Capacity and Achievable Rate Regions for Linear Network Coding Over Ring Alphabets

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

Abstract—The rate of a network code is the ratio of the block size of the network's messages to that of its edge codewords. We compare the linear capacities and achievable rate regions of networks using finite field alphabets to the more general cases of arbitrary ring and module alphabets. For non-commutative rings, two-sided linearity is allowed. Specifically, we prove the following for directed acyclic networks. First, the linear rate region and the linear capacity of any network over a finite field depend only on the characteristic of the field. Furthermore, any two fields with different characteristics yield different linear capacities for at least one network. Second, whenever the characteristic of a given finite field divides the size of a given finite ring, each network's linear rate region over the ring is contained in its linear rate region over the field. Thus, any network's linear capacity over a field is at least its linear capacity over any other ring of the same size. An analogous result also holds for linear network codes over module alphabets. Third, whenever the characteristic of a given finite field does not divide the size of a given finite ring, there is some network whose linear capacity over the ring is strictly greater than its linear capacity over the field. Thus, for any finite field, there always exist rings over which some networks have higher linear capacities than over the field.

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

I. INTRODUCTION

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

inferior to more general types of network coding in terms of both solvability and capacity. Nevertheless, linear codes over finite fields are attractive for both theoretical and practical reasons [30].

In certain cases, linear coding over finite ring alphabets can offer solvability advantages over finite field alphabets [8], [9]. An open question has been whether the linear capacity of a network over a finite field can be improved by using some other ring of the same size as the field. In other words, does the improvement in network solvability, from using more general rings than fields, also carry over to network capacity? In the present paper, we answer this question in the negative. That is, we prove that the linear capacity of a network cannot be improved by changing the network coding alphabet from a field to any other ring of the same size.

Another open question has been whether the linear capacity of a network over a finite field can depend on any aspect of the field other than its characteristic. Indeed it has been previously observed that the linear capacity of a network can vary as a function of the field (e.g., [7], [14], [15]), but all known examples had linear capacities that only depended on the fields' characteristics. We also answer this question in the negative. That is, we prove that any two fields with the same characteristic will result in the same linear capacity for any given network. Furthermore, any two fields with different characteristics will result in different linear capacities for at least one network. We prove analogous (and more general) results for linearly achievable rate regions of networks over finite fields.

Unlike finite fields, finite rings need not have prime-power size, which may be advantageous in certain applications. An open question has been whether a network can increase its linearly achievable rate region by allowing the alphabet to be a ring of non-power-of-prime size. However, we again answer this question in the negative by showing that a network's linear rate region over a ring is contained in its linear rate region over any field whose characteristic divides the ring's size. This result follows from the fact that every finite ring is isomorphic to some direct product of rings of prime-power sizes. As a consequence of this result, any network's linear capacity over a particular ring is at most its linear capacity over any field whose characteristic divides the ring's size. These results extend naturally to the more general case of linear network codes in which the alphabet has the structure of a finite module.

A. Modules, Linear Functions, and Tensor Products

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

Definition I.1. A *left R-module* is an Abelian group $(G, \oplus)$ together with a ring $(R, +, *)$ of *scalars* and an action $\cdot : R \times G \to G$ such that for all $r, s \in R$ and all $g, h \in G$ the following hold:

$$r \cdot (g \oplus h) = (r \cdot g) \oplus (r \cdot h)$$
$$(r + s) \cdot g = (r \cdot g) \oplus (s \cdot g)$$
$$(r * s) \cdot g = r \cdot (s \cdot g)$$
$$1 \cdot g = g.$$

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

- The ring of integers $\mathbb{Z}$ acts on any Abelian group G by repeated addition in G.
- Any ring R acts on its own additive group $(R, +)$ by multiplication in R. We denote this module by $_R R$.
- Any ring R acts on the set of all t-vectors over R, denoted by R^t, by scalar multiplication. When R is a field, this module is a vector space.
- If $_R G$ is a module, then the ring of all $t \times t$ matrices with entries in R, denoted $M_t(R)$, acts on the group, G^t, of all t-vectors over G via matrix-vector multiplication where multiplication of elements of R with elements of G is given by the action of $_R G$. A special case of this module, $_{M_t(R)} G^t$, occurs when $G = (R, +)$, in which case matrices over R act on vectors over R via matrix-vector multiplication over R.

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

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

where $a_1, \ldots, a_m \in R$, is a (left) *one-sided linear function* with respect to both the ring R and the left module $_R R$. [1] A function $f' : R^m \to R$ of the form

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

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

[1] Every right one-sided linear function with respect to a ring or a right module can be described as a corresponding left one-sided linear function with respect to a left module with the same Abelian group. Hence, in this paper, it suffices for us to exclusively use left one-sided linear functions.

is also a one-sided linear function, since in a commutative ring,

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

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

Example I.2. Let R be the (non-commutative) ring of all 2×2 matrices over a field. The function $f : R \to R$ given by

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

is a two-sided linear function over R. It can be verified that, for all $A, B \in R$, the function $f(X)$ is not the function AXB. By allowing for sums of X terms multiplied by coefficients on both the left and the right, a broader class of functions can be attained than with a single X term multiplied by coefficients on the left and the right. This also implies $f(X)$ cannot be written as a (left or right) one-sided linear function.

In the remainder of this section, we will show that two-sided linear functions over rings can be written as one-sided linear functions with respect to some module, i.e., f' in (1) can be written as

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

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

Example I.3. Suppose $\mathbb{F}$ is a field and $U \subseteq \mathbb{F}^m$ and $V \subseteq \mathbb{F}^n$ are vector spaces. For each $u \in U$ and $v \in V$, define the mn vector (u, v) by

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

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

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

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

If R is a ring and E is a set, the *free R-module generated by E* is denoted $R^{(E)}$. In this module, the group is the subset of the Cartesian product $\prod\limits_{e \in E} R$ consisting only of the elements that have finitely many non-zero components together with component-wise addition, and the ring R acts on $R^{(E)}$ component-wise. By mapping the element $e \in E$ to the vector in $R^{(E)}$ whose eth component is 1 and all other components are 0, we can view $R^{(E)}$ as the set of all finite R-linear combinations of elements of E. In other words, every element of $R^{(E)}$ can be uniquely written as $\sum\limits_{e \in E} a_e \, e$, where only finitely many $a_e \in R$ are non-zero, so the set E is a basis for $R^{(E)}$.

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

$$\left\{ r_1 \, e_1 + \cdots + r_m e_m \; : \; \begin{array}{l} m \in \mathbb{N}, \\ r_1, \ldots, r_m \in R, \\ e_1, \ldots, e_m \in E \end{array} \right\}.$$

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

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

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

$$(g, h) + (g', h) = (g + g', h)$$
$$(g, h) + (g, h') = (g, h + h')$$
$$r\,(g, h) = (r\,g, h)$$
$$r\,(g, h) = (g, r\,h).$$

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

Definition I.4. Let R and S be finite rings, and let $\mathbb{Z}$ denote the ring of integers. The *tensor product ring $R \otimes S$* is the Abelian group $R \otimes_{\mathbb{Z}} S$ together with multiplication given by

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

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

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

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

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

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

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

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

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

$$((a, b) + (a', b)) \cdot x = a \, x \, b + a' \, x \, b$$
$$= (a + a') \, x \, b = (a + a', b) \cdot x$$
$$((a, b) + (a, b')) \cdot x = a \, x \, b + a \, x \, b'$$
$$= a \, x \, (b + b') = (a, b + b') \cdot x$$
$$n\,(a, b) \cdot x = n\,(a \, x \, b)$$
$$= (n \, a) \, x \, b = (na, b) \cdot x$$
$$n\,(a, b) \cdot x = n\,(a \, x \, b)$$
$$= a \, x \, (n \, b) = (a, nb) \cdot x.$$

The two-sided linear function f' in (1) can now be written as

$$f'(x_1, \ldots, x_m) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n_i} (a_{i,j}, b_{i,j}) \right) \cdot x_i$$

which is a one-sided linear function with respect to the module $_{R \otimes R^{op}} R$. This shows that any *two-sided* linear function over a ring is a special case of a *one-sided* linear function over a left module. It then follows that two-sided linear codes over rings are a special case of one-sided linear codes over left modules.

Example I.5. *Let R be the (non-commutative) ring of all 2×2 matrices over a field. The two-sided linear function $f : R \to R$ from Example I.2 can be written as a one-sided linear function over the module $_{R \otimes R^{op}} R$ as*

$$f \left(\begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix} \right) = A \cdot \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix}$$

where A is the tensor in $R \otimes R^{op}$ given by

$$\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right) + \left(\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right).$$

B. Network Coding Model

A *network* will refer to a finite, directed, acyclic multigraph, some of whose nodes are *sources* or *receivers*. Source nodes generate one or more *message vectors* whose components are arbitrary elements of a fixed, finite set of size at least 2, called an *alphabet*. The elements of an alphabet are called *symbols*. We will denote the cardinality of an alphabet $\mathcal{A}$ by $|\mathcal{A}|$. The *inputs* to a node are the message vectors, if any, originating at the node and the symbols on the incoming edges of the node. Each outgoing edge of a network node has associated with it an *edge function* that maps the node's inputs to the vector of symbols carried by the edge, called the *edge vector*. Each receiver node has *demands*, which are a specified subset of the network's message vectors the receiver wishes to obtain. Each receiver node also has *decoding functions* that map the receiver's inputs to a vector of alphabet symbols in an attempt to recover the receiver's demands.

In a network with m message vectors, a $(k_1, \ldots, k_m, n)$ *code over an alphabet $\mathcal{A}$* (also called a *fractional* code) is an assignment of edge functions to the edges in the network and an assignment of decoding functions to the receivers in the network such that the ith message vector is an element of $\mathcal{A}^{k_i}$ and the edge vectors are elements of $\mathcal{A}^n$. In other words, the alphabet and the lengths of the message and edge vectors are specified by the parameters of the code, not the network itself. The *rate vector* of a $(k_1, \ldots, k_m, n)$ network code is $\mathbf{r} = (k_1/n, \ldots, k_m/n)$. A fractional code is a *solution* if each receiver recovers its demanded message vector from its inputs, and a rate vector $\mathbf{r}$ is *achievable for a network* if the network has a fractional solution with rate vector $\mathbf{r}$ over some alphabet.

C. Linearity Over Finite Rings and Modules

A function $f : G^s \to G^t$ is *linear with respect to the module $_R G$* if it can be written as a matrix-vector product, $f(\mathbf{x}) = A\mathbf{x}$, where

- A is a $t \times s$ matrix with elements from R,
- multiplication of elements of R by elements of G is the action of the module.

A fractional code is *linear over the module $_R G$* if the message vectors and edge vectors have components from G and all edge functions and decoding functions are linear over the module. For each network node, the vector $\mathbf{x} \in G^s$ is a concatenation of all the input vectors of the node. In other words, the network alphabet is G, and the outgoing edge vectors and decoded symbol vectors at a node are linear combinations of the node's vector inputs, where the coefficients describing the linear combination are from R. We use modules as a tool to prove results related to linear coding over rings, since linear network coding over modules generalizes linear network coding over rings and fields. The module approach is especially useful for non-commutative rings with two-sided linear codes.

If R is a finite ring, then a fractional linear code over the module $_{R \otimes R^{op}} R$ is said to be a *fractional two-sided linear code over R*. In particular, the network alphabet is R, and the outgoing edge vectors carry linear combinations of the node's input components, where each input component in the combination is multiplied on the left and right by constants from R. If R is commutative, then then a fractional two-sided linear code over R is also a fractional linear code over the module $_R R$, since left-sided and two-sided linearity are equivalent in this case. In other words, any two-sided linear code over a commutative ring can be written as a left-sided linear code over the ring. A rate vector $\mathbf{r}$ is *linearly achievable for a network over a finite ring R* if the network has a fractional two-sided linear solution over R with rate vector $\mathbf{r}$.

D. Rate Regions, Capacity, and Solvability

The *rate region* of a network $\mathcal{N}$ is

$$\mathcal{R}(\mathcal{N}) = \{\mathbf{r} \in \mathbb{Q}^m : \mathbf{r} \text{ is achievable for } \mathcal{N}\},[2]$$

the *capacity* (also known as the "uniform capacity" or the "symmetric capacity") is

$$\mathcal{C}(\mathcal{N}) = \sup \{r \in \mathbb{Q} : (r, \ldots, r) \text{ is achievable for } \mathcal{N}\},$$

the *linear rate region* with respect to a ring alphabet R is

$$\mathcal{R}_{lin}(\mathcal{N}, R) = \left\{ \mathbf{r} \in \mathbb{Q}^m : \begin{array}{l} \mathbf{r} \text{ is linearly achievable} \\ \text{for } \mathcal{N} \text{ over } R \end{array} \right\},$$

and the *linear capacity* with respect to a ring alphabet R is

$$\mathcal{C}_{lin}(\mathcal{N}, R) = \sup \left\{ r \in \mathbb{Q} : \begin{array}{l} (r, \ldots, r) \text{ is linearly} \\ \text{achievable for } \mathcal{N} \text{ over } R \end{array} \right\}.$$

While the emphasis of this paper is on rate regions and capacities of networks, we define several solvability properties, as they will be useful in proving our main results. A $(k_1, \ldots, k_m, n)$ code, for which $k_1 = \cdots = k_m = n = t$, is also called a *$t$-dimensional vector* code, i.e., the block size of every message and edge is t, and a 1-dimensional vector code is called a *scalar* code. A network is said to be

- *solvable* if it has a scalar solution over some alphabet,
- *scalar linearly solvable over $_R G$* if it has a scalar linear solution over the module $_R G$, and
- *vector linearly solvable over $_R G$* if it has a t-dimensional vector linear solution over the module $_R G$, for some positive integer t.

Special cases of scalar and vector linear solvability over modules include scalar and vector linear solvability over rings, in which case the module is $_{R \otimes R} R$ (or equivalently, $_R R$,

---

[2] Some authors refer to the rate regions and linear rate regions of networks as "capacity regions" or "achievable rate regions" and sometimes define them as the convex hull or the topological closure of the set. We compare a network's linear rate regions over finite rings to its linear rate regions over finite fields, and our results immediately extend to these alternate definitions of rate regions.

if R is commutative). The all-one's vector is an achievable rate vector for any solvable network. We also comment that if a network has a t-dimensional vector solution over some alphabet $\mathcal{A}$, then it has a (possibly non-linear) scalar solution over the alphabet $\mathcal{A}^t$, so the network is solvable.

E. Related Work

In 2000, Ahlswede *et al.* [1] showed that some networks can attain higher capacities by using linear coding at network nodes, rather than just using routing operations. Since then, many results on linear network coding over finite fields have been achieved. On the other hand, the theoretical potential and limitations of linear network coding over non-field alphabets has been much less understood.

Li *et al.* [29] showed that when each of a network's receivers demands all of the messages (i.e., a *multicast* network), the linear capacity over any finite field is equal to the (nonlinear) capacity. Ho *et al.* [22] showed that for multicast networks, random fractional linear codes over finite fields achieve the network's capacity with probability approaching one as the block sizes increase. Jaggi *et al.* [25] developed polynomial-time algorithms for constructing capacity-achieving fractional linear codes over finite fields for multicast networks. Algorithms for constructing fractional linear solutions over finite fields for other classes of networks have also been a subject of considerable interest (e.g., [17], [24], [40], and [45]).

It is known (e.g., [11]) that for general networks, fractional linear codes over finite fields do not necessarily attain the network's capacity. In fact, it was shown by Lovett [31] that, in general, fractional linear network codes over finite fields cannot even approximate the capacity to any constant factor. Blasiak *et al.* [2] demonstrated a class of networks whose capacities are larger than their linear capacities over any finite field, by a factor that grows polynomially with the number of messages. Langberg and Sprintson [28] showed that, for general networks, constructing fractional solutions whose rates even approximate the capacity to any constant factor is NP-hard.

It was shown in [4] that the capacity of a network is independent of the coding alphabet. However, there are multiple examples in the literature (e.g., [7], [11], [15]) of networks whose linear capacity over a finite field can depend on the field alphabet, specifically by way of the characteristic of the field. Muralidharan and Rajan [35] demonstrated that a fractional linear solution over a finite field $\mathbb{F}$ exists for a network if and only if the network is associated with a discrete polymatroid representable over $\mathbb{F}$. Linear rank inequalities of vector subspaces and linear information inequalities (e.g., [44]) are known to be closely related and have been shown to be useful in determining or bounding networks' linear capacities over finite fields (e.g., [14], [15], and [18]).

Chan and Grant [5] demonstrated a duality between entropy functions and rate regions of networks and provided an alternate proof that fractional linear codes over finite fields do not necessarily attain the capacity. The relationship between network rate regions and entropy functions has been further studied, for example, in [6], [21], [36], and [43]. It has

also been shown (e.g., [13]) that non-Shannon information inequalities may be needed to determine the capacity of a network.

It was shown in [5] that fractional linear network codes over finite rings (and modules) are special cases of codes generated by Abelian groups. However, most other studies of linear capacity have generally been restricted to finite field alphabets. We will consider the case where the coding alphabet is viewed, more generally, as a finite ring.

We recently showed in [8] and [9] that scalar linear network codes over finite rings can offer solvability advantages over scalar linear network codes over finite fields in certain cases. Some of the results from these papers will be used in proofs in the present paper.

F. Main Results

The remainder of the paper is outlined as follows.

In Section II, we explore a connection between fractional linear codes and vector linear codes, which allows us to exploit network solvability results over modules [8], [9] in order to achieve capacity results over rings. For a given network $\mathcal{N}$ and rate vector $\mathbf{r}$, we show (in Lemma II.2) there exists a network $\mathcal{N}'$ that is vector linearly solvable over a given module if and only if the rate vector $\mathbf{r}$ is linearly achievable for $\mathcal{N}$ over the module. In Section II-B, we order finite modules based on fractional solvability and show that under certain conditions, fractional linear solutions over a given module imply the existence of fractional linear solutions over other modules. The results in Sections II-B and II-C are used to show (in Lemma II.14) that fractional linear solutions over modules imply the existence of fractional linear solutions over modules in which the ring of matrices over a field acts on vectors over the field.

In Section III, we use the results relating solvability and fractional codes from Section II to show our main results on linear rate regions over fields. We prove (in Theorem III.3) that for any two finite fields with different characteristics, there exists a network whose linear rate regions over the fields are not contained in one another. This indicates that some rate vectors may only be linearly achievable over certain fields, while other rate vectors may only be linearly achievable over other fields. Additionally, for any two finite fields with different characteristics, there exists a network whose linear capacities over the two fields are different (Corollary III.2).

We also show (in Theorem III.4) that for any two finite fields with the same characteristic, every network's linear rate region over the first field is the same as its linear rate region over the second field. In other words, the linear rate region of any network over a field depends only on the characteristic of the field. Consequently, the linear capacity of any network over a field depends only on the characteristic of the field as well (Corollary III.5). This contrasts with linear solvability over fields, since scalar linear solvability can depend not only on the field's characteristic, but more specifically, on the precise cardinality of the field (e.g., see [8, Lemma III.2], [37], [39]).

In Section IV, we prove our main results on linear rate regions and linear capacities over finite rings. We show (in Theorem IV.2) that for any network, any finite field,

and any finite ring whose size is divisible by the field's characteristic, the network's linear rate region over the ring is contained within the network's linear rate region over the field, and consequently the network's linear capacity over the ring is at most its linear capacity over the field (Corollary IV.3). In this sense, it suffices to restrict attention to finite fields when choosing a coding alphabet from among all rings. In other words, the general class of rings does not provide any benefit over the restricted class of finite fields, in terms of achieving linear rate regions with network coding. In order to prove Theorem IV.2, we show (in Theorem IV.1) that whenever a network has a fractional linear solution over some module with a given rate vector, the network has a fractional linear solution over some field with the same rate vector and potentially larger block sizes.

Even though Theorem IV.2 asserts non-field rings cannot provide an increase in linear capacity over fields for *all* networks, we show (in Corollary IV.4) that generally certain rings, smaller than a given field, can increase the linear capacity over at least *some* (but not all) networks. In fact, we show (in Theorem IV.5) that for any finite field and any finite ring, there exists a network with higher linear capacity over the ring than over the field if and only if the field's size and the ring's size are relatively prime. Finally, we show (in Corollary IV.6) that whenever a network has a fractional linear solution over some ring (or module) with a uniform rate arbitrarily close to 1, the network must also have a fractional linear solution over some field with the same uniform rate. This strengthens results in [7] and [11] by showing that the non-linearly solvable networks presented in these papers additionally are not asymptotically linearly solvable over rings and modules.

II. FRACTIONAL AND VECTOR CODES OVER MODULES

Many techniques for upper bounding network linear capacities over finite fields (e.g., [7], [11], [14]) exploit linear algebra results that sometimes do not extend to matrices over arbitrary rings. For example, it is known (e.g., see [20]) that the transpose of an invertible matrix over a non-commutative ring is not necessarily invertible. [3] This suggests that directly computing network linear rate regions and linear capacities over finite rings and modules may be somewhat difficult.

One method for determining whether a network satisfies some solvability or capacity property is to transform the question into whether a certain related network satisfies a corresponding property (e.g., [26], [41], and [42]). Namely, in [41] and [42], the authors show that determining the rate region and linear rate region of a general network can be reduced to determining the rate region and linear rate region of a corresponding network where each message vector is demanded by exactly one receiver (i.e., a *multiple unicast* network). In [26], it is shown that determining whether a multiple unicast network has a solution with a given rate vector can be reduced to determining whether a corresponding unicast network with two message-receiver pairs has a solution with a corresponding rate vector.

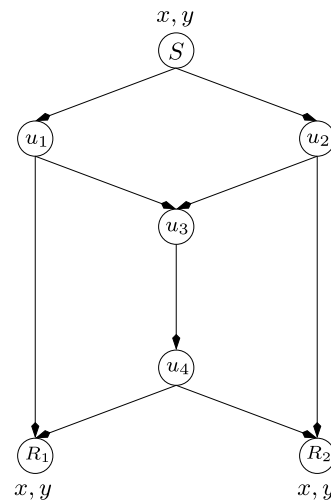[3]See [3] and [33] for more information on linear algebra over rings.

Fig. 1. The Butterfly network has a single source node S, which generates message vectors x and y. Each of the receiver nodes R_1 and R_2 demands both x and y. The linear rate region of the Butterfly network is $\{(r_x, r_y) \in \mathbb{Q}^2 : r_x, r_y \geq 0 \text{ and } r_x + r_y \leq 2\}$ over any ring.

We use a similar approach to relate the existence of fractional linear solutions over modules to scalar and vector linear solvability over modules (which was studied in [8] and [9]). The results in this section allow us to more easily relate a network's linear rate region over a ring to the network's linear rate region over some field.

A. Fractional Equivalent Network

For any network $\mathcal{N}$ with m message vectors and integers $k_1, \ldots, k_m \geq 0$ and $n \geq 1$, the following defines a new network which is vector linearly solvable over a module $_RG$ if and only if $\mathcal{N}$ has a fractional linear solution over $_RG$ whose rate vector is $(k_1/n, \ldots, k_m/n)$. We prove this fact in Lemma II.2. This network construction can be used to show many linear solvability properties extend to the existence of fractional linear solutions.

Definition II.1. For any network $\mathcal{N}$ with m message vectors and any integers $k_1, \ldots, k_m \geq 0$ and $n \geq 1$, let $\mathcal{N}^{(k_1,\ldots,k_m,n)}$ denote the network $\mathcal{N}$ but with

(i) each edge replaced with n parallel edges, and
(ii) the ith message vector replaced with k_i message vectors.

The *Butterfly network* is defined in Figure 1, and, for each $k_x, k_y \geq 0$ and $n \geq 1$, the (k_x, k_y, n)-*Butterfly network* is defined in Figure 2. These networks are consistent with Definition II.1, if they are denoted by $\mathcal{N}$ and $\mathcal{N}^{(k_x,k_y,n)}$, respectively.

Lemma II.2. *Let $\mathcal{N}$ be a network with m message vectors, let $k_1, \ldots, k_m \geq 0$ and $n, t \geq 1$ be integers, let $_RG$ be a module, and let $\mathcal{N}^{(k_1,\ldots,k_m,n)}$ denote the network in Definition II.1 corresponding to $\mathcal{N}$ and $k_1, \ldots, k_m$ and n. The network $\mathcal{N}$ has a $(tk_1, \ldots, tk_m, tn)$ linear solution over $_RG$ if and only if $\mathcal{N}^{(k_1,\ldots,k_m,n)}$ has a t-dimensional vector linear solution over $_RG$.*

Proof: In a $(tk_1, \ldots, tk_m, tn)$ linear code over module $_RG$ for network $\mathcal{N}$, suppose a node generates the l_1th,$\ldots$,l_uth

$x_1, \ldots, x_{k_x}$
$y_1, \ldots, y_{k_y}$

$x_1, \ldots, x_{k_x}$　　　　　$x_1, \ldots, x_{k_x}$
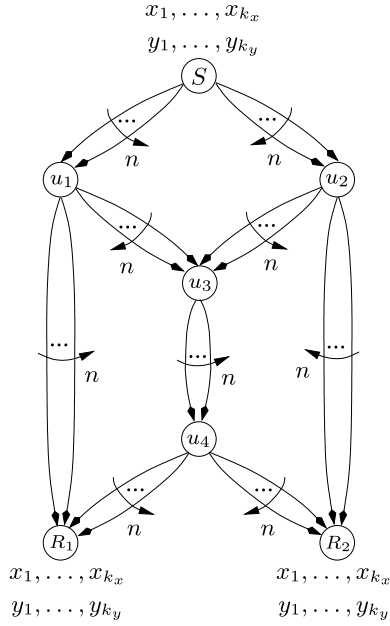$y_1, \ldots, y_{k_y}$　　　　　$y_1, \ldots, y_{k_y}$

Fig. 2.　　The (k_x, k_y, n)-Butterfly network has a single source node, which generates message vectors $x_1, \ldots, x_{k_x}$ and $y_1, \ldots, y_{k_y}$. Each receiver demands all of the message vectors. The (k_x, k_y, n)-Butterfly network is vector linearly solvable over a given ring if and only if $k_x + k_y \le 2n$.

message vectors and has v incoming edges, where the ith message vector is an element of G^{tk_i} and the edge vectors are elements of G^{tn}. Then an edge function

$$f : \underbrace{G^{tk_{l_1}} \times \cdots \times G^{tk_{l_u}}}_{u \text{ message vectors}} \times \underbrace{G^{tn} \times \cdots \times G^{tn}}_{v \text{ edge vectors}} \longrightarrow G^{tn}$$

of an outgoing edge of the node is of the form $f(\mathbf{x}) = A\mathbf{x}$ where A is a $tn \times (tk_1 l_1 + \cdots + tk_{l_u} + vtn)$ matrix with entries in R and $\mathbf{x}$ is a vector over G formed by concatenating the input vectors of the node. Let $A_1, \ldots, A_n$ denote the $t \times (tk_1 l_1 + \cdots + tk_{l_u} + vtn)$ matrices such that A can be written in block form as

$$A = \begin{bmatrix} A_1 \\ \vdots \\ A_n \end{bmatrix}.$$

The corresponding node in $\mathcal{N}^{(k_1, \ldots, k_m, n)}$ generates $k_{l_1} + \cdots + k_{l_u}$ message vectors and has vn incoming edge vectors. Define the t-dimensional vector code for $\mathcal{N}^{(k_1, \ldots, k_m, n)}$ over $_R G$ by letting the edge function of the ith parallel corresponding outgoing edge be the linear mapping

$$f_i : \underbrace{G^t \times \cdots \times G^t}_{k_{l_1} + \cdots + k_{l_u} \text{ message vectors}} \times \underbrace{G^t \times \cdots \times G^t}_{vn \text{ edge vectors}} \longrightarrow G^t$$

given by $f_i(\mathbf{x}) = A_i \mathbf{x}$, where $i = 1, \ldots, n$. The edge in the code for $\mathcal{N}$ carries the same linear combination of its inputs as the n parallel edges in the code for $\mathcal{N}^{(k_1, \ldots, k_m, n)}$.

Similarly, in a $(tk_1, \ldots, tk_m, tn)$ code for $\mathcal{N}$, suppose a receiver generates the l_1th,$\ldots, l_u$th message vectors, has v

incoming edges, and demands x_j. Then the decoding function

$$d : \underbrace{G^{tk_{l_1}} \times \cdots \times G^{tk_{l_u}}}_{u \text{ message vectors}} \times \underbrace{G^{tn} \times \cdots \times G^{tn}}_{v \text{ edge vectors}} \longrightarrow G^{tk_j}$$

corresponding to x_j is of the form $f(\mathbf{x}) = D\mathbf{x}$ where D is a $tk_j \times (tk_1 l_1 + \cdots + tk_{l_u} + vtn)$ matrix and $\mathbf{x}$ is a vector over G formed by concatenating the input vectors of the node. Let $D_1, \ldots, D_{k_j}$ denote the $t \times (tk_1 l_1 + \cdots + tk_{l_u} + vtn)$ matrices such that D can be written in block form as

$$D = \begin{bmatrix} D_1 \\ \vdots \\ D_{k_j} \end{bmatrix}.$$

The corresponding node in $\mathcal{N}^{(k_1, \ldots, k_m, n)}$ generates $k_{l_1} + \cdots + k_{l_u}$ message vectors, has vn incoming edge vectors, and demands the k_j message vectors corresponding to x_j. Define the t-dimensional vector code for $\mathcal{N}^{(k_1, \ldots, k_m, n)}$ over $_R G$ by letting the decoding function, corresponding to the ith such message vector, be the linear mapping

$$d_i : \underbrace{G^t \times \cdots \times G^t}_{k_{l_1} + \cdots + k_{l_u} \text{ message vectors}} \times \underbrace{G^t \times \cdots \times G^t}_{vn \text{ edge vectors}} \longrightarrow G^t$$

given by $d_i(\mathbf{x}) = D_i \mathbf{x}$, where $i = 1, \ldots, k_j$. If the function d correctly reproduces its demanded message vectors in the $(tk_1, \ldots, tk_m, tn)$ code for $\mathcal{N}$, then each of $d_1, \ldots, d_{k_j}$ correctly reproduces its demanded message vector in the t-dimensional code for $\mathcal{N}^{(k_1, \ldots, k_m, n)}$. Hence, any $(tk_1, \ldots, tk_m, tn)$ linear solution over a module $_R G$ for $\mathcal{N}$ can be translated to a t-dimensional vector linear solution over $_R G$ for $\mathcal{N}^{(k_1, \ldots, k_m, n)}$.

A t-dimensional vector linear solution over the module $_R G$ for $\mathcal{N}^{(k_1, \ldots, k_m, n)}$ can similarly be translated to a $(tk_1, \ldots, tk_m, tn)$ linear solution over $_R G$ for $\mathcal{N}$. In particular, if $f_1, \ldots, f_n$ are the edge functions of the n parallel edges at a node in a t-dimensional vector linear solution for $\mathcal{N}^{(k_1, \ldots, k_m, n)}$, then in the $(tk_1, \ldots, tk_m, tn)$ linear code over $_R G$ for $\mathcal{N}$, define the corresponding edge function to be

$$f(\mathbf{x}) = \begin{bmatrix} f_1(\mathbf{x}) \\ \vdots \\ f_n(\mathbf{x}) \end{bmatrix}.$$

Similarly, if $d_1, \ldots, d_{k_j}$ are the decoding functions at a node in a t-dimensional vector linear solution for $\mathcal{N}^{(k_1, \ldots, k_m, n)}$, then in the $(tk_1, \ldots, tk_m, tn)$ linear code over $_R G$ for $\mathcal{N}$, define the corresponding decoding function $d(\mathbf{x})$ to be the vector obtained by concatenating $d_1(\mathbf{x}), \ldots, d_{k_j}(\mathbf{x})$. This $(tk_1, \ldots, tk_m, tn)$ linear code for $\mathcal{N}$ over $_R G$ is a solution, since the t-dimensional vector linear code for $\mathcal{N}^{(k_1, \ldots, k_m, n)}$ is a solution. ∎

When $_R G$ is a module and t is a positive integer, $_{M_t(R)} G^t$ denotes the module in which the ring of all $t \times t$ matrices with entries in R acts on the set of all t-vectors over G with matrix-vector multiplication, where multiplication of elements of R with elements of G is given by the action of $_R G$. The following lemma shows an equivalence between fractional linear codes over modules and fractional linear codes over these vector modules.

Lemma II.3. *Let $_RG$ be a module, let $\mathcal{N}$ be a network, and let $k_1, \ldots, k_m \geq 0$ and $n, t \geq 1$ be integers. Network $\mathcal{N}$ has a $(k_1, \ldots, k_m, n)$ linear solution over $_{M_t(R)}G^t$ if and only if $\mathcal{N}$ has a $(tk_1, \ldots, tk_m, tn)$ linear solution over $_RG$.*

Proof: This lemma follows from the fact that a scalar linear solution over $_{M_t(R)}G^t$ is equivalent to a t-dimensional vector linear solution over $_RG$. In particular, in both a scalar linear code over $_{M_t(R)}G^t$ and a t-dimensional vector linear code over $_RG$, inputs to a node are t-vectors over G and outputs carry linear combinations of the inputs, where the coefficients that describe the linear combination are $t \times t$ matrices over R. Any scalar linear solution over $_{M_t(R)}G^t$ can be translated to a t-dimensional vector linear solution over $_RG$ and vice versa. This idea generalizes to fractional linear solutions:

$\mathcal{N}$ has a $(k_1, \ldots, k_m, n)$ linear solution over $_{M_t(R)}G^t$

$\iff \mathcal{N}^{(k_1, \ldots, k_m, n)}$ has a scalar linear solution over $_{M_t(R)}G^t$

$\iff \mathcal{N}^{(k_1, \ldots, k_m, n)}$ has a t-dim linear solution over $_RG$

$\iff \mathcal{N}$ has a $(tk_1, \ldots, tk_m, tn)$ linear solution over $_RG$

where the first and third implications follow from Lemma II.2. ∎

B. Fractional Dominance

Definition II.4. Let $_RG$ and $_SH$ be modules. We say that

(a) $_SH$ *scalarly dominates* $_RG$ if every network with a scalar linear solution over $_RG$ also has a scalar linear solution over $_SH$,

(b) $_SH$ *fractionally dominates* $_RG$ if for each $k_1, \ldots, k_m \geq 0$ and $n \geq 1$, every network with a $(k_1, \ldots, k_m, n)$ linear solution over $_RG$ also has a $(k_1, \ldots, k_m, n)$ linear solution over $_SH$.

We are ultimately concerned with comparing capacities and rate regions using one-sided and two-sided linear codes over rings, and module dominance provides a useful tool for comparing these classes of codes. In the following remark, we discuss one-sided and two-sided linear codes over rings in the context of fractional dominance of modules.

Remark II.5. *Any left-sided fractional linear code over a ring is a special case of a two-sided fractional linear code over the ring in which the inputs are multiplied on the right by the identity element. In the language of modules, this means that any fractional linear solution over $_RR$ is also a fractional linear solution over $_{R \otimes R^{op}}R$. Hence $_{R \otimes R^{op}}R$ fractionally dominates $_RR$ for every finite ring R. Furthermore, if the ring R is commutative, then any two-sided fractional linear code over R can equivalently be written as a left-sided fractional linear code over R. This implies $_RR$ fractionally dominates $_{R \otimes R^{op}}R$ when R is commutative.*

We also comment that if R and S are finite rings such that $_{S \otimes S^{op}}S$ fractionally dominates $_{R \otimes R^{op}}R$, then for each network $\mathcal{N}$, we have

$$\mathcal{R}_{lin}(\mathcal{N}, S) \supseteq \mathcal{R}_{lin}(\mathcal{N}, R) \quad \text{and} \quad \mathcal{C}_{lin}(\mathcal{N}, S) \geq \mathcal{C}_{lin}(\mathcal{N}, R).$$

The following lemma shows that scalar dominance and fractional dominance of modules are, in fact, equivalent.

However, it is cleaner to prove results on scalar dominance, as the block sizes of the message vectors and edge vectors are all one, and we can use results from [9].

Lemma II.6. *Let $_RG$ and $_SH$ be modules. $_SH$ scalarly dominates $_RG$ if and only if $_SH$ fractionally dominates $_RG$.*

Proof: It follows immediately from the definition that $_SH$ fractionally dominates $_RG$ implies $_SH$ scalarly dominates $_RG$. To prove the converse, suppose $_SH$ scalarly dominates $_RG$. Let $\mathcal{N}$ be a network with m message vectors, let $k_1, \ldots, k_m \geq 0$ and $n \geq 1$ be integers, and let $\mathcal{N}^{(k_1, \ldots, k_m, n)}$ be the network in Definition II.1 corresponding to $\mathcal{N}$, $k_1, \ldots, k_m$, and n. Then

$\mathcal{N}$ has a $(k_1, \ldots, k_m, n)$ linear solution over $_RG$

$\implies \mathcal{N}^{(k_1, \ldots, k_m, n)}$ has a scalar linear solution over $_RG$

[from Lemma II.2]

$\implies \mathcal{N}^{(k_1, \ldots, k_m, n)}$ has a scalar linear solution over $_SH$

$\left[\text{from } S \text{ scalarly dominates } R\right]$

$\implies \mathcal{N}$ has a $(k_1, \ldots, k_m, n)$ linear solution over $_SH$

[from Lemma II.2].

Hence, for any network, any fractional linear solution over $_RG$ implies the existence of a fractional linear solution over $_SH$ with the same block sizes. ∎

Definition II.7. A module $_RG$ is *faithful* if for each $r \in R \backslash \{0\}$, there exists $g \in G$ such that $r \cdot g \neq 0$.

Lemmas II.8, II.9, and II.10 follow immediately from Lemma II.6 and results from [9], and we include their proofs in the appendix for reference. Lemma II.8 shows that, for a fixed ring R, fractional linear solutions over faithful R-modules induce fractional linear solutions over every other R-module. Lemma II.9 shows that fractional linear solutions over non-faithful modules induce fractional linear solutions over some faithful module. Lemma II.10 shows that ring homomorphisms also induce fractional dominance.

Lemma II.8. *Let R be a fixed ring, let $_RG$ and $_RH$ be modules, and let $_RG$ be faithful. Then $_RH$ fractionally dominates $_RG$.*

In [9], an example was given in which a network has a scalar linear solution over a non-faithful R-module but does not have any scalar linear solutions over another R-module. This shows the importance of the faithfulness of the module in Lemma II.8.

Lemma II.9. *Let $_RG$ be a module. There exists a finite ring S and an action such that $_SG$ is a faithful module, and $_SG$ fractionally dominates $_RG$.*

A *ring homomorphism* is a mapping ϕ from a ring R to a ring S such that for all $a, b \in R$

$$\phi(a + b) = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(a)\phi(b)$$
$$\phi(1_R) = 1_S$$

where 1_R and 1_S are the multiplicative identities of R and S, respectively. It follows from this definition that $\phi(0_R) = 0_S$, where 0_R and 0_S are the additive identities of R and S, respectively.

Lemma II.10. *Let R and S be rings, let $\phi : R \to S$ be a ring homomorphism, let $_RG$ be a faithful module, and let $_SH$ be a module. Then $_SH$ fractionally dominates $_RG$.*

By the fundamental theorem of finite Abelian groups, every finite Abelian group is isomorphic to a direct product of cyclic groups whose sizes are prime powers (with component-wise addition) [16, p. 161]. As an example, $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$. The following lemma shows that if a finite Abelian group can be written as a direct product of Abelian groups G and H whose sizes are relatively prime, then whenever $_R(G \times H)$ is a module for some ring R, the ring R acts on $G \times H$ component-wise. This implies that G and H are also R-modules. Since fractional linear solutions over faithful R-modules induce fractional linear solutions over every other R-module, this is a useful tool for showing fractional dominance.

Lemma II.11. *Let G and H be finite groups such that $|G|$ and $|H|$ are relatively prime, and let $_R(G \times H)$ be a module. Then there exist modules $_RG$ and $_RH$.*

Proof: Let $g \in G$ and $r \in R$, and suppose $r \cdot (g, 0) = (g_r, h_r) \in G \times H$. It follows from Lagrange's theorem of finite groups (e.g., [16, p. 45]) that $|G|g = \underbrace{g \oplus \cdots \oplus g}_{|G| \text{ times}} = 0$, so

$$(0, 0) = r \cdot (0, 0) = r \cdot (|G|\, g, 0) = |G|\, r \cdot (g, 0)$$
$$= |G|\, (g_r, h_r) = (|G|g_r, |G|h_r) = (0, |G|h_r).$$

Since $|G|$ and $|H|$ are relatively prime, it follows from Cauchy's theorem of finite groups (e.g., [16, p. 93]) that H contains no non-identity elements whose order divides $|G|$, so it must be the case that $h_r = 0$. Similarly, for each $h \in H$ and each $r \in R$, there exists $h_r \in H$ such that $r \cdot (0, h) = (0, h_r)$. This implies R acts on $G \times H$ component-wise. In other words, if $r \cdot (g, h) = (g_r, h_r)$, then $r \cdot (g, 0) = (g_r, 0)$ and $r \cdot (0, h) = (0, h_r)$. Thus the mapping $\odot : R \times G \to G$ given by $r \odot g = g_r$ satisfies the properties of an action, so G is an R-module with action $\odot$. It can similarly be shown that $_RH$ is a module. ∎

We comment that Lemma II.11 does not extend to finite groups whose sizes are not relatively prime. As an example, the field GF(4) acts on its own additive group $(\mathrm{GF}(4), +)$ by multiplication in the field. If the elements of GF(4) are represented as $\{0, 1, \alpha, \alpha + 1\}$ where $\alpha^2 = \alpha + 1$, then for all $(a_0 + \alpha a_1), (b_0 + \alpha b_1) \in \mathrm{GF}(4)$

$$(a_0 + \alpha a_1)(b_0 + \alpha b_1)$$
$$= a_0\, b_0 + a_1\, b_1 + \alpha(a_0\, b_1 + a_1\, b_0 + a_1\, b_1).$$

The additive group of GF(4) is isomorphic to the set $\mathrm{GF}(2) \times \mathrm{GF}(2)$ with component-wise addition in GF(2), so GF(4) acts on $\mathrm{GF}(2) \times \mathrm{GF}(2)$ by

$$(a_0 + \alpha\, a_1) \cdot (b_0, b_1)$$
$$= (a_0\, b_0 + a_1\, b_1, \; a_0\, b_1 + a_1\, b_0 + a_1\, b_1).$$

This action is not component-wise, since $(1 + \alpha) \cdot (1, 0) = (1, 1)$ and $\alpha \cdot (0, 1) = (1, 1)$.

If GF(4) acts on GF(2), then the action must be such that $1 \cdot a = a$ and $0 \cdot a = 0$ for all $a \in \mathrm{GF}(2)$ and $x \cdot 0 = 0$ for all $x \in \mathrm{GF}(4)$. If $\alpha \cdot 1 = 1$, then

$$0 = 1 + 1 = (\alpha \cdot 1) + (1 \cdot 1) = (\alpha + 1) \cdot 1$$
$$= (\alpha^2) \cdot 1 = \alpha \cdot (\alpha \cdot 1) = \alpha \cdot 1 = 1$$

which is a contradiction. If $\alpha \cdot 1 = 0$, then

$$1 = 0 + 1 = (\alpha \cdot 1) + (1 \cdot 1) = (\alpha + 1) \cdot 1$$
$$= (\alpha^2) \cdot 1 = \alpha \cdot (\alpha \cdot 1) = \alpha \cdot 0 = 0$$

which is a contradiction. Thus GF(2) cannot form a GF(4)-module, but $\mathrm{GF}(2) \times \mathrm{GF}(2)$ together with the action described above is a GF(4)-module.

C. Matrix Rings Over Fields

If a ring R has a proper two-sided ideal I, then there is a surjective homomorphism from R to R/I. It is known (e.g., [32, p. 20]) that every finite ring with no proper two-sided ideals is isomorphic to some ring of matrices over a finite field. In fact, every finite ring R has a two-sided ideal I such that R/I is a matrix ring over a field. This implies the following lemma, which was more formally shown in [9].

Lemma II.12. *[9, Lemmas II.1 and II.3]: Let R be a finite ring. There exists a positive integer t, a finite field $\mathbb{F}$, and a surjective homomorphism from R to $M_t(\mathbb{F})$.*

Lemmas II.10 and II.12 together imply that fractional linear solutions over modules induce fractional linear solutions over modules in which the ring is a matrix ring over a field. The following lemma proves a result on the cardinality of such modules.

Lemma II.13. *Let $\mathbb{F}$ be a finite field and t a positive integer. If $_{M_t(\mathbb{F})}G$ is a finite non-zero module, then $|\mathbb{F}|^t$ divides $|G|$.*

Proof: Since G is finite and non-zero, there exists a submodule of $_{M_t(\mathbb{F})}G$ with no proper submodules (possibly $_{M_t(\mathbb{F})}G$ itself). It is known (e.g., [27, Theorem 3.3 (2), p. 31]) that $\mathbb{F}^t$ is the only $M_t(\mathbb{F})$-module with no proper submodules, so $\mathbb{F}^t$ is a submodule of G. Hence by Lagrange's theorem of finite groups, $|\mathbb{F}|^t$ divides $|G|$. ∎

Lemma II.14 shows that every module is fractionally dominated by a module whose group is the set of t vectors over some field and whose ring is the set of all $t \times t$ matrices over the field. In network coding, arbitrarily large block sizes may be needed to achieve a solution with a particular rate. Das and Rai [10] showed that for each $k, n \geq 1$ and each $t \geq 2$, there exists a network that has a $(tk, \ldots, tk, tn)$ linear solution over any finite field, yet the network has no $(sk, \ldots, sk, sn)$ linear solution over any finite field when $s < t$. It was also shown in [9] that for each $t \geq 2$, there exist networks with scalar linear solutions over certain rings but with no s-dimensional vector linear solutions over any field whenever $s < t$. This suggests that the quantity t in Lemma II.14 may need to be arbitrarily large.

Lemma II.14. *Let $_RG$ be a module. For each prime p that divides $|G|$, there exists a finite field $\mathbb{F}$ of characteristic p and a positive integer t such that $_{M_t(\mathbb{F})}\mathbb{F}^t$ fractionally dominates $_RG$.*

Proof: By Lemma II.9 there exists a finite ring S such that the faithful module $_SG$ fractionally dominates $_RG$. By the fundamental theorem of finite Abelian groups, the group G is isomorphic to a direct product of Abelian groups whose sizes are prime powers, and since $p \mid |G|$, the size of at least one of these groups is a power of p. Let H be the direct product of all such groups whose sizes are powers of p. Then there exists a finite group G' such that $G \cong G' \times H$ and $|G'|$ and

$|H|$ are relatively prime. Hence by Lemma II.11, H is also an S-module, and since G is a faithful S-module, by Lemma II.8, the module $_SH$ fractionally dominates $_SG$.

By Lemma II.9, there exists a finite ring S' such that H is a faithful S'-module and $_{S'}H$ fractionally dominates $_SH$. By Lemma II.12, there exists a positive integer t, a finite field $\mathbb{F}$, and a surjective homomorphism from S' to $M_t(\mathbb{F})$. By Lemma II.10, the module $_{S'}H$ is fractionally dominated by every $M_t(\mathbb{F})$-module, and the ring $M_t(\mathbb{F})$ acts on the set of all t-vectors over $\mathbb{F}$ by matrix-vector multiplication over $\mathbb{F}$, so $_{M_t(\mathbb{F})}\mathbb{F}^t$ fractionally dominates $_{S'}H$. The proof of Lemma II.10 also implies H is an $M_t(\mathbb{F})$-module, so Lemma II.13 implies $|\mathbb{F}|^t \mid |H|$. Since $|H|$ is a power of p, this implies $\mathbb{F}$ is a field of characteristic p. Finally, by the transitivity of fractional dominance, $_{M_t(\mathbb{F})}\mathbb{F}^t$ fractionally dominates $_RG$. ∎

Lemma II.15 uses ideas similar to those in [38, Proposition 1] and [17], and we include a proof for completeness. This lemma, along with Lemma II.3, implies that a fractional linear solution over any non-prime finite field induces a fractional linear solution over the corresponding prime field with the same rate vector. A fractional linear solution over a field $\mathbb{F}$ is equivalent to a fractional linear solution over the faithful module $_\mathbb{F}\mathbb{F}$, since $\mathbb{F}$ is commutative.

Lemma II.15. *Let q be a prime power and t a positive integer. Then $_{M_t(\mathrm{GF}(q))}\mathrm{GF}(q)^t$ fractionally dominates $_{\mathrm{GF}(q^t)}\mathrm{GF}(q^t)$.*

Proof: It is known (e.g., see [16, p. 531]) that every extension field $\mathrm{GF}(q^t)$ is isomorphic to a set of $t \times t$ matrices over $\mathrm{GF}(q)$. This implies there exists an injective homomorphism from $\mathrm{GF}(q^t)$ to $M_t(\mathrm{GF}(q))$. By Lemma II.10, any network with a fractional linear solution over $_{\mathrm{GF}(q^t)}\mathrm{GF}(q^t)$ also has a fractional linear solution over any $M_t(\mathrm{GF}(q))$-module. In particular, $_{M_t(\mathrm{GF}(q))}\mathrm{GF}(q)^t$ fractionally dominates $_{\mathrm{GF}(q^t)}\mathrm{GF}(q^t)$. ∎

III. Linear Rate Regions Over Fields

We define, for each integer $m \geq 2$, the *Char-m network* in Figure 3. The Char-m network is denoted by $\mathcal{N}_2(m,1)$ in [7], with a slight relabeling of sources, and the Char-m network is known to be vector linearly solvable over a field if and only if the characteristic of the field divides m. When $m = 2$, this network exhibits solvability properties similar to those of the Fano network [13].

Let R be a finite ring whose characteristic divides m. Then $m = 0$ in R, and the following scalar linear code:

$$e = \sum_{j=0}^{m+1} x_j \quad \text{and} \quad e_i = \sum_{\substack{j=0 \\ j \neq i}}^{m+1} x_j$$

over R is a solution for the Char-m network, where $i = 0, 1, \ldots, m+1$, and the receivers linearly recover their demands as follows

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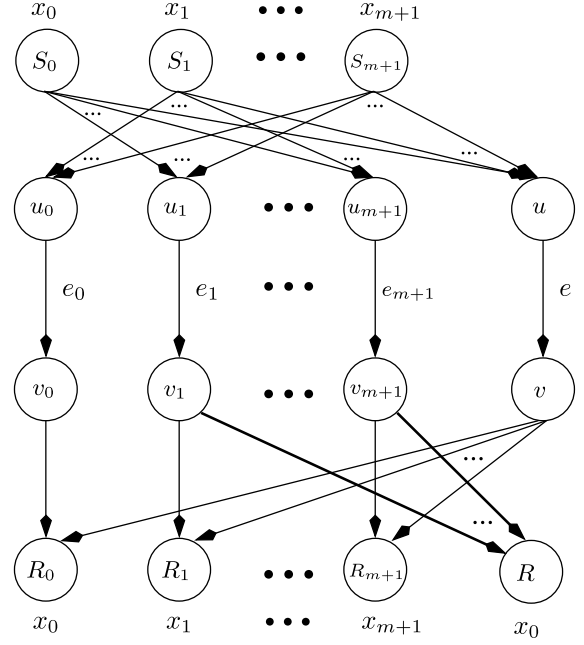$$= x_0 \qquad [\text{from char}(R) \mid m].$$

Fig. 3. The Char-m network has source nodes $S_0, S_1, \ldots, S_{m+1}$ which generate message vectors $x_0, x_1, \ldots, x_{m+1}$, respectively. Node u has a single incoming edge from each source node, and the edge connecting nodes u and v carries the edge vector e. For each $i = 0, 1, \ldots, m+1$, node u_i has a single incoming edge from each source node, except S_i. The edge connecting nodes u_i and v_i carries edge vector e_i. The receiver R_i demands x_i and has an incoming edge from node v_i and an incoming edge from v. The receiver R demands x_0 and has an incoming edge from each of nodes $v_1, \ldots, v_{m+1}$.

This code relies on the fact that $m = 0$ in R, and it turns out the Char-m network has no scalar linear solutions over any ring whose characteristic does not divide m (see [7, Lemma IV.6]).

Lemma III.1. *[7, Lemma IV.7]: For each $m \geq 2$ and each finite field $\mathbb{F}$, the linear capacity of the Char-m network is*

- *equal to 1, whenever $\mathrm{char}(\mathbb{F}) \mid m$, and*
- *upper bounded by $1 - \frac{1}{2m+3}$, whenever $\mathrm{char}(\mathbb{F}) \nmid m$.*

A. Comparing Linear Rate Regions Over Different Fields

It follows from Lemma III.1 that certain fields may yield strictly larger linear capacities for some networks than other fields. In particular, whenever the characteristics of two finite fields are different, there exists some network whose linear capacities over the fields differ.

Corollary III.2. *If $\mathbb{F}$ and $\mathbb{K}$ are finite fields with different characteristics, then there exist networks $\mathcal{N}_1$ and $\mathcal{N}_2$, such that $\mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{F}) > \mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{K})$ and $\mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{K}) > \mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{F})$.*

Proof: Suppose $\mathrm{char}(\mathbb{F}) = p \neq q = \mathrm{char}(\mathbb{K})$ and let $\mathcal{N}_1$ and $\mathcal{N}_2$ be the Char-p network and the Char-q network, respectively. Then by Lemma III.1, $\mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{F}) = 1$ and $\mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{K}) \leq 1 - \frac{1}{2p+3}$. Similarly, $\mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{K}) = 1$ and $\mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{F}) \leq 1 - \frac{1}{2q+3}$. ∎

In [14], it was shown that for any finite fields $\mathbb{F}$ and $\mathbb{K}$ of even and odd characteristic, respectively: (i) the linear rate region of the non-Fano network over $\mathbb{F}$ is a proper subset of its linear rate region over $\mathbb{K}$, and (ii) the linear rate region of the Fano network over $\mathbb{K}$ is a proper subset of its linear rate

region over $\mathbb{F}$. In these instances, it is strictly "better" to use an even (respectively, odd) characteristic field instead of an odd (respectively, even) characteristic field. However, the following theorem demonstrates that it may not always be the case that one field is necessarily "better" than the other for a particular network. In particular, for some networks, some rate vectors may only be linearly achievable over certain fields while other rate vectors may only be linearly achievable over other fields.

Theorem III.3. *For any two finite fields with different characteristics, there exists a network whose linear rate regions over the fields do not contain one another.*

Proof: A *disjoint union* of networks refers to a new network whose nodes/edges/sources/receivers are the disjoint union of the nodes/edges/sources/receivers in the smaller networks. Let $\mathbb{F}$ and $\mathbb{K}$ be finite fields of characteristic p and q, for some distinct primes p and q. Let $\mathcal{N}$ be the disjoint union of the Char-p network and the Char-q network. Whenever node (respectively, edge and message) labels are repeated, add an arbitrary additional level of labeling each node (respectively, edge and message) to avoid repeated labels. Then, by Lemma III.1, the rate vector, in which the rates for the Char-p network are all one and the rates for the Char-q network are all zero, is linearly achievable over $\mathbb{F}$ but not over $\mathbb{K}$. Similarly, the rate vector in which the rates for the Char-q network are all one and the rates for the Char-p network are all zero is linearly achievable over $\mathbb{K}$ but not over $\mathbb{F}$. Thus the linear rate regions of $\mathcal{N}$ over $\mathbb{F}$ and $\mathbb{K}$ do not contain one another. ■

We can use a similar network construction to show that there is not necessarily a particular finite field that can linearly achieve all linearly achievable rate vectors. In other words, there may not be a "best" field for a particular network. Let p and q be distinct primes, and let $\mathcal{N}$ be the disjoint union of the Char-p network and the Char-q network. Then, by a similar argument to the proof of Theorem III.3, there exists a rate vector that is only linearly achievable over fields of characteristic p, and there exists another rate vector that is only linearly achievable over fields of characteristic q. Thus there is no finite field which can linearly achieve both of these rate vectors. A similar result can be obtained by taking the disjoint union of the Fano and non-Fano networks.

Theorem III.3 demonstrates that for any two finite fields of distinct characteristics, there always exists some network whose linear rate regions differ over the two fields. In the following theorem, we show that the linear rate region of a network over a field depends only on the characteristic of the field. This contrasts with the scalar linear solvability of networks over fields, since some networks can be scalar linearly solvable only over certain fields of a given characteristic.

Theorem III.4. *Let $\mathbb{F}$ and $\mathbb{K}$ be finite fields. Then* char$(\mathbb{F}) =$char$(\mathbb{K})$ *if and only if for each network $\mathcal{N}$, we have* $\mathcal{R}_{lin}(\mathcal{N}, \mathbb{F}) = \mathcal{R}_{lin}(\mathcal{N}, \mathbb{K})$.

Proof: Let r and s be positive integers, p a prime, and $\mathcal{N}$ a network with m messages. Then GF(p) is a subfield GF(p^s), which implies the identity mapping is an injective

homomorphism from GF(p) to GF(p^s). So

$\mathcal{N}$ has a $(k_1, \dots, k_m, n)$ linear solution over GF(p^r)
$\implies \mathcal{N}$ has $(rk_1, \dots, rk_m, rn)$ linear solution over GF(p)
[from Lemma II.15]
$\implies \mathcal{N}$ has $(rk_1, \dots, rk_m, rn)$ linear solution over GF(p^s)
[from Lemma II.10] .

Both a

$$(k_1, \dots, k_m, n)$$

linear solution and an

$$(rk_1, \dots, rk_m, rn)$$

linear solution have the rate vector $(k_1/n, \dots, k_m/n)$. Hence any rate vector that is linearly attainable over GF(p^r) is also linearly attainable over GF(p^s) (with possibly larger vector sizes). Similarly, any rate vector that is linearly attainable over GF(p^s) is also linearly attainable over GF(p^r) (with possibly larger vector sizes). Hence if char$(\mathbb{F}) =$char$(\mathbb{K})$, then the linear rate regions of any network over $\mathbb{F}$ and $\mathbb{K}$ are equal. The reverse direction follows from Theorem III.3. ■

Immediately following Definition II.4, we showed that for any finite rings S and R,

$_{S \otimes S^{op}}S$ fractionally dominates $_{R \otimes R^{op}}R$
$\implies \mathcal{R}_{lin}(\mathcal{N}, S) \supseteq \mathcal{R}_{lin}(\mathcal{N}, R)$ for every network $\mathcal{N}$.

Theorem III.4 can be used to show the converse is not necessarily true. There are numerous examples in the literature (e.g., see [8, Lemma III.2], [37], [39]) of networks that are scalar linearly solvable over GF(p^r) but not over GF(p^s), for some prime p and some distinct positive integers r and s. In such cases, GF(p^s) does not fractionally dominate GF(p^r); however, by Theorem III.4, any network's linear rate region over either field is the same, since both fields have characteristic p.

Corollary III.5. *Let $\mathbb{F}$ and $\mathbb{K}$ be finite fields. Then* char$(\mathbb{F}) =$char$(\mathbb{K})$ *if and only if for each network $\mathcal{N}$, we have* $\mathcal{C}_{lin}(\mathcal{N}, \mathbb{F}) = \mathcal{C}_{lin}(\mathcal{N}, \mathbb{K})$.

Proof: This corollary is an immediate consequence of Theorem III.4 and Corollary III.2. ■

IV. LINEAR RATE REGIONS OVER RINGS

The following theorem demonstrates that if a network has a fractional linear solution over some module and if p is a prime that divides the alphabet size (i.e., the size of the group), then the network must also have a fractional linear solution over every field of characteristic p with the same rate vector and possibly larger vector sizes.

Theorem IV.1. *Let $_RG$ be a module and let $\mathbb{F}$ be a finite field whose characteristic divides $|G|$. For each network $\mathcal{N}$ and each $k_1, \dots, k_m \geq 0$ and $n \geq 1$ such that $\mathcal{N}$ has a $(k_1, \dots, k_m, n)$ linear solution over $_RG$, there exists a positive integer t such that $\mathcal{N}$ has a $(tk_1, \dots, tk_m, tn)$ linear solution over $\mathbb{F}$.*

Proof: Let $p =$char$(\mathbb{F})$. By Lemma II.14, there exists a finite field $\mathbb{K}$ of characteristic p and a positive integer s such

that $_{M_s(\mathbb{K})}\mathbb{K}^s$ fractionally dominates $_R G$. Lemma II.3 implies a network $\mathcal{N}$ with a $(k_1, \ldots, k_m, n)$ linear solution over $_{M_s(\mathbb{K})}\mathbb{K}^s$ must also have an $(sk_1, \ldots, sk_m, sn)$ linear solution over $\mathbb{K}$. Since $\mathbb{F}$ and $\mathbb{K}$ both have characteristic p, and since the rate vector $(k_1/n, \ldots, k_m/n)$ is linearly achievable for $\mathcal{N}$ over $\mathbb{K}$, by Theorem III.4, the rate vector $(k_1/n, \ldots, k_m/n)$ is also linearly achievable for $\mathcal{N}$ over $\mathbb{F}$. Hence there exists a positive integer t such that $\mathcal{N}$ has a $(tk_1, \ldots, tk_m, tn)$ linear solution over $\mathbb{F}$. ∎

We now prove one of our main results regarding linear rate regions over rings.

Theorem IV.2. *If R is a finite ring and $\mathbb{F}$ is a finite field whose characteristic divides $|R|$, then the linear rate region of any network over R is contained in the network's linear rate region over $\mathbb{F}$.*

Proof: Let R be a finite ring, let $\mathcal{N}$ be a network, and let $\mathbb{F}$ finite field whose characteristic divides $|R|$. A fractional two-sided linear solution over R is a fractional linear solution over the module $_{R\otimes R^{op}}R$, so by Theorem IV.1, whenever $\mathcal{N}$ has a fractional linear solution over R with a given rate vector, $\mathcal{N}$ also has a fractional linear solution over $\mathbb{F}$ with the same rate vector and possibly larger vector sizes. Hence,

$\{\mathbf{r} \in \mathbb{Q}^m : \mathbf{r}$ is linearly achievable for $\mathcal{N}$ over $R\}$

$\subseteq \{\mathbf{r} \in \mathbb{Q}^m : \mathbf{r}$ is linearly achievable for $\mathcal{N}$ over $\mathbb{F}\}$. ∎

Corollary IV.3. *If R is a finite ring and $\mathbb{F}$ is a finite field whose characteristic divides $|R|$, then the linear capacity of any network over R is less than or equal to its linear capacity over $\mathbb{F}$.*

In some cases, the containment in Theorem IV.2 (and the inequality in Corollary IV.3) is strict for some networks, while in other cases, there may be equality for all networks. As an example, by taking $\mathbb{F} = \text{GF}(2)$ and $R = \mathbb{Z}_6$ in Theorem IV.2, any network's linear rate region over GF(2) contains its linear rate region over $\mathbb{Z}_6$. However, the linear capacity of the Char-2 network is 1 over the field GF(2) and is upper bounded by 6/7 over the field GF(3) (see Lemma III.1). Since $3 = \text{char}(\text{GF}(3))$, which divides $6 = |\mathbb{Z}_6|$, by Corollary IV.3, the Char-2 network's linear capacity over $\mathbb{Z}_6$ is upper bounded by 6/7. This demonstrates that the linear rate regions of R and $\mathbb{F}$ are not necessarily equal for all networks.

As another example, by taking $\mathbb{F} = \text{GF}(4)$ and $R = \mathbb{Z}_2[X]/\langle X^2 \rangle$ in Theorem IV.2, any network's linear rate region over GF(4) contains its linear rate region over $\mathbb{Z}_2[X]/\langle X^2 \rangle$. The field GF(2) is isomorphic to a subring of $\mathbb{Z}_2[X]/\langle X^2 \rangle$ (namely $\mathbb{Z}_2$), so there is an injective homomorphism from GF(2) to $\mathbb{Z}_2[X]/\langle X^2 \rangle$, which by Lemma II.10, implies any network's linear rate region over $\mathbb{Z}_2[X]/\langle X^2 \rangle$ contains its linear rate region over GF(2). However, by Theorem III.4, any network's linear rate regions over GF(4) and GF(2) must be equal. Thus the linear rate regions of GF(4) and $\mathbb{Z}_2[X]/\langle X^2 \rangle$ are equal for all networks. Precisely characterizing for which rings and fields the linear rate regions are equal for all networks remains an open problem.

A. Comparing Linear Capacities Over Different Rings

Determining the exact linear capacity and the linear rate region of the Char-m network over each finite ring (or even

each finite field) are also presently open problems. Another related open question is for which finite rings R and S does there exist a network $\mathcal{N}$ such that $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, S)$. We have answered this second question in some select special cases:

- In Theorem III.4, we showed that when R and S are finite fields, such a network exists if and only if the characteristics of R and S differ.
- In Theorem IV.2, we showed that when S is a field whose characteristic divides $|R|$, no such network exists. This includes the special case where $|S| = |R|$.

Corollary IV.4. *Let R and S be finite rings. If some prime factor of $|S|$ is not a factor of $|R|$, then there exists a network $\mathcal{N}$ such that $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, S)$.*

Proof: Let p divide $|S|$ but not $|R|$, and let $\mathcal{N}$ denote the Char-$|R|$ network. Then,

$\mathcal{C}_{lin}(\mathcal{N}, S)$
$\leq \mathcal{C}_{lin}(\mathcal{N}, \text{GF}(p))$ [from Theorem IV.2]
$\leq 1 - \dfrac{1}{2|R| + 3}$ [from $p \nmid |R|$ and Lemma III.1]
< 1
$\leq \mathcal{C}_{lin}(\mathcal{N}, R)$ $\big[$from $\text{char}(R) \mid |R|\big]$

where the last inequality uses the fact that $\mathcal{N}$ must be scalar linearly solvable over R, since the characteristic of R divides the size of R. ∎

Corollary IV.4 implies that if the sizes of two rings do not share the same set of prime factors, then at least one of the rings induces a higher linear capacity than the other on some network. As an example, the Char-6 network has a strictly larger linear capacity over the ring $\mathbb{Z}_6$ than over the field GF(25) of larger size.

Corollary IV.4, in particular, implies that for *every* finite field and *every* ring, whose sizes are relatively prime, there is *some* network for which the linear capacity of the network over the ring is strictly larger than the linear capacity over the field. In contrast, Theorem IV.2 shows that for *every* ring and *every* network, there is *some* field for which the linear capacity of the network over the ring is less than or equal to the linear capacity over the field. These facts are succinctly summarized in the following theorem.

Theorem IV.5. *Let $\mathbb{F}$ be a finite field and R be a finite ring. Then $|\mathbb{F}|$ and $|R|$ are relatively prime if and only if there exists a network $\mathcal{N}$ such that $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, \mathbb{F})$.*

Proof: Let $p = \text{char}(\mathbb{F})$. Then $|\mathbb{F}|$ and $|R|$ are relatively prime if and only if $p \nmid |R|$.

If $p \nmid |R|$, then by Corollary IV.4, there exists a network $\mathcal{N}$ such that $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, \mathbb{F})$. The converse is a restatement of Corollary IV.3. ∎

B. Asymptotic Solvability

We say that a network $\mathcal{N}$ is *asymptotically solvable over* $\mathcal{A}$ if for all $\epsilon \in (0, 1)$, the rate vector

$$(1 - \epsilon, \ldots, 1 - \epsilon)$$

is contained in the network's rate region. In other words, a uniform rate arbitrarily close to, or above, 1 is attainable. A network which is asymptotically solvable but is not solvable

was demonstrated in [12], and non-linearly solvable networks were demonstrated in [7] and [11] that are not asymptotically linearly solvable over any finite field. The following corollary demonstrates that such networks are additionally not asymptotically linearly solvable over any module (or ring).

Corollary IV.6. *If a network is asymptotically linearly solvable over some module or ring, then it must be asymptotically linearly solvable over some finite field.*

Proof: Suppose a network $\mathcal{N}$ is asymptotically linearly solvable over some module $_R G$. By Theorem IV.1, there exists a finite field $\mathbb{F}$ such that any rate vector that is linearly achievable over $_R G$ must also be linearly achievable over $\mathbb{F}$. Hence $\mathcal{N}$ is also asymptotically linearly solvable over $\mathbb{F}$. This also implies any network that is asymptotically linearly solvable over some ring must also be asymptotically linearly solvable over some field, since a fractional linear code over a ring is a special case of a fractional linear code over a module. ∎

V. CONCLUDING REMARKS

Linear network codes over finite rings (and modules) constitute a much broader class of codes than linear network codes over finite fields. Linear codes over rings have many of the attractive properties of linear codes over fields, including implementation complexity and possibly mathematical tractability. We have demonstrated, however, that with respect to linear capacity and linear rate regions, this broader class of codes does *not* offer an improvement over linear codes over fields. This particularly contrasts with the network solvability problem where we demonstrated certain cases where a ring alphabet can offer scalar linear solutions when a field alphabet cannot.

APPENDIX A
PROOFS OF LEMMAS IN SECTION II

The proofs in this appendix are results from [9] that we include for completeness.

A. Proof of Lemma II.8 [9, Lemma I.3]

Proof of Lemma II.8: Let $\mathcal{N}$ be a network that is scalar linearly solvable over the faithful R-module $(G, \oplus)$ with action $\cdot$. Any scalar linear solution for $\mathcal{N}$ over $_R G$ is a scalar 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 scalar linear solution over $_R G$, 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

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

Now let $_R H$ be a module with action $\odot$, and suppose the corresponding inputs to the node in the scalar linear code over $_R H$ 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

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

so by induction, every edge and decoding function in the scalar linear code over $_R H$ is the same linear combination of the messages as in the scalar linear solution over $_R G$. In other words, if an edge/decoding function in the scalar linear solution over $_R G$ produces the linear combination

$$\bigoplus_{j=1}^{n} (A_j \cdot z_j)$$

where $A_1, \ldots, A_n \in R$, then the corresponding edge/decoding function in the scalar linear code over $_R H$ produces the linear combination

$$\bigoplus_{j=1}^{n} (A_j \odot z'_j).$$

$_R G$ is faithful, so 1 and 0, respectively, are the only elements of R such that $1 \cdot g = g$ and $0 \cdot g = 0$, respectively, for all $g \in G$. Hence a decoding function in the scalar linear solution over $_R G$ that produces z_i must be of the form

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

In other words, since $_R G$ is faithful, it must be the case that $A_i = 1$ and $A_j = 0$ for all $j \neq i$. As shown above, every edge and decoding function in the scalar linear code over $_R H$ produces the same linear combination of the messages (i.e. the ring coefficients are the same), so the corresponding decoding function in the scalar linear code over $_R H$ is

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

Thus, each receiver can linearly recover its demands, so the scalar linear code over $_R H$ is, in fact, a solution. This implies that $_R H$ scalarly dominates $_R G$, which along with Lemma II.6, shows that $_R H$ fractionally dominates $_R G$. ∎

B. Proof of Lemma II.9 [9, Lemma II.6]

Proof of Lemma II.9: We use ideas from [11, 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 scalar linearly solvable over $_R G$. Every output y' in the solution over $_R G$ is of the form

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

where the x_i's are the parent node's inputs and the C_i's are constants from R. Form a linear code over $_S G$ replacing each coefficient C_i in (2) by $(C_i + J)$. Let y be the edge symbol in the code over $_S G$ corresponding to y' in the code over $_R G$. Then

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

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

This implies $_S G$ scalarly dominates $_R G$, which along with Lemma II.6, implies $_S G$ fractionally dominates $_R G$. ∎

C. Proof of Lemma II.10 [9, Lemma I.6]

Proof of Lemma II.10: Let $_S H$ be a 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 $_S H$. One can verify that $_R H$ is a module under $\odot$. Now, let $_R G$ be a module, and suppose $\mathcal{N}$ has a linear solution over $_R G$. By Lemma II.8, $\mathcal{N}$ is scalar linearly solvable over $_R H$, so every output $y' \in H$ in the solution over $_R H$ is of the form

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

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 $_S H$ by replacing each coefficient C_i in (3) by $\phi(C_i)$. Let $y \in H$ be the output in the code over $_S H$ corresponding to y' in the code over $_R H$. Then

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

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

This implies that $_R H$ scalarly dominates $_R G$, which along with Lemma II.6, shows that $_R H$ fractionally dominates $_R G$. ∎

REFERENCES

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

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

[3] W. Brown, *Matrices Over Commutative Rings*. London, U.K.: Taylor & Francis, 1992.

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

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

[6] T. Chan and A. Grant, "Network coding capacity regions via entropy functions," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5347–5374, Sep. 2014.

[7] J. Connelly and K. Zeger, "A class of non-linearly solvable networks," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 201–229, Jan. 2017.

[8] 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. 274–291, Jan. 2018.

[9] J. Connelly and K. Zeger, "Linear network coding over rings—Part II: Vector codes and non-commutative alphabets," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 292–308, Jan. 2018.

[10] N. Das and B. K. Rai, "On achievability of an (r, l) fractional linear network code," *IET Netw.*, vol. 6, no. 3, pp. 54–61, May 2017.

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

[12] 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.

[13] 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.

[14] R. Dougherty, C. Freiling, and K. Zeger, "Achievable rate regions for network coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2488–2509, May 2015.

[15] R. Dougherty, E. Freiling, and K. Zeger, "Characteristic-dependent linear rank inequalities with applications to network coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2510–2530, May 2015.

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

[17] 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.

[18] A. Gómez, C. Mejía, and J. Montoya, "Network coding and the model theory of linear information inequalities," in *Proc. Int. Symp. Netw. Coding*, Aalborg, Denmark, Jun. 2014, pp. 1–6.

[19] P. A. Grillet, *Abstract Algebra*. New York, NY, USA: Springer-Verlag, 2007.

[20] R. N. Gupta, A. Khurana, D. Khurana, and T. Y. Lam, "Rings over which the transpose of every invertible matrix is invertible," *J. Algebra*, vol. 322, no. 5, pp. 1627–1636, Sep. 2009.

[21] N. J. A. Harvey, R. Kleinberg, and A. R. Lehman, "On the capacity of information networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2345–2364, Jun. 2006.

[22] T. Ho *et al.*, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[23] R. Horn and C. Johnson, *Topics in Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1991.

[24] S. Huang and A. Ramamoorthy, "On the multiple-unicast capacity of 3-source, 3-terminal directed acyclic networks," *IEEE/ACM Trans. Netw.*, vol. 22, no. 1, pp. 285–299, Feb. 2014.

[25] S. Jaggi *et al.*, "Polynomial time algorithms for multicast network code construction," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 1973–1982, Jun. 2005.

[26] S. Kamath, V. Anantharam, D. Tse, and C.-C. Wang, "The two-unicast problem," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3865–3882, May 2018. [Online]. Available: http://ieeexplore.ieee.org/document/7744471/

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

[28] M. Langberg and A. Sprintson, "On the hardness of approximating the network coding capacity," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1008–1014, Feb. 2011.

[29] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[30] S.-Y. R. Li, Q. T. Sun, and Z. Shao, "Linear network coding: Theory and algorithms," *Proc. IEEE*, vol. 99, no. 3, pp. 372–387, Mar. 2011.

[31] S. Lovett, "Linear codes cannot approximate the network capacity within any constant factor," in *Proc. Electron. Colloq. Comput. Complexity*, vol. 21, 2014, pp. 1–19.

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

[33] B. R. McDonald, *Linear Algebra Over Commutative Rings*. London, U.K.: Taylor & Francis, 1984.

[34] M. Médard, M. Effros, T. Ho, and D. Karger, "On coding for non-multicast networks," in *Proc. Conf. Commun. Control Comput.*, Monticello, IL, USA, Oct. 2003, pp. 1–9.

[35] V. T. Muralidharan and B. S. Rajan, "Linear network coding, linear index coding and representable discrete polymatroids," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 4096–4119, Jul. 2016.

[36] L. Song, R. W. Yeung, and N. Cai, "Zero-error network coding for acyclic networks," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3129–3139, Dec. 2003.

[37] Q. T. Sun, S.-Y. R. Li, and Z. Li, "On base field of linear network coding," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7272–7282, Dec. 2016.

[38] Q. 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.

[39] Q. T. Sun, X. Yin, Z. Li, and K. Long, "Multicast network coding and field sizes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6182–6191, Nov. 2015.

[40] X. Xu, Y. Zeng, Y. L. Guan, and T. Ho, "An achievable region for double-unicast networks with linear network coding," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3621–3630, Oct. 2014.

[41] M. F. Wong, M. Langberg, and M. Effros, "On a capacity equivalence between multiple multicast and multiple unicast," in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Monticello, IL, USA, Oct. 2013, pp. 1537–1544.

[42] M. F. Wong, M. Langberg, and M. Effros, "Linear capacity equivalence between multiple multicast and multiple unicast," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jun./Jul. 2014, pp. 2152–2156.

[43] X. Yan, R. W. Yeung, and Z. Zhang, "An implicit characterization of the achievable rate region for acyclic multisource multisink network coding," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5625–5639, Sep. 2012.

[44] R. W. Yeung, "A framework for linear information inequalities," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1924–1934, Nov. 1997.

[45] W. Zeng, V. R. Cadambe, and M. Médard, "Alignment-based network coding for two-unicast-Z networks," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3183–3211, Jun. 2016.

Joseph Connelly (S'12–M'18) was born in Milwaukee in 1991. He received Bachelor's degrees in electrical and computer engineering from the University of Minnesota Twin Cities in 2013. He received the M.S. and Ph.D. degrees in electrical engineering from the University of California, San Diego in 2016 and 2018, respectively. In 2016, he was with the NASA Jet Propulsion Lab, and he is currently with Air Force Research Labs. Dr. Connelly was the recipient of the UCSD Shannon Memorial Fellowship in 2016, and he received the UCSD ECE Department Best Thesis Award in 2018.

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.