Linear Network Coding Over Rings – Part II: Vector Codes and Non-Commutative Alphabets

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

***Abstract*— In Part I, we studied linear network coding over finite commutative rings and made comparisons to the well-studied case of linear network coding over finite fields. Here, we consider the more general setting of linear network coding over finite (possibly non-commutative) rings and modules. We prove the following results regarding the linear solvability of directed acyclic networks over various finite alphabets. For any network, the following are equivalent: (i) vector linear solvability over some field, (ii) scalar linear solvability over some ring, and (iii) linear solvability over some module. Analogously, the following are equivalent: (a) scalar linear solvability over some field, (b) scalar linear solvability over some commutative ring, and (c) linear solvability over some module whose ring is commutative. Whenever any network is linearly solvable over a module, a smallest such module arises in a vector linear solution for that network over a field. If a network is scalar linearly solvable over some non-commutative ring but not over any commutative ring, then such a non-commutative ring must have size at least 16, and for some networks, this bound is achieved. An infinite family of networks is demonstrated, each of which is scalar linearly solvable over some non-commutative ring but not over any commutative ring. Whenever p is prime and $1 \leq k \leq 6$, if a network is scalar linearly solvable over some ring of size p^k, then it is also k-dimensional vector linearly solvable over the field GF(p), but the converse does not necessarily hold. This result is extended to all $k \geq 1$ when the ring is commutative.**

***Index Terms*— Linear coding, network solvability, network coding, modules (abstract algebra).**

I. Introduction

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

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

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

A. Linear Codes Over Modules

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

Definition I.1: An *R-module* (specifically a left R-module) is an Abelian group [1] $(G, \oplus)$ together with a ring [2] $(R, +, *)$ of *scalars* 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:

$$\begin{aligned} r \cdot \ (g \oplus h) &= (r \cdot g) \oplus \ (r \cdot h) \\ (r + s) \cdot g &= (r \cdot g) \oplus \ (s \cdot g) \\ (r * s) \cdot g &= r \cdot \ (s \cdot g) \\ 1 \cdot g &= g. \end{aligned}$$

Manuscript received August 8, 2016; revised February 7, 2017; accepted April 8, 2017. Date of publication April 24, 2017; date of current version December 20, 2017. This work was supported by the National Science Foundation.

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).

Communicated by P. Sadeghi, Associate Editor for Coding Techniques.
Digital Object Identifier 10.1109/TIT.2017.2697422

[1] In this paper, we consider network codes over finite alphabets, so we assume that all groups are finite, even when not explicitly stated.

[2] We also assume that all rings have a multiplicative identity, and in Section IV-B, we briefly mention why we do not consider linear coding over rings without identity.

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

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

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

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

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

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

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

For basic network coding definitions, see Part I [2, Sec. I-A]. We will use the same models as in Part I for networks, alphabets, etc., except we now study the generalized case of linear codes over modules, as opposed to restricting to linear codes over rings. An edge function on the out-edge of a network node is *linear with respect to the module* ${}_RG$ if it can be written in the form

$$f(x_1, \ldots, x_m) = (C_1 \cdot x_1) \oplus \cdots \oplus (C_m \cdot x_m) \qquad (1)$$

where $x_1, \ldots, x_m \in G$ are the inputs of the node and $C_1, \ldots, C_m \in R$ are constants. That is, the messages and edge symbols are elements of the Abelian group G, and the linear edge and decoding functions are determined by coefficients of the ring R. A decoding function is linear with respect to ${}_RG$ if it has a form analogous to (1), and a code is *linear over a module* ${}_RG$ if all edge and decoding functions are linear with respect to ${}_RG$. The alphabet size in a linear code over a module is the size of the module, i.e. $|G|$.

For any ring R, we denote its additive (Abelian) group by $(R, +)$. The special case of a module where the finite ring R acts on its own additive group $(R, +)$ by multiplication in R is denoted by ${}_RR$, and in this case, (1) is equivalent to the definition of a scalar linear code over a ring that we used in Part I.

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

(i) A *scalar linear code over a ring* R is a linear code over the module ${}_RR$. A network is *scalar linearly solvable over* R if it has a linear solution over the module ${}_RR$.

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

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

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

B. Our Contributions

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

Section II analyzes the linear solvability of networks over ring alphabets which are not necessarily commutative. In Part I, we proved that whenever a network is scalar linearly solvable over some commutative ring, then the smallest commutative ring over which the network is scalar linearly solvable is a field (and thus the ring is unique) [2, Th. II.10]. Here, we prove (in Theorem II.5) that if a network is scalar linearly solvable over some (not necessarily commutative) ring, then a smallest such ring is a matrix ring over a field. It remains unknown, however, whether there can be more than one smallest (not necessarily commutative) ring over which a network is linearly solvable, since in general, there can exist multiple matrix rings over fields that are the same size. We demonstrate (in Corollaries II.14 and III.8) that for two infinite classes of networks studied in this paper, the smallest size ring over which each network is linearly solvable is indeed unique.

We prove (in Theorem II.10) that if a network is linearly solvable over some module, then a smallest such module (i.e. with a smallest associated Abelian group) corresponds to a vector linear solution over some finite field.[3] We prove (in Theorem II.13), in contrast to the commutative ring case, that the minimum size module with respect to linear solvability is not necessarily unique. Thus, for a fixed network, vector linear codes over fields are "best" in a certain sense, as these codes can minimize the alphabet size needed for a linear solution.

We also show (in Corollary II.15) that for all networks, the following properties are equivalent: (i) vector linear solvability over some field, (ii) scalar linear solvability over some ring, and (iii) linear solvability over some module. Similarly, we show (in Corollary II.16) that for all networks, the following properties are equivalent: (a) scalar linear solvability over some field, (b) scalar linear solvability over some commutative ring, and (c) linear solvability over some module whose ring is commutative.

[3]For example, in a k-dimensional vector linear code over a field $\mathbb{F}$, the alphabet size of the module is $|\mathbb{F}|^k$.

In Section III, we present a family of networks that generalize the M Network of [8] and [16], and we enumerate (in Theorem III.6) the particular vector dimensions over which each of these networks has vector linear solutions. A similar result was obtained by Das and Rai [5]. We prove (in Corollary III.7) that these networks have scalar linear solutions over certain non-commutative matrix rings yet do not have scalar linear solutions over any commutative ring. We also show (in Theorem III.10) that if a network is scalar linearly solvable over a non-commutative ring R and is not scalar linearly solvable over any commutative ring, then $|R| \geq 16$. This lower bound is shown to be achievable (in Corollary III.7 and Example III.9) by exhibiting a network which has a scalar linear solution over a non-commutative ring of size 16 but not over any commutative ring.

Section IV focuses on linear solvability of networks over different modules with the same alphabet size, specifically, k-dimensional vector codes over GF(p) and scalar codes over rings of size p^k. We prove (in Theorem IV.1) that for each prime power p^k, there exists a network with a linear solution over a module of size p^k but with no scalar linear solutions over any ring of size p^k. These particular networks have k-dimensional vector linear solutions over GF(p). Using a result of Sun et al. [18], we also show (in Corollary IV.3) that there exists a class of multicast networks with similar properties.

On the other hand, we show (in Theorem IV.6) that any network with a scalar linear solution over a commutative ring of size p^k has a k-dimensional vector linear solution over GF(p). We prove a similar result (in Theorem IV.17) for general rings of size p^k when $k \leq 6$. In this sense, k-dimensional vector linear codes over GF(p) are better than any scalar linear code over a ring of size p^k. Additionally, we show (in Theorems IV.6 and IV.17) that these results generalize in a natural way to rings of non-power-of-prime sizes.

C. Comparisons of Modules

If G is a $\mathbf{Z}$-module, then as a consequence of Lagrange's theorem of finite groups,

$$(n|G|) \cdot g = 0$$

for all $g \in G$ and all $n \in \mathbf{Z}$. In other words, there are multiple elements of $\mathbf{Z}$ that act on G in the same way. Modules in which every element of the ring acts on G in a different way will be frequently discussed in this paper.

Definition I.2: An R-module G is *faithful* if for each $r \in R\backslash\{0\}$, there exists $g \in G$ such that $r \cdot g \neq 0$.

Equivalently, $r \cdot g = 0$ for all g if and only if $r = 0$. For any finite ring R and positive integer k, the $M_k(R)$-module R^k is faithful, so vector and scalar linear codes over rings are special cases of linear codes over faithful modules.

On the other hand, it can be verified that the ring $\mathbf{Z}_6$ of integers mod 6, acts on the additive group $(\mathbf{Z}_2, \oplus)$ of integers mod 2, where the action is multiplication modulo 2. For each $a = 0, 1$, we have

$$0 = 2a = 4a \mod 2$$

so the $\mathbf{Z}_6$-module $(\mathbf{Z}_2, \oplus)$ is not faithful.

For a fixed ring R, there are generally multiple modules over R. For example, if R is a subring of S, then $(S, +)$ is an R-module where the action is multiplication in S, and $(R, +)$ is also an R-module where the action is multiplication in R. The following lemma shows that the linear solvability of a network over a faithful R-module is determined entirely by the ring of scalars R and not by the module's underlying Abelian group.

However, we note that not every ring and group pair can form a module. For example, the additive group of GF(2) cannot be a GF(3)-module. If $(\mathrm{GF}(2), \oplus)$ were a GF(3)-module, then we would have

$$\begin{aligned} 0 &= 0 \cdot 1 = (1 + 1 + 1) \cdot 1 \\ &= (1 \cdot 1) \oplus (1 \cdot 1) \oplus (1 \cdot 1) = 1 \oplus 1 \oplus 1 = 1 \end{aligned}$$

but $0 \neq 1$ in GF(2).

Lemma I.3: Let R be a fixed ring. If a network is linearly solvable over some faithful R-module, then it is linearly solvable over every R-module.

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

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

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

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

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

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

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

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

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

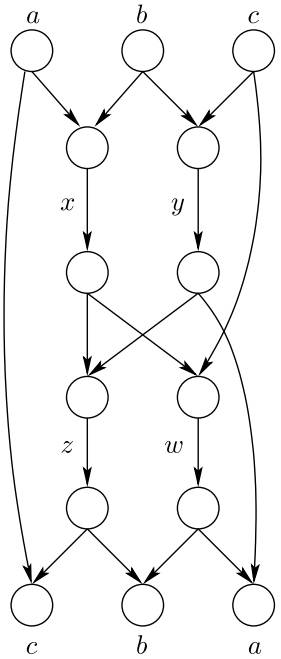

Fig. 1. The Fano Network is constructed from the Fano matroid [8].

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

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

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

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

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

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

In contrast to Lemma I.3, if G is both an R-module and an S-module, then there may exist a network that is linearly solvable over ${}_S G$ but not ${}_R G$. For example, when

$$G = (\mathrm{GF}(4), +), \ R = \mathrm{GF}(2), \quad \text{and } S = \mathrm{GF}(4).$$

GF(2) is a subfield of GF(4), so G is both a faithful R-module and a faithful S-module. We demonstrate (in Corollary II.14) a network that is scalar linearly solvable over GF(4) but not GF(2), and by Lemma I.3, this network is linearly solvable over ${}_S G$ but not ${}_R G$.

The *Fano Network* is given in Figure 1 and has been used to show numerous interesting properties of network coding. The following example illustrates the importance of the premise in Lemma I.3 by demonstrating that the Fano Network has a linear solution over an unfaithful $\mathbf{Z}_6$-module yet has no linear solutions over another $\mathbf{Z}_6$-module.

Example I.4: The Fano Network has a linear solution over the unfaithful $\mathbf{Z}_6$-module $(\mathbf{Z}_2, \oplus)$ but not the faithful $\mathbf{Z}_6$-module $(\mathbf{Z}_6, +)$.

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

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

$$\begin{aligned} x &= a \oplus b \\ y &= b \oplus c \\ z &= x \oplus y \\ w &= x \oplus c. \end{aligned}$$

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

$$\begin{aligned} z \oplus a &= c \\ z \oplus w &= b \\ w \oplus y &= a. \end{aligned}$$

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

If we take the linear code given in Example I.4 to be over the $\mathbf{Z}_6$-module $(\mathbf{Z}_6, +)$, i.e., the same linear combinations of inputs in a scalar linear code over $\mathbf{Z}_6$, then

$$\begin{aligned} x &= a + b \\ y &= b + c \\ z &= x + y \end{aligned}$$

and

$$z + a = 2a + 2b + c \neq c$$

so clearly this code is not a solution when taken over the $\mathbf{Z}_6$-module $\mathbf{Z}_6$, which agrees with the result from [7].

If R is any ring such that $(\mathbf{Z}_2, \oplus)$ is an R-module, then the linear solution for the Fano Network in Example I.4 is a linear solution over the R-module $(\mathbf{Z}_2, \oplus)$. For example, for each positive integer n, $(\mathbf{Z}_2, \oplus)$ is a $\mathbf{Z}_{2n}$-module where the action is multiplication modulo 2.

In fact, whenever n and m are positive integers, the ring $\mathbf{Z}_{nm}$ acts on $(\mathbf{Z}_m, +)$ by multiplication modulo m. Such a module is faithful when $n = 1$ and is unfaithful otherwise. So if a network has a scalar linear solution over $\mathbf{Z}_{nm}$, which is equivalent to a linear solution over the faithful $\mathbf{Z}_{nm}$-module $(\mathbf{Z}_{nm}, +)$, then the network also has a linear solution over the (possibly unfaithful) $\mathbf{Z}_{nm}$-module $(\mathbf{Z}_n, \oplus)$. Although, as demonstrated in Example I.4, the converse may not be true.

While these trivial examples may not seem particularly useful, Corollary I.5 demonstrates an important special case of Lemma I.3 which will be used frequently in later proofs.

It demonstrates an equivalence between scalar linear solutions over matrix rings and vector linear solutions over rings.

Corollary I.5: Let R be a finite ring, k a positive integer, and $\mathcal{N}$ a network. Then $\mathcal{N}$ is scalar linearly solvable over the ring of $k \times k$ matrices whose elements are from R if and only if $\mathcal{N}$ has a k-dimensional vector linear solution over R.

Proof: The "if" and the "only if" directions are each obtained by separately applying Lemma I.3, since $M_k(R)$ and R^k are faithful $M_k(R)$-modules with matrix-matrix multiplication and matrix-vector multiplication, respectively. □

Note that in a k-dimensional vector linear code over a ring R, the alphabet size is $|R|^k$, whereas in a scalar linear solution over $M_k(R)$, the alphabet size is $|R|^{k^2}$. So any network that is scalar linearly solvable over the matrix ring $M_k(R)$ is also linearly solvable over a smaller module alphabet. We will generalize this idea in Theorem II.10.

As is common in mathematics literature, it will be assumed throughout this paper that ring homomorphisms preserve both additive and multiplicative identities.

Lemma I.6: If $\phi : R \to S$ is a ring homomorphism and network $\mathcal{N}$ is linearly solvable over some faithful R-module, then $\mathcal{N}$ is linearly solvable over every S-module.

Proof: Let H be an S-module and define a mapping

$$\odot : R \times H \to H$$

by $r \odot h = \phi(r) \cdot h$, where $\cdot$ is the action of ${}_SH$. One can verify that H is an R-module under $\odot$. Now, let G be a faithful R-module, and suppose $\mathcal{N}$ has a linear solution over ${}_RG$. By Lemma I.3, $\mathcal{N}$ is linearly solvable over ${}_RH$, so every output $y' \in H$ in the solution over ${}_RH$ is of the form

$$y' = (C_1 \odot x_1) \oplus \cdots \oplus (C_m \odot x_m) \tag{2}$$

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

Form a linear code for $\mathcal{N}$ over ${}_SH$ by replacing each coefficient C_i in (2) by $\phi(C_i)$. Let $y \in H$ be the output in the code over ${}_SH$ corresponding to y' in the code over ${}_RH$. Then

$$\begin{aligned} y &= (\phi(C_1) \cdot x_1) \oplus \cdots \oplus \ (\phi(C_m) \cdot x_m) \\ &= (C_1 \odot x_1) \oplus \cdots \oplus \ (C_m \odot x_m) = y'. \end{aligned}$$

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

Corollary I.7 was also shown in Part I as Lemma II.5. However, Corollary I.7 can also be viewed as a special case of Lemma I.6.

Corollary I.7: Let R and S be finite rings. If there exists a ring homomorphism from R to S, then every network that is scalar linearly solvable over R is also scalar linearly solvable over S.

Proof: $(R, +)$ is a faithful R-module for any finite ring R, so this is a special case of Lemma I.6 where the modules are ${}_RR$ and ${}_SS$. □

For finite rings R and S, special cases of Corollary I.7 include:

(1) R is a subring of S:
The identity mapping is an injective homomorphism from R to S, so any network that is scalar linearly solvable over R is also scalar linearly solvable over S.

(2) R has a two-sided ideal I:
There is a surjective homomorphism from R to R/I (see Lemma II.2), so any network that is scalar linearly solvable over R is also scalar linearly solvable over R/I.

(3) $\phi : R \times S \to R$ is the projection mapping:
ϕ is a surjective homomorphism, so any network that is scalar linearly solvable over $R \times S$ is also scalar linearly solvable over R (and likewise over S).

Cases (1), (2), and (3) agree with Corollaries II.6 and II.9 and Lemma II.12, respectively, from Part I.

II. Commutative and Non-Commutative Rings

In this section, we will focus on linear codes over modules whose ring acts on its own Abelian group, i.e. scalar linear codes over rings. As noted after Corollary I.7, for any two-sided ideal I of a finite ring R, every network that is scalar linearly solvable over R is also scalar linearly solvable over R/I, so in determining the smallest ring over which a network is scalar linearly solvable, it is natural to focus attention on rings without two-sided ideals.

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

Lemma II.1: A finite ring is simple if and only if it is isomorphic to a matrix ring over a field.

Proof: This is a corollary of the Artin-Wedderburn theorem (e.g. [14, p. 36, Th. 3.10 (4)] and [15, p. 20, Th. II.9]). □

Lemma II.2 [9, Th. 7, p. 243]: If I is a two-sided ideal of ring R, then the mapping $\phi : R \to R/I$ given by $\phi(x) = x + I$ is a surjective homomorphism.

Lemma II.3: For each finite ring R, there exists a simple ring S such that the following hold:

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

Proof: If R is a simple ring, then each statement is trivially true by taking $S = R$, so we may assume R is not a simple ring. Thus, R has a proper maximal two-sided ideal I. Let $S = R/I$, and note that since I is maximal, S is simple. The mapping $\phi : R \to R/I$ given by $\phi(x) = x + I$ is a surjective homomorphism by Lemma II.2, which proves (a). Hence by Corollary I.7, any network that is scalar linearly solvable over R is also scalar linearly solvable over S, which proves (b). Since R is finite, we know that $|R/I|$ divides $|R|$, which proves (c). □

If R is a finite commutative ring and S is a simple ring satisfying (a)-(c) in Lemma II.3, then S must also be commutative, since there is a surjective homomorphism from R to S. However, as we demonstrate in the following example, if R is non-commutative, then such an S is not necessarily non-commutative.

Example II.4: The following demonstrates: (i) a class of non-commutative rings for which the simple ring in Lemma II.3 is non-commutative, and (ii) a class of non-commutative rings for which the simple ring in Lemma II.3 is commutative.

(i) *For any positive integers k, n, and prime divisor p of n, there exists a surjective homomorphism from the non-commutative ring $M_k(\mathbf{Z}_n)$ to the non-commutative simple ring $M_k(\mathbf{Z}_p)$, given by matrix-component-wise reduction mod p.*

(ii) *For each field $\mathbb{F}$ and integer $k \geq 2$, there exists a surjective homomorphism from the non-commutative ring of upper triangular $k \times k$ matrices with entries in $\mathbb{F}$ to the commutative simple ring $\mathbb{F}$ (see the proof of Lemma IV.10).*

The following theorem demonstrates that any smallest ring over which a network is scalar linearly solvable is simple.

Theorem II.5: If a network is scalar linearly solvable over a ring R but not over any smaller ring, then R is a matrix ring over a field.

Proof: Suppose a network $\mathcal{N}$ is scalar linearly solvable over a ring R that is not simple. By Lemma II.3 (a) (b), there exists a simple ring S and a surjective homomorphism $\phi : R \to S$, such that $\mathcal{N}$ is scalar linearly solvable over S. Since ϕ is surjective, $|R| \geq |S|$, but since S is simple and R is not, the two rings cannot be isomorphic, so $|R| \neq |S|$, and therefore $|R| > |S|$.

This proves that every smallest size ring over which $\mathcal{N}$ is scalar linearly solvable must be simple, which implies that such a ring is a matrix ring over a field by Lemma II.1. □

In Part I [2, Th. II.10], we showed that the smallest-size commutative ring over which a network is scalar linearly solvable is unique. However, there may exist multiple simple rings of the same size. For example, $\mathrm{GF}(p^4)$ and $M_2(\mathrm{GF}(p))$ are non-isomorphic simple rings of size p^4. An interesting open question is whether every network with a scalar linear solution over multiple simple rings of the same size also must have a scalar linear solution over some smaller simple ring. I.e. is the smallest ring R in Theorem II.5 unique for a given network?

We demonstrate (in Corollaries II.14 and III.8) that for two infinite classes of networks (one of which is a class of multicast networks) studied in this paper, the smallest-size ring over which each network is scalar linearly solvable is unique.

A. Modules and Vector Linear Codes

In a linear network code over a module ${}_RG$, in principle, the ring R need not be finite (although representing linear code coefficients might be problematic). However, in a linear network code over a module, the alphabet is finite, so the Abelian group G must be finite.[4] The following lemma and corollary show that linear solutions over unfaithful modules (whose ring may be infinite) admit linear solutions over faithful modules (whose ring is finite).

Lemma II.6: Let G be an R-module. There exists a finite ring S such that G is a faithful S-module, and any network that is linearly solvable over ${}_RG$ is linearly solvable over ${}_SG$.

Proof: We use ideas from [6, p. 2750] here. Let

$$J = \{r \in R \ : \ r \cdot g = 0, \ \forall g \in G\}$$

which is easily verified to be a two-sided ideal of R. Let $S = R/J$. It can also be verified that G is an S-module with action $\odot : S \times G \to G$ given by

$$(r + J) \odot g = r \cdot g.$$

If $(r + J), (s + J) \in S$ are such that

$$(r + J) \odot g = (s + J) \odot g$$

for all $g \in G$, then $(r - s) \cdot g = 0$, which implies $(r - s) \in J$. Hence $(r + J) = (s + J)$, so the ring S acts faithfully on G. A faithful module requires different elements of the ring to yield different functions when acting on elements of the group. Since G is finite, the number of such functions must be finite, which implies the ring S must also be finite.

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

$$y' = (C_1 \cdot x_1) \oplus \cdots \oplus (C_m \cdot x_m) \tag{3}$$

where the x_i's are the parent node's inputs and the C_i's are constants from R. Form a linear code over ${}_SG$ replacing each coefficient C_i in (3) by $(C_i + J)$. Let y be the edge symbol in the code over ${}_SG$ corresponding to y' in the code over ${}_RG$. Then

$$\begin{aligned} y &= ((C_1 + J) \odot x_1) \oplus \cdots \oplus \ ((C_m + J) \odot x_m) \\ &= (C_1 \cdot x_1) \oplus \cdots \oplus \ (C_m \cdot x_m) = y'. \end{aligned}$$

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

Corollary II.7: Let G be an R-module such that R is commutative. There exists a finite commutative ring S such that G is a faithful S-module, and any network that is linearly solvable over ${}_RG$ is linearly solvable over ${}_SG$.

Proof: This proof is identical to the proof of Lemma II.6. However, since R is commutative, the ring $S = R/J$ is also commutative. □

A *submodule* of an R-module G is a subgroup H of G such that H is closed when acted on by R. That is, both H and G are R-modules and $H \subseteq G$. Submodules are of particular interest, since by Lemma I.3, if G and H are faithful

[4] We will call a module "finite" if and only if its Abelian group is finite.

R-modules, then the set of networks that are linearly solvable over ${}_RG$ and the set of networks that are linearly solvable over ${}_RH$ are equal, yet a linear code over ${}_RH$ has a smaller alphabet if H is a proper submodule of G.

As an example, let I be a two-sided ideal in the ring R. Then $(I,+)$ is a subgroup of $(R,+)$ that is closed under multiplication in R, so ${}_RI$ is a submodule of the R-module R. As another example, for each finite field $\mathbb{F}$ and integer $k \geq 2$, the $M_k(\mathbb{F})$-module $\mathbb{F}^k$ is a proper submodule of the $M_k(\mathbb{F})$-module $M_k(\mathbb{F})$.

Lemmas II.8 and II.9 show results related to submodules that will be used to prove Theorem II.10.

Lemma II.8 [14, Th. 3.3 (2), p. 31]: Let $\mathbb{F}$ be a finite field and k a positive integer. Then $\mathbb{F}^k$ is the only $M_k(\mathbb{F})$-module that has no proper submodules.

By Lemma I.3, for each ring R, if a network is linearly solvable over a faithful R-module, then it is linearly solvable over every R-module. When a network is solvable over the R-modules for a particular ring R, it may be desirable for linear network coding to determine the minimum-size R-modules. Lemma II.9 considers this question for rings of matrices over a finite field.

Lemma II.9: Let $\mathbb{F}$ be a finite field and k a positive integer. If G is a finite non-zero $M_k(\mathbb{F})$-module, then $|\mathbb{F}|^k$ divides $|G|$.

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

The following theorem is a generalization of Theorem II.5, where we characterize smallest-size modules over which networks are linearly solvable. Theorem II.10 demonstrates that if a network is linearly solvable over some module, then there exists a vector linear code over a field that minimizes the alphabet size needed for a linear solution.

Theorem II.10: Suppose a network $\mathcal{N}$ is linearly solvable over an R-module G. Then the following hold:

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

Proof: If the ring R is infinite, then by Lemma II.6, $\mathcal{N}$ is linearly solvable over some faithful module with a finite ring. If R is commutative, then by Corollary II.7, $\mathcal{N}$ is linearly solvable over some faithful module with a finite commutative ring. So without loss of generality, assume R is finite and G is a faithful R-module. By Lemmas II.1 and II.3 (a), since R is finite, there exists a field $\mathbb{F}$, a positive integer k, and a surjective homomorphism $\phi : R \to M_k(\mathbb{F})$. By Lemma I.6 any network that is linearly solvable over the faithful R-module G is also linearly solvable over every $M_k(\mathbb{F})$-module, so in particular, $\mathcal{N}$ has a k-dimensional vector linear solution over $\mathbb{F}$. Since ϕ is a homomorphism, any R-module is also an $M_k(\mathbb{F})$-module (see the proof of Lemma I.6). Thus, both G and $\mathbb{F}^k$ are $M_k(\mathbb{F})$-modules, so by Lemma II.9, it must be the case that $|\mathbb{F}|^k$ divides $|G|$.

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

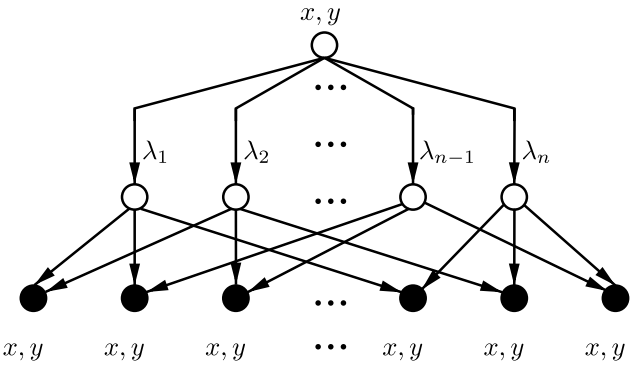

Fig. 2. The n-Choose-Two Network is parameterized by an integer $n \geq 2$. The network's name indicates the number of receivers.

Theorem II.10 demonstrates that, in some sense, vector linear codes over finite fields are optimal for linear network coding, as they can minimize the alphabet size needed for a linear solution. In particular, if G is an R-module that yields a minimum-size linear solution for a network $\mathcal{N}$, then Theorem II.10 implies there exists a field $\mathbb{F}$ and an integer k such that $\mathcal{N}$ has a k-dimensional vector linear solution over $\mathbb{F}$ and $|\mathbb{F}|^k \mid |G|$. Since the linear code over ${}_RG$ yields a minimum-size solution, we must have $|G| = |\mathbb{F}|^k$, so the $M_k(\mathbb{F})$-module $\mathbb{F}^k$ also a yields a minimum-size linear solution.

The following lemmas will be used to show (in Theorem II.13) that a minimum-size module over which a network is linearly solvable is not necessarily unique. Lemma II.11 is a result of Sun et al. [18], and similar results have been shown in, for example, [10].

Lemma II.11 [18, Proposition 1]: Let q be a prime power and k a positive integer. If a network has a scalar linear solution over $\mathrm{GF}(q^k)$, then it has a k-dimensional vector linear solution over $\mathrm{GF}(q)$.

For each integer $n \geq 3$, the *n-Choose-Two Network* is a multicast network given in Figure 2. These networks were described by Rasala Lehman and Lehman [17] and were further studied in our Part I.

Lemma II.12 [17, p. 144]: Let $\mathcal{A}$ be an alphabet and let integer $n \geq 3$.

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

Theorem II.13: For each integer $k \geq 2$ and prime p, the (p^k+1)-Choose-Two Network is linearly solvable over at least two distinct modules of size p^k but not over over any smaller modules.

Proof: By Lemma II.12, the (p^k+1)-Choose-Two Network is scalar linearly solvable over $\mathrm{GF}(p^k)$ and is not solvable over any alphabet whose size is less than p^k. By

Lemma II.11, any network with a scalar linear solution over GF(p^k) has a k-dimensional vector linear solution over GF(p). Hence the (p^k+1)-Choose-Two Network has a scalar linear solution over GF(p^k) and a k-dimensional vector linear solution over GF(p), yet the network has no linear solution over any module whose size is less than p^k. □

The following corollary generalizes Theorem II.16 from Part I, which showed the (p^k+1)-Choose-Two Network is not scalar linearly solvable over any commutative ring of size p^k other than the field GF(p^k). In fact, as a result of Corollary II.14, the (p^k+1)-Choose-Two Network is not scalar linearly solvable over any ring of size p^k other than the field.

Corollary II.14: For each integer $k \geq 2$ and prime p, the unique smallest-size ring over which the (p^k+1)-Choose-Two Network is scalar linearly solvable is GF(p^k).

Proof: By Lemma II.12, the (p^k+1)-Choose-Two Network is scalar linearly solvable over GF(p^k) and is not solvable over any smaller alphabet.

Suppose the (p^k+1)-Choose-Two Network is scalar linearly solvable over a ring R of size p^k. By Lemmas II.1 and II.3 (a) (b), there exists a field $\mathbb{F}$, a positive integer n, and a surjective homomorphism

$$\phi : R \to M_n(\mathbb{F})$$

such that the (p^k+1)-Choose-Two Network is scalar linearly solvable over the ring $M_n(\mathbb{F})$. Since ϕ is surjective,

$$|R| = p^k \geq |\mathbb{F}|^{n^2}.$$

By Corollary I.5, the (p^k+1)-Choose-Two Network has an n-dimensional vector linear solution over $\mathbb{F}$, so by Lemma II.12 (a), $|\mathbb{F}|^n \geq p^k = |R|$. Hence

$$|\mathbb{F}|^n \geq |R| \geq |\mathbb{F}|^{n^2}$$

which implies $n = 1$ and $|\mathbb{F}| = |R| = p^k$. Since $\phi : R \to \mathbb{F}$ is a surjective homomorphism and we have $R \cong \mathbb{F}$, and since $|R| = p^k$, we have $R \cong$ GF(p^k). □

The following corollaries summarize our results on the linear solvability of networks using scalar and linear vector codes over fields, scalar linear codes over rings, and linear codes over modules. Corollary II.15 shows an equivalence between vector linear solvability over fields and linear solvability over rings and modules, while Corollary II.16 shows an equivalence between scalar linear solvability over fields and linear solvability over commutative rings and modules.

Corollary II.15: For any network $\mathcal{N}$, the following three statements are equivalent:

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

Proof: If a network has a k-dimensional vector linear solution over some field $\mathbb{F}$, then by Corollary I.5 it has a scalar linear solution over the ring $M_k(\mathbb{F})$, hence (i) implies (ii). A scalar linear code over a ring is a special case of a linear code over a module, so (ii) implies (iii). By Theorem II.10 (a), (iii) implies (i). □

Corollary II.16: For any network $\mathcal{N}$, the following three statements are equivalent:

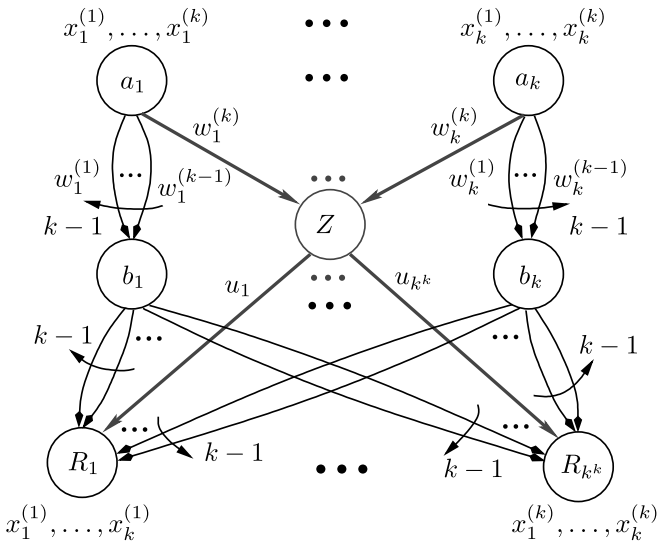

Fig. 3. The Dim-k Network. For each $i = 1, \ldots, k$, the node a_i is a source node that generates messages $x_i^{(1)}, \ldots, x_i^{(k)}$, and a_i has $k-1$ parallel out-edges to node b_i and one out-edge to node Z. For each $j = 1, \ldots, k^k$, the receiver R_j has $k-1$ parallel in-edges from each of the nodes $b_1, \ldots, b_k$ and a single in-edge from node Z. Each receiver demands a single message from each source node and each set of k messages demanded by each receiver is unique; that is, for any $i_1, \ldots, i_k \in \{1, \ldots, k\}$, there is exactly one receiver which demands $x_1^{(i_1)}, \ldots, x_k^{(i_k)}$.

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

Proof: A scalar linear code over a finite field is a special case of a scalar linear code over a commutative ring, hence (i) implies (ii). A scalar linear code over a commutative ring is a special case of a linear code over a module where the ring is commutative, so (ii) implies (iii). By Theorem II.10 (b), (iii) implies (i). □

III. The Dim-k Network

For each integer $k \geq 2$, the *Dim-k Network* is defined in Figure 3 and is referred to as such because it has vector linear solutions precisely over vector dimensions that are multiples of k. We prove this fact in Theorem III.6. This infinite family of networks will be used to demonstrate several theorems related to commutative and non-commutative rings. The special case of $k = 2$ corresponds to the *M Network* of [16], shown later in Figure 4.

Das and Rai [5] presented a class of networks, called the *Generalized M Networks*, which are similar to the Dim-k Networks. They independently proved a result analogous to Theorem III.6, using a more general approach involving matroid theory. We include our proof of Theorem III.6 for completeness.

Remark III.1: The Dim-k Network has $k^k + 2k + 1$ nodes and $k^k\ (k^2 - k + 1) + k^2$ edges.

A *k-dimensional vector routing code over an alphabet $\mathcal{A}$* is a code in which messages and edge symbols are elements of $\mathcal{A}^k$ and edge and decoding functions copy certain input vector

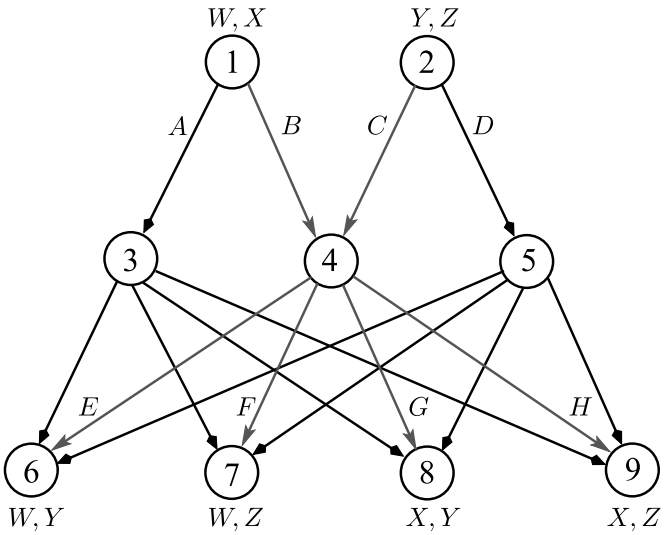

Fig. 4. The M Network has a non-commutative scalar linear solution. The messages W, X, Y, Z take values in $M_2(\mathrm{GF}(2))$. The variables A, B, C, D, E, F, G, H also take values in $M_2(\mathrm{GF}(2))$ and represent the symbols carried on the 8 indicated edges.

components to certain output vector components. A vector routing code over $\mathcal{A}$ is, in fact, a special case of a vector linear code over $\mathcal{A}$ where each row of each of the matrices $C_1, \ldots, C_m$ in (1) is either all zero or else has 1 one and $k-1$ zeros, and for each $i \leq k$, at most one of the matrices $C_1, \ldots, C_m$ has a non-zero ith row.

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

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

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

That is, the lth component of the jth out-edge of the ith source node carries the jth component of the lth message originating at the ith source node.

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

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

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

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

The following lemmas will be used in later proofs, and similar results have been noted in other works, such as [18, Proposition 5] and [10, Example VI.2].

Lemma III.3: Let R be a finite ring and let $k_1, \ldots, k_t$ be positive integers. If a network has $k_1, \ldots, k_t$-dimensional vector linear solutions over R, then the network has a $(k_1 + \cdots + k_t)$-dimensional vector linear solution over R.

Proof: Assume a network has a k_i-dimensional vector linear solution over R for each $i = 1, \ldots, t$. In the k_i-dimensional vector linear solution over R, every edge function is of the form

$$y^{(i)} = C_1^{(i)} x_1^{(i)} + \cdots + C_m^{(i)} x_m^{(i)}$$

where $x_j^{(i)} \in R^{k_i}$ are the inputs to the node and $C_j^{(i)}$ are $k_i \times k_i$ matrices over R. For any such edge function, define a $(k_1 + \cdots + k_t)$-dimensional vector linear edge function over R by letting

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

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

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

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

and the *conditional entropy* of X given Y as

$$H(X|Y) = H(X, Y) - H(Y).$$

The proof of Theorem III.6 will make use of Lemmas III.4 and III.5 and the following basic information inequalities:

$$\begin{aligned} H(X|Y) &\leq H(X) && (4)\\ &\leq H(X, Y) && (5)\\ &\leq H(X) + H(Y). && (6) \end{aligned}$$

Lemma III.4: Let $X, Y_1, \ldots, Y_k$ be collections of discrete random variables. Then

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

Proof:

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

where the inequality follows from (4). □

Lemma III.5 [8, Lemma V.9]: Let $L : \mathbb{F}^m \to \mathbb{F}^n$ be a linear map, and let x be a uniformly distributed random variable on $\mathbb{F}^m$. Then $L(x)$ is uniformly distributed on the range of L, and

the base $|\mathbb{F}|$ entropy of $L(x)$ is $H(L(x)) = \dim(\text{range}(L(x)) \cdot \log|\mathbb{F}|$.

Theorem III.6: For each integer $k \geq 2$ and each field $\mathbb{F}$, the Dim-k Network has an n-dimensional vector linear solution over $\mathbb{F}$ if and only if $k \mid n$.

Proof: Suppose $k \mid n$. Then $n = kt$ for some integer $t \geq 1$. By Lemma III.2, the Dim-k Network has a k-dimensional vector linear solution over $\mathbb{F}$, so by taking $k_1 = \cdots = k_t = k$ in Lemma III.3, the Dim-k Network has an $n = kt$-dimensional vector linear solution over $\mathbb{F}$.

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

$$\mathbf{x_i} = x_i^{(1)}, \ldots, x_i^{(k)}$$
$$\mathbf{w_i} = w_i^{(1)}, \ldots, w_i^{(k-1)}.$$

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

$$H(\mathbf{x_1}, \ldots, \mathbf{x_k}) = \sum_{i,j=1}^{k} H\left(x_i^{(j)}\right). \tag{7}$$

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

$$H(\mathbf{w_i} \mid \mathbf{x_i}) = 0. \tag{8}$$

The receiver R_1 demands the messages $x_1^{(1)}, \ldots, x_k^{(1)}$ and recovers its demands from its in-edges, so

$$H\left(x_1^{(1)}, \ldots, x_k^{(1)} \mid \mathbf{w_1}, \ldots, \mathbf{w_k}, u_1\right) = 0. \tag{9}$$

For each $i, j \in \{1, \ldots, k\}$, the edge symbol $w_i^{(j)}$ is a linear function of only $x_i^{(1)}, \ldots, x_i^{(k)}$, and the network's messages are jointly independent, which implies

$$\begin{aligned}
&\sum_{i=1}^{k} H\left(\mathbf{w_i}, x_i^{(1)}\right) \\
&\quad = H\left(x_1^{(1)}, \ldots, x_k^{(1)}, \mathbf{w_1}, \ldots, \mathbf{w_k}\right) && \text{[from ind.]} \\
&\quad \leq H\left(u_1, x_1^{(1)}, \ldots, x_k^{(1)}, \mathbf{w_1}, \ldots, \mathbf{w_k}\right) && \text{[from (5)]} \\
&\quad = H(u_1, \mathbf{w_1}, \ldots, \mathbf{w_k}) && \text{[from (9)]} \\
&\quad \leq H(u_1) + \sum_{i=1}^{k}\sum_{j=1}^{k-1} H\left(w_i^{(j)}\right) && \text{[from (6)]} \\
&\quad \leq n(1 + k(k-1)).
\end{aligned}$$

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

$$\sum_{j=1}^{k} H\left(\mathbf{w_j}, x_j^{(i_j)}\right) \leq n(k^2 - k + 1). \tag{10}$$

Since

$$\left\{\mathbf{w_1}, w_1^{(k)}, \ldots, \mathbf{w_k}, w_k^{(k)}\right\}$$

is a cut-set for each receiver, we have

$$H\left(\mathbf{x_1}, \ldots, \mathbf{x_k} \mid \mathbf{w_1}, w_1^{(k)}, \ldots, \mathbf{w_k}, w_k^{(k)}\right) = 0. \tag{11}$$

Therefore,

$$\begin{aligned}
nk^2 &= H(\mathbf{x_1}, \ldots, \mathbf{x_k}) && \text{[from (7)]} \\
&\leq H\left(\mathbf{x_1}, \ldots, \mathbf{x_k}, \mathbf{w_1}, w_1^{(k)}, \ldots, \mathbf{w_k}, w_k^{(k)}\right) && \text{[from (5)]} \\
&= H\left(\mathbf{w_1}, w_1^{(k)}, \ldots, \mathbf{w_k}, w_k^{(k)}\right) && \text{[from (11)]} \\
&\leq \sum_{i=1}^{k}\sum_{j=1}^{k} H\left(w_i^{(j)}\right) && \text{[from (6)]} \\
&\leq nk^2 && (12)
\end{aligned}$$

which implies

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

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

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

This implies the bounds in (12) are tight, so

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

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

$$H(\mathbf{w_i}) = n(k-1) \quad (i = 1, \ldots, k). \tag{13}$$

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

$$\begin{aligned}
&\sum_{i=1}^{k} H\left(\mathbf{w_j}, x_j^{(i)}\right) \\
&\quad \geq (k-1)H\left(\mathbf{w_j}\right) + H\left(\mathbf{w_j}, \mathbf{x_j}\right) && \text{[from Lemma III.4]} \\
&\quad = n(k-1)(k-1) + H\left(\mathbf{x_j}\right) && \text{[from (8), (13)]} \\
&\quad = n(k^2 - k + 1) && \text{[from (7)]}. \qquad (14)
\end{aligned}$$

By fixing $i_1 = 1$ and summing over all $i_2, \ldots, i_k$ in (10), we have

$$\begin{aligned}
&k^{k-1} n(k^2 - k + 1) \\
&\quad \overset{(a)}{\geq} \sum_{i_2, \ldots, i_k = 1}^{k} \left(H\left(\mathbf{w_1}, x_1^{(1)}\right) + \sum_{j=2}^{k} H\left(\mathbf{w_j}, x_j^{(i_j)}\right)\right) \\
&\quad = k^{k-1} H\left(\mathbf{w_1}, x_1^{(1)}\right) + k^{k-2} \sum_{j=2}^{k}\sum_{i=1}^{k} H\left(\mathbf{w_j}, x_j^{(i)}\right) \\
&\quad \overset{(b)}{\geq} k^{k-1} H\left(\mathbf{w_1}, x_1^{(1)}\right) + k^{k-2} \sum_{j=2}^{k} n(k^2 - k + 1) \\
&\quad = k^{k-1} H\left(\mathbf{w_1}, x_1^{(1)}\right) + k^{k-2} n(k-1)(k^2 - k + 1)
\end{aligned}$$

where (a) and (b) follow from (10) and (14), respectively. Solving for $H(\mathbf{w_1}, x_1^{(1)})$ in the previous equation yields

$$H\left(\mathbf{w_1}, x_1^{(1)}\right) \leq n\left(\frac{k^2-k+1}{k}\right).$$

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

$$H\left(\mathbf{w_i}, x_i^{(j)}\right) \leq n\left(\frac{k^2-k+1}{k}\right). \tag{15}$$

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

$$\begin{aligned} n\ (k^2-k+1) &\leq \sum_{j=1}^{k} H\left(\mathbf{w_i}, x_i^{(j)}\right) && \text{[from (14)]} \\ &\leq \sum_{j=1}^{k} n\left(\frac{k^2-k+1}{k}\right) && \text{[from (15)]} \\ &= n\,(k^2-k+1) \end{aligned}$$

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

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

The variables $w_i^{(1)}, \ldots, w_i^{(k-1)}, x_i^{(j)}$ are linear functions of the uniformly distributed messages, so by Lemma III.5, $H(\mathbf{w_i}, x_i^{(j)})$ (with logarithms in base $|\mathbb{F}|$) is an integer. However,

$$\begin{aligned} \gcd\left(k, k^2-k+1\right) &= \gcd\left(k, (k^2-k+1)-k(k-1)\right) \\ &= \gcd(k, 1) = 1 \end{aligned}$$

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

A. Insufficiency of Commutative Rings

The following corollary demonstrates it is possible for a network to be scalar linearly solvable over a non-commutative ring but not over any commutative rings, which is, in fact, equivalent to a network being vector linearly solvable over some field but not scalar linearly solvable over any field, by Corollaries II.15 and II.16. This fact agrees with the result of Médard et al. [16], which demonstrate the M Network is vector linearly solvable over fields but not scalar linearly solvable over any field.

Corollary III.7: For all integers $k \geq 2$, $n \geq 1$, and prime p, the Dim-k Network has a scalar linear solution over a non-commutative ring of size p^{nk^2} but has no scalar linear solution over any commutative ring.

Proof: If the Dim-k Network were scalar linearly solvable over a commutative ring, then by Corollary II.16, the Dim-k Network would also be scalar linearly solvable over some finite field. However, by Theorem III.6, the Dim-k Network is not scalar linearly solvable over any finite field.

By Theorem III.6, the Dim-k Network has a k-dimensional vector linear solution over $\mathrm{GF}(p^n)$, so by Corollary I.5 the Dim-k Network has a linear solution over the ring $M_k(\mathrm{GF}(p^n))$. □

Corollary III.8: For each integer $k \geq 2$, the unique smallest-size ring over which the Dim-k Network is scalar linearly solvable is the ring of all $k \times k$ matrices over GF(2).

Proof: By taking $p = 2$ in Corollary III.7, the Dim-k Network has a linear solution over the ring $M_k(\mathrm{GF}(2))$.

Suppose the Dim-k Network is scalar linearly solvable over a ring R such that $|R| \leq 2^{k^2}$. By Lemmas II.1 and II.3 (a) (b) there exists a field $\mathbb{F}$, a positive integer n, and a surjective homomorphism $\phi : R \to M_n(\mathbb{F})$ such that the Dim-k Network is scalar linearly solvable over $M_n(\mathbb{F})$. By Corollary I.5, this implies the Dim-k Network has an n-dimensional vector linear solution over $\mathbb{F}$, which by Theorem III.6, implies k divides n. Since ϕ is surjective, $|M_n(\mathbb{F})| \leq |R|$. Hence we have

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

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

It is interesting to note that, while the smallest-size ring over which the Dim-k Network is scalar linearly solvable has size 2^{k^2}, the Dim-k Network also has a k-dimensional vector linear solution over GF(2), which has alphabet size 2^k. This demonstrates that linear codes over modules can require smaller alphabet sizes than scalar linear codes over rings. This also agrees with Theorem II.10, which showed that vector linear codes over fields minimize the alphabet size needed for a linear solution.

Example III.9: Setting $n = 1$ and $p = k = 2$ in Corollary III.7 results in the M Network (see Figure 4) having no scalar linear solution over any commutative ring but having a scalar linear solution over a non-commutative ring of size 16. *The non-commutative ring $M_2(\mathrm{GF}(2))$ consists of all 2×2 binary matrices under ordinary matrix addition and multiplication mod* 2. *Denote the* 16 *ring elements by:*

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

A scalar linear solution for the M Network over the non-commutative ring $M_2(\mathrm{GF}(2))$ (i.e. where $A, B, C, D, E, F, G, H, W, X, Y, Z \in M_2(\mathrm{GF}(2))$) is given by:

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

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

We also note that if the messages and edge symbols of the M Network are 2*-dimensional vectors over* GF(2)*, instead of* 2×2 *binary matrices, then a small modification of the linear code described above provides the* 2*-dimensional vector linear solution over* GF(2) *given in [16]. This agrees with Corollary I.5.*

The bound in the following theorem is tight via Example III.9.

Theorem III.10: If a network is scalar linearly solvable over some non-commutative ring R, but not over any commutative rings, then $|R| \geq 16$*.*

Proof: Suppose network $\mathcal{N}$ is scalar linearly solvable over some non-commutative ring R but not over any commutative ring. By Theorem II.5, there exists a positive integer k and a field $\mathbb{F}$ such that $\mathcal{N}$ has a scalar linear solution over $M_k(\mathbb{F})$ and $|R| \geq |M_k(\mathbb{F})|$. If $k = 1$, then $\mathcal{N}$ is scalar linearly solvable over a field, which contradicts the assumption that $\mathcal{N}$ is not scalar linearly solvable over any commutative ring. So $k \geq 2$, which implies $|R| \geq |M_k(\mathbb{F})| = |\mathbb{F}|^{k^2} \geq |\mathbb{F}|^4 \geq 2^4 = 16$. □

Suppose R is a non-commutative ring of size p^n, for some prime p. It also follows from the proof of Theorem III.10 that if a network $\mathcal{N}$ is scalar linearly solvable over R, but not over any commutative ring, then $n \geq 4$. In fact, we later show in (Theorem IV.15) that whenever $n \leq 3$, any network with a scalar linear solution over some ring of size p^n must also have a scalar linear solution over the field GF(p^n), which agrees with Theorem III.10.

IV. Modules of the Same Size

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

Theorem IV.1: For each integer $k \geq 2$ *and prime* p*, the Dim-*k *Network has a* k*-dimensional vector linear solution over the field* GF(p) *but is not scalar linearly solvable over any ring of size* p^k*.*

Proof: By Theorem III.6, the Dim-k Network has a k-dimensional vector linear solution over GF(p). Let R be a ring of size p^k and suppose the Dim-k Network has a scalar linear solution over R. By Lemmas II.1 and II.3 (b) (c), there exists a field $\mathbb{F}$ and a positive integer n such that any network that is scalar linearly solvable over R is also scalar linearly solvable over $M_n(\mathbb{F})$ and $|\mathbb{F}|^{n^2}$ divides p^k. Hence $\mathbb{F}$ is a field of characteristic p and $n^2 \leq k$.

Since the Dim-k Network is scalar linearly solvable over R, the Dim-k Network is scalar linearly solvable over the ring $M_n(\mathbb{F})$. By Corollary I.5, this implies the Dim-k Network has an n-dimensional vector linear solution over $\mathbb{F}$, which by Theorem III.6 implies $k \mid n$. However, this contradicts the fact that $n^2 \leq k$. Thus, no such ring R exists. □

While the Dim-k Network is a non-multicast network, we note that a similar result can occur for multicast networks as well. The following result was shown by Sun et al. [18].

Lemma IV.2 [18, Th. 4 and Corollary 11]: For each integer $k \geq 2$ *and prime* p*, there exists a multicast network with*

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

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

Corollary IV.3: For each integer $k \geq 2$ *and prime* p*, there exists a multicast network that has a* k*-dimensional vector linear solution over* GF(p) *but is not scalar linearly solvable over any ring of size* p^k*.*

Proof: Let $\mathcal{N}$ denote the network constructed by Sun et al. [18] in Lemma IV.2 corresponding to p and k. Such a network has a k-dimensional vector linear solution over GF(p).

Since $\mathcal{N}$ is vector linearly solvable, by Corollary II.15, it must be scalar linearly solvable over some ring. Now suppose R is a minimum-size ring over which $\mathcal{N}$ is scalar linearly solvable. By Theorem II.5, there exists a prime-power q and an integer n such that $R \cong M_n(\text{GF}(q))$. By Corollary I.5, $\mathcal{N}$ has an n-dimensional vector linear solution over GF(q), but by Lemma IV.2 (c), this implies $q^n \geq p^k$.

If $n \geq 2$, then $|R| = q^{n^2} > q^n \geq p^k$. If $n = 1$, then $\mathcal{N}$ has a scalar linear solution over GF(q), which, by Lemma IV.2 (b), implies $p^k < q = |R|$. Thus the minimum size ring over which $\mathcal{N}$ is scalar linearly solvable has cardinality greater than p^k, so in particular, $\mathcal{N}$ is not scalar linearly solvable over any ring of size p^k. □

A. Commutative Rings

Both a scalar linear code over a ring of size p^k and a k-dimensional vector linear code are linear codes over a module of size p^k. We have already seen (in Theorem IV.1) that there exists a network with a k-dimensional vector linear solution over GF(p) yet with no scalar linear solutions over any ring of size p^k. The main result of this section (Theorem IV.6) will show that any network that is scalar linearly solvable over a commutative ring of size p^k must also have a k-dimensional vector linear solution over GF(p).

The following lemma was proved in Part I (in [2, Lemmas II.12 and V.3]) and will be used in what follows.

Lemma IV.4: For each prime p *and positive integer* k*, if a network* $\mathcal{N}$ *has a scalar linear solution over some commutative ring of size* p^k*, then there exists an integer partition* $(n_1, \ldots, n_r)$ *of* k *such that* $\mathcal{N}$ *is scalar linearly solvable over each of the fields* GF(p^{n_1}), …, GF(p^{n_r})*.*

The following standard result on rings will be used in later proofs.

Lemma IV.5 [15, Th. I.1]: Every finite ring is isomorphic to a direct product of rings of prime power sizes.

Theorem IV.6: Let m be a positive integer with prime factorization $m = p_1^{k_1} \cdots p_t^{k_t}$. If a network $\mathcal{N}$ has a scalar linear solution over some commutative ring of size m, then the following hold:

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

Proof: Suppose $\mathcal{N}$ is scalar linearly solvable over a commutative ring R of size m. By Lemma IV.5, there exist rings $R_1, \ldots, R_t$ such that

$$R \cong R_1 \times \cdots \times R_t$$

and $|R_i| = p_i^{k_i}$ for all i.

Let $i \in \{1, \ldots, t\}$. Since the projection mapping from R to R_i is a surjective homomorphism, by Corollary I.7, network $\mathcal{N}$ is scalar linearly solvable over R_i. Then by Lemma IV.4, there exists an integer partition $(n_1, \ldots, n_r)$ of k_i such that $\mathcal{N}$ is scalar linearly solvable over each of the fields $\mathrm{GF}(p_i^{n_1}), \ldots, \mathrm{GF}(p_i^{n_r})$. By Lemma II.11, this implies that $\mathcal{N}$ has an n_j-dimensional vector linear solution over $\mathrm{GF}(p_i)$ for each $j = 1, \ldots, r$. However, by Lemma III.3, this then implies that $\mathcal{N}$ has a $k_i = (n_1 + \cdots + n_r)$-dimensional vector linear solution over $\mathrm{GF}(p_i)$.

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

In Part I, we showed (in [2, Ths. V.8 and V.9]) that with respect to ring domination for scalar linear coding, some ring sizes give rise to multiple maximal commutative rings whereas other ring sizes yield only a single unique maximal commutative ring. If there is just one maximal commutative ring of size m, then every network that is linearly solvable over some commutative ring of size m is also linearly solvable over the maximal ring.

In contrast, if there are multiple maximal commutative rings of size m, then for any commutative ring R of size m, there is always a different commutative ring S also of size m, such that some network is scalar linearly solvable over S but not over R. Thus, in this sense, there is no "best" commutative ring of a given size.

However, by Theorem IV.6 (b), if a network has a linear solution over some commutative ring of size $m = p_1^{k_1} \cdots p_t^{k_t}$, then it has a linear solution over the

$$M_{k_1}(\mathrm{GF}(p_1)) \times \cdots \times M_{k_t}(\mathrm{GF}(p_t))\text{-module}$$

$\mathrm{GF}(p_1)^{k_1} \times \cdots \times \mathrm{GF}(p_t)^{k_t}$, which also has size m. In fact, we showed (in Theorem IV.1) that when $m = p^k$, the converse is not true. So in this sense, k-dimensional vector linear codes over $\mathrm{GF}(p)$ are strictly "better" than scalar linear codes over commutative rings of size p^k.

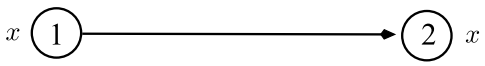

Fig. 5. A trivial network with one message x that is demanded by the receiver.

B. Non-Commutative Rings

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

The following lemma was proved in Part I (in [2, Th. V.9]) and will be used in what follows.

Lemma IV.7: For each $k \in \{1, 2, 3, 4, 6\}$ and prime p, if a network is scalar linearly solvable over some commutative ring of size p^k, then it is scalar linearly solvable over $\mathrm{GF}(p^k)$.

Lemma IV.8 characterizes the non-commutative rings of prime-power size whose multiplicity is at most three.

Lemma IV.8 [11, pp. 512–513]: For each prime p, all rings of size p and of size p^2 are commutative, and the ring of all upper-triangular 2×2 matrices over $\mathrm{GF}(p)$ *is the only non-commutative ring of size p^3.*

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

For example, consider the trivial network shown in Figure 5 consisting of a single message x emitted by a source directly connected by a single edge to a receiver demanding message x. The only possible linear functions that can be carried on the edge are of the form cx for some fixed $c \in \{0, 2, 4, 6\}$. However, no matter what the choice of c is, the messages 0 and 4 always get received as 0 mod 8, so the receiver cannot uniquely determine x in general. Thus, there is no linear solution for the network over this ring (with no multiplicative identity). A similar issue arises for the set $\{0, 2\}$ with mod 4 addition and multiplication, which also satisfies all of the properties of a ring except there is no multiplicative identity.

Lemma IV.9: For each prime p, if a network is scalar linearly solvable over some ring of size p^2, then it is a scalar linearly solvable over $\mathrm{GF}(p^2)$.

Proof: By Lemma IV.8, every ring of size p^2 is commutative, and by Lemma IV.7, every network that is scalar linearly solvable over some commutative ring of size p^2 has a scalar linear solution over $\mathrm{GF}(p^2)$. □

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

Lemma IV.10: For each finite field $\mathbb{F}$ and integer $k \geq 2$, any network that is scalar linearly solvable over the ring of upper-triangular $k \times k$ matrices over $\mathbb{F}$ is also scalar linearly solvable over $\mathbb{F}$.

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

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

Then ϕ is clearly surjective and preserves identities, and for any $A, B \in R$,

$$\phi(A+B) = a_{1,1} + b_{1,1} = \phi(A) + \phi(B)$$
$$\phi(AB) = a_{1,1}\, b_{1,1} = \phi(A)\phi(B).$$

Thus ϕ is a surjective homomorphism, so by Corollary I.7, any network that is scalar linearly solvable over R is scalar linearly solvable over $\mathbb{F}$. □

Lemma IV.11: For each prime p, if a network is scalar linearly solvable over some ring of size p^3, then it is scalar linearly solvable over $\mathrm{GF}(p^3)$.

Proof: By Lemma IV.8, the only non-commutative ring of size p^3 is the ring of upper triangular matrices with entries in $\mathrm{GF}(p)$, and by Lemma IV.10, any network that is scalar linearly solvable over this ring is also scalar linearly solvable over $\mathrm{GF}(p)$. Since $\mathrm{GF}(p)$ is a subring of $\mathrm{GF}(p^3)$, any network that is scalar linearly solvable over $\mathrm{GF}(p)$ is scalar linearly solvable over $\mathrm{GF}(p^3)$.

By Lemma IV.7, every network that is scalar linearly solvable over some commutative ring of size p^3 has a scalar linear solution over $\mathrm{GF}(p^3)$. □

The following three lemmas are proved in the Appendix.

Lemma IV.12: For each prime p, if a network is scalar linearly solvable over some ring of size p^4, then it is scalar linearly solvable over at least one of the rings $\mathrm{GF}(p^4)$ *or* $M_2(\mathrm{GF}(p))$.

Lemma IV.13: For each prime p, if a network is scalar linearly solvable over some ring of size p^5, then it is scalar linearly solvable over at least one of the commutative rings $\mathrm{GF}(p^5)$ *or* $\mathrm{GF}(p^3) \times \mathrm{GF}(p^2)$.

Lemma IV.14: For each prime p, if a network is scalar linearly solvable over some ring of size p^6, then it is scalar linearly solvable over $\mathrm{GF}(p^6)$.

Theorem IV.15 is a generalization of Lemma IV.7 to scalar linear codes over non-commutative rings. Extending Theorem IV.15 to $|R| = p^k$ for $k \geq 7$ is left as an open problem.

Theorem IV.15: Let p be a prime, and suppose $\mathcal{N}$ is scalar linearly solvable over a ring R. Then $\mathcal{N}$ is scalar linearly solvable over

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

Proof: This follows immediately from Lemmas IV.9, IV.11, IV.12, IV.13, and IV.14. □

We also note that by Corollary II.14, the (p^4+1)-Choose-Two Network is scalar linearly solvable over $\mathrm{GF}(p^4)$ but not over $M_2(\mathrm{GF}(p))$, and the (p^5+1)-Choose-Two Network is scalar linearly solvable over $\mathrm{GF}(p^5)$ but not over $\mathrm{GF}(p^3) \times \mathrm{GF}(p^2)$. By Corollary III.7, the Dim-2 Network is scalar linearly solvable over $M_2(\mathrm{GF}(p))$ but not over $\mathrm{GF}(p^4)$. We showed in Part I [2, Th. III.8] that there exists a network that is scalar linearly solvable over $\mathrm{GF}(p^3) \times \mathrm{GF}(p^2)$ but not over $\mathrm{GF}(p^5)$. Hence it is necessary to include both rings in (c) and (d) in Theorem IV.15.

Corollary IV.16: Let p be a prime and $k \in \{2, 3, 4, 5, 6\}$, and suppose $\mathcal{N}$ is scalar linearly solvable over a ring of size p^k. Then $\mathcal{N}$ has a k-dimensional vector linear solution over $\mathrm{GF}(p)$.

Proof: If $k \in \{2, 3, 5, 6\}$, then by Theorem IV.15, $\mathcal{N}$ has a scalar linear solution over a commutative ring of size p^k, since fields and direct products of fields are commutative rings. So, by Theorem IV.6, $\mathcal{N}$ has a k-dimensional vector linear solution over $\mathrm{GF}(p)$.

Now suppose $k = 4$. If $\mathcal{N}$ is scalar linearly solvable over $\mathrm{GF}(p^4)$, then by Lemma II.11, $\mathcal{N}$ has a 4-dimensional vector linear solution over $\mathrm{GF}(p)$. If $\mathcal{N}$ is not scalar linearly solvable over $\mathrm{GF}(p^4)$, then by Theorem IV.15 (c), $\mathcal{N}$ must be scalar linearly solvable over $M_2(\mathrm{GF}(p))$, so by Corollary I.5, $\mathcal{N}$ has a 2-dimensional vector linear solution over $\mathrm{GF}(p)$, in which case $\mathcal{N}$ also has a 4-dimensional vector linear solution over $\mathrm{GF}(p)$ by Lemma III.3. □

Theorem IV.17 generalizes the results of Theorem IV.6 to rings of size m with prime factor multiplicity less than or equal to 6.

Theorem IV.17: Let m be a positive integer with prime factorization $m = p_1^{k_1} \cdots p_t^{k_t}$. If a network $\mathcal{N}$ has a scalar linear solution over a ring of size m, then, for each $i = 1, \ldots, t$ such that $k_i \leq 6$, network $\mathcal{N}$ has a k_i-dimensional vector linear solution over $\mathrm{GF}(p_i)$.

Proof: Suppose $\mathcal{N}$ is scalar linearly solvable over a ring R of size m. By Lemma IV.5, there exists rings $R_1, \ldots, R_t$ such that

$$R \cong R_1 \times \cdots \times R_t$$

and $|R_i| = p_i^{k_i}$ for all i.

Now, let $i \in \{1, \ldots, t\}$ and suppose $k_i \leq 6$. The projection mapping from R to R_i is a surjective homomorphism, so by Corollary I.7, network $\mathcal{N}$ is scalar linearly solvable over R_i. Since $\mathcal{N}$ is scalar linearly solvable over a ring of size $p_i^{k_i}$ where $k_i \leq 6$, by Corollary IV.16, $\mathcal{N}$ has a k_i-dimensional vector linear solution over $\mathrm{GF}(p_i)$. □

We leave as an open question whether the restriction that $k_i \leq 6$ can be removed from the statement of Theorem IV.17. If this generalization is false, then for what primes p and positive integers k is it the case that there exists a network with a scalar linear solution over a ring of size p^k but with no k-dimensional vector linear solution over $\mathrm{GF}(p)$? If such a ring and such a network do exist, the ring must be non-commutative and $k \geq 7$.

V. Concluding Remarks

For each positive integer k and prime p, we have shown that the set of networks with scalar linear solutions over commutative rings of size p^k is properly contained in the set of networks with k-dimensional vector linear solutions over GF(p).

So in this sense, k-dimensional vector linear codes over GF(p) may be advantageous compared to scalar linear codes over commutative rings of the same size p^k. In addition, there are more k-dimensional linear functions over GF(p) than there over a commutative ring of size p^k. Vector linear codes over fields are also optimal in the sense that they minimize the alphabet size needed for a linear solution over a particular network. On the other hand, the complexity of implementing vector linear codes is generally higher than for scalar linear codes over commutative rings of the same size.

A. Summary of Results

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

- If a network is scalar linearly solvable over some commutative ring, then the (unique) smallest such commutative ring is a field [2, Th. II.10].
- If a network is scalar linearly solvable over some ring, then a smallest such ring is a matrix ring over field (Theorem II.5). It is not known whether such a smallest ring is unique.
- If a network is linearly solvable over some module, then a smallest such module yields a vector linear solution over a field (Theorem II.10). Such a module may not be unique (Theorem II.13).

Additionally, we summarize our results on the linear solvability of networks over fields, rings, and modules in Corollaries II.15 and II.16.

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

- A network can have no scalar linear solutions over a given field yet be scalar linearly solvable over a commutative ring of the same size [2, Th. III.8]. Part I particularly focuses on commutative rings for which there exists a network that is scalar linearly solvable over the ring but not over any other commutative ring of the same size.
- A network can have no scalar linear solutions over any commutative ring yet be scalar linearly solvable over a non-commutative ring (Corollary III.7). Such a non-commutative ring must have size at least 16 (Theorem III.10), and for the M Network, this bound is achieved.
- When $k \leq 6$, any network with a scalar linear solution over a ring of size p^k has a k-dimensional vector linear solutions over GF(p) (Corollary IV.16). This extends to all positive integers k when the ring is commutative (Theorem IV.6).
- There exists a multicast network (Corollary IV.3) and a non-multicast network (Theorem IV.1) with k-dimensional vector linear solutions over GF(p) but with no scalar linear solutions over any ring of size p^k.

B. Open Questions

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

- Does there exist a network with a linear solution over some ring of size p^k but with no k-dimensional vector linear solution over GF(p)? We have shown that if such a network and such a ring exist, then the ring is non-commutative and $k \geq 7$.
- More generally, does there exist a network with a linear solution over some module of size p^k but with no k-dimensional vector linear solution over GF(p)?
- When a network has a scalar linear solution over a ring of a given size, over what other rings does the network have scalar linear solutions? In particular, how does Theorem IV.15 extend to rings of size p^k when $k \geq 7$?
- Does there exist a network that is scalar linearly solvable over at least two rings of a given size but not over any smaller ring? I.e., is the smallest-size ring over which a network scalar linearly solvable unique?
- In Part I, we characterized commutative rings with the property that there exists a network with a scalar linear solution over the ring but no other commutative ring of the same size? Is there a similar characterization when removing the commutative restriction?
- Can the linear capacity of a network over some ring (or module) be greater than the network's linear capacity over any field? I.e., are higher rates attainable using linear codes over rings and modules?

Appendix

The main purpose of this Appendix is to prove Lemmas IV.12, IV.13, and IV.14, which are used in the proof of Theorem IV.15. It is an open question whether Theorem IV.17 can be extended to all finite rings. The techniques presented in this section may additionally be useful for examining such questions.

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

- *local* [5] if R/J is a field.
- *semi-local* if R/J is simple, or equivalently R is isomorphic to a matrix ring over some local ring (e.g. [15, p. 162]).
- *semi-simple* if R is isomorphic to a direct product of simple rings (matrix rings over fields) or equivalently, $J = \{0\}$ (e.g. [15, pp. 75, 128]).

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

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

(a) *[15, Th. VIII.26]* $R \cong M_r(S)$
(b) *[1, Th. 6.1.2]* $|S| = p^s$

[5] If R is a local commutative ring, then R has a single maximal ideal, which corresponds to our definition of a commutative local ring in Part I.

(c) *[1, Th. 6.1.2]* $\mathrm{GF}(p^t) \cong S/J$, *where* J *is the radical of* S *and* $t \mid s$.

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

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

Lemma A.2 [15, Proposition IV.6, Th. VIII.4]: Let R *be a finite ring with radical* J. *Then there exist fields* $\mathbb{F}_1, \ldots, \mathbb{F}_s$ *and positive integers* $r_1, \ldots, r_s$ *such that*

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

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

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

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

Proof: By Lemma II.2, there exists a surjective homomorphism $\phi : R \to R/J$. Let $i \in \{1, \ldots, s\}$. Then the projection mapping $\psi_i : R/J \to M_{r_i}(\mathbb{F}_i)$ is a surjective homomorphism. Hence the composition of mappings $\psi_i \circ \phi : R \to M_{r_i}(\mathbb{F}_i)$ is a surjective homomorphism. Thus by Corollary I.7, any network with a scalar linear solution over R has a scalar linear solution over the ring $M_{r_i}(\mathbb{F}_i)$. □

The following is an enumeration of semi-simple rings that we will reference in upcoming proofs. Semi-simple rings are direct products of rings of matrices over fields. There are a limited number of small-size matrix rings over fields, so the semi-simple rings of small sizes can be easily enumerated. For each prime p, it can be verified that the rings given in (16)–(48) are all of the semi-simple rings of sizes p, p^2, p^3, p^4, p^5, or p^6 (up to isomorphism). In particular, these semi-simple rings must be direct products of the simple rings $\mathrm{GF}(p)$, $\mathrm{GF}(p^2)$, $\mathrm{GF}(p^3)$, $\mathrm{GF}(p^4)$, $M_2(\mathrm{GF}(p))$, $\mathrm{GF}(p^5)$, and $\mathrm{GF}(p^6)$.

- Size p:

$$\mathrm{GF}(p) \tag{16}$$

- Size p^2:

$$\mathrm{GF}(p^2) \tag{17}$$
$$\mathrm{GF}(p) \times \mathrm{GF}(p) \tag{18}$$

- Size p^3:

$$\mathrm{GF}(p^3) \tag{19}$$
$$\mathrm{GF}(p^2) \times \mathrm{GF}(p) \tag{20}$$
$$\mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{21}$$

- Size p^4:

$$M_2(\mathrm{GF}(p)) \tag{22}$$
$$\mathrm{GF}(p^4) \tag{23}$$
$$\mathrm{GF}(p^3) \times \mathrm{GF}(p) \tag{24}$$
$$\mathrm{GF}(p^2) \times \mathrm{GF}(p^2) \tag{25}$$
$$\mathrm{GF}(p^2) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{26}$$
$$\mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{27}$$

- Size p^5:

$$\mathrm{GF}(p^5) \tag{28}$$
$$M_2(\mathrm{GF}(p)) \times \mathrm{GF}(p) \tag{29}$$
$$\mathrm{GF}(p^4) \times \mathrm{GF}(p) \tag{30}$$
$$\mathrm{GF}(p^3) \times \mathrm{GF}(p^2) \tag{31}$$
$$\mathrm{GF}(p^3) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{32}$$
$$\mathrm{GF}(p^2) \times \mathrm{GF}(p^2) \times \mathrm{GF}(p) \tag{33}$$
$$\mathrm{GF}(p^2) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{34}$$
$$\mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{35}$$

- Size p^6:

$$\mathrm{GF}(p^6) \tag{36}$$
$$\mathrm{GF}(p^5) \times \mathrm{GF}(p) \tag{37}$$
$$M_2(\mathrm{GF}(p)) \times \mathrm{GF}(p^2) \tag{38}$$
$$\mathrm{GF}(p^4) \times \mathrm{GF}(p^2) \tag{39}$$
$$M_2(\mathrm{GF}(p)) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{40}$$
$$\mathrm{GF}(p^4) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{41}$$
$$\mathrm{GF}(p^3) \times \mathrm{GF}(p^3) \tag{42}$$
$$\mathrm{GF}(p^3) \times \mathrm{GF}(p^2) \times \mathrm{GF}(p) \tag{43}$$
$$\mathrm{GF}(p^3) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{44}$$
$$\mathrm{GF}(p^2) \times \mathrm{GF}(p^2) \times \mathrm{GF}(p^2) \tag{45}$$
$$\mathrm{GF}(p^2) \times \mathrm{GF}(p^2) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{46}$$
$$\mathrm{GF}(p^2) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{47}$$
$$\mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \tag{48}$$

We now prove Lemmas IV.12, IV.13, and IV.14.

Proof of Lemma IV.12: Let R be a ring of size p^4 with radical J, and suppose $\mathcal{N}$ is scalar linearly solvable over R. Then $|R/J| \in \{p, p^2, p^3, p^4\}$, so by Lemma A.2, R/J is isomorphic to one of the rings in (16)–(27).

If R/J is isomorphic to any of these rings except those in (19) and (22), then by Lemma A.3, $\mathcal{N}$ is also scalar linearly solvable over at least one of $\mathrm{GF}(p)$, $\mathrm{GF}(p^2)$, or $\mathrm{GF}(p^4)$. Since $\mathrm{GF}(p)$ and $\mathrm{GF}(p^2)$ are both subrings of $\mathrm{GF}(p^4)$, in these cases, $\mathcal{N}$ is also scalar linearly solvable over $\mathrm{GF}(p^4)$.

On the other hand, if R/J is isomorphic to the ring in (22), then by Lemma A.3, $\mathcal{N}$ is also scalar linearly solvable over $M_2(\mathrm{GF}(p))$. It follows from Lemma A.1 that R/J is not isomorphic to the ring in (19). □

Proof of Lemma IV.13: Let R be a ring of size p^5 with radical J, and suppose $\mathcal{N}$ is scalar linearly solvable over R. Then $|R/J| \in \{p, p^2, p^3, p^4, p^5\}$, so by Lemma A.2, R/J must be isomorphic to one of the rings in (16)–(35).

If R/J is isomorphic to one of the rings in (22)–(27) (i.e. $|R/J| = p^4$), then $|J| = p$. Since $(J, +)$ is an R-module and $\mathcal{N}$ has a linear solution over the faithful module ${}_R R$, by Lemma I.3, $\mathcal{N}$ has a linear solution over ${}_R J$. By Theorem II.10, this implies $\mathcal{N}$ has a scalar linear solution over GF(p). Since GF(p) is a subring of GF(p^5), in these cases, $\mathcal{N}$ also has a scalar linear solution over GF(p^5).

It follows from Lemma A.1 that R/J is not isomorphic to either of the rings in (17) or (19). If R/J is isomorphic to the ring in (31), then by Lemma A.3, $\mathcal{N}$ is scalar linearly solvable over GF(p^3) $\times$ GF(p^2).

If R/J is isomorphic to any of the remaining cases, then by Lemma A.3, network $\mathcal{N}$ is scalar linearly solvable over either GF(p) or GF(p^5). Since GF(p) is a subring of GF(p^5), in these cases, $\mathcal{N}$ also has a scalar linear solution over GF(p^5).□

Proof of Lemma IV.14: Let R be a ring of size p^6 with radical J, and suppose $\mathcal{N}$ is scalar linearly solvable over R. Then $|R/J| \in \{p, p^2, p^3, p^4, p^5, p^6\}$, so by Lemma A.2, R/J must be isomorphic to one of the rings in (16)–(48). It follows from Lemma A.1 that R/J is not isomorphic to any of the rings in (22), (23), or (28).

If R/J is isomorphic to any of the remaining cases, then it follows from Lemma A.3 that $\mathcal{N}$ is scalar linearly solvable over GF(p^n) for some $n \in \{1, 2, 3, 6\}$. Since $n \mid 6$, GF(p^n) is a subring of GF(p^6), which implies $\mathcal{N}$ is scalar linearly solvable over GF(p^6). □

REFERENCES

[1] G. Bini and F. Flamini, *Finite Commutative Rings and Their Applications*. Norwell, MA, USA: Kluwer, 2002.

[2] J. Connelly and K. Zeger, "Linear network coding over rings—Part I: Scalar codes and commutative alphabets," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 275–291, Jan. 2018.

[3] B. Corbas and G. D. Williams, "Rings of order p^5 part I. Nonlocal rings," *J. Algebra*, vol. 231, no. 2, pp. 677–690, 2000.

[4] B. Corbas and G. D. Williams, "Rings of order p^5 part II. Local rings," *J. Algebra*, vol. 231, no. 2, pp. 691–704, 2000.

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

[6] 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.

[7] 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.

[8] 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.

[9] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed. Hoboken, NJ, USA: Wiley, 2004.

[10] J. B. Ebrahimi and C. Fragouli, "Algebraic algorithms for vector network coding," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 996–1007, Feb. 2011.

[11] K. E. Eldridge, "Orders for finite noncommutative rings with unity," *Amer. Math. Monthly*, vol. 75, no. 5, pp. 512–514, May 1968.

[12] B. Fine, "Classification of finite rings of order p^2," *Math. Mag.*, vol. 66, no. 4, pp. 248–252, Oct. 1993.

[13] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, 3rd ed. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[14] T.-Y. Lam, *A First Course in Noncommutative Rings*, 2nd ed. New York, NY, USA: Springer-Verlag, 2001.

[15] B. R. McDonald, *Finite Rings With Identity*. New York, NY, USA: Marcel Dekker, 1974.

[16] M. Médard, M. Effros, T. Ho, and D. Karger, "On coding for non-multicast networks," in *Proc. Annu. Allerton Conf. Commun. Control Comput.*, Monticello, VA, USA, Oct. 2003, pp. 21–29.

[17] A. R. Lehman and E. Lehman, "Complexity classification of network information flow problems," in *Proc. ACM-SIAM Symp. Discrete Algorithms*, 2004, pp. 142–150.

[18] Q. T. Sun, X. Yang, K. Long, X. Yin, and Z. Li, "On vector linear solvability of multicast networks," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5096–5107, Dec. 2016.

Joseph Connelly (S'12) was born in Milwaukee in 1991. He received a Bachelor's degree in electrical and computer engineering from the University of Minnesota Twin Cities in 2013. In 2016, he was with the information processing group at the NASA Jet Propulsion Laboratory, and he received the M.S. degree in electrical and computer engineering from the University of California, San Diego, where he is currently a Ph.D. candidate.

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.