma_1 - 1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)} - 1} \tag{4}$$

$$\mu(m, i) = \min\left\{\alpha \geq 0 : \ p_i^\alpha \geq f(m)\right\} \tag{5}$$

$$g(m, i) = p_i^{\gamma_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega(m)} p_j^{\mu(m,j)}. \tag{6}$$

We construct network $\mathcal{N}_4(m)$ from the following *disjoint union* [3] of networks:

$$\begin{aligned}\mathcal{N}_4(m) = &\left(\bigcup_{\substack{\text{prime } q \\ q \nmid m \\ q < f(m)}} \mathcal{N}_1(q)\right) \cup \left(\bigcup_{i=1}^{\omega(m)} \mathcal{N}_2\left(p_i^{\gamma_i}, \ (m/p_i^{\gamma_i})\right)\right)\\ &\cup \left(\bigcup_{\substack{i=1 \\ \gamma_i > 1}}^{\omega(m)} \mathcal{N}_3\left(p_i, \ g(m, i)\right)\right).\end{aligned} \tag{7}$$

Theorem VI.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 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 VI.4, VI.5, VI.8, VI.9, and Corollaries VI.6 and VI.11. ∎

Example VI.3: Consider the special cases of the square-free integer [4] 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

$$f(6) = 2^{(1-1)} 3^{(1-1)} = 1,$$

[3] 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.

[4] An integer is *square-free* if it is not divisible by the square of any prime.

so $\mathcal{N}_4(6)$ has neither $\mathcal{N}_1$ nor $\mathcal{N}_3$ components. Thus by (7), 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

$$f(27) = 3^{(3-1)} = 9 \quad \text{and} \quad g(27,1) = 3^{(3-1)} = 9,$$

and the primes less than $f(27)$ which do not divide 27 are 2, 5, and 7. Thus by (7), network $\mathcal{N}_4(6)$ is the disjoint union of networks:

$$\mathcal{N}_1(2) \cup \mathcal{N}_1(5) \cup \mathcal{N}_1(7) \cup \mathcal{N}_2(27,1) \cup \mathcal{N}_3(3,9).$$

- $m = 100 = 2^2 5^2$. 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

$$g(100,1) = 2^1 5^2 \quad \text{and} \quad g(100,2) = 5^1 2^4,$$

and the primes less than $f(100)$ which do not divide 100 are 3 and 7. Thus by (7), 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 VI.3 as running examples throughout this section and will refer back to these constructions.

A. 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 VI.4 and VI.5 make use of the functions f, μ, and g defined in (4), (5), and (6), respectively.

Theorem VI.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 (7), network $\mathcal{N}_4(m)$ contains a copy of $\mathcal{N}_1(q)$. $\mathbf{Z}_m$ is a standard $\mathbf{Z}_m$-module and $\mathsf{char}(\mathbf{Z}_m) = m$ is relatively prime to q, so by Lemma III.3, network $\mathcal{N}_1(q)$ is scalar linearly solvable over the ring $\mathbf{Z}_m$.

For each $i = 1, \ldots, \omega(m)$, by (7), network $\mathcal{N}_4(m)$ contains a copy of $\mathcal{N}_2\left(p_i^{\gamma_i}, (m/p_i^{\gamma_i})\right)$. By Lemma IV.4, network $\mathcal{N}_2\left(p_i^{\gamma_i}, (m/p_i^{\gamma_i})\right)$ is solvable over an alphabet of size m.

For each $i = 1, \ldots, \omega(m)$ such that $\gamma_i > 1$, by (7), 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 (6), $g(m,i)$ is the product of $p_i^{\gamma_i - 1}$ and a term which is relatively prime to p_i, so by Corollary V.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 VI.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 $i = 1, \ldots, \omega(m)$, by (7), network $\mathcal{N}_4(m)$ contains a copy of $\mathcal{N}_2\left(p_i^{\gamma_i}, (m/p_i^{\gamma_i})\right)$. Network $\mathcal{N}_2\left(p_i^{\gamma_i}, (m/p_i^{\gamma_i})\right)$ is solvable over $\mathcal{A}$, so by Lemma IV.5, p_i is not relatively prime to $|\mathcal{A}|$. Since p_i is prime, we have $p_i \,|\, |\mathcal{A}|$, and thus each of $p_1, \ldots, p_{\omega(m)}$ 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

$$\begin{aligned} |\mathcal{A}| &= \delta\, p_1 \cdots p_{\omega(m)} \\ &\geq f(m)\, p_1 \cdots p_{\omega(m)} \\ &= p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}} = m \quad \text{[from (4)]}, \end{aligned}$$

which again contradicts the assumption that $|\mathcal{A}| < m$, so we assume $\delta < f(m)$.

Consider the prime factorization of δ. Let $\{q_1, \ldots, q_\rho\}$ 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 $\{p_1, \ldots, p_{\omega(m)}\}$ or it does not divide m and is in the set $\{q_1, \ldots, q_\rho\}$. Thus δ must be a product of $q_1, \ldots, q_\rho$ and $p_1, \ldots, p_{\omega(m)}$ terms, so there exist $\alpha_1, \ldots, \alpha_{\omega(m)} \geq 1$ and $\beta_1, \ldots, \beta_\rho \geq 0$ such that we can write $|\mathcal{A}|$ as

$$|\mathcal{A}| = p_1^{\alpha_1} \ldots p_{\omega(m)}^{\alpha_{\omega(m)}}\, q_1^{\beta_1} \ldots q_\rho^{\beta_\rho}. \tag{8}$$

For each prime $q < f(m)$ such that $q \nmid m$, by (7), 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 III.2, we have $\mathsf{gcd}(q, |\mathcal{A}|) = 1$. Thus in (8) we have $\beta_1 = \cdots = \beta_\rho = 0$.

For each $i = 1, \ldots, \omega(m)$ such that $\gamma_i > 1$, by (7), 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 V.5, $|\mathcal{A}|$ does not divide $g(m,i)$. Expressing $|\mathcal{A}|$ and $g(m,i)$ as their prime factorizations yields:

$$p_1^{\alpha_1} \ldots p_{\omega(m)}^{\alpha_{\omega(m)}} \;\nmid\; p_i^{\gamma_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{\omega(m)} p_j^{\mu(m,j)} \quad \text{[from (6), (8)]}.$$

This implies that for each $i \in \{1, \ldots, \omega(m)\}$ 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 $j \in \{1, \ldots, \omega(m)\}$ such that

$$\alpha_j \geq \mu(m, j) + 1,$$

then we have

$$\begin{aligned} |\mathcal{A}| &= p_1^{\alpha_1} \cdots p_{\omega(m)}^{\alpha_{\omega(m)}} \quad \text{[from (8)]} \\ &\geq p_j^{\alpha_j - 1} \left(p_1 \cdots p_{\omega(m)}\right) \quad \text{[from } \alpha_l \geq 1\text{]} \\ &\geq p_j^{\mu(m,j)} \left(p_1 \cdots p_{\omega(m)}\right) \\ &\geq f(m) \left(p_1 \cdots p_{\omega(m)}\right) = m \quad \text{[from (4), (5)]}, \end{aligned}$$

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

$$\begin{aligned} |\mathcal{A}| &= p_1^{\alpha_1} \cdots p_{\omega(m)}^{\alpha_{\omega(m)}} \quad \text{[from (8)]} \\ &\geq p_1^{\gamma_1} \cdots p_{\omega(m)}^{\gamma_{\omega(m)}} = m, \end{aligned}$$

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 VI.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 VI.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 VI.5 that each of $p_1, \ldots, p_{\omega(m)}$ 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 VI.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 $2 \,|\, |\mathcal{A}|$. Similarly for $\mathcal{N}_2(3, 2)$, we have that $3 \,|\, |\mathcal{A}|$. 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 $3 \,|\, |\mathcal{A}|$, 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 $10 \,|\, |\mathcal{A}|$, 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.

B. 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 VI.8: For each prime p, the network $\mathcal{N}_4(p)$ is scalar linearly solvable over GF(p).

Proof: If p is a prime number, then $f(p) = 1$ and the power of p is one, so by (7), network $\mathcal{N}_4(p)$ consists solely of a copy of network $\mathcal{N}_2(p, 1)$. By Lemma IV.6, network $\mathcal{N}_2(p, 1)$ has a scalar linear solution over every finite-field alphabet with characteristic p. ∎

Theorem VI.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 (7), network $\mathcal{N}_4(p^\gamma)$ contains copies of $\mathcal{N}_2(p^\gamma, 1)$ and $\mathcal{N}_3\left(p,\ p^{\gamma-1}\right)$. Since network $\mathcal{N}_2(p^\gamma, 1)$ is linearly solvable over G, by Lemma IV.6, the characteristic of R divides p^γ. Since network $\mathcal{N}_3\left(p,\ p^{\gamma-1}\right)$ is linearly solvable over G, by Lemma V.6, the characteristic of R is relatively prime to p. If the characteristic of R both divides p^γ 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 (7), network $\mathcal{N}_4(m)$ contains copies of networks $\mathcal{N}_2\left(p_1^{\gamma_1},\ (m/p_1^{\gamma_1})\right)$ and $\mathcal{N}_2\left(p_2^{\gamma_2},\ (m/p_2^{\gamma_2})\right)$. Both of these networks are linearly solvable over G, so by Lemma IV.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 I.3 implies there are no linear solutions for $\mathcal{N}_4(m)$ over any module. ∎

C. Capacity and Linear Capacity of $\mathcal{N}_4(m)$

Theorem VI.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 VI.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 (7), network $\mathcal{N}_4(p^\gamma)$ contains copies of $\mathcal{N}_2(p^\gamma, 1)$ and $\mathcal{N}_3\left(p,\ p^{\gamma-1}\right)$. By Lemma IV.7, network $\mathcal{N}_2(p^\gamma, 1)$ has linear capacity upper bounded by

$$1 - \frac{1}{2p^\gamma + 3}$$

for finite-field alphabets with characteristic other than p. By Lemma V.8, network $\mathcal{N}_3\left(p,\ p^{\gamma-1}\right)$ 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 γ.

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 (7), the network $\mathcal{N}_4(m)$ contains copies of network $\mathcal{N}_2\left(p_1^{\gamma_1},\ (m/p_1^{\gamma_1})\right)$ and network $\mathcal{N}_2\left(p_2^{\gamma_2},\ (m/p_2^{\gamma_2})\right)$. By Lemma IV.7, network $\mathcal{N}_2\left(p_i^{\gamma_i},\ (m/p_i^{\gamma_i})\right)$ 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 alphabet is left as an open problem.

Corollary VI.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 VI.10, the linear capacity of $\mathcal{N}_4(m)$ is bounded away from one over all finite-field alphabets. ∎

D. 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 (4), (5), (6).

Theorem VI.12: For each $m \geq 2$, the number of nodes in network $\mathcal{N}_4(m)$ is asymptotically

(a) Ω(m),
(b) $O(m)$, when mis 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 text nor a prime-power.

Proof: By Remark III.1, the number of nodes in $\mathcal{N}_1(q)$ is

$$4q + 7.$$

By Remark IV.1, the number of nodes in $\mathcal{N}_2(m, w)$ is

$$4mw + 9w + 2.$$

By Remark V.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 (7), the total number of nodes in $\mathcal{N}_4(m)$ is:

$$\left(\sum_{\substack{\text{prime q} \\ q \nmid m \\ q < f(m)}} (4q + 7)\right) + \left(\sum_{i=1}^{\omega(m)} (4m + 9(m/p_i^{\gamma_i}) + 2)\right) + \left(\sum_{\substack{i=1 \\ \gamma_i > 1}}^{\omega(m)} (4g(m, i) + 4p_i + 12)\right) \tag{9}$$

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 $\mathcal{N}_4(m)$.

It is known [27, p. 257] that

$$\sum_{\substack{\text{prime } q \\ q \leq m}} q = O\left(\frac{m^2}{\log m}\right). \tag{10}$$

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

$$\sum_{\substack{\text{prime q} \\ q \nmid m \\ q < f(m)}} (4q + 7) \geq 0 \tag{11}$$

and

$$\sum_{\substack{\text{prime q}\\ q\nmid m\\ q<f(m)}} (4q+7) < \sum_{\substack{\text{prime } q\\ q\le m}} (4q+7) \tag{12}$$

$$= O\left(\frac{m^2}{\log m}\right) \quad \text{[from (10)]}. \tag{13}$$

The total number of nodes in $\mathcal{N}_4(m)$ from $\mathcal{N}_2$ networks is

$$\sum_{i=1}^{\omega(m)} (4m + 9(m/p_i^{\gamma_i}) + 2) > \sum_{i=1}^{\omega(m)} 4m$$
$$= \Omega(\omega(m)\, m) \tag{14}$$

and

$$\sum_{i=1}^{\omega(m)} (4m + 9(m/p_i^{\gamma_i}) + 2) < \sum_{i=1}^{\omega(m)} (13m+2)$$
$$= O(\omega(m)\, m). \tag{15}$$

For each $i = 1, \ldots, \omega(m)$ we have

$$p_i^{\mu(m,i)} < p_i\, f(m) \quad \text{[from (5)]} \tag{16}$$

$$g(m,i) = p_i^{\gamma_i - 1} \prod_{\substack{j=1\\ j\neq i}}^{\omega(m)} p_j^{\mu(m,j)} \quad \text{[from (6)]}$$
$$< p_i^{\gamma_i - 1} \prod_{\substack{j=1\\ j\neq i}}^{\omega(m)} p_j\, f(m) \quad \text{[from (16)]}$$
$$< p_i^{\gamma_i}\, f(m)^{\omega(m)-1} \prod_{j=1}^{\omega(m)} p_j$$
$$= p_i^{\gamma_i}\, f(m)^{\omega(m)-2}\, m \quad \text{[from (4)]}. \tag{17}$$

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

$$\sum_{\substack{i=1\\ \gamma_i>1}}^{\omega(m)} (4g(m,i) + 4p_i + 12) \ge 0. \tag{18}$$

and

$$\sum_{\substack{i=1\\ \gamma_i>1}}^{\omega(m)} (4g(m,i) + 4p_i + 12)$$
$$\le \sum_{i=1}^{\omega(m)} 20 g(m,i) \quad \text{[from (6)]}$$
$$< 20m\, f(m)^{\omega(m)-2} \sum_{i=1}^{\omega(m)} p_i^{\gamma_i} \quad \text{[from (17)]}$$
$$< 20m\, f(m)^{\omega(m)-2} \prod_{i=1}^{\omega(m)} p_i^{\gamma_i} \quad \text{[from } ab \ge a+b,\ \forall a,b \ge 2\text{]}$$
$$= 20m^2\, f(m)^{\omega(m)-2}$$
$$< 20m^{\omega(m)} = O\left(m^{\omega(m)}\right) \quad \text{[from (4)]}. \tag{19}$$

To prove part (a), consider the lower bounds of each term of (9). By equations (9), (11), (14), and (18), 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, Th. 11] that

$$\omega(m) = O\left(\frac{\log m}{\log\log m}\right). \tag{20}$$

To prove parts (b)-(e), we will consider the upper bounds on the number of nodes of each term of (9). 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 (9) and (15), 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 (20), yields the desired bound.

To prove part (d), consider a prime power $m = p^\gamma$, where $\gamma \ge 2$. We have $\omega(p^\gamma) = 1$, so by (15), the number of nodes from $\mathcal{N}_2$ components is $O(m)$, and, by (19), the number of nodes from $\mathcal{N}_3$ components is $O(m)$. By (13), 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 $\omega(m) \ge 2$) nor square-free (so there are $\mathcal{N}_3$ components in $\mathcal{N}_4(m)$). By equations (9), (13), (15), and (19), The number of nodes in $\mathcal{N}_4(m)$ is

$$O\left(\frac{m^2}{\log m}\right) + O(\omega(m)\, m) + O\left(m^{\omega(m)}\right)$$
$$= O\left(m^{\omega(m)}\right) \qquad \text{[from } \omega(m) \ge 2\text{]},$$

which, along with (20), yields the desired bound. ■

Example VI.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 $\mathcal{N}_2(2,3)$ 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 $\mathcal{N}_2(27,1)$,
  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 $\mathcal{N}_3(2,50)$, 352 from $\mathcal{N}_3(5,80)$.

VII. 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 [24], [34], 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 $S \subseteq \mathbf{N}$ 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?

Appendix

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 A.1 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 III.3 and V.6 to more easily characterize the classes of modules over which $\mathcal{N}_1$ and $\mathcal{N}_3$ are linearly solvable.

Lemma A.1: 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 $\mathsf{char}(R)$ and m are relatively prime.

The following definition and lemmas will be used in the proofs of Lemmas III.4, IV.7, and V.8.

Definition A.2: Let $\mathbb{F}$ be a finite field and suppose

$$a_1 \in \mathbb{F}^{s_1}, \ldots, a_q \in \mathbb{F}^{s_q} \quad \text{and} \quad b_1 \in \mathbb{F}^{t_1}, \ldots, b_r \in \mathbb{F}^{t_r}$$

are functions of variables $x_1, \ldots, x_w$. We write

$$a_1, \ldots, a_q \longrightarrow b_1, \ldots, b_r$$

to mean that there exist $t_j \times s_i$ matrices $M_{j,i}$ over $\mathbb{F}$ such that for all choices of the variables $x_1, \ldots, x_w$,

$$b_j = \sum_{i=1}^{q} M_{j,i}\, a_i \quad (j = 1, \ldots, r).$$

I.e. each of $b_1, \ldots, b_r$ can be written as a linear combination of $a_1, \ldots, a_q$. In the context of network coding, the variables $x_1, \ldots, x_w$ will always be taken as the network messages. Lemma A.3 is known from linear algebra [28, p. 124] and will be used in later proofs. In particular, Lemmas A.3, A.4, and A.5 will be used in bounding the linear capacities of $\mathcal{N}_1, \mathcal{N}_2$, and $\mathcal{N}_3$.

Lemma A.3: Let $\mathbb{F}$ be a finite field. If $A : \mathbb{F}^m \to \mathbb{F}^n$ and $B : \mathbb{F}^k \to \mathbb{F}^m$ are linear maps, then

$$\begin{aligned} &\mathsf{rank}\,(A) + \mathsf{rank}\,(B) - m \\ &\quad \leq \mathsf{rank}\,(A\,B) \qquad (21) \\ &\quad \leq \min(\mathsf{rank}\,(A), \mathsf{rank}\,(B)). \qquad (22) \end{aligned}$$

The following two lemmas were proved in slightly different form in [7, Lemma IV.2, Th. IV.4].

Lemma A.4: 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

$$B\,A = \begin{bmatrix} I_k \\ 0 \end{bmatrix}.$$

In what follows, the transitive relation $\longrightarrow$ will be used to describe linear coding functions at network nodes.

Lemma A.5: 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 $x \in \mathbb{F}^n$

$$Ax,\ Qx \longrightarrow x.$$

A. Proofs of Lemmas in Section II

Proof of Lemma II.3: Equating message components at the receiver R_i yields

$$\begin{aligned} 1_R &= d_{i,e}\, c_i \quad (i = 0, 1, \ldots, m) \\ 0_R &= d_{i,e}\, c_j + d_i\, c_{i,j} \quad (i, j = 0, 1, \ldots, m \text{ and } j \neq i) \end{aligned}$$

which implies the following elements of R are invertible:

$$\begin{aligned} &d_{i,e} \text{ and } c_i \quad (i = 0, 1, \ldots, m) \\ &d_i \text{ and } c_{i,j} \quad (i, j = 0, 1, \ldots, m \text{ and } j \neq i). \end{aligned}$$

The result then follows by solving for $c_{i,j}$. ∎

Proof of Lemma II.4: Let G be a standard R-module. The network $\mathcal{N}_0(m)$ has the following linear solution over G:

$$\begin{aligned} e_i &= \bigoplus_{\substack{j=0 \\ j \neq i}}^{m} x_j \quad (i = 0, 1, \ldots, m) \\ e &= \bigoplus_{j=0}^{m} x_j \end{aligned}$$

and decoding at each receiver as follows:

$$R_i: \quad e \ominus e_i = x_i \quad (i = 0, 1, \ldots, m).$$

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. ∎

B. Proofs of Lemmas in Section III

Proof of Lemma III.2: 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 II.2, the edge functions within $B(m)$ must satisfy Property $P(m)$. Thus, there exists an Abelian group $(\mathcal{A}, \oplus)$ and permutations $\pi_0, \pi_1, \ldots, \pi_m$ and $\sigma_0, \sigma_1, \ldots, \sigma_m$ of $\mathcal{A}$, such that the edges carry the symbols:

$$e_i = \sigma_i \left(\bigoplus_{\substack{j=0 \\ j \neq i}}^{m} \pi_j(x_j) \right) \quad (i = 0, 1, \ldots, m) \tag{23}$$

$$e = \bigoplus_{j=0}^{m} \pi_j(x_j).$$

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 $p \,|\, m$, we have

$$\underbrace{a \oplus \cdots \oplus a}_{m \text{ adds}} = 0.$$

Define two collections of messages as follows:

$$x_j = \pi_j^{-1}(0) \text{ and } \hat{x}_j = \pi_j^{-1}(a),$$

where $j = 0, 1, \ldots, m$. Since $a \neq 0$ and each π_j is bijective, it follows that $x_j \neq \hat{x}_j$ for all j.

By Property $P(m)$, for each $i = 0, 1, \ldots, m$, we have

$$e_i = \sigma_i \left(\underbrace{0 \oplus \cdots \oplus 0}_{m \text{ adds}} \right) = \sigma_i(0) \quad \text{[from (23)]}$$

for the messages $x_0, x_1 \ldots, x_m$, and

$$e_i = \sigma_i \left(\underbrace{a \oplus \cdots \oplus a}_{m \text{ adds}} \right) = \sigma_i(0) \quad \text{[from (23)]}$$

for the messages $\hat{x}_0, \hat{x}_1 \ldots, \hat{x}_m$. For both collections of messages, the edge symbols $e_0, e_1, \ldots, e_m$ are the same, and therefore the decoded value x_0 at R_x must be the same. However, this contradicts the fact that $x_0 \neq \hat{x}_0$. ∎

Proof of Lemma III.3: By Lemma A.1, m is invertible in R if and only if $\mathsf{char}(R)$ 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:

$$e_i = \bigoplus_{\substack{j=0 \\ j \neq i}}^{m} (c_{i,j} \cdot x_j) \quad (i = 0, 1, \ldots, m) \tag{24}$$

$$e = \bigoplus_{j=0}^{m} (c_j \cdot x_j) \tag{25}$$

and there exist $d_{i,e}, d_i, d_{x,i} \in R$, such that each receiver can linearly recover its demands from its inputs by:

$$R_i: \; x_i = (d_{i,e} \cdot e) \oplus (d_i \cdot e_i) \quad (i = 0, 1, \ldots, m) \tag{26}$$

$$R_x: \; x_0 = \bigoplus_{i=0}^{m} (d_{x,i} \cdot e_i). \tag{27}$$

Since $\mathcal{N}_1(m)$ contains $\mathcal{N}_0(m)$, by Lemma II.3 and (24)–(26), each c_i and each d_i is invertible in R, and

$$c_{i,j} = -d_i^{-1} d_{i,e} c_j \quad (i, j = 0, 1, \ldots, m \text{ and } j \neq i). \tag{28}$$

Equating message components at R_x yields:

$$\begin{aligned} 1_R &= \sum_{i=1}^{m} d_{x,i} c_{i,0} \quad \text{[from (24), (27)]} \\ &= -\sum_{i=1}^{m} d_{x,i} d_i^{-1} d_{i,e} c_0 \quad \text{[from (28)]} \end{aligned} \tag{29}$$

and for each $j = 1, 2, \ldots, m$,

$$\begin{aligned} 0_R &= \sum_{\substack{i=0 \\ i \neq j}}^{m} d_{x,i} c_{i,j} \quad \text{[from (24), (27)]} \\ &= -\left(\sum_{\substack{i=0 \\ i \neq j}}^{m} d_{x,i} d_i^{-1} d_{i,e} \right) c_j \quad \text{[from (28)]}. \end{aligned} \tag{30}$$

For each $j = 1, 2, \ldots, m$, right multiplying (30) by $c_j^{-1} c_0$ yields

$$0_R = \sum_{\substack{i=0 \\ i \neq j}}^{m} d_{x,i} d_i^{-1} d_{i,e} c_0. \quad \text{[from (30)]}. \tag{31}$$

By summing (31) over $j = 1, 2, \ldots, m$ and subtracting (29), we get

$$\begin{aligned} -1_R &= \sum_{j=0} \sum_{\substack{i=0 \\ i \neq j}}^{m} d_{x,i} d_i^{-1} d_{i,e} c_0 \quad \text{[from (29), (31)]} \\ &= m \sum_{i=0}^{m} d_{x,i} d_i^{-1} d_{i,e} c_0. \end{aligned}$$

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:

$$e_i = \bigoplus_{\substack{j=0\\ j\neq i}}^{m} x_j \quad (i = 0, 1, \ldots, m)$$
$$e = \bigoplus_{j=0}^{m} x_j.$$

Receiver R_i can linearly recover x_i from its received edge symbols e and e_i by:

$$R_i: \; e \ominus e_i = x_i \quad (i = 0, 1, \ldots, m)$$

and receiver R_x can linearly recover x_0 from its received edge symbols $e_0, e_1, \ldots, e_m$ 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 $\mathcal{N}_1(m)$. ∎

Proof of Lemma III.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 III.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 II.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 $\mathsf{char}(\mathbb{F}) \,|\, m$, 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:

$$e_i = \sum_{\substack{j=0\\ j\neq i}}^{m} M_{i,j}\, x_j \quad (i = 0, 1, \ldots, m) \tag{32}$$
$$e = \sum_{j=0}^{m} M_j\, x_j \tag{33}$$

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:

$$R_i: \quad x_i = D_{i,e}\, e + D_i\, e_i \quad (i = 0, 1, \ldots, m). \tag{34}$$

Since receiver R_x linearly recovers x_0 from $e_0, e_1, \ldots, e_m$, we can write

$$e_0, e_1, \ldots, e_m \;\longrightarrow\; x_0. \tag{35}$$

We also have

$$x_0, \; \sum_{j=1}^{m} M_j\, x_j \longrightarrow e \quad [\text{from (33)}]. \tag{36}$$

For each $i = 0, 1 \ldots, m$, if we set $x_i = 0$ in (34), then we get the following relationship among the remaining m message vectors (since e_i does not depend on x_i):

$$0 = D_{i,e} \sum_{\substack{j=0\\ j\neq i}}^{m} M_j\, x_j + D_i\, e_i \quad [\text{from (32), (33), (34)}], \tag{37}$$

and thus, for each $i = 1, 2, \ldots, m$,

$$e_i \longrightarrow D_{i,e} \sum_{\substack{j=0\\ j\neq i}}^{m} M_j\, x_j \quad [\text{from (37)}] \tag{38}$$
$$\sum_{j=1}^{m} M_j\, x_j \longrightarrow D_0\, e_0 \quad [\text{from (37)}]. \tag{39}$$

For each $i = 1, 2, \ldots, m$, let $Q_{i,e}$ be the matrix Q in Lemma A.5 corresponding to when $D_{i,e}$ is the matrix A in Lemma A.5. Similarly, let Q_0 be the matrix Q in Lemma A.5 corresponding to taking A to be D_0.

Let L be the following list of $2m + 1$ vector functions of $x_0, x_1, \ldots, x_m$:

$$Q_0\, e_0,$$
$$e_i, \quad (i = 1, 2, \ldots, m)$$
$$Q_{i,e} \sum_{\substack{j=0\\ j\neq i}}^{m} M_j\, x_j \quad (i = 1, 2, \ldots, m).$$

For each $i = 1, 2, \ldots, m$, we have

$$L \longrightarrow D_{i,e} \sum_{\substack{j=0\\ j\neq i}}^{m} M_j\, x_j \quad [\text{from (38)}] \tag{40}$$
$$L \longrightarrow \sum_{\substack{j=0\\ j\neq i}}^{m} M_j\, x_j \quad [\text{from Lemma A.5, (40)}], \tag{41}$$

and

$$\left\{\sum_{\substack{j=0\\ j\neq i}}^{m} M_j\, x_j : \; i = 1, 2, \ldots, m\right\}$$
$$\longrightarrow \sum_{i=1}^{m} \sum_{\substack{j=0\\ j\neq i}}^{m} M_j\, x_j$$
$$= m\, M_0\, x_0 + (m-1) \sum_{j=1}^{m} M_j\, x_j$$
$$= -\sum_{j=1}^{m} M_j\, x_j \qquad \left[\text{from } \mathsf{char}(\mathbb{F}) \,|\, m\right]. \tag{42}$$

Thus we have

$$L \longrightarrow \sum_{j=1}^{m} M_j\, x_j \quad [\text{from (41), (42)}] \tag{43}$$
$$L \longrightarrow D_0\, e_0 \quad [\text{from (39), (43)}] \tag{44}$$
$$L \longrightarrow e_0 \quad [\text{from Lemma A.5, (44)}] \tag{45}$$
$$L \longrightarrow x_0 \quad [\text{from (35), (45)}] \tag{46}$$
$$L \longrightarrow e \quad [\text{from (36), (43), (46)}] \tag{47}$$

and for each $i = 1, 2, \ldots, m$,

$$L \longrightarrow x_i \quad \text{[from (34), (47)]}. \tag{48}$$

We will now bound the number of independent entries in the list L. By equating message components in equation (34), for each $i = 0, 1, \ldots, m$, we have:

$$I_k = D_{i,e}\, M_i \quad \text{[from (32), (33), (34)]}. \tag{49}$$

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

$$\begin{aligned} &\min\big(\mathsf{rank}\left(D_{i,e}\right), \mathsf{rank}\left(M_i\right)\big) \\ &\quad \geq \mathsf{rank}\left(D_{i,e}\, M_i\right) \quad \text{[from (22)]} \\ &\quad = \mathsf{rank}\left(I_k\right) = k \quad \text{[from (49)]}, \end{aligned}$$

and so $\mathsf{rank}\left(D_{i,e}\right) = \mathsf{rank}\left(M_i\right) = k$, which, by Lemma A.5, implies

$$\mathsf{rank}\left(Q_{i,e}\right) = n - k \quad (i = 1, 2, \ldots, m). \tag{50}$$

Since $\mathsf{rank}\left(M_0\right) = k$, by Lemma A.4, there exists an $n \times n$ nonsingular matrix W over $\mathbb{F}$ such that

$$W M_0 = \begin{bmatrix} I_k \\ 0_{(n-k)\times k} \end{bmatrix}. \tag{51}$$

Partition each of the $k \times n$ matrix products $D_{i,e} W^{-1}$ into a $k \times k$ block T_i to the left of a $k \times (n-k)$ block U_i:

$$D_{i,e} W^{-1} = [T_i \quad U_i] \tag{52}$$

and then let V be the following $n \times n$ matrix over $\mathbb{F}$:

$$V = \begin{bmatrix} I_k & U_0 \\ 0_{(n-k)\times k} & I_{n-k} \end{bmatrix}. \tag{53}$$

It is easy to verify that

$$V^{-1} = \begin{bmatrix} I_k & -U_0 \\ 0_{(n-k)\times k} & I_{n-k} \end{bmatrix}. \tag{54}$$

For each $i = 0, 1, \ldots, m$, change the network encoding and decoding matrices from M_i and $D_{i,e}$, respectively, to

$$M'_i = V W M_i \tag{55}$$

$$D'_{i,e} = D_{i,e} W^{-1} V^{-1}. \tag{56}$$

We have

$$T_0 = D_{0,e} W^{-1} W M_0 = I_k \quad \text{[from (49), (51), (52)]} \tag{57}$$

and therefore

$$\begin{aligned} M'_0 &= \begin{bmatrix} I_k \\ 0 \end{bmatrix} \quad \text{[from (51), (53), (55)]} \\ D'_{0,e} &= [I_k \quad 0] \quad \text{[from (52), (54), (56), (57)]}. \end{aligned} \tag{58}$$

In this case,

$$e' = \sum_{j=0}^{m} M'_j\, x_j$$

and for each $i = 0, 1, \ldots, m$, the message vectors can be recovered by:

$$\begin{aligned} &D'_{i,e} e' + D_i e_i \\ &= D_{i,e} W^{-1} V^{-1} \sum_{j=0}^{m} V W M_j\, x_j + D_i e_i \quad \text{[from (55), (56)]} \\ &= D_{i,e} e + D_i e_i = x_i \quad \text{[from (33), (34)]}. \end{aligned}$$

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:

$$M_i = \begin{bmatrix} R_i \\ S_i \end{bmatrix} \tag{59}$$

and let

$$\rho = \mathsf{rank}\left([R_1 \quad \cdots \quad R_m]\right)$$

where $[R_1 \quad \cdots \quad R_m]$ is the concatenation of the matrices R_i into a $k \times mk$ matrix.

Clearly $\rho \leq k$. We have

$$\begin{aligned} D_0 \sum_{j=1}^{m} M_{0,j}\, x_j &= D_0\, e_0 \quad \text{[from (32)]} \\ &= -D_{0,e} \sum_{j=1}^{m} M_j\, x_j \quad \text{[from (37)]} \\ &= -\sum_{j=1}^{m} R_j\, x_j \quad \text{[from (58), (59)]}. \end{aligned}$$

This gives us

$$D_0\, [M_{0,1} \quad \cdots \quad M_{0,m}] = -[R_1 \quad \cdots \quad R_m],$$

which implies

$$\begin{aligned} &\mathsf{rank}\left(D_0\right) \geq \mathsf{rank}\left([R_1 \quad \cdots \quad R_m]\right) = \rho \quad \text{[from (22)]} \\ &\therefore\ \mathsf{rank}\left(Q_0\right) = n - \mathsf{rank}\left(D_0\right) \leq n - \rho. \end{aligned} \tag{60}$$

Since the matrix

$$[R_1 \quad \cdots \quad R_m]$$

has rank ρ, there exists a $k \times k$ permutation matrix P such that the first ρ rows of

$$P\ [R_1 \quad \cdots \quad R_m]$$

are linearly independent and the remaining $k - \rho$ rows are linear combinations of those first ρ rows. Thus, there exists a $(k-\rho) \times k$ matrix X, whose right-most $k - \rho$ columns form $I_{k-\rho}$, and such that

$$X P\ [R_1 \quad \cdots \quad R_m] = 0_{(k-\rho)\times mk}. \tag{61}$$

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 $\mathsf{rank}\left(X\right) = k-\rho$, and since P is a permutation matrix, we have $\mathsf{rank}\left(P\right) = k$. Since XP has dimensions $(k-\rho) \times k$, we have

$$\begin{aligned} k - \rho &\geq \mathsf{rank}\left(XP\right) \\ &\geq \mathsf{rank}\left(X\right) + \mathsf{rank}\left(P\right) - k \quad \text{[from (21)]} \\ &= (k-\rho) + k - k = k - \rho \end{aligned}$$

and thus $\mathsf{rank}\left(XP\right) = k - \rho$.

Define a $(k-\rho)\times n$ matrix Y by concatenating the product XP with an all-zero matrix as follows:

$$Y = \begin{bmatrix} XP & 0_{(k-\rho)\times(n-k)} \end{bmatrix}.$$

For each $i = 1, 2, \ldots, m$ we have

$$\begin{aligned} YM_i &= \begin{bmatrix} XP & 0_{(k-\rho)\times(n-k)} \end{bmatrix} \begin{bmatrix} R_i \\ S_i \end{bmatrix} \\ &= 0_{(k-\rho)\times k} \quad \text{[from (59), (61)]}. \end{aligned} \tag{62}$$

Since, for each $i = 1, 2, \ldots, m$, we have

$$YM_i = 0_{(k-\rho)\times k}$$

and by (49),

$$D_{i,e}M_i = I_k,$$

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 A.5, we may choose $Q_{i,e}$ such that its first $k-\rho$ rows are the rows of Y. By (50), 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

$$Y \sum_{\substack{j=0 \\ j\neq i}}^{m} M_j x_j = YM_0 x_0 \quad \text{[from (62)]}. \tag{63}$$

If we view the message vectors $x_0, x_1, \ldots, x_m$ 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:

$$\begin{aligned} H(Q_0 e_0) &\leq n-\rho \quad \text{[from (60)]} \\ H(e_1, \ldots, e_m) &\leq mn \quad \left[\text{from } e_i \in \mathbb{F}^n\right] \end{aligned}$$

and

$$\begin{aligned} &H\left(Q_{i,e} \sum_{\substack{j=0 \\ j\neq i}}^{m} M_j x_j \;:\; i = 1, 2, \ldots, m \right) \\ &\quad \leq m(n-k) - (m-1)(k-\rho) \quad \text{[from (50), (63)]}. \end{aligned}$$

Therefore, the entropy of all of the vector functions in the list L is bounded by summing these bounds:

$$\begin{aligned} H(L) &\leq (2m+1)n - (m+1)k - (k-\rho)(m-2) \\ &\leq (2m+1)n - (m+1)k \end{aligned} \tag{64}$$

where the final inequality follows from the fact $\rho \leq k$ and $m \geq 2$. However, then we have:

$$\begin{aligned} (m+1)k &= H(x_0, x_1, \ldots, x_m) \quad \left[\text{from } x_i \in \mathbb{F}^k\right] \\ &\leq H(L) \quad \text{[from (46), (48)]} \\ &\leq (2m+1)n - (m+1)k \quad \text{[from (64)]} \\ \therefore \frac{k}{n} &\leq \frac{2m+1}{2m+2}. \end{aligned}$$

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 ith 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:

$$[e_0]_l = \begin{cases} \displaystyle\sum_{\substack{j=1 \\ j\neq l}}^{m} [x_j]_l & (l = 1, 2, \ldots, m) \\ \displaystyle\sum_{j=1}^{m} [x_j]_l & (l = m+1, \ldots, 2m+1) \\ \displaystyle\sum_{j=2}^{m} [x_j]_j & (l = 2m+2) \end{cases}$$

$$[e]_l = \begin{cases} \displaystyle\sum_{\substack{j=0 \\ j\neq l}}^{m} [x_j]_l & (l = 1, 2, \ldots, m) \\ \displaystyle\sum_{j=0}^{m} [x_j]_l & (l = m+1, \ldots, 2m+1) \\ [x_0]_{m+1} + \displaystyle\sum_{j=1}^{m} [x_j]_j & (l = 2m+2) \end{cases}$$

and for each $i = 1, 2, \ldots, m$,

$$[e_i]_l = \begin{cases} \displaystyle\sum_{\substack{j=0 \\ j\neq i \\ j\neq l}}^{m} [x_j]_l & (l = 1, 2, \ldots, m \text{ and } l \neq i) \\ [x_0]_{m+1} + \displaystyle\sum_{\substack{j=1 \\ j\neq i}}^{m} [x_j]_j & (l = i) \\ \displaystyle\sum_{\substack{j=0 \\ j\neq i}}^{m} [x_j]_l & (l = m+1, \ldots, 2m+1) \\ [x_0]_{m+1+i} & (l = 2m+2). \end{cases}$$

For each $l = 1, 2, \ldots, m$, we have

$$\begin{aligned} \sum_{\substack{i=0 \\ i\neq l}}^{m} [e_i]_l &= \sum_{\substack{i=0 \\ i\neq l}}^{m} \sum_{\substack{j=0 \\ j\neq i \\ j\neq l}}^{m} [x_j]_l = (m-1) \sum_{\substack{j=0 \\ j\neq l}}^{m} [x_j]_l \\ &= -\sum_{\substack{j=0 \\ j\neq l}}^{m} [x_j]_l \quad \left[\text{from } \mathsf{char}(\mathbb{F}) \,\middle|\, m\right]. \end{aligned} \tag{65}$$

For each $i = 1, 2, \ldots, m$, the receivers within $B(m)$ can linearly recover all $2m + 1$ components of their respective demands by:

$$\begin{aligned} &R_0 : [e]_l - [e_0]_l = [x_0]_l \quad (l = 1, 2, \ldots, 2m+1) \\ &R_i : [e]_l - [e_i]_l = [x_i]_l \quad (l = 1, \ldots, 2m+1 \text{ and } l \neq i) \\ &\qquad [e]_{2m+2} - [e_i]_i = [x_i]_i \end{aligned}$$

and the additional receiver can linearly recover all components of x_0 by:

$$\begin{aligned} R_x : \quad & -[e_0]_l - \sum_{\substack{i=0 \\ i \neq l}}^{m} [e_i]_l \quad (l = 1, 2, \ldots, m) \\ &= [x_0]_l \quad \text{[from (65)]} \\ &\quad [e_1]_1 - [e_0]_{2m+2} = [x_0]_{m+1} \\ &\quad [e_{l-m-1}]_{2m+2} = [x_0]_l \quad (l = m+2, \ldots, 2m+1). \end{aligned}$$

Thus, the code is in fact a solution for $\mathcal{N}_1(m)$. ∎

C. Proofs of Lemmas in Section IV

Proof of Lemma IV.2: Assume $w = 1$ and let ψ and π_1 be identity permutations. For each $a \in \mathbf{Z}_{mw}$ we have

$$\psi(w\pi_1(a)) = \psi(a) = a.$$

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

$$wy = wr_y \pmod{mw}. \tag{66}$$

For all integers x, y we have

$$\begin{aligned} wx = wy \pmod{mw} &\iff wr_x = wr_y \pmod{mw} \quad \text{[from (66)]} \\ &\iff r_x = r_y \quad \big[\text{from } 0 \leq r_x, r_y < m\big]. \end{aligned} \tag{67}$$

For each $a = q_a m + r_a \in \mathbf{Z}_{mw}$ such that $0 \leq r_a < m$, let $\hat{r}_a$ be the unique integer in $\{0, 1, \ldots, m-1\}$ such that

$$\hat{r}_a = r_a + 1 \pmod{m},$$

and for each $l = 1, 2, \ldots, w-1$, define permutations of $\mathbf{Z}_{mw}$ as follows:

$$\pi_l(a) = \begin{cases} q_a m + \hat{r}_a & \text{if } q_a = l \\ q_a m + r_a & \text{otherwise} \end{cases} \tag{68}$$

$$\pi_w(a) = a = q_a m + r_a. \tag{69}$$

Note that for all $l = 1, 2, \ldots, w-1$, the (non-linear) permutation π_l modifies the remainder r_a if $q_a = l$ and otherwise acts as the identity permutation. Also, π_w is the identity permutation. Since $a \in \mathbf{Z}_{mw}$, we have $0 \leq q_a < w$.

For each $a \in \mathbf{Z}_{mw}$, we will now show the mapping given by

$$a \longmapsto (w\pi_1(a), \ldots, w\pi_w(a))$$

is injective. For each $a, b \in \mathbf{Z}_{mw}$, suppose

$$w\pi_l(a) = w\pi_l(b) \pmod{mw} \quad (l = 1, 2, \ldots, w), \tag{70}$$

where

$$a = q_a m + r_a \text{ and } b = q_b m + r_b,$$

with

$$0 \leq r_a, r_b < m \text{ and } 0 \leq q_a, q_b < w.$$

Then we have

$$\begin{aligned} w\pi_w(a) = w\pi_w(b) \pmod{mw} \quad &\text{[from (70)]} \qquad (71) \\ wr_a = wr_b \pmod{mw} \quad &\text{[from (66), (69), (71)]} \\ \therefore r_a = r_b \quad &\text{[from (67)]}. \qquad (72) \end{aligned}$$

Let $\hat{r}_b$ be the unique integer in $\{0, 1, \ldots, m-1\}$ 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 we have:

$$\begin{aligned} w\pi_{q_b}(a) = w\pi_{q_b}(b) \pmod{mw} \quad &\text{[from (70)]} \qquad (73) \\ \therefore wr_a = w\hat{r}_b \pmod{mw} \quad &\text{[from (66), (68), (73)]} \\ \therefore r_a = r_a + 1 \pmod{m} \quad &\text{[from (67), (72)]}, \end{aligned}$$

which is a contradiction, so we must have $q_a = q_b$. Thus $a = b$.

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

$$(w\pi_1(a), w\pi_2(a), \ldots, w\pi_w(a)).$$

This implies the existence of the claimed mapping. ∎

Proof of Lemma IV.5: Assume $\mathcal{N}_2(m, w)$ is solvable over $\mathcal{A}$. For each $l = 1, 2, \ldots, w$, the block $B^{(l)}(m+1)$ together with source nodes $S_z, S_1^{(l)}, S_2^{(l)}, \ldots, S_{m+1}^{(l)}$ forms a copy of $\mathcal{N}_0(m+1)$, so by Lemma II.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 $\pi_0^{(l)}, \pi_1^{(l)}, \ldots, \pi_{m+1}^{(l)}$ and $\sigma_0^{(l)}, \sigma_1^{(l)}, \ldots, \sigma_{m+1}^{(l)}$ of $\mathcal{A}$, such that for each $i = 1, \ldots, m+1$, the edges carry the symbols:

$$\begin{aligned} e_0^{(l)} &= \sigma_0^{(l)} \left(\bigoplus_{j=1}^{m+1} \pi_j^{(l)} \left(x_j^{(l)} \right) \right) \\ e_i^{(l)} &= \sigma_i^{(l)} \left(\pi_0^{(l)}(z) \oplus_l \bigoplus_{\substack{j=1 \\ j \neq i}}^{m+1} \pi_j^{(l)} \left(x_j^{(l)} \right) \right) \\ e^{(l)} &= \pi_0^{(l)}(z) \oplus_l \bigoplus_{j=1}^{m+1} \pi_j^{(l)} \left(x_j^{(l)} \right), \end{aligned} \tag{74}$$

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 $l = 1, 2, \ldots, w$, 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:

$$\underbrace{(a \ominus_l b) \oplus_l \cdots \oplus_l (a \ominus_l b)}_{m \text{ adds}} = 0_l \quad [\text{from } (\mathcal{A}, \oplus_l) \text{ Abelian}]$$

$$\iff a = b \quad [\text{from } \gcd(m, |\mathcal{A}|) = 1].$$

Thus, for each l the mapping

$$a \longmapsto \underbrace{a \oplus_l \cdots \oplus_l a}_{m \text{ adds}}$$

is injective on the finite set $\mathcal{A}$ and therefore is bijective, and its inverse $\phi_l : \mathcal{A} \to \mathcal{A}$ satisfies

$$\underbrace{\phi_l(a) \oplus_l \cdots \oplus_l \phi_l(a)}_{m \text{ adds}} = a \quad (l = 1, 2, \ldots, w). \tag{75}$$

For each $a \in \mathcal{A}$ such that $a \neq 0_1$ and each $l = 2, \ldots, w$, let

$$f_l(a) = \pi_0^{(l)}\left(\pi_0^{(1)^{-1}}(0_1)\right) \ominus_l \pi_0^{(l)}\left(\pi_0^{(1)^{-1}}(a)\right). \tag{76}$$

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 $l = 2, \ldots, w$ and $j = 1, 2, \ldots, m+1$. Since $a \neq 0_1$ and $\pi_0^{(1)}$ is bijective, it follows that $z \neq \hat{z}$.

By Property $P(m+1)$ and (74), for each $i = 1, 2, \ldots, m+1$ and each $l = 2, \ldots, w$, we have:

$$e_i^{(1)} = \sigma_i^{(1)}\left(\underbrace{\phi_1(a) \oplus_1 \cdots \oplus_1 \phi_1(a)}_{m \text{ adds}}\right) = \sigma_i^{(1)}(a) \quad [\text{from (75)}]$$

$$e_i^{(l)} = \sigma_i^{(l)}\left(\pi_0^{(l)}\left(\pi_0^{(1)^{-1}}(0_1)\right)\right)$$

for the messages $x_j^{(l)}, z$, and

$$e_i^{(1)} = \sigma_i^{(1)}(a)$$

$$e_i^{(l)} = \sigma_i^{(l)}\left(\pi_0^{(l)}\left(\pi_0^{(1)^{-1}}(a)\right) \oplus_l \underbrace{\phi_l(f_l(a)) \oplus_l \cdots \oplus_l \phi_l(f_l(a))}_{m \text{ adds}}\right)$$

$$= \sigma_i^{(l)}\left(\pi_0^{(l)}\left(\pi_0^{(1)^{-1}}(a)\right) \oplus_l f_l(a)\right) \quad [\text{from (75)}]$$

$$= \sigma_i^{(l)}\left(\pi_0^{(l)}\left(\pi_0^{(1)^{-1}}(0_1)\right)\right) \quad [\text{from (76)}]$$

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 $l = 1, 2, \ldots, w$ and $i = 1, 2, \ldots, m+1$, and therefore the decoded value z at R_z must be the same. However, this contradicts the fact that $z \neq \hat{z}$. ∎

Proof of Lemma IV.6: 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 $l = 1, 2, \ldots, w$ and each $i = 1, 2, \ldots, m+1$, the edge symbols can be written as:

$$e_0^{(l)} = \bigoplus_{j=1}^{m+1}\left(c_{0,j}^{(l)} \cdot x_j^{(l)}\right) \tag{77}$$

$$e_i^{(l)} = \left(c_{i,0}^{(l)} \cdot z\right) \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m+1}\left(c_{i,j}^{(l)} \cdot x_j^{(l)}\right) \tag{78}$$

$$e^{(l)} = \left(c_0^{(l)} \cdot z\right) \oplus \bigoplus_{j=1}^{m+1}\left(c_j^{(l)} \cdot x_j^{(l)}\right) \tag{79}$$

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:

$$R_0^{(l)}: \quad z = \left(d_{0,e}^{(l)} \cdot e^{(l)}\right) \oplus \left(d_0^{(l)} \cdot e_0^{(l)}\right) \tag{80}$$

$$R_i^{(l)}: \; x_i^{(l)} = \left(d_{i,e}^{(l)} \cdot e^{(l)}\right) \oplus \left(d_i^{(l)} \cdot e_i^{(l)}\right). \tag{81}$$

Since R_z linearly recovers z from its inputs, there exists $d_{z,i}^{(l)} \in R$ such that

$$R_z: \quad z = \bigoplus_{l=1}^{w}\bigoplus_{i=1}^{m+1}\left(d_{z,i}^{(l)} \cdot e_i^{(l)}\right). \tag{82}$$

For each $l = 1, 2, \ldots, w$, the block $B^{(l)}(m+1)$ together with source nodes $S_z, S_1^{(l)}, S_2^{(l)}, \ldots, S_{m+1}^{(l)}$ forms a copy of network $\mathcal{N}_0(m+1)$, so by Lemma II.3 and (77) – (81), each $c_i^{(l)}$ and each $d_i^{(l)}$ is invertible in R, and for each distinct $i, j \in \{0, 1, \ldots, m+1\}$, we have

$$c_{i,j}^{(l)} = -\left(d_i^{(l)}\right)^{-1} d_{i,e}^{(l)}\, c_j^{(l)}. \tag{83}$$

Equating message components at R_z yields:

$$1_R = \sum_{l=1}^{w}\sum_{i=1}^{m+1} d_{z,i}^{(l)}\, c_{i,0}^{(l)} \quad [\text{from (78), (82)}]$$

$$= -\sum_{l=1}^{w}\sum_{i=1}^{m+1} d_{z,i}^{(l)}\left(d_i^{(l)}\right)^{-1} d_{i,e}^{(l)}\, c_0^{(l)} \quad [\text{from (83)}] \tag{84}$$

and for each $l = 1, 2, \ldots, w$ and each $j = 1, 2, \ldots, m+1$,

$$0_R = \sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)}\, c_{i,j}^{(l)} \quad [\text{from (78), (82)}]$$

$$= -\left(\sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)}\left(d_i^{(l)}\right)^{-1} d_{i,e}^{(l)}\right) c_j^{(l)} \quad [\text{from (83)}]. \tag{85}$$

By right multiplying (85) by $\left(c_j^{(l)}\right)^{-1} c_0^{(l)}$, we have

$$0_R = \sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)}\left(d_i^{(l)}\right)^{-1} d_{i,e}^{(l)}\, c_0^{(l)} \quad [\text{from (85)}] \tag{86}$$

and by summing (86) over $j = 1, 2, \ldots, m+1$, we have

$$0_R = \sum_{j=1}^{m+1} \sum_{\substack{i=1 \\ i \neq j}}^{m+1} d_{z,i}^{(l)} \left(d_i^{(l)}\right)^{-1} d_{i,e}^{(l)} c_0^{(l)}$$
$$= m \sum_{i=1}^{m+1} d_{z,i}^{(l)} \left(d_i^{(l)}\right)^{-1} d_{i,e}^{(l)} c_0^{(l)}. \quad (87)$$

By summing (87) over $l = 1, 2, \ldots, w$, we have

$$0_R = m \sum_{i=1}^{w} \sum_{i=1}^{m+1} d_{z,i}^{(l)} \left(d_i^{(l)}\right)^{-1} d_{i,e}^{(l)} c_0^{(l)} \quad \text{[from (87)]}$$
$$\therefore 0_R = m \quad \text{[from (84)]}.$$

To prove the converse, let G be a standard R-module such that $m\, 1_R = 0_R$. Define a linear code over G such that for each $l = 1, 2, \ldots, w$, we have

$$e_0^{(l)} = \bigoplus_{j=1}^{m+1} x_j^{(l)}$$
$$e_i^{(l)} = z \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m+1} x_j^{(l)} \quad (i = 1, 2, \ldots, m+1)$$
$$e^{(l)} = z \oplus \bigoplus_{j=1}^{m+1} x_j^{(l)}.$$

For each $l = 1, 2, \ldots, w$, the receivers within each block $B^{(l)}(m+1)$ can linearly recover their respective demands as follows:

$$R_0^{(l)} : e^{(l)} \ominus e_0^{(l)} = z$$
$$R_i^{(l)} : e^{(l)} \ominus e_i^{(l)} = x_i^{(l)} \quad (i = 1, 2, \ldots, m+1).$$

Receiver R_z can linearly recover z as follows:

$$R_z : \bigoplus_{i=1}^{m+1} e_i^{(1)} = z \oplus (m\, z) \oplus \left(m \bigoplus_{j=1}^{m+1} x_j^{(1)}\right)$$
$$= z \qquad \text{[from } m = 0_R\text{]}.$$

Thus the code is a linear solution for $\mathcal{N}_2(m, w)$. ∎

Proof of Lemma IV.7: Since a scalar linear solution over a finite-field alphabet is a special case of a linear solution over a standard module, by Lemma IV.6, $\mathcal{N}_2(m, w)$ is scalar linearly solvable over any finite-field alphabet whose characteristic divides m, so the linear capacity for such finite-field alphabets is at least 1. By Lemma II.4, network $\mathcal{N}_0(m+1)$ has capacity equal to 1, and the block $B^{(1)}(m+1)$ together with the source nodes $S_z, S_1^{(1)}, S_2^{(1)}, \ldots, S_{m+1}^{(1)}$ 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 alphabet 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 $\mathsf{char}(\mathbb{F}) \nmid m$, 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 $l = 1, 2, \ldots, w$ the edge vectors can be written as:

$$e_0^{(l)} = \sum_{j=1}^{m+1} M_{0,j}^{(l)} x_j^{(l)}$$
$$e_i^{(l)} = M_{i,0}^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_{i,j}^{(l)} x_j^{(l)} \quad (i = 1, 2, \ldots, m+1) \quad (88)$$
$$e^{(l)} = M_0^{(l)} z + \sum_{j=1}^{m+1} M_j^{(l)} x_j^{(l)} \quad (89)$$

and there exist $k \times n$ decoding matrices $D_{i,e}^{(l)}$ and $D_i^{(l)}$ over $\mathbb{F}$, such that for each $l = 1, 2, \ldots, w$ and each $i = 1, 2, \ldots, m+1$, 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:

$$R_i^{(l)} : \quad x_i^{(l)} = D_{i,e}^{(l)} e^{(l)} + D_i^{(l)} e_i^{(l)}. \quad (90)$$

Since receiver R_z linearly recovers z from its incoming edge vectors, we have

$$\left\{ e_i^{(l)} : \begin{matrix} l = 1, 2, \ldots, w \\ i = 1, 2, \ldots, m+1 \end{matrix} \right\} \longrightarrow z. \quad (91)$$

For each $l = 1, 2, \ldots, w$ and each $i = 1, 2, \ldots, m+1$, by (88) and (89), if we set $x_i^{(l)} = 0$ in (90), then, since $e_i^{(l)}$ does not depend on $x_i^{(l)}$, we get the following relationship among the remaining message vectors:

$$0 = D_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) + D_i^{(l)} e_i^{(l)} \quad (92)$$

and therefore

$$e_i^{(l)} \longrightarrow D_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) \quad \text{[from (92)]}. \quad (93)$$

For each $l = 1, 2, \ldots, w$ and each $i = 1, 2, \ldots, m+1$, let $Q_{i,e}^{(l)}$ be the matrix Q in Lemma A.5 corresponding to when the matrix A is $D_{i,e}^{(l)}$.

For each $l = 1, 2, \ldots, w$, let $L^{(l)}$ be the following list of $2(m+1)$ vector functions of $z, x_1^{(l)}, x_2^{(l)}, \ldots, x_{m+1}^{(l)}$:

$$Q_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) \quad (i = 1, 2, \ldots, m+1)$$
$$e_i^{(l)} \quad (i = 1, 2, \ldots, m+1).$$

For each $l = 1, 2, \ldots, w$ and each $i = 1, 2, \ldots, m+1$, we have

$$L^{(l)} \longrightarrow D_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) \quad \text{[from (93)]},$$

which, along with Lemma A.5, implies

$$L^{(l)} \longrightarrow M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)}. \tag{94}$$

We also have

$$\begin{aligned} z, \quad & \left\{ M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \ : \ i = 1, 2, \ldots, m+1 \right\} \\ & \longrightarrow \sum_{i=1}^{m+1} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) - M_0^{(l)} z \\ & = (m+1) M_0^{(l)} z + m \sum_{j=1}^{m+1} M_j^{(l)} x_j^{(l)} - M_0^{(l)} z \\ & = m e^{(l)} \longrightarrow e^{(l)} \quad \left[\text{from (89) and } \mathsf{char}(\mathbb{F}) \nmid m\right] \end{aligned} \tag{95}$$

and

$$L^{(1)}, \ldots, L^{(w)} \longrightarrow z \quad \text{[from (91)]} \tag{96}$$

For each $l = 1, 2, \ldots, w$ and each $i = 1, 2, \ldots, m+1$, we have

$$L^{(l)}, z \longrightarrow e^{(l)} \quad \text{[from (94), (95)]} \tag{97}$$

$$L^{(l)}, z \longrightarrow x_i^{(l)} \quad \text{[from (90), (97)]}. \tag{98}$$

Thus it follows from (96) and (98) that

$$L^{(1)}, \ldots, L^{(w)} \longrightarrow z, \left\{ x_i^{(l)} : \begin{matrix} l = 1, 2, \ldots, w \\ i = 1, 2, \ldots, m+1 \end{matrix} \right\}. \tag{99}$$

We will now bound the number of independent entries in each list $L^{(l)}$.

By equating message components in equation (90), for each $l = 1, 2, \ldots, w$ and each $i = 1, 2, \ldots, m+1$, we have:

$$I_k = D_{i,e}^{(l)} M_i^{(l)} \quad \text{[from (88), (89), (90)]} \tag{100}$$

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

$$\begin{aligned} & \mathsf{rank} \left(D_{i,e}^{(l)} \right) \\ & \quad \geq \mathsf{rank} \left(D_{i,e}^{(l)} M_i^{(l)} \right) \quad \text{[from (22)]} \\ & \quad = \mathsf{rank} \left(I_k \right) = k \quad \text{[from (100)]}. \end{aligned}$$

Hence $\mathsf{rank} \left(D_{i,e}^{(l)} \right) = k$, which by Lemma (A.5), implies $\mathsf{rank} \left(Q_{i,e}^{(l)} \right) = n - k$. Therefore each vector function

$$Q_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) \qquad \begin{matrix} (l = 1, 2, \ldots, w) \\ (i = 1, 2, \ldots, m+1) \end{matrix}$$

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:

$$\begin{aligned} & H \left(Q_{i,e}^{(l)} \left(M_0^{(l)} z + \sum_{\substack{j=1 \\ j \neq i}}^{m+1} M_j^{(l)} x_j^{(l)} \right) : \begin{matrix} l = 1, 2, \ldots, w \\ i = 1, 2, \ldots, m+1 \end{matrix} \right) \\ & \leq w(m+1)(n-k) \end{aligned} \tag{101}$$

and

$$H \left(e_i^{(l)} : \begin{matrix} l = 1, 2, \ldots, w \\ i = 1, 2, \ldots, m+1 \end{matrix} \right) \leq w(m+1) n. \tag{102}$$

Therefore, the entropy of all of the vector functions in the list of lists $L^{(1)}, \ldots, L^{(w)}$ is bounded by summing the bounds in (101) and (102):

$$H \left(L^{(1)}, \ldots, L^{(w)} \right) \leq w(m+1) n - w(m+1) k. \tag{103}$$

But since each message is independent and uniformly distributed over $\mathbb{F}$ and $z, x_i^{(l)} \in \mathbb{F}^k$, we have

$$(w(m+1)+1) k = H \left(z, \left\{ x_i^{(l)} : \begin{matrix} l = 1, 2, \ldots, w \\ i = 1, 2, \ldots, m+1 \end{matrix} \right\} \right).$$

However, (99) implies this quantity is upper bounded by:

$$\begin{aligned} & H \left(L^{(1)}, \ldots, L^{(w)} \right) \\ & \leq 2w(m+1) n - w(m+1) k \quad \text{[from (103)]}, \end{aligned}$$

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

$$1 - \frac{1}{2mw + 2w + 1}.$$

D. Proofs of Lemmas in Section V

Proof of Lemma V.2: Define permutations π_1, π_2 of $\mathbf{Z}_{m^{\alpha+1}}$ as follows. For each $a \in \mathbf{Z}_{m^{\alpha+1}}$, let

$$\sum_{i=0}^{\alpha} m^i a_i$$

denote the base m representation of a. We define

$$\pi_1(a) = m^\alpha a_0 + \sum_{i=1}^{\alpha} m^{i-1} a_i \tag{104}$$

$$\pi_2(a) = a = \sum_{i=0}^{\alpha} m^i a_i. \tag{105}$$

The (non-linear) permutation π_1 performs a right-cyclic shift of the base-m digits of a, and π_2 is the identity permutation. For each $a \in \mathbf{Z}_{m^{\alpha+1}}$, we will show that the mapping given by

$$a \longmapsto (m\pi_1(a), \ sm^\alpha \pi_2(a))$$

is injective. For each $a, b \in \mathbf{Z}_{m^{\alpha+1}}$, suppose

$$m\pi_1(a) = m\pi_1(b) \pmod{m^{\alpha+1}} \tag{106}$$

$$sm^{\alpha}\pi_2(a) = sm^{\alpha}\pi_2(b) \pmod{m^{\alpha+1}} \tag{107}$$

where $a = \sum_{i=0}^{\alpha} m^i a_i$ and $b = \sum_{i=0}^{\alpha} m^i b_i$. Then we have

$$\sum_{i=1}^{\alpha} m^i a_i = \sum_{i=1}^{\alpha} m^i b_i \pmod{m^{\alpha+1}} \quad \text{[from (104), (106)]}.$$

Therefore

$$a_i = b_i \quad (i = 1, 2, \ldots, \alpha) \quad \text{[from } 0 \le a_i, b_i < m\text{]}$$

and

$$sm^{\alpha}a_0 = sm^{\alpha}b_0 \pmod{m^{\alpha+1}} \quad \text{[from (105), (107)]}$$

$$\therefore\ m^{\alpha}a_0 = m^{\alpha}b_0 \pmod{m^{\alpha+1}} \quad \text{[from } \gcd(m, s) = 1\text{]}$$

$$\therefore\ a_0 = b_0 \quad \text{[from } 0 \le a_0, b_0 < m\text{]}.$$

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. ∎

Proof of Lemma V.5:

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 $S_z, S_1^{(l)}, S_2^{(l)}, \ldots, S_{m_l}^{(l)}$ forms a copy of $\mathcal{N}_0(m_l)$, so by Lemma II.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 $\pi_0^{(l)}, \pi_1^{(l)}, \ldots, \pi_{m_l}^{(l)}$ and $\sigma_0^{(l)}, \sigma_1^{(l)}, \ldots, \sigma_{m_l}^{(l)}$ of $\mathcal{A}$, such that for each $l = 1, 2$ and each $i = 1, 2, \ldots, m_l$, the edges carry the symbols:

$$e_0^{(l)} = \sigma_0^{(l)}\left(\bigoplus_{j=1}^{m_l} \pi_j^{(l)}\left(x_j^{(l)}\right)\right) \tag{108}$$

$$e_i^{(l)} = \sigma_i^{(l)}\left(\pi_0^{(l)}(z) \oplus_l \bigoplus_{\substack{j=1 \\ j\neq i}}^{m_l} \pi_j^{(l)}\left(x_j^{(l)}\right)\right) \tag{109}$$

$$e^{(l)} = \pi_0^{(l)}(z) \oplus_l \bigoplus_{j=1}^{m_l} \pi_j^{(l)}\left(x_j^{(l)}\right)$$

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

$$\underbrace{a \oplus_2 \cdots \oplus_2 a}_{m_2 \text{ adds}} = 0_2 \quad \left[\text{from } |\mathcal{A}| \,\middle|\, m_2\right]. \tag{110}$$

Since m_1 and $|\mathcal{A}|$ are not relatively prime, m_1 and $|\mathcal{A}|$ share a common factor p. Since $p \,|\, |\mathcal{A}|$, by Cauchy's Theorem, there exists $a \in \mathcal{A}\backslash\{0_1\}$ 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:

$$x_j^{(1)} = \pi_j^{(1)^{-1}}(0_1) \quad (j = 1, 2, \ldots, m_1)$$

$$x_j^{(2)} = \pi_j^{(2)^{-1}}\left(\pi_0^{(2)}\left(\pi_0^{(1)^{-1}}(0_1)\right)\right) \quad (j = 1, 2, \ldots, m_2)$$

$$z = \pi_0^{(1)^{-1}}(0_1)$$

and

$$\hat{x}_j^{(1)} = \pi_j^{(1)^{-1}}(a) \quad (j = 1, 2, \ldots, m_1)$$

$$\hat{x}_j^{(2)} = \pi_j^{(2)^{-1}}\left(\pi_0^{(2)}\left(\pi_0^{(1)^{-1}}(a)\right)\right) \quad (j = 1, 2, \ldots, m_2)$$

$$\hat{z} = \pi_0^{(1)^{-1}}(a).$$

Since $a \neq 0_1$ and $\pi_0^{(1)}$ is bijective, it follows that $z \neq \hat{z}$.

By Properties $P(m_1)$ and $P(m_2)$ and (108) and (109), we have

$$e_i^{(1)} = \sigma_i^{(1)}\left(\underbrace{0_1 \oplus_1 \cdots \oplus_1 0_1}_{m_1 \text{ adds}}\right) = \sigma_i^{(1)}(0_1) \quad (i = 0, 1, \ldots, m_1)$$

$$e_i^{(2)} = \sigma_i^{(2)}\left(\underbrace{\pi_0^{(2)}\left(\pi_0^{(1)^{-1}}(0_1)\right) \oplus_2 \cdots \oplus_2 \pi_0^{(2)}\left(\pi_0^{(1)^{-1}}(0_1)\right)}_{m_2 \text{ adds}}\right)$$

$$= \sigma_i^{(2)}(0_2) \qquad (i = 0, 1, \ldots, m_2) \qquad \text{[from (110)]}$$

for the messages $x_j^{(l)}, z$, and

$$e_i^{(1)} = \sigma_i^{(1)}\left(\underbrace{a \oplus_1 \cdots \oplus_1 a}_{m_1 \text{ adds}}\right) = \sigma_i^{(1)}(0_1) \quad (i = 0, 1, \ldots, m_1)$$

$$e_i^{(2)} = \sigma_i^{(2)}\left(\underbrace{\pi_0^{(2)}\left(\pi_0^{(1)^{-1}}(a)\right) \oplus_2 \cdots \oplus_2 \pi_0^{(2)}\left(\pi_0^{(1)^{-1}}(a)\right)}_{m_2 \text{ adds}}\right)$$

$$= \sigma_i^{(2)}(0_2) \qquad (i = 0, 1, \ldots, m_2) \qquad \text{[from (110)]}$$

for the messages $\hat{x}_j^{(l)}, \hat{z}$. For both collections of messages, the edge symbols $e_0^{(1)}, e_1^{(1)}, \ldots, e_{m_1}^{(1)}$ and $e_0^{(2)}, e_1^{(2)}, \ldots, e_{m_2}^{(2)}$ are the same, and therefore the decoded value z at R_z must be the same. However, this contradicts the fact that $z \neq \hat{z}$. ∎

Proof of Lemma V.6:

For any integers $a, b, c \ge 1$, we have

$$\gcd(a, b, c) = \gcd(\gcd(a, b), c),$$

so by Lemma A.1 the integer $\gcd(m_1, m_2)$ is invertible in the ring R if and only if

$$\gcd(m_1, m_2, \mathrm{char}(R)) = 1.$$

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 $i = 1, 2, \ldots, m_l$, the edge symbols can be written as:

$$e_0^{(l)} = \bigoplus_{j=1}^{m_l} \left(c_{0,j}^{(l)} \cdot x_j^{(l)} \right) \tag{111}$$

$$e_i^{(l)} = \left(c_{i,0}^{(l)} \cdot z \right) \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m_l} \left(c_{i,j}^{(l)} \cdot x_j^{(l)} \right) \tag{112}$$

$$e^{(l)} = \left(c_0^{(l)} \cdot z \right) \oplus \bigoplus_{j=1}^{m_l} \left(c_j^{(l)} \cdot x_j^{(l)} \right) \tag{113}$$

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:

$$R_0^{(l)}: \quad z = \left(d_{0,e}^{(l)} \cdot e^{(l)} \right) \oplus \left(d_0^{(l)} \cdot e_0^{(l)} \right) \tag{114}$$

$$R_i^{(l)}: \quad x_i^{(l)} = \left(d_{i,e}^{(l)} \cdot e^{(l)} \right) \oplus \left(d_i^{(l)} \cdot e_i^{(l)} \right). \tag{115}$$

Since R_z linearly recovers z from its inputs, there exists $d_{z,i}^{(l)} \in R$ such that

$$R_z: \quad z = \bigoplus_{l=1}^{2} \bigoplus_{i=0}^{m_l} \left(d_{z,i}^{(l)} \cdot e_i^{(l)} \right). \tag{116}$$

For each $l = 1, 2$ the block $B^{(l)}(m_l)$ together with the source nodes $S_z, S_1^{(l)}, S_2^{(l)}, \ldots, S_{m_l}^{(l)}$ forms a copy of $\mathcal{N}_0(m_l)$, so by Lemma II.3 and (111) – (115), each $c_i^{(l)}$ and each $d_i^{(l)}$ is invertible in R, and for each distinct $i, j \in \{0, 1, \ldots, m_l\}$, we have

$$c_{i,j}^{(l)} = -\left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} \, c_j^{(l)}. \tag{117}$$

Equating message components at R_z yields:

$$\begin{aligned} 1_R &= \sum_{l=1}^{2} \sum_{i=1}^{m_l} d_{z,i}^{(l)} \, c_{i,0}^{(l)} \qquad \text{[from (111), (112), (116)]} \\ &= -\sum_{l=1}^{2} \sum_{i=1}^{m_l} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} \, c_0^{(l)} \quad \text{[from (117)]} \end{aligned} \tag{118}$$

and for each $l = 1, 2$ and each $j = 1, 2, \ldots, m_l$, we have

$$\begin{aligned} 0_R &= \sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} \, c_{i,j}^{(l)} \qquad \text{[from (111), (112), (116)]} \\ &= -\left(\sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} \right) c_j^{(l)} \quad \text{[from (117)]}. \end{aligned} \tag{119}$$

For each $l = 1, 2$, by right multiplying (119) by $\left(c_j^{(l)} \right)^{-1} c_0^{(l)}$, we have

$$0_R = \sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} \, c_0^{(l)} \quad (j = 1, 2, \ldots, m_l). \tag{120}$$

Summing (120) over $l = 1, 2$ and $j = 1, 2, \ldots, m_l$ and subtracting (118), yields

$$\begin{aligned} -1_R &= \sum_{l=1}^{2} \sum_{j=0}^{m_l} \sum_{\substack{i=0 \\ i \neq j}}^{m_l} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} \, c_0^{(l)} \\ &= \sum_{l=1}^{2} m_l \sum_{i=0}^{m_l} d_{z,i}^{(l)} \left(d_i^{(l)} \right)^{-1} d_{i,e}^{(l)} \, c_0^{(l)}. \end{aligned} \tag{121}$$

Equation (121) implies there exist $r_1, r_2 \in R$ such that

$$1_R = m_1 \, r_1 + m_2 \, r_2. \tag{122}$$

Since $\gcd(m_1, m_2)$ can be factored out of both terms on the right-hand side of equation (122), 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:

$$\begin{aligned} e_0^{(l)} &= \bigoplus_{j=1}^{m_l} x_j^{(l)} \\ e_i^{(l)} &= z \oplus \bigoplus_{\substack{j=1 \\ j \neq i}}^{m_l} x_j^{(l)} \quad (i = 1, 2, \ldots, m_l) \\ e^{(l)} &= z \oplus \bigoplus_{j=1}^{m_l} x_j^{(l)}. \end{aligned}$$

For each $l = 1, 2$, the receivers within $B^{(l)}(m_l)$ can linearly recover their respective demands by:

$$\begin{aligned} &R_0^{(l)}: e^{(l)} \ominus e_0^{(l)} = z \\ &R_i^{(l)}: e^{(l)} \ominus e_i^{(l)} = x_i^{(l)} \quad (i = 1, 2, \ldots, m_l). \end{aligned}$$

Let

$$m_1' = m_1 / \gcd(m_1, m_2) \quad \text{and} \quad m_2' = m_2 / \gcd(m_1, m_2).$$

Then m_1' and m_2' are relatively prime, so there exist $n_1, n_2 \in \mathbf{Z}$ 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:

$$\begin{aligned} R_z: \quad & \bigoplus_{l=1}^{2} \left(\left(n_l \gcd(m_1, m_2)^{-1} \right) \cdot \left(\bigoplus_{i=0}^{m_l} e_i^{(l)} \ominus \left(m_l e_0^{(l)} \right) \right) \right) \\ &= \bigoplus_{l=1}^{2} \left(\left(n_l \gcd(m_1, m_2)^{-1} \right) \cdot (m_l \, z) \right) \\ &= (n_1 m_1' \, z) \oplus (n_2 m_2' \, z) \\ &= \left((n_1 m_1') \, 1_R + (n_2 m_2') \, 1_R \right) z = z. \end{aligned}$$

Thus the code is a linear solution for $\mathcal{N}_3(m_1, m_2)$. ■

Proof of Lemma V.8: By Lemma V.6, the network $\mathcal{N}_3(m_1, m_2)$ is scalar linearly solvable over any finite-field alphabet whose characteristic is relatively prime to m_1 or m_2, so the network's linear capacity for such finite-field alphabets is at least 1. By Lemma II.4, network $\mathcal{N}_0(m_1)$ has capacity

equal to 1, the block $B^{(1)}(m_1)$ together with the source nodes $S_z, S_1^{(1)}, S_2^{(1)}, \ldots, S_{m_1}^{(1)}$ 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 alphabet 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 $\mathsf{char}(\mathbb{F}) \,\big|\, m_1$ and $\mathsf{char}(\mathbb{F}) \,\big|\, m_2$, 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:

$$e_0^{(l)} = \sum_{j=1}^{m_l} M_{0,j}^{(l)}\, x_j^{(l)} \tag{123}$$

$$e_i^{(l)} = M_0^{(l)}\, z + \sum_{\substack{j=1 \\ j\neq i}}^{m_l} M_{i,j}^{(l)}\, x_j^{(l)} \quad (i = 1, 2, \ldots, m_l) \tag{124}$$

$$e^{(l)} = M_0^{(l)}\, z + \sum_{j=1}^{m_l} M_j^{(l)}\, x_j^{(l)} \tag{125}$$

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:

$$R_0^{(l)}: \quad z = D_{0,e}^{(l)}\, e^{(l)} + D_0^{(l)}\, e_0^{(l)} \tag{126}$$

$$R_i^{(l)}: \; x_i^{(l)} = D_{i,e}^{(l)}\, e^{(l)} + D_i^{(l)}\, e_i^{(l)} \quad (i = 1, 2, \ldots, m_l). \tag{127}$$

Since the receiver R_z recovers message vector z linearly from its incoming edge vectors, we have

$$\left\{ e_i^{(l)} \;:\; \begin{matrix} l = 1, 2 \\ i = 0, 1, \ldots, m_l \end{matrix} \right\} \longrightarrow z. \tag{128}$$

For each $l = 1, 2$, by (123) and (125), if we set $z = 0$ in (126), we have

$$0 = D_{0,e}^{(l)} \sum_{j=1}^{m_l} M_j^{(l)}\, x_j^{(l)} + D_0^{(l)}\, e_0^{(l)}$$

$$\therefore \sum_{j=1}^{m_l} M_j^{(l)}\, x_j^{(l)} \longrightarrow D_0^{(l)}\, e_0^{(l)}, \tag{129}$$

and similarly, for each $i = 1, 2, \ldots, m_l$, by (124) and (125), if we set $x_i^{(l)} = 0$ in (127), we have

$$0 = D_{i,e}^{(l)} \left(M_0^{(l)}\, z + \sum_{\substack{j=1 \\ j\neq i}}^{m_l} M_j^{(l)}\, x_j^{(l)} \right) + D_i^{(l)}\, e_i^{(l)}$$

$$\therefore\; e_i^{(l)} \longrightarrow D_{i,e}^{(l)} \left(M_0^{(l)}\, z + \sum_{\substack{j=1 \\ j\neq i}}^{m_l} M_j^{(l)}\, x_j^{(l)} \right). \tag{130}$$

As in Lemma III.4, for each $l = 1, 2$ and $i = 1, 2, \ldots, m_l$, let $Q_0^{(l)}$ be the matrix Q in Lemma A.5 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 III.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

$$Q_0^{(l)}\, e_0^{(l)}$$
$$e_i^{(l)} \quad (i = 1, 2, \ldots, m_l)$$
$$Q_{i,e}^{(l)} \left(M_0^{(l)}\, z + \sum_{\substack{j=1 \\ j\neq i}}^{m_l} M_j^{(l)}\, x_j^{(l)} \right) \quad (i = 1, 2, \ldots, m_l).$$

For each $l = 1, 2$, we have

$$L^{(l)} \longrightarrow D_{i,e}^{(l)} \left(M_0^{(l)}\, z + \sum_{\substack{j=1 \\ j\neq i}}^{m_l} M_j^{(l)}\, x_j^{(l)} \right) \quad \text{[from (130)]}$$

which, along with Lemma A.5, implies

$$L^{(l)} \longrightarrow M_0^{(l)}\, z + \sum_{\substack{j=1 \\ j\neq i}}^{m_l} M_j^{(l)}\, x_j^{(l)}. \tag{131}$$

For each $l = 1, 2$, we also have

$$\left\{ M_0^{(l)}\, z + \sum_{\substack{j=1 \\ j\neq i}}^{m_l} M_j^{(l)}\, x_j^{(l)} \;:\; i = 1, 2, \ldots, m_l \right\}$$

$$\longrightarrow \sum_{i=1}^{m_l} \left(M_0^{(l)}\, z + \sum_{\substack{j=1 \\ j\neq i}}^{m_l} M_j^{(l)}\, x_j^{(l)} \right)$$

$$= m_l\, M_0^{(l)}\, z + (m_1 - 1) \sum_{j=1}^{m_l} M_j^{(l)}\, x_j^{(l)}$$

$$= -\sum_{j=1}^{m_l} M_j^{(l)}\, x_j^{(l)} \qquad \big[\text{from } \mathsf{char}(\mathbb{F}) \,\big|\, m_l\big], \tag{132}$$

and so

$$L^{(l)} \longrightarrow \sum_{j=1}^{m_l} M_j^{(l)}\, x_j^{(l)} \quad \text{[from (131), (132)]} \tag{133}$$

$$L^{(l)} \longrightarrow D_0^{(l)}\, e_0^{(l)} \quad \text{[from (129), (133)]} \tag{134}$$

$$L^{(l)} \longrightarrow e_0^{(l)} \quad \text{[from Lemma A.5, (134)]}. \tag{135}$$

We have

$$L^{(1)}, L^{(2)} \longrightarrow z \quad \text{[from (128), (135)]}. \tag{136}$$

For each $l = 1, 2$, we also have

$$z, \sum_{j=1}^{m_l} M_j^{(l)} x_j^{(l)} \longrightarrow e^{(l)} \quad \text{[from (125)]} \tag{137}$$

$$L^{(l)}, z \longrightarrow e^{(l)} \quad \text{[from (133), (137)]} \tag{138}$$

and for each $i = 1, 2, \ldots, m_l$, we have

$$L^{(l)}, z \longrightarrow x_i^{(l)} \quad \text{[from (127), (138)]}. \tag{139}$$

Thus equations (136) and (139) imply

$$L^{(1)}, L^{(2)} \longrightarrow z, \left\{ x_i^{(l)} : \begin{matrix} l = 1, 2 \\ i = 1, 2, \ldots, m_l \end{matrix} \right\}. \tag{140}$$

We have $L^{(l)}$ corresponding to the same set of vector functions as the list L for $\mathcal{N}_1(m_l)$ in Lemma III.4 (with a slight change of labeling). Thus the bound on the entropy of the list L in (64) in Lemma III.4 can be used to bound the entropy of the list $L^{(1)}, L^{(2)}$:

$$H\left(L^{(1)}, L^{(2)}\right) \leq \sum_{l=1}^{2} (2m_l + 1)\, n - (m_l + 1)\, k. \tag{141}$$

But since each message is independent and uniformly distributed over $\mathbb{F}$ and $z, x_i^{(l)} \in \mathbb{F}^k$, we have

$$(m_1 + m_2 + 1)\, k = H\left(z, \left\{ x_i^{(l)} : \begin{matrix} l = 1, 2 \\ i = 1, 2, \ldots, m_l \end{matrix} \right\}\right).$$

However, (140) implies this quantity is upper bounded by

$$\begin{aligned} &H(L_1, L_2) \\ &\leq (2m_1 + 2m_2 + 2)\; n - (m_1 + m_2 + 2)\; k \quad \text{[from (141)]}, \end{aligned}$$

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

$$\left[e_0^{(1)}\right]_l = \begin{cases} \displaystyle\sum_{\substack{j=1 \\ j \neq l}}^{m_1} \left[x_j^{(1)}\right]_l & (l = 1, 2, \ldots, m_1) \\ \displaystyle\sum_{j=1}^{m_1} \left[x_j^{(1)}\right]_l & (l = m_1 + 1, \ldots, k) \\ \displaystyle\sum_{j=2}^{m_1} \left[x_j^{(1)}\right]_j & (l = k + 1) \end{cases}$$

$$\left[e^{(1)}\right]_l = \begin{cases} [z]_l + \displaystyle\sum_{\substack{j=1 \\ j \neq l}}^{m_1} \left[x_j^{(1)}\right]_l & (l = 1, 2, \ldots, m_1) \\ [z]_l + \displaystyle\sum_{j=1}^{m_1} \left[x_j^{(1)}\right]_l & (l = m_1 + 1, \ldots, k) \\ [z]_{m_1+1} + \displaystyle\sum_{j=1}^{m_1} \left[x_j^{(1)}\right]_j & (l = k + 1) \end{cases}$$

and for each $i = 1, 2, \ldots, m_1$, let

$$\left[e_i^{(1)}\right]_l = \begin{cases} [z]_l + \displaystyle\sum_{\substack{j=1 \\ j \neq i \\ j \neq l}}^{m_1} \left[x_j^{(1)}\right]_l & \begin{pmatrix} l = 1, 2, \ldots, m_1 \\ \text{and } l \neq i \end{pmatrix} \\ [z]_{m_1+1} + \displaystyle\sum_{\substack{j=1 \\ j \neq i}}^{m_1} \left[x_j^{(1)}\right]_j & (l = i) \\ [z]_l + \displaystyle\sum_{\substack{j=1 \\ j \neq i}}^{m_1} \left[x_j^{(1)}\right]_l & (l = m_1 + 1, \ldots, k) \\ [z]_{m_1+i+1} & (l = k + 1). \end{cases}$$

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

$$\left[e_0^{(2)}\right]_l = \begin{cases} \displaystyle\sum_{j=1}^{m_2} \left[x_j^{(2)}\right]_l & (l = 1, 2, \ldots, \delta) \\ \displaystyle\sum_{\substack{j=1 \\ j \neq l-\delta}}^{m_2} \left[x_j^{(2)}\right]_l & (l = \delta + 1, \ldots, k) \\ \displaystyle\sum_{j=2}^{m_2} \left[x_j^{(2)}\right]_{\delta+j} & (l = k + 1) \end{cases}$$

$$\left[e^{(2)}\right]_l = \begin{cases} [z]_l + \sum_{j=1}^{m_2} \left[x_j^{(2)}\right]_l & (l = 1, 2, \ldots, \delta) \\ [z]_l + \sum_{\substack{j=1 \\ j \neq l-\delta}}^{m_2} \left[x_j^{(2)}\right]_l & (l = \delta+1, \ldots, k) \\ [z]_\delta + \sum_{j=1}^{m_2} \left[x_j^{(2)}\right]_{\delta+j} & (l = k+1) \end{cases}$$

and for each $i = 1, 2, \ldots, m_2$, let

$$\left[e_i^{(2)}\right]_l = \begin{cases} [z]_l + \sum_{\substack{j=1 \\ j \neq i}}^{m_2} \left[x_j^{(2)}\right]_l & (l = 1, 2, \ldots, \delta) \\ [z]_\delta + \sum_{\substack{j=1 \\ j \neq i}}^{m_2} \left[x_j^{(2)}\right]_{\delta+j} & (l = \delta + i) \\ [z]_l + \sum_{\substack{j=1 \\ j \neq i \\ j \neq l-\delta}}^{m_2} \left[x_j^{(2)}\right]_l & \begin{pmatrix} l = \delta+1, \ldots, k \\ \text{and } l \neq \delta + i \end{pmatrix} \\ [z]_{2m_1+1+i} & (l = k+1). \end{cases}$$

For each $l = 1, 2, \ldots, m_1$, we have

$$\begin{aligned} \sum_{\substack{i=1 \\ i \neq l}}^{m_1} \left[e_i^{(1)}\right]_l &= (m_1 - 1)\,[z]_l + (m_1 - 2) \sum_{\substack{j=1 \\ j \neq l}}^{m_1} \left[x_j^{(1)}\right]_l \\ &= -[z]_l - 2\left[e_0^{(1)}\right]_l \quad \left[\text{from } \mathsf{char}(\mathbb{F}) \,\middle|\, m_1\right]. \end{aligned} \tag{142}$$

Similarly, for each $l = \delta + 1, \ldots, k$, we have

$$\begin{aligned} \sum_{\substack{i=1 \\ i \neq l-\delta}}^{m_2} \left[e_i^{(2)}\right]_l &= (m_2 - 1)\,[z]_l + (m_2 - 2) \sum_{\substack{j=1 \\ j \neq l-\delta}}^{m_2} \left[x_j^{(2)}\right]_l \\ &= -[z]_l - 2\left[e_0^{(2)}\right]_l \quad \left[\text{from } \mathsf{char}(\mathbb{F}) \,\middle|\, m_2\right]. \end{aligned} \tag{143}$$

Each of the receivers can linearly recover each of the

$$k = 2m_1 + 2m_2 + 2$$

components of its demanded message vector as shown below.

For each $i = 1, 2, \ldots, m_1$, the left-hand-side receivers can linearly recover their demands as follows:

$$\begin{aligned} R_0^{(1)}: \quad & \left[e^{(1)}\right]_l - \left[e_0^{(1)}\right]_l = [z]_l \quad (l = 1, 2, \ldots, k) \\ R_i^{(1)}: \quad & \left[e^{(1)}\right]_{k+1} - \left[e_i^{(1)}\right]_i = \left[x_i^{(1)}\right]_i \\ & \left[e^{(1)}\right]_l - \left[e_i^{(1)}\right]_l = \left[x_i^{(1)}\right]_l \quad \begin{pmatrix} l = 1, 2, \ldots, k \\ \text{and } \ l \neq i \end{pmatrix}. \end{aligned}$$

For each $i = 1, 2, \ldots, m_2$, the right-hand-side receivers can linearly recover their demands as follows:

$$\begin{aligned} R_0^{(2)}: \quad & \left[e^{(2)}\right]_l - \left[e_0^{(2)}\right]_l = [z]_l \quad (l = 1, 2, \ldots, k) \\ R_i^{(2)}: \quad & \left[e^{(2)}\right]_{k+1} - \left[e_i^{(2)}\right]_{\delta+i} = \left[x_i^{(2)}\right]_{\delta+i} \\ & \left[e^{(2)}\right]_l - \left[e_i^{(2)}\right]_l = \left[x_i^{(2)}\right]_l \quad \begin{pmatrix} l = 1, 2, \ldots, k \\ \text{and } l \neq \delta + i \end{pmatrix}. \end{aligned}$$

The shared receiver can recover z as follows:

$$\begin{aligned} R_z: \quad & -2\left[e_0^{(1)}\right]_l - \sum_{\substack{i=1 \\ i \neq l}}^{m_1} \left[e_i^{(1)}\right]_l \quad (l = 1, 2, \ldots, m_1) \\ & = [z]_l \quad [\text{from (142)}] \\ & \left[e_1^{(1)}\right]_1 - \left[e_0^{(1)}\right]_{k+1} = [z]_{m_1+1} \\ & \left[e_{l-m_1-1}^{(1)}\right]_{k+1} = [z]_l \quad (l = m_1 + 2, \ldots, 2m_1 + 1) \\ & \left[e_{l-2m_1-1}^{(2)}\right]_{k+1} = [z]_l \quad (l = 2m_1 + 2, \ldots, \delta - 1) \\ & \left[e_1^{(2)}\right]_{\delta+1} - \left[e_0^{(2)}\right]_{k+1} = [z]_\delta \\ & -2\left[e_0^{(2)}\right]_l - \sum_{\substack{i=1 \\ i \neq l-\delta}}^{m_2} \left[e_i^{(2)}\right]_l \quad (l = \delta + 1, \ldots, k) \\ & = [z]_l \quad [\text{from (143)}]. \end{aligned}$$

Thus the code is, in fact, a linear solution for $\mathcal{N}_3(m_1, m_2)$. ■

REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] A. Blasiak, R. Kleinberg, and E. Lubetzky, "Lexicographic products and the power of non-linear network coding," in *Proc. IEEE Symp. Found. Comput. Sci. (FOCS)*, Oct. 2011, pp. 609–618.

[3] K. Cai and G. Han, "On the solvability of three-pair networks with common bottleneck links," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2014, pp. 546–550.

[4] J. Cannons, R. Dougherty, C. Freiling, and K. Zeger, "Network routing capacity," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 777–788, Mar. 2006.

[5] T. Chan and A. Grant, "Dualities between entropy functions and network codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4470–4487, Oct. 2008.

[6] N. Das and B. K. Rai, "On the message dimensions of vector linearly solvable networks," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1701–1704, Sep. 2016.

[7] R. Dougherty, C. Freiling, and K. Zeger, "Insufficiency of linear coding in network information flow," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2745–2759, Aug. 2005.

[8] R. Dougherty, C. Freiling, and K. Zeger, "Linear network codes and systems of polynomial equations," *IEEE Trans. Inf. 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 Trans. Inf. Theory*, vol. 50, no. 10, pp. 2243–2256, Oct. 2004.

[10] R. Dougherty, C. Freiling, and K. Zeger, "Networks, matroids, and non-Shannon information inequalities," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 1949–1969, Jun. 2007.

[11] R. Dougherty, C. Freiling, and K. Zeger, "Unachievability of network coding capacity," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2365–2372, Jun. 2006.

[12] D. Dummit and R. Foote, *Abstract Algebra*, 3rd ed. Hoboken, NJ, USA: Wiley, 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 Trans. Inf. Theory*, vol. 56, no. 7, pp. 3187–3195, Jul. 2010.
[14] T. Etzion and A. Wachter-Zeh, "Vector network coding based on subspace codes outperforms scalar linear network coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 1949–1953.
[15] M. Feder, D. Ron, and A. Tavory, "Bounds on linear codes for network multicast," in *Proc. Electron. Colloq. Comput. Complex. (ECCC)*, 2003, pp. 1–9.
[16] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.
[17] R. Koetter, presentation at the Int. Symp. Modeling Optim. Mobile, Ad Hoc, Wireless Netw. (WiOpt), Mar./Apr. 2008.
[18] P. Krishnan and B. S. Rajan, "A matroidal framework for network-error correcting codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 836–872, Feb. 2015.
[19] F. Kschischang, "An introduction to network coding," in *Network Coding: Fundamentals and Applications*, M. Médard and A. Sprintson, Eds. San Diego, CA, USA: Academic, 2012, ch. 1.
[20] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.
[21] M. Médard, M. Effros, T. Ho, and D. Karger, "On coding for non-multicast networks," in *Proc. Conf. Commun. Control Comput.*, Monticello, IL, USA, Oct. 2003, pp. 1–9.
[22] V. Muralidharan and B. Rajan, "Linear network coding, linear index coding and representable discrete polymatroids," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 4096–4119, Jul. 2016.
[23] B. K. Rai and B. K. Dey, "On network coding for sum-networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 50–63, Jan. 2012.
[24] A. Rasala Lehman and E. Lehman, "Complexity classification of network information flow problems," in *Proc. ACM-SIAM Symp. Discrete Algorithms*, 2004, pp. 142–150.
[25] S. Riis, "Linear versus non-linear Boolean functions in network flow," in *Proc. Conf. Inf. Sci. Syst. (CISS)*, Princeton, NJ, USA, Mar. 2004.
[26] G. Robin, "Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction ω(n) nombre de diviseurs premiers de n," (in French), *Acta Arithmetica*, vol. 42, no. 4, pp. 367–389, 1983.
[27] J. Sándor, D. S. Mitrinović, and B. Crstici, *Handbook of Number Theory I*. The Netherlands: Springer, 2006.
[28] I. Satake, *Linear Algebra*. New York, NY, USA: Marcel Dekker, 1975.
[29] S. Shenvi and B. K. Dey, "A simple necessary and sufficient condition for the double unicast problem," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2010, pp. 1–5.
[30] A. T. Subramanian and A. Thangaraj, "Path gain algebraic formulation for the scalar linear network coding problem," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4520–4531, Sep. 2010.
[31] Q. Sun, X. Yang, K. Long, X. Yin, and Z. Li, "On vector linear solvability of multicast networks," *IEEE Trans. Commun.*, Sep. 2016. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7575624
[32] Q. T. Sun, S.-Y. R. Li, and C. Chan, "Matroidal characterization of optimal linear network codes over cyclic networks," *IEEE Commun. Lett.*, vol. 17, no. 10, pp. 1992–1995, Oct. 2013.
[33] Q. Sun, X. Yin, Z. Li, and K. Long, "Multicast network coding and field sizes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6182–6191, Nov. 2015.
[34] C. Yuan and H. Kan, "A characterization of solvability for a class of networks," *Sci. China Inf. Sci.*, vol. 55, no. 4, pp. 747–754, Apr. 2012.
[35] C. Yuan, H. Kan, X. Wang, and H. Imai, "A construction method of matroidal networks," *Sci. China Inf. Sci.*, vol. 55, no. 11, pp. 2445–2453, 2012.

Joseph Connelly (S'12) was born in Milwaukee, and he received a Bachelor's degree in electrical and computer engineering from the University of Minnesota Twin Cities in 2013. He received an M.S. degree in 2016 and is currently pursuing a Ph.D. in electrical and computer engineering at the University of California, San Diego, where he is advised by Kenneth Zeger.

Kenneth Zeger (S'85–M'90–SM'95–F'00) was born in Boston in 1963. He received both the S.B. and S.M. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology in 1984, and both the M.A. degree in mathematics and the Ph.D. in electrical engineering at the University of California, Santa Barbara, in 1989 and 1990, respectively. He was an Assistant Professor of Electrical Engineering at the University of Hawaii from 1990 to 1992. He was in the Department of Electrical and Computer Engineering and the Coordinated Science Laboratory at the University of Illinois at Urbana-Champaign, as an Assistant Professor from 1992 to 1995, and as an Associate Professor from 1995 to 1996. He has been in the Department of Electrical and Computer Engineering at the University of California at San Diego, as an Associate Professor from 1996 to 1998, and as a Professor from 1998 to present. He received an NSF Presidential Young Investigator Award in 1991. He served as Associate Editor At-Large for the IEEE TRANSACTIONS ON INFORMATION THEORY during 1995-1998, as a member of the Board of Governors of the IEEE Information Theory Society during 1998-2000, 2005-2007, and 2008-2010, and is an IEEE Fellow.