Linear Capacity of Networks over Ring Alphabets [*]

Joseph Connelly and Kenneth Zeger

Abstract

The rate of a network code is the ratio of the block sizes of the network's messages and its edge codewords. The linear capacity of a network over a finite ring alphabet is the supremum of achievable rates using linear codes over the ring. We prove the following for directed acyclic networks:

(i) For every finite field $\mathbb{F}$ and every finite ring R, there is some network whose linear capacity over R is greater than over $\mathbb{F}$ if and only if the sizes of $\mathbb{F}$ and R are relatively prime.

(ii) Every network's linear capacity over a finite ring is less than or equal to its linear capacity over every finite field whose characteristic divides the ring's size. As a consequence, every network's linear capacity over a finite field is greater than or equal to its linear capacity over every ring of the same size. Additionally, every network's linear capacity over a module is at most its linear capacity over some finite field.

(iii) The linear capacity of any network over a finite field depends only on the characteristic of the field.

(iv) Every network that is asymptotically linearly solvable over some finite ring (or even some module) is also asymptotically linearly solvable over some finite field.

These results establish the sufficiency of finite field alphabets for linear network coding. Namely, linear network coding capacity cannot be improved by looking beyond finite field alphabets to more general ring alphabets. However, certain rings can yield higher linear capacities for certain networks than can a given field.

1 Introduction

Network solvability determines whether or not a network's receivers can adequately deduce from their inputs a 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 [30], 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 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 [26].

In certain cases, linear coding over finite rings can offer solvability advantages over finite fields [8, 9]. An open question has been whether the linear capacity of a network over a finite field can be increased 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 increased 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 coding 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, 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.

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 linear capacity 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 capacity over a ring is at most its linear capacity over any field whose characteristic divides the ring's size. This result is analogous to the fact that every finite ring is isomorphic to some direct product of rings of prime-power sizes.

A fourth question we investigate concerns asymptotic linear solvability. A network is asymptotically linearly solvable if its linear coding capacity is at least one. An open question has been whether a network could be asymptotically linearly solvable over some ring or module, but not over any field. We also answer this question in the negative.

1.1 Network Model

A *network* will refer to a finite, directed, acyclic multigraph, some of whose nodes are *sources* or *receivers*. Source nodes generate *message vectors*, whose components are arbitrary elements of a fixed, finite set of size at least 2, called an *alphabet*. The elements of an alphabet are called

symbols. We will denote the cardinality of an alphabet $\mathcal{A}$ by $|\mathcal{A}|$. The *inputs* to a node are the message vectors, if any, originating at the node and the symbols on the incoming edges of the node. Each outgoing edge of a network node has associated with it an *edge function* that maps the node's inputs to the vector of symbols carried by the edge, called the *edge vector*. Each receiver node has *decoding functions* that map the receiver's inputs to a vector of alphabet symbols in an attempt to recover the receiver's *demands*, which are the message vectors the receiver wishes to obtain.

A (k, 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 message vectors (or "message blocks") are elements of $\mathcal{A}^k$ and edge vectors (or "edge blocks") are elements of $\mathcal{A}^n$. The *rate* of a (k, n) network code is k/n. A fractional code is a *solution* if each receiver recovers its demanded message vectors from its inputs.

For any ring R, let char(R) denote the characteristic of R. If R is a ring and $n, m_1, \ldots, m_s$ are positive integers, then we say a function

$$f : R^{m_1} \times \cdots \times R^{m_s} \longrightarrow R^n$$

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

$$f(x_1, \ldots, x_s) = (A_1 \cdot x_1) + \cdots + (A_s \cdot x_s)$$

where, for each i,

- $x_i \in R^{m_i}$,
- A_i is an $n \times m_i$ matrix whose elements are constants in the ring R,
- $+$ is n-vector addition over R, and
- $\cdot$ is matrix-vector multiplication over R.

A fractional code is *linear over* R if all edge functions and decoding functions are linear over R, i.e. the outgoing edge vectors and decoded symbols at a node are linear combinations of the node's inputs.

The *capacity* of a network is

$$\mathcal{C}(\mathcal{N}) = \sup\{k/n \ : \ \exists \, \text{a} \, (k, n) \text{ solution over some alphabet } \mathcal{A}\}.$$

The *linear capacity* of a network with respect to a ring alphabet R is

$$\mathcal{C}_{lin}(\mathcal{N}, R) = \sup\{k/n \ : \ \exists \, \text{a} \, (k, n) \text{ linear solution over } R\}.$$

A network is said to be

- *solvable* if it has a $(1, 1)$ solution over some alphabet $\mathcal{A}$,
- *scalar linearly solvable over* R if it has a $(1, 1)$ linear solution over R, and
- *vector linear solvable over* R if it has a (t, t) linear solution over R, for some $t \geq 1$.

1.2   Related Work

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

Li, Yeung, and Cai [25] 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 [20] 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 [22] 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. [16], [21], [36], and [41]).

It is known (e.g. [11]) that for general networks, fractional linear codes over finite fields do not necessarily attain the capacity. In fact, it was shown by Lovett [27] that, in general, fractional linear network codes over finite fields cannot even approximate the capacity to any constant factor. Blasiak, Kleinberg, and Lubetzky [2] demonstrated a class of networks whose capacities are larger than their linear capacities over any finite field by a factor that grows polynomially with the number of messages. Langberg and Sprintson [24] 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 [31] 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. [40]) are known to be closely related and have been shown to be useful in determining networks' linear capacities over finite fields (e.g. [14], [15], and [17]).

Chan and Grant [5] demonstrated a duality between entropy functions and capacity 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 capacities and entropy functions has been further studied, for example, in [6], [19], [32], and [39]. 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.

1.3 Main Results

The remainder of the paper is outlined as follows.

 In Section 2, we explore a connection between fractional linear codes and vector linear codes, which allows us to exploit network solvability results over rings [8, 9] in order to achieve capacity results over rings. For a given network $\mathcal{N}$ and rate r we show (in Lemma 2.3) there exists a network $\mathcal{N}'$ that is vector linearly solvable over a ring R if and only if $\mathcal{N}$ has a fractional linear solution at rate r over the ring R. We then use this result (in Lemma 2.5 and Corollaries 2.7 and 3.2) to extend scalar linear solvability results to the more general case of fractional linear codes.

 In Section 3, we use the results relating solvability and fractional codes from Section 2 to show our main results on network coding capacity over rings. We prove (in Theorem 3.6) that the linear capacity of any network over a field depends only on the characteristic of the field. 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.

 We prove (in Theorem 3.9) that for any network, any finite field, and any finite ring whose size is divisible by the field's characteristic, the network's linear capacity over the ring is less than or equal to its linear capacity over the field. As a consequence, for any finite ring there exists a field, not larger than the ring, such that every network's linear capacity over the ring is at most its linear capacity over the field. 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 capacity with network coding. In order to prove Theorem 3.9, we show (in Lemma 3.8) that whenever a network has a fractional linear solution over some ring at a given rate, the network has a fractional linear solution over some field at the same rate but with potentially larger block sizes.

 Even though Theorem 3.9 asserts non-field rings cannot provide an increase in linear capacity over fields for *all* networks, we show (in Corollary 3.10) 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 3.11) 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.

 In Section 4, we extend the notion of linearity to modules and define fractional linear codes over modules, which include fractional linear codes over finite rings as a special case. We also extend some of the results in Section 2 to fractional linear codes over modules (in Lemma 4.2). We use these results to prove (in Theorem 4.5) that for any network and any finite module, there exists a finite field, whose characteristic divides the module's size, such that any network's linear capacity over the module is at most its linear capacity over the field. Finally, we prove (in Corollary 4.6) that whenever a network has a fractional linear solution over some ring (or module) at a rate arbitrarily close to 1, the network must also have a fractional linear solution over some field at the same 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 modules.
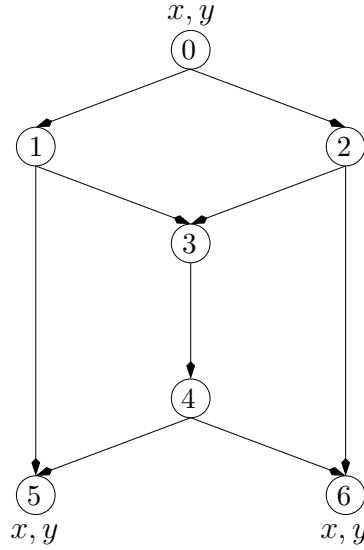
2   Fractional and Vector Codes

Figure 1:   The Butterfly network has a single source node 0, which generates message vectors x and y. Each of the receivers, nodes 5 and 6, demands both x and y. The Butterfly network has capacity 1 and is scalar linearly solvable over any ring.

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 [18]) that the transpose of an invertible matrix over a non-commutative ring is not necessarily invertible.[1] Consequently, directly computing network linear capacities over finite rings appears 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. [23], [37], and [38]). We use this approach to relate the existence of fractional linear solutions over rings to scalar and vector linear solvability over rings (which was studied in [8] and [9]). Specifically, we show that for any given network $\mathcal{N}$ and rate r, the network $\mathcal{N}$ has a fractional linear solution over a ring R at rate r if and only if a corresponding network is vector linearly solvable over R. This allows us to more easily relate a network's linear capacity over a ring to the network's linear capacity over some field.

2.1   Fractional Equivalent Network

For any network $\mathcal{N}$ and positive integers k and n, the following defines a new network which is vector linearly solvable over a ring R if and only if $\mathcal{N}$ has a rate k/n fractional linear solution over R. We prove this fact in Lemma 2.3.

---

[1]See [3] and [29] for more information on linear algebra over rings.

Definition 2.1. For any network $\mathcal{N}$ and any positive integers k and n, let $\mathcal{N}^{(k,n)}$ denote the network $\mathcal{N}$ but with

  (i) each edge replaced with n parallel edges, and

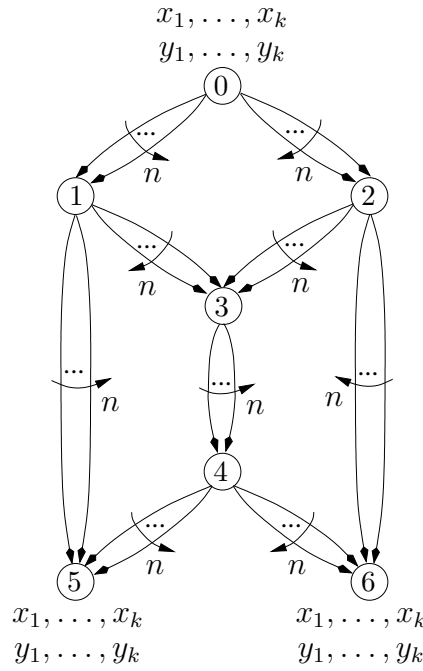 (ii) each message vector replaced with k message vectors.

Figure 2: The (k, n)-Butterfly network has a single source node, which generates message vectors $x_1, \ldots, x_k$ and $y_1, \ldots, y_k$. Each receiver demands all of the message vectors. The (k, n)-Butterfly network is vector linearly solvable over a given ring if and only if $k \leq n$.

The *Butterfly network* is defined in Figure 1, and, for each $k, n \geq 1$, the (k, n)-*Butterfly network* is defined in Figure 2. These networks are consistent with Definition 2.1, if they are denoted by $\mathcal{N}$ and $\mathcal{N}^{(k,n)}$, respectively. Part (c) of the following motivational example is also consistent with Lemma 2.3.

Example 2.2. *Let R be a finite ring. In what follows, we show, for each $k, n \geq 1$:*

  (a) *The Butterfly network has a (k, n) linear solution over R if and only if $k/n \leq 1$.*

  (b) *The (k, n)-Butterfly network is vector linearly solvable over R if and only if $k/n \leq 1$.*

  (c) *The Butterfly network has a rate k/n fractional linear solution over R if and only if the (k, n)-Butterfly network is vector linear solvable over R.*

Proof.   (a) Let $e_{u,v}$ denote the symbol carried by the edge connecting nodes u and v in the Butterfly network. A $(1,1)$ linear solution for the Butterfly network over any ring is given by

$$e_{0,1} = e_{1,3} = e_{1,5} = x$$
$$e_{0,2} = e_{2,3} = e_{2,6} = y$$
$$e_{3,4} = e_{4,5} = e_{4,6} = x + y$$

where each receiver recovers one message directly and linearly recovers the other message using

$$e_{4,5} - e_{1,5} = (x + y) - x = y \quad \text{and} \quad e_{4,6} - e_{2,6} = (x + y) - y = x.$$

Hence for any $k, n \geq 1$ such that $k/n \leq 1$, the Butterfly has a (k, n) linear solution over any ring R.

Conversely, suppose the Butterfly network has a (k, n) linear solution over a ring R. Since the pair of edges $\{e_{0,1}, e_{0,2}\}$ is a minimum-cut for the network, and since $x, y \in R^k$ and $e_{0,1}, e_{0,2} \in R^n$, we have $2k \leq 2n$. Thus $k/n \leq 1$.

(b) Let $e_{u,v}^{(i)}$ denote the symbol carried by the ith parallel edge connecting nodes u and v in the (k, n)-Butterfly network. Whenever $k \leq n$, a $(1, 1)$ linear solution for the Butterfly network over any ring is given by

$$
\begin{array}{ll}
e_{0,1}^{(i)} = e_{1,3}^{(i)} = e_{1,5}^{(i)} = x_i & (i = 1, \ldots, k) \\
e_{0,2}^{(i)} = e_{2,3}^{(i)} = e_{2,6}^{(i)} = y_i & (i = 1, \ldots, k) \\
e_{3,4}^{(i)} = e_{4,5}^{(i)} = e_{4,6}^{(i)} = x_i + y_i & (i = 1, \ldots, k)
\end{array}
$$

where the receivers linearly recover their demands similarly to the $(1, 1)$ code described for the Butterfly network in (a).

Conversely, suppose the (k, n)-Butterfly network has a (t, t) linear solution over a ring R, for some $t \geq 1$. Since the edge set

$$\{e_{0,1}^{(1)}, \ldots, e_{0,1}^{(n)}, e_{0,2}^{(1)}, \ldots, e_{0,2}^{(n)}\}$$

is a minimum-cut for the network, and since $x_i, y_i, e_{0,1}^{(j)}, e_{0,2}^{(j)} \in R^t$, we have $2tk \leq 2tn$. Thus $k \leq n$.

(c) This follows immediately from (a) and (b).

■

In fact, any (k, n) linear solution for the Butterfly network can be translated to a $(1, 1)$ linear solution for the (k, n)-Butterfly network. Similarly, any $(1, 1)$ linear solution for the (k, n)-Butterfly network can be translated to a (k, n) linear solution for the Butterfly network. This concept is generalized in Lemma 2.3.

Lemma 2.3. *Let $\mathcal{N}$ be a network, let k, n, and t be positive integers, let R be a finite ring, and let $\mathcal{N}^{(k,n)}$ denote the network in Definition 2.1 corresponding to $\mathcal{N}$ and k and n. Then $\mathcal{N}$ has a (tk, tn) linear solution over R if and only if $\mathcal{N}^{(k,n)}$ has a (t, t) linear solution over R.*

Proof. In a (tk, tn) code over R for $\mathcal{N}$, suppose a node generates message vectors $x_1, \ldots, x_r \in R^{tk}$ and has incoming edge vectors $y_1, \ldots, y_s \in R^{tn}$. Then an edge function

$$f : \underbrace{R^{tk} \times \cdots \times R^{tk}}_{r \text{ message vectors}} \times \underbrace{R^{tn} \times \cdots \times R^{tn}}_{s \text{ edge vectors}} \longrightarrow R^{tn}$$

can equivalently be written as n functions:

$$f_i : \underbrace{R^t \times \cdots \times R^t}_{rk \text{ message vectors}} \times \underbrace{R^t \times \cdots \times R^t}_{sn \text{ edge vectors}} \longrightarrow R^t \qquad (i = 1, \ldots, n)$$

which can be used to describe equivalent edge functions for the n parallel edges in a (t, t) code over R for $\mathcal{N}^{(k,n)}$. The function f is linear over R if and only if each of $f_1, \ldots, f_n$ is also linear over R.

Similarly, a decoding function in a (tk, tn) code for $\mathcal{N}$

$$f : \underbrace{R^{tk} \times \cdots \times R^{tk}}_{r \text{ message vectors}} \times \underbrace{R^{tn} \times \cdots \times R^{tn}}_{s \text{ edge vectors}} \longrightarrow R^{tk}$$

can equivalently be written as k functions:

$$f_i : \underbrace{R^t \times \cdots \times R^t}_{rk \text{ message vectors}} \times \underbrace{R^t \times \cdots \times R^t}_{sn \text{ edge vectors}} \longrightarrow R^t \qquad (i = 1, \ldots, k)$$

which can be used to describe equivalent decoding functions for the k message vectors in a (t, t) code over R for $\mathcal{N}^{(k,n)}$. The function f is linear over R if and only if each of $f_1, \ldots, f_k$ is also linear over R. Additionally, the function f correctly reproduces its demanded message vector in the (tk, tn) code for $\mathcal{N}$ if and only if each of $f_1, \ldots, f_k$ correctly reproduces its demanded message vector in the (t, t) code for $\mathcal{N}^{(k,n)}$.

Hence, any (tk, tn) linear solution over a ring R for $\mathcal{N}$ can be translated to a (t, t) linear solution over R for $\mathcal{N}^{(k,n)}$, and similarly, any (t, t) linear solution over R for $\mathcal{N}^{(k,n)}$ can be translated to a (tk, tn) linear solution over R for $\mathcal{N}$. ∎

2.2   Fractional Dominance

Definition 2.4. Let R and S be rings. We say that

   (a) S *scalarly dominates* R if every network with a $(1,1)$ linear solution over R also has a $(1,1)$ linear solution over S.

   (b) S *fractionally dominates* R if for all integers $k, n \geq 1$, every network with a (k,n) linear solution over R also has a (k,n) linear solution over S.

The scalar dominance relation was studied in [8], where it was shown that scalar dominance is a quasi-order on the set of commutative rings of a given size. We note that if S fractionally dominates R, then for every network $\mathcal{N}$,

$$\{k/n \,:\, \exists \text{ a } (k,n) \text{ linear solution over } S\} \supseteq \{k/n \,:\, \exists \text{ a } (k,n) \text{ linear solution over } R\}$$

which implies

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

Lemma 2.5. *Let R and S be finite rings. Then S fractionally dominates R if and only if S scalarly dominates R.*

Proof. It follows immediately from Definition 2.4 that fractional dominance implies scalar dominance. To prove the converse, suppose S scalarly dominates R. Let $\mathcal{N}$ be a network, let k and n be positive integers, and let $\mathcal{N}^{(k,n)}$ be the network in Definition 2.1 corresponding to $\mathcal{N}$, k, and n. Then

        $\mathcal{N}$ has a (k,n) linear solution over R

        $\implies \mathcal{N}^{(k,n)}$ has a $(1,1)$ linear solution over R [from Lemma 2.3]

        $\implies \mathcal{N}^{(k,n)}$ has a $(1,1)$ linear solution over S [from S scalarly dominates R]

        $\implies \mathcal{N}$ has a (k,n) linear solution over S [from Lemma 2.3] .

Hence for all $k, n \geq 1$, every network with a (k,n) linear solution over R also has a (k,n) linear solution over S.   ■

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.

As an example, for any integer $n \geq 2$ and any divisor m of n, there is a homomorphism from $\mathbf{Z}_n$ to $\mathbf{Z}_m$ using reduction modulo m.

Fractional linear codes consist of addition and multiplication operations, both of which are preserved under homomorphisms. In fact, Lemma 2.6 and Corollary 2.7 show that ring homomorphisms induce scalar dominance and fractional dominance, respectively.

Lemma 2.6. *[8, Lemma II.5]: Suppose R and S are finite rings. If there exists a homomorphism from R to S, then S scalarly dominates R.*

Corollary 2.7. *Suppose R and S are finite rings. If there exists a homomorphism from R to S, then S fractionally dominates R.*

Proof. This follows immediately from Lemmas 2.5 and 2.6.   ∎

Special cases of Corollary 2.7 include:

(1) R is a subring of S:
    The identity mapping is an injective homomorphism from R to S. In a later proof (Theorem 3.6), we will use the fact that $\mathrm{GF}(p^r)$ is a subfield of $\mathrm{GF}(p^s)$ whenever $r \mid s$, which implies $\mathrm{GF}(p^s)$ fractionally dominates $\mathrm{GF}(p^r)$ in such cases.

(2) $\phi_i : R_1 \times R_2 \to R_i$ is the projection mapping:
    ϕ_i is a surjective homomorphism. It is known (see Lemma 3.7) that each finite ring is isomorphic to some direct product of rings with prime-power sizes, which implies that each finite ring is fractionally dominated by certain rings with prime-power sizes. These facts will be used in the proof of later results (Lemma 3.8).

Corollary 2.7 does not necessarily extend to non-linear solutions. For example, in [7] it was shown that for any prime p and integer $\alpha \geq 2$, there is a network that has a $(1,1)$ non-linear solution over an alphabet of size p^α but not over any smaller alphabets. In particular, the constructed network has a $(1,1)$ non-linear solution over the ring $\mathbf{Z}_{p^\alpha}$ but not over $\mathbf{Z}_p$. However, there is a surjective homomorphism from the ring $\mathbf{Z}_{p^\alpha}$ to $\mathbf{Z}_p$ given by reduction modulo p, which implies any network that is scalar linearly solvable over $\mathbf{Z}_{p^\alpha}$ must also be scalar linearly solvable over $\mathbf{Z}_p$.

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. [28, 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. This implies the following lemma, which was more formally shown in [9].

Lemma 2.8. *[9, Lemmas II.1 and II.3]: Let R be a finite ring. Then there exist a positive integer t and a finite field $\mathbb{F}$ such that there exists a surjective homomorphism from R to $M_t(\mathbb{F})$ and $|M_t(\mathbb{F})|$ divides $|R|$.*

Corollary 2.7 and Lemma 2.8 together imply that every finite ring is fractionally dominated by some matrix ring over a field. Lemma 2.9 and Corollary 2.10 demonstrate an equivalence between fractional linear codes over matrix rings and larger block size fractional linear codes.

Lemma 2.9. *[9, Corollary I.5]: Let R be a finite ring, let t be a positive integer, and let $\mathcal{N}$ be a network. Then $\mathcal{N}$ has a (t,t) linear solution over R if and only if $\mathcal{N}$ has a $(1,1)$ linear solution over the ring of $t \times t$ matrices over R.*

Corollary 2.10. *Let R be a finite ring, let k, n, and t be positive integers, and let $\mathcal{N}$ be a network. Then $\mathcal{N}$ has a (k, n) linear solution over the ring of $t \times t$ matrices whose elements are from R if and only if $\mathcal{N}$ has a (tk, tn) linear solution over R.*

Proof. Let $\mathcal{N}^{(k,n)}$ denote the network in Definition 2.1 corresponding to $\mathcal{N}$ and k and n. Then

$\mathcal{N}$ has a (k, n) linear solution over $M_t(R)$

$\iff$ $\mathcal{N}^{(k,n)}$ has a $(1, 1)$ linear solution over $M_t(R)$ [from Lemma 2.3]

$\iff$ $\mathcal{N}^{(k,n)}$ has an (t, t) linear solution over R [from Lemma 2.9]

$\iff$ $\mathcal{N}$ has an (tk, tn) linear solution over R [from Lemma 2.3] .

∎

3   Comparing Linear Capacities over Rings and Fields

Lemma 3.1 is a result of Sun, Yang, Long, Yin, and Li. We use this lemma to prove Corollary 3.2, which shows that a fractional linear solution over any non-prime finite field induces a fractional linear solution over the corresponding prime field at the same rate but with a larger block size.

Lemma 3.1. *[34, Proposition 1]: Let q be a prime power and t a positive integer. If a network has a $(1,1)$ linear solution over $\mathrm{GF}(q^t)$, then it has a (t,t) linear solution over $\mathrm{GF}(q)$.*

Corollary 3.2. *Let p be a prime and let k, n, and t be positive integers. If network $\mathcal{N}$ has a (k,n) linear solution over $\mathrm{GF}(p^t)$, then $\mathcal{N}$ has an (tk,tn) linear solution over $\mathrm{GF}(p)$.*

Proof. Let $\mathcal{N}$ be a network, and let $\mathcal{N}^{(k,n)}$ be the network in Definition 2.1 corresponding to $\mathcal{N}$, k, and n. Then

$$\mathcal{N} \text{ has a } (k,n) \text{ linear solution over } \mathrm{GF}\big(p^t\big)$$
$$\implies \mathcal{N}^{(k,n)} \text{ has a } (1,1) \text{ linear solution over } \mathrm{GF}\big(p^t\big) \qquad \text{[from Lemma 2.3]}$$
$$\implies \mathcal{N}^{(k,n)} \text{ has an } (t,t) \text{ linear solution over } \mathrm{GF}(p) \qquad \text{[from Lemma 3.1]}$$
$$\implies \mathcal{N} \text{ has a } (tk,tn) \text{ linear solution over } \mathrm{GF}(p) \qquad \text{[from Lemma 2.3]}.$$

∎

3.1   Linear Capacity 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. This network is a generalization of the Fano network [13] and is known to be vector linearly solvable over a field if and only if the characteristic of the field divides m.

Let R be a finite ring whose characteristic divides m. Then $m = 0$ in R, and the following scalar linear code over R is a solution for the Char-m network

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

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

$$R_i : \quad e_x - e_i = x_i$$
$$R_x : \quad \sum_{i=1}^{m+1} e_i = x_0 + m \sum_{i=0}^{m+1} x_i$$
$$= x_0 \qquad\qquad\qquad \big[\text{from } \mathsf{char}(R) \,\big|\, m\big].$$

This code relies on the fact $m = 0$ in R, and in fact, the Char-m network has no scalar linear solutions over any ring whose characteristic does not divide m.
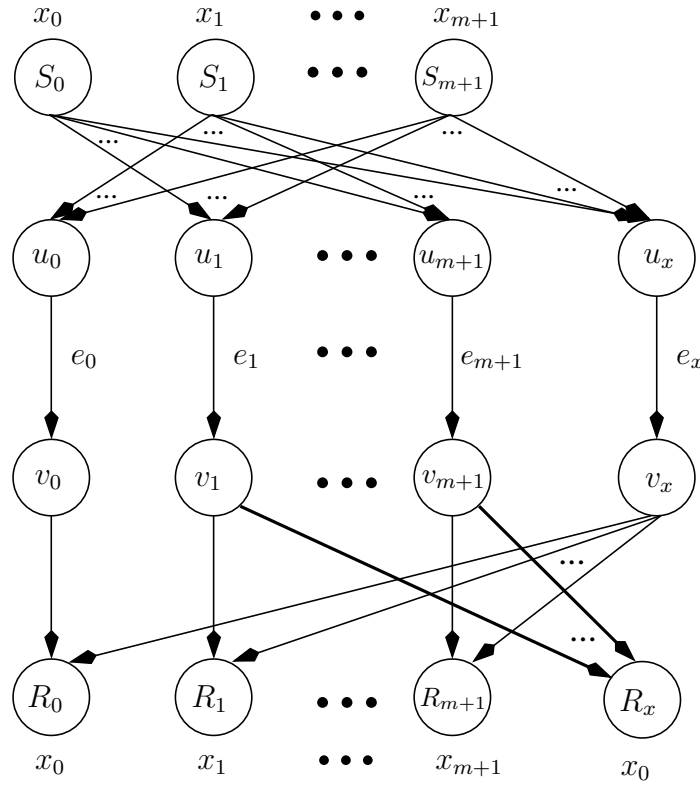
Figure 3: The Char-m network has source nodes $S_0, S_1, \ldots, S_{m+1}$ which generate message vectors $x_0, x_1, \ldots, x_{m+1}$, respectively. Node u_x has a single incoming edge from each source node, and the edge connecting nodes u_x and v_x carries the edge vector e_x. For each $i = 0, 1, \ldots, m+1$, 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_x. The receiver R_x demands x_0 and has an incoming edge from each of nodes $v_1, \ldots, v_{m+1}$.

Lemma 3.3. *[7, Lemma IV.6]: For each $m \geq 2$ and each finite ring R, the Char-m network is scalar linearly solvable over R if and only if $\mathsf{char}(R) \mid m$.*

Lemma 3.4. *[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 $\mathsf{char}(\mathbb{F}) \mid m$, and*

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

Corollary 3.5. *If $\mathbb{F}_1$ and $\mathbb{F}_2$ are finite fields with different characteristics, then there exist networks $\mathcal{N}_1$ and $\mathcal{N}_2$, such that*

$$\mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{F}_1) > \mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{F}_2) \quad and \quad \mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{F}_2) > \mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{F}_1).$$

Proof. Suppose $\mathrm{char}(\mathbb{F}_1) = p \neq q = \mathrm{char}(\mathbb{F}_2)$ and let $\mathcal{N}_1$ and $\mathcal{N}_2$ be the Char-p network and Char-q network, respectively. Then by Lemma 3.4, $\mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{F}_1) = 1$ and $\mathcal{C}_{lin}(\mathcal{N}_1, \mathbb{F}_2) \leq 1 - \frac{1}{2p+3}$. Similarly, $\mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{F}_2) = 1$ and $\mathcal{C}_{lin}(\mathcal{N}_2, \mathbb{F}_1) \leq 1 - \frac{1}{2q+3}$. ∎

The following theorem demonstrates that the linear capacity 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 3.6 also demonstrates that for any two finite fields of distinct characteristics, there always exists some network whose linear capacities differ over the two fields.

Theorem 3.6. *Let $\mathbb{F}_1$ and $\mathbb{F}_2$ be finite fields. Then $\mathrm{char}(\mathbb{F}_1) = \mathrm{char}(\mathbb{F}_2)$ if and only if for all networks $\mathcal{N}$, we have $\mathcal{C}_{lin}(\mathcal{N}, \mathbb{F}_1) = \mathcal{C}_{lin}(\mathcal{N}, \mathbb{F}_2)$.*

Proof. Let r and s be positive integers, p a prime, and $\mathcal{N}$ a network. Since $\mathrm{GF}(p)$ is a subfield of $\mathrm{GF}(p^s)$, there exists an injective homomorphism from $\mathrm{GF}(p)$ to $\mathrm{GF}(p^s)$. Thus,

> $\mathcal{N}$ has a (k, n) linear solution over $\mathrm{GF}(p^r)$
> $\implies$ $\mathcal{N}$ has an (rk, rn) linear solution over $\mathrm{GF}(p)$ [from Lemma 3.2]
> $\implies$ $\mathcal{N}$ has an (rk, rn) linear solution over $\mathrm{GF}(p^s)$ [from Corollary 2.7] .

Both (k, n) linear solutions and (rk, rn) linear solutions have rate k/n. Hence any rate that is linearly attainable over $\mathrm{GF}(p^r)$ is also linearly attainable over $\mathrm{GF}(p^s)$ (with possibly larger block sizes), which implies

$$\{k/n \,:\, \exists \text{ a } (k, n) \text{ linear solution over } \mathrm{GF}(p^r)\} \subseteq \{k/n \,:\, \exists \text{ a } (k, n) \text{ linear solution over } \mathrm{GF}(p^s)\}$$

and so

$$\mathcal{C}_{lin}(\mathcal{N}, \mathrm{GF}(p^r)) \leq \mathcal{C}_{lin}(\mathcal{N}, \mathrm{GF}(p^s)).$$

Similarly, we have

$$\mathcal{C}_{lin}(\mathcal{N}, \mathrm{GF}(p^s)) \leq \mathcal{C}_{lin}(\mathcal{N}, \mathrm{GF}(p^r)).$$

Hence if $\mathrm{char}(\mathbb{F}_1) = \mathrm{char}(\mathbb{F}_2)$, then the linear capacities of any network over $\mathbb{F}_1$ and $\mathbb{F}_2$ are equal. The reverse direction follows from Corollary 3.5. ∎

Immediately following Definition 2.4, we showed that for any finite rings S and R,

> S fractionally dominates $R \implies \mathcal{C}_{lin}(\mathcal{N}, S) \geq \mathcal{C}_{lin}(\mathcal{N}, R)$ for every network $\mathcal{N}$.

Theorem 3.6 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], [33], [35]) of networks that are scalar linearly solvable over $\mathrm{GF}(p^r)$ but not over $\mathrm{GF}(p^s)$, for some prime p and some distinct positive integers r and s. In such cases, $\mathrm{GF}(p^s)$ does not fractionally dominate $\mathrm{GF}(p^r)$; however, by Theorem 3.6, any network's linear capacity over either field is the same, since both fields have characteristic p.

3.2   Linear Capacity over Rings

Unlike finite fields, a finite ring need not have prime-power size. This may be advantageous in applications which call for non-power-of-prime alphabet sizes; however, the following lemma shows that all such rings decompose into a direct product of rings of prime-power sizes. As an example, the ring $\mathbf{Z}_6$ is isomorphic to $\mathbf{Z}_3 \times \mathbf{Z}_2$ by the Chinese Remainder Theorem.

Lemma 3.7. *[28, Theorem I.1]: Every finite ring is isomorphic to some direct product of rings with prime-power sizes.*

In [9, Theorem IV.6], it is shown that whenever a network is scalar linearly solvable over a commutative ring of size p^k, the network must have a (k, k) linear solution over the prime field $\mathrm{GF}(p)$. The following lemma demonstrates that if a network has a fractional linear solution at a given rate over a ring and if p is a prime that divides the size of the ring, then the network must also have a fractional linear solution over the field $\mathrm{GF}(p)$ at the same rate but with possibly larger block sizes.

Lemma 3.8. *Let R be a finite ring, let k and n be positive integers, and let p be a prime divisor of $|R|$. Then there exists a positive integer t such that any network with a (k, n) linear solution over R also has a (tk, tn) linear solution over $\mathrm{GF}(p)$.*

Proof. Suppose $\mathcal{N}$ is a network with a (k, n) linear solution over R. By Lemma 3.7, the ring R is isomorphic to a direct product of rings with prime-power sizes. Let S denote one of the rings in the direct product, and suppose its size is p^α, for some positive integer α. Then the usual projective mapping from R to S is a surjective homomorphism, so by Corollary 2.7, network $\mathcal{N}$ also has a (k, n) linear solution over S.

By Lemma 2.8, since $|S| = p^\alpha$, there exist positive integers r and s such that there is a surjective homomorphism from S to the matrix ring $M_r(\mathrm{GF}(p^s))$. So

$$\mathcal{N} \text{ has a } (k, n) \text{ linear solution over } M_r(\mathrm{GF}(p^s)) \qquad \text{[from Corollary 2.7]}$$
$$\implies \mathcal{N} \text{ has an } (rk, rn) \text{ linear solution over } \mathrm{GF}(p^s) \qquad \text{[from Corollary 2.10]}$$
$$\implies \mathcal{N} \text{ has an } (rsk, rsn) \text{ linear solution over } \mathrm{GF}(p) \qquad \text{[from Corollary 3.2]}.$$

Taking $t = rs$ proves the lemma.   ∎

In network coding, arbitrarily large block sizes may be needed to achieve a solution at 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, tn) linear solution over any finite field but which has no (mk, mn) linear solution over any finite field when $m < t$. In fact, Corollary 2.10 implies that for any finite field $\mathbb{F}$, such a network has a (k, n) linear solution over the matrix ring $M_t(\mathbb{F})$. This also implies that the quantity t in Lemma 3.8 may need to be arbitrarily large.

We now prove one of our main results regarding linear capacity over rings. One consequence of Theorem 3.9 is that any network's linear capacity over a ring of prime-power size is never greater than the network's linear capacity over a field of the same size.

Theorem 3.9. *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 at most the network's linear capacity over $\mathbb{F}$.*

Proof. Let R be a finite ring, let $\mathcal{N}$ be a network, and let p be a prime that divides $|R|$. It follows from Lemma 3.8, that whenever $\mathcal{N}$ has a fractional linear solution over R at a given rate, $\mathcal{N}$ also has a fractional linear solution over $\mathrm{GF}(p)$ at the same rate and with possibly larger block sizes. Hence, $\mathcal{N}$'s linear capacity over R is upper bounded by $\mathcal{N}$'s linear capacity over $\mathrm{GF}(p)$. By Theorem 3.6, for all $n \geq 1$, the linear capacities of $\mathcal{N}$ over $\mathrm{GF}(p)$ and $\mathrm{GF}(p^n)$ are equal, thus proving the theorem. ∎

As an example, the linear capacity of the Char-2 network is 1 over the field $\mathrm{GF}(2)$ and is upper bounded by $6/7$ over the field $\mathrm{GF}(3)$ (see Lemma 3.4). Since $2 = \mathrm{char}(\mathrm{GF}(2))$ and $3 = \mathrm{char}(\mathrm{GF}(3))$ both divide $6 = |\mathbf{Z}_6|$, by Theorem 3.9, the Char-2 network's linear capacity over $\mathbf{Z}_6$ is upper bounded by both 1 and $6/7$.

Determining the exact linear capacity of the Char-m network over each finite ring (or even each finite field) is presently an open problem. Another 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 3.6, 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 3.9, we showed that when S is a field whose characteristic divides $|R|$, no such network exists. This includes the special case where S is a field and $|S| = |R|$.

Corollary 3.10. *Let R and S be finite rings. If some prime factor of $|S|$ is not a factor of $|R|$, then there exists a network $\mathcal{N}$ such that $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, S)$.*

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

$$
\begin{aligned}
\mathcal{C}_{lin}(\mathcal{N}, S) &\leq \mathcal{C}_{lin}(\mathcal{N}, \mathrm{GF}(p)) && \text{[from Theorem 3.9]} \\
&\leq 1 - \frac{1}{2|R| + 3} && \text{[from } p \nmid |R| \text{ and Lemma 3.4]} \\
&< 1 \\
&\leq \mathcal{C}_{lin}(\mathcal{N}, R) && \left[\text{from } \mathrm{char}(R) \,\big|\, |R| \text{ and Lemma 3.3}\right]
\end{aligned}
$$

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

Corollary 3.10 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 $\mathbf{Z}_6$ than over the field $\mathrm{GF}(25)$ of larger size.

Corollary 3.10, 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 3.9 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 3.11. *Let $\mathbb{F}$ be a finite field and R be a finite ring. Then there exists a network $\mathcal{N}$ such that $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, \mathbb{F})$ if and only if $|\mathbb{F}|$ and $|R|$ are relatively prime.*

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

If $p \mid |R|$, then by Theorem 3.9, any network's linear capacity over R is at most its linear capacity over $\mathbb{F}$. Conversely, if $p \nmid |R|$, then by Corollary 3.10, there exists a network $\mathcal{N}$ such that $\mathcal{C}_{lin}(\mathcal{N}, R) > \mathcal{C}_{lin}(\mathcal{N}, \mathbb{F})$. ∎

4   Linear Capacity over Modules

We have thus far considered fractional linear codes in which the messages, the edge symbols, and the scalars that determine the linear functions are all ring elements. However, a fractional code can also be linear with respect to a module, which is a more general type of linearity. In fact, linear coding over modules generalizes both scalar and vector linear coding over rings. The linear solvability of networks over module alphabets was studied in [9]. In this section, we will show that Theorem 3.9 extends to modules in a natural way.

Definition 4.1. An R-*module* (specifically 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:

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

For brevity, we will sometimes refer to such an R-module as $_R G$. As an example, any ring R acts on its own additive group $(R, +)$ by multiplication in R. Some other examples of modules include

- Any ring R acts on the set of k-vectors over R by scalar multiplication. In fact, when R is a field, this module is a vector space.

- Any ring R acts on any left ideal I of R by multiplication in R.

- The ring of all $k \times k$ matrices over any ring R acts on the set of k-vectors over R by matrix-vector multiplication over R.

- The ring of integers $\mathbf{Z}$ acts on any Abelian group G by repeated addition in G.

- Any subring S of a ring R acts on R by multiplication in R.

- The ring $\mathbf{Z}_n$ acts on $\mathbf{Z}_m$ by multiplication modulo m whenever m divides n.

An edge (or decoding) function

$$f : G^{m_1} \times \cdots \times G^{m_t} \to G^n$$

is linear with respect to the R-module G if it can be written in the form

$$f(x_1, \ldots, x_t) = (A_1 \cdot x_1) + \cdots + (A_t \cdot x_t)$$

where

- $x_i \in G^{m_i}$,

- A_i are $n \times m_i$ matrices over R,

- $+$ is n-vector addition over the Abelian group G, and

- $\cdot$ is matrix-vector multiplication, where multiplication of elements of R by elements of G is the action of the module.

A (k, n) code is *linear over the R-module G* if each message vector is an element of G^k, each edge vector is an element of G^n, and each edge function and each decoding function is linear with respect to $_RG$. The *linear capacity* of a network with respect to an R-module alphabet G is:

$$\mathcal{C}_{lin}(\mathcal{N}, {}_RG) = \sup\{k/n \; : \; \exists \text{ a } (k, n) \text{ linear solution over } {}_RG\}.$$

Since network coding alphabets are presumed to be finite, we restrict attention to modules whose Abelian group is finite; however, in principle, the ring need not be finite. We also note that every fractional linear codes over a ring is a special case of a fractional linear code over a module, where a finite ring acts on its own additive group.

The following lemma is an extension of Lemma 2.3 to include fractional linear codes over modules.

Lemma 4.2. *Let $\mathcal{N}$ be a network, let k, n, and t be positive integers, let G be an R-module, and let $\mathcal{N}^{(k,n)}$ denote the network in Definition 2.1 corresponding to $\mathcal{N}$ and k and n. Then the network $\mathcal{N}$ has a (tk, tn) linear solution over the module $_RG$ if and only if $\mathcal{N}^{(k,n)}$ has a (t, t) linear solution over $_RG$.*

Proof. The proof is identical to the proof of Lemma 2.3, except the messages and edge symbols are elements of G, rather than R. ∎

The following lemma can be shown similarly to [9, Theorem II.10]. In particular, [9, Theorem II.10] shows that for each network $\mathcal{N}$ with a $(1, 1)$ linear solution over the R-module G, there exists a field $\mathbb{F}$ and positive integer t such that $|\mathbb{F}|^t$ divides $|G|$ and $\mathcal{N}$ has a (t, t) linear solution over $\mathbb{F}$. However, the proof of [9, Theorem II.10] can be slightly modified to show the results in Lemma 4.3. I.e. $\mathbb{F}$ and t are the same field and integer, respectively, for every network. Lemma 4.3 is used to show Corollary 4.4, which demonstrates that fractional linear solutions over modules induce fractional linear solutions over fields at the same rate but with possibly larger block sizes.

Lemma 4.3. *Let G be an R-module. Then there exist a finite field $\mathbb{F}$ and positive integer t such that $|\mathbb{F}|^t$ divides $|G|$, and any network with a $(1, 1)$ linear solution over $_RG$ has a (t, t) linear solution over $\mathbb{F}$.*

Corollary 4.4. *Let G be an R-module. Then there exist a finite field $\mathbb{F}$ and positive integer t such that $|\mathbb{F}|^t$ divides $|G|$, and for all $k, n \geq 1$, any network with a (k, n) linear solution over $_RG$ has a (tk, tn) linear solution over $\mathbb{F}$.*

Proof. Let $\mathbb{F}$ and t be the finite field and positive integer, respectively, from Lemma 4.3 corresponding to the R-module G. Then for all positive integers k and n and for each network $\mathcal{N}$,

$\quad \mathcal{N}$ has a (k, n) linear solution over the R-module G

$\quad \implies \mathcal{N}^{(k,n)}$ has a $(1, 1)$ linear solution over the R-module G [from Lemma 4.2]

$\quad \implies \mathcal{N}^{(k,n)}$ has a (t, t) linear solution over $\mathbb{F}$ [from Lemma 4.3]

$\quad \implies \mathcal{N}$ has a (tk, tn) linear solution over $\mathbb{F}$ [from Lemma 2.3] .

$\hfill\blacksquare$

We now prove our main result regarding linear capacity of networks over modules.

Theorem 4.5. *If G is an R-module, then there exists a finite field $\mathbb{F}$ whose characteristic divides $|G|$, such that the linear capacity of any network over the R-module G is at most the network's linear capacity over $\mathbb{F}$.*

Proof. Let $\mathbb{F}$ be the field from Corollary 4.4 corresponding to the R-module G, and let $\mathcal{N}$ be a network. Then whenever $\mathcal{N}$ has a fractional linear solution over $_R G$ at a given rate, $\mathcal{N}$ also has a fractional linear solution over some field $\mathbb{F}$ at the same rate but with possibly larger block sizes. Hence $\mathcal{N}$'s linear capacity over $_R G$ is upper bounded by $\mathcal{N}$'s linear capacity over $\mathbb{F}$. By Corollary 4.4, the field size $|\mathbb{F}|$ divides the module size $|G|$, so the characteristic of $\mathbb{F}$ also divides $|G|$. $\hfill\blacksquare$

4.1   Asymptotic Solvability

We say that a network $\mathcal{N}$ is *asymptotically solvable over $\mathcal{A}$* if for each $\epsilon > 0$, there exist $k, n \geq 1$ such that $k/n \geq 1 - \epsilon$ and $\mathcal{N}$ has a (k, n) solution over $\mathcal{A}$. I.e. a rate arbitrarily close to, or above, 1 is attainable. A network which is asymptotically solvable but not solvable was demonstrated in [12], and solvable networks were demonstrated in [7] and [11] that are not asymptotically linearly solvable over any finite field. The following corollary demonstrates that such networks are additionally not asymptotically linearly solvable over any module (or ring).

Corollary 4.6. *If a network is asymptotically linearly solvable over some module, then it must be asymptotically linearly solvable over some finite field.*

Proof. We will prove the contrapositive of this corollary. Suppose $\mathcal{N}$ is a network that is not asymptotically linearly solvable over any finite field. Then for each finite field $\mathbb{F}$, there exists $\epsilon > 0$ such that $\mathcal{N}$'s linear capacity over $\mathbb{F}$ is at most $1 - \epsilon$. Then, by Theorem 4.5, for each R-module G, there exists a field $\mathbb{F}$ such that $\mathcal{N}$'s linear capacity over $_R G$ is upper bounded by $1 - \epsilon$. Hence $\mathcal{N}$ cannot be asymptotically linearly solvable over $_R G$, since its linear capacity over $_R G$ is bounded away from (i.e. below) 1. $\hfill\blacksquare$

5   Concluding Remarks

Linear network codes over finite rings 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, this broader class of codes does not offer an improvement compared to linear codes over fields.

This particularly contrasts with the network solvability problem where we demonstrated certain cases where a ring alphabet can offer scalar linear solutions when a field alphabet cannot.

References

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

[2] A. Blasiak, R. Kleinberg, and E. Lubetzky, "Lexicographic products and the power of non-linear network coding," *IEEE Symposium on Foundations of Computer Science (FOCS)*, Palm Springs, CA, pp. 609 – 618, 2011.

[3] W. Brown, *Matrices over Commutative Rings*, Taylor & Francis, 1992.

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

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

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

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

[8] J. Connelly and K. Zeger, "Linear network coding over rings – Part I: Scalar codes and commutative alphabets," to appear in *IEEE Transactions on Information Theory*, Available on-line at: `http://ieeexplore.ieee.org/document/7908937/`.

[9] J. Connelly and K. Zeger, "Linear network coding over rings – Part II: Vector codes and non-commutative alphabets," to appear in *IEEE Transactions on Information Theory*, Available on-line at: `http://ieeexplore.ieee.org/document/7909041/`.

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

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

[12] R. Dougherty, C. Freiling, and K. Zeger, "Unachievability of network coding capacity," *IEEE Transactions on Information Theory (joint issue with IEEE/ACM Transactions on Networking)*, vol. 52, no. 6, pp. 2365 – 2372, June 2006.

[13] R. Dougherty, C. Freiling, and K. Zeger, "Networks, matroids, and non-Shannon information inequalities," *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 1949 – 1969, June 2007.

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

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

[16] J.B. Ebrahimi and C. Fragouli, "Algebraic algorithms for vector network coding," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 996 – 1007, February 2011.

[17] A. Gómez, C. Mejía, and J. Montoya, "Network coding and the model theory of linear information inequalities," *International Symposium on Network Coding*, Aalborg, Denmark, pp. 1 – 6, 2014.

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

[19] N. Harvey, R. Kleinberg, and A. Rasala Lehman, "On the capacity of information networks," *IEEE Transactions on Information Theory (joint issue with IEEE/ACM Transactions on Networking)*, vol. 52, no 6, pp. 2345 – 2364, June 2006.

[20] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413 – 4430, October 2006.

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

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

[23] S. Kamath, V. Anantharam, D. Tse, C.C. Wang, "The two-unicast problem," to appear in *IEEE Transactions on Information Theory*, Available on-line at: `http://ieeexplore.ieee.org/document/7744471/`.

[24] M. Langberg and A. Sprintson, "On the hardness of approximating the network coding capacity," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1008 – 1014, February 2011.

[25] S.-Y.R. Li, R.W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371 – 381, February 2003.

[26] S.-Y.R. Li, Q. Sun, and S. Ziyu, "Linear network coding: theory and algorithms," *Proceedings of the IEEE,* vol. 99, no. 3, pp. 372–387, March 2011.

[27] S. Lovett, "Linear codes cannot approximate the network capacity within any constant factor," *Electronic Colloquium on Computational Complexity*, vol. 21, no. 141, pp. 1 – 19, 2014.

[28] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker Inc., 1974.

[29] B.R. McDonald, *Linear Algebra over Commutative Rings*, Taylor & Francis, 1984.

[30] M. Médard, M. Effros, T. Ho, and D. Karger, "On coding for non-multicast networks," *Conference on Communication Control and Computing*, Monticello, IL, October 2003.

[31] V. T. Muralidharan and S. Rajan, "Linear network coding, linear index coding, and representable discrete polymatroids," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 4096 – 4119, July 2016.

[32] L. Song, R.W. Yeung, and N. Cai, "Zero-error network coding for acyclic networks," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3129 – 3139, December 2003.

[33] Q. Sun, S.-Y.R. Li, and Z. Li, "On base field of linear network coding," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7272 – 7282, December 2016.

[34] Q. Sun, X. Yang, K. Long, X. Yin, and Z. Li, "On vector linear solvability of multicast networks," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 5096 – 5107, September 2016.

[35] Q. Sun, X. Yin, Z. Li, and K. Long, "Multicast network coding and field sizes," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6182 – 6191, November 2015.

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

[37] M. F. Wong, M. Langberg, and M. Effros, "On a capacity equivalence between multiple multicast and multiple unicast," *Allerton Conference on Communication, Control, and Computing*, Monticello, IL, pp. 1537 – 1544, 2013.

[38] M. F. Wong, M. Langberg, and M. Effros, "Linear capacity equivalence between multiple multicast and multiple unicast," *IEEE International Symposium on Information Theory*, Honolulu, HI, pp. 2152 – 2156, 2014.

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

[40] R.W. Yeung, "A framework for linear information inequalities," *IEEE Transactions on Information Theory*, vol. 43, no. 6, pp. 1924 - 1934, November 1997.

[41] W. Zeng, V. R. Cadambe, and M. Médard, "Alignment-based network coding for two-unicast-Z networks," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3183 – 3211, June 2016.